Schieb Report

Ausgabe 2020.02

4 Dinge auf die man achten sollte, wenn man Torrent Filesharing nutzt

Wer sich nicht nur im Web mit Inhalten versorgt, stolpet früher oder später sehr wahrscheinlich auch über Torrent Filesharing. Darüber lassen sich auch große Datenmengen extrem schnell und effektiv verteilen - und auf dem eigenen Rechner laden.

Torrent Filesharing ist eigentlich eine tolle Sache. Es ist einfach zu nutzen. Das Praktische: Wer Dateien verteilen möchte, kann auf einen zentralen Download-Server verzichten. Denn Torrent Filesharing beruht auf dem Peer-to-Peer (P2P) Prinzip. Die Download-Last wird somit auf alle teilnehmenden Computer verteilt. So ist zumindest das Grundprinzip.

Mit dem Aufkommen des Breitband-Internet in den letzten Jahren wurden Torrents bzw. P2P Filesharing sehr populär, da sich so schnell große Datenmengen hoch- bzw. herunterladen lassen. Parallel zur Popularität kam es allerdings auch zunehmend in Verruf, weil auf diese Art und Weise auch in großem Maße urheberrechtlich geschützte Musik, Filme und Software verteilt wurden und werden.

Urheberrechtlich geschützte Inhalte unerlaubt zu verteilen ist eindeutig illegal. Viele Rechteinhaber ahnden daher aktiv und oft auch erfolgreich Missbrauch. Schlüssel für die erfolgreiche Strafverfolgung ist meist die IP-Adresse der Nutzer, die ein Torrent-Netzwerk verwenden, um Dateien auszutauschen. Wer bei Urheberrechtsverletzungen erwischt wird, dem drohen - zu Recht! - kostspielige Abmahnungen oder gar Strafverfahren.

Ruf der Torrents dauerhaft geschädigt

Illegales Filesharing und die möglichen juristischen Folgen haben den Ruf von Torrent-Filesharing nachhaltig beschädigt, manche sagen sogar zerstört. Das hält viele davon ab, Torrents zu nutzen. Einfach aus der Sorge heraus, im Bittorent-Netzwerl versehentlich etwas Illegales zu tun. Dabei ist es nicht verboten oder illegal, ein Torrent-Netzwerl zu nutzen. Es ist lediglich illegal, urheberrechtlich geschützter Werke zu verteilen.

Deshalb hier vier Aspekte, auf die man bei der Nutzung von Torrent-Filesharing unbedingt achten sollte:

Tipp 1: Keine illegalen Dateien herunterladen

Der erste Tipp ist eine ganz einfache Sache: Lass die Finger von illegalen Inhalten.

Aber woran erkennt man die? Der gesunde Menschenverstand kann dabei durchaus hilfreich sein. So ist ein zum Download angebotener Kinofilm, der erst kürzlich im Kino gelaufen ist oder sogar immer noch dort zu sehen ist, ganz sicher ein urheberrechtsverletzender illegaler Download. Eigentlich alle Filme sind urheberrechtlich geschützt.

Auch Software, die im Laden viel Geld kostet und als Torrent zum „kostenlosen“ Download verfügbar sein soll, ist mit Sicherheit nicht legal. Auch davon unbedingt die Finger lassen. Dasselbe gilt für Musik, eBooks und andere Inhalte.

Tipp 2: Torrents nur von vertrauenswürdigen Webseiten herunterladen

Selbstverständlich sollte man für den Download von Torrents nur vertrauenswürdige Webseiten nutzen und nicht etwa irgendwelche schnell mal gegoogelten, zwielichtigen Webseiten.

Zwar muss man auch hier darauf achten, dass man die Finger von urheberrechtlich geschützten Dateien lässt. Aber der Hintergrund ist dann doch ein anderer. Denn auf zwielichtigen Seiten ist das Risiko deutlich höher, dass man sich mit dem Download Malware und Viren einfängt.

Tipp 3: Ein VPN Nutzen

Auch wenn man lediglich legale Dateien via Torrent herunterlädt oder verteilt und somit rechtlich gesehen nichts falsch macht, kann der ein oder andere doch das Bedürfnis haben, anonym zu bleiben.

Mittel der Wahl um dies zu erreichen ist in der Regel die Nutzung eines virtuellen privaten Netzwerkes (VPN) wie zum Beispiel ExpressVPN. Dank End-to-End Verschlüsselung und die Nutzung eines VPN Proxys kann man so maximale Anonymität erreichen. In einem VPN verschleiert man seine IP-Adresse - und das völlig legal.

Tipp 4: Einen guten Torrent Client nutzen

Natürlich solltest Du auch einen guten und praktischen Torrent Client nutzen. Der muss auch vernünftig konfiguriert werden. Oftmals lässt sich auch so schon ein gewissen Maß an Anonymität erreichen. So lässt sich auch schon im Client der Datenverkehr verschlüsseln. Zudem lässt sich auch hier schon ein Proxy angeben, der helfen kann, Deine IP-Adresse zu verschleiern.

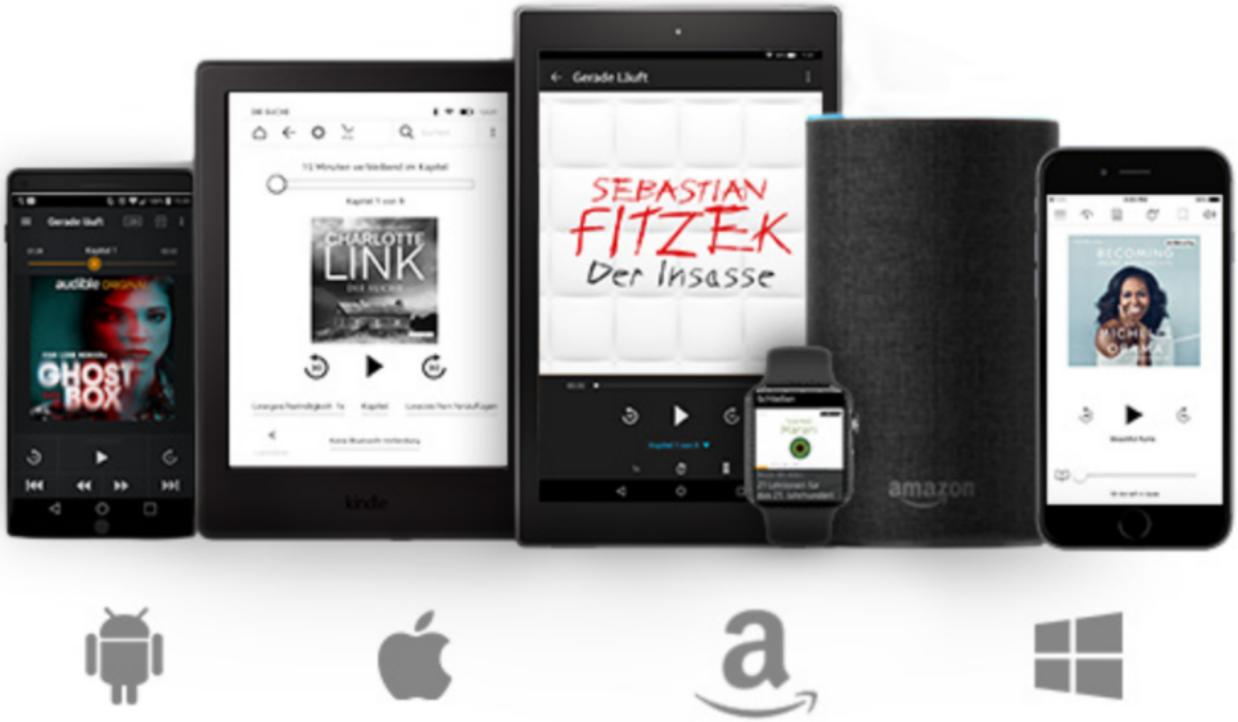
Beachtet man diese vier Tipps, erspart man sich der Regel schon eine Menge Ärger mit Anwälten oder gar Malware.

Hörbücher hören - wird immer komfortabler

Podcasts sind derzeit nicht ohne Grund populär: Es macht einfach Spaß, sich mal ausgiebig und ohne Zeitnot einem Thema zu widmen. Ideralerweise werbefrei. Nicht nur ein paar Minuten, sondern gene auch schon mal eine Stunde. Oder mehr. Podcasts ermöglichen das - und Hörbücher erst recht.

Während die meisten Podcasts gratis sind, muss man für seriöse Hörbücher bezahlen. Der zum Amazon-Konzern gehörende Anbieter Audible ist der wohl mit Abstand größte und wichtigste Anbieter von Hörbüchern. Weit mehr als 200.000 Titel stehen hier zur Verfügung. Eine gigantische Auswahl: Egal ob Romane, Science-fiction, Ratgeber, Sachbücher oder Kinderbücher - es gibt (fast) alles.

Zum ersten Mal ganz bewusst und mehrere Hörbücher bei Audible gehört habe ich, als ich längere Zeit im Krankenhaus lag - und nicht so gut lesen konnte. Gleich habe ich den besonderen Flaire von Hörbüchern zu schätzen gewusst: Der kleine Prinz im Original - gesprochen von einem französischen Schauspieler. Während die deutsche Ausgabe von Jan Josef Liefers gelesen wird. Ebenfalls ein Genuss. Und danach ein Sachbuch. Klasse.



Hörbücher einfach weiterhören

Die Welt der Hörbücher hat sich schon enorm verändert. Früher hat man sich ein Hörbuch gekauft, konnte die CD abhören. Fertig. Heute gibt es jede Menge Komfort. Lesezeichen.

Weiterlesen im anderen Gerät.

Man kann ein Hörbuch im Sessel anfangen (auf dem Smartphone), im Auto weiterhören - und sich von Alexa vorgespielt das Ende anhören. Die Audible-App weiß immer, wo man zuletzt gewesen ist und macht da weiter, wo man aufgehört hat. Egal, wie viele Geräte man verwendet, um seine Hörbücher anzuhören. Das gefällt mir besonders gut.

Wer Abonnent ist, kann jeden Monat ein weiteres eBook laden - mit seinem Guthaben. Wer mal pausiert, verliert sein Guthaben nicht - und kann später dann gleich mehrere Hörbücher laden. Aber wer erst einmal auf den Geschmack gekommen ist - Hörbücher beim Joggen, beim Ausruhen, im Auto... - der hat schnell gleich mehrere Hörbücher am Start.

Auch Podcasts im Angebot

Es gibt auch einige Podcasts, die exklusiv bei Audible laufen. Etwa "Wahre Verbrechen" oder "Geo, der Podcast". Abonnenten und Mitglieder hören diese Podcasts ohne weitere Kosten - und ohne ihe Guthaben belasten zu müssen. So ähnlich, wie Prime-Mitglieder bei Amazon kostenlos eBooks laden oder einige Serien und Filme bei Prime Video anschauen können.

Aber niemand muss Abonnent werden. Es ist natürlich auch möglich, bei Bedarf nur einzelne Titel zu laden. Es ist auch möglich, gekaufte Hörbücher weiterzugeben: Über die App lassen sich die Hörbücher an Freunde und Familie weitergeben/ausleihen. Nicht beliebig viele TItel - aber doch einige.

Facebook will weniger Deepfake-Videos

Facebook hat schon vor Monaten angekündigt, aktiv etwas gegen Manipulationen zu unternehmen - schließlich sind bald Präsidentschaftswahlen in den USA. Jetzt hat Facebook angekündigt, künftig Deepfake-Videos aus dem Netzwerk zu verbannen.

Mit Künstlicher Intelligenz (KI) ist heute so Einiges möglich. Es ist zum Beispiel kein Problem, praktisch jeden Text mit einer fremden Stimme sprechen zu lassen. Adobe hat solche Software in der Entwicklung: Sie wird trainiert - etwa mit Beispielen aus öffentlich zugänglichen Interviews - und wenig später plappert die Software mit der Stimme von Trump, Putin oder Merkel.

Andere KI-Software wiederum kann Videobilder so manipulieren, dass man zum Audio auch noch das passende Video bekommt. Deepfake nennt sich das dann. Für den Laien sind solche Videos von echten Aufnahmen praktisch nicht zu unterscheiden.

Erkennbare Deepfakes werden entfernt - außer bei Satire

Wenn man sich die Ergebnisse anschaut, die heutzutage durchaus beeindruckend sind, ist das erst mal unterhaltsam. Bei näherer Betrachtung aber auch bedrohlich: Denn was, wenn jemand Donald Trump - in diesen hässlichen Zeiten - bestimmte Worte in den Mund legt, die er gesagt haben könnte, aber nicht gesagt hat? Etwa eine Kriegserklärung an den Iran. Alles denkbar - und leider auch technisch möglich. Und was möglich ist, das wird auch passieren - früher oder später.

Deshalb hat sich Facebook entschlossen, Deepfakes aus dem Angebot zu entfernen. Freilich erst, wenn sie entdeckt werden - was aufgrund der Qualität mancher Deepfakes alles andere als einfach ist. Und: Die Deepfakes sollen nur dann entfernt werden, wenn sie "ernst gemeint sind", erklärt das Unternehmen. Bedeutet: Parodien und Satire mit Deepfakes sind erlaubt. Die Content-Moderatoren müssen also ganz genau hinschauen. Und wie wir wissen: Satire kann auch Empörungsstürme auslösen.

Blockchain könnte Authentizität von Fotos und Videos dokumentieren

Generell ist es aber eine gute Idee, kritische Deepfakes nicht zuzulassen und sie aktiv zu entfernen. Mittelfristig werden wir uns wohl auch privat Gedanken darüber machen müssen, die Authentizität von Fotos, Videos und Audios besser überprüfen zu können. Kommt das Video aus dem Weißen Haus wirklich aus dem Weißen Haus? Mit Blockchain wäre es durchaus möglich, die Echtheit nachzuweisen - und zu sehen, ob etwas manipuliert wurde und von wem.

Das scheint dringend nötig. Facebook betrachtet Deepfakes als "große Herausforderung für unsere Branche und Gesellschaft, wenn ihr Einsatz zunimmt". Redaktionen müssen noch genauer hinsehen, "normale" User, die so etwas in einem Sozialen Netzwerk sehen, könnten Deepfakes schnell für glaubhaft halten. Wie genau Facebook solche gefälschten Videos identifizieren will, erklärt das Unternehmen nicht. Der Konzern verweist lediglich auf die Brancheninitiative Deepfake Detection Challenge und eine Zusammenarbeit mit der Nachrichtenagentur Reuters.

Der Zeitpunkt für die Ankündigung ist nicht zufällig: Dieses Jahr wird in den USA gewählt - und da ist mit zahlreichen Manipulationsversuchen zu rechnen. Auch mit Deepfakes. Mark Zuckerberg hat der US-Politik Zusagen gemacht (machen müssen), etwas gegen Manipulationen zu unternehmen. Gut, dass das Unternehmen mal etwas unternimmt, wenn es noch nicht zu spät ist.

https://vimeo.com/301803531

Seehofer will: Passfotos künftig nur noch unter staatlicher Aufsicht

Zehn Jahre hält ein Personalausweis – oder Reisepass. Bei Erwachsenen. Dann müssen wir zum Amt, einen neuen Pass beantragen. Und Fotos mitbringen. Seit einigen Jahren müssen die bestimmten Kriterien genügen: Geradeaus schauen, nicht lächeln – damit daraus biometrische Merkmale ausgelesen werden können. Diese Fotos haben wir häufig beim Fotoladen um die Ecke gemacht. Damit könnte bald Schluss sein. Denn Innenminister Seehofer will, dass Passbilder nur noch unter Aufsicht in der Behörde entstehen. Warum das?

Bundesinnenminister Seehofer will Fotobuden in Ämtern aufstellen. Da sollen wir unsere Fotos unter Aufsicht der Beamten machen – und unsere Fingerabdrücke hinterlassen. Warum sind die Fotos, die wir mitbringen, nicht mehr gut genug?

Der Grund liegt auf der Hand: Moderne Methoden der Fotomanipulation ermöglichen heute Veränderungen an Fotos, so sehr im Detail, dass es dem normalen Auge des Beamten nicht auffällt – doch mit enormen Auswirkungen. Beispiel Das so genannte Morphing: Englisch für Verwandlung. Hier werden zwei oder mehr Fotos durch die Morphing-Software gejagt. Die Bilder verschmelzen zu einem ganz neuen.

Mehrer Gesichter in einem Foto durch Morphing

Das Foto sieht dann dem Passinhaber ähnlich, aber auch zum Beispiel einer anderen Person, irgendwie auch logisch, wenn man aus zwei Bildern von Menschen eines macht, ähnelt das entstanden Bild beiden etwas. Der Beamte hat kaum die Möglichkeit den Unterschied zur realen Person zu sehen.

Aber: Der menschliche Beamte kann vielleicht irren. Beim Erstellen eines Passes wird jedoch per Computerprogramm kontrolliert, ob alle biometrischen Daten vorliegen.

Die biometrischen Daten sind aber nicht weg, sie sind nur leicht variiert. Das Foto enthält durch das Morphing unter Umständen auch biometrische Daten von anderen Personen. Bedeutet: Der Beamte denkt, es handelt sich um die Person, die den Pass beantragt. Weil irgendwie ja zwei Gesichter in der gemorphten Aufnahme stecken. Später kann aber eine ganz andere Person zum automatischen Gesichts-Check gehen – das ist mit biometrischen Daten ja möglich – und wird auch authentifiziert, also durchgelassen. Weil die biometrischen Daten der zweiten Person im Foto ebenfalls enthalten sind – und auch die Software das Morphing nicht bemerkt.

Natürlich kann man nicht die Bilder von Schwarzenegger und Greta Thunberg kombinieren. Die

Personen müssen schon zumindest eine gewisse Ähnlichkeit haben. Aber wenn das gewährleistet ist, kann es klappen: Die biometrischen Daten mehrerer Personen, die sich nur im Detail unterscheiden, sind dann im Bild drin. Denn die Systeme, die Gesichter prüfen, haben natürlich eine gewisse Fehlertoleranz. In diesem Bereich muss sich die Manipulation bewegen. Das ist nichts, was man mal so eben macht – aber auf jeden Fall denkbar. Es hat auch schon Belege dafür gegeben, dass so etwas tatsächlich funktioniert.

Es hat schon Fälle gegeben: Genorphte Fotos angenommen

Das Künstlerkollektiv Peng hat im Rahmen der Kunstaktion MaskID hat im September 2018 dem Meldeamt in Berlin ein gefälschtes Foto vorgelegt – und es wurde anstandslos ein Pass ausgestellt. Die Künstler haben das Foto einer Aktivistin mit dem der EU-Vertreterin für Außen- und Sicherheitspolitik Federica Mogherini per Morphing verschmolzen. Und: Es hat geklappt. Das zeigt, dass es eindeutig Sicherheitslücken gibt. Sie auszunutzen ist nicht trivial – aber möglich.

Im Foto-Booth direkt im Amt sind Manipulationen natürlich ausgeschlossen. Die Aufnahmen wandern unmittelbar zum Sachbearbeiter. Es gäbe sicher auch andere Möglichkeiten, Passfotos sicherer zu machen. Man könnte zum Beispiel verlangen, dass Fotos eine digitale Signatur aufweisen. Wenn zertifizierte Studios die Aufnahmen machen und signieren. Dann ist nichts mit Morphing, das würde nämlich auffallen... Das Gesicht als sichere Referenz, darum geht es ja im Grund, hat aber immer mehr Probleme. Leider ist es aber heute sehr einfach, zu manipulieren. Nicht nur Fotos, sondern auch Audios und Videos, da gibt es im Netz immer mehr Probleme.

Besonders gefährlich: Deepfake Videos

Es gibt noch die ganz andere Seite, so genannte Deepfake-Videos: Da sprechen Politiker, etwa Barack Obama, und sagen etwas, das sie nie gesagt haben. Es sieht echt aus, es hört sich echt an. Mundbewegungen, Gesichtsmimik – alles passt. Doch die Aufnahmen kommen aus einem Computerprogramm. Sogar komplett künstliche Gesichter möglich, die wirken wie echte Menschen. Es gibt schon beeindruckende Beispiele, die für Furore gesorgt haben. Etwa Barack Obama, der sich über Trump lustig macht. Oder Mark Zuckerberg, der zugibt, die Herrschaft über die Welt an sich reißen zu wollen. Facebook plant deshalb jetzt, solche Deepfake-Videos zu löschen, wenn sie entdeckt werden. Auch hier wird also etwas gegen die zunehmende Manipulation in Fotos und Videos unternommen.

Wir werden immer mehr Betrügereien sehen – etwa, um Sicherheits-Checks zu überlisten oder um die Öffentlichkeit zu täuschen. So etwas wird uns mehr und mehr beschäftigen und es braucht Methoden, das zu verhindern. Im Fall der Passbilder wäre es aber erst dann so richtig wirksam, wenn das alle Staaten so handhaben. So könnten Terroristen sich einfach zB einen französischen Pass ausstellen. Der Schritt, die Fotoaufnahmen sicherer zu machen, halte ich deshalb für keinen übertriebenen Schnickschnack, sondern durchaus für nachvollziehbar – und auch angemessen. Wir haben keinen wirklichen Nachteil dadurch. Die kleinen Fotoläden

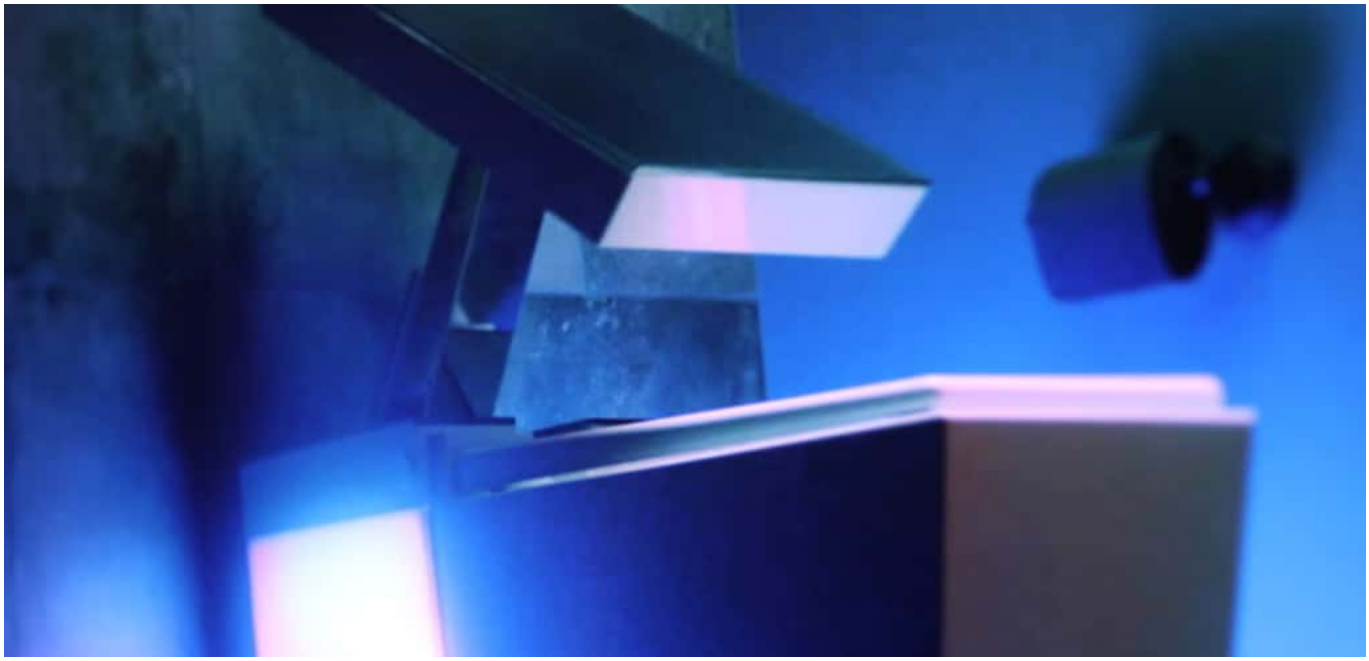
natürlich schon.

CES2020: Alexa, wie ist mein Stuhlgang?

Die CES (Consuer Electronics Show) ist die weltgrößte Konsumermesse. Hier zeigen die Hersteller, was sie in diesem Jahr und darüber hinaus veraufen wollen. Gerne auch schon mal ein paar Verrücktheiten. Trendsetter ist die Messe allemal.

Wir leben in merkwürdigen Zeiten. In den Sozialen Netzwerken wird der Ton immer rauher und unversöhnlicher – und zu Hause machen wir es uns richtig schön bequem. Wir holen uns Geräte in die Wohnung, die uns zuhören, mit uns reden, kleine Dinge für uns erledigen. Ja, auch mit sanfter Stimme zu uns sprechen. Wie angenehm. Jetzt ist das sogar im Badezimmer möglich. Auf der Konsumermesse CES ist ein Duschkopf mit Alexa zu sehen – und sogar ein Alexa-Klo.

Kein Witz: Die Luxus-Toilette Numi 2.0 von Kohler verfügt nicht nur über Sitzheizung und Beleuchtung, sondern auch über eingebaute Alexa und Surround-Sound. Während der "Sitzung" die Börsenkurse abfragen, den Nachrichten lauschen, einen Podcast hören oder einfach im Netz recherchieren – alles möglich.



Wegweiser für das Zuhause von Morgen

Auf der weltgrößten Konsumermesse CES (Consumer Electronics Show) gab es schon immer solch einen Unsinn, über den dann jeder berichtet. Weil solche Dinge zeigen, in welche Bereiche Technologie vordringt. Heute finden wir die Vorstellung noch irritierend, im Bad und auf dem Klo mit Alexa reden zu können. Morgen schon nicht mehr. Das gilt auch für andere Hightech-Spielereien. Etwa Miniroboter wie RollBot oder Lovot aus Japan. Was der kann? Zum Beispiel auf Zuruf Klopapier holen – kein Witz! Das verspricht der Hersteller wirklich.

So richtig ernst nehmen können wir Roboter aber noch nicht. Der 16.000 EUR teure Pepper

zum Beispiel ist nicht viel mehr als ein rollender Sprachassistent, der einen auch noch schlecht versteht. Deshalb versucht es das französische Startup Pollen Robotics jetzt mit einem humanoiden Roboter Reachy (ab 8.000 EUR), der funktionstüchtige Arme hat – und im Haushalt helfen kann. Immerhin 500 Gramm kann er bewegen. Wer mag, kann sich den Roboter selbst zusammenbauen und Teile sogar im 3D-Drucker ausdrucken.

Future-Autos und hochauflösende Fernseher

Kann ich aber ehrlich gesagt auch nicht ernst nehmen. Ernst gemeinter sind die Autos, die es auf der CES zu sehen gibt. Daimler hat den "Avatar" gezeigt. Future-Design und Schwerpunkt auf Nachhaltigkeit. Ein echter Hingucker. Und Sony - ja, wirklich Sony! - hat ebenfalls ein Auto präsentiert. Das wirkt sogar serienreif – könnte also bald in Produktion gehen.

Aber auch in der Halle "Werden wir mal wieder seriös" gibt es einiges zu sehen: Neue Fernseher zum Beispiel. Auch auf der CES zeigen die Hersteller 8K-Modelle. Das erlaubt große Geräte mit feiner Auflösung.

Nur: Noch sendet kein Sender der Welt in 8K. Selbst die Streeamingdienste nicht. Auch das also eher ein Gimmick. Interessanter ist da die neue Technologie namens Mini-LED: Diese ermöglicht Fernsehgeräte, die fast so schöne Bilder liefern wie das teure OLED – aber deutlich günstiger sind. Von so etwas haben die Konsumenten wenigstens was.

Also: Die CES ist dieses Jahr irgendwie mehr eine Future-Messe, keine Konsumer-Show. Aber das ist ja auch was.

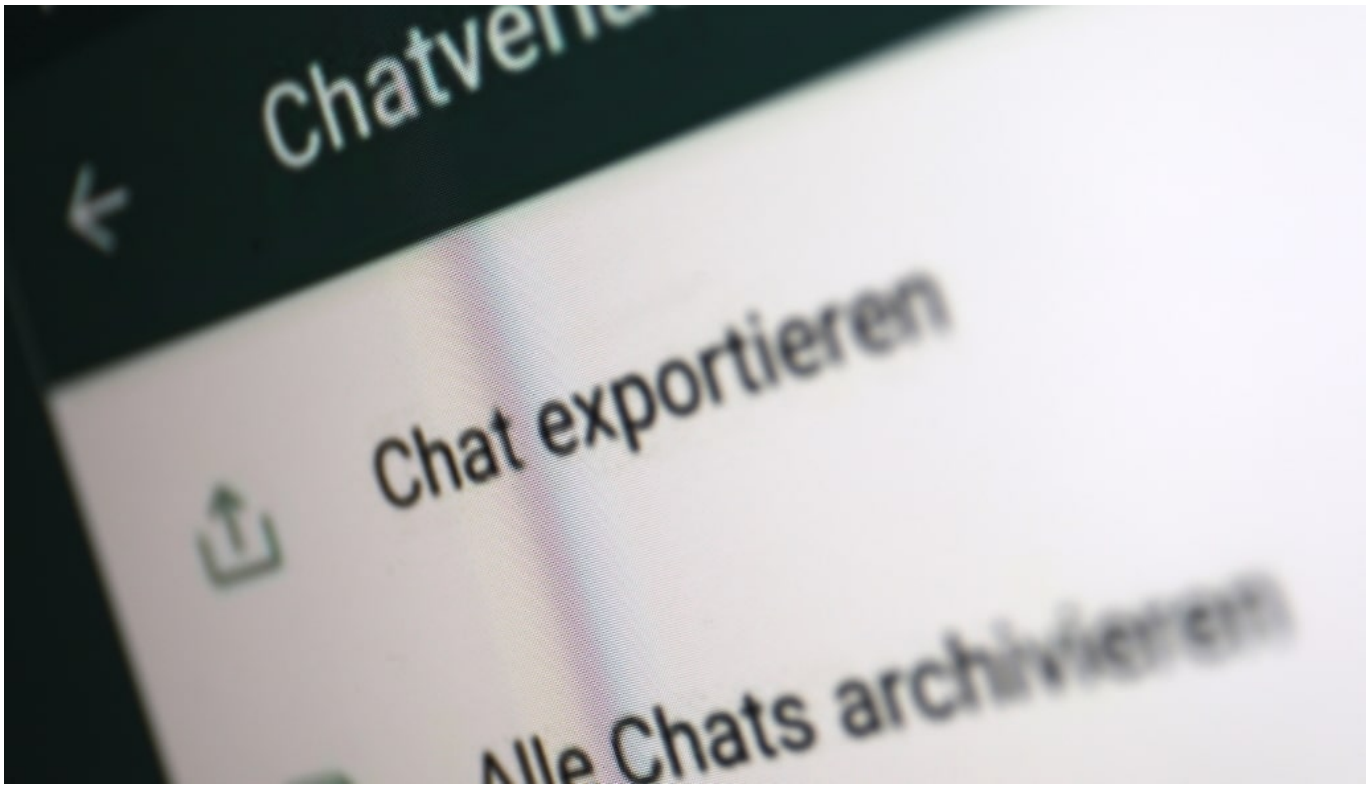
https://vimeo.com/383249275

Wegen Patentstreit: Kein Chat-Export mehr in WhatsApp

WhatsApp-User können keine Chats mehr exportieren und so dauerhaft speichern: Die Funktion ist einfach verschwunden - aber nur in Deutschland. Hintergrund sind Patentstreitigkeiten.

So mancher Chat im Messenger ufert aus – und irgendwann möchte man ihn nicht mehr im Smartphone gespeichert haben. Etwa, um den Speicher zu schonen (wenn viele Bilder oder Videos enthalten sind) oder weil man sich nicht ständig daran erinnern möchte. Ganz wegwerfen will man den Chat aber auch nicht. Was tun? Exportieren!

Bislang gab es in WhatsApp die Möglichkeit, Einzel-Chats oder Gruppen-Chats zu exportieren, also dauerhaft zu speichern (etwa auf dem PC oder in der Cloud). Jetzt nicht mehr. Denn WhatsApp hat die "Exportieren"-Funktion entfernt. Allerdings nur in Deutschland!



Gesperrt wegen Patentstreitigkeiten

Irgendeine offizielle Ankündigung oder Erklärung gibt es nicht. Wer sich jedoch die entsprechende Support-Seite von WhatsApp anschaut, findet den deutlichen Hinweis: "Bitte beachte, dass diese Funktion in Deutschland nicht unterstützt wird."

> Bitte beachte, dass diese Funktion in Deutschland nicht unterstützt wird.
> *WhatsApp Support*

Die durchaus praktische Funktion wird also nur in Deutschland abgeschaltet. Falls Ihr sie noch sehen könnt: Nicht zu früh gefreut. Spätestens mit dem nächsten Update der App dürfte die Export-Funktion verschwunden sein.

Aber warum? Der Verdacht liegt nahe, dass WhatsApp die Funktion abschalten **muss**. Patentstreitigkeiten. Laut Gerichtsurteil darf WhatsApp die Funktion in Deutschland nicht nutzen. Es ist zu einem Rechtsstreit zwischen Blackberry und WhatsApp gekommen. Darin ging es um ein Patent zum Verschicken von Chat-Historien. Nicht ganz dasselbe, aber sehr vergleichbar. Blackberry hat gewonnen – und deshalb darf WhatsApp die Funktion nicht nutzen (oder müsste dafür zahlen).

Möglicherweise kommt die Funktion zurück

Zwar halten Patent-Experten wie Florian Müller die Patente für nichtig, dennoch hat die 7. Zivilkammer Blackberry erst mal recht gegeben. So ist das bei Patentstreitigkeiten leider häufig: Mit gesundem Menschenverstand hat das oft nichts zu tun – und meist zahlen die Nutzer die Zeche (ehrlich gesagt immer, denn sie müssen auch anfallende Lizenzen irgendwie bezahlen).

Die Sache wird noch vor dem Bundespatentgericht verhandelt. Experte Müller meint: Die Funktion sei keineswegs schutzwürdig. Vielleicht wird dann wieder alles einkassiert und die Export-Funktion kommt in WhatsApp (und anderen Messengern) zurück.

Wichtig: Die Backup-Funktion lässt sich nach wie vor verwenden. Hier werden alle Chats auf dem Smartphone bzw. in der Cloud gesichert – und lassen sich bei Bedarf rekonstruieren, etwa bei einem Gerätewechsel.

https://vimeo.com/339064785

FTC erwägt Spaltung von Facebook, WhatsApp und Instagram

Facebook, WhatsApp, Instagram und Facebook Messenger: Diese vier Welten sind eigentlich gar keine vier Welten. Sie gehören alle zum Facebook-Konzern. Und der möchte die vier Dienste enger miteinander verknüpfen. Damit User aus dem einen mit Usern aus dem anderen Netzwerk chatten können, zum Beispiel. Das wurde schon vor Monaten angekündigt – und soll nun allmählich durchgeführt werden. Doch die Kontrollbehörde FTC (Federal Trade Commission) in den USA will das jetzt verhindern.

Laut „Wall Street Journal“ (WSJ) sind für diese Monat erste Schritte geplant: Die FTC will das Zusammenschmelzen der Dienste verhindern.

Mark Zuckerberg hat vor ziemlich genau einem Jahr angekündigt, die Dienste Facebook Messenger, WhatsApp und Instagram enger zu verbinden. Es soll möglich etwa sein, eine Nachricht aus Instagram an WhatsApp zu schicken, also alle Dienste untereinander zu verknüpfen. Denkbar ist sogar, aus der Facebook-Oberfläche heraus auf alle Messenger zugreifen zu können.

Facebook argumentiert: Cool für die User, denn die können dann bequem mit Usern aus allen Netzwerken kommunizieren, sogar mit WhatsApp. Das stimmt natürlich auch. Allerdings macht das Facebook noch viel mächtiger als ohnehin schon: Wie soll ein anderer Messenger jemals gegen diese Marktmacht ankommen? Unmöglich. Deshalb erwägt die FTC, diesen Zusammenschluss zu verbieten. Weil es wettbewerbsschädigend ist.

Verprechen gebrochen

Als Facebook sich den Messenger-Dienst WhatsApp vor einigen Jahren einverleibt hat, war doch eigentlich eine strikte Trennung von Facebook Messenger und WhatsApp Bedingung, um diesen Kauf zuzulassen.

Facebook hat WhatsApp 2014 für unglaubliche 19 Milliarden Dollar gekauft. Damals hieß es: Für WhatsApp-User würde sich nichts ändern. WhatsApp bliebe unabhängig. Bei der Übernahme von Instagram 2010 war es ganz ähnlich. Jetzt ist die Frage, was damit gemeint ist. Denn „unabhängig“ in dem Sinne, dass die Apps separat existieren, das ist durchaus der Fall. Allerdings musste Facebook auch zusichern, dass keine Daten von WhatsApp und Instagram zu Facebook fließen.

Wir wissen, dass das schon längst nicht mehr stimmt. Die Netzwerke sind miteinander verbunden. Es fließen sehr wohl Daten zum Facebook-Konzern und werden dort verarbeitet. Die Nutzerprofile werden verschärft. Eine klare Missachtung der Auflagen damals und ein klarer Bruch des Versprechend. Deshalb erwägt die FTC sogar, eine Zerschlagung von Facebook einzuleiten. Das ist leichter, wenn nun der Zusammenschluss der Messenger nicht genehmigt wird – deshalb wird die FTC gerade aktiv.

Netzwerke zusammengelegt

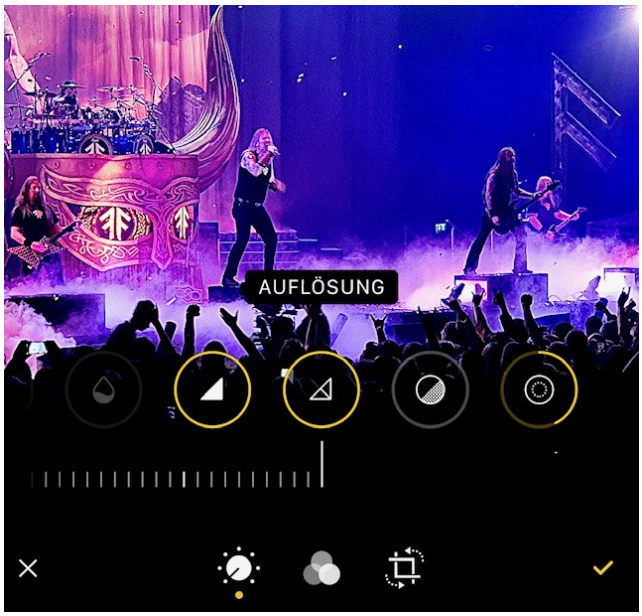
Fallen Facebook-Server aus, fallen oft auch WhatsApp und Instagram aus. Und wer Werbung schaltet bei Facebook und/oder im Facebook Messenger, kann bequem und gleichzeitig auch Werbung auf Instagram schalten. Ist alles längst eng miteinander vernetzt: Dieselbe Anzeige in allen Netzwerken. Nur in WhatsApp nicht, das ist noch werbefrei. Man muss wohl davon ausgehen, dass auch andere Daten, etwa Nutzungs- und Bewegungsdaten sowie soziale Netzwerke nicht in den jeweiligen Netzwerken verbleiben, sondern zusammengetragen werden. Facebook gibt so etwas aber immer erst zu, wenn es nicht mehr zu leugnen ist. Auf Versprechen oder Erklärungen kann man sich leider nicht verlassen – das zeigt die Vergangenheit eindeutig.

Natürlich: Es ist ungeheuer praktisch, wenn die User aller(!) Netzwerke miteinander kommunizieren könnten. Deshalb sollte das die Auflage sein: User aus jedem Netzwerk sollen mit Usern aus jedem anderen Netzwerk kommunizieren können. Die Netzwerke sollen sich öffnen. Das nennt sich Interoperabilität. Das wäre dann wirklich gut für die User – und für den Wettbewerb. Denn dann kann ich das sichere Threema nutzen und trotzdem mit einem User mit WhatsApp kommunizieren. Das will Facebook natürlich verhindern. Also ist die Aussage, Facebook läge das Wohl der User am Herzen, schlichtweg gelogen. In der Politik gibt es erste zarte Bestrebungen, die Interoperabilität voranzubringen.

Geheime Bildbearbeitungsfunktionen bei iOS

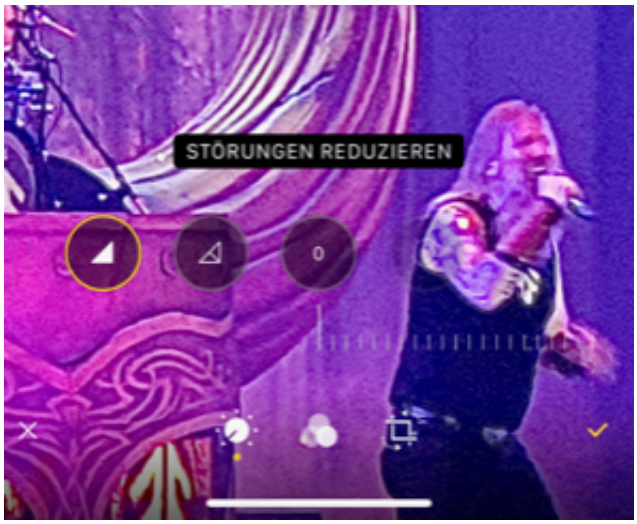
Die Kamera eines Smartphone ist auf dem Weg, die früher so gebräuchliche Immer-dabei-Kamera zu ersetzen. Auflösung, Farbtiefe, Bildqualität sind bei den Top-Modellen hervorragend, und Sie haben Ihr Smartphone sowieso dabei. Neben dem Schießen der Bilder kommt später ein weiterer Schritt hinzu: Die Bearbeitung. Auch wenn ein Bild schon gut aussieht, mit den richtigen Einstellungen können Sie noch deutlich mehr herausholen. Und das sogar ohne Zusatzsoftware!

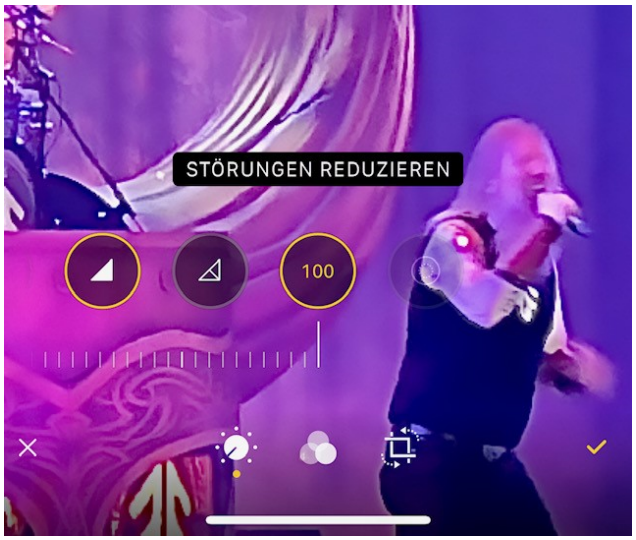
Apple hat bei den iPhones neben der Hardware, einer zusätzlichen Linse und einem neuen Sensor, auch bei der Software einen Riesenschritt gemacht. Der ist aber nicht auf den ersten Blick ersichtlich.



Wenn Sie ein Foto gemacht haben, dann lassen Sie es sich in der internen Foto-App anzeigen. Tippen Sie dann auf **Bearbeiten** oben rechts in der Fotoansicht. Im Standard finden Sie dort nur die Symbole für **Auto-Anpassung**, **Belichtung** und **Brillinz**. Die spannenden Funktionen aber zeigt Ihnen die App an, wenn Sie mit dem Finger nach links wischen: über 10 weitere Anpassungsregler kommen so Stück für Stück zum Vorschein.

Vor allem **Schärfe**, **Auflösung** und **Störungen reduzieren** haben erheblichen Einfluss auf die Bildqualität. Die ersten beiden helfen, das Bild zu schärfen. Das führt oft allerdings auch dazu, dass das Bild pixeliger wird.





Gegenteilige Wirkung hat **Störungen reduzieren**. Diese Funktion ist dazu da, sichtbare Pixel zu reduzieren. Diese entstehen beispielsweise in schlechten Lichtbedingungen. Das Bild wird damit glatter, aber in der Konsequenz auch unschärfer.

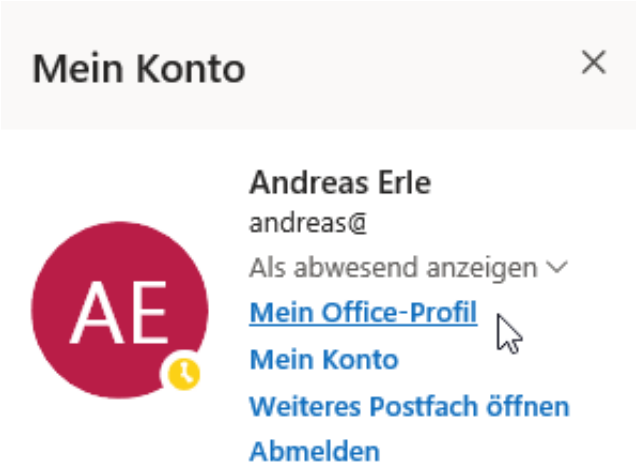
Den richtigen Effekt gibt es nicht, nur die Summe der spezifischen Einstellungen für das spezielle Bild, das Sie gerade bearbeiten wollen.

Schnellzugriff auf die Organisation bei Office 365

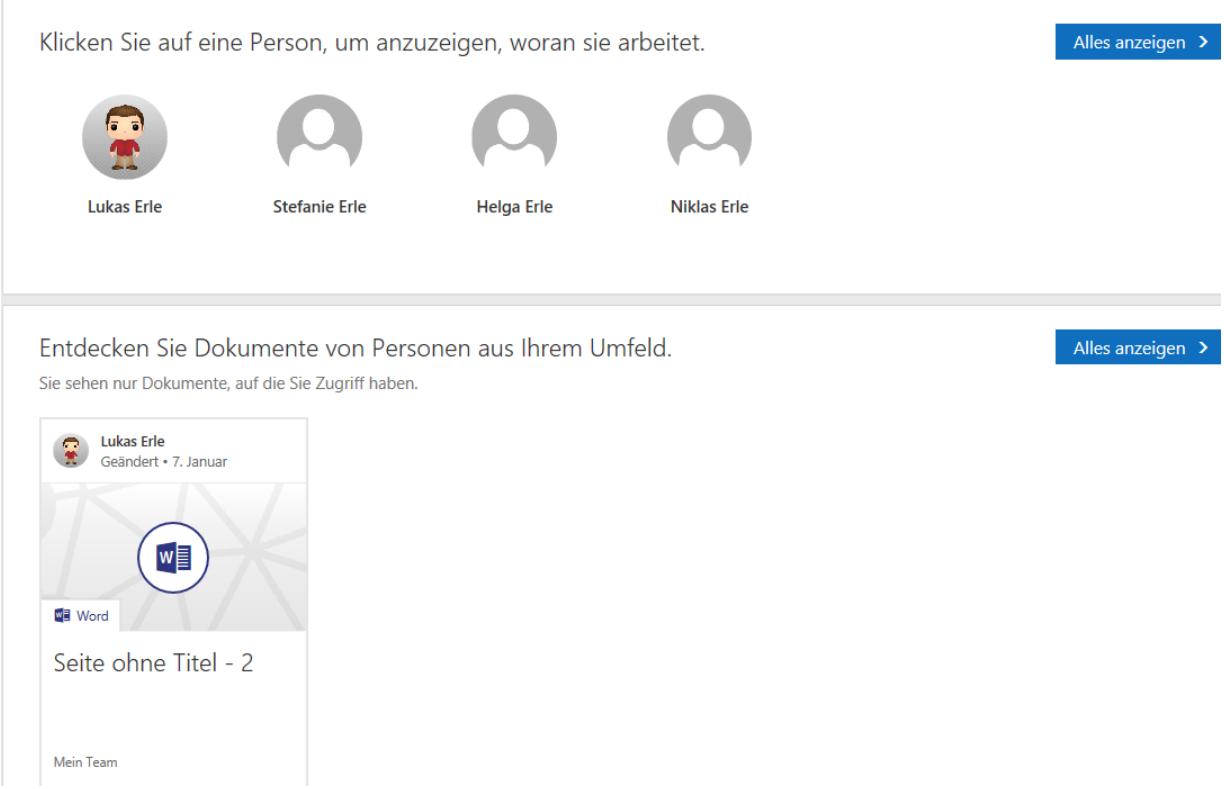
Office 365 hat ja den Ruf, eine Umgebung für Firmen zu schaffen. Das springt aber zu kurz: Auch für die private Anwendung - beispielsweise in der Familie - ist Office 365 eine große Hilfe. Die schnelle und unkomplizierte Zusammenarbeit in Dokumenten, Terminen und E-Mails kann Ihnen eine Menge Zeit sparen. Die Verwaltung der Organisation ist einfacher, als man denken würde.

Wichtig ist, dass Sie Berechtigungen für die einzelnen Konten haben. Idealerweise sind Sie Administrator für Ihre Organisation, denn dann haben Sie Zugriff auf alle Einstellungen. Ist das nicht der Fall, dann müssen Sie den Administrator ausfindig machen und ihn die Einstellungen vornehmen lassen.

Zugriff auf die generellen Einstellungen bekommen Sie auf der Administrationsseite von Office 365. Um nun in Ihrer Organisation auf die Dateien zugreifen zu können, klicken Sie in Ihrem Office 365-Konto (beispielsweise in Outlook) auf Ihr Kontobild, dann auf **Mein Konto**.



Sie sehen darin auf den ersten Blick alle Dateien, an denen Sie selbst zuletzt gearbeitet haben. Neben den Dateien im OneDrive finden Sie in der Übersicht auch die Dateien, die in E-Mails als Anhänge eingegangen sind.



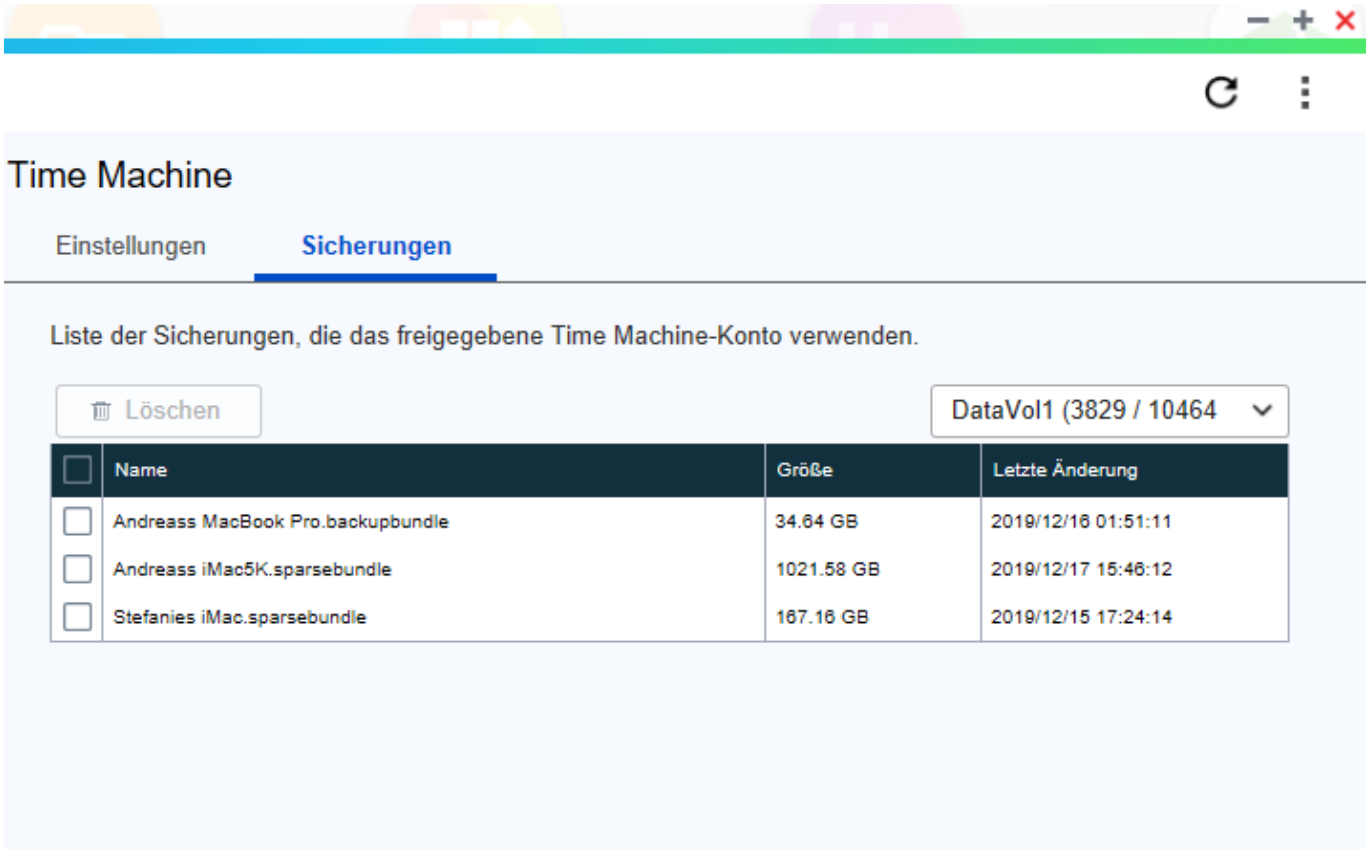
Darunter sehen Sie die Mitglieder Ihrer Organisation, beispielsweise der Familie. Für jedes Mitglied können Sie die Dateien, die dieses Ihnen freigegeben hat, sehen und öffnen. Das ist vor allem toll, wenn Sie den Freigabelink verloren haben.

Probleme mit Time Machine Backups auf dem Mac lösen

Datensicherungen sind der Garant für die schnelle Wiederaufnahme Ihrer Arbeit, wenn PC oder Mac einmal nicht mehr wollen. Wenn Sie einen Mac benutzen, dann werden Sie sicherlich das in macOS integrierte Time Machine nutzen. Das lässt sich ohne großen Aufwand einrichten und legt eine lupenreine Historie Ihrer Dateien an. Was aber, wenn die Sicherung nicht mehr so recht funktionieren will?

Die Einrichtung von Time Machine ist simpel: Schließen Sie eine Festplatte an Ihren Mac an, dann fragt dieser automatisch nach, ob Sie sie für Time Machine verwenden möchten. Bejahen Sie das, dann führt Ihr Mac oder MacBook in regelmäßigen Abständen automatisch Sicherungen der geänderten Dateien auf die Festplatte durch. Wenn Sie ein NAS haben, dann können Sie dieses in den allermeisten Fällen ebenfalls zur Datensicherung über Time Machine verwenden.

Schauen Sie in die Online-Hilfe Ihres NAS, um die Einrichtung durchzuführen.



Funktioniert eine Sicherung nicht, dann liegt das meist daran, dass entweder das Laufwerk nicht verführbar ist oder die Sicherungsdatei defekt ist. Kontrollieren Sie die Kabelverbindung zur externen Festplatte bzw. die Netzwerkverbindung. Sind diese in Ordnung, dann löschen Sie einmal die Backup-Datei.

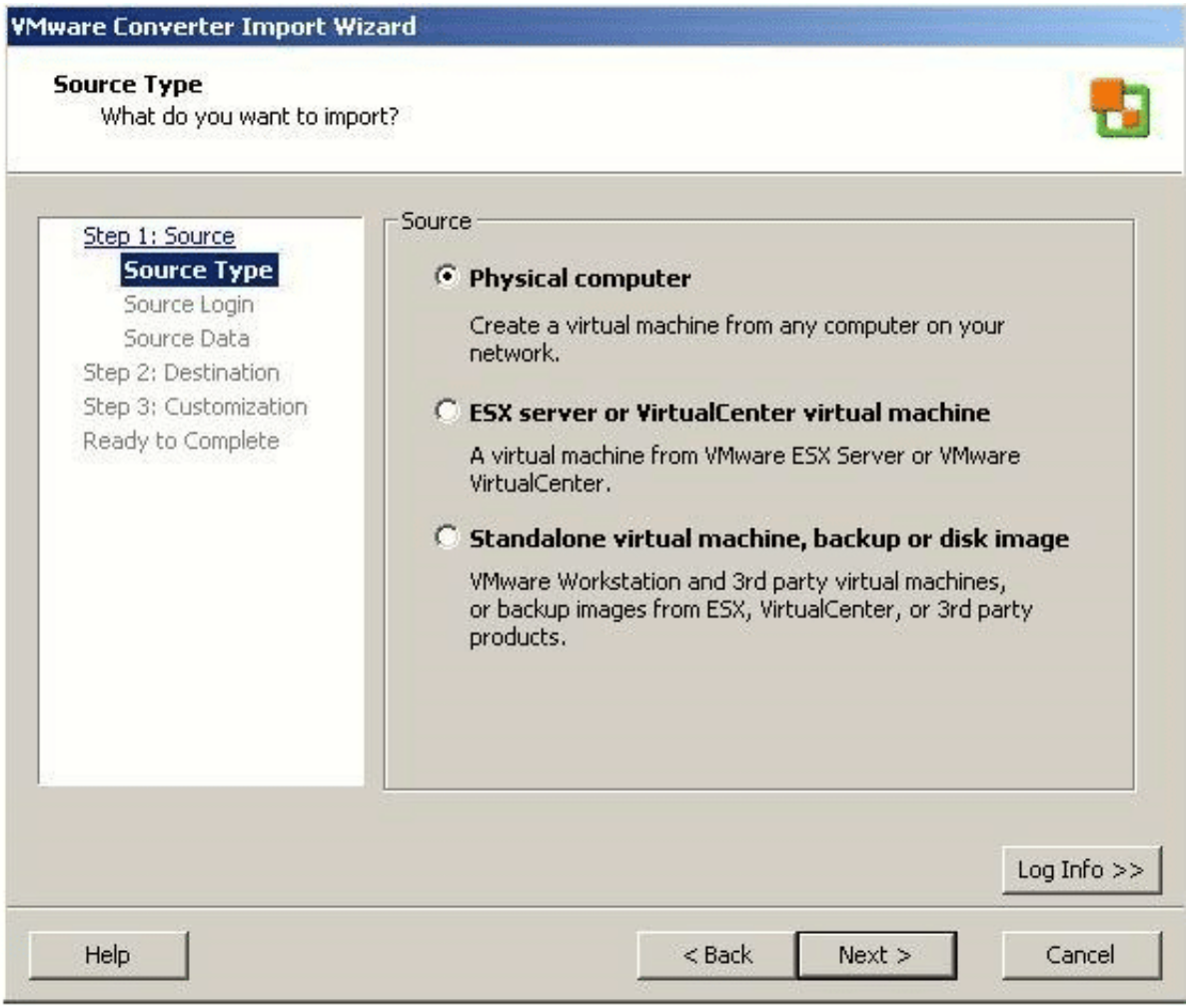
Es macht Sinn, in einem solchen Fall erst einmal alle wichtigen Daten Ihres Mac auf eine

externe Festplatte zu sichern, denn mit dem Löschen der Time Machine-Sicherung löschen Sie ja Ihr Backup komplett. Dann gehen Sie mit dem Finder auf die Time Machine-Festplatte. Dort finden Sie einen Eintrag, der en Namen Ihres Macs hat. Klicken Sie diesen an und löschen Sie ihn. Schalten Sie dann Time Machine auf dem Mac aus, entfernen Sie das Sicherungslaufwerk und koppeln Sie es erneut.

Windows in eine virtuelle Maschine umwandeln

Auf einem PC sammeln sich über Jahre, ja sogar Jahrzehnte Programme an, die Sie dringend brauchen. Viele davon werden irgendwann nicht mehr weiterentwickelt und stehen so einem Wechsel der Betriebssystemversion entgegen. Auch bei dem Wechsel auf einen anderen Rechner, den Sie frisch aufsetzen, kann es sinnvoll sein, den alten Rechner noch zur Verfügung zu haben. Die einfache Lösung, bei der Sie die alte Hardware nicht mehr behalten müssen: Überführen Sie Ihr altes Windows in eine virtuelle Maschine.

Damit können Sie den alten Rechner wie ein Programm auf einem anderen PC starten und Programme und Daten weiterverwenden. Einen Unterschied merken Sie – einen entsprechend leistungsfähigen PC vorausgesetzt – eher nicht.



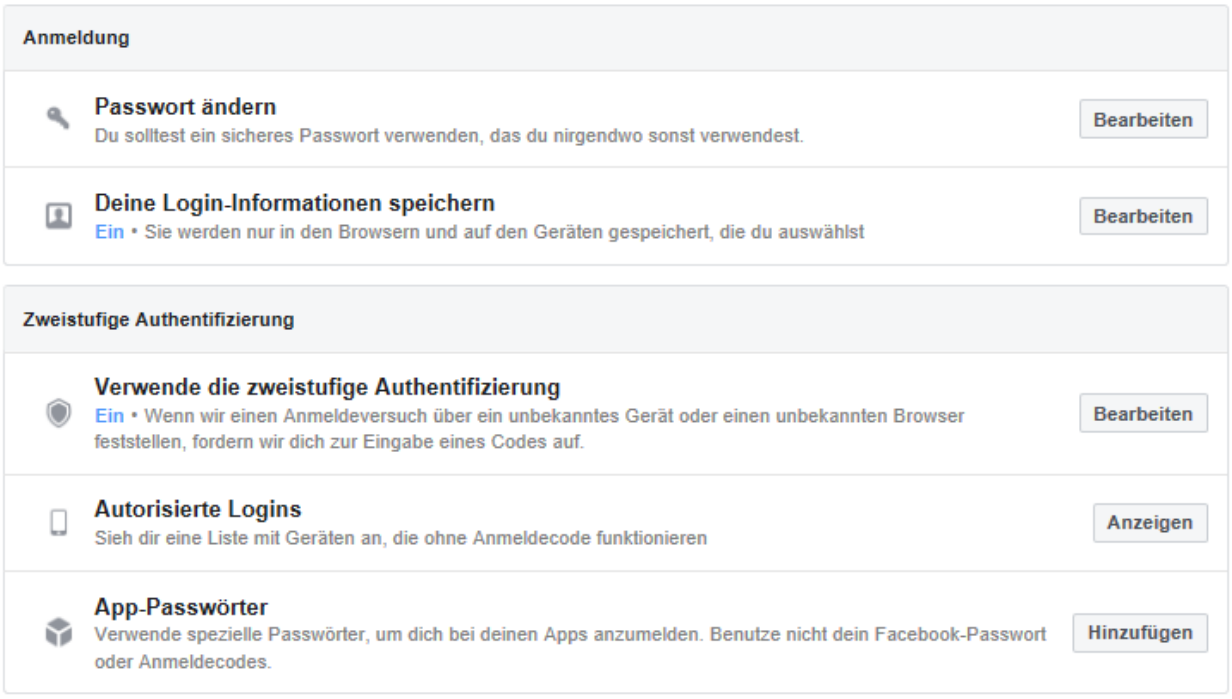
Ein kostenloses Tool dafür ist der VCenter Converter von VMWare. Folgen Sie nach Installation einfach den Anweisungen des Programms und wandeln Sie Ihren alten Rechner in eine virtuelle Maschine um. Diese können Sie dann mit dem ebenfalls kostenlosen VMPlayer auf Ihrem Windows 10 PC ausführen und damit auf alle Programme und Daten weiterhin zugreifen.

Wichtig dabei: Alle Änderungen, die Sie auf der virtuellen Maschine vornehmen, haben natürlich keinerlei Auswirkungen auf Ihren neuen PC. Die virtuell Maschine läuft in einer Sandbox, einem komplett abgeschotteten System, das keine Verbindung nach außen hat. Sie sollten also Datensicherungen auf USB-Sticks machen, um geänderte Dateien auch auf dem normalen PC zur Verfügung zu haben.

Vorsicht bei Paßwortwechseln bei Facebook

Ihr Passwort ist ohne Frage der Kern Ihrer Sicherheitsstrategie. Ohne dieses - und im besten Fall verwenden Sie noch einen zweiten Faktor wie einen wechselnden Zahlencode - sind Sie Angriffen ausgesetzt. Hat ein Angreifer die Zugangsdaten, dann kann er mit Ihrem Konto machen, was er will. Vorbeugend sollten Sie es dann auch in regelmäßigen Abständen ändern. Das kann bei Facebook aber ungewollte Nebeneffekte haben!

Facebook ist ja nicht nur soziales Netzwerk, sondern auch ein Anmeldedienst. Eine zunehmende Zahl von Webseiten nutzt das Anmelden per Facebook mittlerweile als Anmeldemethode. Statt ein eigenes Konto anlegen zu müssen, können Sie sich mit Ihrem Facebook-Konto anmelden. Die Webseite ruft dazu Facebook auf, Sie melden sich bei Facebook an und Facebook meldet dann einige Informationen (Wie Name und E-Mail-Adresse) und die erfolgreiche Anmeldung an die Webseite zurück. Der Vorteil: Ihre Anmeldedaten bleiben auf der Facebook-Seite und Sie müssen sich nur ein Kennwort merken.



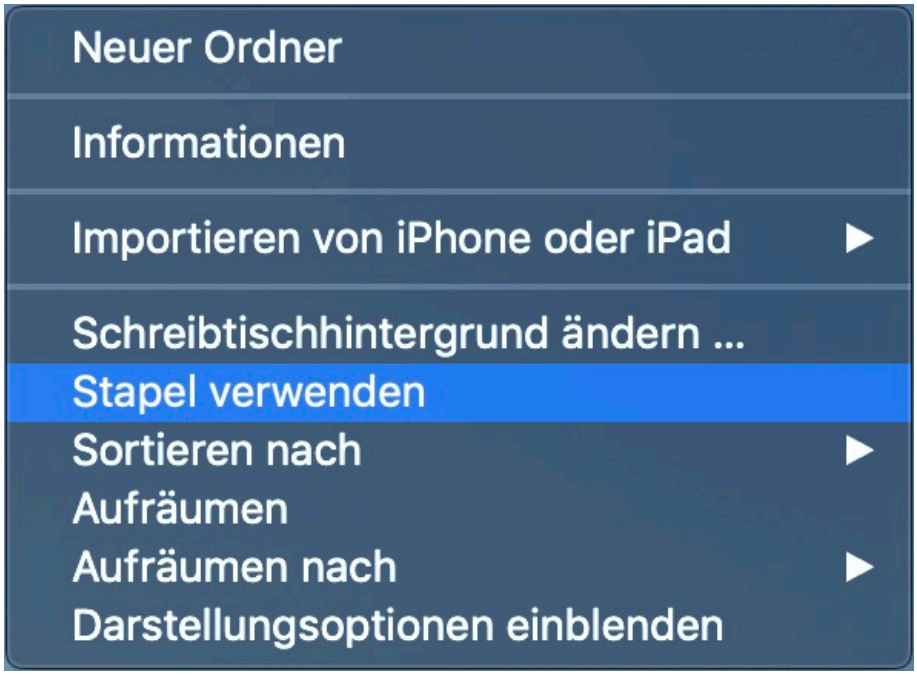
Ändern Sie das Kennwort, dann weiß Facebook das. Die Webseiten, die sich mit Facebook anmelden, ebenfalls. Ihre ganzen Apps aber, die auf das Facebook-Konto zugreifen, die eben nicht. Je mehr Geräte Sie einsetzen, desto mehr Anmeldungen registriert Facebook mit dem falschen Kennwort. Das wird schnell als Hacking-Versuch erkannt. Facebook denkt, dass ein Fremder sich an Ihrem Konto anmelden will und Passwörter durchprobiert und sperrt schnell Ihr Konto. Der Verwaltungsaufwand, dieses wieder frei zu bekommen, ist nicht unerheblich.

Die Lösung: Nach einem Passwortwechsel kontrollieren Sie alle Geräte (Smartphones wie Notebooks, Tablets und Desktops) und ändern Sie dort das Kennwort ebenfalls. Damit minimieren Sie die Zahl der Fehlversuche und damit die Kontosperre.

Mehr Ordnung auf dem Mac-Schreibtisch: Stapel

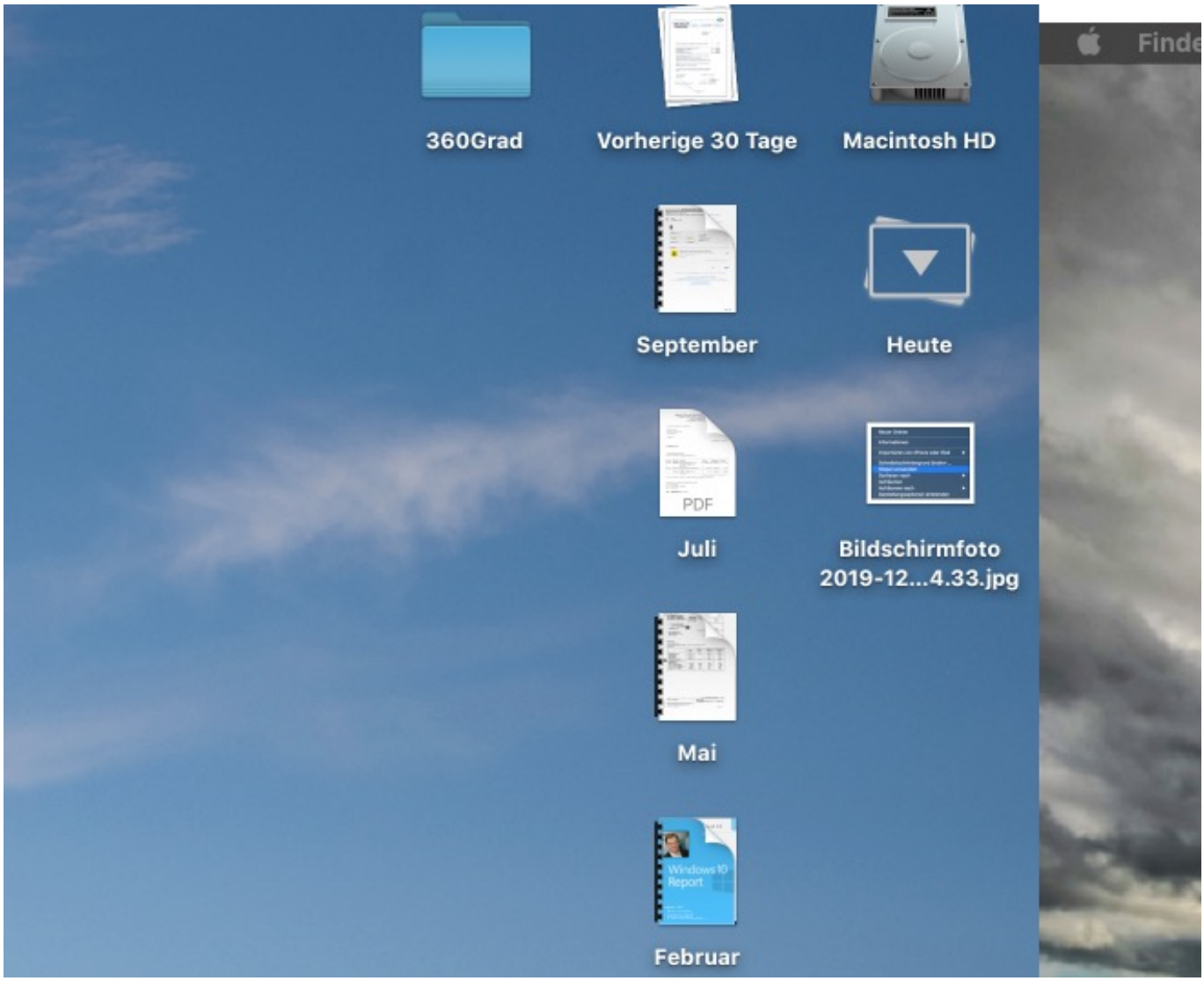
Der Schreibtisch ist auf einem PC oder Mac wie im wahren Leben der Ort, an dem Sie eben schnell mal etwas ablegen. "Eben schnell" hat nur leider die Eigenschaft, dauerhafter zu sein, als der Begriff erwarten ließe. Schnell kommt das nächste abzulegende Objekt, und schon beginnt das Chaos. MacOS bietet Ihnen dazu die Stapel.

Die Idee dahinter: Auf Ihrem normalen Schreibtisch gehen Sie zum besseren Überblick auch dazu über, Stapel aus gleichartigen Dokumenten zu Bilden. Das selbe versucht macOS mit den virtuellen Stapeln zu erreichen. Klicken Sie mit der rechten Maustaste auf den Schreibtisch, dann auf **Stapel verwenden**.



Im Standard sortiert macOS jetzt alle Elemente auf dem Desktop auf Stapel, die nach dem Dateityp sortiert sind: Ein Stapel für die Dokumente, einer für die PDFs, einer für Bilder und so weiter. Das können Sie aber schnell ändern: Klicken Sie wieder mit der rechten Maustaste auf den Schreibtisch, dann auf **Stapel gruppieren nach**.

Sie können nun verschiedene Sortierkriterien angeben. Legen Sie Dokumente nach Tagen ab? Dann wählen Sie **Änderungsdatum** oder **Erstellungsdatum**. Wenn Sie Ihren Dateien **Tags** zuweisen, dann können Sie diese auch als Stapelkriterium verwenden.



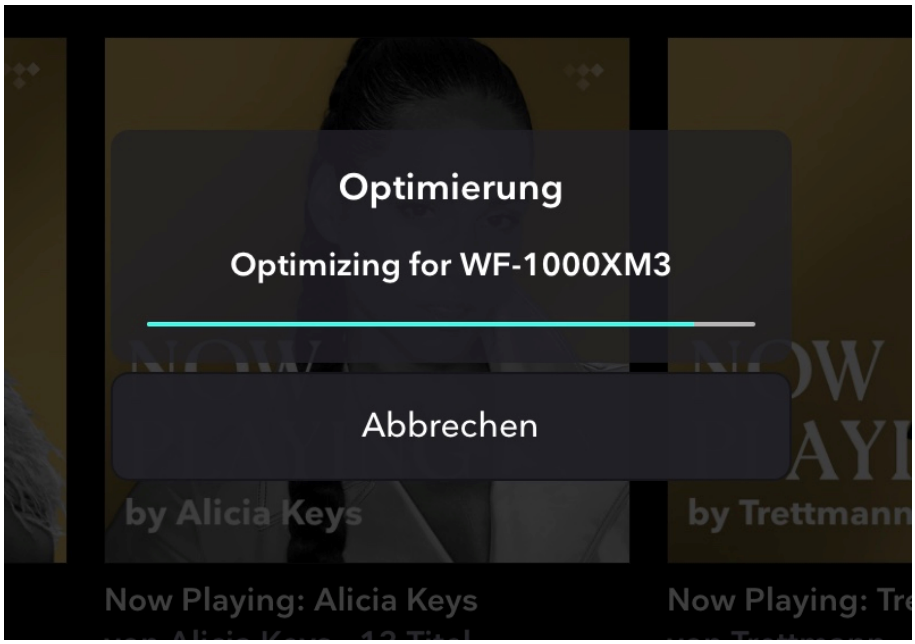
Keine Sorge: Wenn Sie einmal einen Stapel gebildet haben und das für Sie nicht mehr passt, dann können Sie problemlos wieder zurück zum manuellen Chaos Ihres Schreibtisches. Deaktivieren Sie dazu einfach die Anordnung nach Stapeln über das beschriebene Kontextmenü.

360 Reality Audio-Musik bei Tidal nutzen

Im Bereich Musik und Klang gab es schon gefühlt unendlich viele neue Funktionen, mit denen die Immersion, also das Eintauchen des Hörers in das Klangmaterial verbessert werden sollte. 3D-Sound, Dolby Surround und DTS waren nur einige Vertreter der neuen Soundeffekte. Jetzt kommt mit dem 360 Reality Audio-Sound eine weitere Welle auf Ihre Ohren zu, die Sie bereits nutzen können.

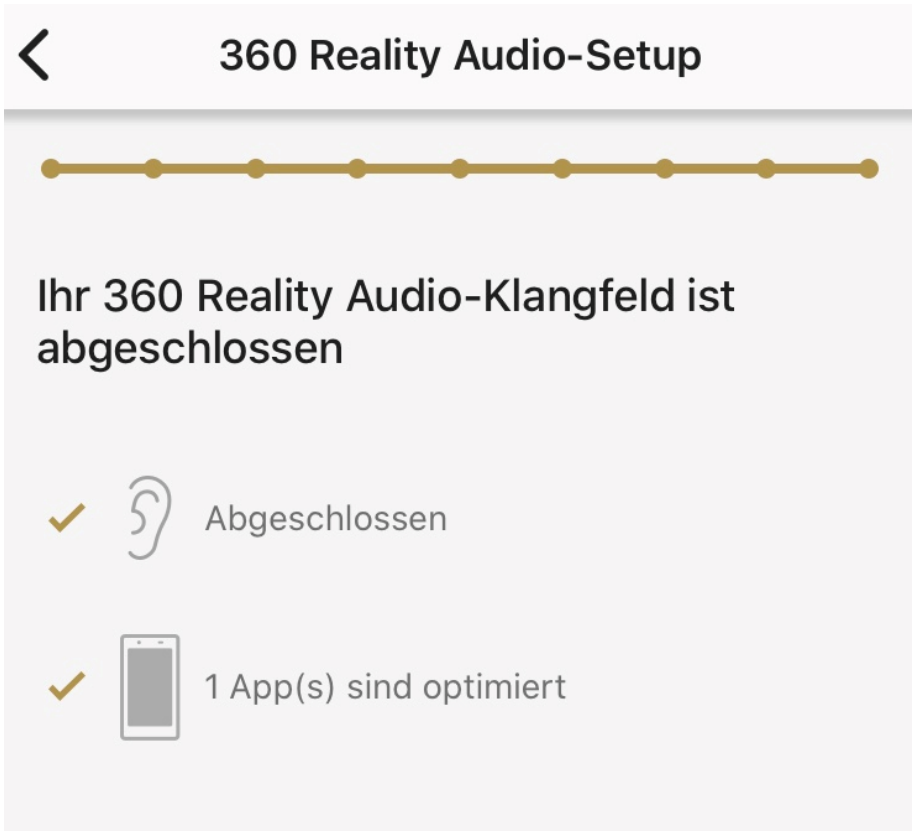
Die Idee hinter 360 Reality Audio ist die viel feinere Verortung von Instrumenten und Stimmen im Raum. Normale Kopfhörer und Boxen schaffen ein "plattes" Klangbild: Instrumente finden sich eher links oder eher rechts im Mix, aber eben nur zweidimensional. Wenn Sie Live-Musik hören, dann sind die einzelnen Instrumente ja auch im Raum verteilt, was ein deutlich differenzierteres Klangbild ergibt.

Dieses versucht Sony jetzt zu erreichen. Dazu sind zwei Voraussetzungen nötig: Das Endgeräte - der Lautsprecher oder Kopfhörer - muss es unterstützen, und das Klangmaterial muss es ebenfalls. Aktuell bietet Sony die Hardware an und kooperiert für die Musik mit diversen Onlinediensten wie Tidal und Deezer.



Die unterstützenden Apps für die Kopfhörer vermessen als erster durch ein Foto die Form der Ohren. Dies sorgt dafür, dass eine Anpassung auf die spezifischen Anforderungen eines jeden Benutzers möglich ist. Das daraus erzeugte Profil wird dann in die Anwendung, die die 360 Reality Audio-Inhalte abspielt, übertragen.

Nun müssen Sie über die Streaming-App nur noch die Inhalte finden: Bei Tidal beispielsweise tippen Sie dazu auf **Entdecken** > **360 Reality Audio**.

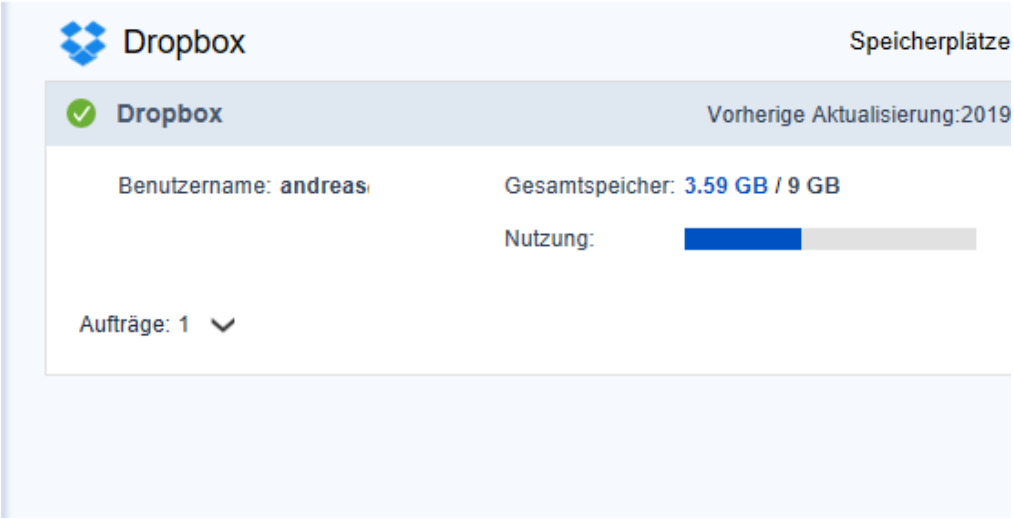


Backup von Dropbox und OneDrive auf ein QNAP NAS automatisieren

Haben Sie schon mal was von der Private Cloud gehört? Cloud Services kennen Sie sicherlich. Datenspeicher irgendwo im Internet, auf denen Ihre Daten gespeichert sind. Bei denen müssen Sie sich keine Gedanken über deren Sicherheit und Verfügbarkeit machen. Der Trend ist aber gerade gegenläufig: Wenn Sie die Cloud nutzen, aber die Sicherheit Ihrer eigenen Festplatten oder Netzwerkspeicher haben wollen, dann schaffen Sie sich eine eigene Lösung.

QNAP hat als Standard-Sicherungslösung die Hybrid Backup Sync-App (HBS) vorgesehen. Wenn diese auf Ihrem NAS noch nicht installiert ist, dann holen Sie das über den QNAP App Store auf dem NAS nach. Starten Sei die App, dann klicken Sie auf das untere Symbol auf der linken Seite, das als Kurztext **Speicherorte** anzeigt. Klicken Sie auf **Erstellen**, dann wählen Sie den Online-Service, von dem Sie die Daten sichern wollen. Sie werden automatisch zum Anmeldebildschirm des Dienstes geleitet und melden sich dort an. Der Vorteil: Ihre Anmeldedaten speichert das NAS nicht, sondern nur einen Token, quasi eine gültige Eintrittskarte für den Cloudspeicher!

Nun können Sie unter **Synchronisieren** > **Erstellen** > **Aktiver Synchronisierungsauftrag** einen neuen Auftrag einstellen. Als Quelle geben Sie dann den neu angelegten DropBox- oder OneDrive-Speicherplatz an, als Ziel einen beliebigen Ort auf Ihrem NAS.


Dropbox
Speicherplätze
Dropbox
Vorherige Aktualisierung:2019
Benutzername: andreas
Gesamtspeicher: 3.59 GB / 9 GB
Nutzung:
Aufträge: 1