Schieb Report

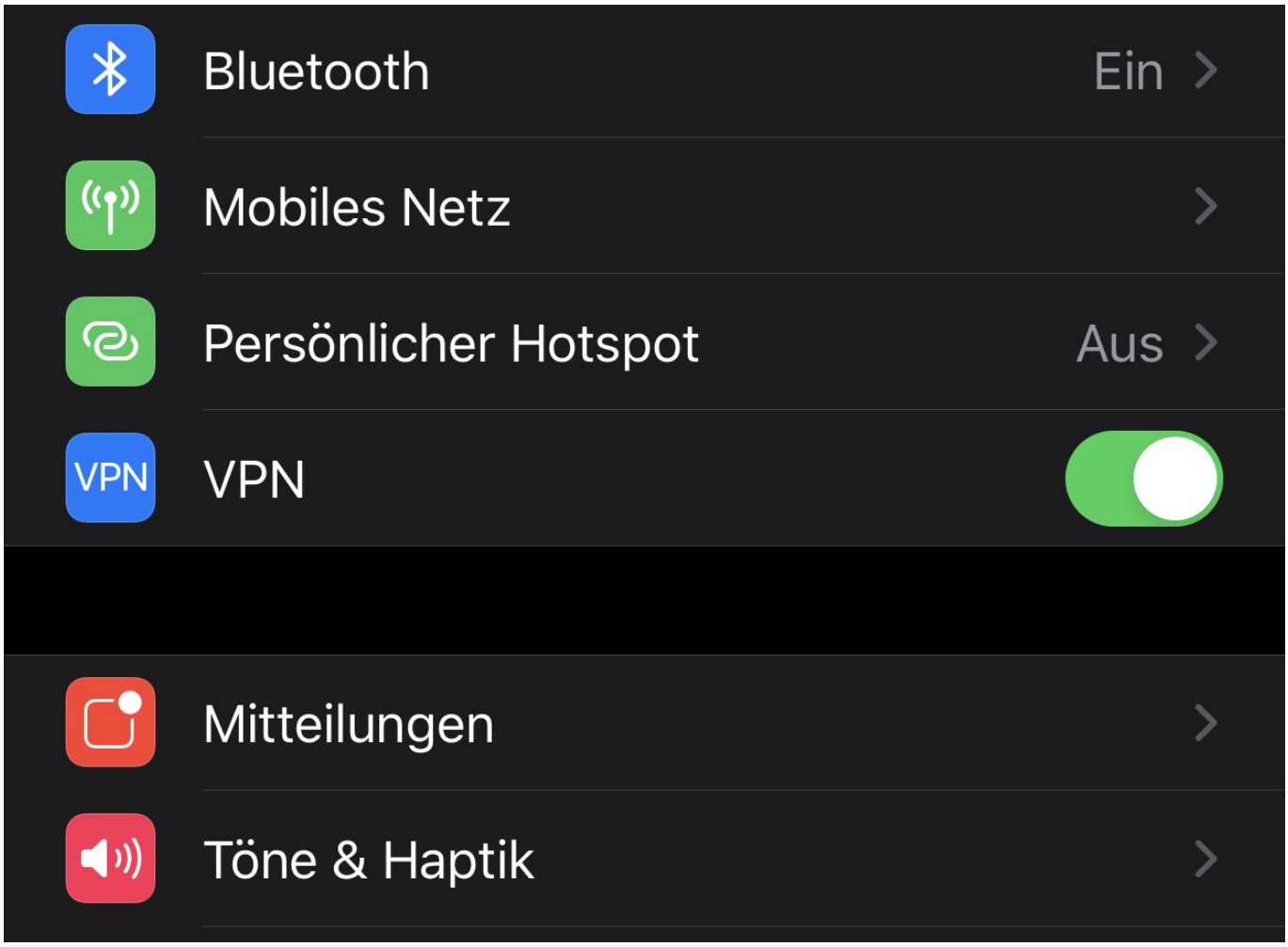
Ausgabe 2020.10

VPN auf dem Smartphone nutzen

Sie kennen die Situation sicherlich: Sie halten sich im Ausland auf, wollen auf dem Smartphone eine Sendung aus einer Mediathek oder einen bestimmten Online-Dienst nutzen. Natürlich sind Sie in einem ausländischen Mobilfunknetz oder WLAN, und damit erkennt der Dienst, dass Sie eben nicht in Deutschland sind. Die Konsequenz: Er verweigert die Wiedergabe mit einer Meldung wie „Diese Sendung ist nur aus Deutschland zugreifbar“. Die Nutzung eines VPN-Dienstleisters schafft nicht nur Sicherheit, sondern auch eine Lösung für das beschriebene so genannte Geofencing.

Eigentlich soll VPN dazu dienen, die Sicherheit des Surfens zu erhöhen: Ein Tunnel zu einem vertrauenswürdigen Server schützt Ihre Daten, und anonymisiert dazu noch Ihre Adresse. Datenpakete können dann nicht mehr so einfach auf Sie zurückverfolgt werden.

Bei den meisten VPN-Diensten wie beispielweise HideMyAss und CyberGhost können Sie als zusätzliche Option beim Verbindungsaufbau das Land wählen, in dem der VPN-Server stehen soll. Wählen Sie hier Deutschland an (die Standardeinstellung ist meist „automatisch“).



Da die aufgerufenen Webseiten dann nicht Ihre IP-Adresse (die ja im Ausland liegt), sondern die des VPN-Servers sehen, ist die oben beschriebene Geoeinschränkung nicht aktiv. Die Anfrage kommt aus Deutschland, und ist damit zulässig. Dem Genuss Ihrer Lieblingsserien steht nichts mehr entgegen!

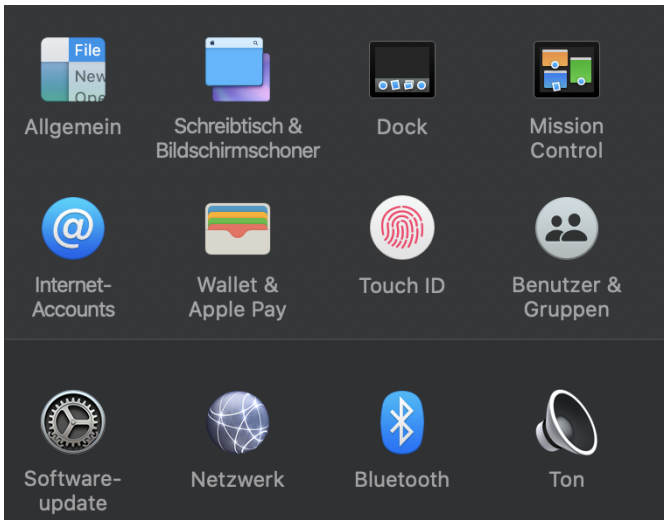
Zugriff auf Sendungen der BBC?

Das Ganze funktioniert natürlich auch anders herum: Wenn Sie aus Deutschland eine Seite der BBC (oder eines anderen Anbieters im Ausland) nutzen wollen, dann laufen sie auch hier oft auf geographische Beschränkungen. In einem solchen Fall verbinden Sie sich dann einfach mit einem VPN-Server im jeweiligen Land des Inhaltsanbieters!

Touch ID beim MacBook einrichten

Das Passwort als Anmeldemethode ist zwar bewährt, aber irgendwie auch aus der Zeit gefallen. Gestalten Sie es zu einfach, dann kann ein Fremder es erraten, ist es zu kompliziert, dann vertippen Sie sich oder vergessen es. Der einfachere Weg: eine biometrische Anmeldemethode wie der Fingerabdruck oder ein 3D-Scan des Gesichtes, wie sie bei Smartphones schon lange Standard sind. Für MacBooks mit TouchBar können Sie den Fingerabdrucksensor im Ein-/Ausschalter nutzen.

Touch ID funktioniert nur dann, wenn sie den Fingerabdrucksensor als Hardware verbaut haben. Das ist nur bei den neueren MacBook Pro (ab 2017) und MacBook Air (ab 2018) der Fall. Wechseln Sie in die Einstellungen von macOS und klicken Sie dann auf **Touch ID**.



macOS fordert nun das Auflegen des Fingers in verschiedenen Winkeln und Neigungen an, um einen möglichst guten Fingerabdruck aufzunehmen. Der Prozess der Erfassung ist ein wenig langwierig, dafür aber der der Nutzung nicht: Durch die Erfassung der Randbereiche des Fingers können Sie diesen später sorglos irgendwie auf den Sensor legen.

Wiederholen Sie die Erfassung für weitere Finger. Dann können Sie bei einer Verletzung eines erfassten Fingers trotzdem noch Touch ID nutzen.

Spielen in der Cloud: Macht das Sinn?

Spieler sind gebeutelt: Kaum kommt eine neue Spielegeneration auf den Markt, muss die Hardware aufgerüstet werden, Treiber aktualisiert werden, mal eben so spielen ist leider kaum möglich. Da kommen die Angebote namhafter Anbieter für Streaming Services ganz gelegen. Statt des eigenen High-End-PCs nutzen Sie damit Server, die der Anbieter immer auf dem aktuellen Stand hält. Aber funktioniert das auch?

NVIDIA mit GeForce Now und Google mit der Stadia-Plattform ringen momentan um die Gunst der Spieler. Für monatliche Kosten bis zu EUR 9,99 ist damit sowohl der Zugriff auf bereits gekaufte Spiele möglich als auch das Spielen von Free2Play-Spielen. Auch der Kauf in den eigenen Stores ist eine Option. Die Gebühr umfasst also in der Hauptsache das Backend.

Beide Dienste funktionieren unter den entsprechenden Bedingungen gut. Diese sind aber stark vom System des Benutzers abhängig. Dabei geht es weniger um die Rechenpower des Endgerätes: auch auf Smartphones und Tablets läuft das Spiel problemlos: Am Ende gehen ja nur die Eingaben des Benutzers an den Server, dieser sendet dann einen Stream des Bildschirminhaltes.

Genau hier aber ist Achtung geboten (und ein Test vor Abschluss eines Vertrages angeraten). Nicht nur die Internetleitung muss entsprechend schnell sein, auch das Netzwerk selbst muss fit sein: Je größer die Latenz, desto ungünstiger bei schnellen Spielen. Schon wenige

Millisekunden/Frames können dazu führen, dass sich sie Steuerung von Figur oder Vehikel unnatürlich anfühlen!

Online-Business: Was ist Dropshipping?

Früher war alles ganz einfach: Irgendwo wurden Produkte hergestellt, dann in einem Laden zum Verkauf angeboten - und gekauft. Heute ist das nicht mehr so. Durch die Digitalisierung hat sich eine Menge verändert. Es gibt auch völlig ungewöhnliche Verkaufsstrategien. Eine ist das "Dropshipping": Hier verkaufen Onlineshops Produkte, die sie gar nicht selbst auf Lager haben. Wird ein Verkauf generiert, löst das die Herstellung und/oder Auslieferung durch einen Dritten aus.

Der Käufer/Kunde merkt nichts davon, welche Dinge hinter der Kulisse vor sich gehen. Auf diese Weise lassen sich Produkte von unterschiedlichen Verkäufern online vermarkten.

Dropshipping gibt es schon länger. Aber die Art und Weise, wie diese Form der Vermarktung und des Verkaufs betrieben wird, hat sich doch stark verändert.

Doch ein Selbstläufer ist das Geschäftsmodell mit Sicherheit nicht. Es gibt nach wie vor viele angehende Unternehmer, die mit ihrem Vorhaben mit Dropshipping erfolgreich zu sein scheitern. Nur die wenigsten schaffen es wirklich einen Dropshipping-Onlineshop mit Zukunftspotential aufzubauen. Oft liegt das allerdings daran, dass sie einige grundlegende Dinge außer Acht lassen. Schauen wir uns daher an, worauf es beim Aufbau zu achten gilt.

Wahl eines Shopsystems

Wer mit Dropshipping Geld verdienen möchte, baut dafür in der Regel einen Online-Shop auf. Einen solchen zu programmieren oder mittels WordPress aufzubauen ist jedoch sehr aufwendig und nimmt viel Zeit in Anspruch. Außerdem ist es schwer, die erforderlichen Funktionen eines Online-Shops zu integrieren.

Allerdings gibt es Shopsysteme wie Shopify, die Abhilfe schaffen können. Der Vorteil von solchen Shopsystemen ist, dass sie den Aufbau eines Online-Shops um einiges erleichtern. Neben zahlreichen Templates gibt es verschiedene Elemente, die mittels Drag-and-Drop in den eigenen Online-Shop eingebaut werden können. Außerdem werden unterschiedliche Geschäftsprozesse seitens des Shopsystems übernommen. Unternehmer sollten also gleich zu Beginn entscheiden, auf welches Shopsystem sie sich festlegen.

Produkte mit Potential

Beim Dropshipping haben Entrepeneure viele Freiheiten. So können sie beispielsweise aus einer breiten Palette an Produkten wählen und im Prinzip alles in ihrem Online-Shop anbieten, was sie möchten. Einschränkungen gibt es praktisch keine. Schließlich verursacht eine Anpassung oder Erweiterung des Sortiments keine Kosten. Das bedeutet jedoch nicht, dass die Wahl der Produkte nicht wichtig ist. Die Produkte sollten ein gewisses Potential haben und auf eine bestimmte Zielgruppe zugeschnitten sein.

Am besten sind die Produkte möglichst nischig, um einen harten Konkurrenzkampf zu vermeiden. Wer sein Sortiment ohne Überlegungen zusammenstellt, wird dabei in der Regel keinen Erfolg haben. Der eigene Online-Shop sollte sich von der Masse abheben. Das ist leider gar nicht so einfach. Wer mit dem Business Erfolg haben möchte, sollte sich jedoch gut überlegen, was für Produkte er in seinem Dropshipping-Onlineshop eigentlich verkaufen möchte.

Zuverlässige Lieferanten

Dropshipping-Shopbetreiber haben nur einen bedingten Einfluss auf die Geschäftsprozesse eines Unternehmens. Die meisten Prozesse des Business werden nämlich von den Lieferanten abgewickelt. Das wiederum bedeutet, dass der Erfolg zu einem großen Teil von der Arbeit und den Produkten der Lieferanten abhängt. Beides sollte also passen, um Schwierigkeiten mit den Kunden zu vermeiden. Problematisch sind beispielsweise Lieferanten, die minderwertige Ware liefern oder sich zu viel Zeit für den Versand lassen.

Im Bereich des Dropshipping ist so etwas jedoch gar nicht so selten. Entrepreneure sollten also unbedingt darauf achten, dass sie ausschließlich mit zuverlässigen Lieferanten zusammenarbeiten. Solche auszumachen, kann gerade am Anfang schwierig sein. Es lohnt sich jedoch, die erforderliche Arbeit dafür zu investieren. Denn zuverlässige Lieferanten sind beim Dropshipping die halbe Miete.

Apple Airpods Pro am Mac nutzen

Kopfhörer können nicht nur zum Musikhören verwendet werden, sondern auch zu anderen Dingen. Je ausgeklügelter sie sind, desto mehr Funktionen haben sie. Das gilt auch für die AirPods Pro von Apple. Die haben sogar so viele Funktionen, dass manche sich in iOS gut verstecken. Weniger bekannt: Wenn sie einmal mit einem Gerät gekoppelt sind, das mit Ihrer Apple ID eingerichtet ist, den können Sie sie direkt auch am Mac nutzen, solange dieser Catalina (macOS 10.15.x) installiert hat!

Schalten Sie die AirPods Pro ein, wenn Sie in der Nähe des Macs sind. Dann klicken Sie mit der Maus oben auf das Symbol für die Lautstärke. Das finden Sie nicht? Unter **Einstellungen** > **Ton** können Sie einen Haken neben **Lautstärke in der Menüleiste anzeigen** setzen. Dann erscheint das Lautsprecher-Symbol, und dort finden Sie neben den internen Lautsprechern des Mac auch die Airpods und können Sie als Ausgabegerät anwählen.

Die komplette Klangausgabe des Mac wird damit auf die AirPods Pro umgeleitet. Und damit nicht genug: Auch die komplette Konfiguration der Funktionen der AirPods Pro können Sie am Mac machen. Dazu müssen Sie in die Bluetooth-Einstellungen wechseln und dort die AirPods Pro auswählen.

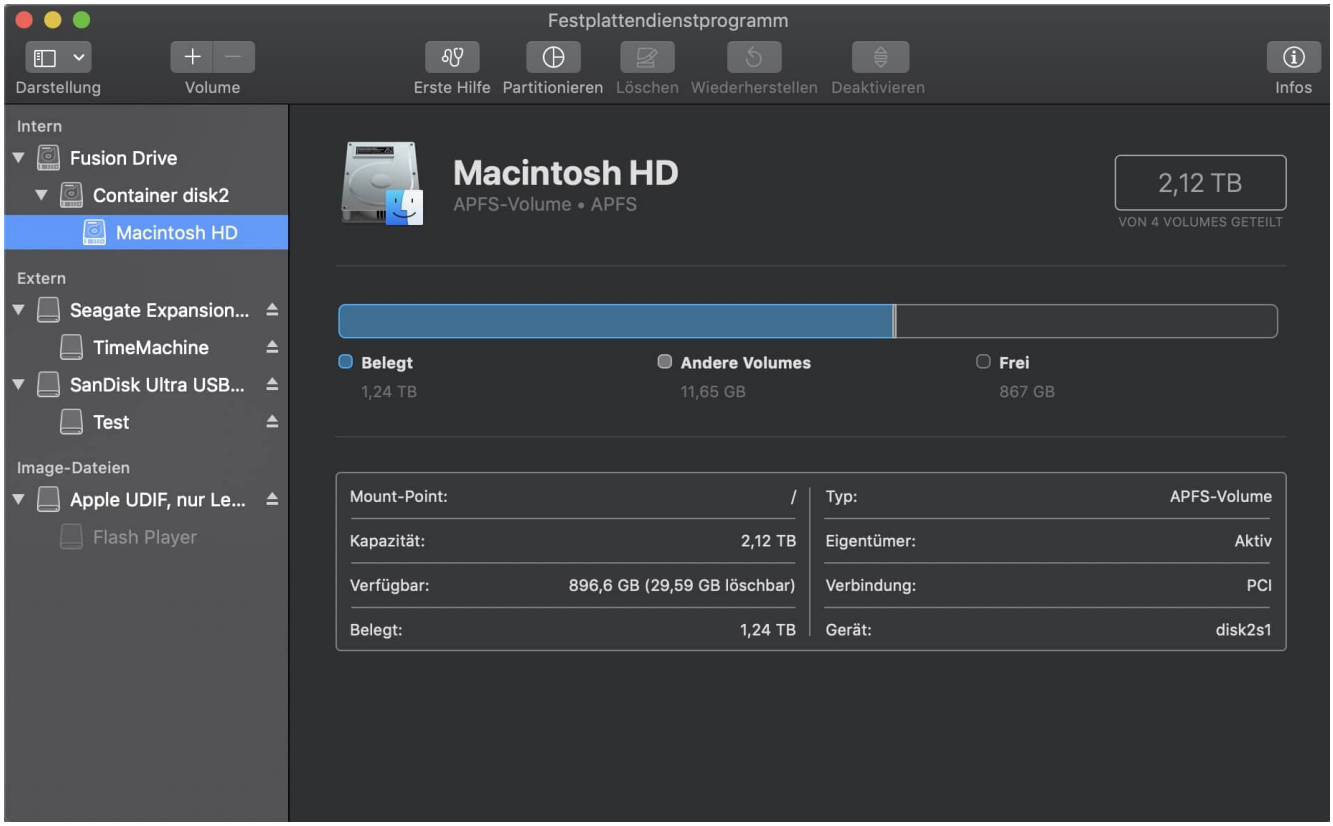
Legen Sie hier die Funktion der Tasten der beiden AirPods fest, das Verhalten des Mikrofons und aktivieren Sie die automatische Ohrerkennung.

Verschlüsseln externer Datenträger bei macOS

Oft ist die Quelle eines Datenlecks gar nicht mal der eigene PC oder ein Netzwerk, auf das Sie zugreifen. In vielen Fällen geht einfach ein Datenträger verloren, der ungeschützt ist. So klein und portabel sind Festplatten. SSDs und USB-Sticks geworden, dass man sie immer dabei hat und immer weniger darauf achtet. Auch bei macOS können Sie hier mit Bordmitteln vorsorgen!

Bei Windows haben Sie es einfach: Neben der integrierten Festplattenverschlüsselung Bitlocker können Sie mit BitlockerToGo auch externe Datenträger - egal welchen Formats - verschlüsseln und die Daten für den Unberechtigten unleserlich machen. Bei macOS ist das Ganze mit Bordmitteln ein wenig schwieriger. Allerdings nicht unmöglich.

Wichtig ist, dass der Datenträger im richtigen Format formatiert ist. Wenn das noch nicht der Fall ist, müssen Sie ihn umformatieren. Sind schon Daten darauf, dann kopieren Sie diese vorher auf einen anderen Speicherort. Starten Sie dann das Festplattendienstprogramm von macOS.



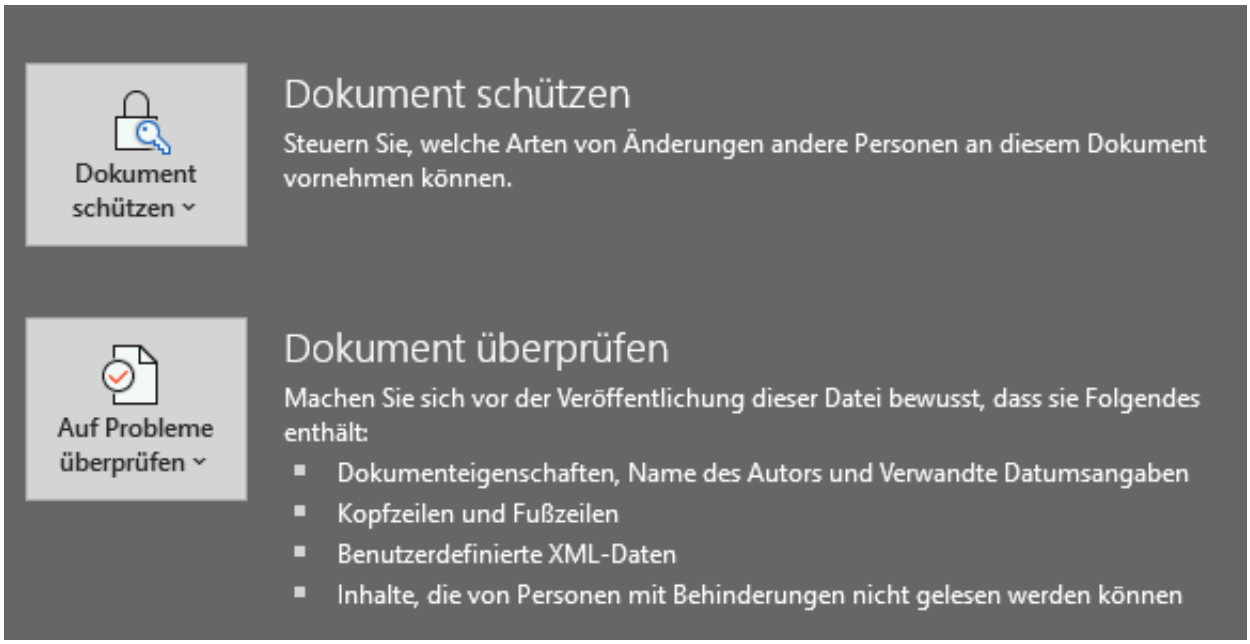
Wählen Sie den Datenträger (nicht das darauf angelegte Volume!) aus und klicken Sie auf **Löschen**. Als Format wählen Sie **Mac OS Extended (Journaled)** und als Schema **GUID-Partitionstabelle**. Wenn Sie das Schema nicht angezeigt bekommen, dann kontrollieren Sie, ob sie wirklich das Laufwerk (und nicht das darunter angezeigte Volume) angeklickt haben.

Ein Klick auf **Löschen** formatiert den Datenträger neu und verschlüsselbar. Jetzt können Sie mit der rechten Maustaste im Finder auf das Laufwerk klicken und **Verschlüsseln** auswählen. Geben Sie Ihr Wunschpasswort zweimal identisch ein, und der Datenträger ist (auf anderen Geräten mit macOS) nur nach Eingabe des Passworts lesbar. Für Windows allerdings bleibt ein so verschlüsselter Datenträger nur Bitbrei.

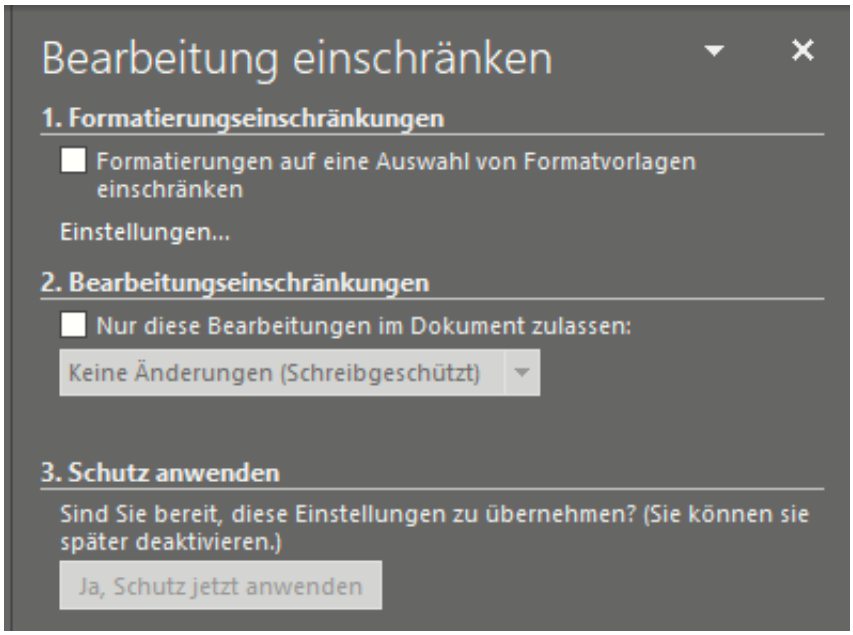
Dokumentschutz in Word

Zusammenarbeit mit Office ist toll: Je mehr Personen an einem Dokument arbeiten, desto besser ist potenziell der Inhalt. Allerdings kann es vorkommen, dass Sie eben nur die Inhalte, nicht aber die Formatierung verändern lassen wollen. Oder vielleicht gar keine Bearbeitung zulassen wollen. Verzichten Sie auf manuelle Anweisungen und schützen Sie das Dokument direkt in Word!

Dazu öffnen Sie das Dokument und klicken dann auf **Datei** > **Informationen** > **Dokument schützen**. In älteren Office-Versionen liegt die Funktion übrigens direkt unter Datei. Unter **Zugriff einschränken** können Sie nun festlegen, welche Berechtigungen der Anwender haben soll. Je vertraulicher die Einstellung, desto weniger können die Anwender mit dem Dokument machen. So können Sie zum Beispiel das Verändern oder das Drucken komplett verbieten.



Wenn Sie eine Bearbeitung zulassen möchten, aber das Dokument zumindest in der richtigen Formatierung halten wollen, dann klicken Sie unter **Dokument schützen** auf **Bearbeitung einschränken**. Ein Klick auf **Formatierungen auf eine Auswahl von Formatvorlagen einschränken** erlaubt es Ihnen, ganz fein auszuwählen, welche Formatierungen der Benutzer vornehmen darf.



Unter **Bearbeitungseinschränkungen** können Sie festlegen, ob er das Dokument komplett überarbeiten darf, nur Kommentare eingeben oder Formulare einschränken darf. Wollen Sie nichts davon, dann wählen Sie **Keine Änderungen (schreibgeschützt)**.

Tabellen aus einer PDF-Datei in Excel bekommen

Das PDF-Format ist weit verbreitet und hilft, zwischen Geräten und Betriebssystemen ohne besondere Softwareanforderungen Dokumente auszutauschen. Die Herausforderung besteht oft darin, die Daten darin wieder in eine bearbeitbare Form zu bekommen. Mit Tricks geht das auch bei Tabellen!

Wenn Sie die kostenpflichtige Version der PDF-Software Acrobat DC von Adobe einsetzen, dann ist das Leben einfach: Klicken Sie auf **PDF-Datei exportieren** > **Arbeitsblatt** > **Microsoft Excel-Arbeitsmappe**. Ein Klick auf Exportieren überführt die Daten in eine Excel-Tabelle. Diese können Sie dann unter einem frei wählbaren Namen speichern und in Excel normal bearbeiten.

Komplizierter wird es, wenn Sie nur die kostenlosen Adobe-Tools nutzen. Hier ist es wichtig, dass die PDF-Datei aus einer Excel-Tabelle erzeugt wurde und nicht aus einem Scan. Dann nämlich lässt sich der Textteil der Tabelle nicht so einfach extrahieren.

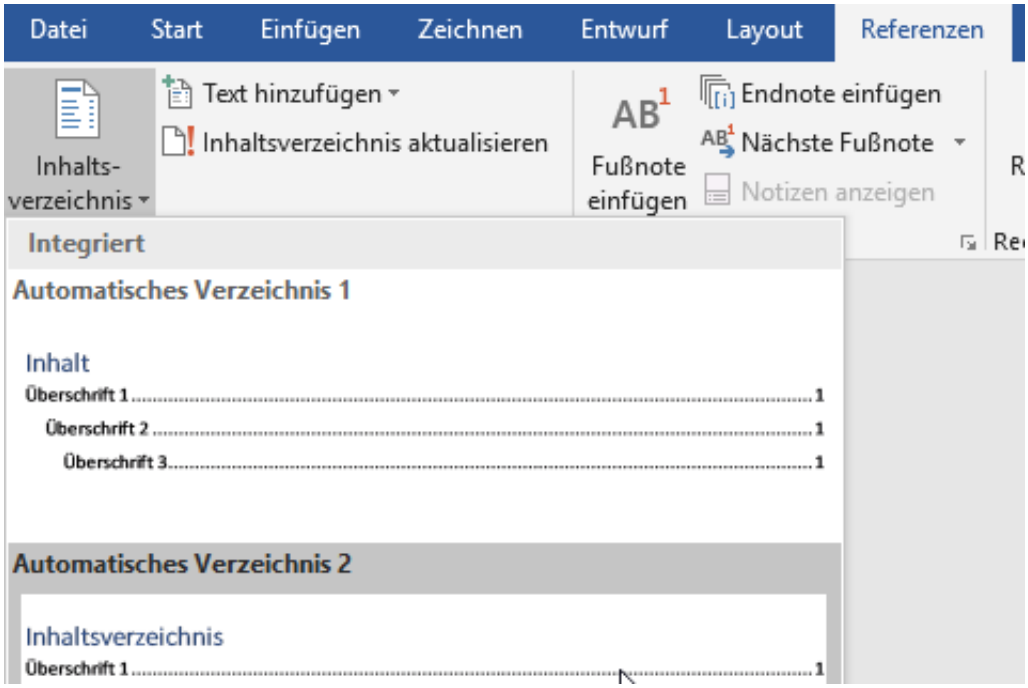
Die Lösung: Klicken Sie mit der rechten Maustaste auf die PDF-Datei, dann **Öffnen mit** > **Microsoft Word**. Word wandelt die Excel-Tabelle nun in ein Word-Dokument um, das unter anderem auch die Tabelle enthält. Dieses speichern Sie jetzt nicht als .DOCX, sondern als .TXT-Datei.

Diese Textdatei können Sie jetzt unter **Datei** > **Öffnen** > **Durchsuchen** öffnen, wenn Sie unten rechts auf **Alle Dateien (.)** klicken. Wie Sie eine Textdatei formatiert in die Spalten von Excel bekommen, haben wir Ihnen hier zusammengeschrieben.

Inhaltsverzeichnis in Word verwenden

Ein Text ist der Kern eines Word-Dokumentes. Um der Leserschaft aber einen einfacheren Überblick darüber zu geben, was wirklich wichtig ist, können Sie Verzeichnisse anlegen. Wenn Sie die einzelnen Verzeichnistypen klug einsetzen, ist der Aufwand minimal und der Effekt immens. Das Inhaltsverzeichnis ist hier eine große Hilfe!

Das bekannteste Verzeichnis in Word ist das Inhaltsverzeichnis. Die Einträge legen Sie fest, indem Sie unter Start > Formatvorlagen eine der Überschrift-Formatierungen vergeben. Die Ebene der Überschrift legt die Position im Inhaltsverzeichnis fest.



Über **Referenzen** > **Inhaltsverzeichnis** können Sie das automatisch generierte Inhaltsverzeichnis einfügen und dessen Layout auswählen. Klicken Sie mit der rechten Maustaste in ein bestehendes Inhaltsverzeichnis und dann auf Aktualisieren, dann fügt Word alle geänderten und neuen Einträge hinzu. Sie haben die Wahl, ob Sie nur die bestehenden Einträge aktualisieren wollen (weil sich beispielsweise die Seitenzahlen der Inhalte verschoben haben) oder das Verzeichnis neu einfügen wollen. Im letzteren Fall werden dann auch neue Einträge hinzugefügt.

Versteckt können Sie aber Einträge im Inhaltsverzeichnis frei bestimmen, ohne manuell eine Überschriften-Vorlage anzuwenden. Markieren Sie einen Text, dann klicken Sie auf Referenzen > Text hinzufügen und wählen dann die Ebene aus. Die Zeile, die im markierten Text liegt, wird in der gewählten Ebene in das Inhaltsverzeichnis aufgenommen.

Verschwörungstheorien Corona

Corona, Corona, Corona: Die Medien sind voll davon. Das Netz natürlich auch. Doch während sich professionelle Redaktionen darum bemühen, Panik zu vermeiden und seriöse von unseriösen Meldungen und Nachrichten zu unterscheiden, landet im Netz alles – einfach so. Niemand kontrolliert es. So gibt es viele Horrorgeschichten und auch Verschwörungstheorien, die Panik erzeugen können. Oder es werden Heilmittelchen vorgestellt, etwa Essig ins Nasenloch, die vor einer Infektion schützen sollen. Auch purer Unsinn. Damit sind viele Infos im Netz – ja: saugefährlich.

Verschwörungstheorien gibt es viele – und schon immer. Eigentlich wollen einige Netzwerke wie YouTube dagegen vorgehen. Aber: Es gibt auch Verschwörungstheorien rund um Corona.

Ein Video aus Kalifornien zeigt frisch aufgestellte 5G-Sendemasten. Daneben eine Schule. Und auch das Gebäude eines Pharmazie-Unternehmens. Die Macher des Videos stellen unverfroren eine Verbindung her: 5G macht krank, erzeugt quasi die Corona-Infektion in Menschen – von Mächten choreographiert. Damit die Medizin-Industrie gut verdient.

Der vermeintliche Beweis: In Wuhan hätte das 5G-Netzwerk gestartet – und wenige Tage später wäre da dann Corona ausgebrochen. Nicht wegen Tieren, die auf engstem Raum zusammengepfercht werden, sondern wegen der 5G-Masten. Klar.

Es gibt viele weitere Beispiele: Die Corona-Epidemie offenbare das "Dunkle in uns" und lasse sich – klar! – mit der Saturn-Pluto-Konjunktion erklären. Oder geheime Biowaffenlabors hätten das Virus entwickelt – und es wäre ausgesetzt worden, um richtig viel Geld zu verdienen.

Die Plattformen machen zu wenig

Eigentlich müsste doch jeder mit gesundem Menschenverstand wissen: Das ist bodenloser Schwachsinn. Aber was tun Google, Facebook, Twitter und Co?

Leider wirken solche Verschwörungsvideos doch ziemlich gut. Sie passen perfekt in die Erregungsökonomie der Sozialen Netzwerke. Aufreger: Super, wird angeklickt, empfohlen, macht die große Runde. Natürlich schaden solche Falschmeldungen enorm. Sie verunsichern, verwirren, verursachen Panik. Nun haben sich alle Netzwerke bereit erklärt, gegen Verschwörungsvideos, Falschmeldungen und Panikmache vorzugehen.

Aber nach meiner Beobachtung geschieht das eher zurückhaltend. So ist es kein Problem, auf Youtube das Verschwörungsvideo zum Thema "5G ist schuld" zu finden. Es gibt lediglich einen Hinweis auf die Bundeszentrale für gesundheitliche Aufklärung. Das war's. Facebook und Twitter entfernen auch Postings. Aber auch nur, weil die WHO ihnen besonders auffällige Postings und Nachrichten meldet. Die WHO macht also die Arbeit. Wirkliches Engagement sieht meiner Ansicht nach anders aus.

Die Plattformen machen zu wenig

Also schwierig. Wer sich im Netz informieren möchte, kann das – aber es gibt eben auch viele schädliche und falsche Informationen.

Ein großes Problem. Auch seriöse Medien machen Fehler – aber sie geben sich alle Mühe, Fakten zu prüfen, Panik zu vermeiden, besprechen den Zungenschlag von Artikeln und Beiträge. Im Netz kann aber jeder einfach alles online stellen – demokratisch eben. Und das ist in solchen Zeiten in meinen Augen ein riesiges Problem.

Was nutzt ein kleiner Hinweis auf Facebook oder Youtube, dass man sich doch bei WHO oder Bundeszentrale für gesundheitliche Aufklärung informieren kann oder soll – dezent in grau, während alles andere knallbunt ist? Das ist ein Witz!

So könnte es besser gehen

Meiner Ansicht nach müssten alle unsinnigen Beiträge sofort entfernt werden. Es gibt zum Beispiel auch zahlreiche "Tipps", wie man sich mit Hausmitteln gegen Corona schützen kann. Etwa durch den Genuss von Knoblauch – oder indem man sich eine selbst angerührte Essiglösung in die Nasenlöcher träufelt. So etwas kann Leben kosten. Und die Netzwerke entfernen nur, was die WHO findet und meldet.

Unerträglich! Es ist das übliche Problem: Die Netzwerke müssten ihre Verantwortung ernst nehmen. Sie wehren sich ja mit Händen und Füßen dagegen, als Medium wahrgenommen zu werden. Das zeigt aber wieder, wie wichtig seriöse Medien sind.

Beim Thema Corona ist es um so wichtiger, sich seriös zu informieren, ÖR-Sender, Spiegel, Zeit, Welt, große Magazine und Zeitungen. Und natürlich die Behörden. Alles andere sollten wir mir aller größter Skepsis betrachten.

Corona: Auch das Netz verträgt eine Portion Desinfektion

Es ist abstoßend: Immer wieder, wenn eine Krise die Medien beherrscht, nutzen Cyberkriminelle und windige Geschäftemacher ihre Chance - und missbrauchen die öffentliche Aufmerksamkeit, um windige Geschäfte zu machen oder sogar zu betrügen. Die großen Netzwerke gehen nur zaghaft dagegen vor.

Corona - ein Schlagwort, das die Medien derzeit dominiert. Wahrscheinlich zu Recht. Denn niemand kann sagen, wie sich die Epidemie weiter entwickelt. Die Menschen wollen eine Einordnung, brauchen Hilfe, müssen sich organisieren.

Leider missbrauchen viele die aktuell hohe Aufmerksamkeit - und versuchen, mit Corona Geld zu machen. Oder einfach nur Angst und Schrecken zu verbreiten.

Kettenbriefe, Phishing-Attacken, Wucher-Angebote

Im Netz geistern zum Beispiel unzählige Postings und auch Videos herum, die völlig haltlose Verschwörungstheorien verbreiten. Manche versprechen etwa, dass wir durch den Genuss von Knoblauch das Ansteckungsrisiko verringern könnten. Fahrlässig! Andere versuchen, gezielt Panik zu verbreiten, indem sie behaupten, Corona wäre in einem Gen-Labor entwickelt worden - und es würde seine Schlagkraft erst noch entfalten.

Wieder andere - davor warnt zum Beispiel die Sicherheitsfirma Sophos - versuchen, mit gezielten Phishing-Attacken an die sensiblen Daten der Userinnen und User zu kommen. Manche Mails kommen vermeintlich von der Gesundheitsorganisation WHO, andere aus dem Bundeskanzleramt oder dem Gesundheitsministerium. Sie alle wollen: Entweder phishen oder Schad-Software auf dem Rechner oder Smartphone einschleusen.

Die Täterinnen und Täter gehen laut Sophos "perfide vor und sind skrupellos". Allerdings.

Wieder andere versuchen, mit der Panik Geld zu machen. Indem sie für Unsummen Masken oder Desinfektionsmittel verkaufen. Oft zu einem 10-fachen des ursprünglichen Preises. Beutelschneiderei!

Den Schrecken eindämmen: Haltloser Unsinn im Umlauf

Da zeigt sich mal wieder, wie wichtig seriöse und verlässliche Informationsquellen sind. Immerhin unternehmen Konzerne wie Google, Facebook und sogar Tiktok etwas, um die Falschinformationen einzudämmen. Allerdings erst auf Drängen der WHO. Sie hat am Montag erklärt, dass WHO-Mitarbeiter rund um die Uhr nach Falschinformationen im Netz fahnden und die Plattformen darüber informieren.

Die nehmen besonders verstörende Desinformationen aus dem Netz oder verweisen auf die WHO. Die wiederum hat sogar selbst einen Account auf TikTok eröffnet.

Ich finde: Die Plattformen sollten sich ihrer Verantwortung bewusst werden. Sie sollten mit aller Macht - koste es, was es wolle - verstörende, falsche, intrigante, verwirrende, Angst machende und schlicht falsche Texte, Fotos und Videos verbannen. Sofort. Und die Konten sperren.

eBay hat vorgemacht, wie es geht: eBay löscht kurzerhand alle(!) Angebote, die sich auf Corona beziehen. Denn es ist sowieso klar, dass hier nur windige Geschäftemacher unterwegs sind.

So könnten Google und Facebook bei Corona helfen

Ungewöhnliche Situationen verlangen nach ungewöhnlichen Lösungen. Warum sollten wir es uns nicht mal zunutze machen, dass Google, Apple und Facebook uns rund um die Uhr überwachen? Die drei Anbieter zusammen könnten im Sekundenbruchteil die Frage beantworten, wer auf einer Veranstaltung war - und so die Fahndung nach Corona-Kontakten erleichtern.

Der Coronavirus sorgt für Aufregung und Verunsicherung. Das ist verständlich - denn wer möchte sich schon mit Covis-19 infizieren? In Südkorea nutzen die Behörden die Digitalisierung für sich. Sie verwenden eine Warn-App, die vor Kälte oder schlechter Luft warnt, um auch vor Orten mit Corona-Kontakten zu warnen.

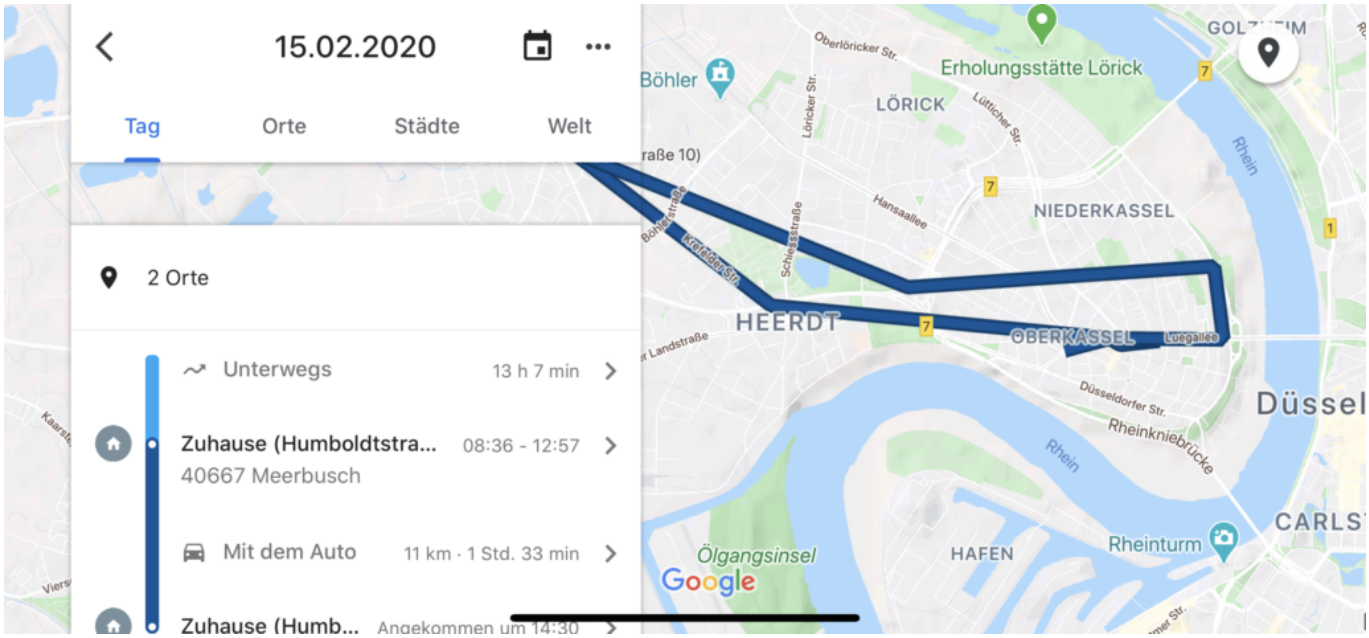
Diese Geschichte hat mich auf eine Idee gebracht - datenschutzrechtlich zweifellos bedenklich. Aber doch einen Gedanken wert. Verwerfen geht ja immer noch...

Wir wissen, dass insbesondere Google und Facebook uns besser kennen als wir selbst. Vor allem, was unsere Gewohnheiten und Bewegungsprofile anbelangt.

Google, Facebook und Apple könnten Suchen helfen

Theoretisch denkbar und technisch zweifellos machbar wäre es doch, mit Hilfe der Datenbestände von Google und Facebook zu ermitteln, wer zum Beispiel auf einer bestimmten Karnevalsveranstaltung gewesen ist - dann müssten die Behörden nicht wochenlang fahnden. Google und Facebook könnten vermutlich blitzschnell sagen, wer alles da war.

Selbst die zurückliegenden Kontakte ließen sich ermitteln. Wer seine Wohnung verlässt, beim Bäcker einkauft, an der Theke einen Espresso trinkt, ein paar Minuten mit der Nachbarin oder Freunden plaudert und/oder mit dem Bus fährt, lässt sich doch alles mühelos ermitteln. Auf diese Weise könnten auch alle anderen Personen ermittelt werden, die sich in der Nähe befunden haben.



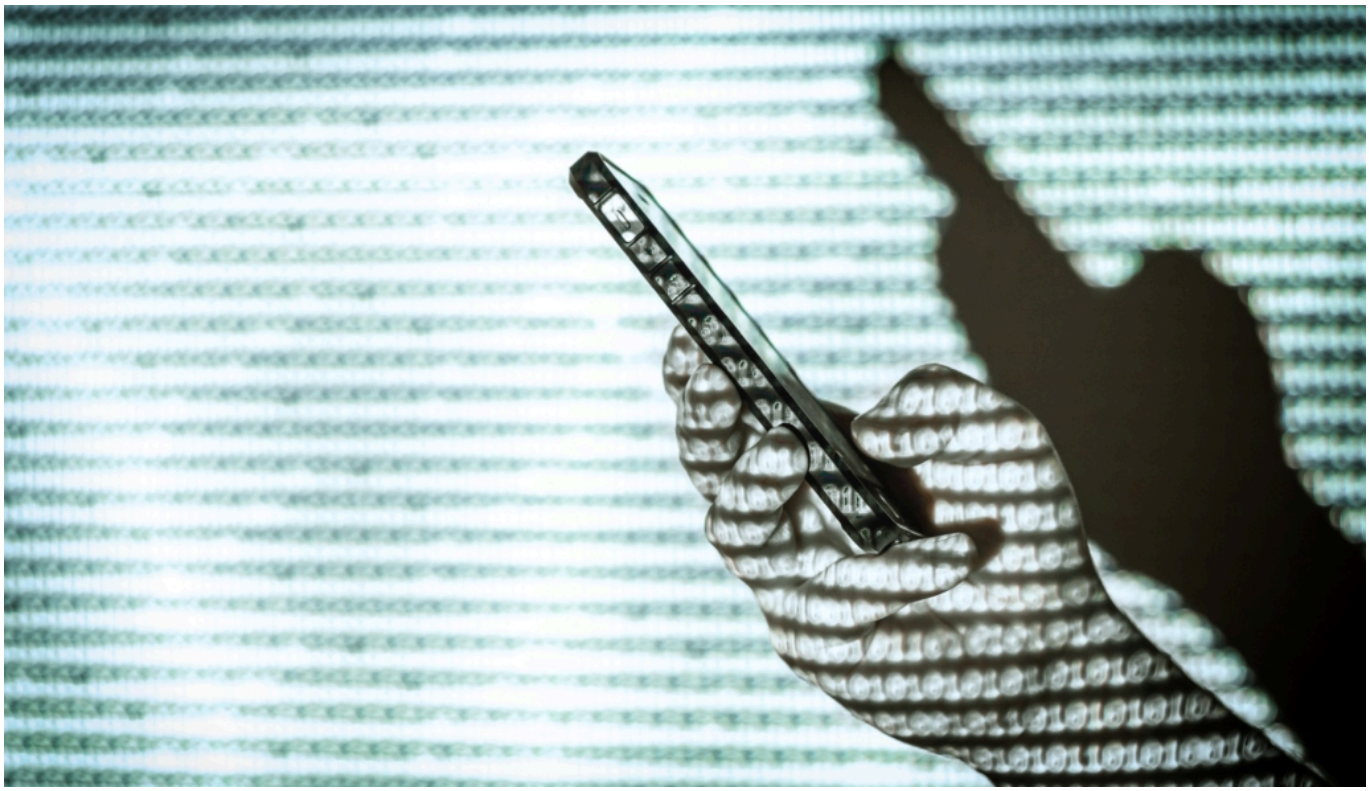
Schneller Kontaktpersonen finden

Es ist also vor allem eine Frage der Fragestellung, was am Ende dabei herauskommt. Aber für Google und Facebook, die uns lückenlos überwachen (sorry: auf Schritt und Tritt begleiten), wäre es nicht sonderlich schwer, solche Fragen zu beantworten.

Wie viele Personen haben am 28.02. abends um 18.00 Uhr am Yoga-Kurs von Isabella in Kalk teilgenommen? 27 sagt Google., 26 meint Facebook. Wer? Hier ist die Liste... Genauso einfach ließen sich auch nahezu alle anderen Kontakt ermitteln.

Zwar hat nicht jeder ein Smartphone in der Tasche oder eine Smartwatch am Arm, aber doch nahezu keder. 90% sagt die Statistik.

Wäre das nicht ein geeignetes, hilfreiches Instrument, um die am Rand ihrer Leistungsfähigkeit befindlichen Gesundheitsämter zu unterstützen und zu entlasten?



Datenschutz bedenken

Natürlich: Es gibt da auch eine Menge zu beachten und zu diskutieren. Denn aus Sicht des Datenschutz ist eine soche Analyse genau das, was verhindert werden soll. Aber schwierige Situationen erfordern auch ungewöhnliche Maßnahmen. Schließlich gibt es auch wenig gute Gründe, Menschen 14 Tage in ihrer Wohnung festzusetzen. Doch das Seuchenschutzgesetz macht es möglich.

Vorsicht bei GooglePay mit PayPal

Mit dem Smartphone oder mit Smartwatch bezahlen: Mittlerweile machen das viele Menschen gerne - denn es ist bequem, einfach und bietet eine Menge Vorteioe. Auch für Händler und Zahlungsempänger. Normalerweise ist Mobile Payment sehr sicher. Doch aktuell gibt es Probleme bei Google Pay mit PayPal.

Mobile Payment ist eine feine Sache - wenn man 's mag. Ob kleine oder große Beträge: Einfach Smartphone zücken, Kredit- oder EC-Karte auswählen, ans Terminal halten - fertig. Selbst die PIN-Eingabe entfällt, weil das Smartphone ja ohnehin abgesichert ist.

Auch mit der Apple Watch kann man auf diese Weise bequem bezahlen. Das geht schneller als Bargeld und auch schneller als mit einer Plastikarte. Außerdem fließen praktisch keine Daten an den jeweiligen Händler. Feine Sache also.

Unautorisierte Abbuchungen - teilweise 4-stellig

Derzeit werden Mobile-Payment-Fans aber aufgeschreckt: Viele haben unautorisierte Belastungen erhalten. Von einem Kaufhaus "Target" aus den USA - oder von Händlern mit Quatschnamen.

Viele Belastungen drei-, manche sogar vierstellig. Das Problem: PayPal erzeugt - wie auch andere Banken - virtuelle Kreditkarten. Allerdings macht es PayPal Betrügern sehr einfach: Die Kreditkartendaten sind leicht zu erraten. Und: PayPal überprüft keine zusätzlichen Daten wie CVC (Kontrollcode), Ablaufdatum, Name oder Sicherheitscode neben dem Unterschriftfeld. Das öffnet Betrügern Tür und Tor.

Allerdings gibt es das Problem nur in Kombination Google Pay und PayPal. Was noch bedenklicher ist: Das Leck ist seit über einem Jahr bekannt. Ein deutscher Entwickler hat das Problem gefunden, es bei PayPal gemeldet und dafür sogar eine Prämie (Bug Bounty) erhalten - aber geschlossen wurde das Leck offensichtlich bis heute nicht.

Markus Fenske, CEO beim Sicherheitsunternehmen exablue, dessen Mitarbeiter Andreas Mayer die Lücke vor einem Jahr entdeckt hat, beschreibt den so genannten Angriffsvektor auf Twitter so:

> Um NFC-Zahlungen zu ermöglichen, generiert die PayPal-App eine virtuelle Kreditkarte. Anders als bei anderen Anbietern kann über diese Karte aber nicht nur eine Zahlung im Einzelhandel autorisiert werden, sondern auch eine Zahlung im Online-Handel. Und in diesem Fall verlangt PayPal lediglich nach Angabe der Kartennummer sowie des Ablaufdatums.

Sicherheit muss unbedingt besser werden

Zwar können sich betroffene Kunden an PayPal wenden und bekommen ihr Geld zurück. Doch ist das trotzdem kein Zustand: In einem sensiblen Bereich wie Mobile Payment derart fahrlässig und nachlässig zu sein, ist unentschuldbar. Sicherheitsexperte Jan Felix Wiebe kritisiert PayPal für diese Schlampigkeit in einem Interview (siehe Video). Zu Recht. Denn spätestens, wenn ein Leck bekannt ist, sollte es doch schleunigst geschlossen werden.

Natürlich hätte auch Google Pay reagieren und PayPal zeitweise ausschließen können. Das alles lässt den Eindruck entstehen, dass Mobile Payment unsicher sei. Normalerweise ist das nicht der Fall. Mobile Payment liefert den Händlern zum Beispiel weniger Daten als bei einer Zahlung mit Kreditkarte. Vor allem Apple Pay macht hier einen guten Job. Und weil Apple auch keine Geschäfte mit Nutzerdaten macht, scheint es derzeit das überlegene Payment-Verfahren zu sein.

Wie wär's mit einer Art TÜV für Zahlungsdienste? Verbockt ein Anbieter relevante Sicherheitsaspekte auf eklatante Weise - wie im aktuellen Fall -, sollten hohe Strafen drohen. Oder Entzug der Lizenz für einige Wochen. Wenn derartiges droht, würden sich die Anbieter mehr anstrengen.

EU-Kommission will verstärkt Signal Messenger einsetzen

WhatsApp ist mit seinen mittlerweile 2 Milliarden Nutzern weltweit der mit Abstand populärste Messenger. Alternativen wie Signal, Threema oder Telegram haben es da nicht leicht, sich gegen das Schwergewicht durchzusetzen. Das gilt nicht nur für uns Privatleute, sondern auch für Behörden – und sogar die hohe Politik, etwa in der EU. Auch hier wird vor allem WhatsApp eingesetzt. Und das wird zunehmend als Sicherheitsrisiko gesehen.

WhatsApp gehört ja zu Facebook und Facebook gilt nun wirklich nicht als besonders vertrauenswürdig. Und trotzdem setzen Politiker und Diplomaten WhatsApp ein?

Den Politikern geht es da genau wie uns: Sie haben WhatsApp, sie kennen WhatsApp – und da ist es naheliegend und vor allem super bequem, per WhatsApp zu kommunizieren. Das Argument: WhatsApp ist verschlüsselt. Also werden WhatsApp-Gruppen angelegt, für jedes Ressort, für jedes Thema, für jede Arbeitsgruppe – und fleißig kommuniziert. Weitgehend ohne schlechtes Gewissen. Der britische Guardien nennt das: „The rise and rise of international Diplomacy bei WhatsApp“, also den Aufstieg der internationalen WhatsApp-Diplomatie.

In der EU regt sich Widerstand

Doch jetzt regt sich Widerstand in der EU. Experten raten dazu, andere Messenger zu nutzen.

Es gibt eine lange Liste von Problemem die Grund dafür sind. Nachrichten werden zwar automatisch ziemlich gut verschlüsselt. Doch in letzter Zeit hat es einige Sicherheitslücken in WhatsApp gegeben. Natürlich stürzen sich Hacker am liebsten auf eine Software, die zwei Milliarden Menschen nutzen. Also finden sich da auch mehr Sicherheitslecks. Wir erinnern uns an den Fall Saudi-Arabien und Amazon-Chef Jeff Bezos: Da wurde ein Sicherheitsleck ausgenutzt, um Bezos auszuspionieren.

Dann gab es gerade die Cryptoleaks-Enthüllungen. Sie zeigen, dass USA und Deutschland seit Jahren die verschlüsselte Kommunikation belauschen. Und selbst wenn man etwas heute noch nicht knacken kann: Die Quantencomputer stehen in den Startlöchern, mit denen das dann gehen wird. Dann lässt sich auf Vorrat gespeicherte Kommunikation dann möglicherweise doch entschlüsseln, irgendwann. Auch die NSA mischt da mit. Es gibt also genügend berechtigte Zweifel, dass WhatsApp für Europäer ein verlässlicher Dienst ist – schließlich wird Facebook alles tun, was US-Behörden verlangen.

EU-Experten empfehlen Signal

Nun gibt es eine interne Notiz einer Expertengruppe in der EU, die ausdrücklich einen anderen Messenger empfiehlt: Signal.

Signal sei die sichere Alternative, heißt es in der Notiz, die netzpolitik.org vorliegt. Daraus wurde eine Empfehlung, die an alle Mitarbeiter verschickt wurde. Es kommt also etwas in Bewegung. Noch gibt es keine Verpflichtung, auf WhatsApp zu verzichten. Aber möglicherweise ist das der nächste Schritt. Noch darf WhatsApp aber eingesetzt werden.

Probem: Metadaten

Ein Problem, das angesprochen wird, sind die sogenannten Metadaten.

Bei den Metadaten handelt es sich um Angaben über Sender und Empfänger, Zeit und Datum sowie Nachrichtengröße. Aus den Metadaten lässt sich ablesen, wer mit wem kommuniziert. Durch die Dateigröße lassen sich Rückschlüsse treffen, ob etwa Bilder oder Videos mitgeschickt wurden. All das speichert Facebook – und weiß daher eine Menge. Außerdem kann Facebook das Telefonbuch auslesen. Signal hingegen speichert nach eigenen Angaben möglichst wenige Informationen über Nutzer:innen. Der Dienst verschlüsselt Metadaten und löscht sie von seinen Servern, sobald die Nachricht verschickt ist.

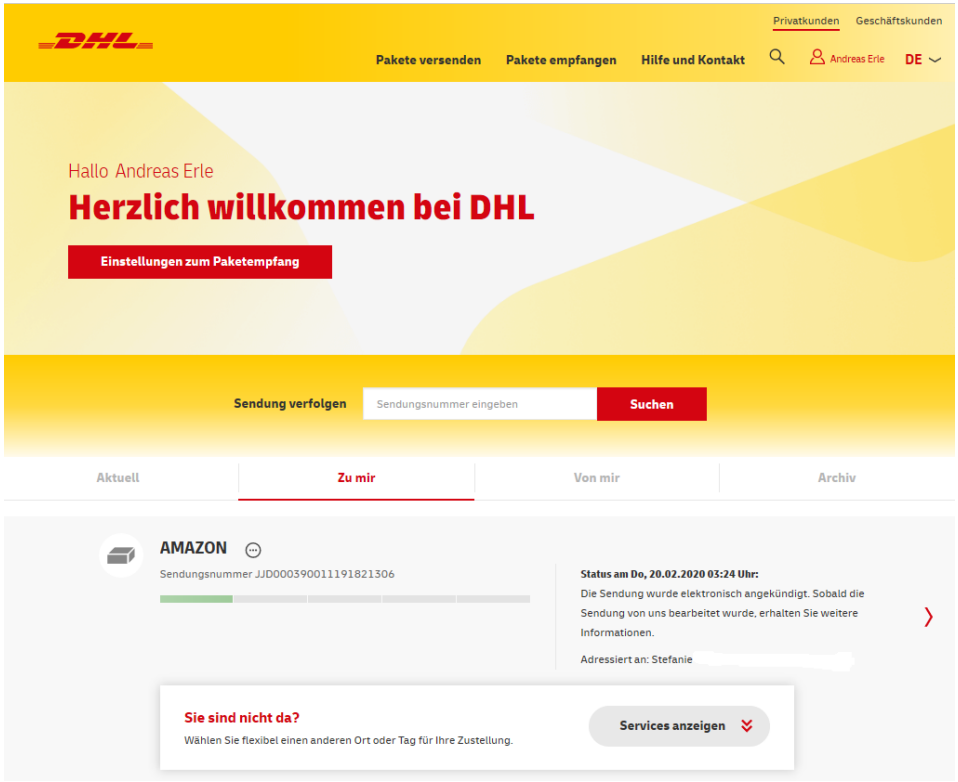
Es ist ein Skandal, dass WhatsApp nicht längst abgesetzt ist in der Diplomatie und Politik. Das ist eine unkalkulierbare Flanke und unverantwortlich, es einzusetzen. Einer der ehemaligen Gründer von WhatsApp, der mit dem Verkauf des Messengers an Facebook Milliarden verdient hat, ist derart schockiert über das was Facebook mit dem Messenger macht, dass er 50 Millionen Dollar an Signal gespendet hat und nun dort mitmacht. Er will Signal ausbauen. Komfortabler machen. Noch sicherer. Und vor allem Gruppen-Chats verbessern. Es gibt da keine Frage: Signal ist die deutlich bessere Variante. Jetzt erst recht.


META

DHL-Pakete verfolgen auch ohne App

Der Online-Handel boomt. Immer mehr Einkäufe werden über das Internet statt den stationären Handel abgewickelt. Auch wenn der eine oder andere Händler mittlerweile eine eigene Liefer-Infrastruktur aufbaut, ist DHL immer noch mit deutlichem Abstand der Marktführer bei den Paketdiensten. Die Verfolgung von Paketen gestaltet sich recht komfortabel auch ohne App!

Dazu müssen Sie sich nur einmal ein kostenloses Konto auf de Paketverfolgungs-Webseite von DHL anlegen. Das können Sie auf Wunsch dann auch nutzen, um Pakete online zu frankieren oder Abholungen zu buchen. Melden Sie sich auf allen Geräten dann mit diesem Konto auf der Webseite an. Das führt dazu, dass Sie Seite weiß, wer Sie sind und damit alle ihre Suchen und selbst versendeten Pakete kennt.



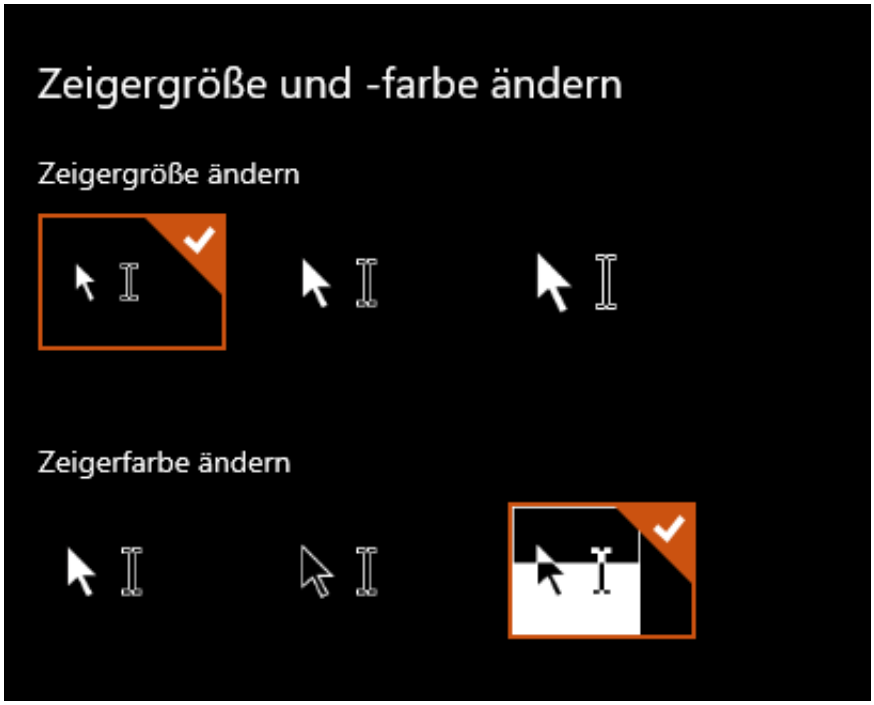
Um ein neues Paket zu tracken, geben Sie dessen Paketnummer unter **Sendung verfolgen** ein. Die Webseite zeigt Ihnen nun den aktuellen Status und den Sendungsverlauf. Wenn dieser schon vorliegt, dann auch den voraussichtlichen Liefertermin. Dieser erscheint, wenn die Sendung das Startpaketzentrum verlassen hat.

Alle Pakete werden automatisch unter Ihrem Konto weitergeführt. Sie müssen also die Paketnummer nicht mehr manuell eingeben, sondern finden das Paket automatisch in der Liste Ihrer Sendungen weiter unten auf der Seite. Klicken sie auf die drei Punkte neben dem Titel des Pakets, dann können Sie ihm einen sprechenderen Namen geben oder es aus der Liste löschen.

Display unter Windows lesbarer machen

Die Darstellung der Windows-Oberfläche ist auf normale Augen ausgelegt. Sie können in den Anzeigeeinstellungen die Größe der Symbole und Schrift verändern und einen allgemeinen Zoomfaktor für die Anzeige einstellen. Weitere Optionen finden Sie in der **Erleichterten Bedienung**, die Sie über die Einstellungen erreichen. Hilfreich, wenn Ihr Sehvermögen beeinträchtigt ist.

Es gibt viele Dinge, die die Sichtbarkeit von Windows-Systemelementen erhöhen können. Zu allererst sind der Cursor und der Mauszeiger schwierig zu sehen. Das können Sie unter **Cursor-& Zeigergröße** ändern. Nicht nur Größer und Form, sondern auch die Farbgebung, und hier findet sich versteckt eine tolle Einstellung unter **Zeigerfarbe ändern**. Klicken Sie auf die rechte von den drei Einstellungen, dann ist der Mauszeiger nicht schwarz oder weiß, sondern invertiert seine Darstellung je nach Hintergrund, auf dem Sie ihn bewegen.



Der Vorteil ist, dass er sich nicht mehr auf einem bestimmten Hintergrund verstecken kann und Ihren Augen anstrengendes Suchen erspart wird.

In die selbe Richtung geht die Einstellung **Hoher Kontrast**. Wenn Sie den aktivieren, dann werden die Farben aller Bedienelemente so dargestellt, dass sie sich bestmöglich voneinander abheben. Auch das schont die Augen deutlich!