Schieb Report

Ausgabe 2019.42

Mit mehreren Leuten WhatsApps austauschen: Gruppen

WhatsApp ist eine der schnellsten Arten, Verabredungen zu treffen und Informationen auszutauschen. Im Standard findet die Kommunikation in einer direkten Unterhaltung zwischen zwei Personen und ihren Smartphones statt. Wenn Sie aber beispielsweise ein Treffen oder eine Patrty organisieren wollen, dann macht es Sinn, das gleich mit allen Teilnehmern zu machen. Im Standard erlaubt WhatApp das aber nicht. Das heisst aber nicht, dass es nicht geht!

Statt - wie es intuitiv wäre - mehrere Teilnehmer zum Chat hinzuzufügen, müssen Sie eine Gruppe anlegen. Das klingt komplizierter, als es tatsächlich ist: Tippen Sie in der Chat-Ansicht oben rechts auf **Neue Gruppe**. Dann geben Sie der Gruppe einen sprechenden Namen. Dieser wird allen Teilnehmern angezeigt, als wäre die Gruppe ein einzelner Kontakt. Es macht als Sinn, diesen sprechend zu wählen!

Wählen Sie danach aus den Kontakten diejenigen aus, die in die Gruppe aufgenommen werden sollen. Das können Sie durch Antippen und Rollen durch die Liste Ihrer Kontakte machen. Ein Tippen auf **Erstellen** schließt den Vorgang ab. Jeder Teilnehmer bekommt nun von WhatsApp eine Information, dass er der Gruppe hinzugefügt wurde und kann das natürlich auch ablehnen.

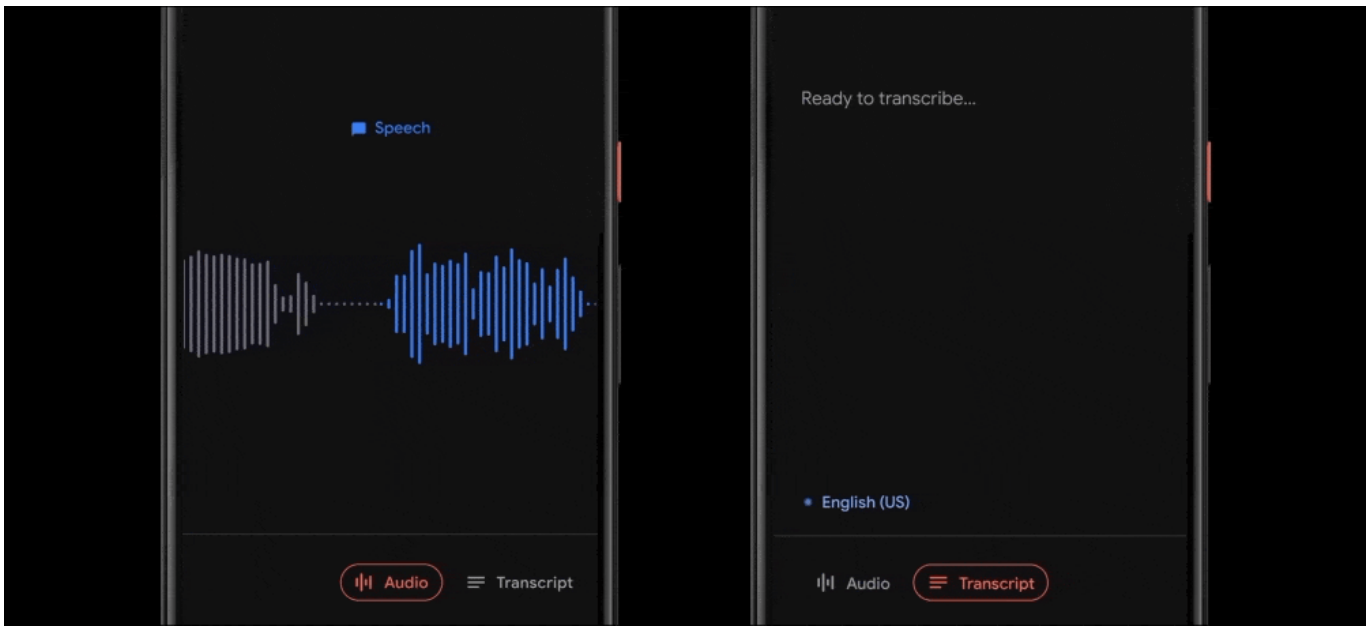
Im Chat selbst fällt Ihnen dann nicht mehr auf, dass es sich um eine Gruppe und nicht um einen einzelnen Kontakt handelt. Einzig die Tatsache, dass mehrere Leute antworten, unterscheidet die Gruppe von einem normalen Chat.

Google Pixel 4: Assistant ohne Cloud-Anbindung

Google hat gerade diverse neue Hardwareprodukte vorgestellt - darunter auch das neue Smartphone Google Pixel 4. Was mir besonders gut gefällt: Googles Smartphone versteht jetzt viele Anweisungen ganz ohne Cloud-Anbindung. Heureka: Das ist gut für den Datenschutz.

Ich finde: Neben dem iPhone ist das Google Pixel das mit Abstand beste Smartphone am Markt. Die Kamera ist klasse. Das Design kann sich sehen lassen. Und jetzt hat Google noch ein paar mehr Funktionen entwickelt, die spannend sind.

Der Radar erkennt Gesten - und so lässt sich das Smartphone mit Handbewegungen bedienen. Das kann durchaus sinnvoll sein - ist in meinen Augen aber nicht das Wichtigste.



Vorbidliches Konzept: Zuhören - aber nicht abhören

Ein regelrechtes Killer Feature ist die neue Art der Spracherkennung. Google ist es gelungen, die KI für die Sprachanalyse derart einzudampfen, dass sie **im Smartphone** funktioniert - ohne Cloud-Anbindung.

Zu verdanken ist das einem selbst entwickelten Chip, den Pixel-Neural-Core. Dieserer Pixel-Neural-Core-Chip unterstützt so nebenbei ber auch die Kamera und hilft bei der 3D-Gesichtserkennung.

Viele Anweisungen werden verstanden, ohne dass eine Verbindung mit Google-Servern hergestellt werden muss. Das bedeutet: Deutlich mehr Datenschutz und Privatsphäre, da Google viel weniger erfährt als bislang. Einen Song suchen, eine App starten, einen Termin eintragen - das geht offline.

Für manche Anweisungen ist nach wie vor eine Online-Anbindung erforderlich, etwa wenn Daten abgerufen werden müssen. Das leuchtet ein.

Ich bin gespennt, ob andere Hersteller - insbesondere Amazon - diesem Beispiel folgemn werden.

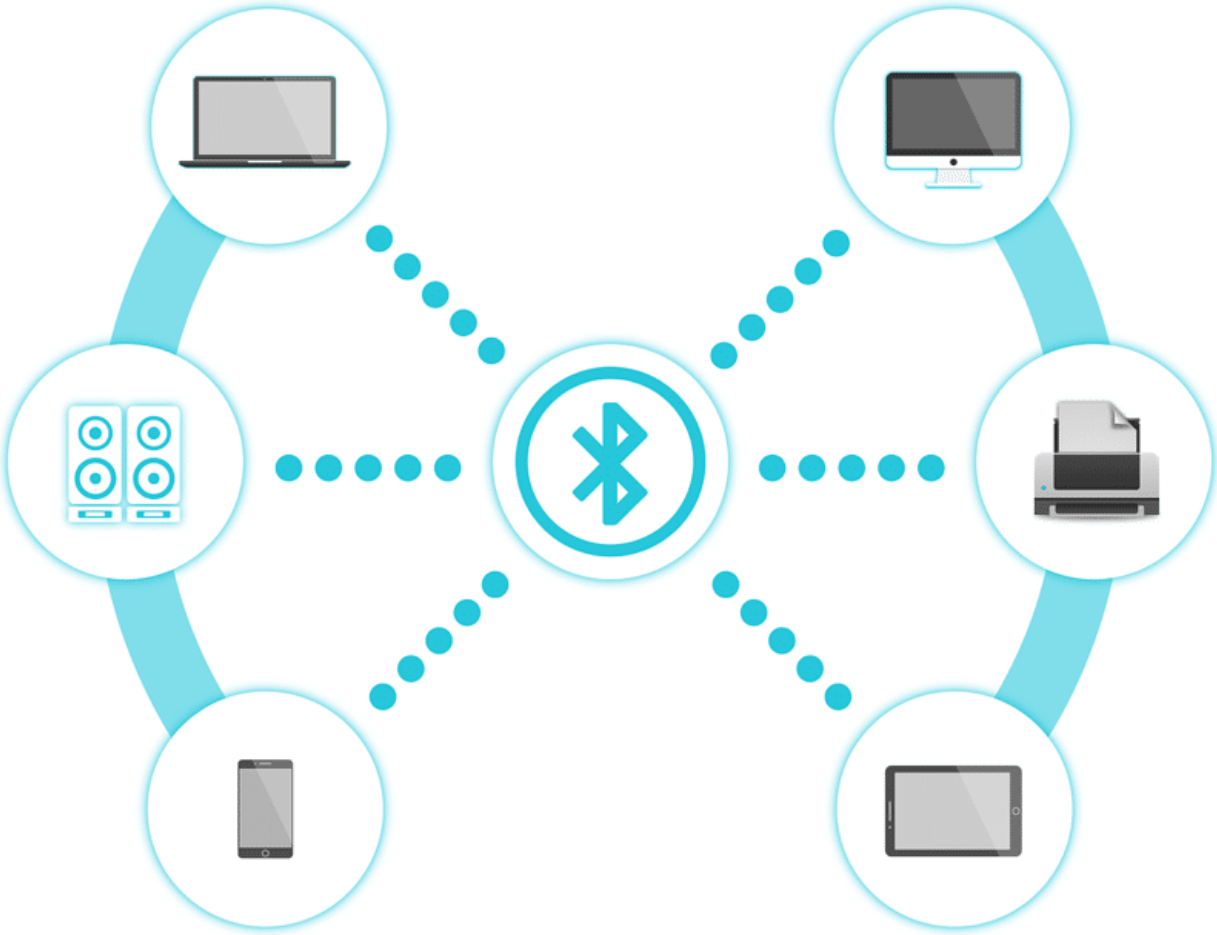
Sicherheit von Bluetooth: So lassen sich Angreifer aussperren

Bluetooth ist ein Funkstandard, der die schnelle und bequeme Verbindung von Geräten ermöglicht - um Daten auszutauschen. Heute funkt Bluetooth schneller denn je - und ist deshalb auch in vielen Geräten im Einsatz. Wir Nutzer merken davon in der Regel nichts oder nicht viel. Allerdings können Bluetooth-Verbindungen auch ein Sicherheitsrisiko darstellen.

Am Anfang war Bluetooth vor allem eine Möglichkeit, Geräte über kurze Distanz miteinander zu verbinden. Bluetooth als Kabelersatz und Kurzstrecken-Funk. Kabellose Headsets, Mäuse oder Tastaturen lassen so schnell und einfach mit dem Smartphone oder Tablet verbinden.

Auch im Auto ist Bluetooth eine schnelle Möglichkeit, die Freisprecheinrichtung einzurichten. Bluetooth ist ein Standard für die kabellose Datenübertragung, auch beispielsweise zwischen zwei Smartphones, um Dateien auszuscuahen.

Heute funktioniert Bluetooth auch über größere Distanzen. Das macht die Verbindung angreifbarer von außen. Es sind, insbesondere im Internet of Things (IoT), besondere Sicherheitsvorkehrungen notwendig: Nur dann bietet die kabellose Verbindung weniger Angriffsfläche für Hacker.



Viele Anwendungsmöglichkeiten

Das Internet der Dinge nimmt in unserem Alltag einen immer größeren Stellenwert ein: Immer mehr Geräte sind vernetzt und ständig online. Genau das macht die Bluetooth-Verbindung neben WLAN und NFC (Near Field Communication) zum wichtigen Verbindungsstandard. Damit funktioniert der Datenaustausch zwischen Endgeräten leicht, beispielsweise zwischen Smartphone und Wearables wie Fitness-Armbänder.

Es ist mittlerweile nur noch ein Mythos, dass Bluetooth und die kurze Reichweite keine Angriffsfläche mehr bieten für Hacker. Angreifer können – im Gegensatz zu Attacken im Internet – zwar nur aus kurzer Entfernung erfolgreich sein. Das macht die Verbindung aber nicht weniger angreifbar. Denn die neuen Versionen ab Bluetooth 5 haben eine viermal so große Reichweite wie bisher. Bluetooth 5 gewährleistet eine Reichweite von bis zu 40 Metern, wie das Magazin Connect berichtet. Diese Reichweite können User mit Headsets, Freisprecheinrichtungen, Fitnessarmbändern, Lautsprechern und Ähnlichem nutzen.

Neben der größeren Reichweite haben die neuen Geräte auch eine größere Bandbreite. Das hat zur Folge, dass auch große Datenmengen in kurzer Zeit von einem auf ein anderes Gerät übertragen werden können. Das hat dazu beigetragen, dass bluetoothfähige Geräte an

Beliebtheit gewinnen. Die Verbreitung steigt. Bis 2020 soll es fast 14 Milliarden bluetoothfähige Geräte geben.

Die Angriffsmöglichkeiten sind vielfältig

Leider ist es auch so, dass weit verbreitete Geräte zum beliebten Angriffsziel werden. Bei Bluetooth ist eine ganz Reihe von Attacken möglich.

- **Bluebugging** – dabei versuchen Hacker Endgeräten Befehle zu erteilen und dabei unerkannt zu bleiben. So können sie mit Bluebugging Textnachrichten senden, Anrufe tätigen, Gespräche mithören oder die Kontakte im Adressbuch ausspionieren.
- **Bluejacking** – das ist eine Art von Spam. Dabei senden Unbefugte Daten an Bluetooth-Geräte, die keiner will. Das ist beispielsweise in Innenstädten weit verbreitet, um Werbung für die Geschäfte in Reichweite zu machen. Die Händler schicken dazu Plakate oder Schaufensterwerbung per Bluetooth an Passanten. Nicht immer ist der Zweck der Nachrichten harmlos, wie bei der Werbung. Es können auch Spam-Mails dahinterstecken, mit denen die Absender versuchen am Ende Malware auf den Endgeräten zu installieren.
- **Bluesnarfing** – das ist der Versuch gezielt Daten aus gespeicherten Nachrichten, dem Telefonbuch oder der Kontaktliste zu stehlen. Schwachstellen für diese Art von Angriffen haben insbesondere ältere bluetoothfähige Geräte.
- **DoS-Attacken oder Denial-of-Service-Attacken** – sie richten sich direkt an die Bluetooth-Schnittstelle. Die Angreifer schicken beispielsweise massenhaft Kontaktanfragen und stören damit die Schnittstelle, was zu einem kurzfristigen Totalausfall der Geräte führen kann.

Sicherheitsfunktionen für die Bluetooth-Verbindung

Die Verbreitung des Internets der Dinge, wie beispielsweise im Smart-Home, trägt wesentlich dazu bei, dass es mehr und mehr bluetooth-fähige Geräte in der Küche und im Haushalt allgemein gibt. Doch fehlende Möglichkeiten Sicherheitssoftware zu installieren, macht die Technologie so angreifbar. Deshalb muss Bluetooth selbst zu mehr Sicherheit beitragen.

Eine wesentliche Sicherheitsfunktion ist die Verschlüsselung der Daten und eine Autorisierung und Authentifizierung bei der Verbindungsaufnahme. Je nach Sicherheitsstufe können zwei bluetoothfähige Geräte nur mittels Pairing eine Verbindung aufbauen. Diese Verbindung lässt sich in den meisten Fällen mit einer PIN schützen. Diese PIN ist gerätespezifisch und gehört nicht zum Benutzer. Sie ist notwendig, um den Schlüssel für die Verbindung zu berechnen.

Lässt sich diese PIN nicht ändern, was bei IoT-Geräten in der Regel so ist, kann dadurch ein großes Sicherheitsrisiko entstehen. Was das Internet der Dinge genau ist, erklärt das BSI (Bundesamt für Sicherheit in der Informationstechnik) auf seiner Internetseite.

Nicht änderbare PIN ist gefährlich

Potenzielle Angreifer können für bestimmte Geräte die Werkseinstellungen kennen und damit auch die PIN. Nutzer sollten diese PIN, sofern möglich, immer zuerst ändern, bevor sie das Gerät benutzen. Es gibt bestimmte Produktklassen und sehr viele Geräte, die eine nicht veränderbare PIN haben. Dann entspricht die PIN einem fest zugewiesenen Geräteschlüssel, der im Benutzerhandbuch steht. Die PIN ist dann meistens mit 0000 angegeben. Das ist zum einen eine viel zu kurze PIN und zum anderen ist sie auch bei jedem Modell dieses speziellen Produktes gleich.

Tipps für mehr Sicherheit bei Bluetooth-Verbindungen

Bei Bluetooth-Angriffen geht es in erster Linie um persönliche Daten, wie gespeicherte Nachrichten, E-Mails, Termine oder Kontakte. Denkbar sind auch unbefugte Telefonate auf Kosten eines anderen.

Angreifer können Malware auf das Endgerät schleusen. Das ist vor allem dann gefährlich, wenn die Schnittstelle für andere Geräte sichtbar ist. Das bedeutet, dass andere Geräte die aktive Schnittstelle bei der Suche nach bluetoothfähigen Geräten finden können. Das ist in öffentlichen Bereichen besonders gefährlich, wie in Fußgängerzone, am Bahnhof oder am Flughafen.

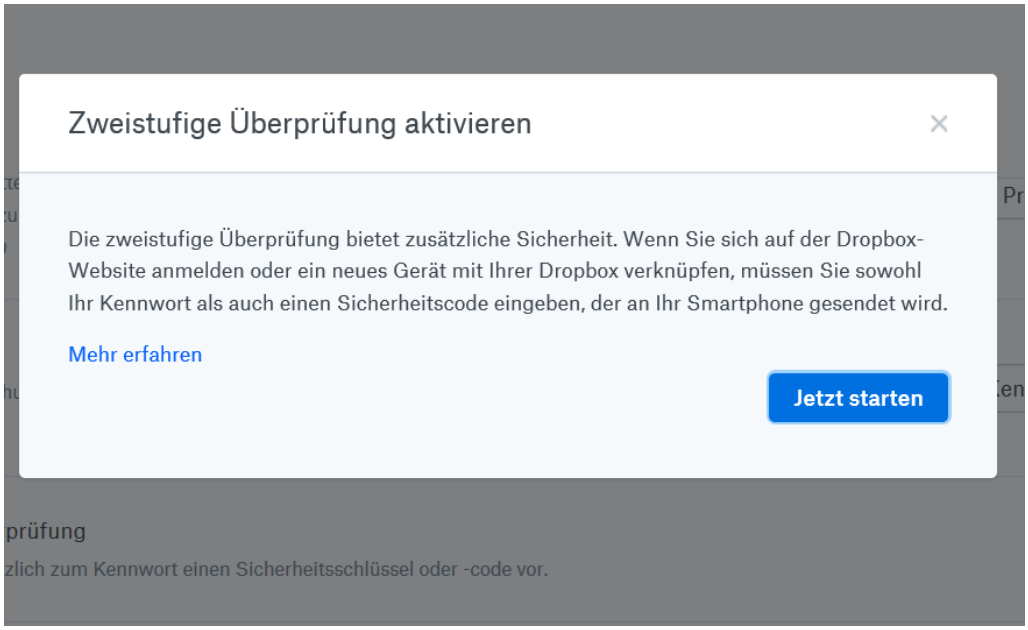
Viele Angreifer nutzen Schwachstellen im System aus, weshalb es wichtig ist, das Betriebssystem der Endgeräte regelmäßig zu aktualisieren. Die Umsetzung dieser Tipps sorgt für mehr Sicherheit bei der Nutzung von Bluetooth-Verbindungen:

- Bei Bluetooth-Aktivierung sollten Nutzer das Gerät in den unsichtbaren Modus versetzen.
- Bluetooth-Schnittstelle nach Gebrauch immer deaktivieren.
- Keiner Datenübertragung aus unbekannten Quellen zustimmen.
- Malware-Schutz auf dem Endgerät installieren. Wenn die Endgeräte keine Software-Installation erlauben, lassen sich die Geräte im IoT durch einen Malware-Schutz im Internet-Gateway schützen.
- Mit unbekannten Geräten sollten Nutzer keine Verbindung erlauben.
- Pairing in öffentlichen Bereichen sollten Nutzer vermeiden.

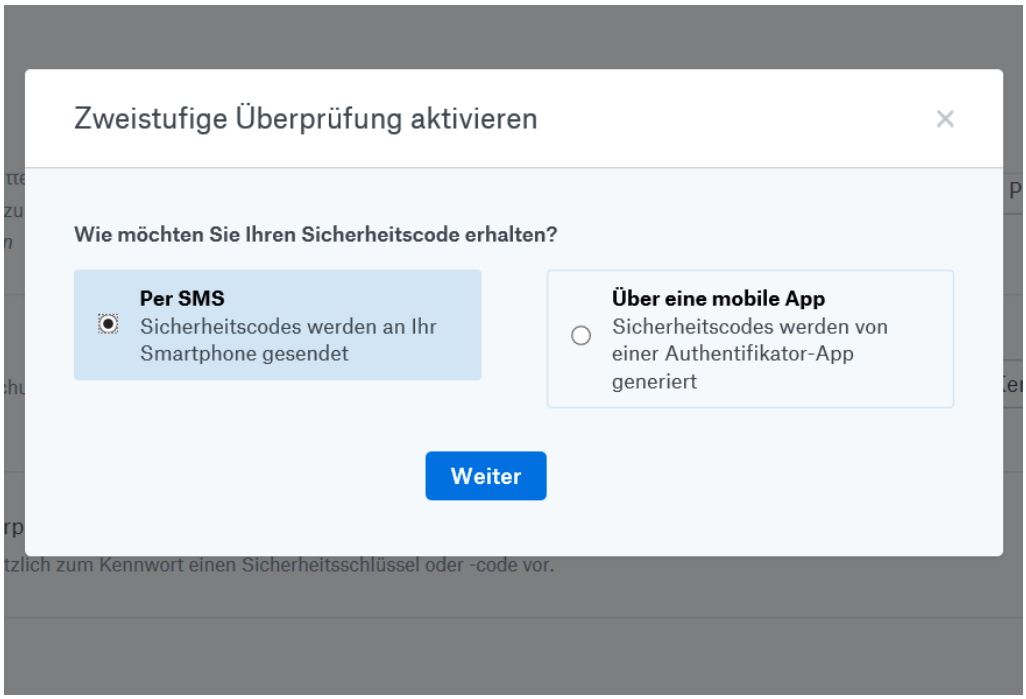
Dropbox mit Zwei-Faktor-Authentifizierung schützen (2FA)

Wenn Sie Daten in einem externen Cloudspeicher ablegen, dann wollen Sie möglichst viel Sicherheit dafür erreichen. Viele der Cloud-Anbieter bieten neben dem normalen Schutz des Kontos durch Benutzername und Passwort auch die zusätzliche Absicherung durch einen zweiten Faktor. Diese können Sie in wenigen Schritten einrichten.

Wechseln Sie in Ihrem Browser auf die Sicherheits-Seite von Dropbox und melden Sie sich an. Im Reiter **Sicherheit** finden Sie in der Mitte einen Schalter, mit dem Sie die Zwei-Faktor-Authentifizierung (2FA) aktivieren können. Schalten Sie sie ein. Dropbox fragt nun auch Sicherheitsgründen nach Ihrem Konto-Passwort.



Sie können nun zwischen dem Zusenden des Codes per SMS oder der Ausgabe in einer Authenticator-App wählen. Der Bequemlichkeit nach bietet es sich eher an, die SMS-Variante zu wählen. Bei dieser müssen sie nun einmalig die Rufnummer eingeben. Diese bleibt in Ihrem Konto gespeichert.



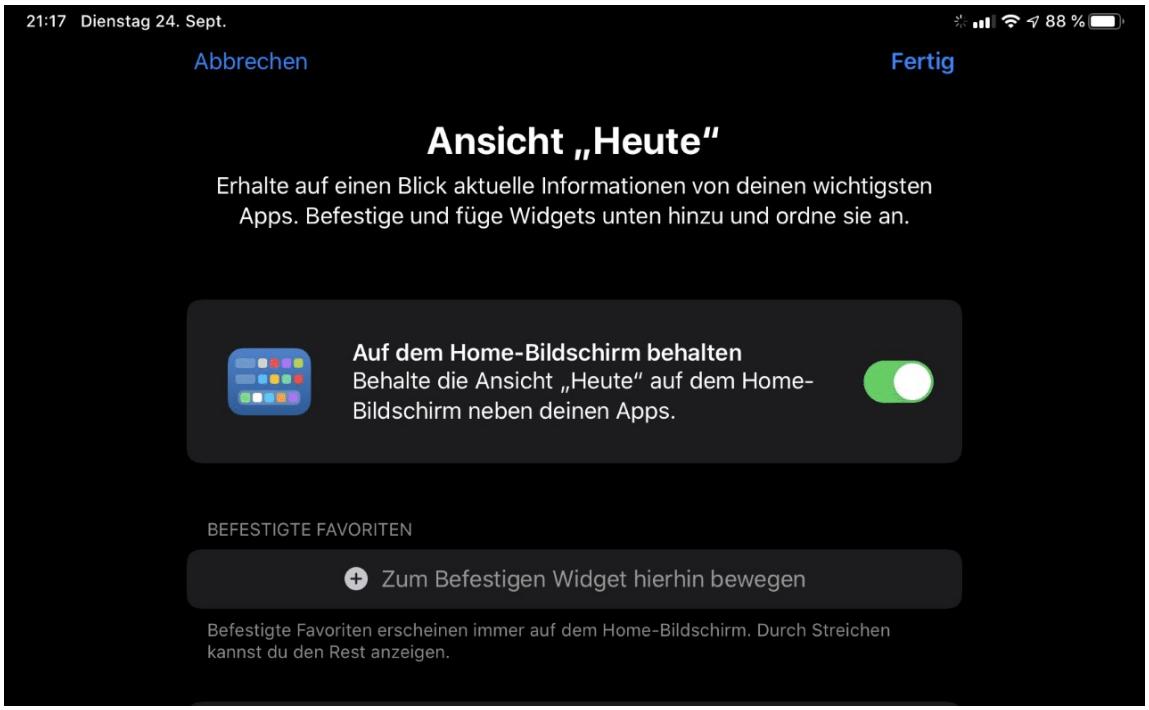
Zur Aktivierung der 2FA schickt Ihnen Dropbox jetzt einen sechsstelligen Code per SMS. Geben Sie diesen in die Eingabemaske ein.

Bei jeder weiteren Anmeldung an die Dropbox bekommen Sie an die angegebene Handynummer wieder einen Code. Es nützt einem Angreifer also nichts mehr, wenn er nur Ihr Kennwort hat. Ohne den jedesmal anderen Code ist keine Anmeldung mehr möglich. Ihre Dateien sind damit deutlich sicherer.

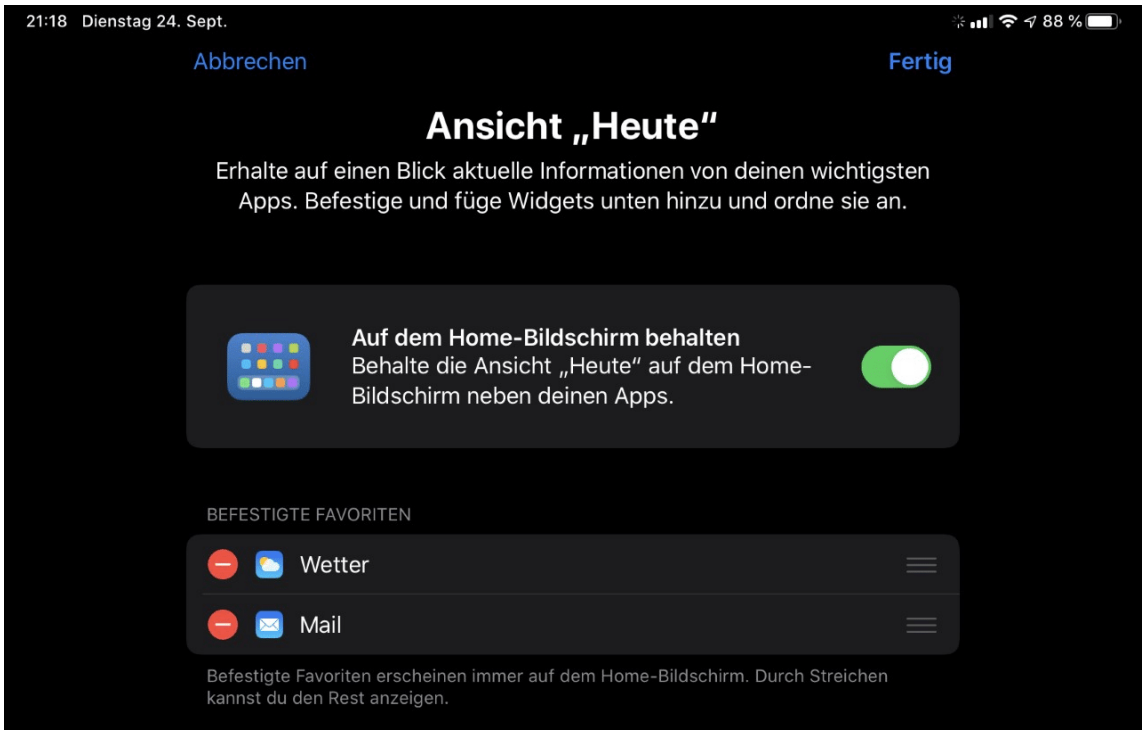
Widgets auf dem Homescreen in iOS13 platzieren

Mit iOS13 ist auf dem iPad endlich mehr Platz für Informationen: Apple hat das Gitter für die App-Symbole verengt. Offensichtlich hat das Begehrlichkeiten geweckt, denn wie bei Android lassen sich jetzt Widgets auf der ersten Seite des Homescreens platzieren. Auch diese Funktion ist allerdings tief versteckt und nicht unbedingt intuitiv zu erreichen. Aber dafür haben Sie ja uns!

Die Widgets sind bei iOS nichts wirklich Neues: Wischen Sie auf dem ersten Bildschirm des HomeScreens nach links, dann finden Sie diese schon seit einiger Zeit und können sie konfigurieren. Neu in iOS 13 allerdings: Sie können Sie direkt auf dem Homescreen platzieren. Dazu wischen Sie von der ersten Seite einmal nach links. Aktivieren Sie dann den neuen Schalter **Auf dem Home-Screen behalten**.



Sie können nun aus der Liste der verfügbaren Widgets die in den Bereich **Befestigte Favoriten** ziehen. Um ein Widget zu löschen, klicken Sie auf das rote Stopp-Schild. Zum Verschieben der Widgets in der Reihenfolge halten Sie den Finger auf die drei Linien rechts neben dem Widget und bewegen Sie es nach unten oder oben.



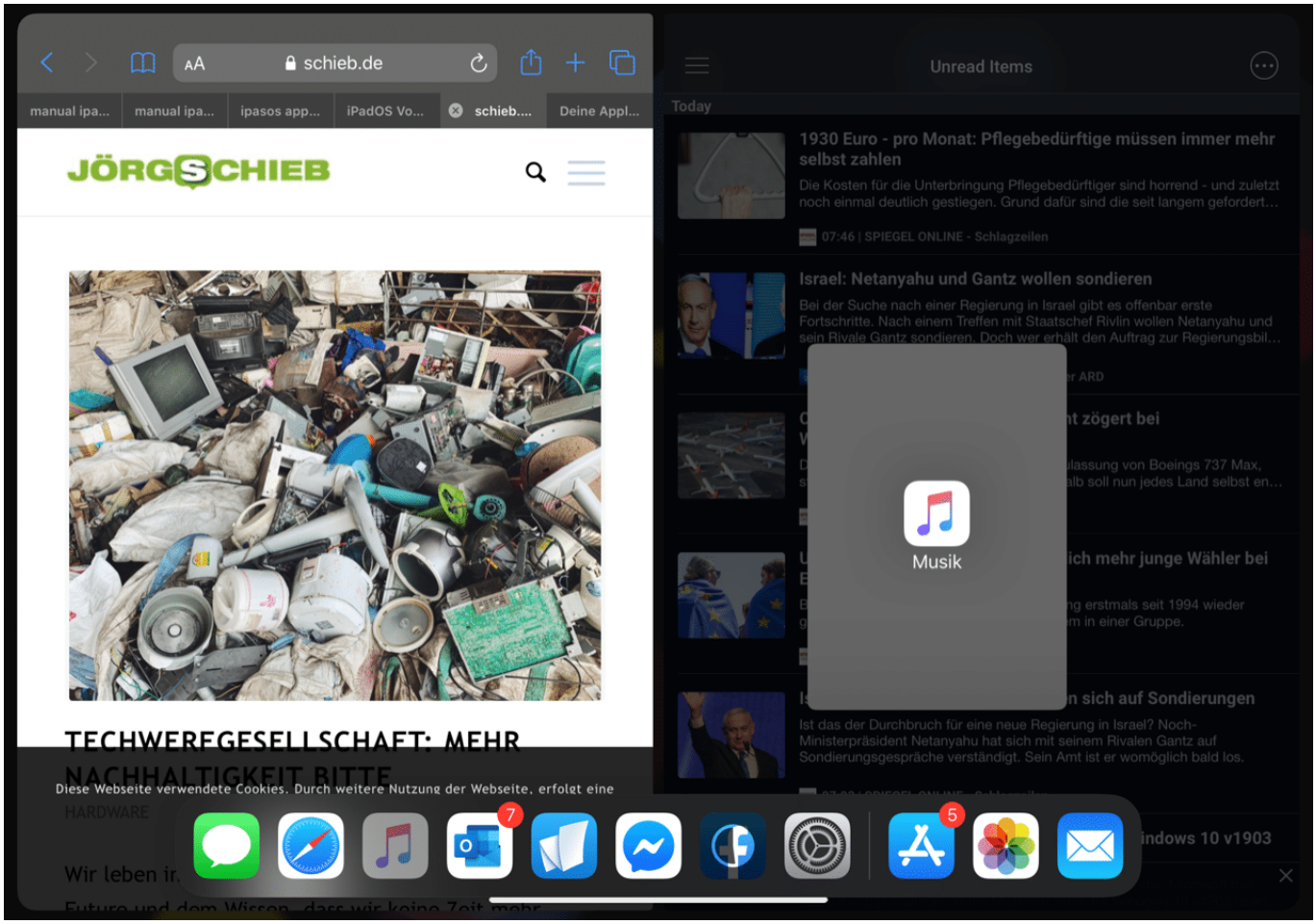
Die Widgets werden konsequent nur dann angezeigt, wenn Sie das iPad im Querformat halten. Dann können Sie auch durch die untereinander angeordneten Widgets durchscrollen.

Splitscreen und Spaces bei iOS13 nutzen

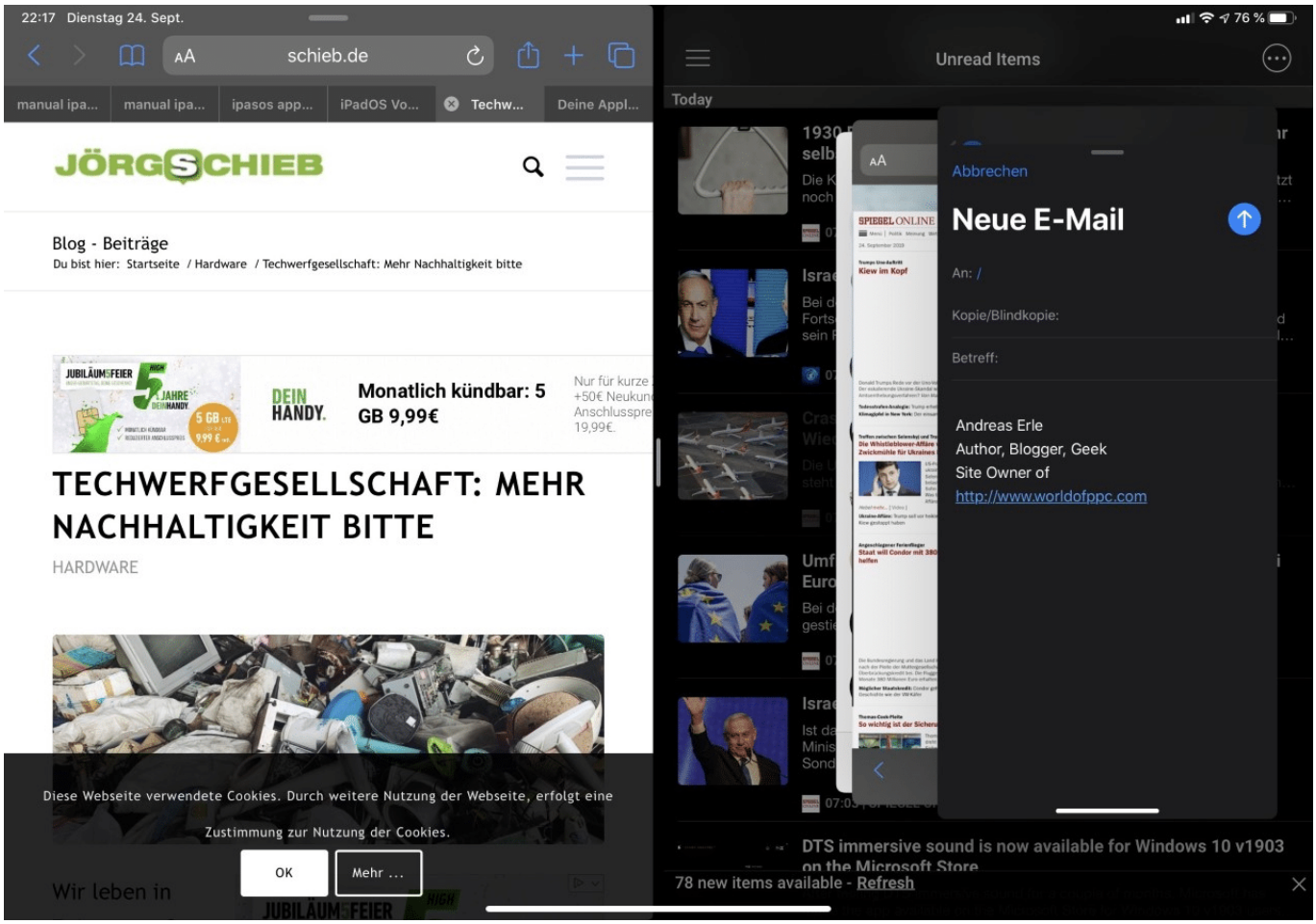
iOS13 geht einen weiteren Schritt dahin, das iPad als echtes Produktivitätswerkzeug zu etablieren. Zusammen mit einer externen Tastatur und einem Stuft können Sie eine Vielzahl der Aufgaben erledigen, für die Sie sonst ein Notebook verwenden würden. Nun haben Sie keinen zweiten Monitor, und der Platz auf dem internen Display ist beschränkt. Dafür hat Apple den Splitscreen und die so genannten Spaces eingeführt. Die Bedienung allerdings ist alles andere als selbstsprechend. Wir zeigen Ihnen, wie es geht.

Um den Bildschirm zu teilen, starten Sie eine der beiden Apps, die in der geteilten Ansicht dargestellt werden sollen. Wischen Sie dann von unten über den Bildschirmrand nach oben. Wichtig: Der Finger darf nur einen kurzen Weg zurücklegen. Gerade so weit, dass das Dock eingeblendet wird. Dann halten Sie den Finger auf das Symbol der zweiten App im Dock. Nach ca. einer Sekunde ziehen Sie das App-Symbol an den linken (oder rechten) Rand des Bildschirms. Das Timing ist hier entscheidend, bedarf aber einer gewissen Übung.

Damit wird die zweite App in die jeweilige Bildschirmhälfte gepackt. Im Standard im Verhältnis 50:50. Sie können durch Ziehen des Trennstriches das Verhältnis auch auf 25:75 oder 75:25 verändern.



Um nun weitere Apps im Zugriff zu haben, führen Sie die ersten beiden Schritte mit der neuen App erneut aus. Diesmal ziehen Sie das Symbol aber mitten auf den Trennstrich zwischen den beiden Apps. Die dritte App wird nun als freischwebender Streifen angezeigt. Wiederholen Sie diesen Vorgang so oft, wie Sie Apps im Schnellzugriff haben wollen.



An der freischwebenden App sehen Sie unten einen Strich. Nicht umsonst erinnert der an den im Hauptbildschirm, der Zugriff auf die laufenden Apps erlaubt: Wischen Sie nach oben, und sie bekommen das Karussell der zusätzlichen Apps auf, in dem Sie wie gewohnt zwischen Apps wechseln können und durch nach oben Wischen Apps beenden können.

Daten von einem zum anderen iPhone übertragen

Es ist mal wieder Zeit, auf das neueste iPhone umzusteigen? Oder auf Grund einer Reparatur das Gerät eher gezwungen zu wechseln? Was auch immer der Auslöser ist, Aufwand bedeutet der Umstieg allemal. Allerdings können Sie diesen Aufwand mit wenigen Schritten minimieren. Wir zeigen Ihnen, wie.

Der allereinfachste Weg bedarf nicht mal einer vorherigen Datensicherung: Haben beide iPhones mindestens iOS 11 als Betriebssystem, dann können Sie direkt zwischen den Geräten alle Daten, Einstellungen und Apps übertragen. Legen Sie beide Geräte nebeneinander. Bei dem alten Gerät sollte auf jeden Fall WLAN und Bluetooth eingeschaltet sein.

Das alte iPhone erkennt das neue und bietet direkt die Datenübertragung an. Tippen Sie auf **Weiter** und folgen Sie den Anweisungen. Nach kurzer Zeit sind die Daten übertragen. Das eine oder andere Passwort bzw. die Registrierung müssen Sie noch nachziehen, das war es aber schon. Wichtig: Auch die iTunes-Partnerschaft wird übertragen. Wenn Sie das neue Gerät an Ihre PC oder Mac anschließen, dann wird es direkt erkannt und wie das alte synchronisiert.

Sollte die direkte Übertragung nicht mehr möglich sein, dann müssen Sie auf ein iTunes- oder iCloud-Backup ausweichen. Schalten Sie diese in iTunes auf PC oder Mac unter **Backups automatisch erstellen** ein. Wählen Sie das Backup in **iCloud**, denn das können Sie direkt auf dem iPhone wiederherstellen.

Wenn Sie das neue Gerät dann neu einrichten, können Sie im Einrichtungsprozess direkt auswählen, dass Sie es nicht komplett neu einrichten, sondern aus dem Backup wiederherstellen wollen.

Was, wenn der US-Präsident die Cloud ausknipst?

Twitter wird US-Präsident Donald Trump wohl eher nicht abschalten (lassen). Denn wer könnte dann noch seine Tweets lesen? Aber die Cloud - warum nicht? Erst vor kurzem hat Donald Trump ein komplettes Land auf die Bann-Liste gesetzt: Venezueala.

Leichter fallen ihm Entscheidungen wie diese: Im August hat der US-Präsident die Exekutivanweisung 13884 unterzeichnet. Sie verbietet - zusammengefasst - jede Art von Transaktion und Dienstleistungen von US-Unternehmen mit Individuen aus Venezuela. Die Folge: Adobe knipst in Venezuela die Lichter aus.

Venezuela wird von der Adobe-Cloud ausgeschlossen

User aus Venezuela können ab 29. Oktober nicht mehr auf ihre in der Creative Cloud gespeicherten Fotos, Illustrationen, Skizzen, Videos oder Dokumente zugreifen. Darüber hinaus werden Adobe-Apps ihren Dienst versagen, da ihre Gültigkeitsdauer (in Abos) nicht mehr verlängert werden kann. Der komplette Kreativbereich in Venezuela wird damit ausgebremst. Weil Adobe sich an die Anordnungen aus Washington D.C. hält - was sollen sie auch sonst anderes machen.

Nicht das erste Mal, dass über die digitale Welt Handelsstreitigkeiten ausgefochten werden. Wir erinnern uns: Huawei-Smartphones dürfen von Google nicht mehr mit Software oder Updates versorgt werden. Auch das ist ein erheblicher Einschnitt - ohne jede Vorankündigung.

Diese Entwicklung macht ein erhebliches Problem deutlich: Wir alle sind viel zu abhängig von

politischen Entscheidungen in den USA. Wir nutzen alle Android, iOS oder Windows. Wir verwenden Apps aus der Cloud. Wir speichern unsere Dokumente in der Cloud. Was, wenn Donald Trump einfallen sollte, auf Europa böse zu sein - und mit einem Federstrich anordnet, den Cloud-Stecker zu ziehen?

Cloud aus = Chaos total

Termine wären verschwunden. Kontakte weg. Wir könnten nicht mehr auf Office-Dokumente in der Cloud zugreifen - und die Apps würden schweigen. Mit einem Wort: Es würde schlichtweg Chaos ausbrechen. Die Fälle Huawei und Venezuela zeigen, dass solche Szenarien nicht ins Reich der Phantasie gehören, sondern einen schwindelerregend realen Charakter haben. Alles ist möglich.

Dessen sollten wir uns bewusst werden - schnell und unbedingt. Wenn schon Cloud, dann muss die Cloud eben in Europa betrieben werden. Es sollte durch entsprechende Gesetze unmöglich sein, dass der Betrieb einer Cloud eingestellt oder der Zugang zu Daten unmöglich gemacht werden kann. All das lässt sich durch entsprechende technische Vorkehrungen durchaus erreichen. Man muss es nur wollen. Und dafür ist ein Umdenken erforderlich.

Natürlich: Wir können uns auch eine eigene private Cloud einrichten. Oder noch mal besser hinhören, was WWW-Erfinder Tim Berners-Lee zu sagen hat. Er plädiert nämlich für eine Dezentralisierung des Webs. Das würde gleich mehrere Probleme lösen: Es würde die Macht der großen Cloud-Player schwächen - und auch mehr Beständigkeit beim Zugriff auf die eigenen Daten sicherstellen.

https://soundcloud.com/user-999041145/usa-betreiben-digitalen-kolonialismus

Live-Videos nicht vom NetzDG erfasst

Plattformen sind heute durch das Netzwerkdurchsetzungsgesetz (NetzDG) dazu verpflichtet, straftrechtlich relevante Inhalte nach Kenntnis zu löschen. Dazu haben sie 24h Zeit. Das Problem: Live-Videos werden auf diese Weise nie blockiert.

Ein schwieriges Thema: Wie lässt sich erreichen, dass Live-Videos inhaltlich in Ordnung sind? Anders als hochgeladene Videos, die danach online gehen, lassen sich Live-Videos nicht wirklich auf problematische oder gar kriminelle Inhalte prüfen. Selbst Künstliche Ingelligenz (KI) ist derzeit überfordert: Sie kann zum Beispiel mitunter gewalttätige Videospiele nicht unterscheiden von realen Bildern.

Ich habe mit dem auf Internetthemen spezialisierten Anwalt Christian Solmecke über das Thema gesprochen. Er hat mir erklärt: Plattformen sind zuständig - haben aber eben 24h Zeit, auf Videos mit kriminellen Inhalten zu reagieren. Eine Menge Zeit. Ausreichend Zeit jedenfalls, solche Videos dann zu kopieren - und sie verbreiten sich wirklich rasant im Netz.

Zwar betreiben die Plattformen mittlerweile einen gewissen Aufwand, um die schneeballartige Verbreitung auszubremsen - allerdings gelingt das nicht, wie wir wissen.

Facebook Libra fast am Ende

Im Sommer hat Facebook seine eigene Kryptowährung Libra angekündigt: Gemeinsam mit rund 20 Partnern will Facebook die Welt auf Kryptogeld einschwören. Doch der Widerstand nimmt zu: Regierungen, Notenbanken und Politiker stellen sich gegen die Pläne. Nun sind einige große Partner ausgestiegen. Allzu groß ist die Chance für Libra nicht mehr.

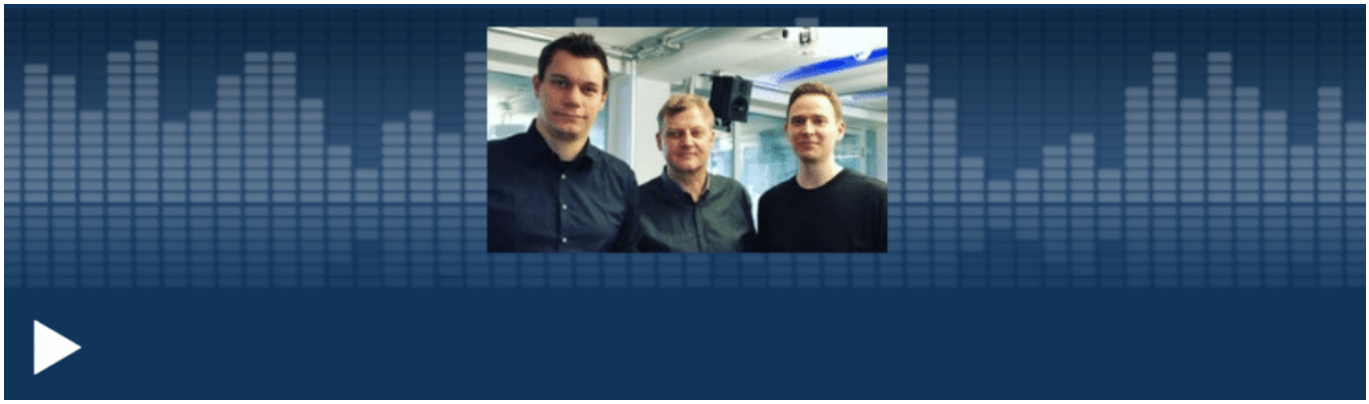
Vor ein paar Wochen hätte man den Eindruck bekommen können, wir hätten eine neue Weltwährung: Facebook hat mit Libra eine Kryptowährung angekündigt, die überall auf der Welt zum Einsatz kommen soll. Vor allem auf Mobilgeräten, aber nicht nur dort. Doch das Projekt wird immer schwächer. Nun sind weitere große Partner ausgestiegen: Das Auktionsportal eBay, der Zahldienst Stripe und die Kreditkartengesellschaften Mastercard und Visa haben die Reißleine gezogen. Sie sind ausgestiegen, machen nicht mehr mit. Auch Paypal ist vor kurzem bei Libra ausgestiegen. Die Schar der Unterstützer schrumpft.

Gegenwind aus der Politik hat zum Umdenken geführt

Die Erfolgschancen für Facebooks Libra als ernstzunehmende Währung gehen damit gegen Null. Eine ungewohnte Erfahrung für erfolgsverwöhnte IT-Konzerne aus dem Silicon Valley, die sich daran gewöhnt sind, dass man sie einfach machen lässt. Normalerweise sieht die Weltgemeinschaft ungerührt zu, wie die Konzerne existierende Branchen zerstören, tradierte Machtgefüge verschieben und Umsatzströme nach Kalifornien holen - in der Regel auf Kosten des Rests der Welt.

Bei Libra ist das nicht gelungen. Ich will kein Geheimnis daraus machen: Ich bin äußerst

erleichtert, dass die Vernunft Einkehr hält. Schon nach Ankündigung der virtuellen Währung war ich ausgesprochen besorgt - und erschrocken, dass das Bundesfinanzministerium und andere Verantwortlichen (noch) keine Haltung hatten. Das hat sich mittlerweile geändert. Die US-Regierung und einige US-Politiker haben sich klar gegen den Libra ausgesprochen. Auch der EU-Finanzkommissar will die Kryptpwährung strikt regulieren. Bundesregierung und Notenbank haben mittlerweile ihre Missbilligung ausgedrückt.



Facebook sollte Libra dicht machen

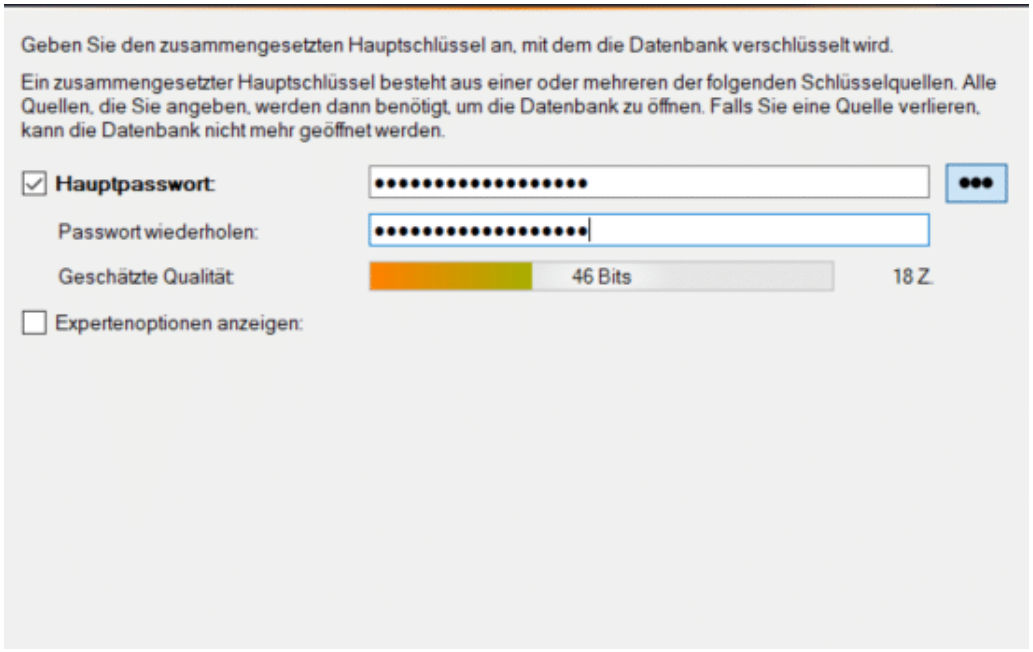
Richtig so. Wenn etwas systemrelevant ist, dann wohl Währungen. Diese sollten immer unter der strengen Kontrolle von Regierungen und Zentralbanken stehen - und ganz sicher nicht den kommerziellen Interessen eines nicht beherrschbaren Konzerns (oder Konsortiums) überlassen werden. Die möglichen Folgen einer global und weit ausgerollten Kryptowährung sind unvorhersehbar. Die Signale von der US-Regierung und aus Europa haben bei einigen Partnern vermutlich nun die Hoffnung zerstört, mit Libra tatsächlich erfolgreich sein zu können.

Es sind bestimmt keine prinzipiellen Gründe oder eine veränderte Überzeugung, dass etwas falsch daran sein könnte, mit dem Libra zu kommen. Es sind wohl eher die schwindenden Hoffnungen, damit Kasse zu machen. Aber das ist am Ende egal.

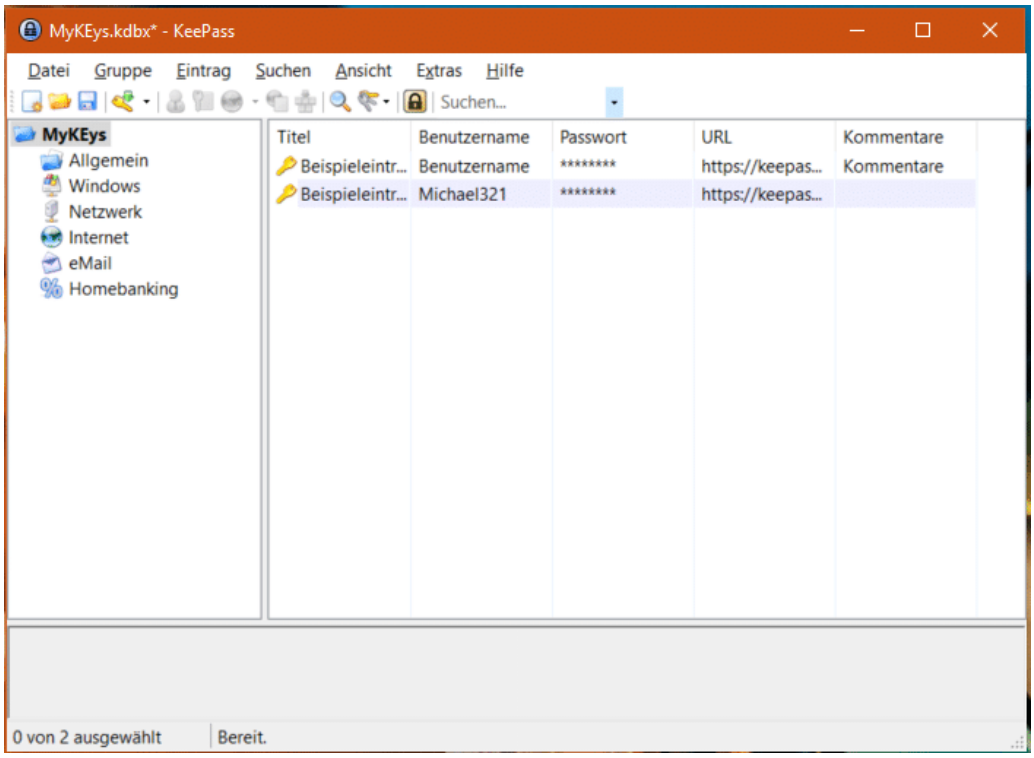
Tipp: Im CosmoTech Podcast "Haste mal 'n Libra" haben sich Dennis Horn, Sebastian Kirsch und ich intensiv mit dem Thema beschäftigt. Hört unbedingt mal rein!

Die Welt der Passwörter: KeePass

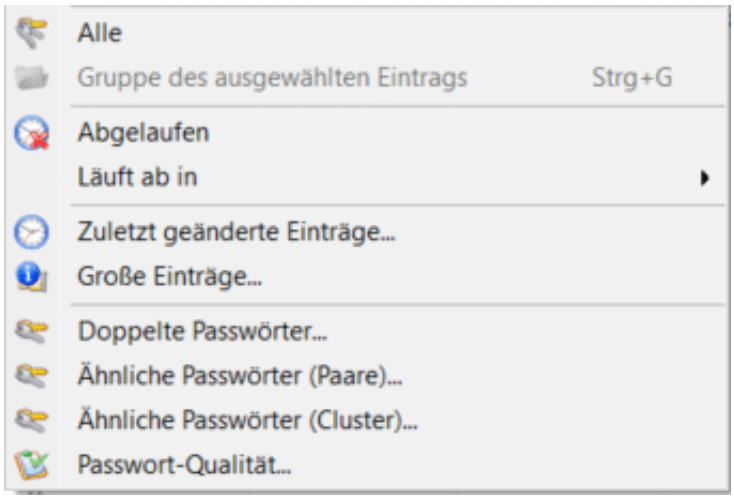
Auch wenn Biometrie immer mehr Einzug in die Betriebssysteme und App hält: Neben Fingerabdruck und Iris- oder Gesichtsscan ist das klassische Passwort der am meisten verbreitete Zugangsschutz. Grund genug, sich darüber immer wieder Gedanken zu machen. Und jede Unterstützung hilft dabei! KeePass ist ein kostenloses Programm, das Ihnen alles rund um Passwörter bietet.Vordergründig handelt es sich bei KeePass erst mal um einen mächtigen und hochsicheren Passwort-Manager. Wenn Sie das Programm das erste Mal starten, müssen Sie ein Master-Passwort eingeben. Dieses verschlüsselt die Datenbank. Je länger dieses Passwort ist, desto wirksamer ist die Verschlüsselung. Ein farbiger Balken unter dem Eingabefeld zeigt Ihnen an, wie gut das Passwort ist.



Ist die Datenbank dann einmal angelegt, dann können Sie wie in anderen Passwort-Managern auch Passwort-Karten anlegen und diese in Kategorien zusammenfassen. Innerhalb der Karten haben Sie alle Freiheiten, Informationen zu hinterlegen.



Interessant ist KeePass aber vor allem wegen der Analysemöglichkeiten: Sie vergeben Passwörter meist schnell und unter Zeitdruck. Auch wenn Sie wissen, wie wichtig ein gutes Passwort ist: Das Risiko liegt oft auch in der Ähnlichkeit von Passwörtern zueinander. Kennt ein Täter das eine, kann er oft durch leichte Modifikationen andere erraten.

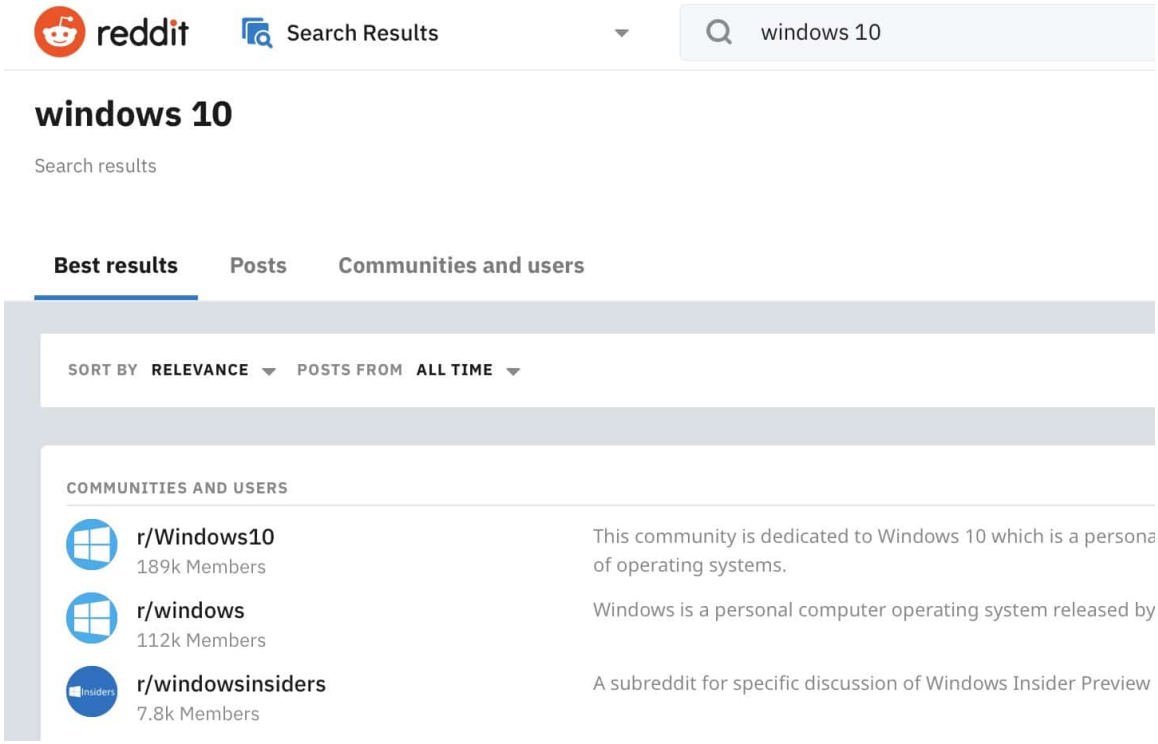


Unter **Suchen** können Sie Analysen auf die gesamte Passwortdatenbank fahren. Darunter eine, die die **Passwort-Qualität** prüft. Eine weitere zeigt Ihnen **Doppelte** und **Ähnliche Passwörter**. Nach der Durchführung der Analyse können Sie die angreifbaren Passwörter schnell austauschen.

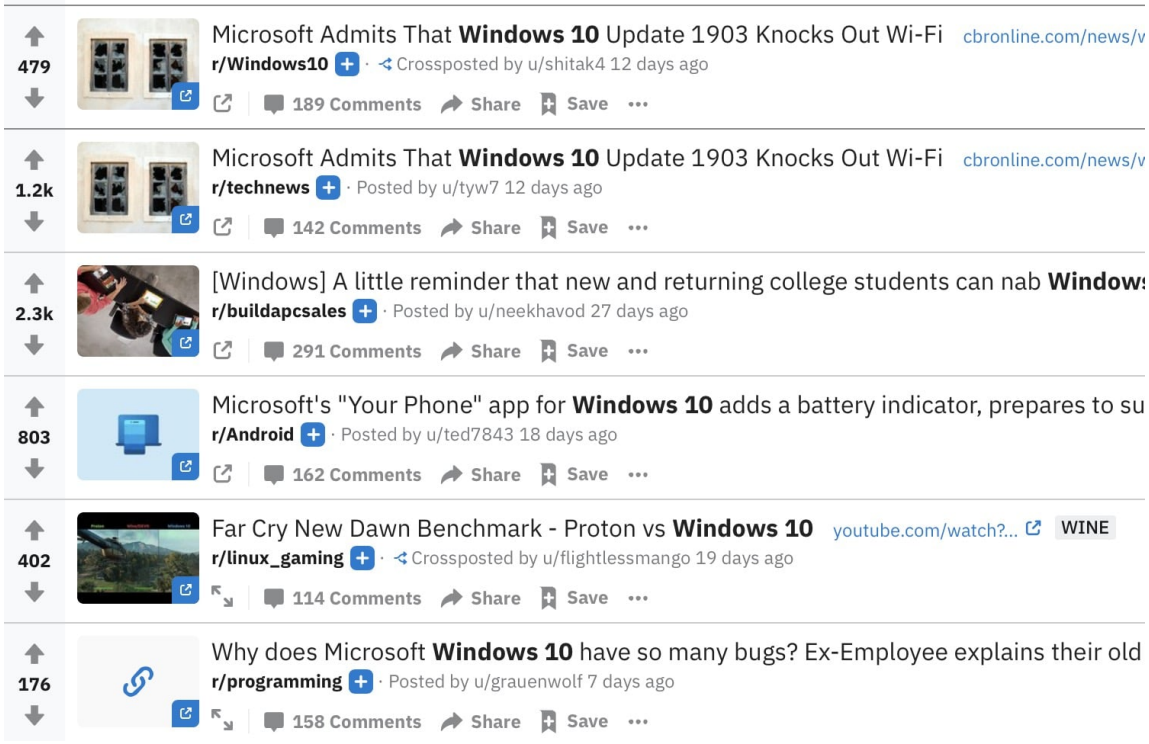
Schwarmintelligenz im Internet: reddit

Einer der großen Vorteile des Internets ist unbestreitbar die breite Menge an Informationen, die Sie darin finden. In Zeiten der viel beschworenen Fake News allerdings ist es schwer, vertrauenswürdige Quellen zu finden. Sowohl die thematische Tiefe als auch die Möglichkeit, die Vertrauenswürdigkeit der Information zu überprüfen stellen eine Herausforderung dar. Eine interessante Alternative dazu ist reddit.

reddit setz sich zusammen aus den Begriffen *read* (lesen) und *edit* (verändern) und sol vom klang her an "read it" (habe es gelesen) erinnern. Der Dienst versucht die Quadratur des Kreises: Jeder angemeldete Anwender kann eigene Bereiche, so genannte Subreddits erstellen. Zu welchem Thema er auch gerade möchte. Darin können Diskussionen eingestellt werden. reddit dient also auf der einen Seite als Informationsquelle, auf der anderen aber auch als Diskussionsforum.



Anwender können auf Beiträge sowohl mit Wortbeiträgen antworten als auch Beiträge (und Antworten) bewerten. Diese Bewertung und Diskussion unterscheidet reddit von anderen Plattformen. Je mehr Benutzer an einer Diskussion teilnehmen, desto mehr Bewertungen gehen auch ein. Sie können schnell erkennen, ob ein Beitrag eine Einzelmeinung oder die Meinung der Masse ist. Das hilft beispielsweise bei neuen Produkten, über die Sie sich eine Meinung bilden möchten.

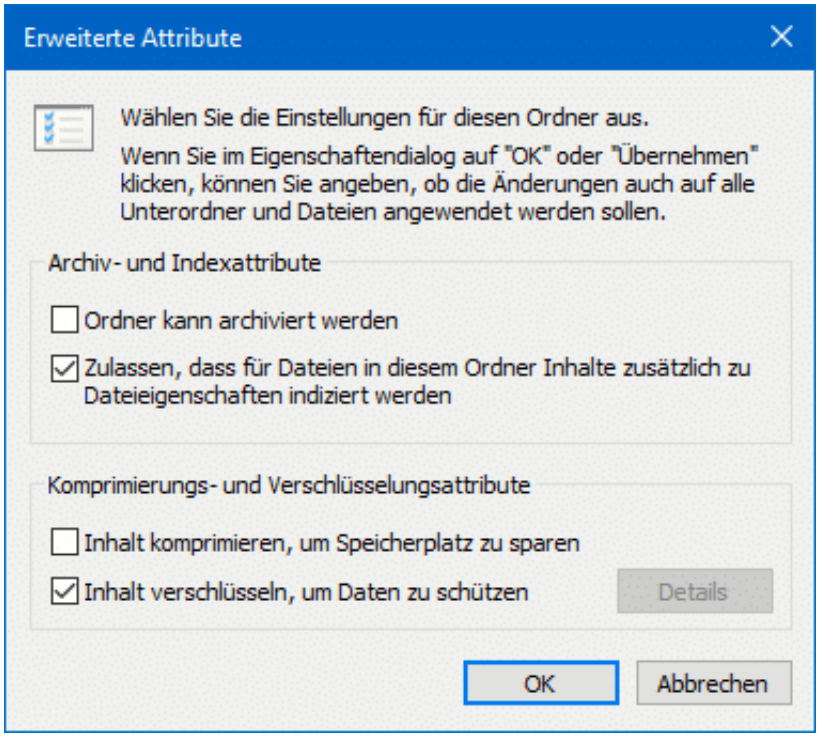


Keine Frage: auch hier können sich Gruppen zusammenschliessen und falsche Produktbewertungen einstellen. Auf Grund der offenen Plattform fällt das aber schnell auf und wird von der Community markiert und abgestraft.

Verschlüsseln einzelner Dateien per EFS

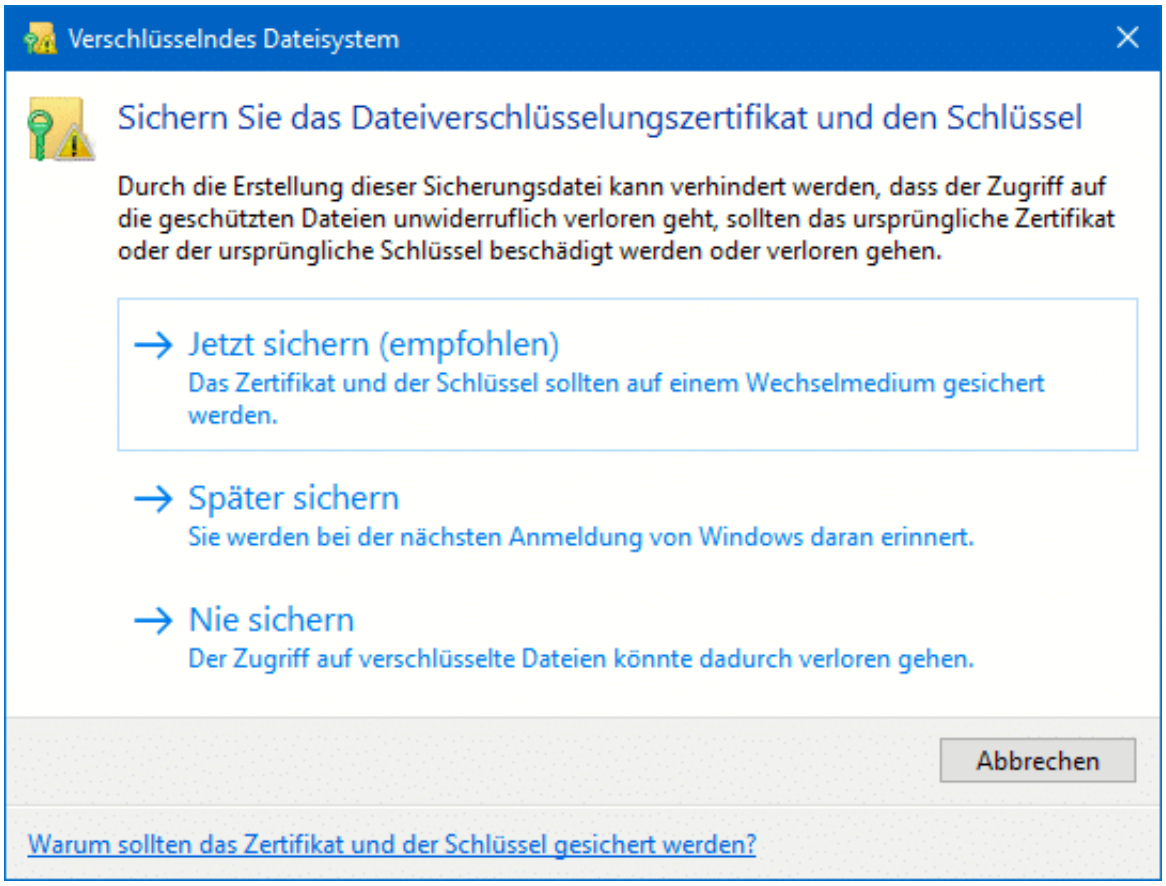
Doppelt gemoppelt hält besser. Bitlocker ist zwar eine schöne und vor allem leicht einzusetzende Möglichkeit, eine Festplatte zu verschlüsseln. Wenn sie zusätzlich einzelne Dateien nochmal verschlüsseln wollen, dann geht das bei einem Windows 10 Pro- oder Enterprise-System ebenfalls mit Bordmitteln. EFS (Encypted File System) heißt hier das Zauberwort.

Um eine Datei zu verschlüsseln, klicken Sie im Windows Explorer einfach mit der rechten Maustaste auf eine Datei. Dann können Sie in der Registerkarte **Allgemein** auf **Erweitert** klicken. Ganz unten sehen Sie dann **Inhalt verschlüsseln, um Daten zu schützen**.



Nachdem Sie das angewählt haben, haben die betroffenen (und jetzt verschlüsselten) Dateien und Ordner ein kleines Schloss als Symbol. Auf dem selben Weg können Sie die Verschlüsselung wieder rückgängig machen.

Wichtig zu wissen: Die Verschlüsselung hängt am Benutzerkonto. Sobald sich jemand erfolgreich anmeldet, kann er die Dateien entschlüsseln. Geben Sie per EFS verschlüsselte Dateien per E-Mail oder einem Datenträger weiter, dann wird automatisch die Verschlüsselung aufgehoben.



Was aber, wenn Sie selber nicht mehr an Ihr Benutzerkonto kommen, weil Sie die Zugangsdaten vergessen haben? Windows 10 versucht dies zu verhindern, indem es Sie beim ersten Verschlüsseln einer Datei daran erinnert, ein Backup der Schlüssel durchzuführen.

Dazu zeigt Ihnen Windows nicht nur kurz einen Dialog an, sondern auch gleich ein Symbol im Tray. Klicken Sie auf das Symbol, dann auf **Jetzt sichern**. Folgen Sie den Dialogen, und geben Sie neben dem Zielort für die Sicherung (am besten ein USB-Stick, den Sie sicher weglegen können) auch ein Kennwort an. Ohne dieses kann der Schlüssel nicht mehr wiederhergestellt werden.

So geht's leichter: Alle Dokumente im Griff

Moderne Festplatten fassen heute mühelos Zehntausende von Dateien und Dokumenten. Nicht einfach, in der Eile die passenden Dateien zu finden. Oder in der Cloud - denn auch dort speichern wir immer mehr Dokumente. Die neueste Ausgabe von **So geht's leichter** zeigt, wie Dokumente und Dateien optimal verwaltet werden.

Ein Dokument speichern - ganz einfach. Aber es wiederfinden? Nicht immer so einfach. In der neuesten Ausgabe von **So geht's leichter** zeigen wir anschaulich, wie Festplatten optimal organisiert werden und wie sich Dateien finden lassen.

Auch wie Dokumente sicher verschlüsselt oder im Netzweril sicher mit anderen Nutzern geteilt werden, erläutert das neue eBook.

Weiteres wichtiges Thema: Dateien in der Cloud. Office-Anwender können Dokumente in der Cloud speichern - und so von allen Geräten bequem darauf zugreifen. Aber was muss beachtet werden, damit die Dokumente sicher gespeichert werden?

Und welche Möglichkeiten bieten sich durch Dropbox? Wer alles richtig einrichtet, kann auch mit seinem Mobilgerät auf Dokumente zugreifen.

So geht's leichter: Dateien und Dokumente im Griff

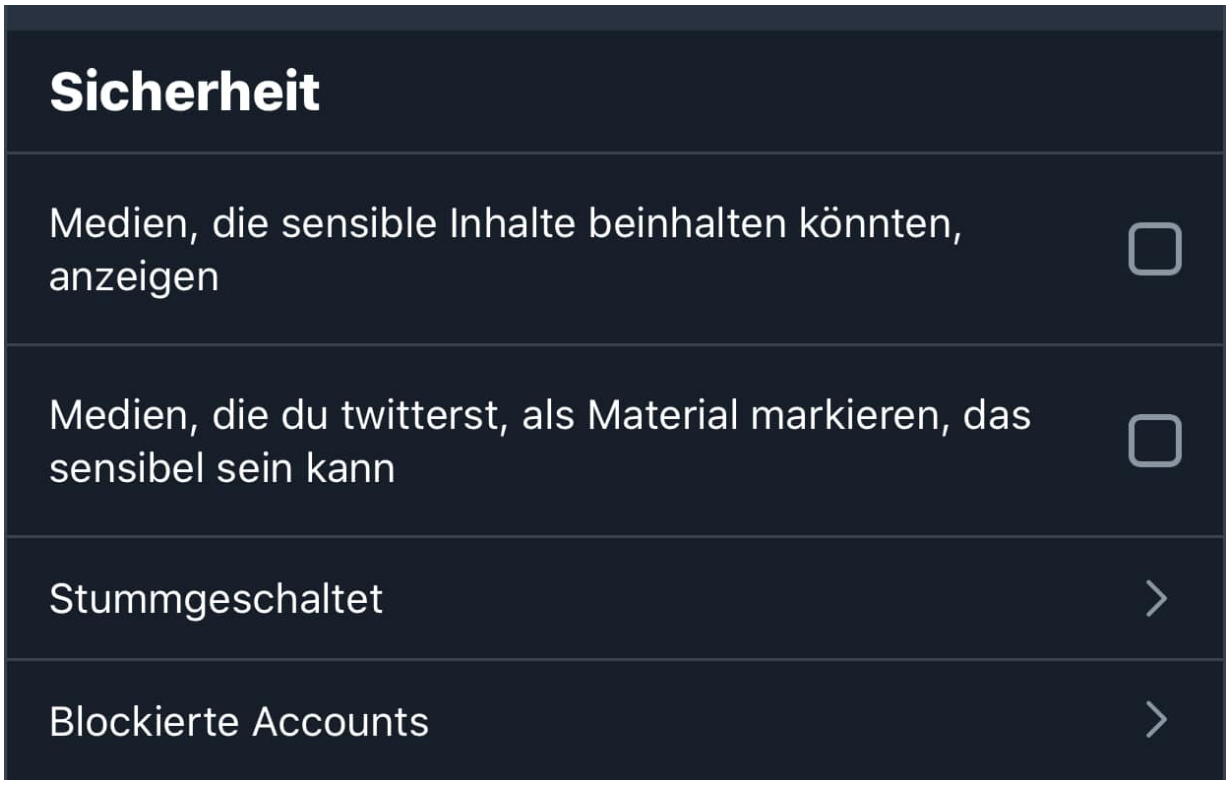

So geht's leichter...
WWW
Dokumente
• Dateien auf Festplatte optimieren
• Dateien in der Cloud
• Office mit OneDrive und Dropbox
• Dokumente mobil nutzen
So geht's leichter...

Unangemessene Inhalte bei Twitter ein- und ausblenden

Das Internet bietet unendliche Freiheiten. Inhalte zu veröffentlichen. Das hat sicherlich eine Menge Vorteile, denn damit kommen sie an Informationen, die sonst nicht verfügbar wären. Auf der anderen Seite besteht das Risiko, dass unbedarfte Betrachter sich von unangemessenen Bildern überfordert fühlen. Soziale Netzwerke wie Twitter versuchen ein Gleichgewicht zu finden. Inhalte, die unangemessen scheinen, filtern sie automatisch. Wollen Sie selbst entscheiden? Hier lesen Sie, wie!

Twitter zeigt bei Tweets, die es für kritisch hält, im Standard eine Warnung an. Meistens geht es dabei um Bilder, die Gewalt darstellen oder andere, vermeintlich anstößige Dinge. Diese Bilder werden nicht direkt dargestellt. An ihrer Stelle sehen Sie dann eine Warnmeldung, die Sie so einfach nicht wegklicken können.

Um solche Inhalte ansehen zu können, müssen Sie die Einstellungen der Twitter-App ändern. Tippen Sie dazu auf Ihr **Kontobild** oben links in der Twitter App. Im sich öffnenden Menü klicken Sie auf **Einstellungen und Datenschutz**. Dort finden Sie die **Inhaltsvorlieben**. Noch einfacher: tippen Sie auf den Link in der Meldung, dass sensible Medien ausgeblendet wurden.



Hier können Sie beide Richtungen beeinflussen: Zum einen können sie deaktivieren, dass Medien in fremden Tweets gesperrt werden. Auf der anderen Seite können Sie aber auch festlegen, ob Twitter bei Ihren eigenen Tweets eine Sicherung vorsehen soll, wenn es diese als sensibel erkennt.

Wie Firmen die Anwesenheit von Arbeitnehmern schnell und sicher erfassen

Ein Arbeitsplatz mit Stechkarte - gibt es heute kaum noch. Viele Arbeitsnehmer haben heute flexible Arbeitszeiten, viele können sogar den Arbeitsort selbst bestimmen. Für Selbständige gilt das sowieso. Aber wie Arbeitszeiten erfassen - transparent für alle, die es betrifft? Es gibt verschiedene Möglichkeiten.

Für Arbeitnehmer ist die wöchentliche Arbeitszeit in der Regel im Arbeitsvertrag festgeschrieben. Gibt es dort keine Vereinbarung, greifen Tarifverträge oder Betriebsvereinbarungen. Sie verpflichten den Arbeitnehmer, die dokumentierte Arbeitszeit zu erbringen und den Arbeitgeber, diese abzunehmen. Selbstständige hingegen sind in der Festlegung ihrer Arbeitszeit grundsätzlich unabhängig und legen sie nach dem Umfang der Kundenaufträge fest.

Arbeitgeber müssen die Arbeitszeit nachvollziehbar festhalten. Aber auch als Selbstständiger ist man gut beraten, die die Arbeitszheit am Arbeitsplatz und/oder für Projekte festzuhalten. Es gibt verschiedene Mittel und Wege, das Ziel zu erreichen. Eine auf den ersten Blick einfache Lösung ist, die Arbeitszeiten in einer Excel-Liste zu dokumentieren.

Am häufigsten genutzt wird allerdings die Zeiterfassung online. Sie ist bequem, modern und nachvollziehbar und damit für Arbeitnehmer und Arbeitgeber zu empfehlen.

Juristische Verpflichtung zur Arbeitszeiterfassung

Für viele Unternehmen kam das Urteil des Europäischen Gerichtshofs im Mai 2019 ein wenig überraschend. Es verpflichtet Firmen dazu, die Zeit, in der ein Mitarbeiter arbeitet, genau zu erfassen. Besonders für Angestellte, die in ihrem Arbeitsvertrag eine Vertrauensarbeitszeit vereinbart haben und deshalb keine detaillierte Aufschreibung der Arbeitszeit vornehmen, bringt diese Vorgabe enorme Veränderungen mit sich. Auf Seiten der Arbeitgeber sieht man die hohen Kosten für die Umsetzung einer IT-Lösung als problematisch an.

Zwar waren entsprechende Regelungen schon zuvor in vielen Unternehmen üblich, doch die neuen Vorgaben gehen darüber hinaus, sie erlegen dem Betrieb und dem Arbeitnehmer weitreichende Verpflichtungen auf. Mit einem Zeiterfassungsprogramm wie dem edtime Programm lässt sich diese Auflage mit wenig Aufwand schnell, transparent und komfortabel erledigen. Das System ist auf einem PC unter Windows ebenso nutzbar wie auf einem MAC und ist damit in vielen Firmen und Branchen nahezu universell einsetzbar. Auf der Zeiterfassungonline.com-Seite gibt es weitere IT-Tools, die gut nutzbar sind und die für den Arbeitgeber ebenso wie für den Arbeitnehmer sicher sind.

Steigende Nachfrage nach mobilen Tools

Wer häufig auf Dienstreisen ist und nicht im Büro arbeitet, ist in der Regel mit einer mobilen IT-Lösung gut beraten. Eine App ist zu empfehlen, wenn Sie die täglich geleistete Anzahl der

Stunden nicht am Computer oder in einer webbasierten Software erfassen wollen. Mit Hilfe dieser Apps können Sie schriftliche Nachweise wie eine Pdf-Datei erstellen, um damit die geleisteten Arbeitsstunden festzuhalten und abzulegen.

Solche Programme sind überall und auf jedem mobilen Endgerät nutzbar. Sie bieten sich somit für viele Branchen an und können im Außendienst ebenso gut eingesetzt werden wie auf einer Baustelle, beim Kunden vor Ort oder bei jeder Gelegenheit, wenn gerade nur ein Smartphone oder Tablet verfügbar sind. Auch wenn Sie am Abend zu Hause nur ganz kurz ein paar E-Mails beantworten wollen, müssen Sie diese Tätigkeit zeitlich erfassen. Mit einer mobilen IT-Lösung ist das schnell und bequem erledigt.

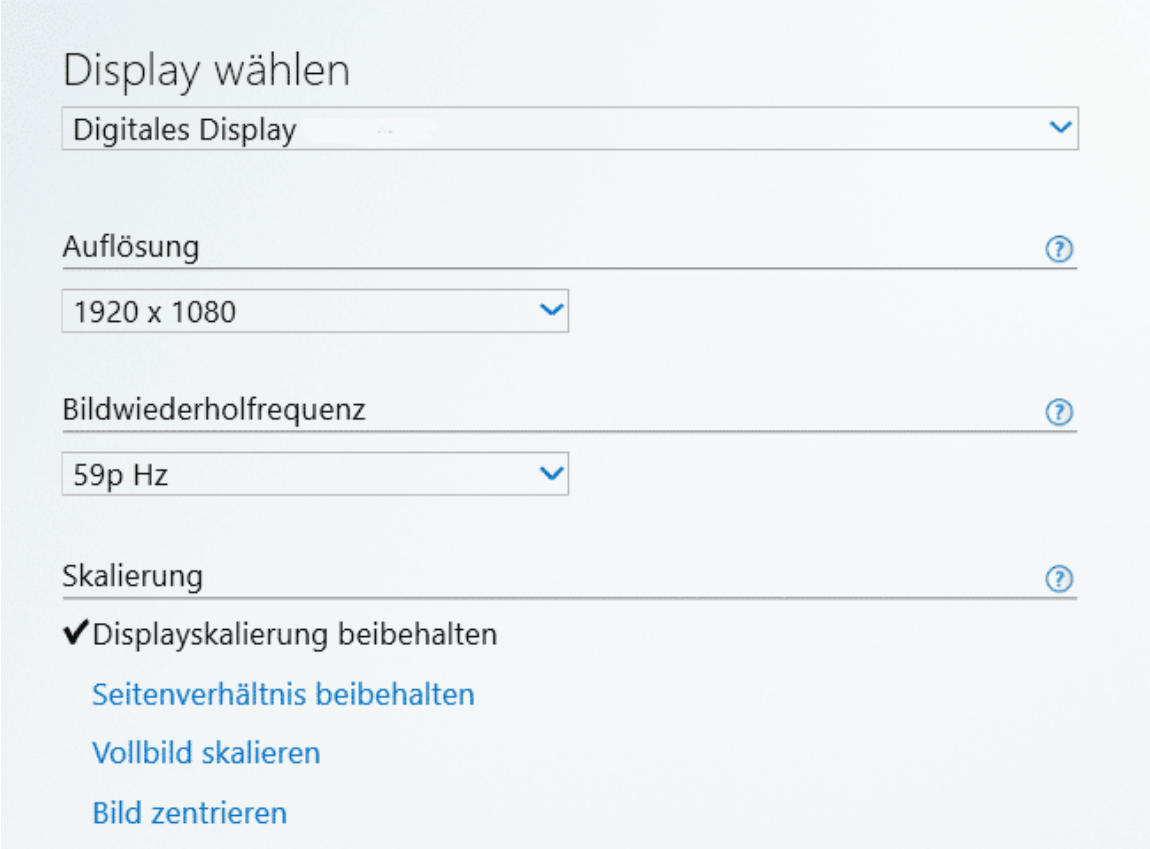
Sichere Datenhaltung in der Cloud

Ein flexibel nutzbares IT-Tool zeichnet sich auch dadurch aus, dass alle Daten sicher und zuverlässig gespeichert sind. Eine Cloud-Lösung ist zu empfehlen, damit sie von jedem Ort zu jeder Zeit für jeden Berechtigten einsehbar sind. Die Zeiterfassungssysteme der neuesten Generation folgen diesem Ansatz. Sie lassen sich bei Bedarf aufstocken und ausbauen, so dass auch bei einer wachsenden Anzahl von Mitarbeitern noch ein leistungsfähiges System gegeben ist. Darüber hinaus sind neue Erfassungssysteme so konzipiert, dass sie sich an Änderungen der Gesetzgebung leicht anpassen lassen. Damit bleiben Arbeitgeber langfristig auf der sicheren Seite, wenn es zu einer Verschärfung der Dokumentationsregeln kommt oder wenn im Tarifvertrag andere Vorgaben für die Arbeitszeit vereinbart werden.

Steuerung der Grafikkarte mit der Intel-Grafiksteuerung

Kaum ein PC hat noch nur ein Display. Besonders die, die über eine Dockingstation oder einen integrierten Displayport-Anschluss verfügen, erlauben den Anschluss von bis zu drei Monitoren. Mehr Bildschirmfläche heißt meist effektiveres Arbeiten. Allerdings nur dann, wenn Sie sich die Bildschirme in Windows so einrichten, dass diese richtig angesteuert werden. Neben den Windows-internen Einstellungen gibt es noch eine Systemsteuerung von Intel, die viele wichtige Einstellungen enthält. Sie müssen nur wissen, wo!

Klicken Sie mit der rechten Maustaste auf einen leeren Bereich des Desktops, dann wählen Sie **Intel-Grafikeinstellungen**. Wenn dieser Eintrag im Kontextmenü nicht auftaucht, dann haben Sie die Systemsteuerung nicht installiert. Da diese am Grafikkartentreiber hängt, aktualisieren Sie diesen. Wenn die Systemsteuerung dann immer noch nicht da ist, dann haben Sie eine Grafikkarte, die diese nicht unterstützt.



Unter **Allgemeine Einstellungen** können Sie Auflösung, Bildwiederholfrequenz und alles rund um die Skalierung des Displays festlegen. Im Gegensatz zu den Einstellungen bei Windows 10 selbst bekommen Sie hier eine Voransicht angezeigt. Damit können Sie ohne Anwendung der Änderungen sehen, wie das Bild dann aussähe.

Unter **DisplayPort Topologie** können Sie einstellen, wie viele (und welche) Monitore angesteuert werden sollen. DisplayPort unterstützt das so genannte Daisy-Chaining. Auch wenn Sie nur einen Port am Notebook oder Rechner haben, können Sie Monitore miteinander verbinden. Diese können dann unterschiedliche Bilder oder Desktops darstellen. Hier können Sie die Software-Einstellungen dafür vornehmen.