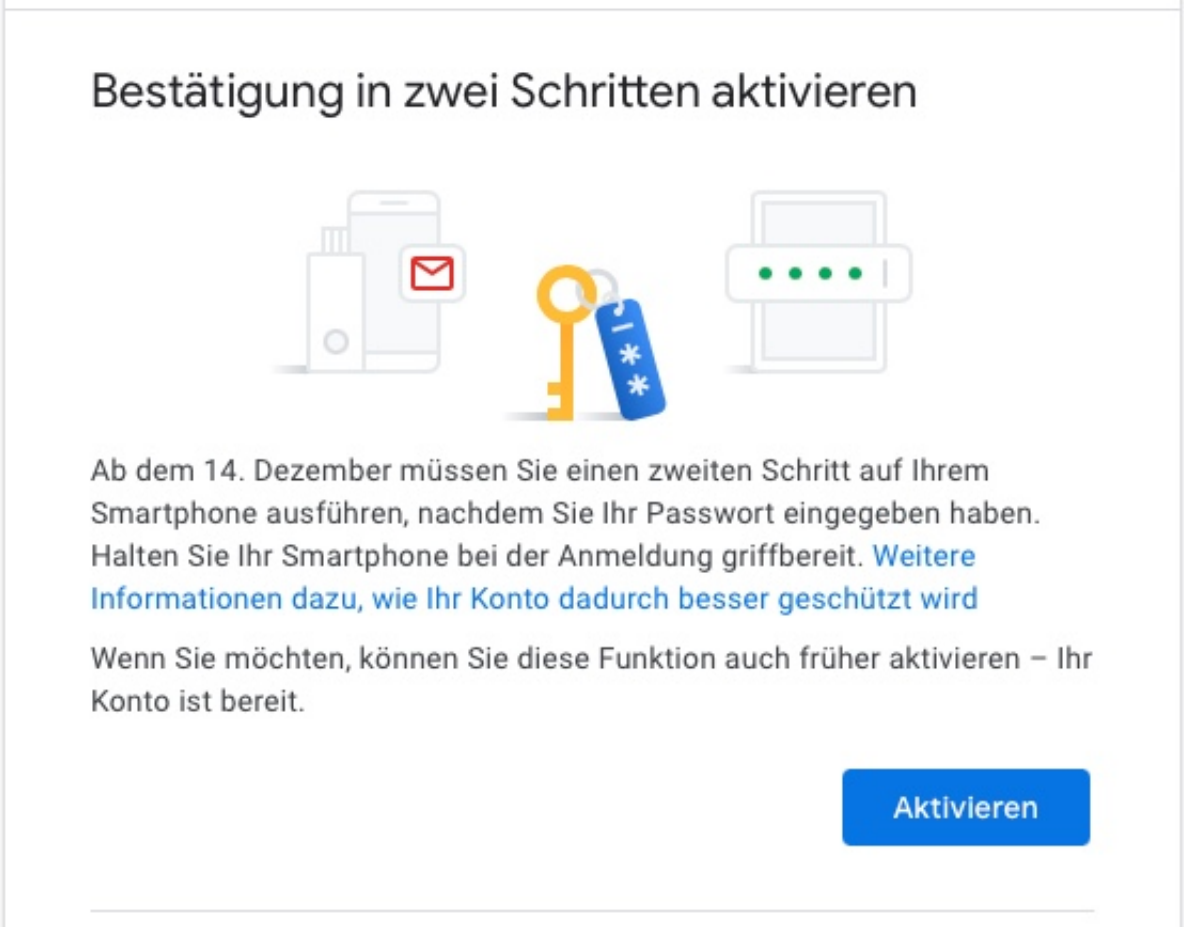
Schieb Report

Ausgabe 2021.49

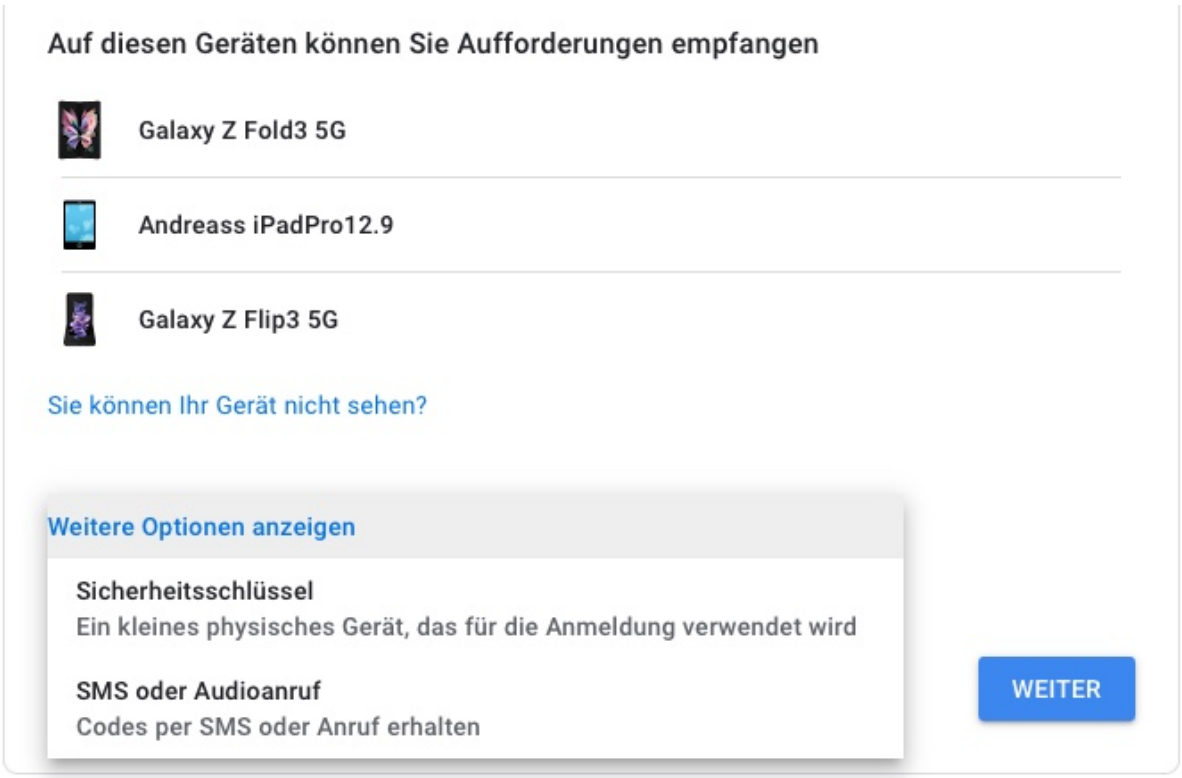
Bestätigung in zwei Schritten wir bei Google Pflicht

Die Zwei-Faktor-Authentifizierung (2FA) ist bei vielen Diensten bereits ein zusätzlicher Sicherheitsmechanismus, bei manchen sogar Pflicht. Google ergreift jetzt die Alternative und macht sie ab dem 14.12. 2021 verpflichtend. Wir zeigen Ihnen, was Sie beachten müssen!

Ihr Google Konto hat eine deutlich höhere Bedeutung als viele andere Ihrer Konten. Wer die Zugangsdaten kennt, kann auf Ihren Suchverlauf, Ihren Positionsverlauf, die E-Mails, Kontakte, sogar auf Ihr Android-Telefon zugreifen. Durch den zweiten Faktor, einen zusätzlichen Code, den Sie eingeben müssen, kann ein Angreifer mit Ihrem Kontopasswort alleine nichts mehr anfangen.



Öffnen Sie unter diesem Link den Security Check von Google und klicken Sie unter **Bestätigung in zwei Schritte aktivieren** auf **Aktivieren**. Sie können nun auswählen, wie sie den Zahlencode, den Google als zweiten Faktor versendet, empfangen wollen. Wenn Sie ein Android-Gerät oder ein anderes Gerät, das an Google angemeldet ist, verwenden und das immer dabei haben, dann können Sie dieses auswählen.



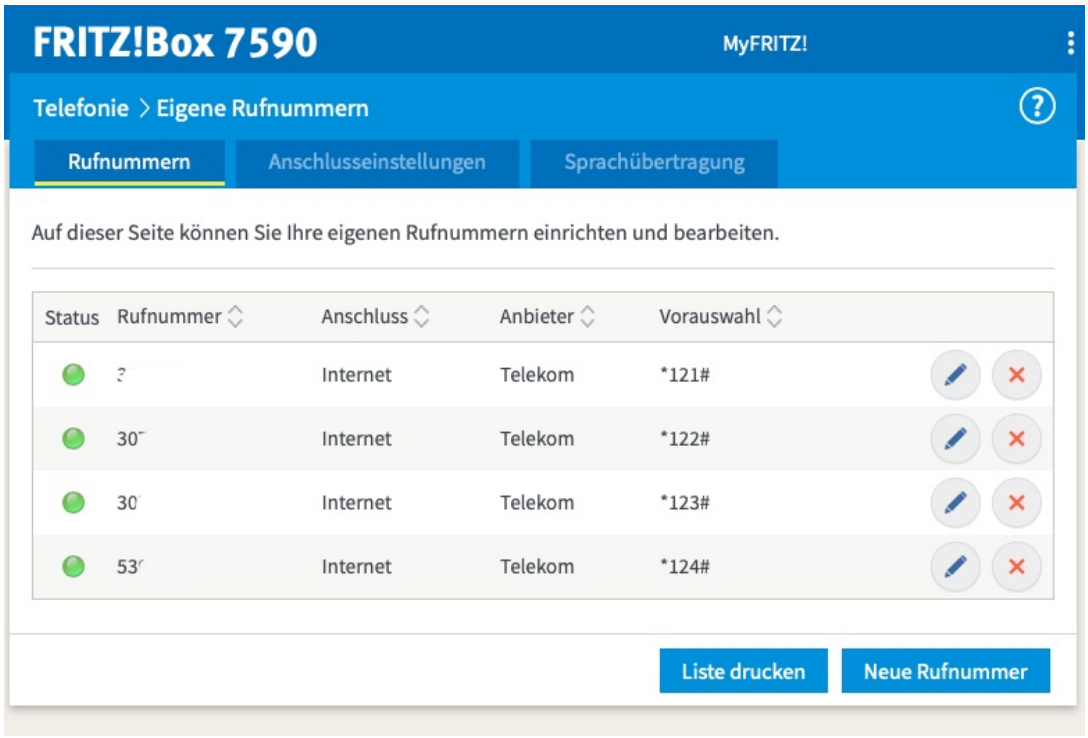
Alternativ können Sie auf **Weitere Optionen anzeigen** klicken und dann **SMS oder Audioanruf** aktivieren, dann kommt der Zahlencode für die Anmeldung per SMS oder Anruf. Das funktioniert dann unabhängig vom Gerät.

Wen Sie die Funktion nicht selbst manuell aktivieren, dann übernimmt Google das ab dem 14. Dezember 2021 automatisch für Sie. Ein Verzicht auf die Zwei-Faktor-Authentifizierung ist dann keine Option mehr.

Wenn ein Fritz!Fon "Interworking Fehler" meldet

Wenn Sie eine Fritz!Box verwenden, dann haben Sie damit eine komplette Telefonanlage mit dabei. Über die Fritz!Fon-Telefone des Herstellers können Sie dann direkt telefonieren. Es sei denn, das Gerät zeigt Ihnen die Fehlermeldung "Interworking-Fehler" an. Den Fehler können Sie selbst beheben!

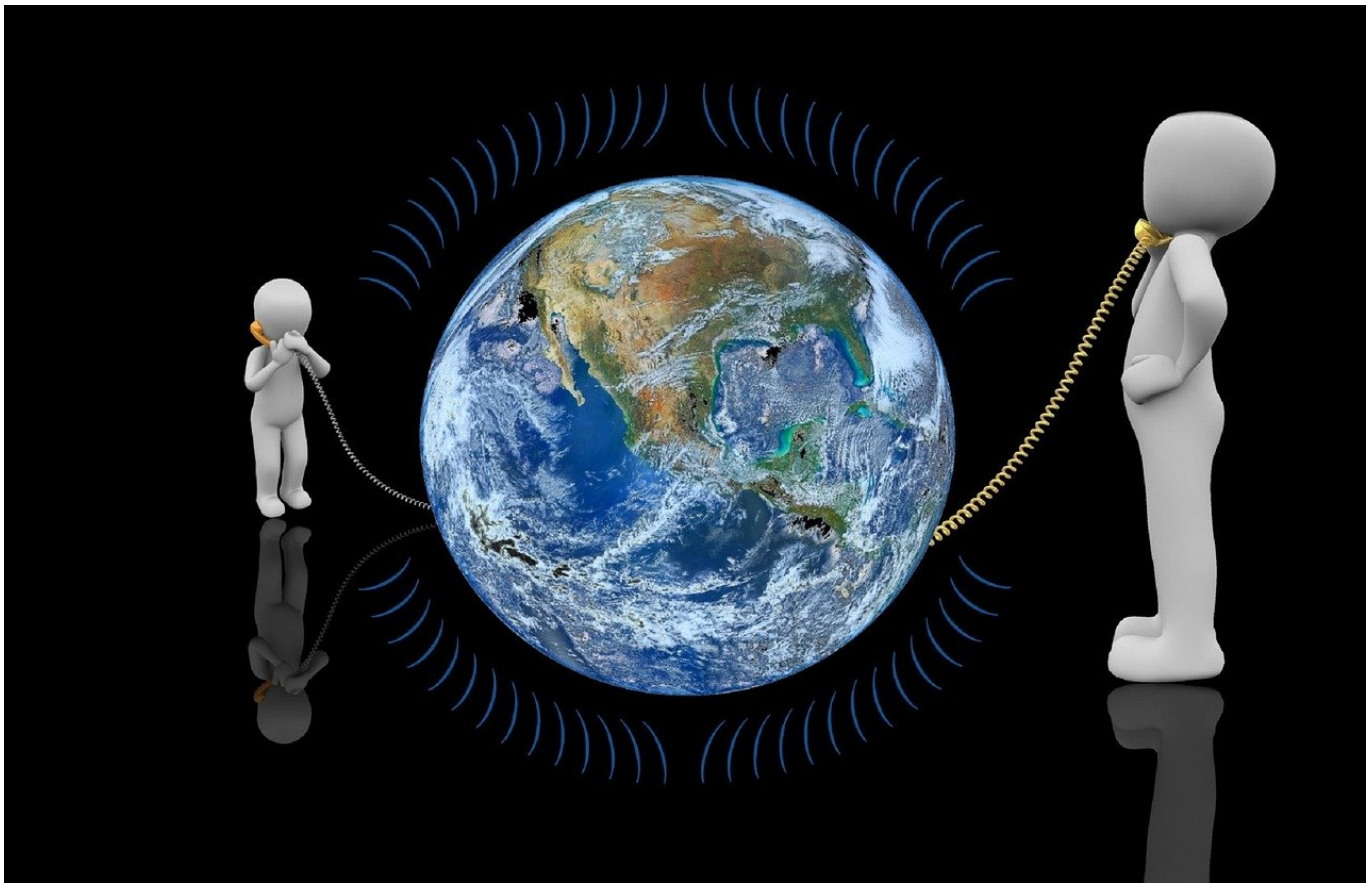
Die Handapparate einer Fritz!Box werden per DECT, dem Standard für Funk-Telefone, mit dem Router verbunden. Dieser übernimmt dann die Anbindung ans Telefonnetz. Ausgehende Anrufe werden dann ins Telefonnetz übertragen, eingehende wieder an die Handapparate weitergeleitet. Manchmal zeigen die Handapparate beim Aufbau einer Verbindung die Fehlermeldung "Interworking Fehler".



Wenn das häufiger vorkommt, dann probieren Sie die folgenden Schritte: Als erstes ist ein Neustart des Routers zu empfehlen, dieser baut automatisch die Verbindungen zu den Geräten wieder neu auf.

Wenn dies nicht hilft, dann richten Sie die Rufnummer, die die Probleme bereitet, neu ein. Dazu klicken Sie in der Benutzeroberfläche der Fritz!Box auf **Telefonie** > **Eigene Rufnummern**. Rechts von jeder Rufnummer finden Sie ein rotes Kreuz. Klicken Sie darauf, um die Rufnummer zu löschen. Klicken Sie dann auf **Neue Rufnummer**, um die gerade gelöschte Rufnummer wieder neu anzulegen. Dabei findet eine erneute Registrierung der Rufnummer im Netz statt. Das sorgt dafür, dass die Übergabe zwischen Fritz!Box und Telefonnetz wieder einwandfrei funktioniert.

Wenn die Gesprächsqualität beim Fritz!Fon schlecht ist

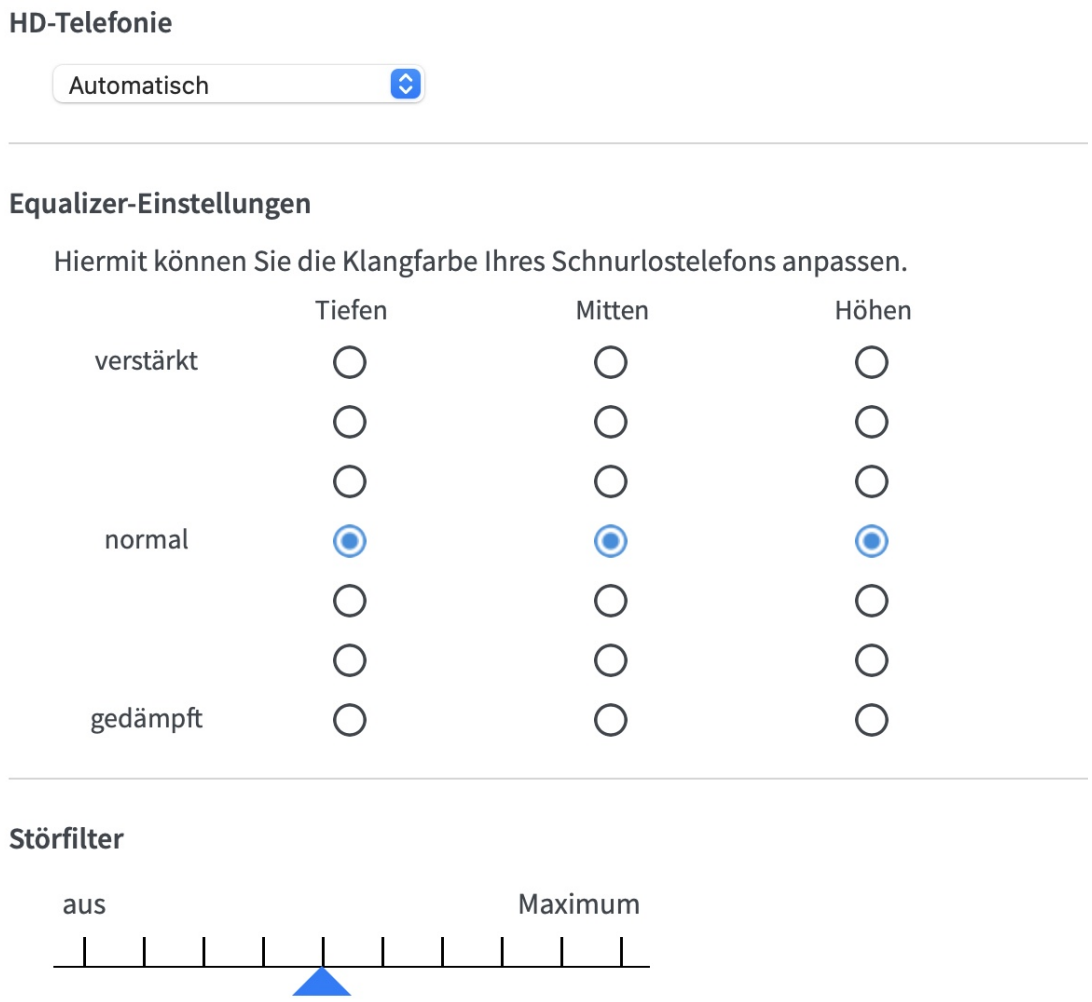


Telefonieren mit dem Router? Für die Router verschiedenster Hersteller gar kein Problem. Wenn Sie ihre Telefonanlage abgebaut und Handapparate für den Router angeschafft haben, dann verlasen Sie sich darauf. Wir zeigen Ihnen, was Sie bei Verbindungsproblemen machen können!

Der DECT-Standard für Mobilteile zum Telefonieren ist ein digitaler Standard. Sie werden also erst einmal keine schlechtere Qualität im Sinne von dumpferer oder niedriger auflösender Sprache erleben. Allerdings bedeutet das nicht, dass Ihr Gesprächspartner nicht unterbrochen zu hören sein kann oder gar wie aus der Konservendose klingen kann. Das hat in der Regel zwei Ursachen:

Wenn auf dem Display des Handapparats immer mal wieder die Meldung "Suche nach Basis" zu lesen ist, dann befinden Sie sich genau am Rand der Reichweite des Routers. Je nach den Geräten, die sich zwischen Ihnen und dem Router befinden, ist die Verbindung mal da, mal eben nicht. Ganz digital. Dieses

Wechselspiel sorgt dafür, dass die Verbindung immer mal wieder abreißt. Versuchen Sie, Router und Telefon näher zusammen zu bekommen und störende Gegenstände und Sender zwischen beiden Geräten zu entfernen. Manchmal reicht schon eine Zimmertür, die offen bleibt!



Technisch können Sie bei einer Fritz!Box zusätzlich in den Einstellungen für den jeweiligen Handapparat über die Qualitätseinstellungen Veränderungen vornehmen. Dazu klicken Sie in der Konfigurationsoberfläche des Routers auf **Telefonie** > **Telefoniegeräte**. Neben dem betroffenen Handapparat klicken Sie auf das **Stift-Symbol**.

Schalten Sie **HD-Telefonie** auf **HD deaktiviert**, wenn die Verbindung immer wieder unterbrochen wird. Das verringert die Qualität, damit aber auch die Datenmenge, die übertragen werden muss. unter den **Equalizer-Einstellungen** können Sie wie bei einem MP3-Player Höhen, Mitten und Bässe anpassen. Jedes Gehör hat unterschiedliche Vorlieben und Empfindlichkeiten. Wenn Sie Ihren

Gesprächspartner nicht gut verstehen, dann können Anpassungen an dieser Stelle helfen!

Was bedeuten die Sicherheitscodes bei DHL-Paketen?

Wer häufiger per DHL Pakete verschickt, der findet seit einiger Zeit auf den online erstellten Paketmarken einen zusätzlichen QR-Code, der aber scheinbar keine Funktion hatte. Vermehrt wird dieser jetzt aber an Packstationen und in Filialen angefordert. Was hat es damit auf sich?

Für die Annahme eines Paketes und später für die Verfolgung der Sendung ist der doppelte Barcode auf dem Paketschein relevant. Dieser enthält die Sendungsnummer und Verwaltungsinformationen. An einer Packstation oder in der Filiale wird der dann eingescannt und dem Paket zugeordnet. Der zusätzliche Sicherheitscode bringt keine zusätzlichen Informationen und was lange Zeit zwar auf den Paketscheinen, wurde aber nicht genutzt.

Sowohl die Packstationen als auch Filialen erfordern jetzt zusätzlich, dass dieser Sicherheitscode gescannt wird. Der Grund dafür: Vermehrte Betrugsversuche mit DHL-Paketmarken von Fremdanbietern. Der Sicherheitscode enthält zusätzliche Daten, mit denen die Echtheit der Paketmarke verifiziert werden kann. Was auf den ersten Blick für den Kunden zusätzlicher Aufwand ist, dient auch der Sicherheit des eigenen Paketes. Bei einer gefälschten Paketmarke - die Sie selber kaum erkennen können - übernimmt DHL natürlich auch keine Haftung für das Paket!

Risiken vermeiden können Sie am besten, indem Sie die Paketmarken direkt bei einem autorisierten Händler kaufen. Schnäppchenangebote im Internet bergen immer die Gefahr, einer Fälschung aufzusitzen!

Ist das Tor-Netzwerk sicher?

Viele Benutzer verwenden das Tor-Netzwerk, um möglichst anonym zu surfen. Das basiert vor allem auf dem Vertrauen, dass die Daten darin wirklich wirksam anonymisiert werden. Aber ist das wirklich der Fall?

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 potenziell 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: **T**he **O**nion **R**outer.

Das funktioniert so: Im Internet laufen die 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.

Nun gibt es immer wieder Gerüchte, dass Server kompromittiert werden und dadurch Nutzer, die einen solchen Server nutzen, identifizierbar wären. Dies ist leider möglich und bedeutet eine gewisse Gefahr für all diejenigen, die sich komplett anonym wähnen. Schutz gibt es gegen diese Gefahr kaum. Die Betreiber des Tor-Netzwerkes können die kompromittierten Server zwar aus dem Netzwerk entfernen. Genauso werden aber neue Server eingestellt die dieselbe Schadfunktion mitbringen. Wenn Sie den Tor-Browser nutzen, dann sollten Sie sich dieser Gefahr bewusst sein.

Vorsicht bei Facebook-Ratespielchen

Facebook ist unterhaltsam. Neben Neuigkeiten Ihrer Freunde und Bekannten finden Sie alle möglichen Ratespielchen der Art "Mein erstes Auto war ein...". Das lädt ein, eben mal schnell eine Antwort zu schreiben und die andern durchzulesen. Das Risiko ist aber nicht zu unterschätzen!

Alleine genommen fallen Ihnen die in solchen Aktionen gestellten Fragen oft nicht auf, wenn Sie sie aber einmal hintereinander ansehen, dann erkennen Sie schnell, dass diese oft eines gemeinsam haben: Diese Fragen werden auch als Sicherheitsfragen für die Passwortwiederherstellung oder als zweiter Schutzfaktor verwendet. Die Wahrscheinlichkeit ist hoch, dass Sie diese Fragen gleich beantwortet haben.

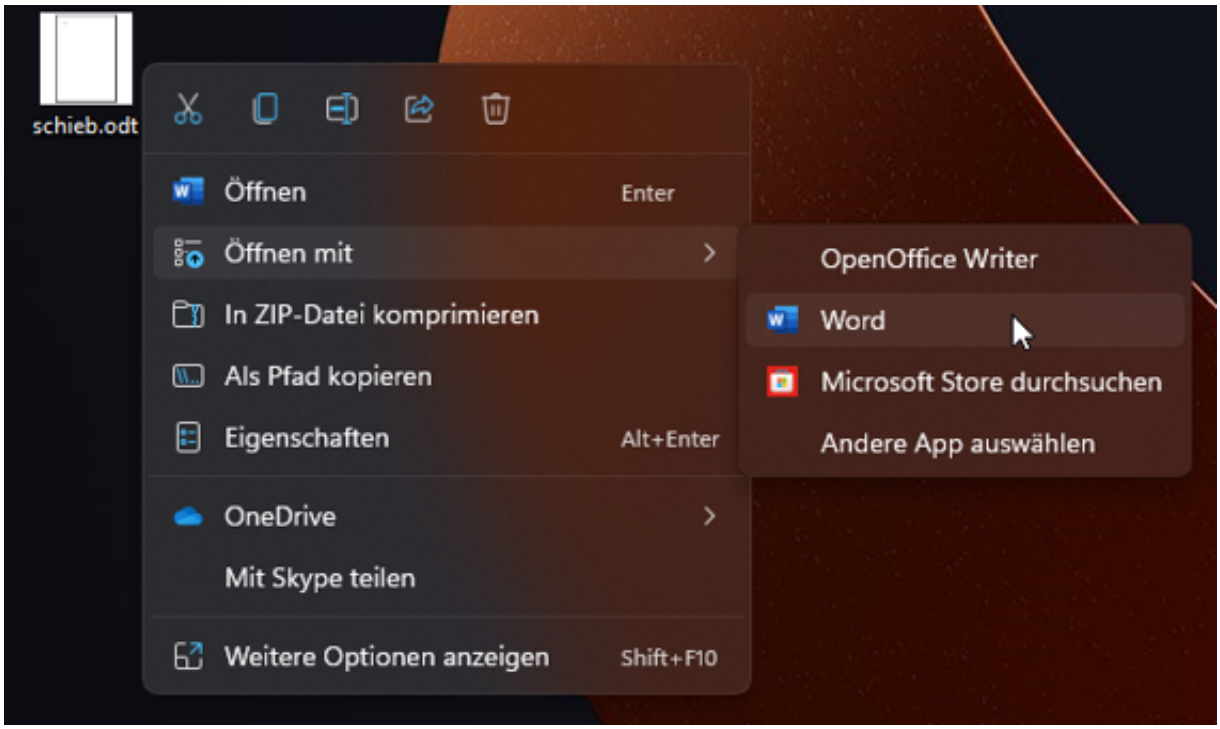
In der Folge hat damit jeder Zugriff auf diese Antworten, denn die "Fragesteller" haben eine öffentliche Timeline, jeder kann die Beiträge lesen. Mit wenigen weiteren Informationen haben Übeltäter damit gegebenenfalls die Möglichkeit, durch einen Passwortreset und die richtige Antwort auf eine Sicherheitsfrage eines Ihrer Konten zu übernehmen. Wenn Sie diese Antworten als Teil Ihrer Passwörter verwenden, dann ist das Risiko noch höher.

Zusammengefasst: Solche Frageaktionen im Internet mögen kurzen Spaß bringen, verursachen aber gegebenenfalls länger andauernden Ärger! Wenn Sie unsicher sind, ob eine Umfrage oder ein Post wirklich echt sind, dann lohnt sich immer ein Blick auf MimiKama. Dort finden Sie viele Hinweise zu momentan beliebten Phishing-Aktionen.

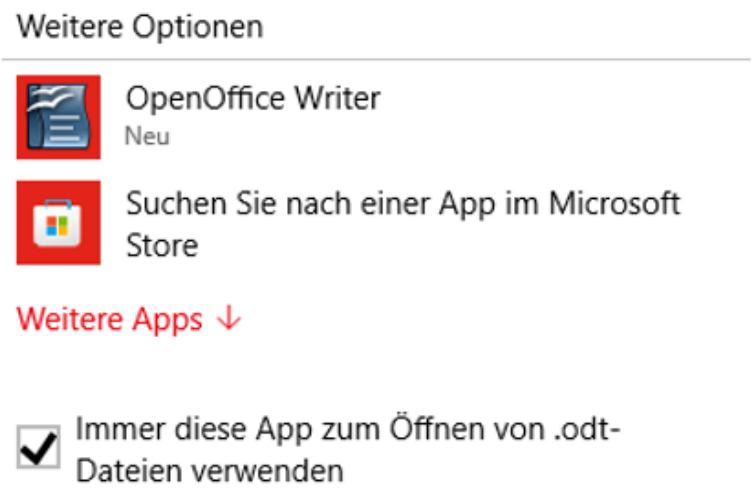
Öffnen von Dateien mit anderen Apps in Windows

Windows hat für jeden Dateityp eine Standard-App, die zum Öffnen verwendet wird. Oft können aber auch andere Apps eine Datei öffnen. Das lässt Windows ein wenig versteckt zu.

Wenn sie zwei oder mehr Programme installiert haben, die einen Dateityp öffnen können, dann hat das meist einen Grund. Das eine ist bei der einen Funktion im Vorteil, das andere bei einer anderen. Es kann also vorkommen, dass Sie die selbe Datei mal mit dem einen, mal mit dem anderen Programm öffnen wollen.



Das können Sie direkt aus dem Windows Explorer! Klicken Sie mit der rechten Maustaste auf die Datei, dann auf **Öffnen mit** und wählen Sie das Programm aus, mit dem Sie die Datei zu dem Zeitpunkt öffnen wollen. Windows zeigt Ihnen alle Apps und Programme an, von denen es weiß, dass die das können.



Beim nächsten Mal verwendet Windows dann wieder das Standardprogramm zum Öffnen der Datei. Wenn Sie das ändern wollen, dann klicken Sie nach Klick auf **Öffnen mit** nicht direkt auf die App, sondern auf **Andere App auswählen**.

Bevor Sie jetzt die App anklicken, setzen Sie einen Haken neben **Immer diese App zum Öffnen von …-Dateien verwenden**. Windows merkt sich Ihre Auswahl

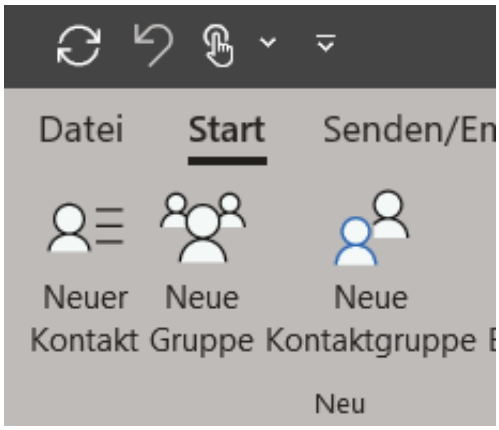
und ändert für den betroffenen Dateityp die Standardzuordnung automatisch.

Mailgruppen in Outlook anlegen

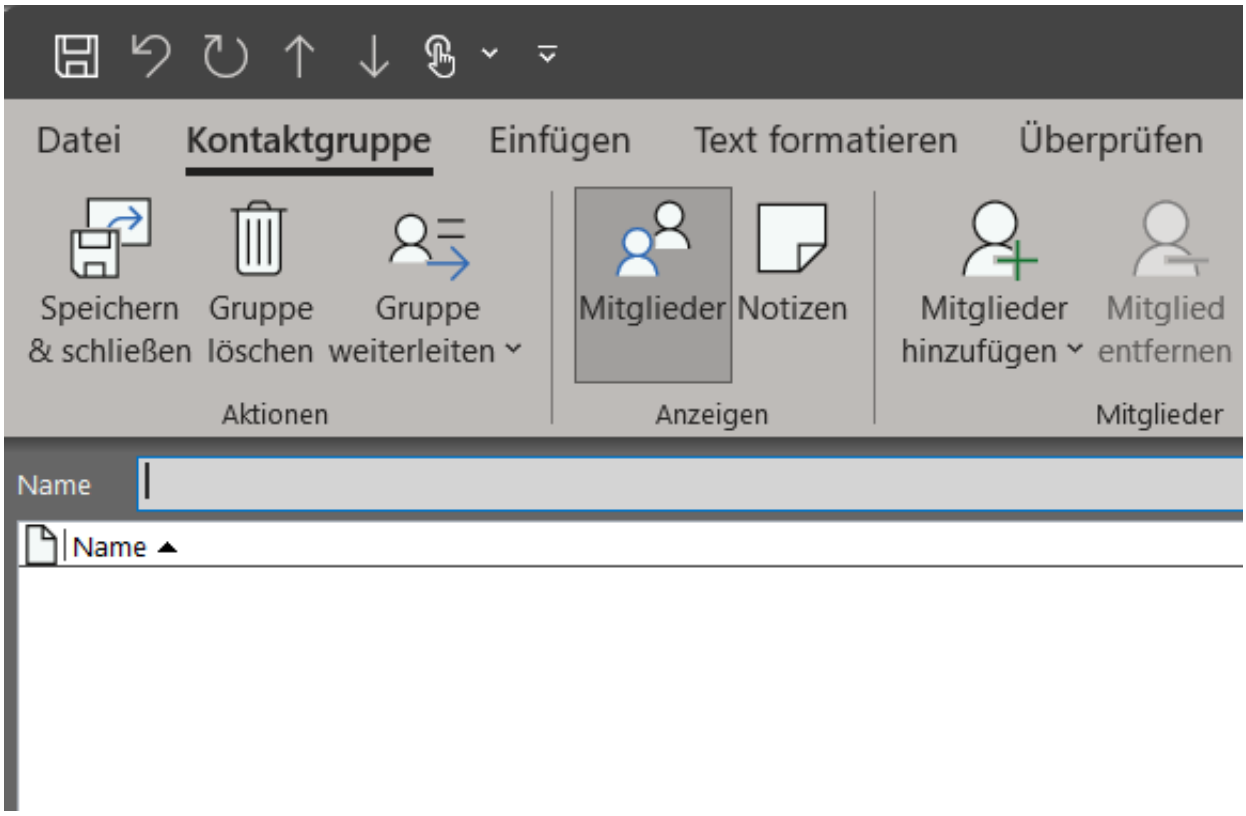
Sie schreiben immer wieder der gleichen Gruppen von Menschen eine E-Mail? Dann macht es unnötigen Aufwand, deren E-Mail-Adressen immer wieder manuell einzugeben. Microsoft Outlook bietet in den neueren Versionen die hilfreiche Funktion der Kontaktgruppen, früher auch als "E-Mail-Verteiler" bekannt.

Die Idee hinter einer Kontaktgruppe ist simpel: In einem neuen Kontakt werden verschiedene bestehende Kontakte zusammengefasst. Dabei ist es egal, in wie vielen Gruppen ein Kontakt ist, die Ursprungskontakte bleiben separat verfügbar und werden nicht verändert. Die Kontaktgruppe können Sie wie einen normalen Kontakt als Empfänger einer E-Mail auswählen. Outlook löst die Gruppe beim Versenden der E-Mail dann in ihre Einzelkontakte auf.

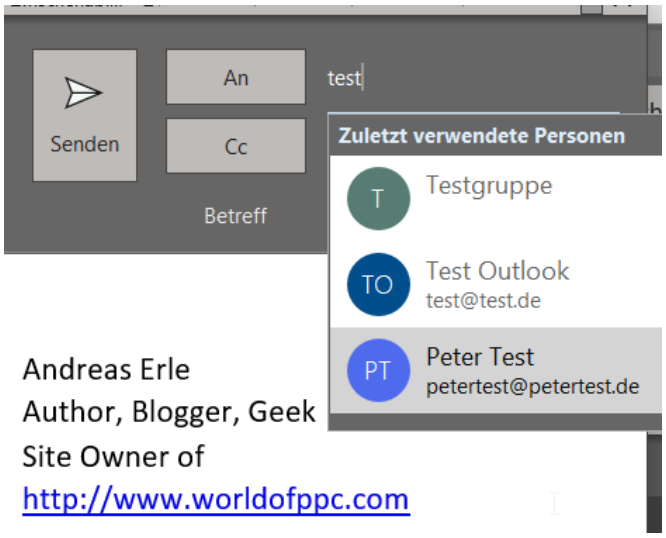
Um eine neue Kontaktgruppe anzulegen, klicken Sie in Outlook unten links auf die beiden Figuren, um die Kontakte zu öffnen. In der Symbolleiste klicken Sie dann auf **Neue Kontaktgruppe**.



Geben Sie der Gruppe einen sprechenden Namen, dann fügen Sie ihr durch einen Klick auf **Mitglieder hinzufügen** bestehende Kontakte hinzu, bis alle Kontakte in der Gruppe vorhanden sind. Dann speichern Sie die Gruppe durch einen Klick auf **Speichern und Schließen**. Die Gruppe erscheint in der Übersicht der Kontakte unter ihrem Namen.



Sie können den Namen der Gruppe direkt als Kontakt in die An-Zeile einer neuen E-Mail eingeben. Wundern Sie sich nicht: Kontaktgruppen werden mit einem kleinen Pluszeichen markiert. Klicken Sie darauf, dann ersetzt Outlook den Namen der Gruppe durch die einzelnen Kontakte, die darin sind. Das ändert aber nichts daran, dass alle Kontakte der Gruppe die Mail bekommen.



Andreas Erle
Author, Blogger, Geek
Site Owner of
http://www.worldofppc.com

Kindesmissbrauch im Netz: Löschen statt Wegschauen

Wenn die Polizei die Drahtzieher von pädokriminellen Foren dingfest machen, ist das immer ein Erfolg. Doch niemand kümmert sich darum, die Aufnahmen aus dem Netz zu entfernen.

Sexuelle Gewalt an Kindern – eins der schwersten Verbrechen, die Menschen in Friedenszeiten begehen können.

Das Internet macht das Verteilen und den Vertrieb von Fotos und Videos im Schatten der Anonymität im Netz besonders einfach. Das Konsumieren ebenso. Die Polizei kommt kaum nach damit, Täterinnen und Täter ausfindig zu machen. Denn im Darknet ist die Fahndungsarbeit besonders schwierig.

Niemand kümmert sich um Löschung

Worum sich allerdings kaum jemand kümmert: Die Fotos und Videos mit Gewalt an jungen Menschen aus dem Netz zu entfernen. Denn das Schlimmste für Opfer und Angehörige ist, dass die Aufnahmen praktisch für immer "im Netz" bleiben.

Selbst wenn Täter mal dingfest gemacht und bestraft werden: Die Aufnahmen verbleiben häufig online, weil so viele Kopien kursieren.

Auf diesen bedrückenden Zustand haben die Kollegen vom NDR nachdrücklich hingewiesen, die das generell empfehlenswerte Online-Reportage-Format STRG-F machen. Viele Missbrauchsbilder der Pädokriminellen-Plattform "Boystown", die deutsche Behörden im April 2021 abgeschaltet hatten, waren danach weiterhin online abrufbar. Nicht ungewöhnlich. Wie in der Reportage zu sehen, fühlt sich die Polizei nicht dafür zuständig, die unzähligen Kopien solcher Aufnahmen zu beseitigen.

Bedeutet: Ermittler nehmen Drahtzieher von Plattformen wie "Boystown" fest. Doch die Fotos und Videos der Plattform werden bei den entsprechenden Speicherdiensten ("Hostern") nicht entfernt – bleiben also sichtbar. Es ist nur eine Frage der Zeit, bis neue Foren auftauchen mit Links auf die Fotos und Videos.

https://www.youtube.com/watch?v=iItLpwkQMUQ

Das Reportageformat STRG-F zeigt, wie einfach es ist, etwas zu unternehmen

Im Darknet vor allem Verweise (Links)

Als Laie staunt man da vielleicht. Zwar nutzen die Täter zum Betreiben ihrer Plattformen das anonyme Darknet. Aber da Fotos und vor allem Videos viel Speicherplatz beanspruchen, werden die bei einschlägigen "Hostern" gespeichert, die im "normalen" Internet liegen, also keineswegs im Darknet. Viele der Hoster haben keine Ahnung davon.

Die Reportage zeigt: Macht man sich die Mühe, den Hostern die Links zu melden, entfernen sie diese meist innerhalb weniger Stunden. Das macht gar keinen großen Aufwand. Führt aber dazu, dass die Aufnahmen tatsächlich verschwinden und die Konsumentinnen und Konsumenten im Darknet "frustriert" sind, weil die Links immer häufiger ins Leere laufen. Eine gute Zermürbungstaktik.

Werden die Aufnahmen nicht konsequent gelöscht – was derzeit leider Status quo ist –, werden die Opfer leider immer wieder zu Opfern. Das wäre völlig vermeidbar.

Löscharbeit ist dringend erforderlich

Es ist daher dringend erforderlich, neben der Fahndungsarbeit endlich auch mal Löscharbeit zu leisten. Bund und Länder sollten eine Stelle schaffen, die nichts anderes macht, als entdeckte Aufnahmen entfernen zu lassen. Sofort und immer wieder. Weltweit. Den nötigen Rechtsrahmen gibt es, dass Provider und Hoster solche Inhalte bei Meldung unverzüglich entfernen müssen.

Vermutlich würden sich sogar genügend Freiwillige melden, die bei der Meldearbeit mitmachen. Der Staat muss "lediglich" den nötigen Rahmen dafür schaffen. Das kostet nicht viel – und bringt eine Menge.

Algorithmen können helfen, Aufnahmen mit Kindesmissbrauch zu entdecken

Warum die Rohingya Facebook auf 150 Mrd. Dollar verklagen

Seitdem die Whistleblowerin Frances Haugen öffentlich aussagt und so Einblicke in die Geschäftspraktiken des Facebook-Konzerns ermöglicht, steht der Konzern mächtig unter Druck.

Denn jetzt gibt es nicht nur den Verdacht, sondern dank der geleakten Dokumente reichlich konkrete Belege dafür, dass Facebook wissentlich die Algorithmen auf Gewinnmaximierung programmiert – und selbst dann nichts unternimmt, wenn sich schädliche Wirkungen in der Gesellschaft zeigen und der Konzern davon Kenntnis hat.

Algorithmen entscheiden immer pro Umsatz

Und nun das: Geflüchtete Rohingya – eine verfolgte muslimische Minderheit in Myanmar – haben eine Klage in Kalifornien eingereicht. Die Kläger stellen einen direkten Zusammenhang zwischen algorithmisch geförderter Desinformation und Aufruf zur Gewalt und tatsächlicher Gewalt her. Facebook sei bereit gewesen, "das Leben der Rohingya gegen eine bessere Marktdurchdringung"

einzutauschen.

> Klagevorwurf: "Unbestreitbare Realität ist, dass Facebooks Wachstum, angeheizt durch Hass, Spaltung und Fehlinformationen, Hunderttausende zerstörte Leben der Rohingya hinterlassen hat."

Das kann man so sagen. Denn laut Whistleblowerin Frances Haugen hatte die Konzernleitung Kenntnis, dass die auch in Myanmar sehr wichtige Plattform nicht unbedingt zur Befriedung des am Ende religiös begründeten Konflikts beiträgt. Im Gegenteil: Facebook hat den Konflikt angeheizt. Öl ins Feuer gekippt.

Myanmar geht uns alle an

In Myanmar kann man sehr schön sehen, dass ein gesellschaftlich noch weiter zugespitzter Konflikt als bei uns für Facebook regelrecht ein Leckerbissen ist. Facebook verhält sich wie bei einem Hahnenkampf: Je mehr Menschen zuschauen, desto mehr wird geboten und verdient. Also wird mächtig Wirbel gemacht. Dafür sorgen schon die Algorithmen, die von Ethik nichts verstehen und auf maximale Erregung programmiert sind.

Wir sollten nicht den Fehler machen zu denken: Der Fall Myanmar interessiert mich nicht. Ist zu weit weg. Auch bei uns gibt es jede Menge gesellschaftliche Konflikte, die heutzutage mit religiösem Eifer ausgefochten werden - vor allem auf den Plattformen. Corona-Leugner gegen Wissenschaft. Bürger gegen Politik. Geimpfte gegen Ungeimpfte. Auch das kann in Mord und Totschlag ausarten - dank Facebook, Twitter und Co.

Natürlich trägt Facebook nicht die Verantwortung für die Konflikte selbst. Aber Facebook ist bekennender Profiteur der Konflikte. Man könnte fast sagen: so wie die Waffen-Industrie.

Myanmar geht uns alle an

Die Klage in den USA mit der unfassbar hohen Klagesumme bringt zumindest auf den Punkt, wie hoch der Schaden sein kann, der damit einhergeht. Es wird

interessant sein zu sehen, wie Kläger argumentieren – und wie sich Facebook wehren will. Denn vor Gericht müssen dann ja konkrete Zahlen und Belege her. Facebook wird sich zum ersten Mal richtig verantworten müssen.

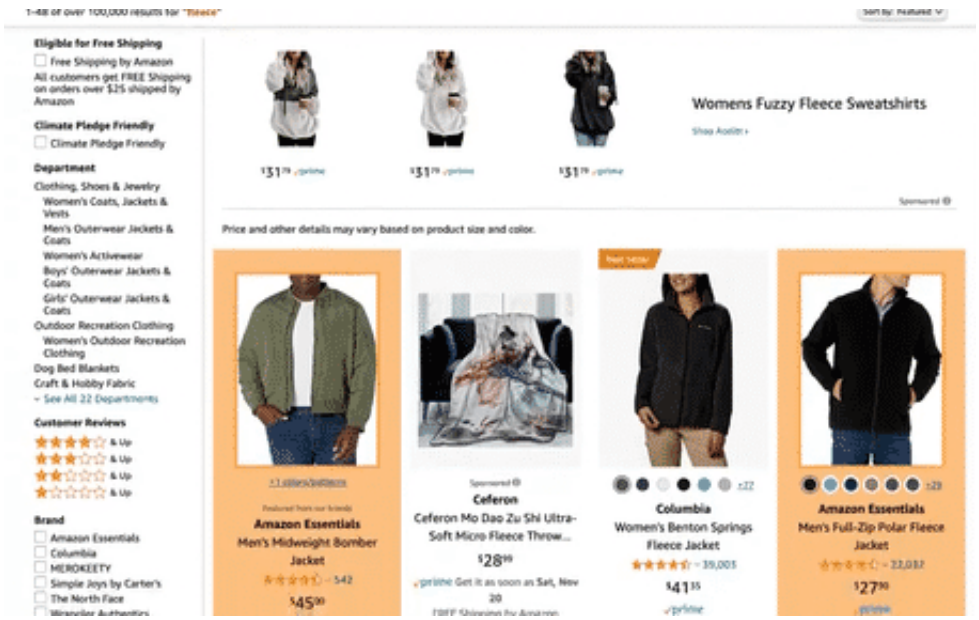
Das wird spannend – und könnte Mark Zuckerberg tatsächlich zum Umdenken zwingen. Denn auch, wenn Facebook der gesellschaftliche Frieden vollkommen Schnuppe zu sein scheint (auch der in den USA): Wenn es droht Geld zu kosten, dann könnten die Herrschenden über die Algorithmen diese endlich anweisen, anders zu entscheiden und zu funktionieren.

/> Die Macht der Algorithmen: Facebook bestimmt, was die Menschen sehen

Brand Detector: Plugin enttarnt Amazons Eigenmarken

Amazon verkauft in seinem Online-Shop diverse Eigenmarken. Um die besser erkennbar zu machen, gibt es jetzt ein kostenloses Plugin namens "Amazon Brand Detector".

Strengere Regeln in den Einkaufspassagen, immer vollere Innenstädte, gesundheitliche Risiken beim Shoppen: Machen wir uns nichts vor - in diesem Jahr kaufen vermutlich noch mehr Menschen online ihre Geschenke ein als sonst ohnehin schon. Und der Inbegriff für Online-Shopping ist Amazon. Weltgrößter Online-Händler – und für viele Menschen eine Art Suchmaschine für alles, was man kaufen kann.



Amazon verkauft auch eigene Produkte

Was viele nicht wissen: Amazon präsentiert keineswegs nur die Waren anderer Hersteller (und im Marketplace sogar anderer Händler), sondern stellt auch selbst Waren her. Bei Hightech-Produkten wie dem digitalen Assistenten Echo (Alex) oder dem Kindle Reader weiß das auch jeder.

Doch Amazon mischt in den meisten Märkten mit. Das, was besonders gut läuft und gute Margen abwirft (und wer wüsste das aufgrund der immensen Datenmengen besser als Amazon...), das stellt Amazon gerne schon mal auch selbst her.

Unter diversen Eigenmarken. "Amazon Basics" dürfte die bekannteste und gilt gleichzeitig auch als erfolgreichste Eigenmarke. Hier versteht jeder: OK, die Yogamatte kommt also nicht nur von Amazon, sondern ist auch von Amazon hergestellt. Doch Amazon hat über 150 solcher Eigenmarken. Teilweise lizenziert Amazon auch Produkte oder kooperiert mit anderen Herstellern. Dann finden sich Hinweis wie:

> *Ultrasport ist eine Amazon-Marke, die an Dritthersteller lizenziert ist. Details zu den Herstellern finden Sie in der Produktverpackung.*

Amazon Brand Detector macht Marken sichtbar

Für Konsumenten ist das völlig undurchsichtig. Aber jetzt gibt es eine Lösung: Der Amazon Brand Detector von Markup ist eine kostenlose Browser-Erweiterung. Ist sie installiert, erscheint beim Durchstöbern von Amazon ein klarer Hinweis: Landet man auf einem Angebot von einer Amazon-Marke, ist dieses Produkt gut erkennbar gelb hinterlegt.

Was man mit der Info anstellt, muss jede/r selbst entscheiden. Manche wollen vielleicht auf gar keinen Fall Amazon-Marken kaufen, andere vor allem. Der Brand Detector hilft dabei. Das erspart Usern, sich auf der offiziellen Übersicht von Amazon umzuschauen, welche Marken zum Konzern gehören.

Nicht in der App, nur im Web

Das Plugin funktioniert nicht in der Amazon-App auf dem Smartphone, sondern nur dann, wenn man Amazons Shop-Seite im Browser aufruft. Die Erweiterung läuft mit Firefox, Chrome und allen Chromium-basierten Browsern wie Microsoft Edge oder Opera.

Ein hilfreiches Plugin. Sehr viel nützlicher wäre aber ein "China Shop Detector", der Menschen beim Einkauf auf Amazon davor bewahrt, versehentlich in einem China-Shop zu bestellen. Das würde einem eine Menge Frust ersparen, der häufig durch mangelhafte Qualität, Fake-Markenprodukte, Zollgebühren und fehlende Umsatzsteuer entsteht.

Auch Saugroboter "Astro" ist eine Amazon-Eigenmarke

Internet zu langsam? Dann einfach weniger zahlen...

Der Gesetzgeber hat die Rechte von Verbrauchern gestärkt: Wer feststellt, dass sein DSL-, Kabel- oder Glasfaser-Anschluss deutlich langsamer ist als versprochen und eingekauft, kann seine Zahlung an den Provider kürzen. Die Messung muss allerdings genau erfolgen - und auch mehrfach.

Alle DSL-, Kabel- und Glasfaser-Provider versprechen blitzschnelles Internet. Doch viele Menschen berichten von langsamen Internetleitungen...

Woran liegt das nur? Unter anderem daran, dass die Provider bislang im Kleingedruckten beim Datentempo schreiben: „**Bis zu** 100 Mbit/Sekunde“. Es könnte also auch die Hälfte sein. Doch damit kommen Provider nicht mehr durch. Wenn sie nicht das volle Datentempo liefern, können Kunden demnächst Geld einbehalten.

Das hat sich für Verbraucher geändert

Seit 1. Dezember ist eine neue Regel im Telekommunikationsnetz in Kraft – und die stärkt das Recht von Verbrauchern. Stellen die Kunden fest, dass die Internetverbindung regelmäßig deutlich mickriger ist das im Tarif versprochen, können Kunden die Monatszahlung kürzen – so ähnlich wie Mieter ihre Miete, wenn erhebliche Mängel vorliegen. Ab sofort lohnt es sich also, das Datentempo an der eigenen DSL-Buchse zu messen.

Denn ergeben sich große Diskrepanzen, kann man wenigstens Geld einbehalten. Das wird DSL-Anbieter künftig zwingen, schneller zu reagieren, wenn es in einer Wohnung, einem Haus oder einer Region zu Engpässen kommt – weil es sie sonst Geld kostet. Während der Pandemie hat es regelmäßig bei DSL-Kunden Probleme bei der Bandbreite gegeben: Sie konnten bei weitem nicht so schnell ins Netz wie versprochen.

Der Grund: Sind mehr Menschen gleichzeitig online als vom Provider in der Vergangenheit im Durchschnitt gemessen und berechnet, sind die Leitungen quasi „überlastet“. Das Problem betrifft dann meist gleich mehrere Haushalte oder gar ganze Straßenzüge.

So messe ich, wie schnell meine Internetverbindung ist

Es gibt verschiedene Möglichkeiten, das eigene Datentempo zu messen. Entweder, man stellt mit seinem Browser eine Verbindung zu einer Webseite her, die das Tempo misst – etwa dem Speed Check von Google.

Doch es gibt noch viele andere Speed-Checker im Netz. Einfach „Speedtest“ bei Google eingeben und eine Webseite aussuchen. Oder man benutzt eine spezielle App für sein Smartphone oder besser noch für seinen Rechner. Optimal ist die Breitbandmessung der Bundesnetzagentur unter breitbandmessung.de.

Hier lassen sich Apps laden, die besonders gut funktionieren. Wichtig ist: Am Desktop-PC wenn möglich ein LAN-Kabel anschließen, denn nur das bietet wirklich und garantiert optimales Datentempo. Wenn das nicht geht, dann auch per WLAN – und dafür sorgen, dass eine optimale WLAN-Verbindung besteht.

Der Desktop-PC sollte idealerweise nicht allzu weit vom Router entfernt sein. Denn sonst misst man das maximale WLAN-Datentempo, das ist aber nicht das optimale Datentempo im Router. Bei einer schlechten WLAN-Verbindung könnte

der Router schneller.

Was tun, wenn mein DSL zu langsam ist?

Ganz so einfach funktioniert es nicht. Wichtig ist erstmal: Die Kunden müssen mehrere Messungen vornehmen. Zu verschiedenen Zeiten und an verschiedenen Tagen. Zweitens ist es erforderlich, die offizielle App für den Desktop der Bundesnetzagentur zu verwenden.

Nur hier ist sichergestellt, dass auch wirklich das tatsächliche Datentempo optimal gemessen wird. Außerdem hilft die App dabei, die nötigen mehreren Messungen durchzuführen und mit statistischen Daten der Anbieter zu vergleichen. Kommt es zu Diskrepanzen, können Kunden die hier offiziell hinterlegten Messwerte nutzen, um sich zu beschweren.

Die App wird gerade von der Bundesnetzagentur überarbeitet, um diese Anforderungen optimal zu erfüllen. Sie soll am 13. Dezember (also in einer Woche) an den Start gehen.

Höhe der möglichen Minderung

Der Anspruch auf Minderung besteht laut Gesetz bei „erheblichen, kontinuierlichen oder regelmäßig wiederkehrenden Abweichungen“. Also nicht, wenn einmal am Abend Netflix etwas länger braucht als sonst. Die Vertragszahlung ist laut Gesetz „in dem Verhältnis herabzusetzen, in welchem die tatsächliche Leistung von der vertraglich vereinbarten Leistung abweicht“.

Bedeutet: Bekommt man nur die Hälfte der versprochenen Leistung, zahlt man nur die Hälfte des Preises. Am Ende ist das aber für die meisten gar kein wirklicher Erfolg. Denn wer auf ein schnelles Internet angewiesen ist, will nicht 20 oder 30 EUR im Monat sparen, sondern die eingekaufte Geschwindigkeit bekommen. Die gute Nachricht ist aber: Durch den Druck, der jetzt auf die Provider entsteht, steigt die Wahrscheinlichkeit, dass die Provider für mehr Datentempo auf den Leitungen sorgen.