# Schieb Report

Ausgabe 2022.28

# Paywall umgehen: Tool macht Artikel sichtbar


**Ein kostenloses Tool - eigentlich: ein Onlinedienst - springt für Euch über die "Paywall" vieler Nachrichtenangebote: Das Tool macht Artikel sichtbar und lesbar, die eigentlich nur zahlender Kundschaft zur Verfügung stehen. Praktisch für alle, die gelegentlich etwas lesen wollen - ärgerlich für Verlage.**

Es ist nicht leicht, mit guten Inhalten im Netz Geld zu verdienen. Die Menschen erwarten, dass (fast) alles kostenlos ist - zumindest Informationen. Also Artikel zum Beispiel. Das war nicht immer so: Früher musste man für gute Texte immer bezahlen, ob für Bücher, Zeitungen, Zeitschriften oder Magazine.

Heute steht fast alles im Netz. Die Verlage wollen und brauchen Aufmerksamkeit. "Kostenlos" Inhalte ziehen die Menschen an. Weil die Suchmaschinen ihnen die Besucher vorbei schicken.

## Inhalteanbieter müssen Aufwand refinanzieren

Aber wie die ganze Arbeit, den Aufwand, die Technik bezahlen? Die meisten Verlage sehen keine andere Möglichkeit und versehen ihre Angebote mit Werbung. Doch auch damit lässt sich nicht genug Geld verdienen, um hochwertigen Journalismus zu finanzieren.

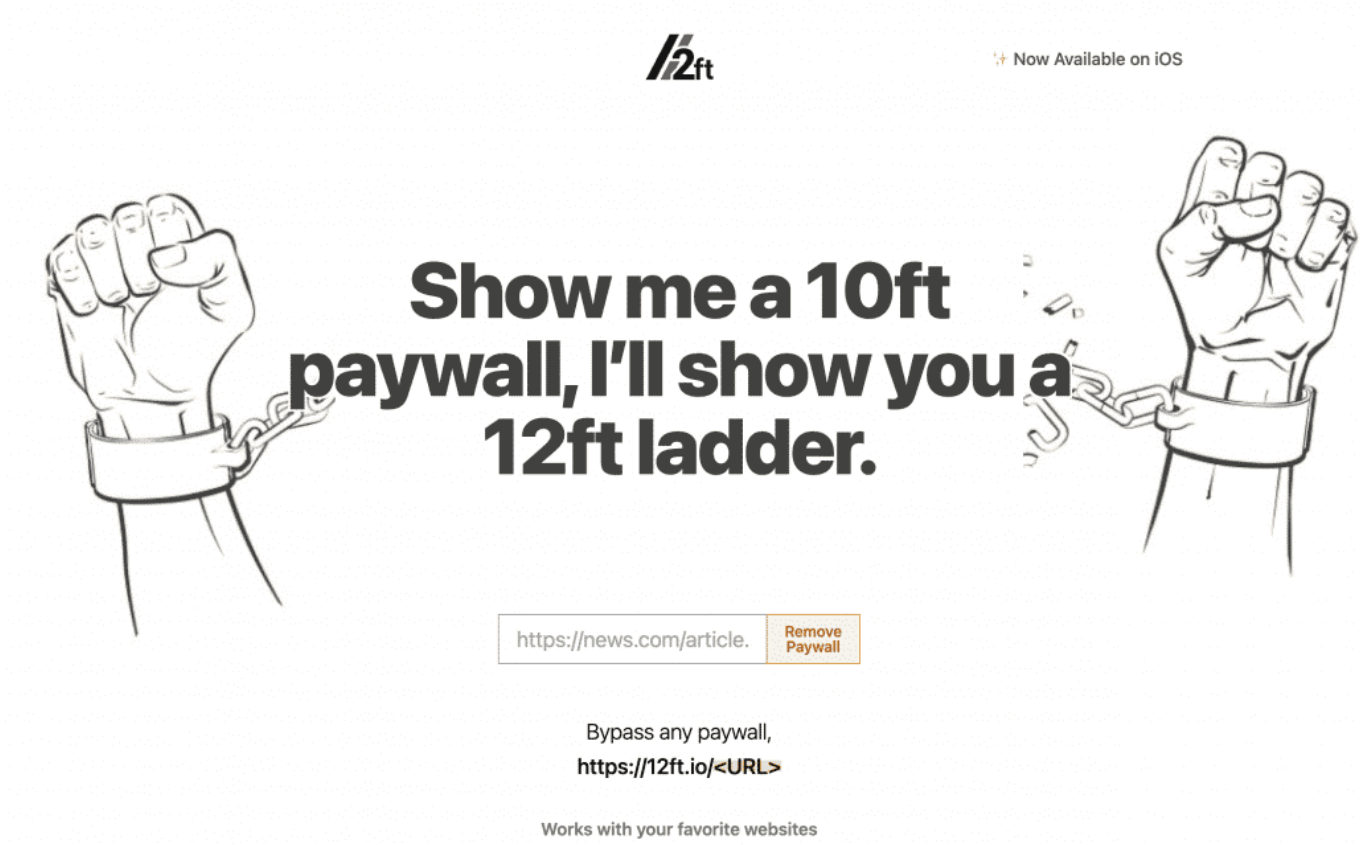
Deshalb gehen die meisten Verlage heute diesen Weg: Kostenlose Nutzung mit Werbung - und wer für Inhalte zahlt, bekommt nicht nur Artikel ohne Werbung zu sehen, sondern auch Artikel und Inhalte, die - zumindest teilweise - exklusiv zahlenden Lesern zur Verfügung stehen.

Solche Artikel liegen hinter der sogenannten "**Paywall**", der Bezahlschranke.

Kennen wir alle: Wir googeln etwas, stoßen auf einen aktuellen interessanten Artikel - doch der wird nur angerissen. Um ihn komplett zu lesen, müssten wir ein Abo abschließen.

Die Verlage und Inhalteanbieter "zeigen" den Suchmaschinen die kompletten Artikel, obwohl sie hinter der Paywall liegen. Deshalb weiß Google, was in einem Artikel steht - und schickt die Leute im Zweifel hin.

Aber wer den Artikel lesen will, bleibt an der Paywall hängen.




## 12ft zeigt Artikel hinter der Paywall

Für dieses Dilemma gibt es eine Lösung: Nutzt in solchen Fällen ist das praktische Online-Tool https://12ft.io/ sehr hilfreich. Ihr müsst einfach die URL (die Webadresse) des geschützten Artikels vorher im Browser in der Adresszeile kopieren und hier bei 12Feet wieder einsetzen. Bei vielen Angeboten sorgt 12Feet dafür, dass Ihr den Artikel danach problemlos hinter der Firewall lesen könnt.

Es klappt oft, aber nicht immer! Probiert es also aus.

Ich mache diesen Tipp mit einem "Aber", denn prinzipiell habe ich absolutes Verständnis dafür, dass Inhalteanbieter Geld verdienen müssen. Ernsthaft zu erwarten, alles müsse kostenlos sein (also gegen Bezahlung, denn man bezahlt ja mit Daten und Werbezeit), ist nicht in Ordnung. Bezahlt für gute Inhalte! Aber für einzelne Ausnahmen und Texte ist dieses Angebot sicher interessant!

# Eine individuelle Website kostenfrei erstellen


**Eine Website ist die Visitenkarte eines jeden Unternehmens, entsprechend viel Wert sollen Sie darauf legen diese professionell zu erstellen und auch laufend zu pflegen. Dabei muss eine professionelle Website nicht teuer sein, mit ein wenig technischem Geschick können Sie selbst tätig werden und eine professionelle Website erstellen.**

## Was eine moderne Website können muss

Wir leben bekanntlich in einer modernen, schnelllebigen Welt, in der man alle Informationen schnell im Internet findet.

Besonders viele Menschen nutzen für ihre Recherchen nicht mehr klassisch einen PC oder Laptop, sondern sind mobil unterwegs, sei es mit Tablet oder Smartphone. Für Sie ist es daher wichtig eine Website zu haben die responsive ist. Sprich die Darstellung der Inhalte muss sich automatisch dem Endgerät anpassen können. Alles andere ist nicht mehr professionell und potenzielle Kunden könnten Ihre Website schnell wieder verlassen.

Natürlich muss die Website auch zu Ihnen, beziehungsweise zu Ihrem Unternehmen, passen. Individuelle Designs sollten daher auf jeden Fall möglich sein und für einen professionellen Gesamteindruck sind entsprechend passende Themes schon fast ein Muss. Themes sind Layoutvorlagen, die durchgestaltet sind und somit ein einheitliches Design ergeben, zum Beispiel eine immer gleiche Überschriftengröße, ein gleicher Zeilenabstand, die gleiche Schriftfarbe, usw.

Zum guten Standard sollten dann auch SEO-Anpassungen gehören, die eine gewisse Suchmaschinenoptimierung ermöglichen, sodass Ihre Website im Ranking weiter vorn erscheint bei Suchen.

## All das muss nicht viel kosten

Wenn Sie sich diesen kleinen Auszug eines Anforderungskataloges anschauen, könnten Sie den Eindruck gewinnen, da kommen hohe Summen auf Sie zu, doch weit gefehlt. Mit wenigen Handgriffen kann man selbst eine kostenlose Website erstellen, die professionell ist und genannte Anforderungen in der Regel erfüllt. Außerdem haben sie in der Regel ein einfach zu verstehendes Content Management System (CMS), über das die Seite verwaltet wird.

Dazu ist es allerdings wichtig ein gewisses technisches Verständnis mitzubringen, denn die Website muss dann von Ihnen in einem Online Tool erstellt werden. Mit relativ wenigen Handgriffen und wenig Aufwand bekommt man dann allerdings ein gutes Ergebnis.

Verschweigen sollte man allerdings nicht, dass gewisse Extras gesondert bezahlt werden müssen. Wenn man also zum Beispiel noch einen Online-Shop integrieren möchte, kann dies kostenpflichtig werden. Einige Anbieter bieten auch passende E-Mail-Adressen an, die den Namen der Domain beinhalten, diese können kostenpflichtig sein. Wichtig ist, dass Sie sich beim Anbieter entsprechend erkundigen, was kostenfrei ist und was gegebenenfalls kostenpflichtig werden könnte.

## Wichtige Basics für den Betrieb einer Website

Mit Sicherheit werden Sie sich über Websites bereits erkundigt haben und einige Ideen haben, wie Ihre Website aussehen soll. Man sollte sich dazu auch viele Gedanken machen, denn wie bereits erwähnt, ist die Website quasi Ihre Visitenkarte.

Wer seriös und professionell auftritt, sollte dies auch auf seiner Website machen. Ein durchdachtes Design, bei dem professionelle Bilder verwendet werden, ist da nur der Anfang. Natürlich sollte die Seite auch sicher sein, sprich mit HTTPS das gängige sichere Übertragungsprotokoll verwenden. Das entsprechende Sicherheitszertifikat kann man in der Regel schnell mit der Website erwerben.

Weiterhin ist es natürlich wichtig sich über die Texte auf seiner Homepage Gedanken zu machen, denn die sollten gut geschrieben und vor allem frei vom Rechtschreib- und Formulierungsfehlern sein. Dazu passt, die Texte auch aktuell zu halten und damit regelmäßig zu prüfen. Wenn Sie ein Unternehmen haben das in den Sozialen Medien, wie Facebook oder Instagram, vertreten ist, sollten Sie dies auch auf Ihrer Website öffentlich machen. In der Regel lassen sich entsprechende Icons schnell einbauen und entsprechend verlinken.

## Ein Fazit

Professionelle Websites kann man sich von entsprechenden Agenturen erstellen lassen und dort auch verwalten lassen. Wer allerdings nur eine kleinere Präsenz im Internet benötigt, kann diese aber auch selbst und vor allem kostenfrei erstellen. Erkundigen Sie sich nach den Möglichkeiten, ein Vergleich lohnt sich.

# Tracking in Microsoft Edge verhindern

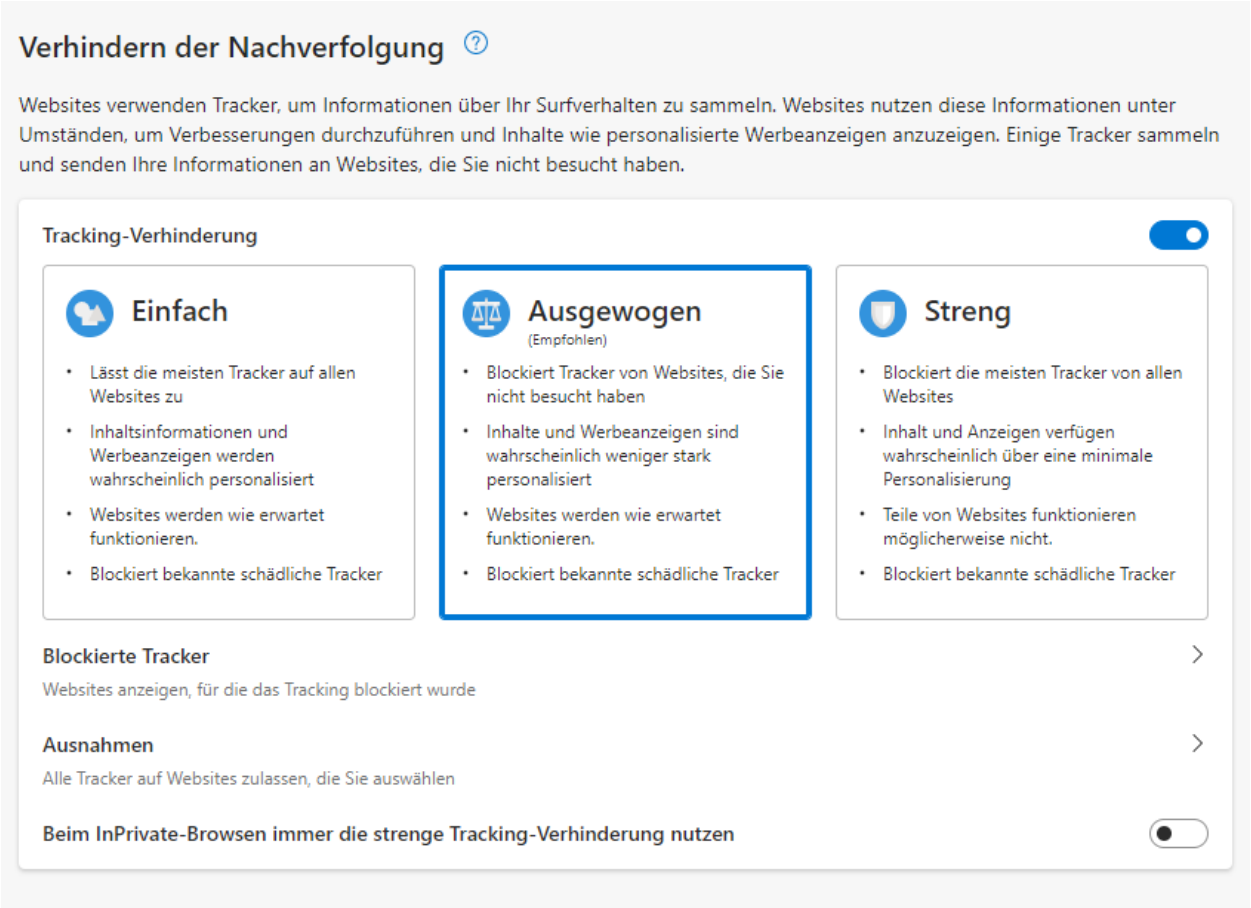
Die Währung des Internets: Eure Daten. Wenn Ihr möglichst wenig über Euer Surfverhalten preisgeben wollt: Nutzt die Anti-Tracking-Mechanismen von Microsoft Edge!

Wenn Ihr im Internet surft, dann habt Ich - für Euch unsichtbar - eine Menge an Daten im Gepäck: Den verwendeten Browser, das Betriebssystem, die Auflösung, installierte Schriftwarten, die Cookies und eine Menge mehr an Informationen, die alleine keinen Rückschluss erlauben. Zusammengenommen aber erlauben Sie eine Identifikation des Nutzers und damit die Verfolgung über Webseiten hinweg. Euer Einkaufsverhalten, Eure aus den besuchten Seiten abgeleiteten Interessen, all das wird ausgewertet.

Microsoft Edge bietet im Standard schon einen sehr ausgeklügelten Trackingschutz:

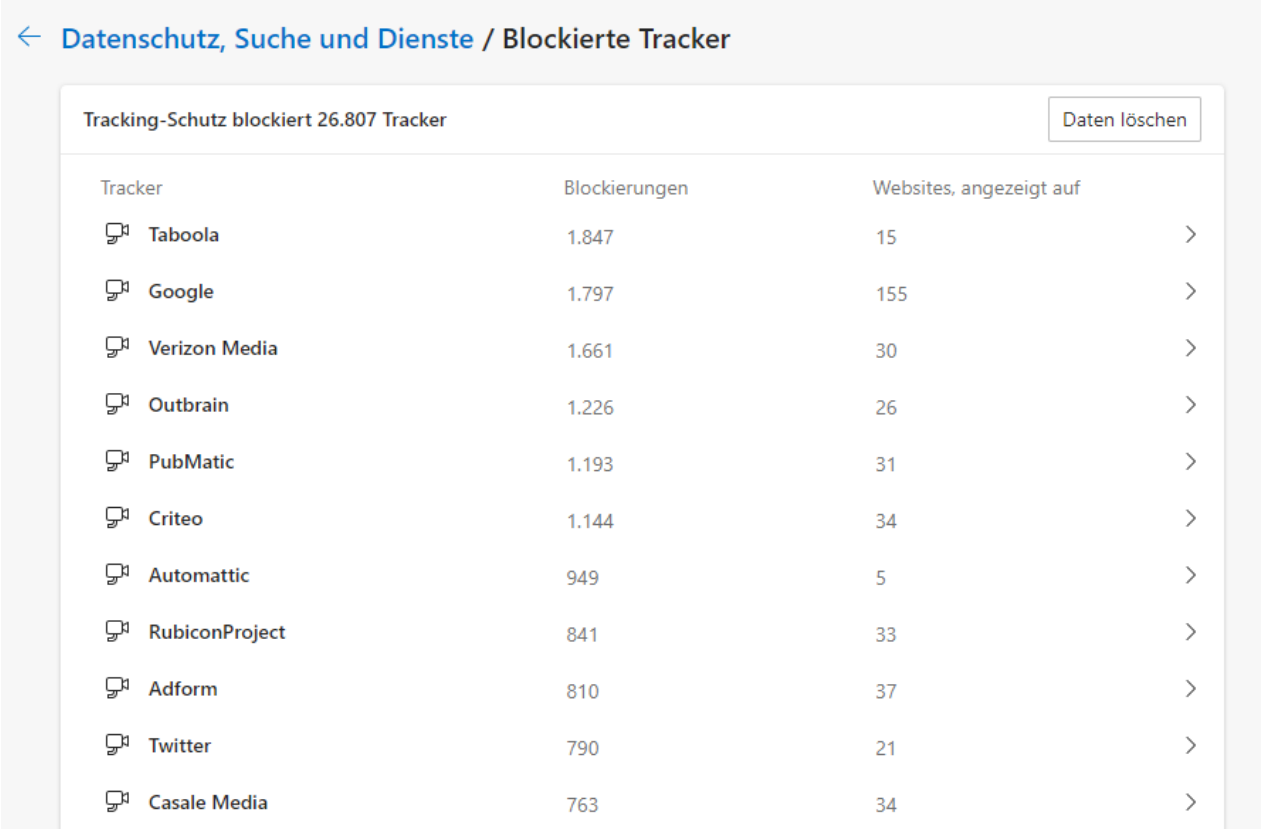
- Klickt in den Einstellungen auf **Datenschutz, Suche und Dienste**.
- Aktiviert die Option **Trackingverhinderung**.

- Empfohlen wird die Einstellung **Ausgewogen**, damit versucht Edge, eine Balance zwischen Schutz und Nutzbarkeit der Webseiten einzustellen.




Wenn Ihr Webseiten besucht, auf denen Ihr eher einen hohen Schutz haben wollt, dann werdet Ihr im Normalfall sowieso den **Privaten Modus** nutzen. Aktiviert in den Einstellungen von Edge **Beim InPrivate-Browsen immer die strenge Tracking-Verhinderung nutzen**, dann erhöht Ihr den Tracking-Schutz, ohne Euch auf normalen Seiten allzu sehr einzuschränken.

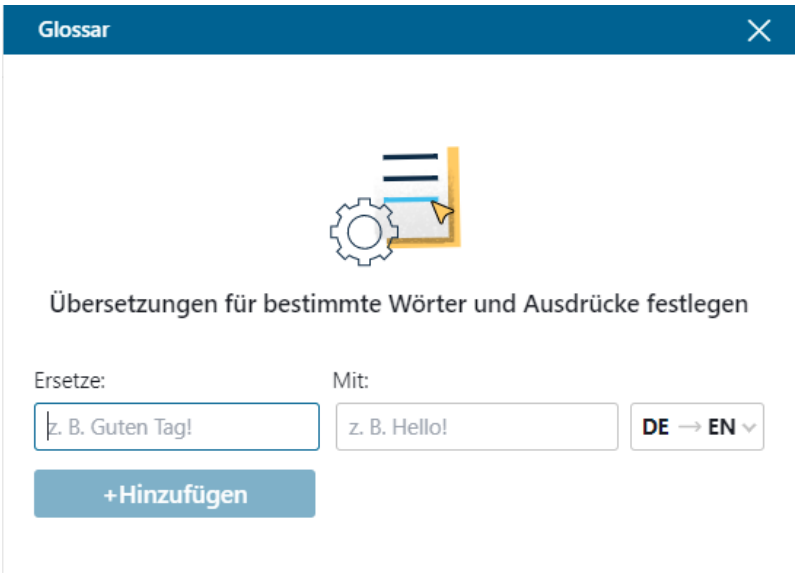
Wenn Ihr sehen wollt, welche Seiten Euch besonders intensiv verfolgen wollen, dann klickt auf den Pfeil neben **Blockierte Tracker**. Hier seht Ihr pro Tracker die Seiten, die ihn verwenden. Im Durchschauen findet Ihr schnell heraus, welche Internetseiten dauernd in der Liste auftauchen. Überlegt, diese zu meiden.


Datenschutz, Suche und Dienste / Blockierte Tracker
Tracking-Schutz blockiert 26.807 Tracker
Daten löschen
Tracker
Blockierungen
Websites, angezeigt auf
Taboola 1.847 15
Google 1.797 155
Verizon Media 1.661 30
Outbrain 1.226 26
PubMatic 1.193 31
Criteo 1.144 34
Automattic 949 5
RubiconProject 841 33
Adform 810 37
Twitter 790 21
Casale Media 763 34

# Feste Begriffsübersetzungen in DeepL: Das Glossar


Übersetzungsprogramme wie DeepL sind durch Maschine Learning immer besser geworden. Perfekt sind sie aber nicht. Wenn Ihr für bestimmte Begriff eine spezielle Übersetzung in der Zielsprache habt, nutzt das Glossar!

Eine Übersetzung kann schwer perfekt sein, wenn eine Maschine sie durchführt. So gut die Algorithmen auch sind, der Zusammenhang eines Satzes und seiner Elemente hat Einfluss auf die beste Übersetzung, das kann eine Maschine nur schwer einordnen. Oft übersetzt Ihr Texte, in denen bestimmte Begriffe in dem Zusammenhang eine feste Übersetzung haben. Das Glossar von DeepL erlaubt es Euch, diese festen Begriffspaare zuzuordnen.



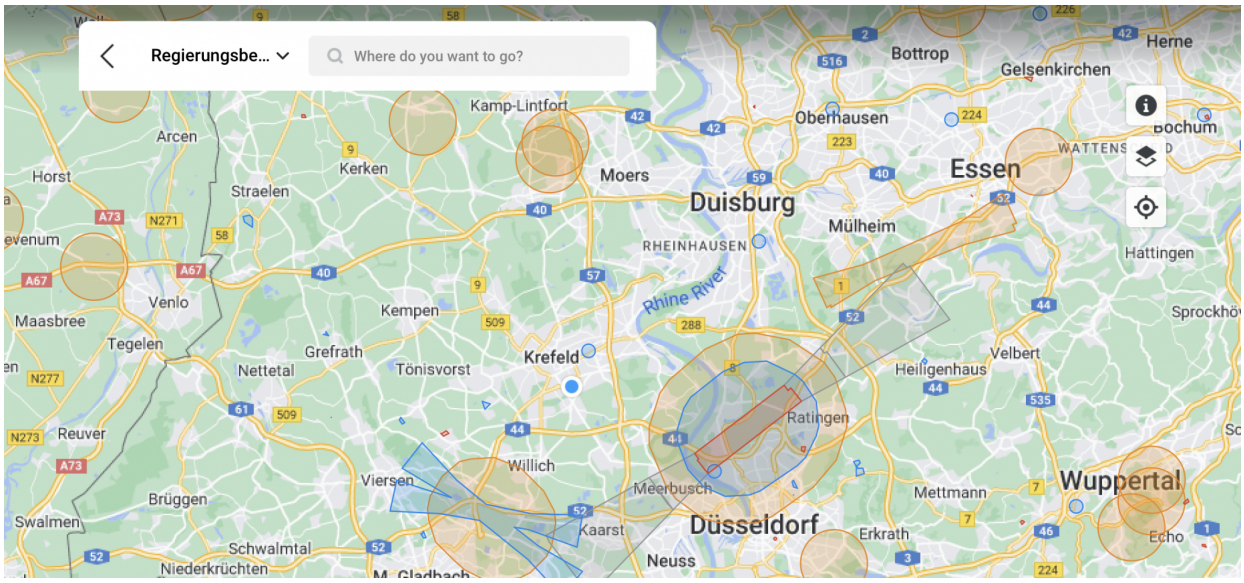

- Wenn Ihr noch kein DeepL-Konto habt, legt kostenlos eines an, dann wird das Glossar auch gespeichert.
- Dazu klickt im Deepl-Fenster (in der Web-App oder der Desktop-Version) rechts oben auf **Glossar**.
- Unter **Ersetze** gebt den Begriff der Quellsprache, unter **Mit** den der Zielsprache ein.
- Rechts daneben müsst Ihr festlegen, welche die Quell- und die Zielsprache sind, DeepL bietet hier "nur" eine begrenzte Auswahl von Kombinationen.

Bei einer Übersetzung in einem Sprachpaar, für das ein Glossar existiert, werden nur die Begriffe so übersetzt, wie Ihr sie zugeordnet habt. Wenn Ihr einen der kostenpflichtigen Pläne verwendet, dann könnt Ihr statt der manuelle Eingabe der Wortpaare direkt eine CSV-Datei mit allen Begriffen hochlanden. In der kostenlosen Version geht das nicht.

# Drohnenführerschein: Teuer muss nicht sein!

Drohnen sind und bleiben ein beliebtes Diskussionsthema. Darf man sie noch fliegen? Unter welchen Voraussetzungen? Im Internet tummeln sich viele Anbieter, die Euch gleich teure Prüfungen aufschwatzen wollen. Hier solltet Ihr vorsichtig sein!

War das Fliegen einer Drohne früher noch cool und aufregend, so sind über die Zeit immer mehr Einschränkungen dazugekommen. Die Menschen um Euch herum reagieren zunehmend gereizt, und spätestens seit Anfang 2021 ist mit der EU-Drohnenverordnung auch noch ein neuer Rechtsrahmen hinzugekommen. Diese fordert für manche Drohnen einen Führerschein, also ein offizielles Dokument.




Das führt schnell dazu, dass findige Anbieter Euch einen kostenpflichtigen Kurs inklusiv einer Prüfung aufschwatzen wollen. Oft deutlich mehr, als Ihr brauchen würdet! Was wirklich nötig ist, findet Ihr immer aktuell auf der Seite des Luftfahrt-Bundesamtes (LBA).

In jedem Fall müsst Ihr Euch als Betreiber registrieren (die so genannte UAS-Betreiberregistrierung), sobald Eure Drohne eine Kamera hat. Dabei bekommt Ihr eine eID zugeordnet, mit der Ihr eindeutig identifizierbar seid. Auch eine Haftpflichtversicherung ist zwingend.

Der "kleine Drohnenführerschein" ist nur dann nötig, wenn Eure Drohne ein Startgewicht von 250 Gram und mehr hat. Das ist auch der Grund, warum viele der am Markt befindlichen Drohnen auf den Punkt 249 Gramm auf die Waage bringen: Für die ist nach der ersten Version der Drohnenverordnung kein Drohnenführerschein nötig. Auch für die größeren Drohnen wie die Mavic-Reihe von DJI hängt die Notwendigkeit eines Führerscheins vom Einsatzgebiet ab: Sie fallen in die Offene Kategorie, die sich nochmal aufteilt. Mit entsprechendem Abstand zu Wohn- Gewerbe- und Industriegebieten lassen sich diese immer noch mit dem kleinen Drohnenführerschein fliegen.

Den könnt Ihr online für EUR 25,- direkt beim Luftfahrtbundesamt ablegen, einen kostenlosen Vorbereitungskurz findet Ihr ebenfalls auf der Seite.

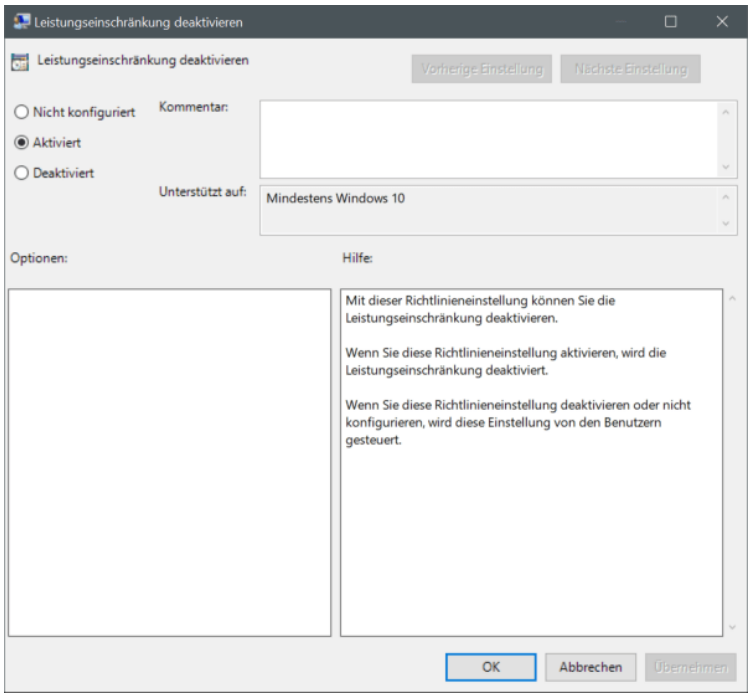
# Langsame Surface Books und Laptop Studio beschleunigen

Das Surface-Gerät ist langsam? Das kann mehrere Ursachen haben, bei den Surfaces und manchen anderen Geräten aber auch eine ganz spezielle, nämlich einen Fehler in der Firmware.

Die Geschwindigkeit eines Notebooks ist von vielen Faktoren abhängig. Die verbaute Hardware, die laufenden Programme, Auslastung des Speichers, all diese Dinge können dafür sorgen, dass ein Gerät langsamer als gewohnt ist. Auch das Netzwerk-Throttling, bei dem der Datendurchsatz im Netzwerk zu Gunsten der Akku-Laufzeit gebremst wird, kann eine Ursache für einegschränkte Performance sein. Bei den Surface-Geräten allerdings kann es spezifische

Ursachen haben, die nicht immer durch den Anwender lösbar sind.

Zum einen ist das so genannte Power-Throttling ein Problem. Dabei wird der Prozessor des Geräts gebremst, weil das zu geringerem Stromverbrauch führt. Das erhöht die Laufzeit im Batteriebetrieb, ist aber bei dem einen oder anderen Programm nicht hilfreich. Das Gerät läuft dann einfach zu langsam und die Anwendung ruckelt. Das zu beheben ist relativ leicht, wie Ihr in diesem Artikel lesen könnt.




Manche Surface-Geräte aber haben ein Firmware-Problem, das zu einer Verlangsamung führt: Der Hersteller hat in die Firmware einen fehlerhaften Wert geschrieben, der dem System vorgaukelt, dass es zu warm sei. Hier hilft keine Einstellung, die Ihr im System vornehmen können. Das so genannte "Throttle-Gate" kommt geräteübergreifend immer mal wieder vor. Nur der Hersteller selber kann durch ein korrigiertes Firmware-Update helfen. Wenn Ihr alle anderen Möglichkeiten für eine Verlangsamung ausgeschlossen habt: Sucht im Internet nach dem Begriff Throttle-Gate und dem Namen Eures Gerätes. Findet Ihr dazu aktuelle Erwähnungen, dann bleibt nichts anderes als Abwarten.

# Mehr Cybersicherheit: Nancy Faeser will Grundgesetzänderung

***Bundesinnenministerin Nancy Faeser hat neue Maßnahmen gegen Cyberangriffe vorgestellt – auch und vor allem vor Angriffen aus Russland. Es geht vor allem darum, die kritische Infrastruktur zu schützen. Dafür soll der Bund deutlich mehr Befugnisse bekommen. Die Forderungen stoßen teilweise auf Entsetzen.***

Schon lange ist klar: Deutschland ist vergleichsweise schlecht gerüstet gegen Cyber-Angriffe jeder Art. In der jüngsten Vergangenheit wurden reihenweise Krankenhäuser, Behörden und ganze Kommunen mit Ransomware-Angriffen lahmgelegt: Schad-Software, die wertvolle Daten verschlüsselt und IT-Infrastruktur in die Knie zwingt.

Aber auch Cyber-Spionage und mögliche Angriffe auf kritische Infrastruktur

nehmen zu – nicht zuletzt durch den Ukraine-Konflikt.

## Bedrohungslage nimmt laut Behörden zu

Immer wieder warnen Behörden wie der Bundesverfassungsschutz oder das „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) vor erhöhten Bedrohungslagen, insbesondere durch russische Hacker-Kollektive.

Bundesinnenministerin Nancy Faeser (SPD) hat heute (12.07.2022) einen umfassenden Maßnahmenkatalog vorgestellt. In der „Cybersicherheitsagenda des Bundesministeriums des Inneren und für Heimat“ sind auf knapp 14 Seiten die Maßnahmen zusammengefasst.

In Berlin hat die Bundesinnenministerin eine bessere Ausstattung der Sicherheitsbehörden versprochen. So soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu einer Zentralstelle zwischen Bund und Ländern ausgebaut werden. Gestärkt werden sollen außerdem Verfassungsschutz und Bundeskriminalamt.

## Faeser schlägt Grundgesetzänderung vor

Nancy Faeser hat sogar eine Grundgesetzänderung vorgeschlagen, um das ihrem Haus unterstellte „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) zur zentralen Koordinierungsstelle auszubauen.

Die Verantwortung für Cybersicherheit liege aktuell noch bei den Ländern, argumentiert die Bundesinnenministerin. Das BSI könne da im Bedarfsfall immer nur Amtshilfe leisten. Die Bundesländer seien mit der Aufgabe langfristig aber „überfordert“. Das würde sich ändern, wenn die Befugnisse anders aussehen – dazu sei aber eine Grundgesetzänderung erforderlich. Beim BSI soll eine Plattform für den Austausch von Informationen zu Cyberangriffen entstehen.

Sinnvoll wäre zweifellos, das noch weiterzudenken: Europaweit. Denn kritische Infrastruktur macht weder an Landesgrenzen, noch an Bundesgrenzen halt. Russische Angreifer haben häufig eine Destabilisierung ganz Europas zum Ziel. Das gilt vor allem für gezielte Desinformationskampagnen, die in der Regel europaweit erfolgen – und ebenfalls ins Visier genommen werden sollen.

## Mehr Cyber-Resilienz

Angesichts des aktuellen Angriffskriegs durch Russland gegen die Ukraine hat das Bundesinnenministerium zudem weitere Maßnahmen für mehr Cybersicherheit vorgestellt. Darunter die Einführung eines zentralen Videokonferenzsystems für die Bundesverwaltung, das höchsten Sicherheitsanforderungen entspricht – und Abhörsicherheit garantieren soll.

Ebenfalls geplant: Wesentliche Investitionen in Maßnahmen zur sogenannten „Cyber-Resilienz“ bei kleinen und mittleren Unternehmen, sofern diese zur „kritischen Infrastruktur” gehören. Dazu zählen unter anderem Branchen wie Verkehr, Gesundheit, Energie, Ernährung und Wasserversorgung. Unter Cyber-Resilienz wird verstanden, dass IT-Systeme nicht gleich unter jeder Attacke zusammenbrechen – und selbst dann weiter arbeiten, wenn auch unter den sonst üblichen Möglichkeiten, wenn ein Angriff oder ein Problem vorliegt. In diesem Punkt gibt es enormen Nachholbedarf.

## Kritik an umfassenden Plänen

Zudem hat Nancy Faeser Pläne zur Modernisierung der IT-Infrastruktur des Bundesamtes für Verfassungsschutz vorgestellt. Es solle auch mehr Befugnisse

zur „Aufklärung technischer Sachverhalte bei Cyberangriffen fremder Mächte” erhalten

Wie sich die Ziele alle konkret umsetzen lassen, hat die Bundesministerin nicht verraten. Manuel Atug, IT-Sicherheitsexperte und Mitglied des Chaos Computer Club (CCC), befürchtet aufgrund der geplanten neuen Befugnisse und finanziellen Mittel nun eine regelrechte Welle an neuer Überwachungstechnologie: „Da ist alles drin und möglich, von der Chat-Kontrolle über Predictive Policing bis hin zu flächendeckender Gesichtserkennung à la Clearview AI“, sagt der Experte von der AG Kritis, die für den Schutz kritischer Infrastruktur zuständig ist. „Kompletter Wahnsinn“, ergänzt Atug im persönlichen Interview noch.

# Kommentar: Nancy Faeser will mehr Cybersicherheit

**Bundesinnenministerin Nancy Faeser will mehr Cyber-Sicherheit in Deutschland: Das ist gut so - auch, dass sie dem "Bundesamt für Sicherheit in der Informationstechnik" (BSI) mehr zutraut und mehr Bedeutung geben will. Aber Behörden wie BKA oder Verfassungsschutz müssen mit Augenmaß erweitert werden. Hier ist mehr und bessere Kommunikation erforderlich!**

Ja, wir alle in Deutschland sind ein leichtes Opfer – Privatpersonen, Unternehmen, Institutionen. Wir sind ein allzu leichtes Opfer für Cyber-Kriminalität jeder Art. Denn wir sind schlecht vorbereitet, miserabel geschult, schlecht informiert und alles andere als wehrhaft. Viel zu lange haben wir alle, aber ganz besonders Behörden und Politik die Gefahr aus dem Netz nicht ernst genug genommen.

Das will Bundesinnenminister Nancy Faeser nun erkennbar ändern. Das nehme ich ihr ab. Sie will die Behörden stärken, besser ausstatten und ausrüsten – und mit den nötigen Befugnissen ausstatten.

## Das BSI bekommt mehr Kompetenzen

Das „Bundesamt für die Sicherheit in der Informationstechnik“ (BSI) zum Beispiel soll dabei eine zentrale Bedeutung bekommen. Das ist gut so, denn das BSI ist kompetent – aber nur selten befugt. Denn Cyber-Abwehr, selbst bei kritischer Infrastruktur, ist oft Ländersache.

Völliger Unsinn, völlig unzeitgemäß. Das auf Bundesebene zu hängen ist richtig – auch wenn dafür eine Grundgesetzänderung nötig ist. Im Grunde müsste die Ministerin das sogar noch größer denken: Europaweit. Denn insbesondere Angriffe aus russischen Cyber-Lagern greifen häufig ganz Europa an. Die Gesellschaft. Den Zusammenhalt. Aber auch die kritische Infrastruktur, sie macht an den Bundesgrenzen nicht halt.

Dem BSI mehr zuzutrauen ist richtig und gut. BKA und Bundesverfassungsschutz mit mehr Kompetenzen auszustatten, scheint auch richtig und wichtig. Allerdings muss das mit Augenmaß geschehen. Hier hat Faeser heute nicht gesagt, was alles geplant ist. Einige Kritiker befürchten nun einen Freifahrtschein für Trojaner, Überwachung, Gesichtserkennung, aufgeweichte Verschlüsselung in der Kommunikation, vielleicht sogar Massenüberwachung.

## Das BSI bekommt mehr Kompetenzen

Zuletzt waren Pläne der EU umstritten, Chats von ganz normalen Menschen zu scannen. Nicht alles, was aus Sicht der Behörden sinnvoll ist, ist für eine Gesellschaft gesund. Güterabwägung, Transparenz und Augenmaß sind wichtig.

Leider hat Nancy Faeser nichts zu solchen konkreten Plänen gesagt – oder auch dazu, wie diese Herausforderungen gemeistert werden, ohne das wichtige Vertrauen zu verspielen.

# Deal geplatzt: Rückzieher von Elon Musk könnte Twitter lähmen


**Es hat sich in den letzten Wochen bereits abgezeichnet: Tech-Milliardär Elon Musk will Twitter nun doch nicht kaufen und lässt die 44-Milliarden-Dollar-Vereinbarung platzen. Das will sich Twitter nicht gefallen lassen und hat gerichtliche Schritte angekündigt. Den Schaden hat Twitter - so oder so.**

Nun wird deutlich, wieso Elon Musk seit Wochen auf Twitter selbst die offiziellen Zahlen des Kurznachrichten-Dienstes anzweifelt: Der Tech-Milliardär, der mit der Gründung von Paypal reich und durch Tesla und ambitionierte Pläne mit seinem Weltraumunternehmen SpaceX überall auf der Welt bekannt geworden ist (Musk will den Mars bevölkern), hat sich offiziell zurückgezogen: Wie seine Anwälte am Freitag der US-Börsenaufsicht SEC mitgeteilt haben, will Musk die schriftlich vereinbarten 44 Milliarden Dollar nicht zahlen.

## Streit um die Zahl der Fake-Accounts

Begründung: Twitter habe ihm über die wahre Geschäftstätigkeit im Unklaren

gelassen. Seit Wochen geht es um die Frage, wie viele sogenannte Fake-Accounts auf Twitter existieren. Accounts also, die nicht von echten Menschen geführt und gefüttert werden, sondern von Bots und Programmen. Solche Accounts sorgen zwar auch für Inhalte, aber nicht für Umsatz: Sie kaufen nichts, klicken keine Werbung an.

Die Geschäftsleitung von Twitter beharrt darauf, es seien weniger als 5 Prozent Fake-Accounts. Der reichste Mensch der Welt sieht es anders und hält diese Zahl für zu gering – freilich ohne konkrete Belege zu nennen. Am Ende wäre es nicht einfach, die Zahl der Fake-Accounts mit absoluter Gewissheit zu bestimmen. Denn viele Bots sind heute so gut programmiert, dass sie sich wie echte Menschen verhalten – etwas nur zu bestimmten Zeiten twittern –, schon allein, um nicht von Schutz-Algorithmen enttarnt und möglicherweise geblockt zu werden.

## Aktienkurs von Twitter unter Druck

Musks Anwälte erklärten nun, Twitter habe es seit nun beinahe zwei Monaten versäumt, valide Daten zur Verifizierung der Angaben zu Fake-Accounts zu liefern. Sie bezeichnen das als einen derart schweren Bruch der Vertragsbedingungen, dass sie die vor Monaten getroffene Kaufvereinbarung auflösen – was nach den Vertragsbedingungen der Vereinbarung auch möglich sei.

Der Aktienkurs von Twitter ist im Anschluss im fünf Prozent gefallen.

Bereits im vergangenen Jahr (Juni 2021) hat der Hackerverbund Anonymouw Elon Musk für seine Aktivitäten und vor allem auch für die Arbeitsbedingungen bei Tesla krisitiert.

## Zeitaufwändige gerichtliche Klärung

Nun droht Twitter damit, die Sache gerichtlich klären zu lassen: Wenn schon die geplante Übernahme nicht erfolgt, dann soll zumindest die Vertragsstrafe von einer Milliarde Dollar von Elon Musk gezahlt werden. Das wiederum will Elon Musk verhindern. Es droht ein langwieriger und teurer Rechtsstreit, den sich Elon Musk wohl eher leisten kann als Twitter. Der Zwitscher-Dienst ist wirtschaftlich nicht sonderlich erfolgreich, da es wenige Innovationen gibt.

## Das Netz spekuliert über die wahren Absichten

Nun spekulieren Experten – natürlich auf Twitter –, was das alles zu bedeuten hat. Der bekannte US-Analyst Dan Ives zum Beispiel sagt deutlich, Elon Musks Plan, Twitter für 44 Milliarden Dollar zu kaufen, sei von Anfang an rätselhaft für ihn gewesen und habe für die Wall Street auch „nie viel Sinn ergeben“.

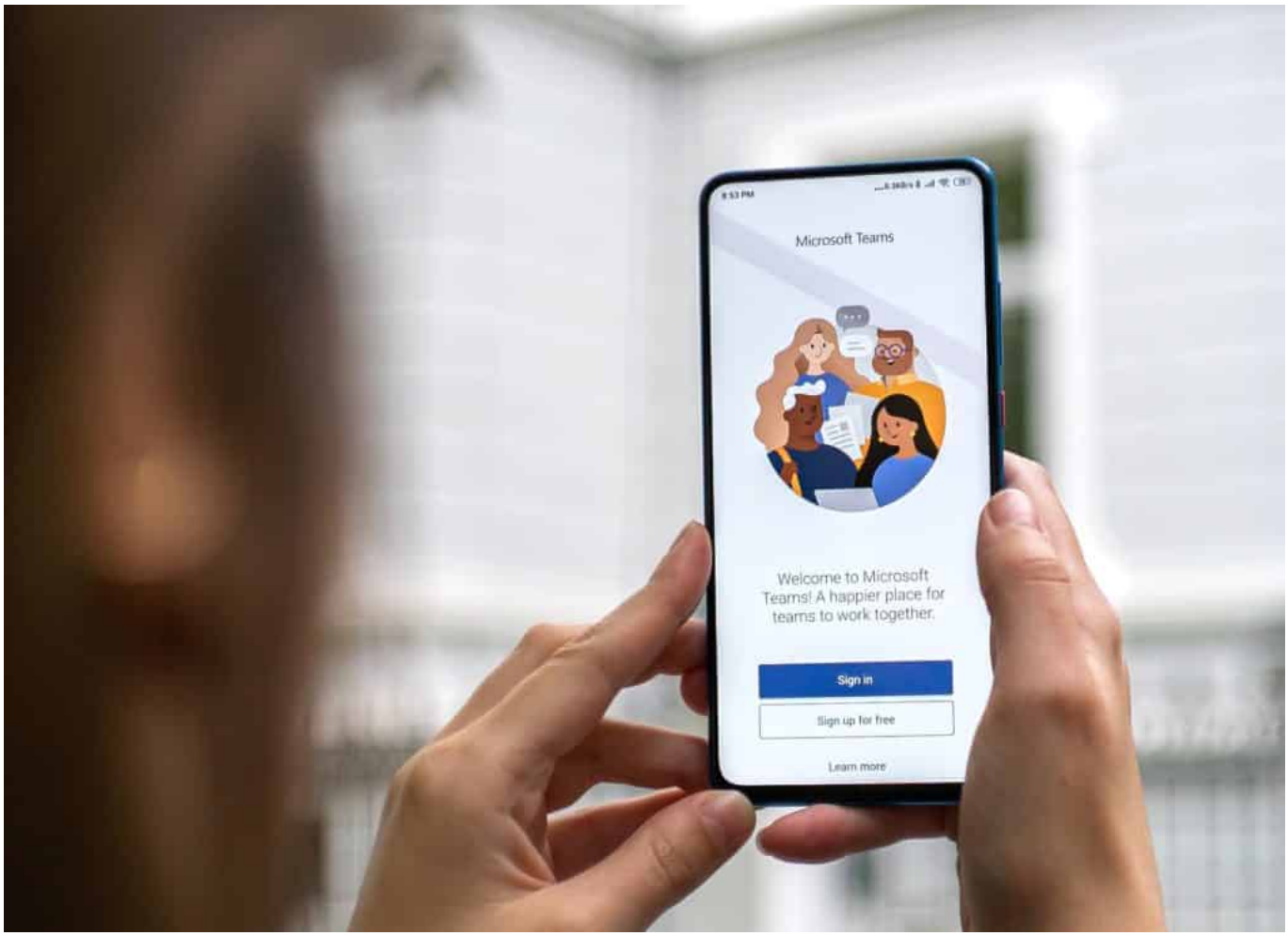
Es ist allerdings nicht auszuschließen, dass Musk immer noch an Twitter interessiert ist, aber den Kaufpreis weiter drücken möchte. Durch den Rechtsstreit kommt Twitter in Bedrängnis – niemand sonst wird im Augenblick eine Übernahme in Betracht ziehen –, nicht Musk. Durch diese Maßnahme könnte sich Elon Musk Hoffnungen auf einen besseren Deal machen: Vielleicht stimmt die Geschäftsleitung angesichts sinkender Aktienkurse einem deutlich geringeren Kaufpreis zu. Es wäre Elon Musk zuzutrauen. Er hat in der Vergangenheit auch häufiger den Bitcoin-Kurs nach oben und unten getrieben.

## Keine guten Nachrichten für Twitter

Elon Musk hatte den Twitter-Aktionären 54,20 Dollar pro Aktie geboten. Ein für die Aktionäre guter Deal: Das war schon zur Ankündigung mehr als der Marktpreis. Nach der „Aus“-Ankündigung am Freitag ging das Papier auf nur 36,81 Dollar aus dem US-Handel.

Für den Kurznachrichten-Dienst Twitter sind das zweifellos keine guten Nachrichten. Es wird in den nächsten Wochen und Monaten nur noch um den Rechtsstreit gehen. Innovationen werden vermutlich auf Eis gelegt – und auch alle anderen, Werbekunden und Nutzer, werden sich fragen, wie es mit Twitter weitergeht und sich mit Investitionen und Projekten eher zurückhalten.

# Risiko: Wenn Apps unbemerkt spionieren




**Seit der Pandemie gehören Videokonferenzen zum Alltag vieler Menschen. Wie Recherchen des Bayerischen Rundfunks zeigen, sollte man die Anwendungen sorgfältig auswählen – und auch im Blick behalten. Denn sie könnten jederzeit unbemerkt die Kamera einschalten und spionieren.**

Spätestens seit der Corona-Pandemie arbeiten viele von uns viel von zu Hause aus. Dabei kommen in der Regel gängige Anwendungen wie Microsoft Teams, Zoom, Webex oder vergleichbare Anwendungen zum Einsatz. Wie selbstverständlich gewähren User hier den Zugriff auf Kamera und Mikrofon, um mit den anderen kommunizieren zu können.

Die meisten gehen davon aus: Kamera und Mikrofon sind nur eingeschaltet und aktiv, wenn die App im Einsatz ist. Aber ist das wirklich so? Oder könnten solche Anwendungen – zumindest theoretisch! – jederzeit, womöglich sogar unbemerkt

Kamera und Mikro aktivieren und so Situationen beobachten oder Gespräche bespitzeln?

## Eine anspruchsvolle Testanwendung

Genau das wollten Journalisten des Bayerischen Rundfunks genauer wissen – und haben ein überaus interessantes Rechercheprojekt auf die Beine gestellt. Sie wollten wissen, ob und unter welchen Umständen Video-Apps zum Risiko werden können. Datenjournalistische Teams von „BR Data“ und „BR AI Automation Lab“ gemeinsam mit Kollegen der Puls-Reportage nachgewiesen: Ja, theoretisch könnten die meisten Kommunikations-Anwendungen jederzeit mithören.

Das Rechercheteam konnte im Versuch belegen, dass Notebook-Programme die Kamera und das Mikrofon jederzeit aktivieren können, um Videos und Gespräche aufzuzeichnen. Ebenso Apps im Smartphone.

Bei dem Versuch wurde nicht etwa der Erweis erbracht, dass Programme wie Microsoft Teams, Zoom oder Webex so etwas tatsächlich machen, sondern erst einmal „nur“, dass es grundsätzlich möglich wäre.

## Demo-App „Cool Chat“ sollte spionieren

Dazu hat Techniker Sebastian Bayerl im Team eine Anwendung namens „Cool Chat“ entwickelt – für die allgemein im Einsatz befindlichen Betriebssysteme Windows, MacOS, iOS und Android. Die App sollte zeigen: Was ist möglich, wenn eine solche Anwendung erst einmal eingerichtet und installiert wurde?

Das Ergebnis: Auf praktisch jedem Gerät war es möglich – zumindest zeitweise! –, selbst dann auf Kamera und Mikrofon zuzugreifen, wenn die Anwendung gar nicht aktuell im Vordergrund aktiv ist. Selbst wenn Probanden die Anwendung offiziell beendet hatten und davon ausgehen konnten, dass die Anwendung nicht mehr aktiv ist, war es Techniker „Sebi“ möglich, Kamera und Mikro aus der Ferne zu aktivieren – und Gespräche zu belauschen. Niemandem fällt das kleine grüne Licht auf, das im Display erscheint, wenn die Kamera aktiv ist.

## Heimliche Gesprächsaufnahmen kein Problem

Auf einem Android-Smartphone war es sogar möglich, die Kamera zu aktivieren, als das Smartphone selbst nicht in Benutzung war – bei ausgeschaltetem Display. Bei älteren Android-Versionen (bis Version 10) ist so etwas tatsächlich noch möglich.

Je nach verwendetem Betriebssystem werden Benutzer nur einmal oder jedes Mal gefragt, ob sie Zugriff auf Kamera und Mikro gewähren. Apples Betriebssysteme bieten nach Erfahrungen der Tests zwar etwas bessere Einstellmöglichkeiten, aber ebenfalls keinen vollständigen Schutz. Auf allen Geräten und unter allen Betriebssystemen war es unter Testbedingungen möglich, unbemerkt Gespräche aufzuzeichnen.

## Auch Bildschirminhalt konnte aufgezeichnet werden

Dasselbe gilt für den aktuellen Inhalt von Bildschirm bzw. Display: Auch darauf konnte der Techniker mehr oder weniger jederzeit zugreifen, selbst wenn die Demo-App „Cool Chat“ nicht im Einsatz war. So etwas ermöglicht es, aktuelle Chat-Inhalte, aber auch Kontakte oder vertrauliche Informationen unbemerkt abzufotografieren – und an Dritte zu übertragen.

Die Pulse-Reportage erklärt sehr anschaulich die Testumgebung – und wie solche Zugriffe möglich sind. Sie zeigt aber auch, wie nachlässig Entwickler von Betriebssystemen noch sind (Microsoft, Google, Apple) – und wie viel noch getan werden muss, damit die Betriebssysteme Anwendungen nicht zu vieles erlauben.

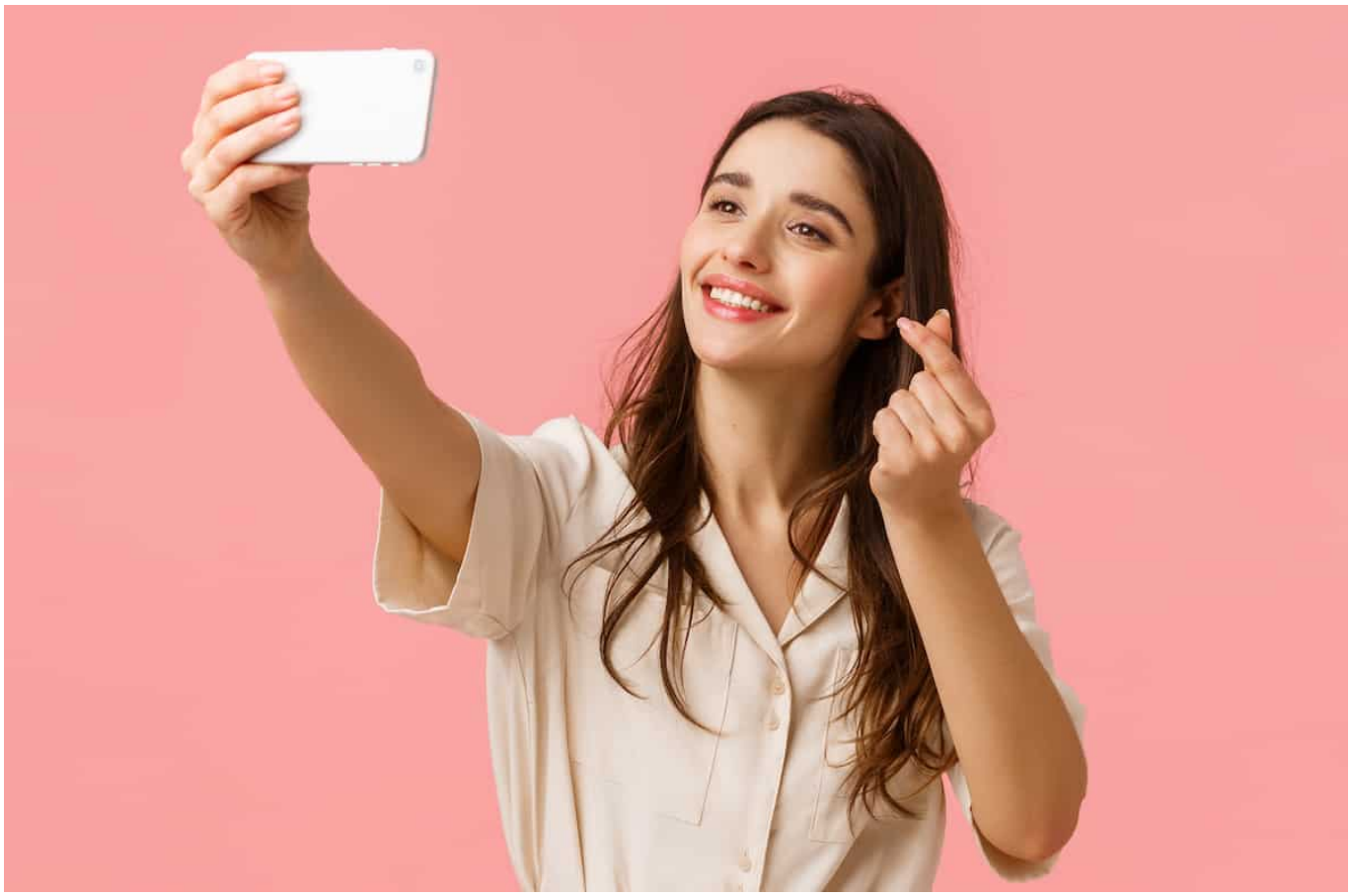
## User müssen Rechte sorgfältig vergeben

Was User lernen können: Anwendungen nicht einfach nur beenden, denn dann könnten sie trotzdem noch aktiv sein. Besser im Task-Manager (Windows) oder in der Aktivitäten-Anzeige (MacOS) schließen oder im mobilen Betriebssystem definitiv beenden. Außerdem Updates laden, um bekannte Sicherheitsprobleme zu schließen.

Wer Anwendungen lädt und benutzt, sollte immer bedenken: Es ist und bleibt Vertrauenssache. Anwendungen und Apps haben eine Menge Möglichkeiten – und könnten spionieren. Deshalb sollte man nur solchen Anwendungen Zugriff auf Kamera, Mikrofon und Display gewähren, bei denen das absolut sinnvoll und nötig ist – und denen man Vertrauen entgegenbringt.

https://www.youtube.com/watch?v=YGKY_F50I_8

# Kommt eine Kennzeichnungspflicht für Fotos mit Beauty-Filter?



**Vor allem auf Instagram gibt es viele Selfies und Fotos zu sehen, die mit Filtern bearbeitet und gepimpt wurden. Das verändert das Körperbild - auf schädliche Weise. Es gibt jetzt Forderungen, Fotos zu kennzeichnen, die mit Filtern nachbearbeitet wurden. Was könnte das bringen?**

Heute schon mal bei Instagram vorbeigeschaut – oder in einer anderen Social Media Plattform Ihres Vertrauens, auf der Selfies und Fotos verteilt werden? Falls ja, sind Sie mit an Sicherheit grenzender Wahrscheinlichkeit bereits auf Fotos gestoßen, die mit Filtern nachbearbeitet wurden.

Aufgehübscht, nachbearbeitet, aufgepimpt: Das ist heute Standard, wenn Fotos gepostet werden. Ganz besonders bei Influencerinnen und solchen, die es sein oder werden wollen. Doch solche aufgepimpten Bilder haben Folgen. Viele junge Menschen, besonders Mädchen und junge Frauen sind unzufrieden mit ihrem

Körper.

Darum überlegt die Politik, etwas zu unternehmen: eine Kennzeichnungspflicht für manipulierte Aufnahmen in Werbung und Social Media. Was ist da geplant und würde das wirklich etwas bringen?

## Politik plant strengere Regeln

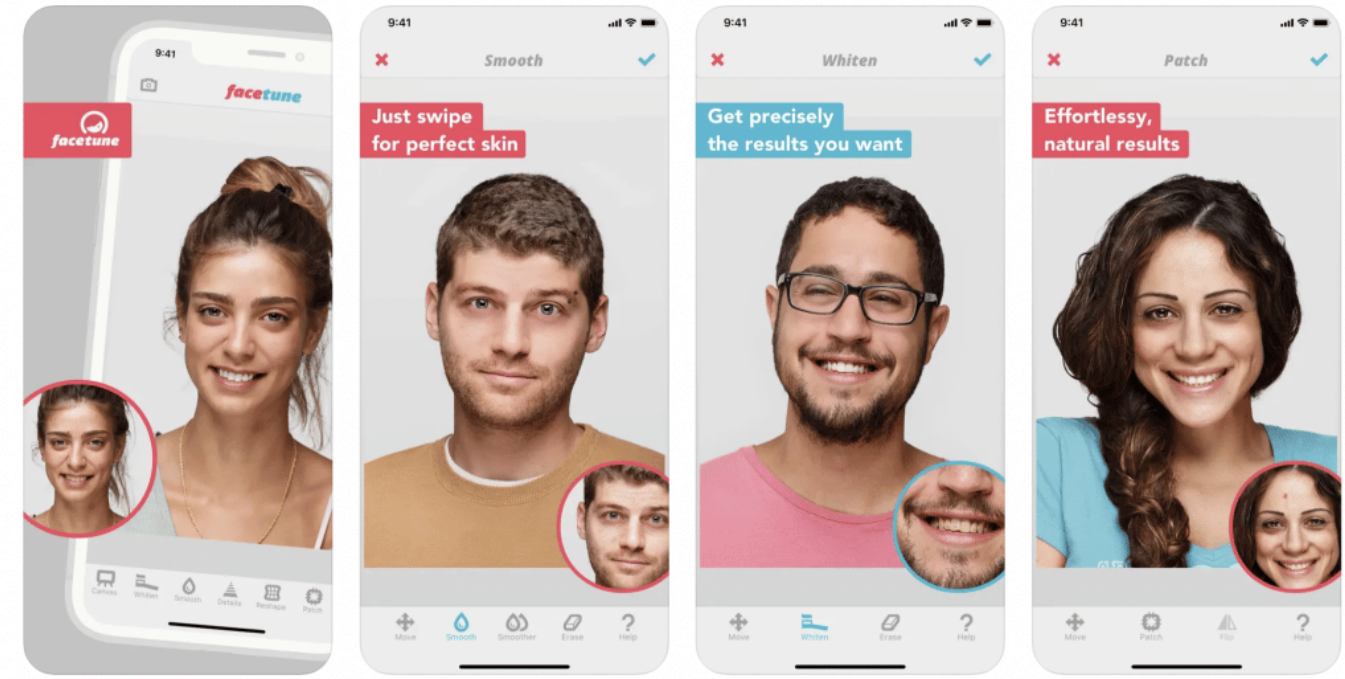
Vor einigen Tagen haben sich die Ministerinnen und Minister für Gleichstellung getroffen – und über die Problematik gesprochen. Sie denken offensichtlich über eine Kennzeichnungspflicht für geschönte Bilder in sozialen Netzwerken bei uns in Deutschland nach. Was steckt dahinter?

Die Politik argumentiert: „Die bei Social Media und in der Werbung eingesetzten Beauty-Filter prägen nachweislich ein unrealistisches Schönheitsideal bei Mädchen und Frauen“. Das Problem ist ja: Man kann heute nicht mehr erkennen, welche Aufnahmen echt sind und welche nachbearbeitet. Es gibt heute Millionen Beauty-Filter, die machen Gesichter schmaler, die Nase kleiner, die Lippen roter, die Haut glatter...

Sowas gibt’s im Profi-Bereich natürlich schon lange, Photoshop hat’s vorgemacht. Aber heute sind solche Filter allgegenwärtig, und jede(r) setzt sie sein. Das verändert natürlich die Wahrnehmung. Vor allem dann, wenn nicht nur die Models in Profiaufnahmen „wie gemalt“ aussehen, sondern auch die sich als „Best Buddy von nebenan“ gebende Influencerin, die trotzdem viel besser aussieht als man selbst.

Wir wissen aus Studien, dass junge Frauen und Mädchen unter diesem Druck leiden. Jede dritte Frau zwischen 11 und 21 Jahren würde kein unretuschiertes Bild von sich hochladen. Die Whistleblowerin Frances Haugen hatte vor einigen Monaten ja auch verraten, dass Facebook von diesem Druck weiß, aber nichts unternimmt.

Die Riege der Gleichstellungsminister hat deshalb mit großer Mehrheit die Bundesregierung aufgefordert, rechtliche Regelungen zur Kennzeichnungspflicht von retuschierten Werbebildern und den Einsatz von Beauty-Filtern einzuführen.




## Wasserzeichen und Kennzeichnungen

Aber wie könnte eine solche Kennzeichnungspflicht denn aussehen? Und wer müsste sie vornehmen?

Wir haben ja gerade schon gehört, wie es in Norwegen gemacht wird. Das ist sicher eine Möglichkeit. Eine solche Kennzeichnung könnte in den Fotos als Wasserzeichen integriert werden („Dieses Foto wurde retuschiert!“), oder es erscheint ein Hinweis in den Social Media Diensten, neben dem Post.

In Frankreich gibt es so etwas auch schon länger. Erlaubt sind dort in Werbung und Social Media nur noch gesamtheitliche Bildbearbeitungen wie Aufhellung, Verdunklung oder Schärfung – aber nicht die Optimierung einzelner Bildteile. Wenn das gemacht wird, ist eine Kennzeichnung erforderlich, etwa wenn Haut oder Körperform verändert wurden, also wenn Filter zum Einsatz kommen, die das Körperbild wirklich maßgeblich verändern.

## Politik plant strengere Regeln

Jetzt ist es ja eine Sache, eine Kennzeichnungspflicht vorzuschreiben. Macht aber vielleicht nicht jeder. Wie gut ließe sich das denn überprüfen, ob alles gekennzeichnet wird, was gekennzeichnet werden müsste?

Das halte ich für einen vergleichsweise schwierigen Punkt. Was wurde durch Licht, Maske oder ein bestimmtes Objektiv erreicht – was durch einen Filter? Darüber würde es vermutlich häufiger Streit geben. Zweifellos kann man Algorithmen entwickeln, die den Einsatz von Filtern erkennen – oder die Wahrscheinlichkeit, nach der solche Filter eingesetzt wurden berechnen.

In Norwegen macht man es dann ja so, dass die Behörde im Zweifel die Originalaufnahmen untersucht. Das ist natürlich ein riesiger Aufwand. Aber es soll ja auch nicht darum gehen, bei jedem privaten Post solche Untersuchungen zu machen, sondern nur bei relevanten Posts.

Die Rede ist von mindestens 10.000 Followern in etwa. Das würde auch bedeuten, dass Privatmenschen sich weiter keine Gedanken machen müssten. Nur dann, wenn man viele Follower hat und/oder mit seinen Posts Geld verdient, im Grunde also Werbung macht, ist ein strengerer Blick und ggf. ein Kennzeichnung notwendig.

Ob allerdings die Menschen, die die Posts konsumieren, diese Hinweise dann überhaupt noch wahrnehmen, wenn sie überall stehen, ist eine andere Frage. Influencer müssen bezahlte Postings ja auch als „Werbung“ kennzeichnen zB. Niemand nimmt das noch ernsthaft wahr.

## Eine gute Idee – oder überflüssig?

Ich bin nicht eindeutig dafür, weil ich einen Abnutzungseffekt befürchte. Auf der anderen Seite ist gar nichts zu tun, wie bislang, ganz sicher der falsche Weg. Denn die Kunstwelt der Sozialen Medien ist zweifellos ein riesiges Problem, vor allem bei der Körperwahrnehmung.

Da hilft es möglicherweise schon, wenn wenigstens dran steht, dass ein Bild verändert wurde. Inwiefern das in einem Metaverse eine Rolle spielen kann, also einer komplett künstlichen virtuellen Welt, wie sie Mark Zuckerberg vorschwebt, ist noch eine ganz andere Frage.

Da haben sich solche Hinweise erledigt, da ja alles künstlich ist. Es gibt aber noch einen weiteren Aspekt, den ich wichtig finde: Deep Fakes – also komplett künstlich erzeugte Bilder, mit KI – sind auch ein zunehmendes Problem.

Dafür zu sensibilisieren, dass Bilder künstlich bearbeitet, sogar künstlich erzeugt werden können, ist richtig und wichtig. Eine Kennzeichnungspflicht für Deep-Fakes wäre sogar wünschenswert. Und natürlich auch, dann Werkzeuge an der Hand zu haben, so etwas schnell und zuverlässig zu erkennen. Da wir uns nicht auf Facebook und Co. verlassen können, ist es gut, sich Gedanken zu machen und Maßnahmen zu ergreifen.

# WhatsApp: "Es wird auf diese Nachricht gewartet."-Fehler beheben

Warten auf Nachrichten? Bei WhatsApp? Was soll das für einen Sinn machen? Trotzdem kommt bei WhatsApp immer mal die Fehlermeldung "Warte auf diese Nachricht." Wir zeigen Euch, was Ihr dagegen tun könnt.

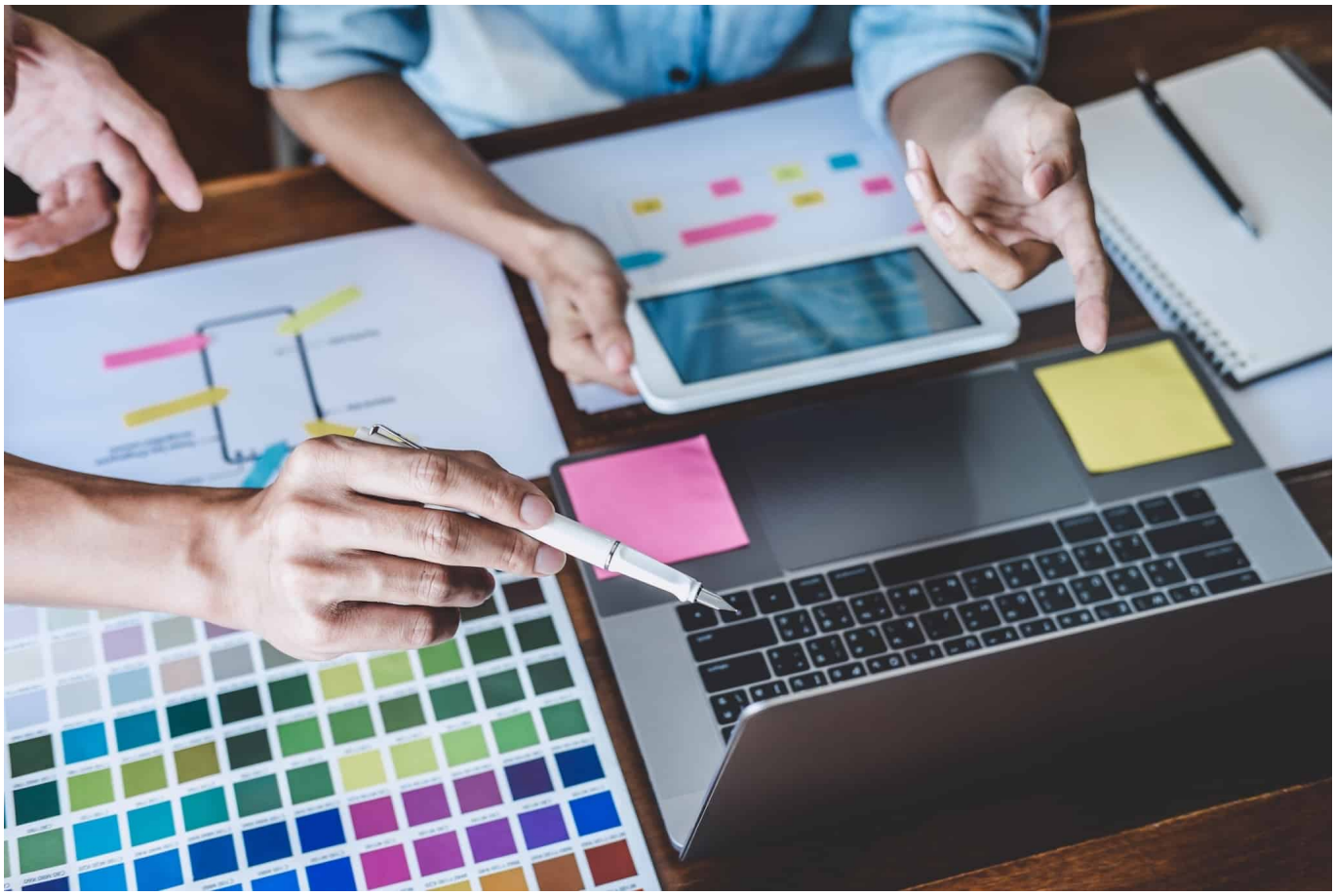
Normalerweise werden WhatsApp-Nachrichten direkt zugestellt und im Chat auf dem Gerät des Empfängers angezeigt. Oft gibt es in Eurem WhatsApp-Konto aber nicht nur ein Gerät, sondern dank der Multi-Geräte-Funktion und WhatsApp Web Access zeigen mehrere Geräte die Konversationen an. Das kann nur funktionieren, indem die Nachrichten über ein Cloud-Backup synchronisiert werden.  Der Versatz ist minimal, die Nachrichten sind nur Sekunden nach dem Ankommen auf Eurem Hauptgerät auf allen anderen Geräten vorhanden.


Wenn Ihr in einer Konversation bei einem oder mehreren Einträgen eines Gesprächspartners die Meldung "Es wird auf diese Nachricht gewartet. Das kann einen Moment dauern." bekommt, dann gibt es ein Problem mit der Synchronisation dieses Chats. Ihr habt dann drei Möglichkeiten:

- Beenden und Neustarten der WhatsApp-App auf dem Gerät, wo der Fehler auftritt.
- Neustarten des Geräts und gegebenenfalls Abwarten.
- Neuregistrierung des Geräts als Web Access-Teilnehmer an WhatsApp

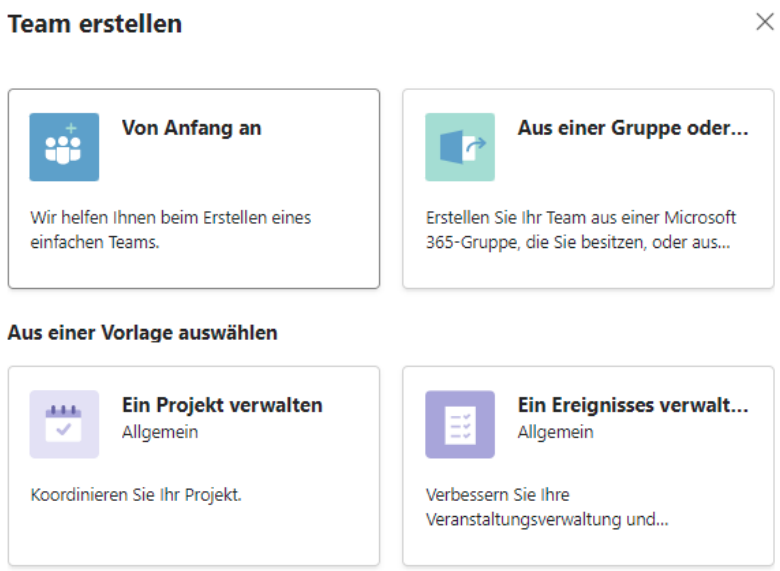
Nach Aufnahme der Synchronisation - die durchaus einige Minuten dauern kann - werden die bisher durch die Fehlermeldung versteckten Meldungen angezeigt.

# Anlegen eines neuen Teams in Microsoft Teams



Microsoft Teams wird immer wichtiger für die Zusammenarbeit, auch im privaten Bereich. Da Ihr meist an unterschiedlichen Aufgaben arbeitet, macht die Unterteilung in einzelne Teams Sinn. Hier lest Ihr, wie Ihr ein neues Team anlegt.

- Um ein neues Team anzulegen, klickt mit der Maus id der linken Übersichtsleiste auf **Teams**, dann ganz unten auf **Team beitreten oder erstellen** > **Team erstellen**.
- Über **Von Anfang an** legt Ihr fest, dass es ein neues, leeres Team sein soll. Alternativ könnt Ihr hier auch von Microsoft gelieferte **Templates** verwenden.
- In den meisten Fällen handelt es sich um ein **Privates** Team, das nur auf Einladung betreten werden kann. Sollen alle Personen zugreifen können, dann wählt **Öffentliches**.




- Nach der Benennung des neuen Teams legt die Software es an.
- Im nächsten Schritt könnt Ihr nun Mitglieder hinzufügen. Die können, müssen aber nicht aus Eurer Organisation stammen. Gerade im privaten Bereich werdet Ihr häufiger E-Mail-Adressen eingeben, über die die Teilnehmer dann eingeladen werden.


Das leere Team kann dann gefüllt werden: Fügt beliebige weitere Personen hinzu, erstellt separate Kanäle für die einzelnen Gesprächsthemen, startet Chats und vieles mehr.

Um das Team zu verwalten, klickt in der Team-Übersicht auf der linken Seite von Teams auf die **drei Punkte** neben dem Team-Namen und dann auf **Team löschen**.

# DVDs auf Windows 11 abspielen: WinX DVD Ripper


DVDs? Wofür gibt es Streaming-Portale? Wenn Ihr spezielle Videos habt, dann findet Ihr die nicht immer bei Netflix, Prime Video und Co. Das macht nichts, denn auch unter Windows 11 könnt Ihr DVDs verwenden.

## Von der DVD zur Videodatei

Das scheitert allerdings meist nicht an der Software, sondern an der Hardware: Viele Geräte haben mittlerweile keine DVD-Laufwerke mehr, folglich müsst Ihr die DVDs vorher umwandeln. Dazu braucht Ihr natürlich ein Gerät, dass ein integriertes DVD-Laufwerk hat.


Auf dem installiert Ihr den kostenlosen WinX DVD Ripper. Der analysiert die DVD, trennt automatisch die einzelnen Videosequenzen auf und empfiehlt Euch, welche Ihr rippen sollt. So könnt Ihr schnell den Hauptfilm identifizieren und dann umwandeln. Wenn es sich um mehrere Sequenzen handelt, dann könnt Ihr die für eine Stalverarbeitung markieren.

Im Normalfall wandelt Ihr die DVD dann in eine MP4-, AVI- oder WMV-Datei um. Dieser Prozess dauert in der Regel um die fünf Minuten. Auch für die Wiedergabe auf Smartphones stehen entsprechende Profile bereit.

In der kostenpflichtigen Platinum-Version (EUR 55,95 als Kauflizenz) kommen dann noch Funktionen wie die Fehlerkorrektur bei verkratzten/defekten DVDs, die Umwandlung in ISO-Images und mehr dazu. Die erstellte(n) Datei(en) könnt Ihr auf das mobile Gerät kopieren und dort abspielen.

## DVD-Player-Software für Windows 11

Die DVD-Wiedergabe ist unter Windows in den Hintergrund gerückt. Wenn Ihr keine vorinstallierte Software auf dem PC findet, dann ist das kostenlose VLC eine gute Alternative: Mit der Software könnt Ihr nicht nur alle möglichen Videoformate (unter anderem auch die vom WinX DVD Ripper) abspielen, sondern auch DVDs direkt. Einzige Voraussetzung: Das DVD-Laufwerk muss vorhanden sein und entsprechen hohe Lesegeschwindigkeiten haben.