# Schieb Report

Ausgabe 2020.05

# Livescribe hinter einem Proxy mit Authentifizierung betreiben

Wenn Sie auf Papier schreiben wollen, aber die Daten direkt digital zur Verfügung haben wollen, dann ist der LiveScribe eine tolle Alternative. Vom Grundsatz her ist dieser ein etwas überdimensionierter Kuli, der einen eingebauten Speicher von 2 oder 4GB hat und auf Anoto-Papier schreibt. Das Papier ist mit fast unsichtbaren Minipunkten versehen, die von der unter der Mine installierten Minikamera des Stiftes aufgenommen werden und so millimetergenau die Position des Stiftes mit aufnehmen. Wenn die Übertragung zum PC dann aber nicht funktioniert, dann ist eine mögliche Ursache die Verwendung eines Proxy-Servers.

Der Stift wird immer an einen (kostenlosen) Livescribe-Account gekoppelt, und dieser wird vor Übertragung der Notizen abgefragt. Das soll sicherstellen, dasst nur der berechtigte Benutzeran die Daten kommt. Mittlerweile unterstützt die Software auch die Nutzung eines Proxys. Dazu wird allerdings die Proxy-Authentifizierung benötigt. Ohne die bricht die Kommunikation immer mit einer Fehlermeldung, man könne nicht auf das Internet zugreifen, ab.


Livescribe selbst schliesst in seiner Knowledgebase in einem solchen Fall, man könne den Stift nicht einsetzen. Die Lösung aber ist einfach und kann auch ohne Admin-Rechte umgesetzt werden:

Im Programmverzeichnis findet sich die Datei *Livescribe Desktop.exe.config*. In diese muss nach dem ersten Programmstart ans Ende, vor dem schließenden  folgendes Code Snippet

eingefügt werden:

Dieses weist das Programm an, für die Internetverbindung die Standardauthentifizierung des Desktops am Proxy zu verwenden (sprich: die Anmeldedaten am System weiterzureichen).

# Schnelleres Laden des Smartphones

Eine der kritischen Größen bei der Nutzung von Geräten unterwegs ist die Stromversorgung: Ist der Akku leer, ist die Nutzung schnell am Ende. Um so wichtiger ist es, wenn Sie Ihr Smartphone so bequem und einfach wie möglich laden. Je einfacher und schneller das geht, desto eher machen sie es eben mal nebenbei. Wir zeigen, worauf Sie achten müssen.

Zu allererst müssen Sie natürlich den richtigen Ladestecker für Ihr Smartphone haben. micro-USB, Lightning (für fast alle Apple-Geräte) und USB-C (für neuere Android-Smartphones und einige iPads) sind hier gebräuchlich. Die meisten Smartphones laden mit 5 Volt, sodass Sie kein separates Netzteil brauchen. Sie können das Kabel an jeden USB-Anschluss anschließen können.

Das ist aber recht langsam. Mehr Spaß macht das Laden, wenn Sie ein Netzteil mit Quick Charge haben und das Smartphone dies unterstützt: Damit kann das Gerät - je nach Version - innerhalb weniger Minuten soweit aufgeladen werden, dass es einige Stunden mehr durchhält. Wichtig dabei: Finger weg von den so genannten Schnelladekabeln! Bei diesen wird durch Kurzschluss von zwei Leitungen simuliert, dass das Gerät von der USB-Schnittstelle nahezu unlimitiert Strom ziehen kann. Das kann funktionieren, kann aber auch den USB-Port oder das Netzteil schädigen.

Die Königklasse ist das kabellose Laden per Qi (sprich "Chi"). Viele neuere Android-Geräte und die iPhones ab der XS-Serie unterstützen dies: Legen Sie das Smartphone auf eine entsprechende Ladeschale, dann müssen Sie keinen Stecker ins Gerät stecken. Das Laden funktioniert per Induktion.

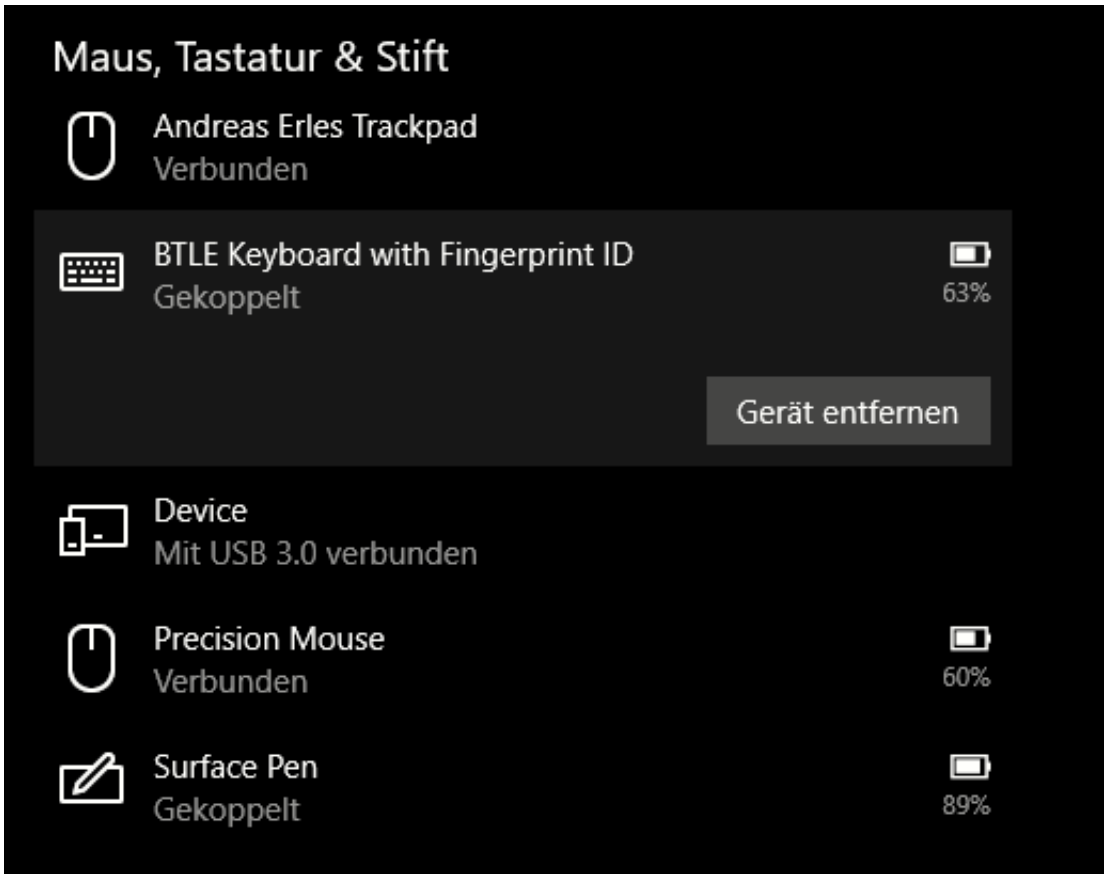
# Probleme mit dem Microsoft Surface Keyboard lösen

Neben den Type Covern für die Microsoft Surface Tablets gibt es auch diverse Tastaturen von Microsoft, die nicht nur an Surface-Geräte, sondern auch an beliebige andere Windows-PCs angeschlossen werden können, so zum Beispiel das Surface Keyboard. Diese Geräte haben natürlich auf normalen Windows 10-Geräten nicht die selbe Softwareunterstützung. Trotzdem lassen sie sich betreiben!

Der erste Schritt zur Nutzung ist der Anschluss an Ihren PC mit dem beiliegenden USB-Kabel. Damit wird nicht nur initial die Verbindung hergestellt, sondern auch die Tastatur in den Kopplungsmodus versetzt. Windows10 erkennt automatisch das neue Gerät und lädt die benötigte Software herunter. Damit wird beispielsweise auch der integrierte Fingerabdruck-Scanner der Surface Keyboards aktiviert.

Nach kurzer Zeit können Sie die Tastatur dann ganz normal benutzen. Was aber, wenn diese dann nicht funktionieren will? Nicht selten verweigert diese die automatische Verbindung per Bluetooth nach einem Neustart. In einem solchen Fall schließen Sie sie wieder mit dem Kabel an. Sonst wird die Anmeldung an Windows mit einem Kennwort schwierig.

Dann klicken Sie auf **Einstellungen** -> **Bluetooth** und schauen Sie unter den den gekoppelten Geräten nach der Tastatur: Rechts neben jedem akkubetriebenen Gerät finden Sie eine Prozentzahl, die den Ladezustand angibt. Ist dieser einstellig, dann sollten Sie die Tastatur umgehen laden!



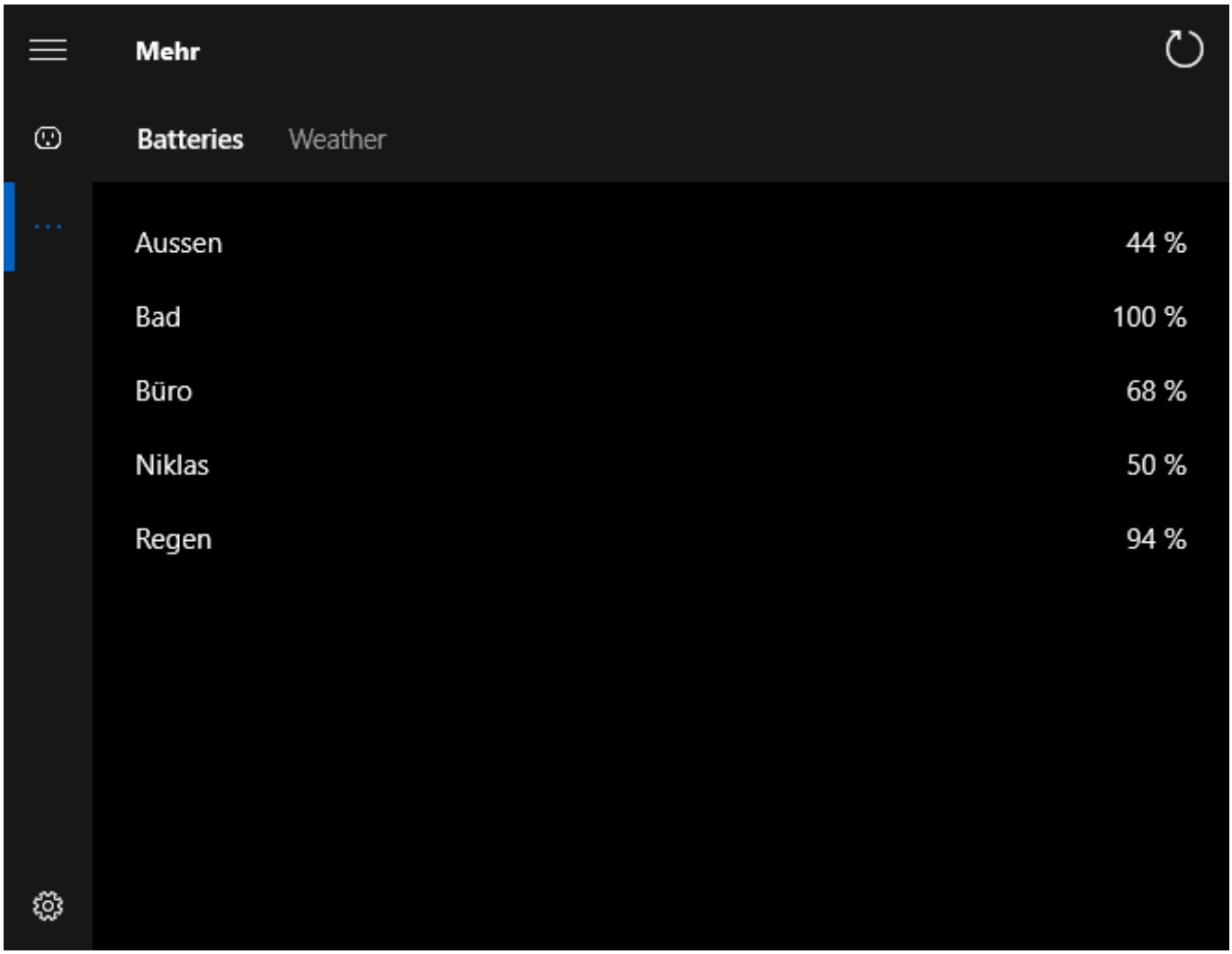

Sollte die Tastatur auch nach dem Laden noch nicht wieder funktionieren, dann lassen Sie sie angeschlossen und starten eine neue Suche nach Bluetooth-Tastaturen. Nach einem Moment ist sie dann wieder verbunden!

# Smarthome-Geräte verwalten unter Windows 10

Windows 10 ist nie als mobiles Betriebssystem wahrgenommen worden. Weder in seiner mobilen Version Windows Phone/Mobile, noch in der Desktop-Version. Auch wenn viele Tablets und Notebooks dauernd unterwegs wie ein mobiles Gerät genutzt werden, gibt es wenig Software, mit der Sie unter Windows Smarthome-Geräte nutzen können. Home Remote ist eine leider noch sehr unbekannte Ausnahme!

Die App existiert - ein seltenes Fall - nicht nur für Windows oder nur für Android und iOS, sondern für alle Systeme gleichzeitig. Die Windows-Version können Sie für EUR 2,99 hier herunterladen, die mobilen Versionen im App Store Ihres Smartphones.


Nach der Installation können Sie dann aus einer riesigen Liste von unterstützten Smarthome-Geräten auswählen. Unter anderem die verbreiteten Anbieter Netatmo, Kasa und Hue, aber auch kleinere wie ecobee und Fibaro. Für jedes Gerät, dass Sie Ihrem Haus hinzufügen, müssen Sie dann einmal die Verbindung herstellen. Das funktioniert durch die Anmeldung an den entsprechenden Webseiten der Hersteller, die über die App aufgerufen werden.

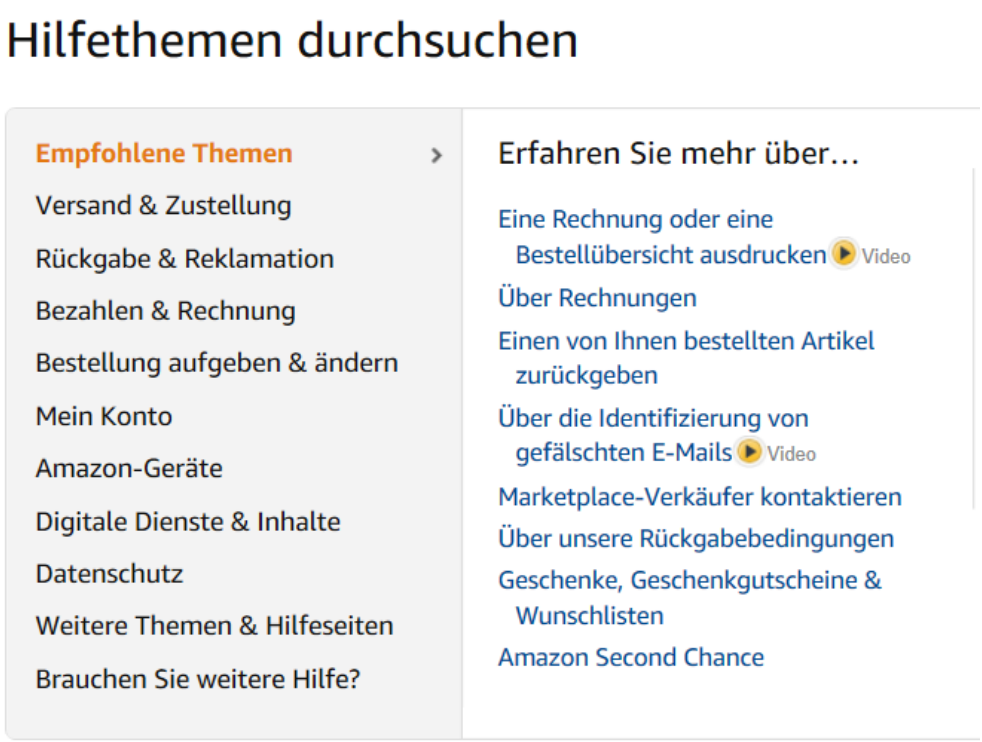



Gegebenenfalls müssen Sie - z.B. bei Hue - noch eine Kopplung mit dem Smartphone-Hub herstellen. Danach werden die Geräte dann erkannt und dargestellt. Sie können nun wie aus den Einzelapps Gruppen von Geräten bilden und diese über die Windows-App ansteuern. Die Werte, die von den Smarthome-Geräten ausgelesen werden, bekommen Sie übersichtlich auf dem Bildschirm dargestellt.

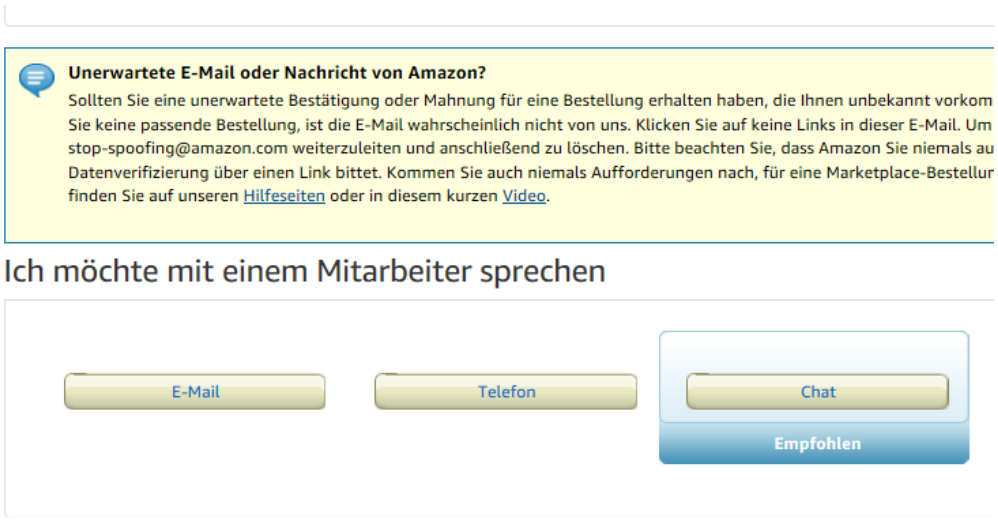
# Hilfe zu einer Bestellung/Rücksendung bei Amazon.de

Der Einkauf bei Amazon geht normalerweise schnell und unkomplizert: Sie suchen Artikel aus, legen sie in den Warenkorb, bezahlen sie, und im Idealfall halten Sie am nächsten Tag die Ware in der Hand. Auch die Rücksendung geht unkompliziert direkt aus der Bestellübersicht. Wenn Sie aber schnell eine Frage zu einer Bestellung oder Rücksendung beantwortet haben wollen, ist das komplizierter.

Eine direkte Kontaktaufnahme abseits der automatisierten Prozesse scheint beim Amazon nicht wirklich gewünscht zu sein und wird dem Kunden entsprechend schwer gemacht. Suchen sie nicht in Ihrer Bestellübersicht nach Kontaktmöglichkeiten. So intuitiv das sein mag, dort werden Sie nicht fündig. Stattdessen klicken Sie ganz unten am Bildschirmrand auf **Hilfe**. Sollte die Bestellung weiter in der Vergangenheit liegen, dann suchen Sie sie aus der Bestellübersicht heraus und kopieren Sie schon einmal die Bestellnummer in die Zwischenablage.




In der Liste der Auswahlmöglichkeiten haben Sie jetzt die Möglichkeit, auf **Brauchen Sie weitere Hilfe?** -> **Kontaktieren Sie uns** zu klicken. Nun müssen Sie die Bestellung, um die es geht, heraussuchen. Entweder klicken Sie diese in der Übersicht an, oder geben Sie die Bestellnummer im Suchfeld ein.

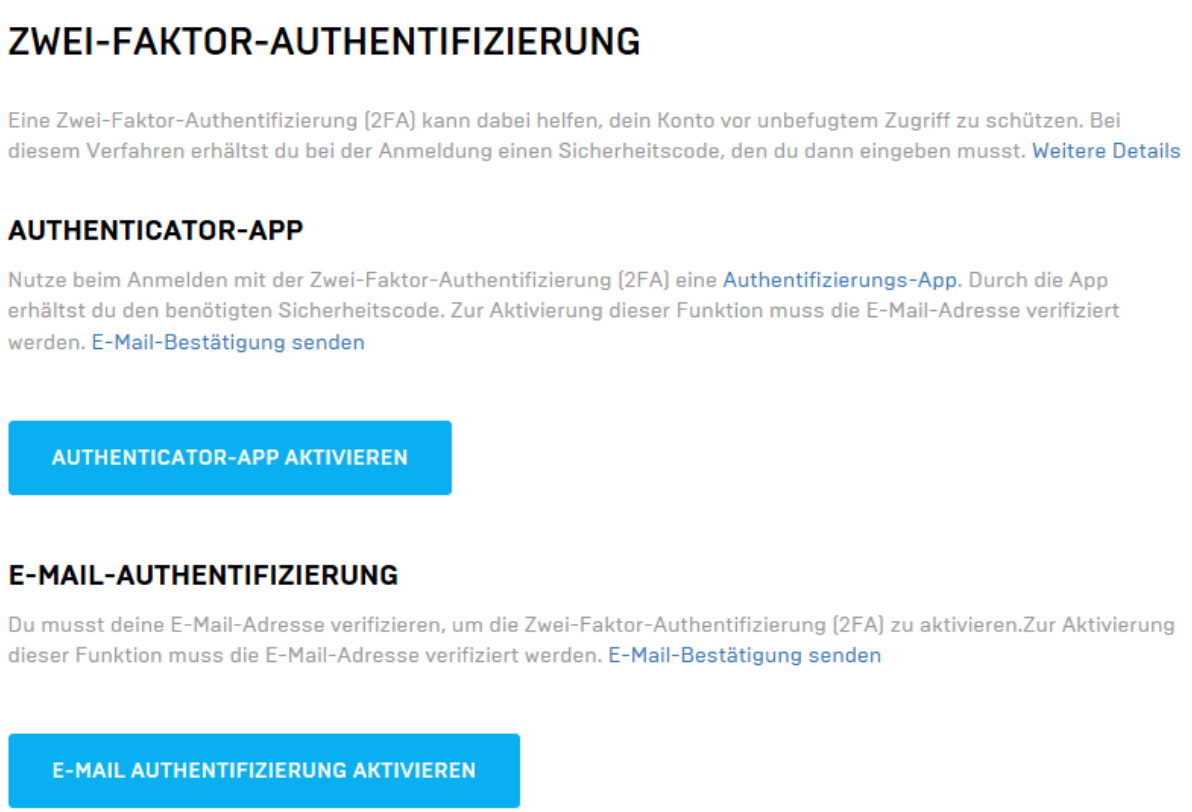



Klicken Sie den Artikel aus der Bestellung an, dann wählen Sie den Grund der Kontaktaufnahme aus den Auswahllisten an. Danach wählen Sie aus, ob Sie per **E-Mail**, **Anruf** oder Chat **Kontakt** aufnehmen wollen. Je nach Artikel und Art der Frage stehen gegebenenfalls nicht alle Kontaktmöglichkeiten zur Auswahl.

# Zwei-Faktor-Authentifizierung für Fortnite aktivieren

Eigentlich ist es kaum zu glauben, wie erfolgreich ein (vermeintlich) kostenloses Spiel wie Fortnite ist. Eine zweistellige Millionenzahl von Menschen weltweit stürzt sich regelmäßig in virtuelle Schlachten und versucht, möglichst lange gegen übermächtige Gegner zu überleben. Je länger Sie spielen, desto mehr Fortschritt und Entwicklung der eigenen Figur erreichen Sie. Da macht es Sinn, Ihr Fortnite-Konto so gut wie möglich zu schützen.

Die vermeintliche Gratis-Mentalität von Fortnite ist schnell am Ende: Wer ohne Aufrüstungen spielt, verliert schnell den Spaß. Zusätzliche Waffen, Ausrüstungsgegenstände und Tänze sind nahezu Pflicht, kosten aber Geld: Die virtuelle Währung "VBucks" lässt sich kaufen - für reales Geld. Meldet sich also ein Fremder mit Ihren Kontodaten an und sperrt Sie aus, dann ist der Verlust durchaus rechenbar. Fortnite bietet hier ebenfalls die Möglichkeit der Zwei-Faktor-Authentifizierung (2FA) an. Damit müssen Sie nicht nur das Kennwort eingeben, sondern noch einen stetig wechselnden zusätzlichen Code.




Um dies einzuschalten, melden Sie sich an Ihrem Epic Games-Konto an. Klicken Sie dann auf **Konto** -> **Passwort und Sicherheit**. Im unteren Teil der Seite können Sie die Zwei-Faktor-Authentifizierung aktivieren. Dazu können Sie auswählen, ob Sie als zweiten Faktor eine E-Mail bekommen wollen oder eine separate App dafür nutzen wollen. Nach Aktivierung können Sie sich ohne den definierten zweiten Faktor anmelden.

# Digitalisierung: Nur Bequemlichkeit – oder Menschheitsgewinn?

Die Digitalisierung scheint nicht mehr aufzuhalten. Sie dringt in praktisch alle Bereiche unseres Lebens vor und ein. Per Smartphone. Per Smarthome. Cloud. 5G. Ohne Digitalisierung scheint nichts mehr zu gehen. Und vieles scheint wirklich einfacher, bequemer, transparenter, demokratischer zu werden durch die Digitalisierung. Aber es gibt auch einige Schattenseiten.

"Digitalisierung first, Bedenken second." Ein Wahlspruch aus dem letzten Bundestagswahlkampf.

Ein Spruch, der fast so zweischneidig ist wie die Digitalisierung und Vernetzung selbst. Der Begriff "Digitalisierung" ist offensichtlich populär genug, um auf einem Wahlplakat zu stehen. Aber "Bedenken second" ist aus meiner Sicht alles andere als klug, Dumm ist es. "Digital first, Bedenken second" heißt nichts anderes als: Erst mal machen – und später nachdenken. Wenn überhaupt.

## Digitalisierung lässt sich nicht ignorieren

Das können wir heute nicht mehr tun. Denn Digitalisierung dringt in jede Ritze unseres Lebens. Ob wir es wollen oder nicht. Bitte nicht falsch verstehen, die Digitalisierung und Vernetzung hat die Welt verändert und oft zum Positiven. Wir erfahren in Sekunden, wie es Verwandten auf der anderen Seite der Welt geht. Kleinbauern in Entwicklungsländern können auf ihrem Smartphone die Weltmarktpreise für Kaffee vergleichen, um nicht betrogen zu werden und fast jede Frage, die wir haben beantwortet das Netz sofort.

Auf der anderen Seite nervt die ständige Vernetzung auch unglaublich, immer online, immer eine Datenspur hinterlassend, immer gläserner. Die Digitalisierung hat strahlende Licht und düstere Schattenseiten - Klar, wir entscheiden selbst, ob wir ein Smartphone haben wollen und wie wir es nutzen. Aber allzu oft bleibt uns kaum eine Wahl. Zum Beispiel, ob wir WhatsApp benutzen wollen. Wenn nicht, bleiben Eltern von Kindern außen vor beim Klassen-Chat oder bekommen keine Infos aus dem Sportverein. Digitalisierung ist also quasi ein Muss geworden.


## Abhängigkeiten nehmen dramatisch zu

Es gibt wirklich viele Beispiele, die mir einfallen, wo Digitalisierung das eigene Leben bequemer zu machen scheint. Ich kann online einkaufen, von unterwegs im Smarthome die Temperatur im Wohnzimmer für meine Ankunft hochstellen. Auf Fingertipp ein Taxi bestellen. Die Rechnung landet im Gerät. Bezahlt wird mit einem digitalen Zahlungssystem. Wie praktisch.

Aber die Abhängigkeiten nehmen zu. Was, wenn das Smartphone weg ist – oder kaputt? Wie öffne ich das Garagentor, wenn alles elektronisch und digital funktioniert? Was ist, wenn mal der Internetzugang ausfällt, oder der Strom? Ganz zu schweigen davon, dass alles, was vernetzt ist, auch angreifbar ist. Und schon öffnet der Hacker die Haustür, nicht jemand aus der Familie.

Auch die sogenannte "Künstliche Intelligenz" ist keineswegs nur ein Segen. Klar, sie kann helfen Energie zu sparen, den Verkehr richtig zu lenken oder Krankheiten zu heilen. Sie ist aber auch das Lieblingsinstrument für Herrscher jeder Art, egal ob sie im Silicon Valley sitzen oder auf irgendeinem Regierungsstuhl. Nie war Totalüberwachung so einfach wie heute.

Wir – und das heißt Politik, Gesellschaft, jeder einzelne von uns – wir sollten lernen, Digitalisierung besser zu begreifen, wo sie Probleme löst und wo sie Probleme schafft.

# Die Polizei und die Gesichtserkennung

Bundesinnenminister Seehofer macht offenbar einen Rückzieher: Die Bundespolizei soll nun wohl doch keine automatisierte Gesichtserkennung an sicherheitsrelevanten Orten einsetzen dürfen. Der aktuell vorgelegte Gesetzentwurf sieht das jedenfalls nicht mehr vor.

Offensichtlich in eine gewisse Einsicht eingekehrt, dass es hoch problematisch ist, im großen Stil und KI-gestützt Plätze oder Orte zu überwachen. Denn Gesichtserkennung funktioniert nicht perfekt - und macht gleichzeitig eine nahezu lückenlose Überwachung möglich.


## US-Behörden füttern den Datenschurken - durch Bezahlung

Genau das ist die Sorge, die mit dem aktuellen Clearview-Fall verbunden ist. Ein US-Unternehmen hat gegen alle Nutzungsbedingungen rund drei Milliarden Fotos mit Gesichtern aus dem Netz gezogen und in einer gigantischen Datenbank gespeichert. Der eigentliche Skandal ist aber, was Clearview AI damit macht: Rund 600 Behörden in den USA zahlen dafür, dass sie Fotos ins System einspeisen dürfen - und erfahren, um wen es sich dabei handelt.

Polizei und Behörden verlassen sich auf ein Privatunternehmen, das niemand kennt, das niemand überprüft und das macht was es will. Unfassbar. Wäre das auch in Deutschland denkbar? Ich habe in Düsseldorf Sebastian Fiedler gesprochen (komplettes Interview, siehe Video) und ihn gefragt, ob die deutsche Polizei so etwas nicht auch praktisch fände.

Klare Antwort des Polizisten: "Auf keinen Fall! Es geht nicht darum, was praktisch ist, sondern was rechtsstaatlich in Ordnung geht." Clearview AI hat mit Rechtsstaatlichkeit nichts zu tun.

## Twitter fordert Löschung der Fotos

Es regt sich Widerstand. Twitter zum Beispiel hat Clearview AI aufgefordert, eingesaugte Bilder unverzüglich zu entfernen. Eine Reaktion, die man auch von Facebook erwarten würde - und im Grunde auch von den US-Behörden und der US-Politik. Aber die US-Behörden füttern diesen Drachen ja. Was schon allein für sich ein Skandal ist. Eigentlich der noch viel größere als dass ein Unternehmen versucht, sich dreist einen Vorteil zu verschaffen.

Denken wir die Sache doch weiter: Wenn Clearview AI keine klaren Grenzen gesetzt werden - und hier geht eigentlich nur eins: Stecker ziehen! -, dann kommt doch schon bald die erste Spaß-App auf den Markt. Check your mate: Foto machen - und erfahren, wer das ist. Die ersten drei Versuche gratis. Danach gegen Dollar. Und dann kommt die schicke Augmented-Reality-Brille auf den Markt, die sogar in Echtzeit Gesichter scannt. Technisch alles denkbar.

Aber ein Albtraum.

# Selbst Avast verkauft Daten: Wir brauchen eine Datenschutz-Ampel

**Virenschutz ist wichtig - und ein kostenloser Virenschutz vielen natürlich sehr willkommen. Deshalb ist Avast Antivirus so beliebt. Doch jetzt wurde bekannt: Die Software sammelt Nutzerdaten - und diese wurden über ein Tochterunternehmen an Verwerter verkauft.**

Die meisten Experten - auch wir hier bei Digitalistan - empfehlen gebetsmühlenartig: Windows-Benutzer sollten einen Virenschutz installieren. Zu groß die Gefahr, in die Fänge von Viren, Würmern und Datenräubern zu geraten. Ein guter Virenschutz kann helfen, unerwünschte Schnüffeleien abzuwenden.

Die Firma AVG bietet mit Avast Antivirus einen eigentlich schönen Virenschutz an. Für Privatleute ist er sogar kostenlos. Rund 435 Millionen Menschen weltweit nutzen Avast Antivirus. Wie schön - und freundlich vom Unternehmen.


## Vertrauensbruch: Erst ausspioniert, dann Daten verkauft

Doch jetzt scheint klar: Die Nutzer zahlen doch einen Preis dafür. Die Software sammelt Informationen über das Surfverhalten: Welche Webseiten werden angesteuert, welche

Suchbegriffe eingegeben, auch GPS-Daten von Google Maps, angeschaute YouTube-Videos oder aufgerufene Linkedin-Profile merkt sich die Software. All die Daten sammelt der Hersteller - und verkauft sie in Bausch und Bogen an Verwerter wie Google, Microsoft, Pepsi, Condé Nast, Yelp, McKinsey und einige andere.

Anonymisiert zwar - aber da Avast von jedem Nutzer eine Nutzer-ID hat, lassen sich die im Zweifel auch wieder eindeutig Personen zuordnen. Es steht zu befürchten, dass Werbenetzwerken wie von Google oder Microsoft das auch auf eigene Art und Weise gelingt. Die Anonymisierung wäre also schnell dahin.

Der eigentliche Skandal ist: Die Nutzer wurden weder darüber informiert, noch gefragt. In den Nutzungsbedingungen gibt es nebulöse Formulierungen, die darauf hindeuten, dass der "Clickstream" ausgewertet wird. Aber wer kommt schon darauf, dass damit das Surfverhalten gemeint ist? Von einer Software, die Schutz vor Angriffen jeder Art verspricht, erwartet doch niemand, dass sie selbst ein Trojaner ist - und die Kundschaft ausspioniert.

Selbst wenn die Software kostenlos ist - das ist ein hemmungsloser Missbrauch des Vertrauens.

Jetzt wieder die Schuld und Verantwortung auf die "dummen Nutzer" zu schieben, lasse ich nicht zu. Die Hersteller haben Verantwortung. Und die Politik, ein derart ungeniertes Verhalten nicht durchgehen zu lassen.

*Foto:* Expertiger

## Ampellösung bringt mehr Transparenz für alle

Niemand kann erwarten, dass arglose Nutzer Dutzende Seiten AGBs durchlesen - und verstehen. Niemand kann das. Deshalb brauchen wir eine andere Art, die Nutzer zuverlässig zu informieren.

Mein Vorschlag: Eine Datenschutz-Ampel.

**Grün:** Wir erheben und speichern Daten, die zum Betrieb des Dienstes erforderlich sind. Sie werden nicht geteilt oder verkauft.

**Gelb:** Wir erheben und speichern Daten, die zum Betrieb erforderlich sind - und teilen sie unentgeltlich mit dritten Diensten.

**Rot:** Wir erheben und speichern Daten - und verkaufen diese an dritte Unternehmen.

Dann wüssten wir endlich, woran wir sind. Meine Befürchtung: Die meisten Apps und Onlinedienste wären mit einer roten Ampel versehen.

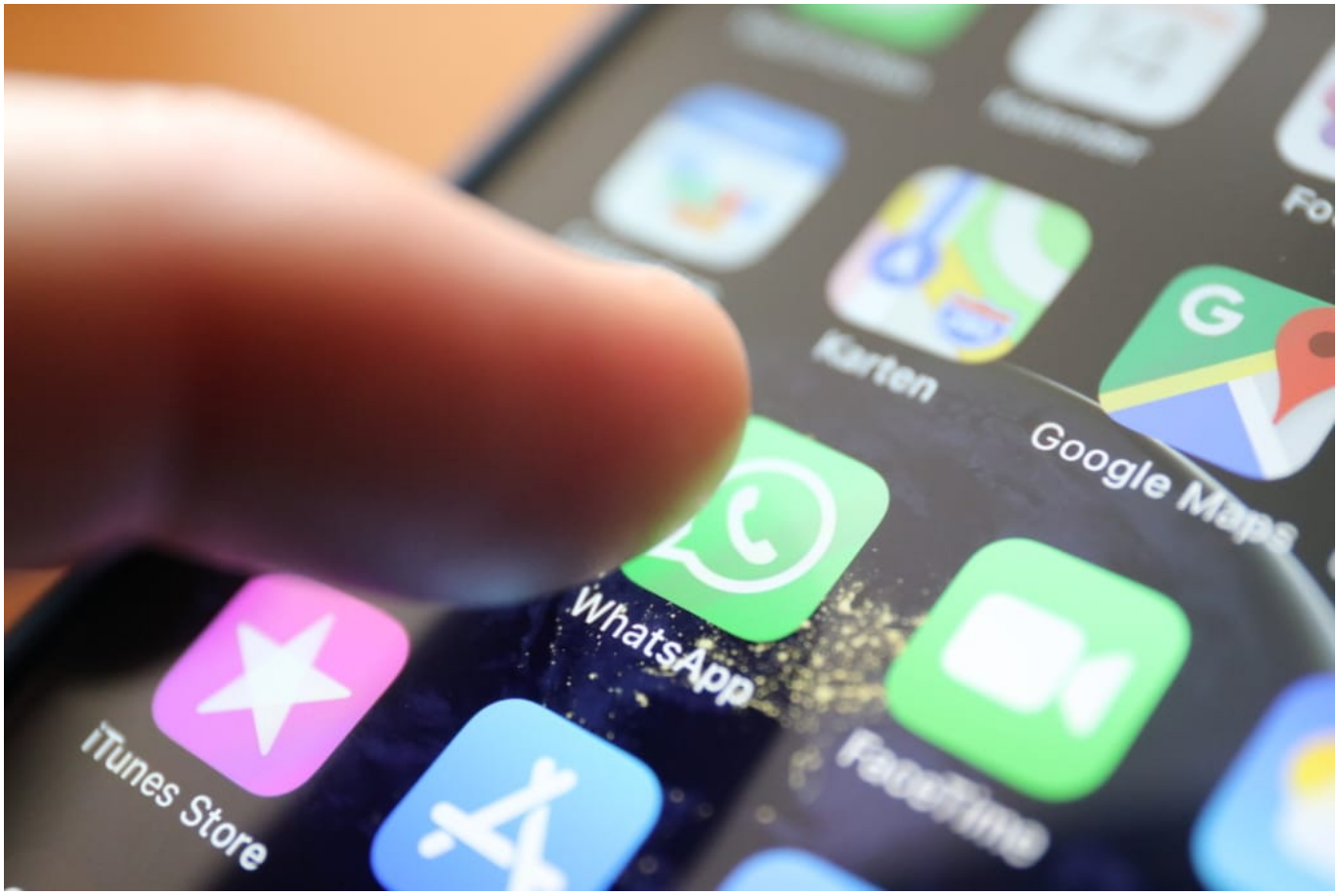
**Update:** Wie mir das Avast um 17:40 Uhr mitteilt, hat das Unternehmen entschieden, Jumpshot zu schließen - also das Tochterunternehmen, das die Daten verkauft hat. Eine Weitergabe der Daten soll künftig nicht mehr erfolgen.

# Kritische Sicherheitslecks in WhatsApp? Die UNO meint: ja

Auch die Großen und Mächtigen der Welt nutzen WhatsApp. Jeff Bezos zum Beispiel. Amazon-Chef und einer der reichsten Männer der Welt. Ihm wurden allem Anschein nach durch Versenden einer WhatsApp-Nachricht mit angehängtem Video im großen Stil Daten aus dem Handy gesaugt. Die UNO hat den Fall untersucht, und ist sich sicher: Ein gezielter Angriff über WhatsApp.

Eine Welt ohne WhatsApp? Für viele denkbar, aber sinnlos. Deshalb hat WhatsApp nun als zweite App, die nicht von Google kommt, in der Android-Welt die Marke von fünf Milliarden Downloads geknackt. Nach der Facebook-App. Zwar unter anderem auch deshalb, weil die App auf vielen Smartphones vorinstalliert ist.

Aber die Message ist überdeutlich: Allein in der Android-Welt ist die App über fünf Milliarden Mal geladen worden. Unter iOS zählt WhatsApp auch zu den populärsten Apps überhaupt.




## WhatsApp: Sechs Mal mehr Sicherheitslecks

Hacker stürzen sich am liebsten auf Anwendungen, die besonders weit verbreitet ist. Das war lange ein Problem für Windows-Nutzer. Aber wie sieht es eigentlich mit WhatsApp aus? Auch der Messenger scheint einige Einfallstore zu haben. Jedenfalls haben die Entwickler selbst in

2019 deutlich mehr Sicherheitslecks an die offizielle Registrierungsstelle "National Vulnerabilities Database" (NVD) gemeldet als in den Jahren zuvor. Die meisten als "kritisch" eingestuft. Also ein bedenkliches Einfallstor.

Dass wir selten oder gar nichts von einer Ausnutzung solcher Lecks hören, bedeutet nicht, dass sie tatsächlich nicht genutzt werden. Ein besonders prominenter Fall, wo möglicherweise ein Sicherheitsleck in Whatsapp ausgenutzt worden sein könnte, ist im Fall Jeff Bezos. Der hat im vergangenen Jahr eine WhatsApp-Nachricht vom saudischen Kronprinzen Mohammed bin Salman erhalten - und ein angehängtes Video angeschaut.

Ab diesem Zeitpunkt sind verdächtig viele Daten von seinem Smartphone aus verschickt worden. Wenig später sind kompromittierende Daten über Bezos aufgetaucht, um ihn unter Druck zu setzen. Ein merkwürdiger Zufall. Zwar ist bislang nicht zweifelsfrei geklärt, ob es wirklich ein Sicherheitsleck in WhatsApp war und ob wirklich der saudische Kronprinz hinter der Sache steckt, aber laut Experten und Fahndern verdichten sich die Hinweise.

## UN-Vertretern ist WhatsApp-Nutzung verboten

Die Sorge, dass WhatsApp ein unzumutbares Sicherheitsrisiko darstellt, nehmen zu: Hochrangige Vertreter der Vereinten Nationen (UN) dürfen kein WhatsApp mehr benutzen. Nicht, weil die Verschlüsselung angezweifelt würde, sondern wegen gravierender Sicherheitsbedenken.

Vielleicht sollten wir aus den Vorfällen lernen - und anderen Messengern den Vorzug geben. Denn Bedenken gibt es ja genug, was WhatsApp anbelangt. Schon allein deswegen, weil der Mutterkonzern Facebook seine Versprechen gebrochen hat, was die Unabhängigkeit von WhatsApp, den Datenfluss zu Facebook und das Thema Werbung in WhatsApp betrifft.

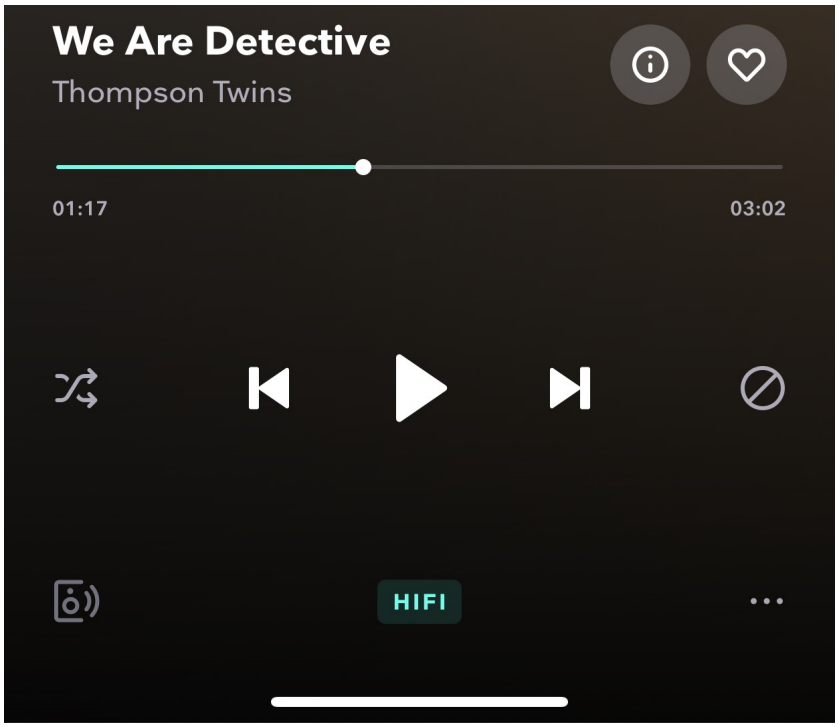
Ihr erreicht mich auf Threema!

https://vimeo.com/339064785

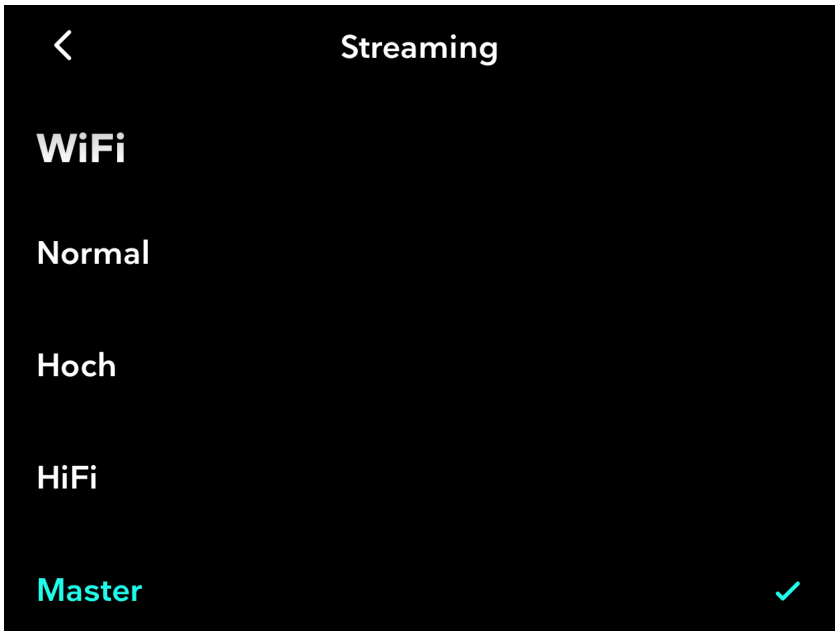
# Optimale Streaming-Qualität bei Tidal einstellen

Streaming-Dienste sind für viele Anwender gleichbedeutend mit komprimierter und damit schlechter Soundqualität. Zumindest der erste Vorwurf stimmt für die einfachen Dienste wie Spotify oder die Standard-Version von Amazon Music. Höherwertige Dienste wie beispielsweise Tidal erlauben unkomprimierten Musikgenuss, ja oft auch Zugriff auf Master-Qualität. Sie müssen nur einstellen, dass Sie Musik in dieser Qualität hören wollen!

Streamingdienste richten sich zu allererst an die Benutzer, die unterwegs Musik hören wollen. Und da ist meist das Datenvolumen ein Thema, darum werden bei der Wiedergabe verschiedene Faktoren zusammengetragen: Die Musik soll so gut wie möglich klingen, aber so wenig wie möglich Datenvolumen verbrauchen. Eigentlich die Quadratur des Kreises, bei Tidal aber als **Normal** bezeichnet. Die aktuelle Wiedergabequalität finden Sie immer am unteren Bildschirmrand im Wiedergabebildschirm.




Tippen Sie mit dem Finger darauf, dann bekommen Sie einen Auswahlbildschirm, der sich in zwei Hälften unterteilt: Unter **Wifi** können Sie die Wiedergabequalität bei einer WLAN-Verbindung festlegen. Unter **Mobil** die bei einer mobilen Datenverbindung. Je weiter Sie in der Liste nach unten gehen, desto besser ist de Qualität und um so höher die Datenmenge.



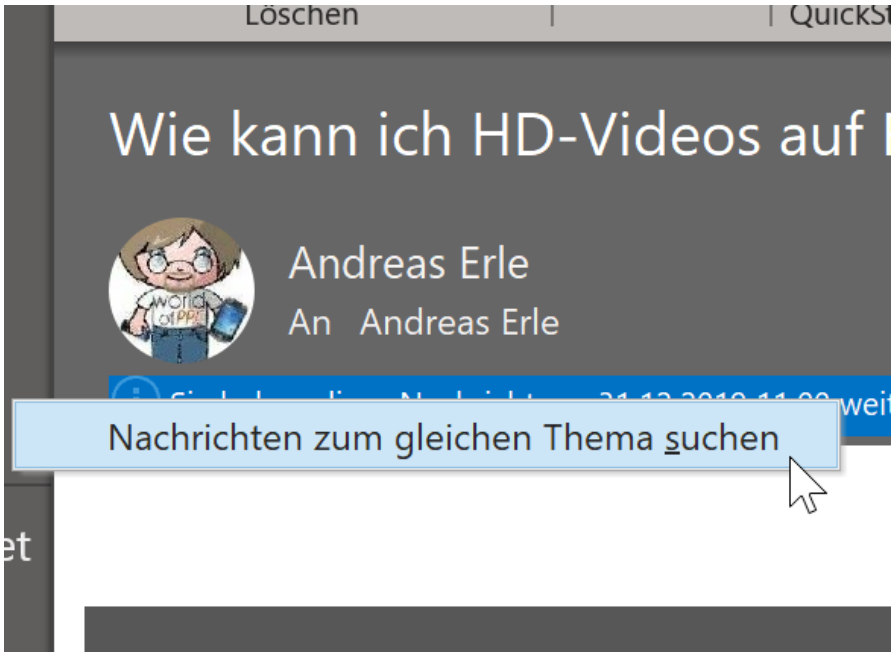

Dabei ist **HiFi** die unkomprimierte CD-Qualität, **Master** die Masterqualität, die dem im Studio erzeugten Klangmaterial erzeugt. Letztere wird nur dann verwendet, wenn die Musik auch in diesem Format angeboten wird. Das ist leider nur bei ca. 10 Prozent der Musikstücke der Fall.

# Die Historie von E-Mails finden

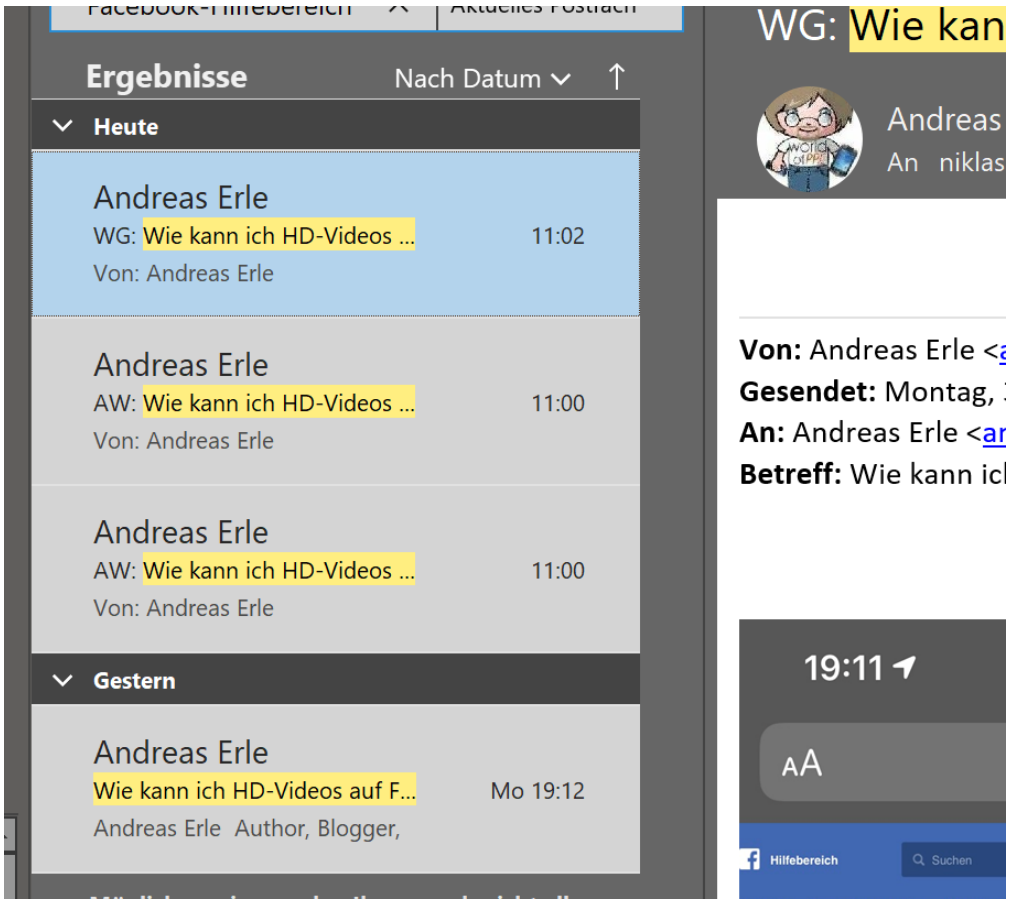
Besonders in der professionellen Anwendung, aber auch bei komplexeren Diskussionen im Privatbereich kann es schnell vorkommen, dass Sie ein und dieselbe E-Mail mehrfach beantworten und weiterleiten. Wenn es dann darum geht, einen Nachrichtenverlauf zu rekonstruieren, dann wird das schnell unübersichtlich. Outlook bietet aber versteckt eine tolle Möglichkeit, alle mit einer bestimmten Nachricht zusammenhängende neue Nachrichten aufzulisten.

Outlook zeigt im Standard an einer Nachricht unter den Betreff- und Adress-Angaben einen Vermerk an, was Sie zuletzt mit der Nachricht gemacht haben. Dort finden Sie beispielsweise "Sie haben diese Nachricht am ... weitergeleitet". Nehmen Sie aber die Quellnachricht und beantworten Sie diese dann noch einmal, dann werden der Text und der Zeitstempel ersetzt. Es wird als immer nur eine Aktion dargestellt.


Um nun alle zugehörigen Nachrichten zu sehen, klicken Sie mit der rechten Maustaste auf den Infotext. Wählen Sie dann **Nachrichten zum gleichen Thema suchen**. Outlook startet nun eine Suche nach allen E-Mails in allen Verzeichnissen Ihres Postfaches, die sich auf die Quell-E-Mail beziehen-




Die gefundenen Ergebnisse werden chronologisch sortiert in einer Liste dargestellt. Wenn Sie die Sortierung ändern wollen, dann klicken Sie auf das Dreieck neben **Nach Datum** und wählen Sie dann das gewünschte Sortierkriterium.



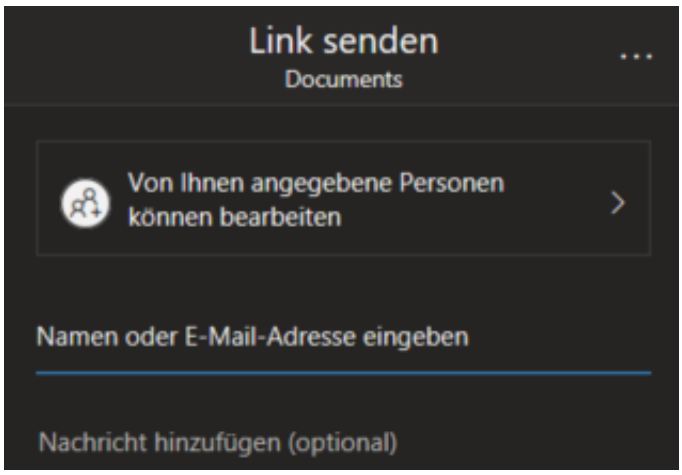

Die gefundenen E-Mails können Sie dann durch einen Doppelklick öffnen und neben dem Inhalt

auch Empfänger und Zeitstempel einsehen.

# Vorsicht beim Teilen von Dateien an mehrere Empfänger

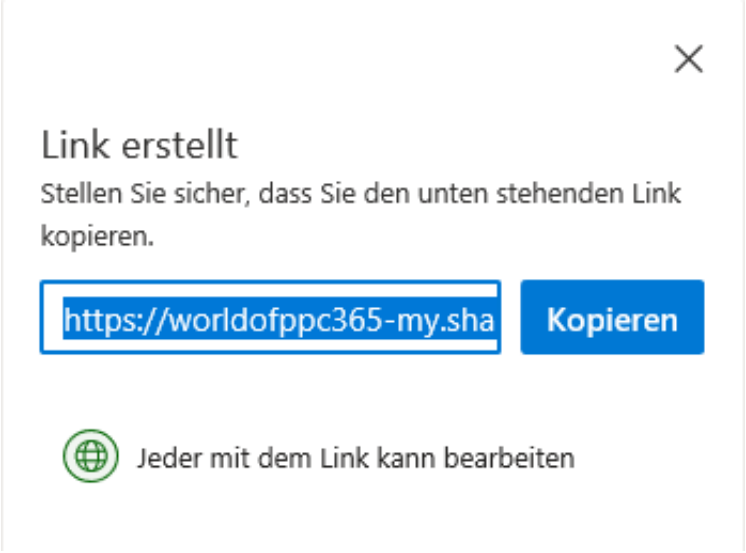
Kollaboration - die Zusammenarbeit mit Anderen in virtuellen Umgebungen - ist ein wichtiger Punkt im modernen Arbeitsleben. SharePoint, OneDrive, Google Docs und DropBox bieten die Möglichkeit, den Zugriff auf Dateien zu gewähren, so dass andere Menschen damit arbeiten können. Beim Teilen der Dateien ist aber Vorsicht geboten!

Während die Freigabe über die reinen Online-Dienste klar geregelt ist, sind OneDrive und SharePoint ein wenig flexibler. Hier können Sie nicht nur Dateien in der Cloud freigeben, sondern auch lokale Dateien. Das ist natürlich relativ, denn hier geht es um Dateien, die mit den OneDrive synchronisiert werden. Nichts desto Trotz funktioniert die Freigabe mit lokalen Mitteln. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, dann auf **Teilen**.




Nun können Sie die E-Mail-Adressen der Empfänger eingeben, die dann die Datei öffnen oder sogar bearbeiten können. Dazu nutzt OneDrive/Windows dann das bei Ihnen als Standard eingerichtete Mailprogramm. Und hier gilt es, genau zu schauen: Die Adressen der Empfänger werden automatisch in die AN-Zeile eingetragen. Damit sieht jeder Empfänger auch jeden anderen. Das ist gegebenenfalls nicht in Ihrem Sinn! Leider können Sie diese automatische E-Mail nicht bearbeiten.

Besser ist es, vor dem Versenden auf **Link kopieren** zu klicken. OneDrive generiert dann den Link, der unsichtbar und damit nicht lesbar alle Angaben zu Empfängern und Berechtigungen enthält. Diese kopieren Sie einfach in eine neue E-Mail und tragen die Empfänger in die BCC-Zeile ein. So bekommt jeder Empfänger den Link, kann aber nur sich selbst als Empfänger sehen.

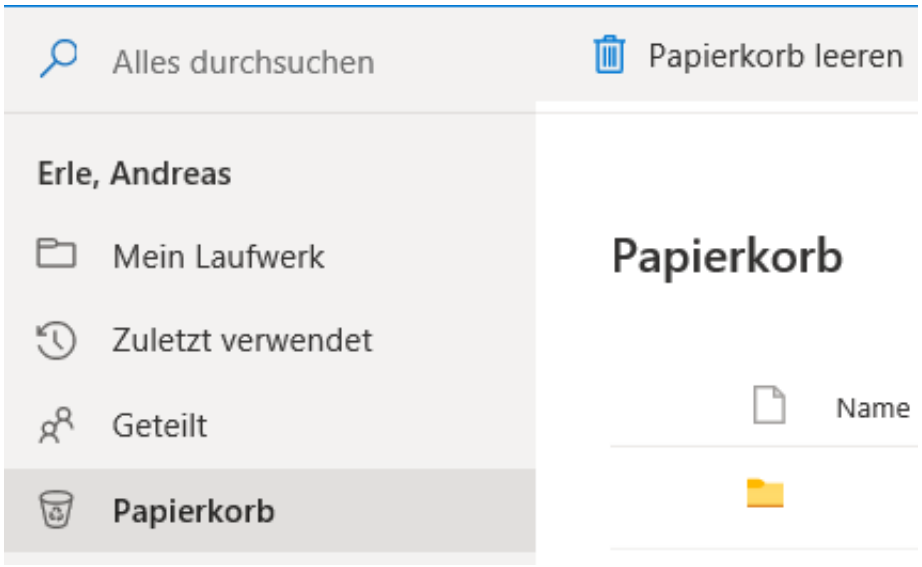

Link erstellt
Stellen Sie sicher, dass Sie den unten stehenden Link kopieren.
https://worldofppc365-my.sha
Kopieren
Jeder mit dem Link kann bearbeiten

# Gelöschte Dateien aus Sharepoint wiederherstellen

Viele Unternehmen gehen von der lokalen Speicherung von Dateien auf Festplatten oder separaten Server-Systemen ab und verwenden eine Cloud-Lösung wie Microsofts SharePoint. So schön die Speicherung in der Cloud ist, so gering Ihre Kontrolle in Krisensituationen. Was, wenn Sie Daten auf dem SharePoint gelöscht haben? Wir zeigen Ihnen, wie Sie schnell wieder an Ihre Daten kommen!

Lokale Speicherung von Dateien scheint reizvoll, hat aber auch seine Nachteile. Zu groß ist der Aufwand, diese aktuell zu halten, sicherheitstechnisch vor Angriffen zu schützen. Auch die Verfügbarkeit der Daten ist ein wichtiges Thema: Backups sind essentiell, liegen bei lokaler Speicherung aber allein in Ihrer Hand (mehr Informationen finden Sie hier). Auf einem SharePoint oder OneDrive trägt Microsoft Sorge dafür.


Wenn sie nun Dateien löschen, dann sind diese erst von Ihrer Festplatte, dann aber auch vom SharePoint/OneDrive verschwunden. Das ein oder andere Mal kann es vorkommen, dass Sie die Löschung versehentlich vorgenommen haben und die Dateien dringend zurück brauchen. Bei einer größeren Zahl gelöschter Dateien meldet sich SharePoint automatisch per E-Mail und weist Sie darauf hin. Klicken Sie dann auf den Link in der E-Mail, um zu den gelöschten Dateien zu kommen.




Alternativ klicken Sie in Ihrem SharePoint/OneDrive auf den **Papierkorb**. Wie beim PC sehen Sie die gerade gelöschten Dateien. Die Besonderheit hier: Dateien werden innerhalb von knapp 90 nach dem Löschen Tagen automatisch endgültig gelöscht! Klicken Sie Dateien und Verzeichnisse links von Ihrem Namen an, um sie zu markieren. Dann können Sie sie durch einen Klick auf **Wiederherstellen** aus dem Papierkorb an ihren ursprünglichen Speicherort verschieben.