

A portrait of a man with short brown hair and a slight smile, wearing a teal button-down shirt. He is positioned on the left side of the frame, with his arms crossed. The background is dark and out of focus.

# Schieb Report

**Ausgabe 2020.08**

## Bestellen von Ersatz-Ear Tips für die Apple AirPods Pro

Apple scheint mit den [Airpods Pro](#) einen Überraschungserfolg gelandet zu haben: Auch Monate nach Marktstart haben diese immer noch Lieferzeiten. So schön und leicht die InEars auch sind, eine Sache macht vielen Anwendern Sorgen: Die Silikon-Passstücke ("Ear Tips") liegen nur jeweils einmal in den Größen S, M und L bei. Einzeln bekommt man sie erst einmal nicht. Was aber, wenn Sie einen verlieren?

Im Apple Store selber bekommen Sie nur die Aussage, dass diese "bald" bestellbar sein sollen. Da der Klang der AirPods Pro aber stark vom vernünftigen Abschluss der Ohr-Passstücke mit dem Hörkanal abhängig ist, haben Sie keinen Spielraum, einen davon zu verlieren. Apple ist hier recht entspannt: Statt die Tips im Store anzubieten, können Sie diese über die Support-Seite für die AirPods bestellen. Klicken Sie dort auf **AirPod oder Ohreinsatz ersetzen**.

Sie müssen sich dann mit Ihrer Apple-ID anmelden und die Seriennummer der AirPods Pro eingeben. Die finden Sie auf dem Karton, in dem die AirPods geliefert wurden.

Produkt und Problem

Versand

Zahlung

Überprüfen und senden

### Benötigen Sie Hilfe?

Wählen Sie die Problembeschreibung aus, die am besten zutrifft.

Ohreinsätze der AirPods Pro austauschen

Wir ersetzen Ihnen gerne das Zubehör. Möglicherweise werden Sie gebeten, das Originalzubehör zurückzugeben, sofern vorhanden.

### Zusammenfassung



AirPods Pro with Wireless Charging Case [Ändern](#)  
Seriennummer: .....KT  
Deutschland [Ändern](#)  
Ohreinsätze der AirPods Pro austauschen

Wählen Sie Ihr Zubehör aus



Kabel, Lightning-auf-USB, 1 m



AirPods Pro, Right, Replacement, ROW



AirPods Pro, Ear Tip, Small

Klicken Sie dann auf **Ohreinsätze der AirPods Pro austauschen**. Wählen Sie die gewünschte Größe aus und schließen Sie die "Reparaturanforderung" ab. Nach kurzer Zeit erhalten Sie die

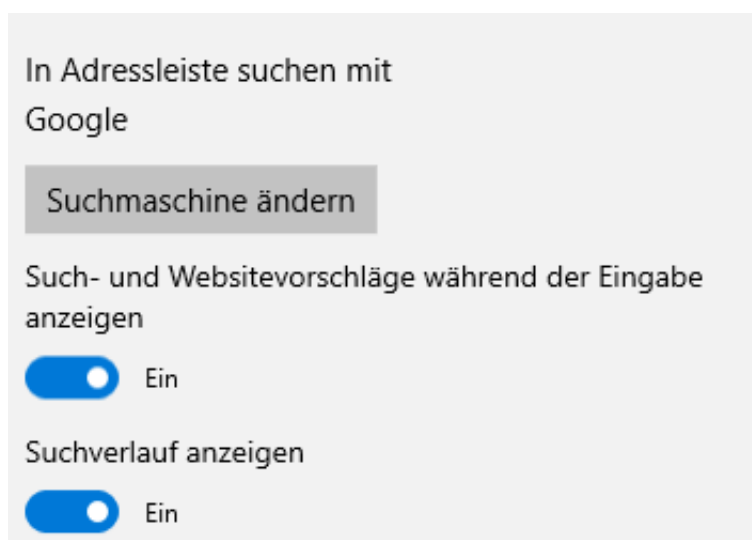
Bestätigungs-E-Mail, nach einigen Tagen dann die Passstücke. Apple fordert die alten übrigens nicht zurück, auch wenn dies in der Bestellung als Möglichkeit angegeben wird!

## Ändern der Standard-Suchmaschine bei Edge Chromium

Microsoft hat mit der [neuen Edge-Version](#) einen weiteren Schritt zu einem modernen und leistungsfähigen Browser gemacht. Durch die Einbindung von Chromium soll der Standard-Browser von Windows 10 standard-kompatibler sein als der "alte" Edge-Browser. Schritt für Schritt wird der alte ausgetauscht. Wie aber können Sie diesen so anpassen, wie Sie es bisher gewohnt sind?

Wie immer verordnet Microsoft seinen Benutzern Bing als Standard-Suchmaschine. Diese wird verwendet, wenn Sie in der Adresszeile keine URL, sondern einen beliebigen Suchbegriff eingeben. Dieser wird dann an die Standard-Suchmaschine übergeben und die Suchergebnisse zurückgegeben. Bing ist nun nicht Jedermanns Geschmack, und so macht der Wechsel beispielsweise zu Google Sinn.

Um die Einstellung zu ändern, müssen Sie in Edge auf die drei Punkte oben rechts im Programmfenster (**Einstellungen und mehr**) klicken. Wählen Sie dann **Datenschutz und Dienste**.



Hier bekommen Sie nun unter anderem die Standard-Suchmaschine angezeigt, in der über die Adressleiste gesucht wird. Klicken Sie dort auf **Suchmaschine ändern**. Sie können nur aus den angebotenen Suchmaschinenanbietern denjenige aussuchen, den Sie als Standard definieren wollen. Wenn Sie bei der Suche ohne weitere Vorschläge arbeiten wollen, dann deaktivieren Sie **Such- und Websitevorschläge während der Eingabe anzeigen** und **Suchverlauf anzeigen**.

## So lässt sich Website Traffic erhöhen

Es gibt viele Gründe, eine Webseite an den Start zu bringen. Die einen wollen einen Blog präsentieren und die Welt mit Infos versorgen. Die anderen wollen ganz konkret etwas verkaufen oder an ihrem Image arbeiten. Wieder andere wollen mit ihren Inhalten indirekt Geld verdienen - über Werbung oder Provisionen. Allen ist eins gemein Sie wollen möglichst viele Besucher auf ihrem Angebot.

Eine Website macht es möglich, die Welt mit Informationen zu versorgen. Aber all die Arbeit soll sich auch lohnen. Daher stellen sich viele die Frage Wie lässt sich der Traffic auf der Website erhöhen?

Einfach ist das nicht. Es gibt viele Methoden, um kurzfristig oder langfristig mehr Besucher auf die Homepage zu holen. Betreiber von Webangeboten können Tipps und Tricks anwenden, um das Ziel zu erreichen. Das funktioniert für private Webseiten und Firmen-Homepages gleichermaßen. Wer gerne etwas verkaufen möchte, ist auf maximale Aufmerksamkeit angewiesen.



## Die Grundlage einer erfolgreichen Website

Eisernes Gesetz: Der Erfolg einer Website hängt vom Traffic ab (also von der Anzahl der

Besucher). Die Seite kann aufwendig und teuer gestaltet worden sein, aber dies ist nicht ausschlaggebend. Der [Seiteninhalt](#) bildet die Grundlage. Ganz gleich, um welche Art von Webseite es sich handelt.

Daher lautet die Empfehlung der meisten Experten: Unbedingt viel Zeit in den Inhalt investieren, damit sowohl die Seite als auch die Marke dahinter profitiert. Daraus entstehen folgende Vorteile:

- Es wird Kompetenz und Wissen ausgestrahlt.
- Besucher speichern die Seite als Favorit (wiederkehrende Besucher).
- Langfristig ist eine Kundenbindung möglich.
- Markenbekanntheit wird — erheblich — gesteigert.
- Blog dient als Sprungbrett für Kaufabschlüsse.
- Bessere Rankings in der Suchmaschine.

All das wird zusammengefasst unter dem Sammelbegriff **Content-Marketing**. Sicherlich ist die Erstellung von einwandfreien und qualitativen Inhalt zeitaufwendig. Aber davon wird die Marke langfristig profitieren.



**Schnellste Möglichkeit: Suchmaschinenwerbung (SEA)**

Wenn sofort Geld verdient werden muss, dann ist die Schaltung von Werbung in der Suchmaschine perfekt. Das **Search Engine Advertising** wird als **SEA** abgekürzt und ist nicht gleichzustellen mit dem SEO, das wir im nächsten Punkt behandeln. Das Ziel von SEA ist, möglichst sofort Umsätze zu generieren.

Werbung in Suchmaschinen lohnt sich durchaus! Die eigene Webseite erscheint damit vor den organischen Suchergebnissen. Doch worin liegen die Vorteile?

- 65 Prozent der Klicks in der Suchmaschine erhalten Werbeanzeigen.
- 41 Prozent aller Klicks erhalten die Top 3 der bezahlten Werbeanzeigen.
- Sofortige Steigerung der Markenbekanntheit.
- Generierung von Besuchern über den Werbezeitraum hinweg.

Ein Laie hat es aber nicht so leicht, denn für optimales Marketing in den Suchmaschinen sind die Fähigkeiten von erfahrenen Profis gefragt. Onlineshops, die im gesamten Bundesgebiet Produkte verkaufen wollen, sollten daher prinzipiell eine [Google AdWords Agentur](#) hinzuziehen. Durch die Zusammenarbeit mit den Profis lässt sich mehr Erfolg erzielen und ein Umsatzanstieg erreichen.

## Langfristige Methode: Suchmaschinenoptimierung (SEO)

Die Suchmaschinenoptimierung (SEO) ist eine andere, eher langfristige Methode, für mehr Besucher auf dem eigenen Webangebot zu sorgen. Fertig ist die Suchmaschinenoptimierung allerdings nie. Es gibt immer wieder etwas, um das Ranking zu verbessern oder den bereits erarbeiteten Vorsprung auszubauen.

Wichtig zu wissen: Guter Content und ideale Ladegeschwindigkeit alleine sind noch [kein Garant für ein Ranking auf Platz Eins](#) in den Suchergebnissen.

Folgende Vorteile ergeben sich aus der Suchmaschinenoptimierung:

- Hohe Platzierung in den Suchergebnissen (ggf. über der Konkurrenz).
- Es entstehen keine Kosten im Vergleich zur Schaltung von Werbung.
- Stets neue Kundengewinnung, obwohl nicht mehr aktiv am SEO gearbeitet wird.

Im SEO gilt es daher immer langfristig zu denken, um die Ziele zu erreichen. Entsprechend viel Zeit muss aber auch investiert werden, denn sonst wird es nicht effektiv. Aber eines bleibt festzuhalten: SEO wird sich lohnen und auszahlen!

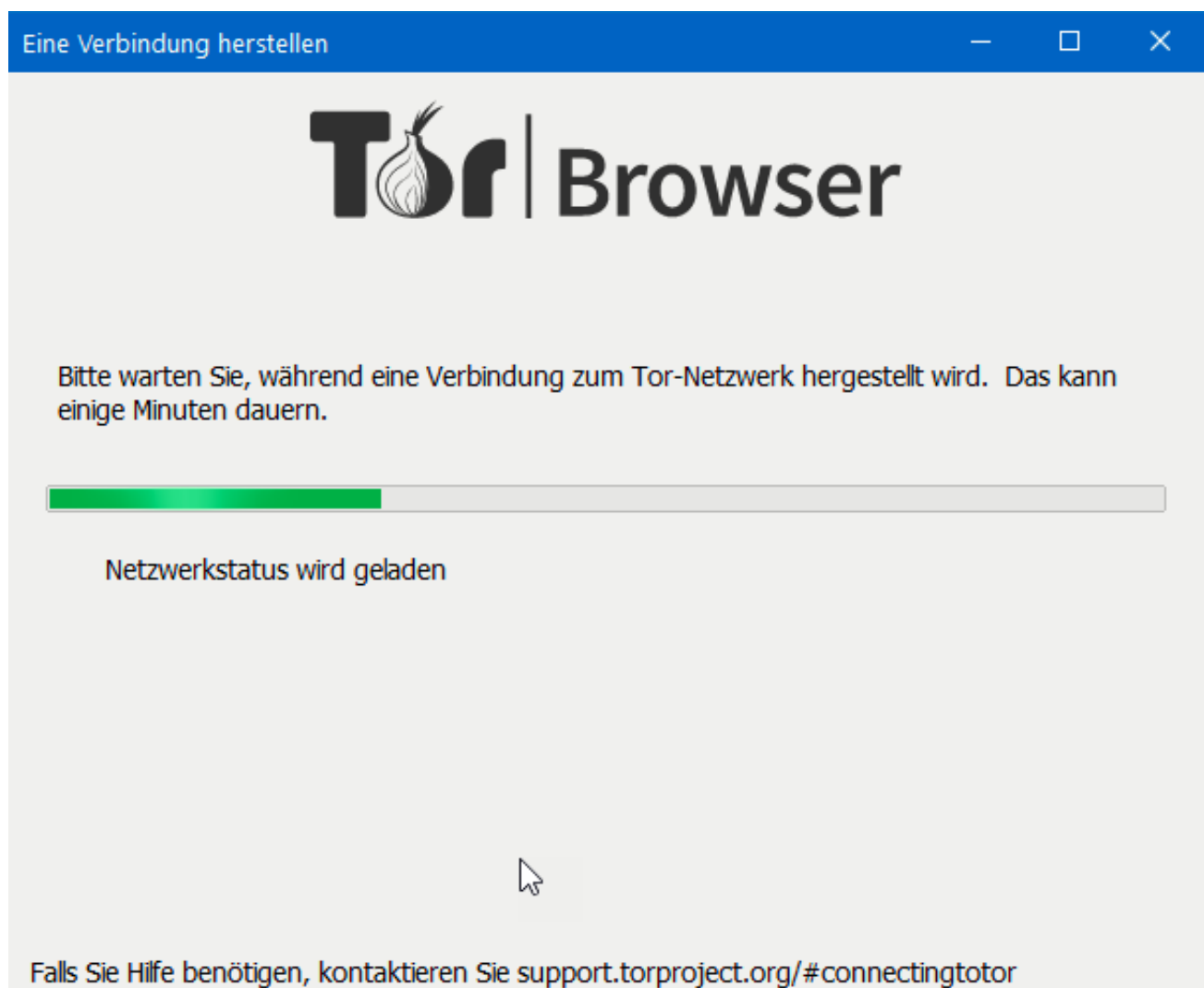
## Fazit

Der Seiteninhalt verbleibt stets als Grundlage, denn auch bei bezahlten Werbeanzeigen ist der Inhalt selbstverständlich wichtig. Ein Interessent würde bei mangelhafter Information sofort die Website verlassen und die Konkurrenz besuchen.

## Anonym Surfen: Der Tor-Browser

Im Internet finden Sie nahezu alle Informationen, die Sie benötigen. Manchmal auch mehr, als Sie tatsächlich wissen wollen. Sicher ist aber: Eine Suche im Internet hinterlässt Spuren. Und bei bestimmten Themen ist es Ihnen vielleicht nicht so Recht, wenn man nachvollziehen kann, dass Sie eine Webseite besucht haben. Eine schnelle Lösung ist hier der kostenlose [Tor-Browser](#).

Die Idee dahinter ist einfach: Das Internet kann Suchen und Webseitenbesuche ja nur deshalb zu Ihnen zurückverfolgen, weil es über die IP-Adresse potentiell Zugriff zu Ihrem Anschluss hat. Der Tor-Browser löst das elegant: Er verwendet das [Zwiebelschalenprinzip](#). Im Englischen heißt das Onion Routing, daher kommt auch der Name des Browsers: **The Onion Router**.



Die Idee: Im Internet laufen sie Daten immer über verschiedene Knotenpunkte, damit ist Ihre Adresse auch all diesen Knoten bekannt. Beim Tor-Browser werden Ihre Daten an jedem Knoten neu ver- bzw. entschlüsselt. Damit sieht am Ende nur der letzte Knoten Ihre Daten im Klartext und kann überhaupt etwas damit anfangen.



The screenshot shows a web browser window with the address bar displaying <https://www.wieistmeineip.de>. The website has a blue navigation bar with links for 'Startseite', 'Speedtest', 'Anbieter', 'Tarifrechner', 'Tipps & Tools', and 'Login'. The main content area displays the website's logo and the following information:

- Ihre IP-Adresse lautet: **2001:67C:2608::1**
- Ihre IPv4-Adresse lautet: nicht vorhanden
- Ihre System-Informationen: Windows 10, Firefox 68.0, Frankreich, Anonym sur

Below this information are two large buttons: 'SPEEDTEST STARTEN' and 'PING-TEST STARTEN'. The 'SPEEDTEST STARTEN' button features a speedometer icon, and the 'PING-TEST STARTEN' button features a clock icon. To the right, a partially visible button labeled 'ANBI...' is also present.

Two featured articles are visible:

- Der verbesserte DSL-Speedtest**: Das neue Testverfahren im DSL-Geschwindigkeitstest analysiert Ihre Internet-Verbindung noch genauer. [Zum kostenlosen Speedtest](#)
- Test: Die besten VPN-Anbieter**: VPN gewährt Anonymität und Sicherheit im Internet. Hier erfahren Sie, welche VPN-Dienste am besten sind.

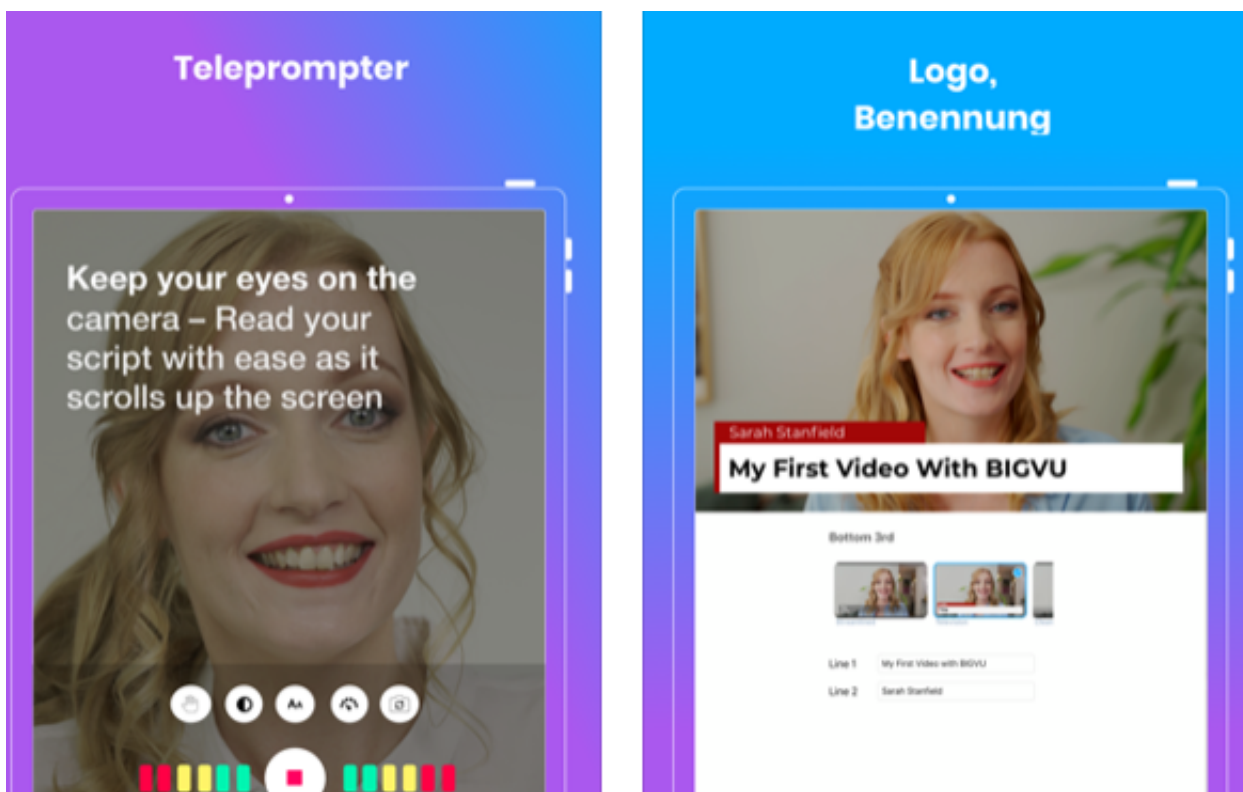
A dark cookie consent banner is at the bottom, stating: 'Diese Webseite verwendet u.a. Cookies zur Analyse und Verbesserung der Webseite, zum Ausspielen personalisierter Anzeigen und zum Teilen von Artikeln in sozialen Netzwerken. Unter [Datenschutz](#) erhalten Sie weitere Informationen und Möglichkeiten, diese Cookies auszuschalten.' An 'OK' button is located on the right side of the banner.

Dazu kommt, dass die Daten durch die immer wieder durchgeführte Verschlüsselung immer anders aussehen, ein Tracking also nicht möglich ist. Und da jeder Knoten nur seinen Nachbarn kennt, kann die Seite, von der Sie Daten herunterladen bzw. an die Sie Daten senden auch nicht identifizieren, dass Sie es sind. Anonymer können Sie kaum Surfen!

## Teleprompter selbst gebaut: BIGVU

Sie müssen kein Fernsehstar sein, um ein Video von sich selbst zu drehen. Influencer, Reviewer, ja selbst Familienmitglieder und Freunde im Ausland, die Sie mit einem Video beglücken wollen, erfordern die Möglichkeit, schnell ein Video von sich selbst zu drehen. Das ist mit den Selfie-Kameras der Smartphones und Tablets kein Problem. Was aber, wenn Sie eine Menge an Text sprechen wollen und keine Zettel platzieren können? Auf dafür gibt es eine App!

Die klassische Lösung im Fernsbereich ist der Teleprompter: Ein Bildschirm, der den zu sprechenden Text mit einer Markierung, was Sie gerade sprechen müssen, anzeigt. Und genau das kann Ihr Tablet oder Smartphone auch. Die App dafür ist BIGVU, von der es eine kostenlose Testversion für iPhone und iPad [im AppStore](#) gibt. Die Idee: Sie legen den Text fest, und die App zeigt ihn über Ihrem Bild an, während gefilmt wird. Damit können Sie direkt in die Kamera schauen (und für den Empfänger den Eindruck erwecken, dass Sie ihn direkt anschauen).



Trotzdem haben Sie keine Texthänger, weil Sie den Text buchstäblich direkt vor Augen haben.

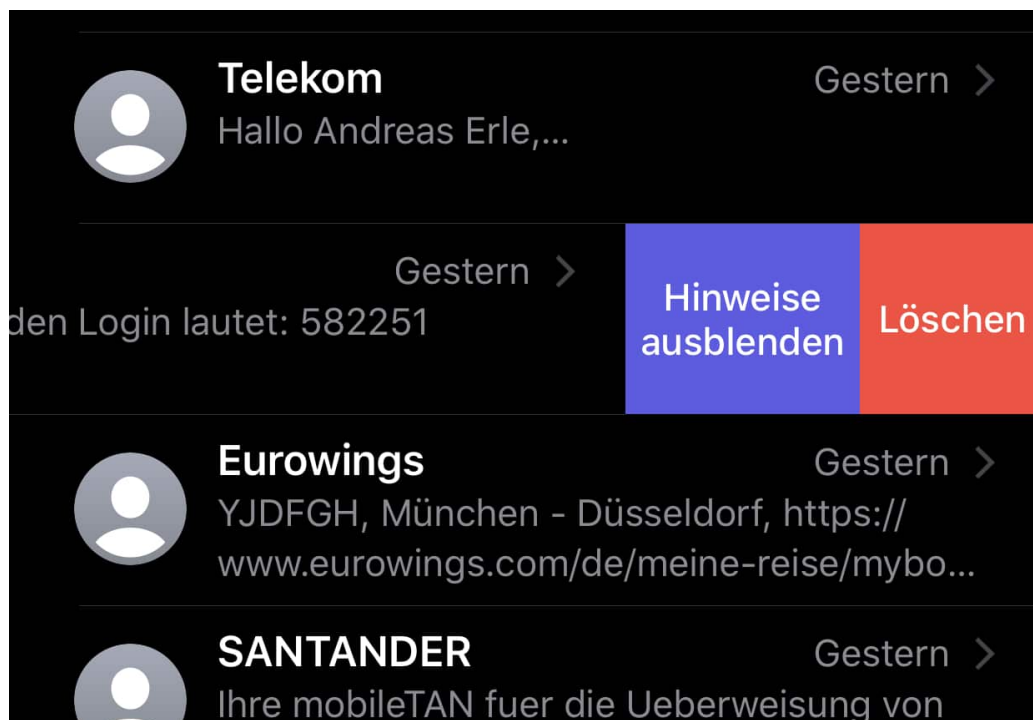
Die App bietet noch weitere Funktionen: Sie können das Video direkt in der App beschneiden und in der Form und Auflösung für Ihren Zweck optimal festlegen. Bei produktiver Nutzung schlägt die App mit einer monatlichen Gebühr ab EUR 10,99 zu Buche.

## iMessage-/SMS-Nachrichten ausblenden

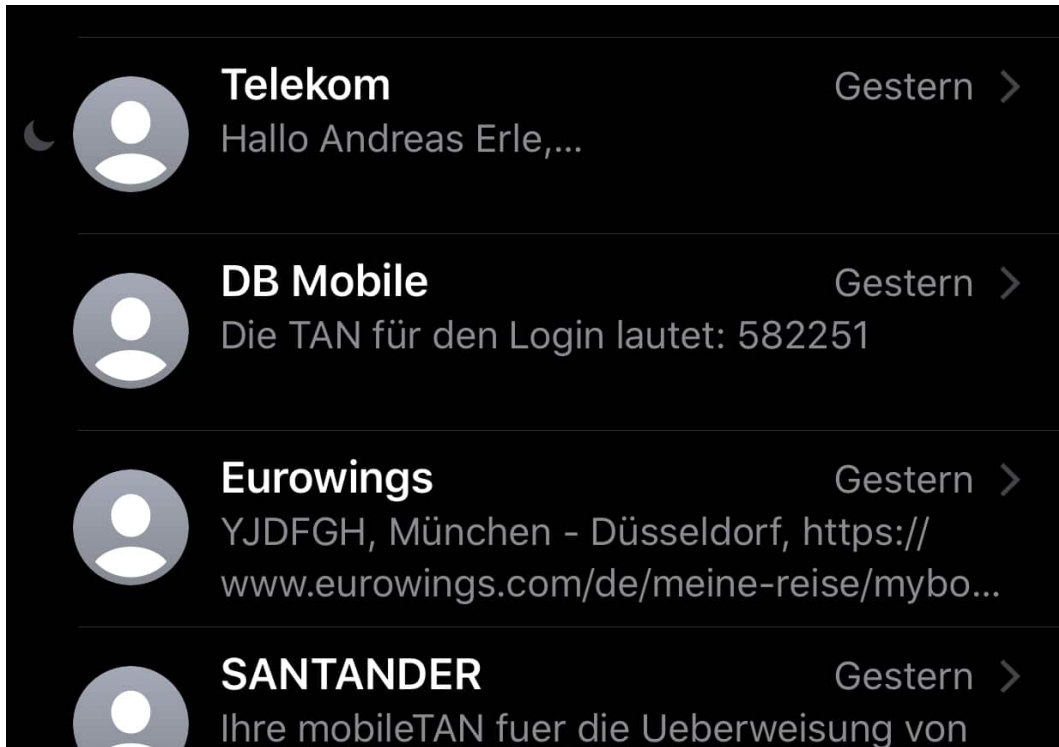
SPAM ist überall. Wenn Sie Ihre Handynummer einmal in den Fängen eines Werbepools verloren haben, dann kann es anstrengend werden: Immer und immer wieder kommen Nachrichten in Ihren Posteingang und werden brav durch ein PopUp benachrichtigt. Auch wichtige Nachrichten, die Sie aber nicht direkt bemerken müssen, können hier ein Thema sein. Die allgemeine Benachrichtigung für Nachrichten auszuschalten, hilft oft nicht. Dann bekommen Sie eben auch bei wichtigen Nachrichten keine Information mehr. iOS bietet hier aber leicht versteckt eine effektive Lösung!

Handelt es sich "nur" um Werbeanrufer handelt, dann können Sie diese schnell komplett blockieren und damit gar nicht mehr mitbekommen. Das haben wir Ihnen [hier](#) schon einmal zusammengeschrieben.

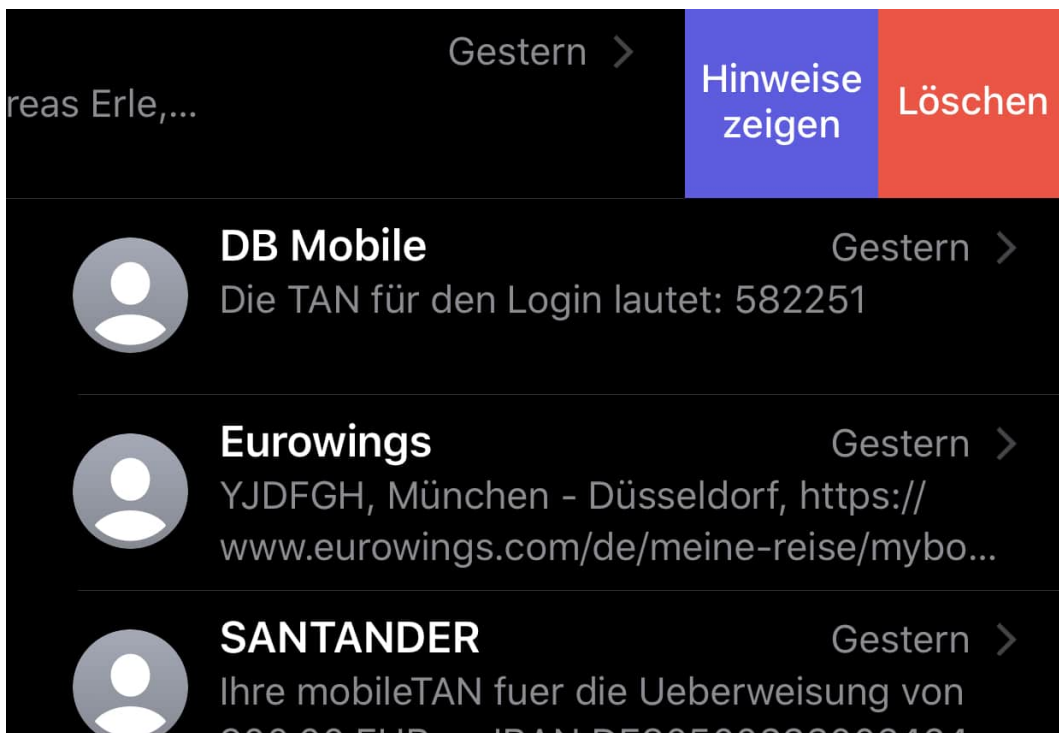
Die Benachrichtigung für einzelne Nachrichten zu unterdrücken ist direkt im Posteingang auf dem iOS-Gerät möglich. Suchen Sie die Nachricht, von deren Absender Sie nicht mehr benachrichtigen werden wollen, heraus. Dann wischen Sie die entsprechende Nachricht mit dem Finger nach links weg.



Klicken Sie dann auf **Hinweise ausblenden**. Die Nachrichten werden ganz normal zugestellt, aber Sie bekommen keinerlei Benachrichtigung mehr. Solche Nachrichten werden im Posteingang dann mit einem kleinen Mond links dargestellt. Dieser soll das "Schlafen" der Benachrichtigungen symbolisieren.



Auf dem selben Weg können Sie dann die Benachrichtigung wieder einschalten: Wischen Sie wieder nach links und tippen Sie dann auf **Hinweise anzeigen**. Sollten bestimmte Nachrichten bei Ihnen nicht aufpoppen, dann Überprüfen Sie, ob Sie versehentlich die Benachrichtigung ausgeschaltet haben!

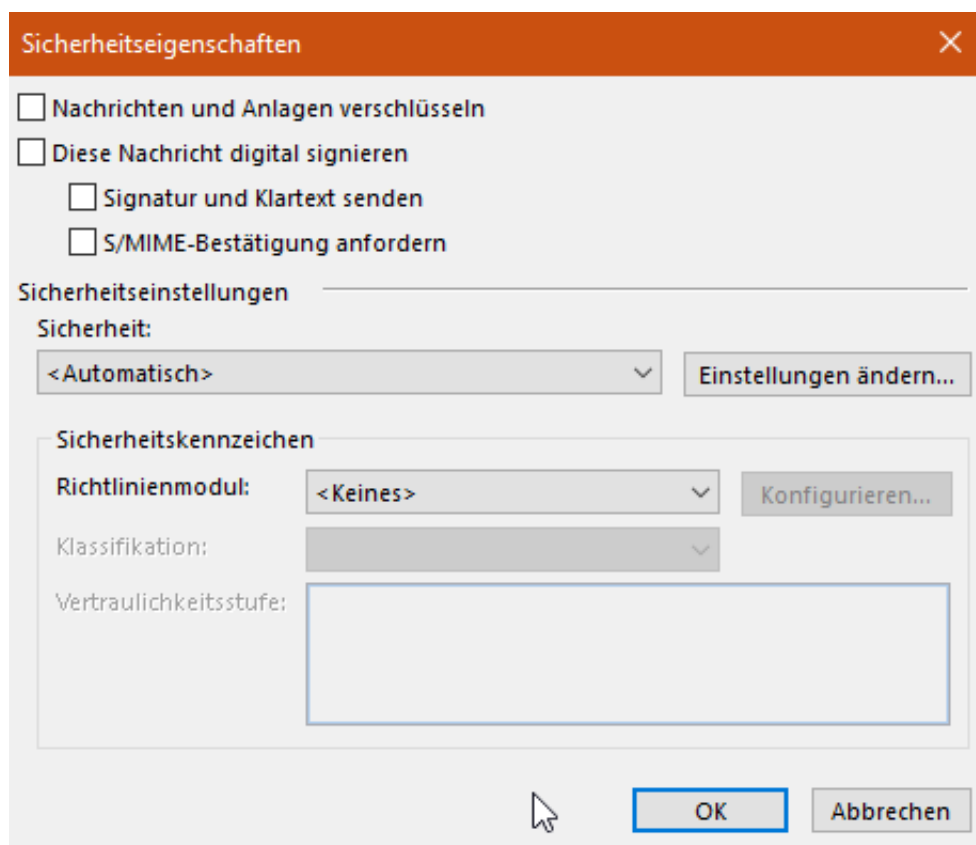


## Wichtigkeit, Vertraulichkeit und Verschlüsselung von E-Mails in Outlook

Eine E-Mail besteht nicht nur aus den Verwaltungsinformationen. Natürlich sind Empfänger, Betreff und der Mailkörper wichtig, weil sie die Informationen transportieren. Zusätzlich können Sie aber noch einige Einstellungen vornehmen, die nahezu unsichtbar mit versendet werden und dem Empfänger weitere Informationen liefern. Wir zeigen Ihnen, wo Sie in Outlook die entsprechenden Einstellungen finden!

Zum Inhalt der Mail gibt es noch drei große Bereiche, die Sie beeinflussen können. Nicht jede E-Mail ist gleich wichtig, und so können Sie eine zusätzliche Kennzeichnung mitgeben, die dem Empfänger Aufschluss darüber gibt. Unter **Markierungen** in der Symbolleiste einer neuen E-Mail können Sie unter **Wichtigkeit** zwischen **Normal**, **Niedrig** und **Hoch** auswählen. Normal ist die Standardeinstellung. Wenn Sie dem Empfänger sagen wollen, dass die Bearbeitung nicht eilig ist, ist niedrig die richtige Wahl. Auf der anderen Seite hoch, wenn es pressiert!

Parallel dazu können Sie unter **Vertraulich** festlegen, dass die E-Mail vertraulich behandelt werden soll. Damit untersagen Sie beispielsweise eine Weiterleitung an Andere.



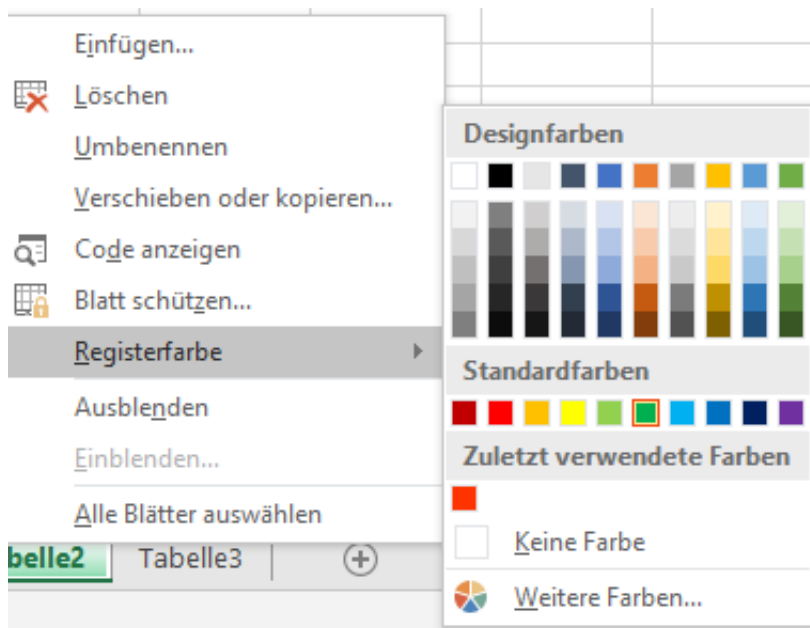
Die dritte Möglichkeit ist die Verschlüsselung von E-Mails. Im Standard versendet Outlook E-Mails im Klartext. Das klingt schlimmer, als es ist, denn der Transfer zwischen den E-Mail-Servern ist im Normalfall schon verschlüsselt. Unter **Sicherheitseinstellungen** können Sie die E-Mail an sich aber noch einmal verschlüsseln. Dazu muss aber ein Zertifikat installiert sein. Das macht am besten der Administrator, der das E-Mail-System aufgesetzt hat.

## Registerkarten in Excel sinnvoll nutzen

Excel ist der Quasi-Standard für Tabellenkalkulationen. Wie so oft bei den Office-Programmen hat Microsoft auch hier Wert darauf gelegt, dass die eigentliche Funktion der Programms schnell und effizient nutzbar ist. Allerdings lässt der Benutzerkomfort an manchen Stellen zu wünschen übrig. So beispielsweise bei der Kennzeichnung von Registerkarten. Wir zeigen Ihnen, wie Sie den Überblick behalten!

Je mehr unterschiedliche Daten eine Tabelle enthält, desto mehr Tabellenblätter haben Sie in der Arbeitsmappe. Nun sind die einen wichtig, die anderen bieten nur Unterstützungsdaten. Am Ende sehen sie in der Registerkarten-Ansicht aber gleich wichtig aus. Ändern Sie das einfach!

Zum einen können Sie die Registerkarten statt mit den Standardnamen "Tabelle1", "Tabelle2" etc. mit sprechenden Namen versehen. Klicken Sie mit der rechten Maustaste in die Registerkarte, dann auf **Umbenennen**. Geben Sie einen sprechenden Namen ein, dann drücken Sie die Eingabetaste, um den Vorgang abzuschließen.



Noch effektiver ist es aber, wenn Sie die Registerkarten dazu auch noch einfärben. Klicken Sie dazu mit der rechten Maustaste auf die Registerkarten, dann auf **Registerfarbe**. Hier können Sie entweder aus den vorhandenen **Designfarben** auswählen oder über **Weitere Farben** ganz feine Farben aus einer Palette auswählen.

31				
32				
33				
34				
35				
36				
37				
38				

Bereit

Wichtig: Die aktuelle Registerkarte ist immer nur leicht eingefärbt, egal, welche Einstellungen Sie vornehmen!



## Verschärftes NetzDG: Reichlich berechtigte Kritik

Seit Anfang 2018 gibt es in Deutschland das "Netzwerkdurchsetzungsgesetz", kurz NetzDG. Es soll helfen, Hass und Hetze im Netz einzudämmen. Allzu gut ist das nicht gelungen. Die Verrohung nimmt zu. Auch und besonders im Netz. Hass, Hetze, Bedrohungen und Beleidigungen nehmen zu.

Jetzt will die Regierung mit einer Verschärfung des NetzDG dagegen vorstellen. Der Entwurf wurde jetzt vom Kabinett auf den Weg gebracht. Doch es regt sich eine Menge Widerstand, unter anderem deswegen, weil das Gesetz vorsieht, dass sogar Passwörter von Usern herausgegeben werden sollen.

Bislang sieht das [NetzDG](#) vor, dass große Plattformen wie Facebook oder Twitter Hasskommentare schneller entfernen müssen, wenn sie Kenntnis davon erlangen.

Nun ist ein regelrechtes Paket an Verschärfungen geplant. In sozialen Medien geäußerte Drohungen, Beleidigungen oder Verleumdungen sollen künftig unter das Strafgesetz fallen und können mehrjährige Haftstrafen nach sich ziehen.

Es ist zum Beispiel ausdrücklich verboten, im Netz Gewalt anzudrohen – auch sexuelle Gewalt. Es sind konkrete Haftstrafen möglich. Das ist eine deutliche Verschärfung der aktuellen Situation – und in meinen Augen auch sehr sinnvoll und nötig.

Wer in Netzwerken unterwegs ist, weiß, wie allgegenwärtig Drohungen, Beleidigungen und Verleumdungen sind. Aber auch gegen Hass und Hetze soll strenger vorgegangen werden. In ganz bestimmten Fällen müssen die Plattformen beanstandete Inhalte nicht nur löschen – wie jetzt schon -, sondern auch melden. An das BKA.



## **Netzwerke sollen von sich aus melden**

Facebook, Youtube, Twitter und Co. sollen also von sich aus melden, wenn sie wahrscheinlich rechtswidrige Inhalte entdecken. Das finden viele falsch.

Das Problem ist, dass der Gesetzentwurf eine umfangreiche Meldung vorsieht. Es soll nicht nur der eigentliche Inhalt gemeldet werden, sondern auch die IP-Adresse und der Port des Urhebers. Alles wird zum BKA übertragen. Problematisch ist, dass das BKA wohl eine Datenbank pflegen soll, in der Opfer und mögliche Täter gespeichert werden.

Die Befürchtung: Es würde ein Register von potenziellen Opfern entstehen, etwa Juden, Homosexuelle, Aktivisten. Auch die potenziellen Täter landen in einer Datenbank. Hunderttausende pro Jahr, ist die Schätzung.

Denn so viele Postings werden gelöscht und müssten künftig gemeldet werden. Eine solche Verdachtsdatenbank wäre natürlich in der Tat bedenklich. Dieser Aspekt muss sicher überarbeitet werden.

## **Behörden müssten deutlich personell aufgestockt werden**

Es sollen hunderttausende von Meldungen sein, die im BKA auflaufen. Aber wäre das überhaupt dafür gerüstet? Klare Antwort: Nein! Deshalb macht ein solches Gesetz auch nur Sinn, wenn der Apparat dahinter das auch bewältigen kann.

Das BKA hat sein Personal schon aufgestockt. Aber das ist auch ein riesiges Problem und ein wichtiger Teil der Kritik: Nicht nur das BKA müsste aufgestockt werden, auch die Länderpolizeien, an die die Fälle weitergereicht werden. Es braucht mehr Personal. Bessere Ausstattung. Bessere Kompetenz und Schulung.

Dasselbe gilt für die Staatsanwaltschaften: Es wären Hunderte von zusätzlichen Staatsanwälten nötig. Auch die Justiz müsste erweitert werden, um die geschätzt 150.000 Fälle zügig bearbeiten zu können. Dazu kein Wort aus der Regierung. Denn das kostet viel Geld – und die Stellen lassen sich ja auch nicht von heute auf morgen besetzen.

Meldung und effektive Strafverfolgung ist zweifellos sinnvoll – wenn der entsprechende Apparat da ist. Aber die Speicherung von solchen sensiblen Daten, weil Soziale Netzwerke Fälle melden – lieber mehr als weniger, um rechtssicher zu sein –, ist höchst problematisch.



## Passwörter rausgeben? So ein Unsinn...

Kritiker stören sich auch daran, dass Polizei und Behörden Passwörter anfordern können, um in die Konten zu schauen.

Zu Recht. Anfangs war das umfangreicher geplant, jetzt nur noch auf richterliche Anordnung. Aber es ist wirklichkeitsfremd: Passwörter werden nicht in Klartext gespeichert und können deshalb auch nicht herausgegeben werden. Das ist also eine Nonsense-Anforderung. Oder die Onlinedienste müssten [Passwörter](#) künftig im Klartext speichern.

Ein aus gutem Grund absolutes Nogo in der Informatik. Viel zu gefährlich, leichter kann man es Hackern nicht machen. Auch [netzpolitik.org warnt davor](http://netzpolitik.org/warnt-davor). Die Begehrlichkeit ist verständlich – aber vollkommen unrealistisch. Oder nur unter extrem hohen Nebeneffekten zu realisieren. Übrigens war eben das auch schon [in der eEvidence-Verordnung geplant](#).



## Korrekturen nötig

Es wird sicher noch Korrekturen am Gesetzentwurf geben, anderenfalls wird der Bundestag das sicher nicht bestätigen. Bedenklich ist, dass Facebook und Co. zu "Hilfs-Sheriffs" gemacht werden, sagen Kritiker. Das stimmt auch. Viel besser wäre es, Schwerpunkt-Staatsanwaltschaften aufzubauen – wie die ZAC (Zentral- und Ansprechstelle Cybercrime) in Köln. Das funktioniert sehr gut.

Mehr davon – und die besser ausstatten. Allerdings müssten die Plattformen dann auch Daten herausgeben, wenn Ermittlungen eingeleitet werden. Das tun sie heute nicht, weil sie nicht müssen, beklagt sich der Chef dieser Staatsanwaltschaft. Solche Aspekte kann und sollte ein NetzDG 2.0 verbessern. Aber ohne Passwort-Herausgabe und Melderegister beim BKA.

## Jeff Bezos stiftet 10 Mrd. Dollar für Klimaschutz

Jeff Bezos - immerhin reichster Mann der Erde - spendet 10 Mrd Dollar aus seinem Privatvermögen für Klimaschutz. Das wirkt edel und ist definitiv besser als alle jene Unternehmen, die rein gar nichts unternehmen. Aber: Es ist auch ein Etikettenschwindel.

Der Nachricht können wir gerade nicht entgehen: "Amazon-Chef Jeff Bezos will 10 Milliarden für Kampf gegen Klima-Wandel spenden", ist überall zu lesen. Der reichste Mann der Welt macht es dem ehemals reichsten Mann der Welt nach und spendet einen Teil seines Vermögens für einen guten Zweck. 10 Milliarden - Wow, das klingt für die meisten von uns nach einer Menge Geld. Aber ist es das auch? Nein.

Die Kollegen vom Handelsblatt haben sich sogar die Mühe gemacht auszurechnen, wie lange ein/e Durchschnittsverdiener/in [arbeiten müsste, um 10 Milliarden Dollar zu verdienen](#): rund 280.000 Jahre. Wenn man so etwas liest, ist man - als gewöhnlicher und einfacher Mensch, der wir nun mal sind - geneigt, beeindruckt zu sein. Den Fehler sollten wir aber nicht machen.



### Bezos und das Zehnt

Alles knallhartes Kalkül. Das mit den 10% ist vermutlich kein Zufall. Schon im alten Testament wird berichtet, [dass ein Zehntel einer Kriegsbeute](#) abgabepflichtig sei. Der berühmte "Zehnte"

also. Später hat sich auch die Kirche ein Zehntel Abgaben bei allen geholt. Ein Zehntel als Abgabe hat also Tradition. Nach dem Motto: Danach ist aber alles gut. Schuldigkeit getan.

Jeff Bezos Vermögen beläuft sich auf 103 Milliarden Dollar. Er "spendet" also rund 10% seines Vermögens. Das ist bestenfalls schön. Aber ganz sicher nicht respektabel. Denn es tut ihm nicht weh. Es ist ihm völlig schnurz. Er bemerkt es nicht einmal. Aber er will als "Big Spender" dastehen. Als ein Mann, der Gutes tut.

## Lange Liste von Sünden

Natürlich will er nicht wirklich was Gutes tun. Jeff Bezos wäre nicht Jeff Bezos, wenn er ein guter Mensch wäre. Der Psychologe und letztlich auch der gesunde Menschenverstand weiß: Bezos denkt auch hier nur an sich. Ich denke: Er will sich von seiner Schuld reinwaschen. Denn selbst so einem wie Jeff Bezos ist doch insgeheim klar, dass er die Welt in Verderben stürzt mit seinem Konzern. Die Liste der Sünden ist lang:

- Explosion des Online-Handels mit bekannten Folgen für Klima und Umwelt
- Potenzierung des Konsums an sich - mit den bekannten Folgen für Klima und Umwelt
- Expansion des Cloud-Geschäfts - mit den bekannten Folgen für Klima und Umwelt
- Vernichtung von Arbeitsplätzen im Einzelhandel weltweit
- Zerstörung ganzer Branchen, etwa den unabhängigen Buchhandel
- Hunderttausende Mitarbeiter in prekärer Beschäftigung
- Steuerflucht und Steuervermeidung (nicht illegal, aber unmoralisch)
- und vieles mehr

Mir ist bewusst: Das werden viele nicht gelten lassen. Sie sehen Bezos als den Heilsbringer, weil er viele innovative Ideen entwickelt hat und ungeheuer erfolgreich ist. Das ist wahr. Verantwortlich für die Folgen ist er dennoch - und nicht die Menschen, die bei ihm bestellen. Denn er allein hat das alles aufgebaut und nichts gegen die möglichen Folgen unternommen. Einzig und allein zu seinem eigenen Vorteil.

Jetzt um die Ecke zu kommen und einen winzigen Teil seines Vermögens zu "spenden" ist daher ein Witz. Nüchtern betrachtet wird das nicht mal reichen, um die durch ihn verursachten Klimaschäden zu beseitigen.

Es dient eben nur dem einen Zweck: Jeff Bezos will gut dastehen. Sich gut fühlen. Vermutlich sogar gefeiert werden. Diesen Gefallen werde ich ihm nicht tun.

<https://vimeo.com/364783887>

*Jeff Bezos Konzern ist Weltmeister beim ungenierten Datensammeln*

## NetzDG 2.0: Neue Regeln, neue Bedenken

Seit zwei Jahren gibt es in Deutschland das Netzwerkdurchsetzungsgesetz (NetzDG). Der Ansatz ist gut, finden viele - selbst Kritiker. Aber im Detail nicht sorgfältig genug durchdacht und formuliert. Jetzt hat das Kabinett eine Gesetzesverschärfung auf den Weg gebracht. Verschärfte Regeln, Meldepflicht ans BKA - und Passwortherausgabe. Da regt sich Widerstand.

Seit 2018 gilt in Deutschland das Netzwerkdurchsetzungsgesetz ([NetzDG](#)). Es soll die zunehmende Hetze und den Hass in den Sozialen Netzwerken eindämmen helfen. Es hat durchaus etwas gebracht. Aber einen Durchbruch, eine wirkliche Besserung der Situation hat das NetzDG dann auch nicht gebracht. Aber immerhin müssen Facebook und Co. Inhalte, die "offensichtlich Rechtsverstoß" begehen, löschen - wenn sie gemeldet werden.



Das aber reicht nicht. Das sehen die User in Facebook, auf Twitter und YouTube jeden Tag. Die Stimmung kocht immer weiter hoch - der Anstand hat sich verabschiedet. Deshalb hat das [Bundesjustizministerium nun eine weitere Zündstufe geschaltet](#). Das NetzDG soll verschärft werden, Künftig müssten die Sozialen Netzwerke auch selbst und aktiv Rechtsverstöße melden. Also Postings melden, die Hass, Hetze oder - das ist neu! - auch die Bedrohung durch sexuelle Gewalt enthalten.

### Das BKA als zentrale Meldestelle für Hass- und Hetzkommentare

Richtig so. Denn nicht selten finden sich Postings wie "Ich f\*\*\*\* Dich durch, Du Schlampe!" im Netz. Ich vermisse nichts, wenn solche Postings komplett verschwinden. Auch wenn es nur ist, weil die Urheber eine aktive Strafverfolgung befürchten müssen. Hass und Hetze - was das ist, lässt sich bekanntlich nicht immer messerscharf erkennen und trennen. Aber die Sozialen Netzwerke sollen ja Meldung machen. Entscheiden, was strafbar ist und was nicht, müssen dann andere.

Die Meldungen landen zentral beim Bundeskriminalamt (BKA). Da wird dann entschieden, wie es weiter geht - und die Sache ggf. an die jeweilige Landespolizeibehörde weitergeleitet. Das erscheint ein sinnvoller Schritt. Denn so beschäftigt sich gleich die Polizei damit.

Allerdings: Die Behörden sind gar nicht ausreichend ausgestattet. Das BKA hat zwar sein Personal aufgestockt - aber die Staatsanwaltschaften und die Polizei nicht. Wer ein solches Gesetz (er)schafft und auf den Weg bringt, der muss auch für die nötige finanzielle, personelle und materielle Ausstattung bei Polizei, Staatsanwaltschaften und Justiz sorgen. Und selbst wenn man das wollte: Das gelingt nicht von jetzt auf gleich. Nötig scheint es aber allemal.

Jeder erfahrene Staatsanwalt und Polizist sagt: Wenn tatsächlich nach Hass, Hetze, Beleidigungen etc. die Polizei auf der Matte steht - und so etwas spricht sich rum! -, dann hinterlässt das Eindruck.

## **Passwörter rausgeben? Das kann nur Ultima Ratio sein**

Kritik gibt es, weil das NetzwerkDG auch vorsieht, dass die Netzwerke Zugangsdaten und Passwörter rausrücken sollen/müssen. Das war auch bei [der eEvidence-Verordnung so vorgesehen](#). Neben der Tatsache, dass Passwörter nicht im Klartext gespeichert werden diese Anforderung gegen jeden gesunden Menschenverstand beim Datenschutz verstößt, ist der grundsätzliche Ansatz nicht verkehrt.

Wieso sollte man schlimme Straftäter schützen? Nach der Kritik wurde der Entwurf des NetzwerkDG insofern geändert, dass diese Herausgabe nur bei schweren Straftaten und auf richterliche Anordnung erfolgen soll. Aber darüber wird sicher noch am meisten diskutiert.

Ich denke: Was nützt ein NetzwerkDG, wenn es Richter/innen gibt, die - wirklich von allen guten Geistern verlassen! - Schmähungen schlimmster Sorte gegen eine Politikerin wie Renate Künast als zulässig erachten? Wie soll man den Menschen da klar machen, dass es ein NetzwerkDG braucht?

Also: Es muss was passieren - und meiner Ansicht nach enthält das NetzwerkDG durchaus gute und sinnvolle Werkzeuge. Allerdings muss Polizei und Justiz auch entsprechend ausgestattet werden. Es braucht Gerichte, die Beleidigungen auch als solche ahnden. Und last not least braucht es natürlich auch eine gesellschaftliche Veränderung. Denn diese schlimme Stimmung gibt es nicht nur im Netz. Druck, Frust und Wut haben ihre Gründe. Auch da muss was passieren.



*netzpolitik.org Markus Bechedahl über das NetzwerkDG (gültige Fassung)*

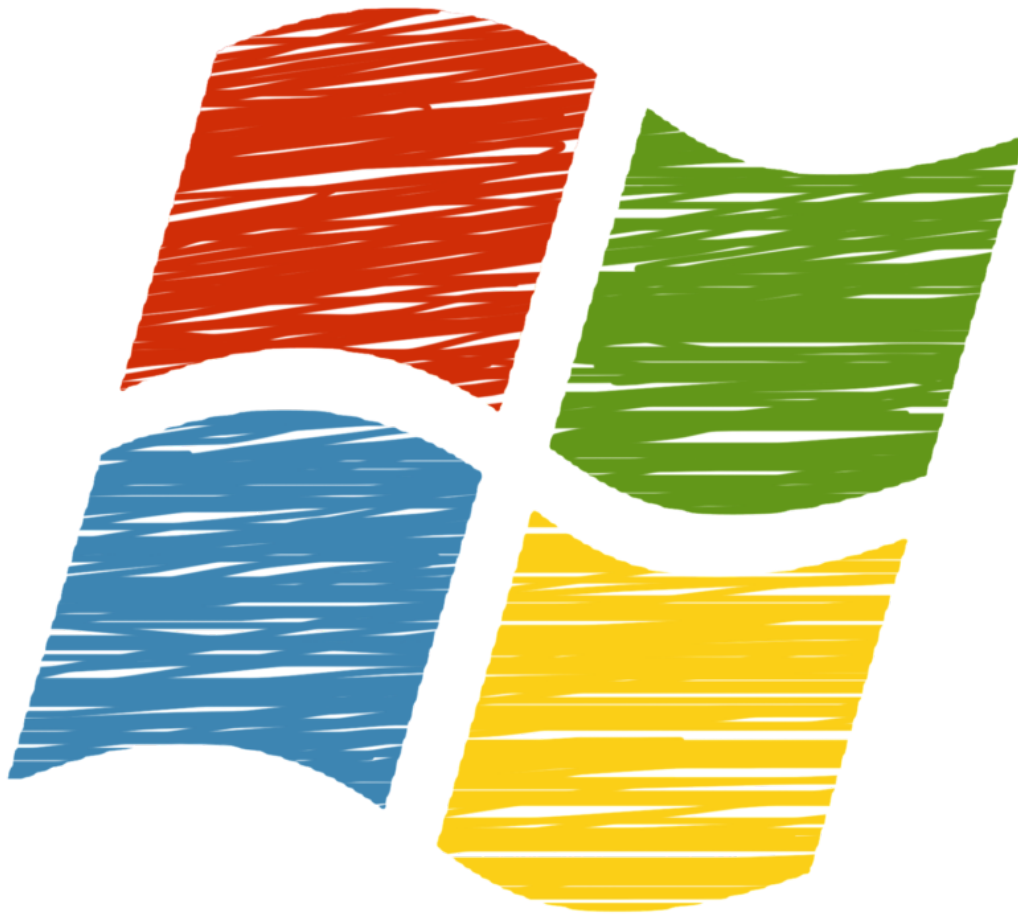
## 20 Jahre Windows 2000: Die Bedeutung von Betriebssystemen heute

Windows kennen die meisten von uns. Als Betriebssystem für den Tisch-PC zu Hause oder im Büro. Bei den Versionsnummern gab es aber schon immer ein gewisses Durcheinander: Windows 3.1, Windows 95 – da steckte die Jahreszahl im Namen. Windows NT. Für Unternehmen. Windows 2000 – wieder mit der Jahreszahl im Namen. Windows XP- Und heute nutzen wir Windows 10. Windows 2000 war ein Meilenstein – aber auch nicht sooooo erfolgreich, könnte man meinen.

20 Jahre es ist her, dass [Windows](#) 2000 auf den Markt gekommen ist. Ich habe es mir damals routinemäßig angeschaut - damals habe ich Bücher zu jedem Windows geschrieben.

Windows 2000 war ein technologischer Meilenstein: Sehr modern, es gab mehrere Versionen, für den Tisch-PC und für Server. Aber „normale“ User, etwa zu Hause, haben sich kein Windows 2000 besorgt. Denn Windows 2000 war ein Betriebssystem für professionelle Ansprüche, für Unternehmen, um Daten zu organisieren.

Etwa durch das damals moderne Dateisystem NTFS: Damit wurden Dateien auf der Festplatte organisiert. Anders als in den anderen Windows-Versionen. So etwas konnte zu Hause niemand gebrauchen. Deswegen besteht heute der Eindruck, Windows 2000 wäre nicht erfolgreich gewesen. Am Ende haben die Windows-Versionen danach auf Windows 2000 aufgebaut. Es war also ein Erfolg.



## **Durcheinander bei den Versionsnummern**

Heute benutzen wir Windows 10, wenn wir auf dem Tischcomputer Windows einsetzen. Bei den Versionsnummern gerät man total durcheinander.

Ein paar Mal wurden Jahreszahlen im Namen des Betriebssystems verwendet, beim extrem erfolgreich Windows 95 zum ersten Mal, bei Windows 98, bei Windows 2000. Dann wurden Kürzel benutzt, etwa „XP“ für „Experience“ – Erfahrung.

Oder NT für „New Technologie“ – neue Technologie. Dann kamen Windows 7, 8 und dann nicht etwa 9, sondern 10. Weil die Mac-Welt auch schon bei der 10. Generation angekommen

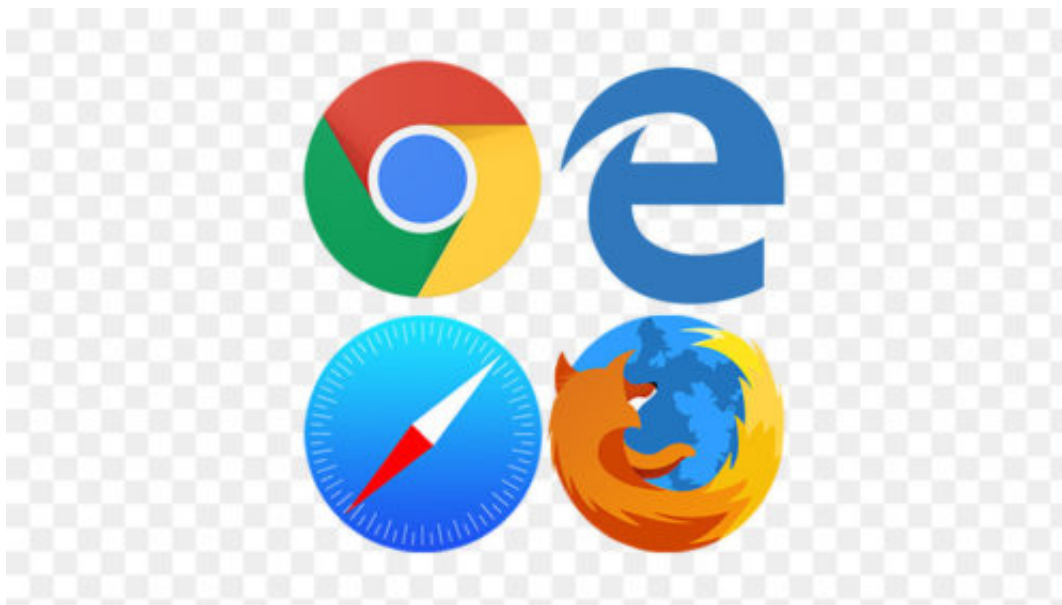
war. Eine Mischung aus PR, Marketing und Durcheinander. Am Ende sind die Namen aber auch egal.

## Der Browser als Betriebssystem?

Früher war es immer sehr wichtig, die neueste Version eines Betriebssystems zu benutzen. Heute scheint das nicht mehr so wichtig.

[Updates](#) sollten Windows-Nutzer selbstverständlich laden und einspielen, damit das Betriebssystem auf dem neuesten Stand ist – und keine Sicherheitslücken hat. Aber es stimmt: Heute sind andere Dinge wichtig. Der Browser ist heute das Betriebssystem. Da wir vor allem im Web und im Netz unterwegs sind, ist es wichtig einen Browser zu verwenden, der alles beherrscht: Der Videos schnell und ruckelfrei abspielt, Downloads organisiert, sich um die Sicherheit im Netz kümmert, Passwörter merkt und vieles andere mehr.

Der Browser gilt heute als das Betriebssystem der Zeit. Hier entscheidet sich, welche Funktionen im Netz genutzt werden können und welche nicht – und nicht im eigentlichen Betriebssystem. Am Ende ist es sogar egal, ob wir PC, Tablet oder Smartphone benutzen. Aber auch die Bedeutung des Browsers beginnt zu schwinden...



## Sprechen mit den Geräten

Es gibt viele Geräte – und davon immer mehr –, da wissen wir nicht mal, ob sie ein Betriebssystem haben – und einen Browser brauchen sie nicht. Man denke an Digitale Assistenten, mit denen wir sprechen. Wir sprechen – wir klicken und tippen nicht. Die Sprach-Schnittstelle ist das Betriebssystem, also Siri, Google Home, Alexa und Co.

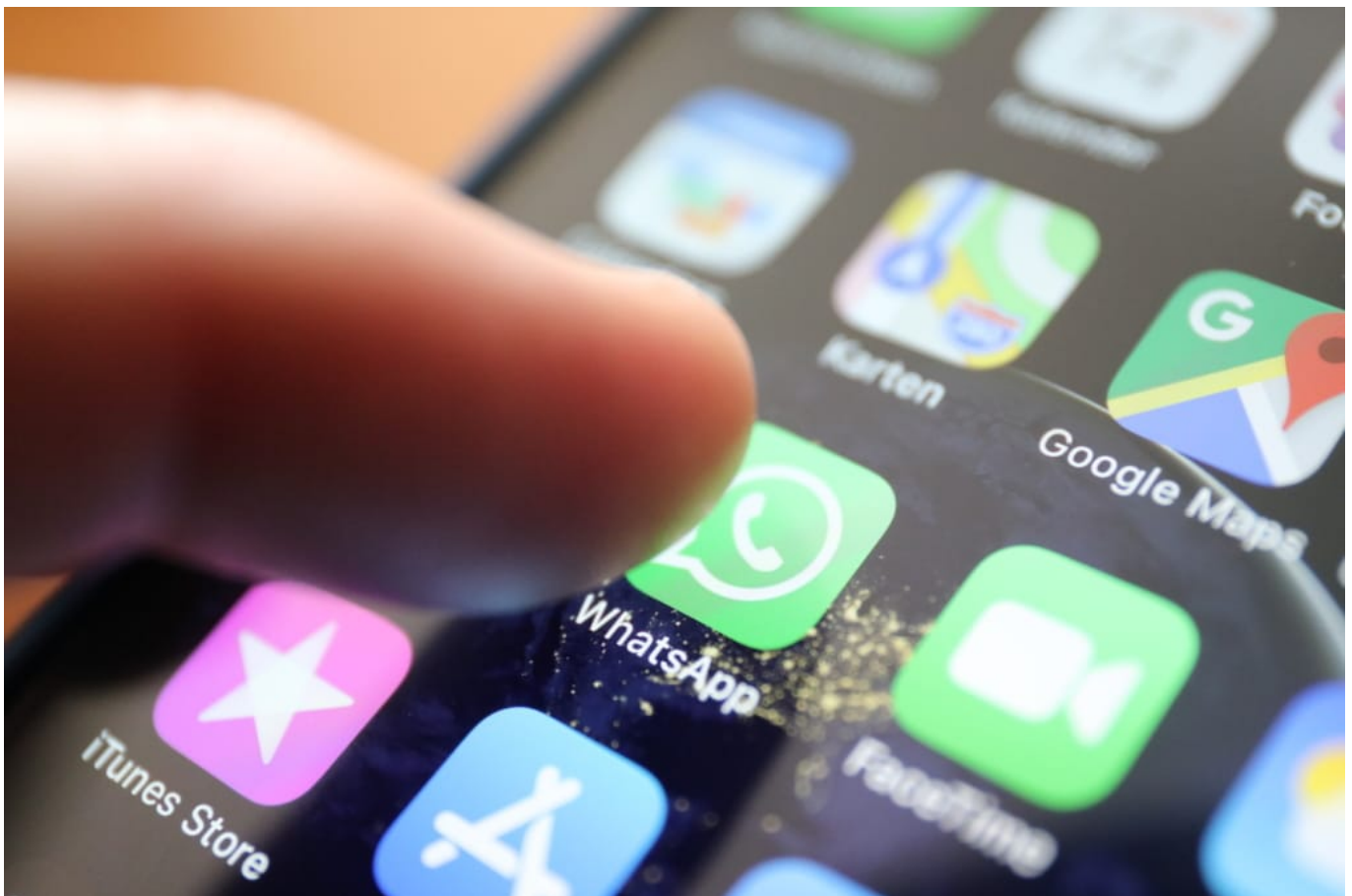
Und die Macht dieser Betriebssysteme ist größer denn je. Denn sie entscheiden, was sie verstehen wollen, was sie ausführen – und zum Beispiel auch, bei welchem Musikdienst ein

Song abgespielt wird. Es wird nur der erste Treffer einer Suche vorgelesen – und nicht 10, 20 oder mehr Treffer, aus denen man auswählen kann. Durch diese neuen Betriebssysteme, die Komfort versprechen, verlieren wir Autonomie und Kontrolle. Leider wird es in diese Richtung weiter gehen.

## WhatsApp und die vielen Metadaten, die anfallen

WhatsApp ist beliebt. WhatsApp ist nützlich. WhatsApp ist kostenlos. Aber halt: Das nicht so ganz. Denn wie so häufig bezahlen wir mit unseren Daten. Im Fall von WhatsApp auf eine ganz subtile Weise: Es fallen jede Menge Metadaten an, von denen wir nichts wissen. Und wir wissen auch nicht, welche davon bei Facebook landen und wie diese verarbeitet und genutzt werden. Das sollte sich dringend ändern. [WhatsApp](#) hat gerade die Marke von zwei Milliarden Nutzern weltweit geknackt. Mark Zuckerberg wird das freuen.

Dabei besteht gar kein Grund zur Freude, denn Facebook legt gerade die Messenger WhatsApp, Instagram und Facebook Messenger in einem Netzwerk zusammen. Schon bald sollen Instagram-Nutzer auch WhatsApp-Usern eine Nachricht schreiben können. Ebenso Usern im Facebook Messenger. Dann hat Facebook die Kontrolle über noch mehr Messenger-User.



### Es fallen unentwegt Metadaten an

Mark Zuckerberg stellt gerne die [Ende-zu-Ende-Verschlüsselung](#) in den Vordergrund, die es in WhatsApp erfreulicherweise schon gibt - und schon bald auch in Instagram (da gibt es noch keine Verschlüsselung) und im Facebook Messenger (hier gibt es in einigen Bereichen noch keine Verschlüsselung) geben soll. Klare Botschaft: Mehr Sicherheit für die User. Ist das nicht

fein? Es stimmt schon, dass selbst Facebook die Inhalte der Nachrichten dann nicht kennt. Aber diese Daten sind auch nicht so spannend für Facebook.

Viel spannender sind die Metadaten. Die fallen in allen Messengern an - und sind unverschlüsselt. Über diese Metadaten redet Mark Zuckerberg gewöhnlich nicht. Er nutzt sie nur. Metadaten sind besonders interessant für Facebook. Sie fallen klammheimlich an. Die Nutzer merken es gar nicht. Aber sie sind ungeheuer aussagekräftig - und wertvoll. Anhand der Metadaten erfährt der Konzern jede Menge über einen.

Jetzt aber mal Butter bei die Fische, damit wir nicht so abstrakt bleiben: Facebook kennt mein Bewegungsprofil. Wer WhatsApp immer "an" hat, liefert unentwegt Bewegungsdaten an Facebook. Facebook weiß, wo man wohnt, wo man gelegentlich übernachtet. Ob man ins WLAN geht (zu Hause, Freunde, Hotel) oder ob man das Funknetzwerk verwendet. Ein perfektes Bewegungsprofil entsteht. Das kennen Google und Co. zwar auch. Doch dank WhatsApp und Instagram hat Facebook gleich zwei Apps, die nahezu immer aktiv sind - und nahezu immer Daten liefern.

## **Bewegungsprofil und Psychogramm dank Metadaten**

Facebook kennt auch mein soziales Umfeld. Die Namen und Rufnummern aller Personen, mit denen ich Nachrichten austausche (bei Instagram nur die Namen). Wann ich kommuniziere. Wie oft ich kommuniziere. Wie schnell ich reagiere. Wer nachts um 3 Uhr eine Nachricht verschickt, schreibt höchstwahrscheinlich gerade mit einem engen Freund/einer engen Freundin. Wer täglich 50 Nachrichten miteinander austauscht, steht sich sehr nah. Außerdem weiß WhatsApp auch, wann, wo und wie oft wir uns sehen (siehe: Bewegungsprofil).

Datenschutzexpertin [Katharina Nocun](#) schildert mir im Interview verschiedene Alltagssituationen, die aussagekräftige Metadaten abwerfen ([siehe Interview im Video](#)).

Auf diese Weise entsteht möglicherweise ein Psychoprofil, das in seiner Detailtiefe erschreckend ist. KI kann Verhaltensmuster errechnen, ja selbst den Gemüts- oder Beziehungsstatus ermitteln. Alles, ohne die Nutzer zu fragen, ohne sie zu informieren und ohne Einblicke in die gesammelten Daten zu geben. Das ist (ein) weiterer Grund, wieso Facebook die Menschen ähnlich gut kennt, wie Partner und die Familie.

Das Problem: Über Metadaten wird nie gesprochen. Facebook schweigt das Thema tot. Aber wir sind gut beraten, das Schlimmste zu befürchten: Nämlich, dass sich Facebook hemmungslos bedient und die Daten ausschachtet. Facebook macht immer, was technisch machbar ist. Moral spielt keine Rolle. Business first.

Ich finde: Wir haben einen Anspruch darauf zu erfahren, welche Metadaten anfallen und welche Metadaten die Konzerne speichern - und welche Schlüsse sie daraus ziehen. Ohne anwaltliche Hilfe in Anspruch nehmen zu müssen. Die EU sollte in diesem Punkt die DSGVO verschärfen: Komplette Transparenz - sofort.

## FamiSafe – Sicherheit für Kinder

Überwachung – ein Szenario, das für Unruhe sorgt. Niemand möchte seine Position, sein Surfverhalten, seine Vorlieben von jemand anderem kontrolliert wissen. Und doch gibt es Szenarien, die den Wunsch dazu aufkommen lassen. Ab einem gewissen – und immer geringer werdenden – Alter seiner Kinder kann man sich kaum noch wehren, diesen ein Smartphone mitzugeben. Erreichbarkeit, Kontaktmöglichkeit, wichtige Apps und sozialer Druck, wie alle anderen ein Smartphone zu haben, machen es zur Pflicht. Es gibt aber Apps, die hier helfen können!

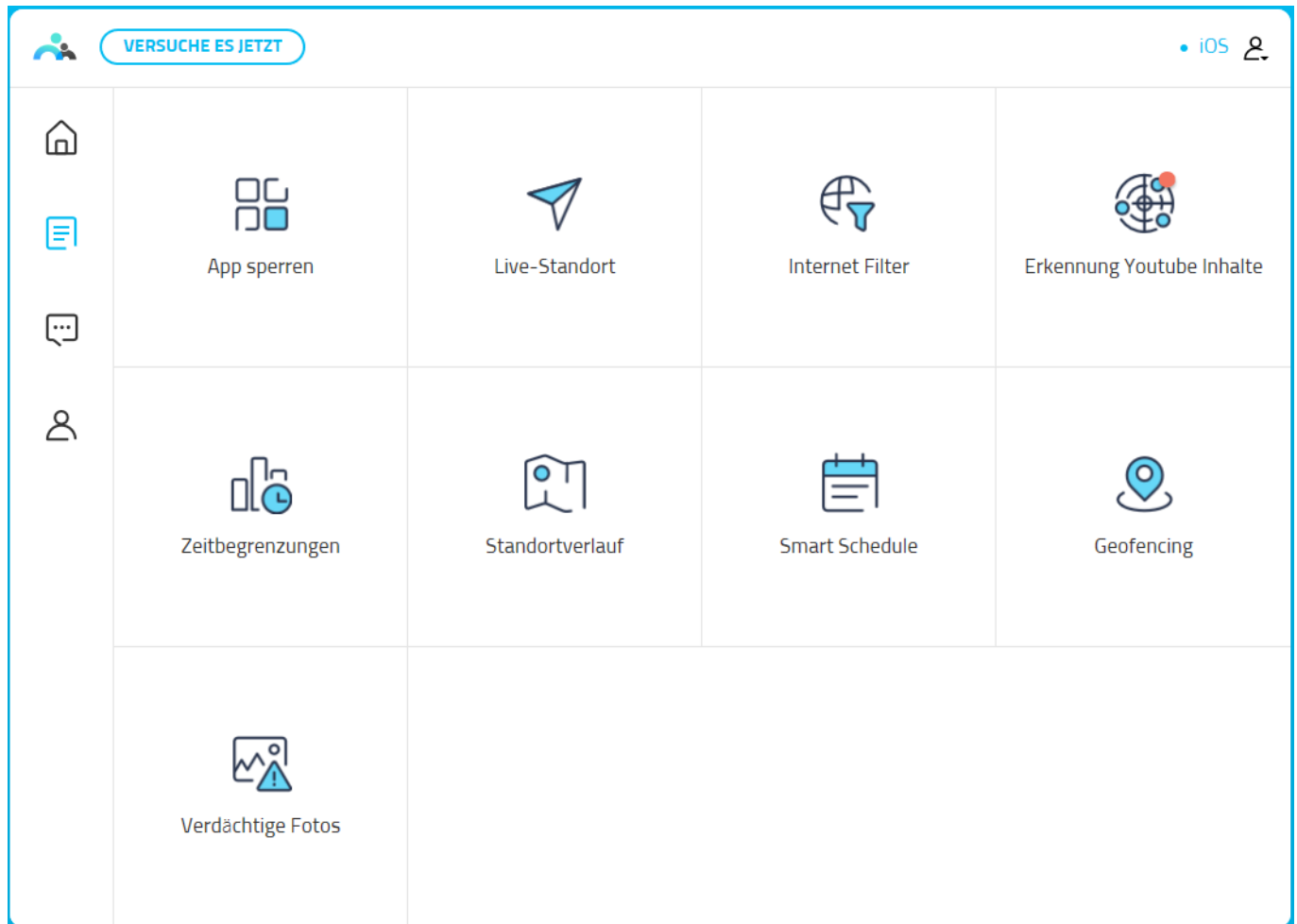


Die freie Nutzung aber, für die Eltern oft unkontrollierbar, ist ein Risiko: wie schnell sind Webseiten aufgerufen, die nicht für Kinder geeignet sind? Wie schützt man Kinder davor, dass sie zu lange vor dem Smartphone hängen? Und wie kann man die Möglichkeiten eines Smartphones nutzen, um das Kind zu schützen?

Die Antwort können Apps wie [FamiSafe](#) geben. Die App, die es für iOS und Android gibt, besteht aus zwei Seiten: Der Erwachsene muss diese auf seinem Handy installieren, die Installation muss natürlich ebenfalls auf dem Gerät des Kindes vorgenommen werden. Wichtig dabei: Beziehen Sie das Kind ein. Erklären Sie, warum Sie was einrichten. Zum eine ist das



eine Frage der Fairness, zum anderen kann es auch für ein Gefühl von mehr Sicherheit beim Kind sorgen!



Folgende Funktionen sind dann möglich und können entweder vom Elterngerät oder von der Weboberfläche eingerichtet werden:

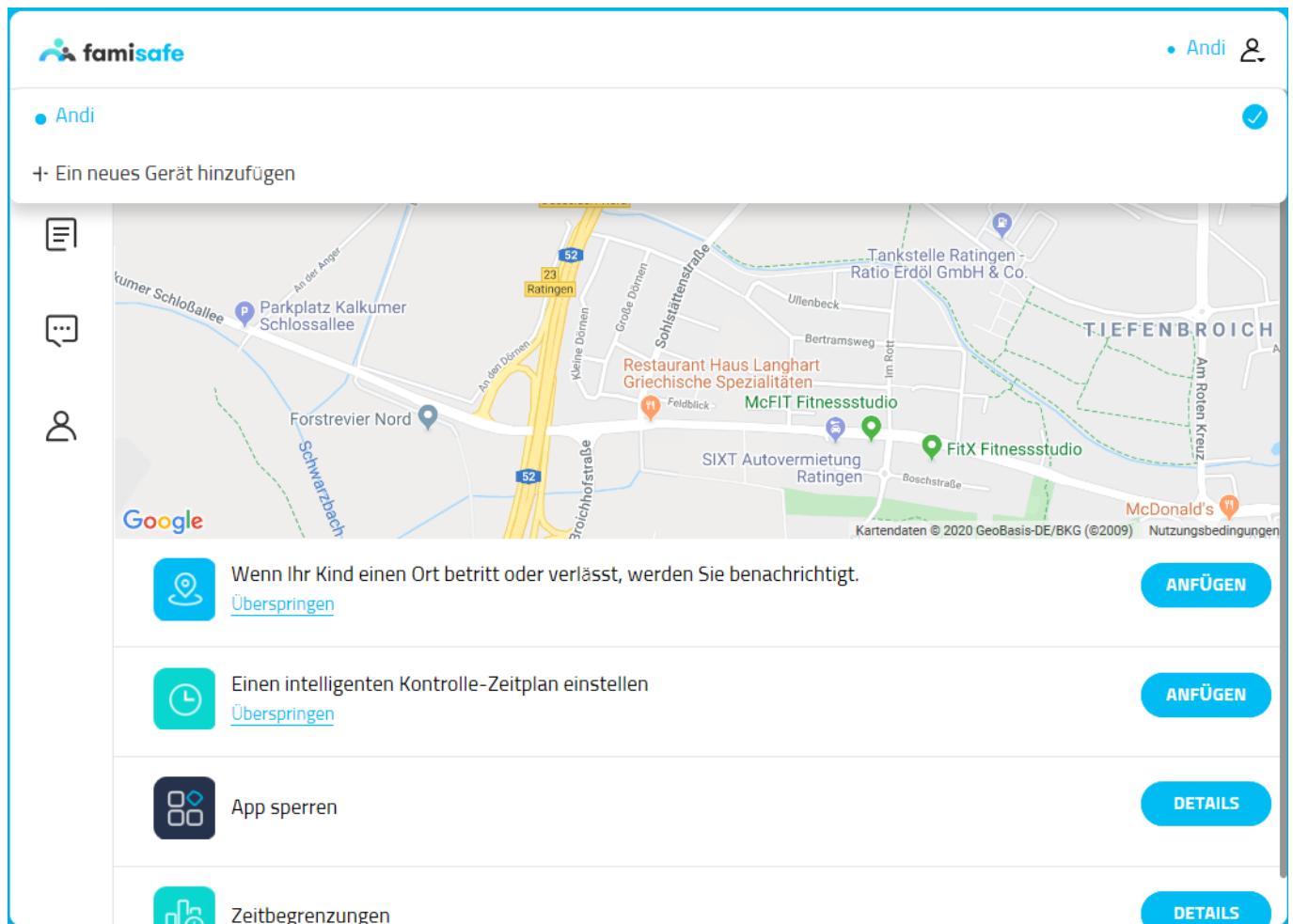
## Kampf gegen Cybermobbing: Analyse verdächtiger Wörter

Cybermobbing ist allgegenwärtig: schnell wird man Ziel von Beschimpfungen und Schmähungen. Wo wir Erwachsenen noch die Möglichkeit haben, uns dem zu widersetzen sind Kinder oft schutzlos. FamiSafe erlaubt es, die SMS, WhatsApp- und Messenger-Nachrichten des überwachten Gerätes auf anstößige Wörter zu überprüfen. Diese vorgefertigte Liste können Sie zusätzlich noch um eigene Begriffe erweitern. Sobald in einer der Nachrichten eines der Schlüsselwörter erscheint, bekommen Sie eine Information und können eingreifen.

## Standorte/Geofencing

Sicherlich eine der diskutabelsten Dinge ist immer die Überwachung der Position einer Person. Bei Kindern ist aber oft der Wunsch vorhanden, sie auffinden zu können. Wenn sie nicht pünktlich nach Hause kommen, nicht da sind, wo man sie abholen will etc. Hier setzt die

Standort-Funktionalität an: Sie können sich jederzeit den letzten Standort anzeigen lassen. Alternativ definieren Sie Bereiche, die das Kind nicht verlassen darf, sonst bekommt das Gerät der Eltern eine Warnung.



## Zeitbegrenzungen

Limitieren Sie die Nutzung von Apps auf Stundenbasis. Dies bezieht sich auf Drittanbieter-Apps wie Facebook, WhatsApp und andere. Über Reports können Sie sehen, wie lange das Kind die Apps genutzt hat. Bei Bedarf können Sie dann Apps mit einem Klick sperren oder ein Stundenkontingent vergeben. Dann sind die Apps eben nicht mehr nutzbar. Die Grund-Apps wie Telefonie, Nachrichten etc, sind davon nicht betroffen, sodass das Kind erreichbar bleibt.

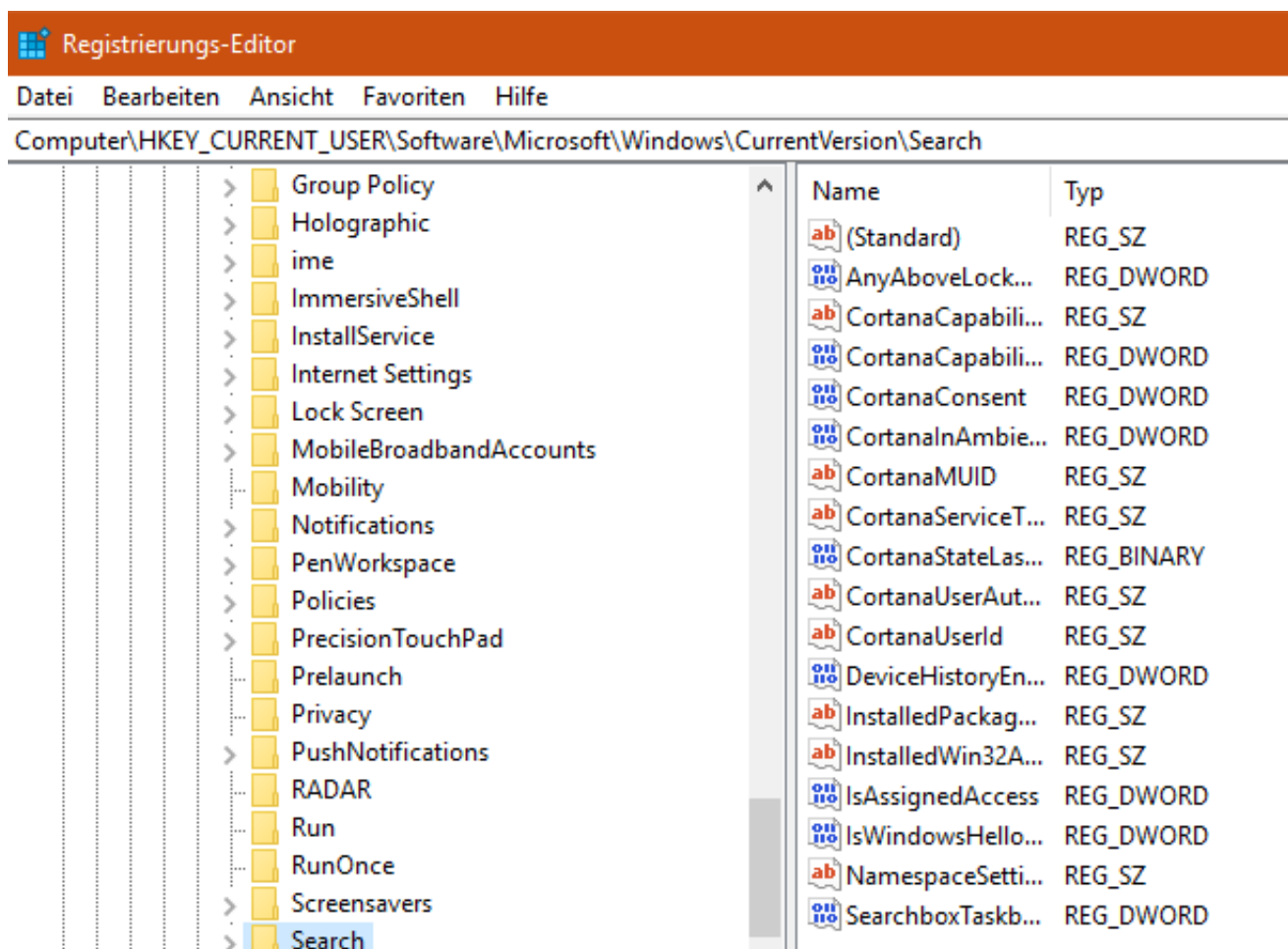
## Sperren von Webinhalten

Auch einen klassischen Webfilter bietet FamiSafe. Hier können Sie Kategorien von Webseiten sperren und Ausnahmen zu dieser Liste definieren. Da werden dann alle Apps gesperrt, aber die Ausnahmen erlaubt. Safari verweigert dann den Aufruf von Seiten der gesperrten Kategorien. So können Sie verhindern, dass Gewalt- oder Erotikseiten aufgerufen werden können.

## Wenn die Windows-Suche nicht mehr funktioniert

Ihr PC ist Ihr zentraler Datenspeicher. E-Mails, Dokumente, Termine, all diese Elemente sammeln Sie in den verschiedenen Programmen und Laufwerken. Egal, wie ordentlich Sie Ihre Daten ablegen und wie gut Sie Ihre eigene Ablage kennen: Wenn Sie ein bestimmtes Element brauchen, bemühen Sie des Komforts wegen die Suche. Was aber, wenn die Suche nicht funktioniert?

Normalerweise geben Sie in die Suchleiste in der Taskleiste bzw. durch Klick auf die Lupe den Suchbegriff ein und lassen Windows 10 den Rest tun: Alle Elemente, die Windows lesen kann (darunter fallen die Office-Dokumente, Textdateien, E-Mails, PDF-Dateien und vieles mehr) werden auf den Suchbegriff durchsucht und die ihn enthaltenden Elemente kategorisiert und sortiert angezeigt. Dazu sucht Windows 10 aber nicht nur die lokalen Verzeichnisse, sondern auch das Internet. Ist Bing eingebunden und es liegt auf der Server-Seite ein Fehler vor, dann bekommt Windows 10 einen Berechtigungsfehler zurückgespielt. Damit scheitert die Suche komplett. Die Lösung: Deaktivieren Sie Bing über die Registry.



Dazu starten Sie den Registry Editor unter **Ausführen** -> **regedit.exe** und navigieren Sie dann zu dem Schlüssel

*HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Search*

Dort legen Sie folgende beiden Schlüssel *BingSearchEnabled* und *CortanaConsent* durch Klick auf **Datei** -> **Neu** -> **DWord** an, sofern diese noch nicht existieren und geben Sie diesen jeweils den Wert *00000000*. Nach dem Speichern der Registry und dem Neustart des PCs sollte die Suche wieder funktionieren.

## Einzelne Seiten aus PDF-Dateien kopieren

Das PDF-Format hat sich als Standard etabliert. Vor allem, weil es über alle Betriebssysteme und Gerätekategorien nutzbar ist und mit dem kostenlosen [Adobe Acrobat Reader](#) gelesen werden kann. Die Konsequenz: Immer mehr Mailanhänge sind nicht mehr einzelne Dateien, sondern eine zusammenfassende PDF-Datei. Das stellt Sie vor Herausforderungen, wenn Sie nur einige Seiten benötigen. Wir zeigen Ihnen die Lösung!

Microsoft hat mit Windows 10 die Möglichkeit mit aufgenommen, aus einer beliebigen Datei eine PDF-Datei zu machen. Die teure Software von Adobe ist dafür nicht mehr nötig. Um das zu nutzen, stellen Sie beim Druck-Dialog einfach den Drucker auf **Microsoft Print to PDF** ein. Und da die Funktion wie ein normaler Druckertreiber funktioniert, können Sie auch genau angeben, welche Seiten gedruckt werden sollen.

Drucken

Drucker: Microsoft Print to PDF Eigenschaften

Exemplare: 1 In Graustufen (s)  
Farbe/Toner spa

**Zu druckende Seiten**

Alle

Aktuelle Seite

Seiten

▶ Weitere Optionen

**Seite anpassen und Optionen** ⓘ

Anpassen

Unter **Seiten** geben Sie einzelne Seiten durch ein Semikolon getrennt an. Wollen Sie die Seiten 1, 3, und 50 drucken, dann eben 1;3;50. Wenn Sie einen Bereich drucken möchten, dann können Sie diesen statt einer einzelnen Seitenzahl als Startseite-Endseite, also zum Beispiel 3-4 eingeben. Einzelne Seiten und Bereiche trennen Sie wieder durch ein Semikolon.

Wichtig: Kontrollieren Sie, dass die Seitenausrichtung korrekt eingestellt ist. Ist das Original im Querformat, sollten Sie auch den Druck so einstellen. Die festgelegten Seiten werden dann eben nicht gedruckt. Stattdessen fragt Windows 10 den Speicherort und Namen der Datei ab. Sie bekommen die selektierten Seiten dann in Form einer PDF-Datei.