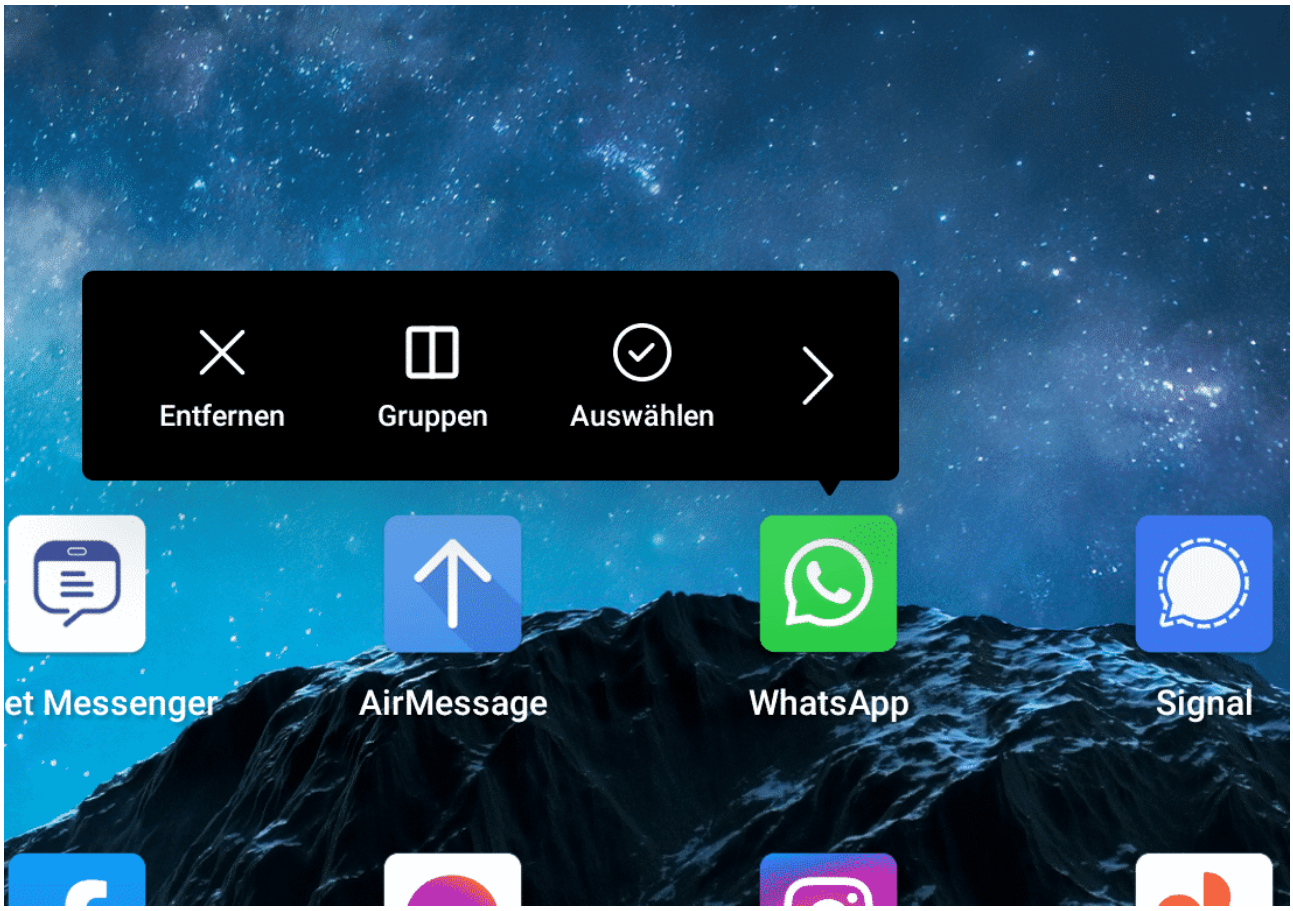
Schieb Report

Ausgabe 2021.36

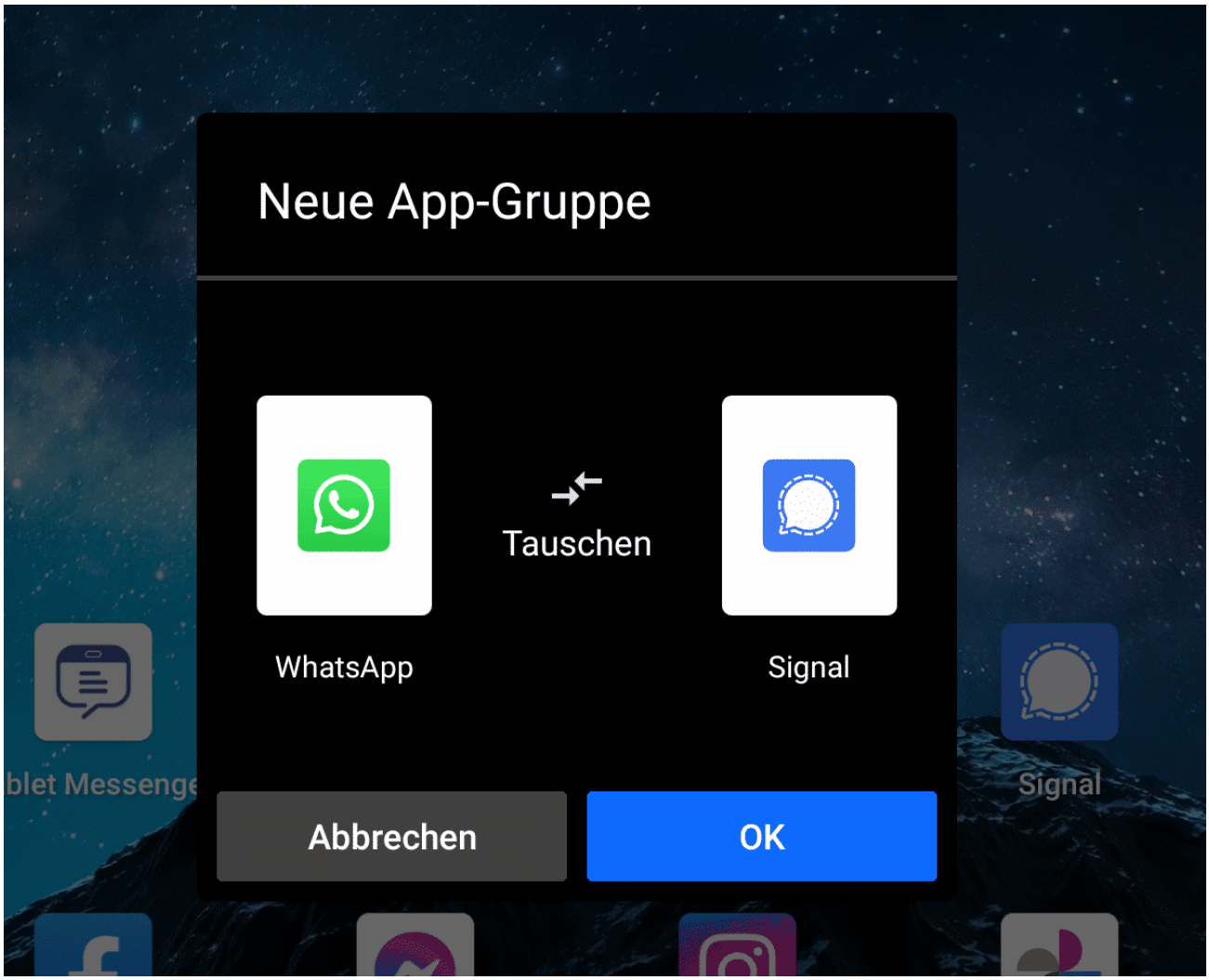
App-Gruppen bei Dual-Screen Android-Geräten einrichten

Wenn Sie zwei Bildschirme an Ihrem Android-Gerät haben, dann bietet es sich an, diese mit zwei unterschiedlichen Apps zu benutzen. Beispielsweise mit OneNote und Edge oder einem Videoplayer und Outlook. Das erlaubt es Ihnen, schnell und ohne manuellen App-Wechsel Daten dazwischen auszutauschen. Bestimmte Kombinationen von Apps werden Sie immer wieder brauchen, und diese können Sie als so genannten App-Gruppen anlegen.

Diese Funktion steht natürlich nur bei unterstützten Geräten wie dem Microsoft Surface Duo oder den Samsung Galaxy Z Fold-Geräten zur Verfügung. Ohne ein zweites Display macht diese keinen Sinn.



Um eine neue Gruppe anzulegen, halten Sie den Finger auf einer App auf dem Display. Wählen Sie dann **Gruppen**. Android nimmt nun automatisch die angewählte App als erste App der Gruppe an und fordert Sie auf, aus der Liste der Apps die zweite auszuwählen. Nachdem Sie dies gemacht haben, tippen Sie auf **Fertig** oben rechts.

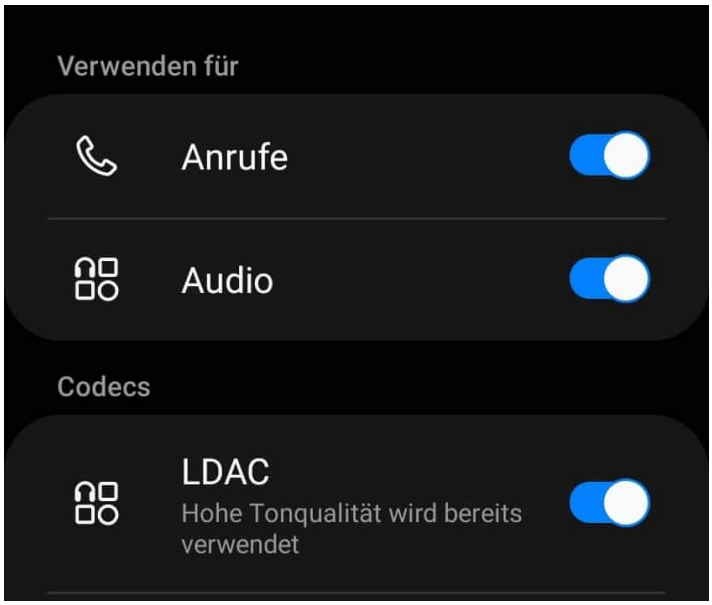


Nun können Sie die neue Gruppe benennen, indem Sie auf **Neue App-Gruppe** tippen und dann Ihren Wunschnamen eingeben. Wenn Sie die Anordnung der Apps auf den Bildschirmen ändern wollen, dann tippen Sie auf **Tauschen**. Ein Tippen auf **OK** speichert die Gruppe, die Sie dann wie eine einfach App verschieben und öffnen können.

Einschalten von LDAC bei Android-Smartphones

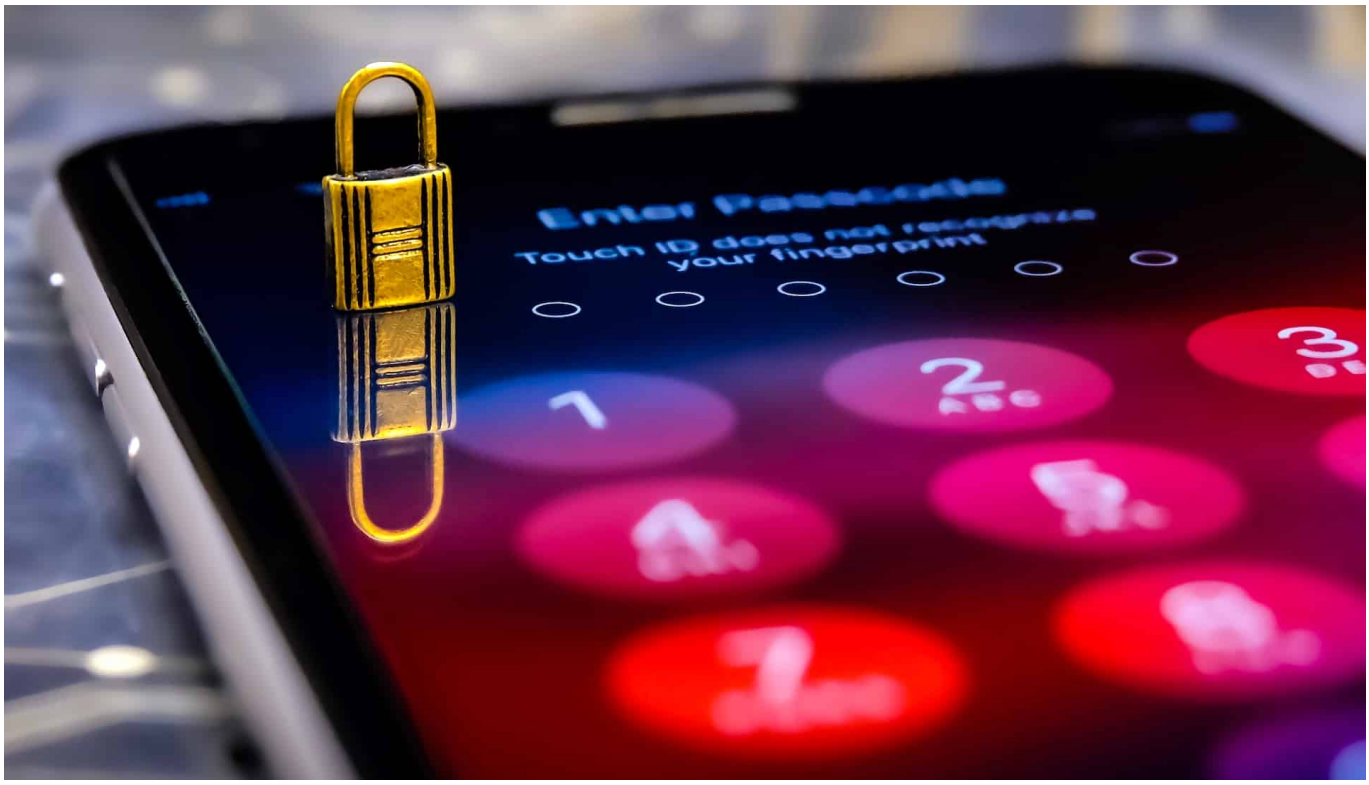
Verwenden Sie noch einen MP3-Player als separates Gerät? Die Wahrscheinlichkeit, dass Sie mit "Warum? Ich habe doch mein Smartphone!" antworten, liegt bei nahe 100 Prozent. Dass diese Anwendung nur eine von vielen für die Smartphone-Hersteller ist, erkennen Sie an den rudimentären Einstellmöglichkeiten für den Klang. Zumindest Android hat aber versteckt eine Einstellung, die Ihnen die Ohren aufgehen lassen wird - den richtigen Kopfhörer vorausgesetzt.

Im Standard verwendet Android als Bluetooth-Übertragungsmethode immer einen Codec, der so weit wie möglich verbreitet ist wie beispielsweise SBC. Wie woanders auch bedeutet mehr Sicherheit auch weniger Leistung: Möglichst viele Kopfhörer sollen den Codec unterstützen, damit wird eben einer ausgewählt, der nicht allzu hochwertig vom Klang ist. Einen Kopfhörer von Sony, die mit dem eigenen Codec LDAC deutlich mehr können, unterfordern Sie damit. Android unterstützt LDAC, aber nur dann, wenn Sie einen entsprechenden Kopfhörer als Bluetooth-Gerät gekoppelt haben.



Tippen Sie auf **Einstellungen** > **Bluetooth**, dann auf das kleine **i** neben dem Namen des Kopfhörers. Unter Verwenden für können Sie einstellen, für welche Anwendungen Ihr Smartphone diesen nutzen soll. Darunter finden Sie einen Schalter **LDAC**. Schalten Sie diesen ein, damit Android die Übertragung dafür optimiert. Nach einem Neustart der Audiowiedergabe werden Sie eine deutliche Verbesserung der Klangqualität bemerken!

#BKA setzt #Pegasus Trojaner ein: Ein paar Hintergründe



Darf die Polizei Trojaner einsetzen - und wenn ja, wann und zu welchem Zweck? Diese Frage wird aktuell wieder geführt. Denn es ist bekannt geworden, dass das BKA den umstrittenen Trojaner Pegasus einsetzt. Der kann eine Menge - und ist in Verruf geraten, weil autokratische Staaten ihn einsetzen.

Im Film ist immer alles ganz einfach: Wenn die Polizei jemanden überwachen will, muss sie nur auf übergroße Kontrollmonitore blicken, sieht die observierte Person aus gleich mehreren Perspektiven – und kann quasi alles mitlesen, was auf dem Smartphone geschrieben wird. Und natürlich können die Beamten auch Telefonate abhören.

Mit der Realität hat das zwar wenig zu tun. Vermutlich sind es aber genau diese Bilder, die die Phantasie der Menschen beflügeln: Wir glauben, auch unsere Polizei könnte all das. Und wenn in den Nachrichten zu hören ist, das BKA habe eine Spionage-Software bei der israelischen Firma NSO gekauft, werden diese Phantasien beflügelt.

Polizei braucht Werkzeuge zur Überwachung

Natürlich muss das BKA die Möglichkeit haben, die Mobilgeräte von Zielpersonen zu überwachen und abzuhören – in Einzelfällen, nach richterlicher Anordnung. Und die selbst programmierte Software des BKA, der sogenannte "Staatstrojaner", war offenbar so schlecht, dass ihn das BKA nach eigenen Aussagen praktisch nie eingesetzt hat.

Doch nun hat das BKA offenbar die objektiv betrachtet beste Software am Markt gekauft: "Pegasus" genannt, bei der israelischen Firma NSO. Diese Software kann E-Mails und Chats mitlesen, Fotos und Videos durchsuchen, eingetippte Passwörter mitlesen. Sogar das eingebaute Mikro und die eingebaute Kamera aktivieren, um Gespräche abzuhören. Es sind so viele Funktionen, dass das BKA offenbar einige nicht gebucht hat - um juristische Schwierigkeiten zu vermeiden. Denn wenn Beweismittel unter fragwürdigen oder unzulässigen Methoden entdeckt wurden, sind diese vor Gericht gar nicht zulässig.

Das BKA nutzt längst nicht alles, was Pegasus kann

Problematisch ist, dass das BKA zu einem Anbieter gegangen ist, der offenbar auch autokratischen Staaten dabei hilft, Journalisten, Menschenrechtler, Rechtsanwälte und sogar Staatsoberhäupter auszuspionieren – zu deren

erheblichem Nachteil. So soll nach Recherchen von WDR, NDR, SZ und "Zeit" zum Beispiel mithilfe des Pegasus-Trojaners das unmittelbare Umfeld des ermordeten saudischen Journalisten Khashoggi ausspioniert worden sein.

Missbrauch vermeiden

Kritiker unterstellen nun, das Bundeskriminalamt werde das neue Werkzeug ähnlich enthemmt einsetzen wie Saudi-Arabien oder Aserbaidschan. Massenüberwachung drohe.

Man könnte natürlich zu Recht fragen: Wie können wir den Einsatz kontrollieren? Doch von vorneherein vom Schlimmsten auszugehen, wird weder der Polizeiarbeit gerecht noch lässt es Vertrauen in den Rechtsstaat erkennen. In Saudi-Arabien entscheidet ein Prinz, was geschieht - in Deutschland ein Gericht. Ich denke, das ist ein Unterschied.

Die Debatte sollte also weniger emotional geführt werden. Denn dann ließen sich die tatsächlichen Probleme, etwa die Tatsache, dass ein Staat, der Trojaner einsetzt, kein Interesse am Stopfen aller Sicherheitslecks hat, besser diskutieren.

https://vimeo.com/577962131

Pegasus ist nach Recherchen für viele Schnüffelangriffe missbraucht worden

Avaaz hat Desinformationskampagnen in Deutschland untersucht

Wo fängt Desinformation an - und wo hört sie auf? Es ist fast unmöglich, eine genaue Linie zu ziehen. Was als Information gilt und was als Desinformation, das hängt auch davon ab, wen man fragt. Doch wenn Fakten verzerrt und ins falsche Licht gerückt werden, um Parteien oder Politikern zu schaden, dann ist das ganz klar Desinformation - und alles andere als ungefährlich. Die Netzwerk Avaaz hat jetzt untersucht, wie es in Deutschland aktuell aussieht.

In den Wochen vor der Bundestagswahl haben Desinformation und Falschinformation im Netz Hochkonjunktur. Sogar Facebook verstärkt aktuell seine Anstrengungen, um auf Facebook, Instagram und WhatsApp etwas gegen Fake News jeder Art zu unternehmen. Niemand bezweifelt ernsthaft, dass im Netz Falschinformationen und Kampagnen kursieren – nur die genaue Dimension kennt keiner.

Ergebnisse von Fakten-Checkern untersucht

Doch jetzt hat das Netzwerk Avaaz - das selbst regelmäßig Kampagnen der verschiedensten Art in aller Welt startet – die Lage eingehender untersucht. Dazu haben sich die Experten die Ergebnisse der Fakten-Checker von dpa, AFP und des Rechercheverbunds Correctiv im Zeitraum vom 1. Januar bis 31. August 2021 genauer angesehen. Die drei Redaktionen gehören zum Fakten-Checker-Team von Facebook, beschäftigen sich also gewissermaßen "von Amts wegen" mit dem Problem.

Demnach gibt es rund 85 "Desinformationsnarrative" zu 30 deutschen Politikerinnen und Politikern. Man könnte auch "Erzählungen" oder "Geschichten" sagen, die einen mal mehr, mal weniger starken Bezug zur Realität haben – und manchmal gar keinen. Mal werden Geschichten aufgebauscht, manchmal erfunden – aber immer mit dem Zweck, Personen oder Parteien zu schaden.

Auch Laschet und Merkel betroffen

Interessant: Nicht etwa Armin Laschet ist das begehrteste Ziel solcher Desinformationskampagnen, sondern die Kanzlerkandidatin der Grünen, Annalena Baerbock. Sie betreffen nach dem Avaaz-Bericht die meisten Desinformationsnarrative im Fernsehen, Print, Online und in sozialen Medien.

25 Prozent der - rein quantitativ überschaubaren - Desinformationen betreffen Baerbock. Bundeskanzlerin Angela Merkel sowie Kanzlerkandidat Armin Laschet folgen mit 13 bzw. zehn Prozent auf den Plätzen zwei und drei. Rund 56 Prozent der Deutschen haben der Auswertung zufolge zudem Falschnachrichten über Baerbock gehört oder gelesen.

Nicht jedes Gerücht weiterverbreiten

Avaaz warnt vor einer ähnlichen Entwicklung wie in den USA, wo Desinformation im öffentlichen Diskurs noch eine deutliche größere Rolle spielt als bei uns. Wichtig scheint: Nicht über jedes Gerücht muss gleich in den seriösen Medien berichtet werden. Denn erst dadurch wird die meist in den Plattformen gezielt platzierte Kampagne für eine breitere Öffentlichkeit sichtbar.

https://www.youtube.com/watch?v=2y2AyWm0zOM

Mein Gespräch mit Guido Bülow von Facebook über den Kampf gegen Falschinformationen

Pegasus: BKA setzt offensichtlich umstrittene Spionage-Software ein

Offenbar hat das BKA eine Version der umstrittenen Überwachungssoftware "Pegasus" gekauft - und womöglich auch bereits im Einsatz. Der Staatstrojaner war zuletzt international wegen der Überwachung von Journalisten, Aktivisten und Oppositionellen in die Schlagzeilen geraten. Die Bundesregierung hat den Vorgang als „geheim“ eingestuft.

Die Polizei hat es heute nicht leicht: Telefongespräche abhören, das war früher. Heute muss man als Polizei schon Chats mitlesen können – und das ist alles andere als einfach. Das Bundeskriminalamt (BKA) hat nun überraschend erklärt, dass die höchst-umstrittene Schnüffel-Software „Pegasus“ aus Israel beim BKA im Einsatz ist, mit der Smartphones überwacht werden können. Darüber wurde heute der Innenausschuss des Bundestages unterrichtet.

Was kann die Software „Pegasus“

Pegasus ist ein „Trojaner“, also eine Software, die durch Ausnutzen unbekannter oder noch nicht gestopfter Sicherheitslücken in ein Gerät kommt. Als Nutzer bemerkt man nicht, dass der Trojaner im Gerät aktiv ist. Das gilt für alle Schnüffelprogramme der Kategorie „Trojaner“ – und auch für Pegasus. Man

muss Pegasus als eine Art Schweizer Taschenmesser bezeichnen, denn damit ist so ziemlich alles möglich.

Mit Pegasus können Anrufe, E-Mails, SMS und verschlüsselte Chats mit Signal, WhatsApp oder anderen Messengern mitgeschnitten werden. Der Trojaner kann Fotos und Videos auf dem Handy durchsuchen und Passwörter auslesen. Darüber hinaus ist Pegasus sogar zur Raumüberwachung tauglich, weil die Betreiber mit dem Trojaner das Mikrofon und die Kamera des Geräts einschalten kann – unbemerkt, versteht sich. Darüber hinaus lässt sich mit dem Trojaner die exakte Position des Handys orten. Pegasus ist also wirklich eine Allzweckwaffe.

Darum ist der Trojaner „Pegasus“ umstritten

Durchaus Werkzeuge, die Polizei und Behörden brauchen können, wenn eine Überwachung angeordnet ist.

Das BKA hat den Trojaner nicht selbst entwickelt, sondern bei der israelischen Firma NSO eingekauft. Die sind wahre Spezialisten, wenn es darum geht, einen Trojaner zu entwickeln, der auf jedem Gerät installiert werden kann, der Sicherheitslecks ausnutzt und nicht entdeckt wird. Das BKA hat in der Vergangenheit selbst einen „Staatstrojaner“ entwickelt, aber der war so schlecht, dass er selbst nach Auskunft des BKA praktisch nie zum Einsatz gekommen ist.

Der Trojaner „Pegasus“ von NSO allerdings schon. Bereits Ende Juli ist bekannt geworden – unter anderem durch die Recherchen von WDR, NDR, SZ und ZEIT –, dass der Trojaner „Pegasus“ bereits in 11 Ländern zum Einsatz kommt. Auch in autokratischen Staaten. Angeblich stehen 50.000 Ziele in der Liste, die ausgespäht werden. Darunter auch Staats- und Regierungschefs, aber auch viele Journalisten, Menschenrechtsvertreter und Rechtsanwälte. NGO bestreitet das – doch es sind besorgniserregende Fälle nachgewiesen.

So kommt der Trojaner in die Geräte

Um so einen Trojaner wie Pegasus auf ein Gerät zu bekommen, müssen Sicherheitslecks ausgenutzt werden – im Betriebssystem, in der Mail-Software, im Browser oder in WhatsApp. Zum Beispiel erhält die Zielperson eine Mail mit einem Anhang. Wird der geöffnet, landet die Software im Gerät – iOS wie Android gleichermaßen. Oder es reicht eine Nachricht per iMessage oder WhatsApp.

Oder die Zielperson wird – etwa durch eine WhatsApp-Nachricht oder eine Mail, die die Beamten unter falscher Adresse verwenden – auf eine Webseite gelenkt, und der Trojaner kommt so über den Browser ins Gerät. Die Wege ins Gerät ändern sich ständig: Sicherheitslecks werden gestopft, neue werden entdeckt. Aber aufwändig ist das nicht.

Da bei NSO Experten arbeiten und in der Regel sogenannte „Zero Day Exploits“ ausgenutzt werden, also bislang noch unbekannte Sicherheitslecks, werden die Eindringlinge nicht entdeckt. iPhone-Benutzer setzen sowieso praktisch nie Sicherheits-Software ein.

Die Reaktionen darauf

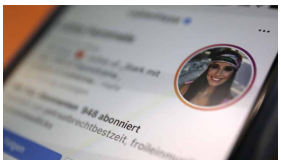
Netzaktivisten sind empört, da sie eine allumfassende Bespitzelung befürchten. Man muss allerdings sagen: In Deutschland sind die Grenzen sehr eng gesteckt, wann, wo und in welchem Umfang Geräte auf diese Weise auskundschaftet werden dürfen. Laut BKA hat die Behörde eine stark abgespeckte Version der Software bestellt, also mit deutlich weniger Funktionen als sie bietet, um juristisch einwandfrei zu sein und eben keine Grenzen zu überschreiten.

Davon hat auch die Polizei nichts, weil sie die Informationen dann nicht verwenden dürfte. Um welche Funktionen die Software abgespeckt wurde, wird aber aktuell nicht verraten. Geheimsache! Auch, ob und wie oft Pegasus in Deutschland bereits eingesetzt wurde.

Influencer und Werbung bei Insta: Wer merkt das überhaupt noch?

Wer Influencer kennt: Sie machen Werbung - praktisch rund um die Uhr. Wenn sie dann mal etwas in die Kamera halten und empfehlen, ohne dafür Geld zu bekommen - ist das dann auch kennzeichnungspflichtige Werbung? Über diese Frage musste nun der Bundesgerichtshof (BGH) entscheidend - und das ist wegweisend.

Der Bundesgerichtshof (BGH) musste sich mit einer Frage beschäftigen, die sich in der "echten Welt" viele stellen: Wann müssen Influencerinnen und Influencer, die sich in ihren Instagram-Kanälen quasi zu lebenden Litfaßsäulen machen, ein Posting eigentlich als "Werbung" kennzeichnen - und wann nicht? Spätestens dann, wenn sie für die Werbung konkret Geld oder kostenlos Waren erhalten haben, oder auch dann, wenn sie nur etwas "empfehlen", ohne einen direkten Vorteil dadurch gehabt zu haben?



Cathy Hummels hat teilweise vor dem BGH gewonnen[/caption]

Teilsieg für die Influencerinnen

Diese Frage beschäftigt die Gerichte schon seit Jahren. Heute (09.09.20219) hat der BGH dazu eine Entscheidung bekannt gegeben: Danach dürfen Influencerinnen wie Cathy Hummels – um sie ging es im verhandelten Fall konkret – durchaus auch schon mal einen Pulli schön finden und ihn per "Tap Tag" verlinken, ohne das Posting als "Werbung" kennzeichnen zu müssen. Bedingung laut den Richtern: Dafür ist kein Geld geflossen, und das Ganze ist auch nicht zu werblich.

Die Entscheidung macht die Sache in Zukunft nicht einfacher, denn natürlich könnte ein werbendes Posting auch mit dem Hintergedanken veröffentlicht werden, später mal Umsatz zu machen. Nach dem Motto: Seht her – ich zeige Eure Produkte, wie wär's mit einem Vertrag?

> "Nach dem aktuellen Stand gilt: Werbende Postings sind immer eine geschäftliche Handlung. Sie müssen trotzdem nach aktuellem Stand nur dann als Werbung oder Anzeige oder ähnliches gekennzeichnet werden, wenn es hierfür ein Entgelt oder eine andere Gegenleistung - und sei es nur das beworbene Produkt als Geschenk - gibt oder der werbende Inhalt nicht aus anderen Gründen offensichtlich erkennbar ist."[caption id="attachment_77621" align="alignnone" width="1030"]
>
> Michael Terhaag, *Fachanwalt aus Düsseldorf*

Der BGH hat damit eine richtungsweisende Entscheidung gefällt, an die sich andere Gerichte halten müssen. Durchaus ein Teilsieg für die Influencerinnen.

Wie soll das gekennzeichnet werden?

Die Menschen haben längst akzeptiert, dass bei ihren Idolen auf Facebook, Instagram, Tiktok und Youtube (fast) nichts ohne Bezahlung läuft. Die perfekte Vermischung von Kommerz, Werbung und Selbstdarstellung ist ohnehin längst traurige Realität in den "Sozialen Netzwerken" und lässt sich nicht mehr zurückdrehen. Daran würden auch Gesetze oder Gerichtsurteile vermutlich nicht viel ändern.

Die Realität ist: Viele "Creators" blenden bei ihren Videos (etwa auf Youtube) schon lange Kennzeichnungen wie "Dauerwerbesendung" oder "Werbung" ein, um sicherzugehen, juristisch keinen Fehler zu machen - selbst dann, wenn kein Geld geflossen ist. Durch den fast schon inflationären Einsatz des "Werbung"-Emblems nehmen das die Menschen beim Betrachten vermutlich ohnehin nicht mehr wahr – oder ernst.

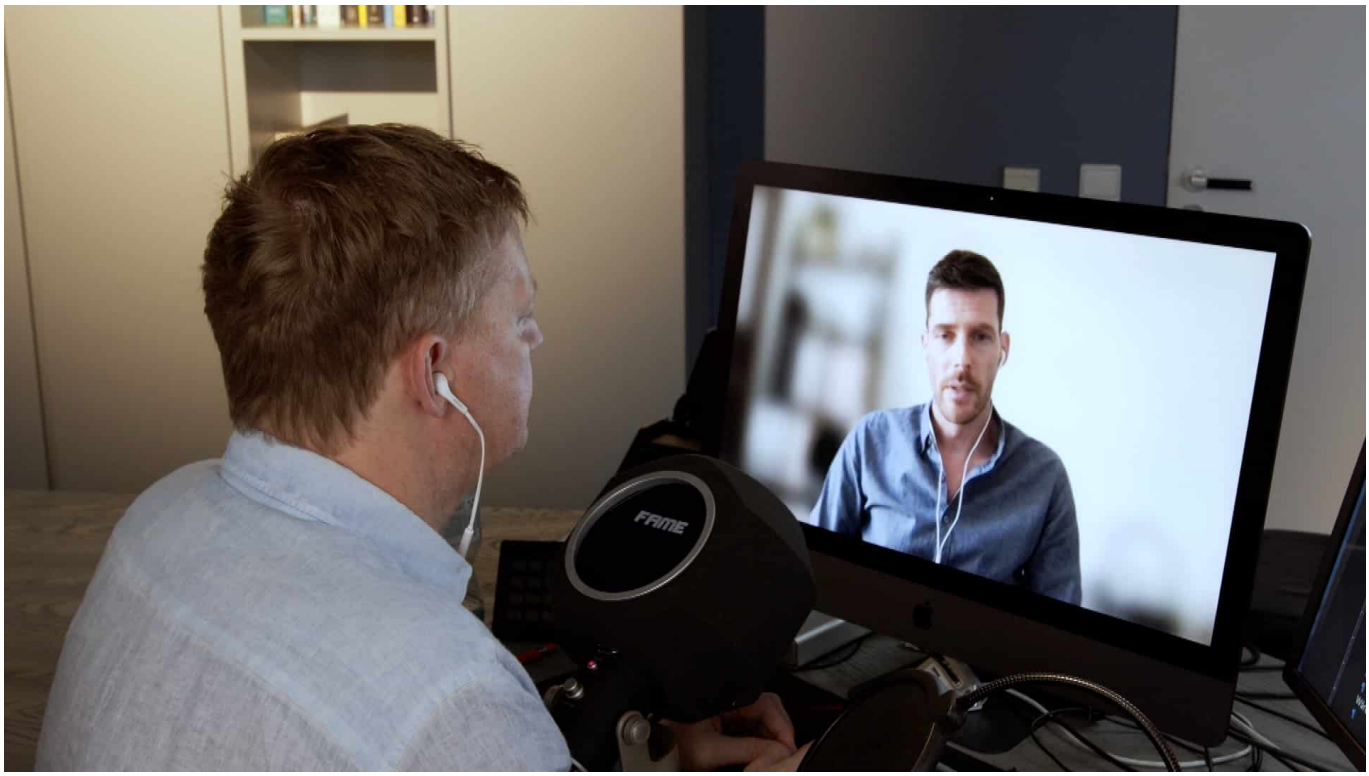
Allerdings: Wie konkret die Kennzeichnung erfolgen soll, ist ohne die ausformulierten Entscheidungsgründe noch nicht zu sagen. In einem der beurteilten Postings kam im beschreibenden Text das Wort "Werbung" zwar vor, allerdings nur versteckt. In diesem Punkt haben die Richter dem Verband recht gegeben, der den Influencerinnen Schleichwerbung vorgeworfen hatte.

Juristisch bleibt's also einigermaßen kompliziert.

https://vimeo.com/393484045

Rechtsanwalt erklärt: Was dürfen Influencer und was nicht?

Fake News: Facebook im Interview



Falschnachrichten und Desinformation gibt es nicht erst, seitdem es Facebook, Instagram und Co. gibt. Doch die Plattformen machen die Verbreitung einfacher - und ermöglichen, jeden einzelnen gezielt mit passenden Botschaften anzusprechen. Darüber habe ich mit Guido Bülow von Facebook gesprochen.

Gerade mal noch drei Wochen – dann haben wir Bundestagswahl hier bei uns in Deutschland. Die Parteien machen Wahlkampf – so gehört sich das. Viele informieren sich aber auch oder sogar vor allem im Netz – und in den Sozialen Netzwerken.

Und es geistern viele Unwahrheiten und auch Falschbehauptungen, die Wähler beeinflussen sollen. Es gibt Kräfte im In- und Ausland, die dafür sorgen, dass solche Fake-News die Runde machen. Aber wie dagegen angehen? Facebook hat nun einige Maßnahmen gestartet, die helfen sollen.

https://www.youtube.com/watch?v=2y2AyWm0zOM

Soziale Netzwerke werden geflutet

Die Wählergunst ist im Fluss - das beweisen die Stimmungsbarometer. Viele informieren sich auch, immer mehr sogar hauptsächlich in Sozialen Netzwerken wie Facebook, Instagram und Co. Und deshalb werden die Plattformen mit Nachrichten und Meldungen geflutet – aus allen Lagern.

Mit Infos und Meldungen, die aufwühlen und möglicherweise Einfluss auf das Wahlverhalten haben können. Darunter auch viele steile Behauptungen – und jede Menge Falschmeldungen, auch Fake-News genannt. Klar: Auch längst nicht alles, was Politiker und Politikerinnen sagen und behaupten, besteht einen strengen Fakten-Check. Aber da weiß man zumindest, wer es sagt.

Das ist in Sozialen Netzwerken anders.

Da machen Kräfte aus dem In- und Ausland gezielt Stimmung, auch und vor allem mit unhaltbaren Falschmeldungen – und niemand weiß, wer dahintersteckt.

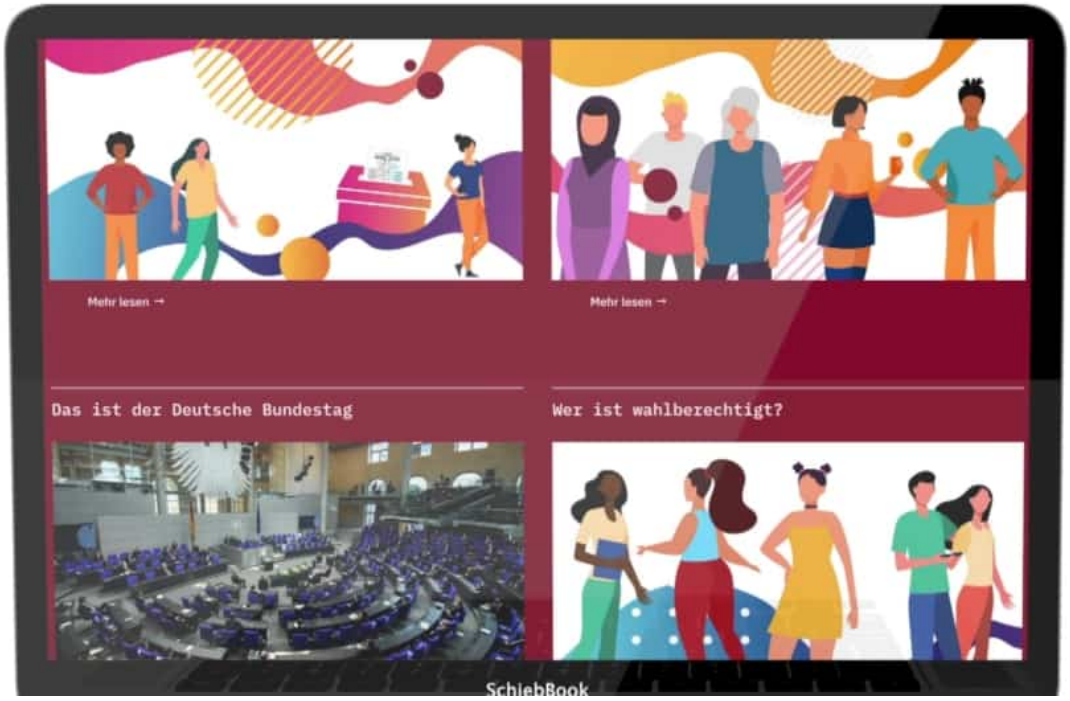
PR-Agenturen aus London bieten Wahlmanipulation an

Wie konkret die Bedrohung ist, zeigt die ARD-Dokumentation „Wahlkampf undercover“: PR-Agenturen aus London bieten gegen Bezahlung Wahlmanipulation an – vor allem auf Facebook. Die Menschen werden gezielt mit Falschmeldungen angesprochen, die sie aufregen.

Am meisten Falschmeldungen erscheinen auf Facebook und Instagram, das auch zu Facebook gehört. Die Kritik ist groß, der Konzern unternehme generell zu wenig. Deshalb hat Facebook nun weitere Maßnahmen angekündigt. Vor allem mehr Aufklärung soll es geben, kündigt Guido Bülow an, der bei Facebook für Kooperationen und journalistische Inhalte zuständig ist.

Guido Bülow: „Wir wissen, dass sowohl junge Menschen, aber eben auch ältere Menschen Aufklärung benötigen, Aufklärung benötigen. Gerade vor einer Wahl, vor einer Bundestagswahl wollen wir sie vor Falschinformationen schützen. Deshalb sind wir eine Partnerschaft eingegangen mit fünf verschiedenen Partnern in Deutschland."

Gemeint ist zum Beispiel duhastdiewahl.de. Die Bundeszentrale für politische Bildung hat einen Infobereich über Demokratie und Wahlen auf die Beine gestellt – auch in Türkisch, Russisch und Arabisch. Darauf wird aus Facebook heraus immer wieder verlinkt. Konkrete Hilfe zum Thema Fake-News gibt's aber eher nicht: Ein Hinweis, dass man nicht alles glauben soll – mehr nicht. Was gibt's also sonst noch?



Mehr Fakten-Checks

Guido Bülow: „Wir haben auf der ganzen Welt spezielle Teams aufgebaut, um

koordinierte Desinformationskampagnen zu stoppen. Wir arbeiten mit Fakten-Prüfern zusammen, das sind in Deutschland die dpa, AFP und Correctiv, um Falschmeldungen zu identifizieren, um sie zu reduzieren in der Sichtbarkeit, aber den Menschen auch weiterführende Informationen zu geben."

Mehr Fakten-Checks – das ist gut. Correctiv und andere untersuchen fragwürdige Inhalte – und zeigen einen Hinweis, wenn etwas nicht stimmt. Als falsch markierte Nachrichten werden allerdings nicht etwa gelöscht, sondern nur weniger häufig gezeigt. Gelöscht werden nur Beiträge, die gegen Gesetze verstoßen.

Verantwortung der Netzwerke

Klar, die Sozialen Netzwerke tragen nicht allein die Verantwortung, dass immer mehr Falschmeldungen kursieren und der Ton in der politischen Debatte immer rauher wird. Aber sie tragen Verantwortung – und zwar einer erhebliche.

Denn würden sie nicht so viele Daten von uns sammeln, könnten nicht windige PR-Agenturen jeden einzelnen von uns gezielt ansprechen und passende Propaganda präsentieren. Das Geschäftsmodell von Facebook, Google und Co. ist eine erhebliche Ursache für das Problem.

Neu: Fakten-Checks auf WhatsApp

Auch auf WhatsApp verbreiten sich viele Falschnachrichten. Allerdings kann Facebook kaum eingreifen, da alle Nachrichten verschlüsselt sind. Neu ist: Wer eine fragwürdige Nachricht erhält, kann die an Fakten-Checker wie AFP oder Correctiv schicken – und bekommt umgehend eine Einschätzung, ob es sich um eine Falschmeldung handelt.

Zum Schluss noch einen Tipp: Wie schwierig es mitunter sein kann, Fake-News und Falschmeldungen zu erkennen und von seriösen Informationen zu unterscheiden, das kann jeder selbst herausfinden. Bei Klicksafe und beim SRF – dem Schweizer Fernsehen – gibt es zwei wirklich gute Online-Tests. Einfach mal machen. Das trainiert nämlich die Reflexe. Und die sind ungeheuer wichtig in den Sozialen Medien.

https://www.klicksafe.de/typo3conf/ext/quiz_maker/Resources/Public/game/?path=https%3A%2F%2Fwww.klicksafe.de%2F%3FeID%3DquizJson%26uid%3D6

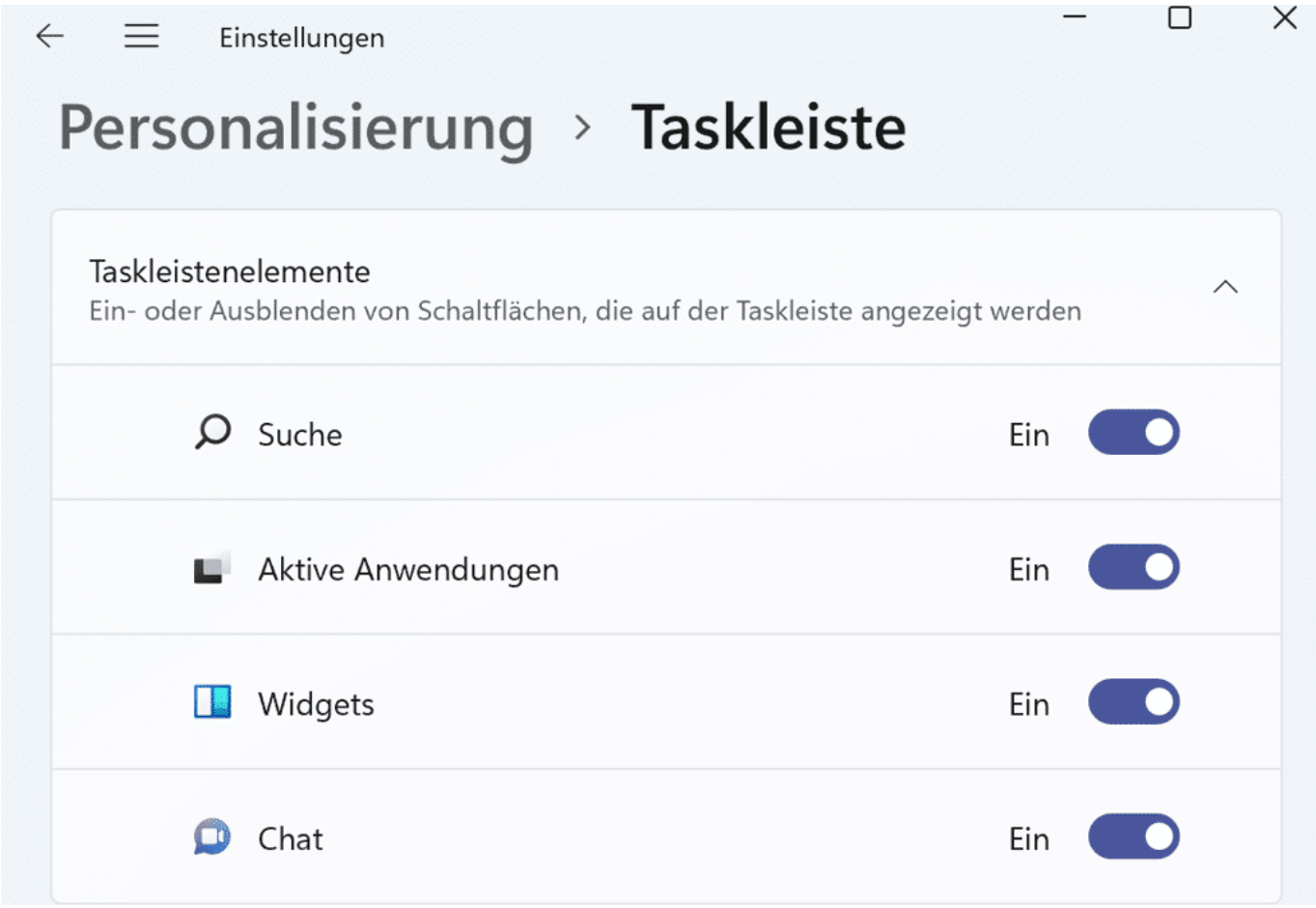
https://www.srf.ch/news/panorama/online-quiz-echt-oder-fake-testen-sie-ihr-urteilsvermoegen

Anpassen der Taskleiste in Windows 11

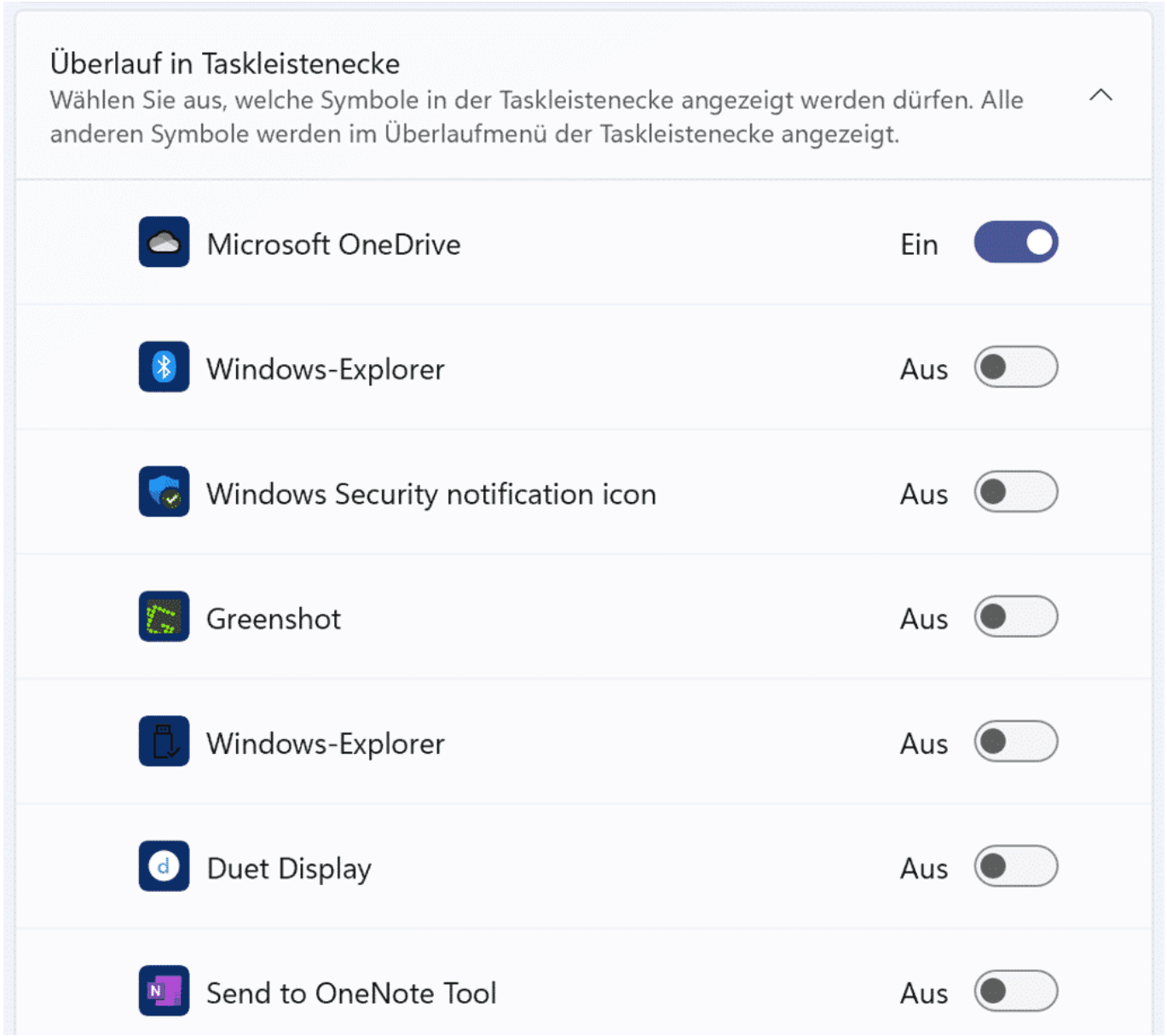
Windows 11 macht einiges anders, auch die Taskleiste ist auf den ersten Blick ungewohnt leer. Die auf den ersten Blick fehlenden, lieb gewonnenen Elemente können Sie schnell wiederbekommen!

Die Einstellung den der Taskleiste von Windows 11 sind im Auslieferungszustand recht spartanisch: Der Eindruck soll eher aufgeräumt als überladen sein. Wenn Sie die Taskleiste aber intensiv nutzen, dann fehlen ihnen einige Funktionen. Diese können Sie über die Einstellungen der Taskleiste einblenden. Die erreichen Sie durch einen Rechtsklick auf die Taskleiste und dann auf **Taskleisteneinstellungen**. Alternativ unter **Personalisierung** > **Taskleiste**.

Hier können Sie beispielsweise Tastatur und Touchpad als Symbol in der Taskleiste einblenden. Wichtig, wenn Sie ein Tablet mit abnehmbarer Tastatur wie ein Surface verwenden und trotzdem Tastatur- und Mausfunktionen nutzen wollen.



Auf der Taskleiste kann der Platz bei vielen laufenden Anwendungen schon einmal eng werden. Dann sind Sie froh darum. wenn Sie unnötige Symbole wie die Suche, den Zugriff auf die virtuellen Desktops oder Teams als Chat-Dienst ausblenden können.

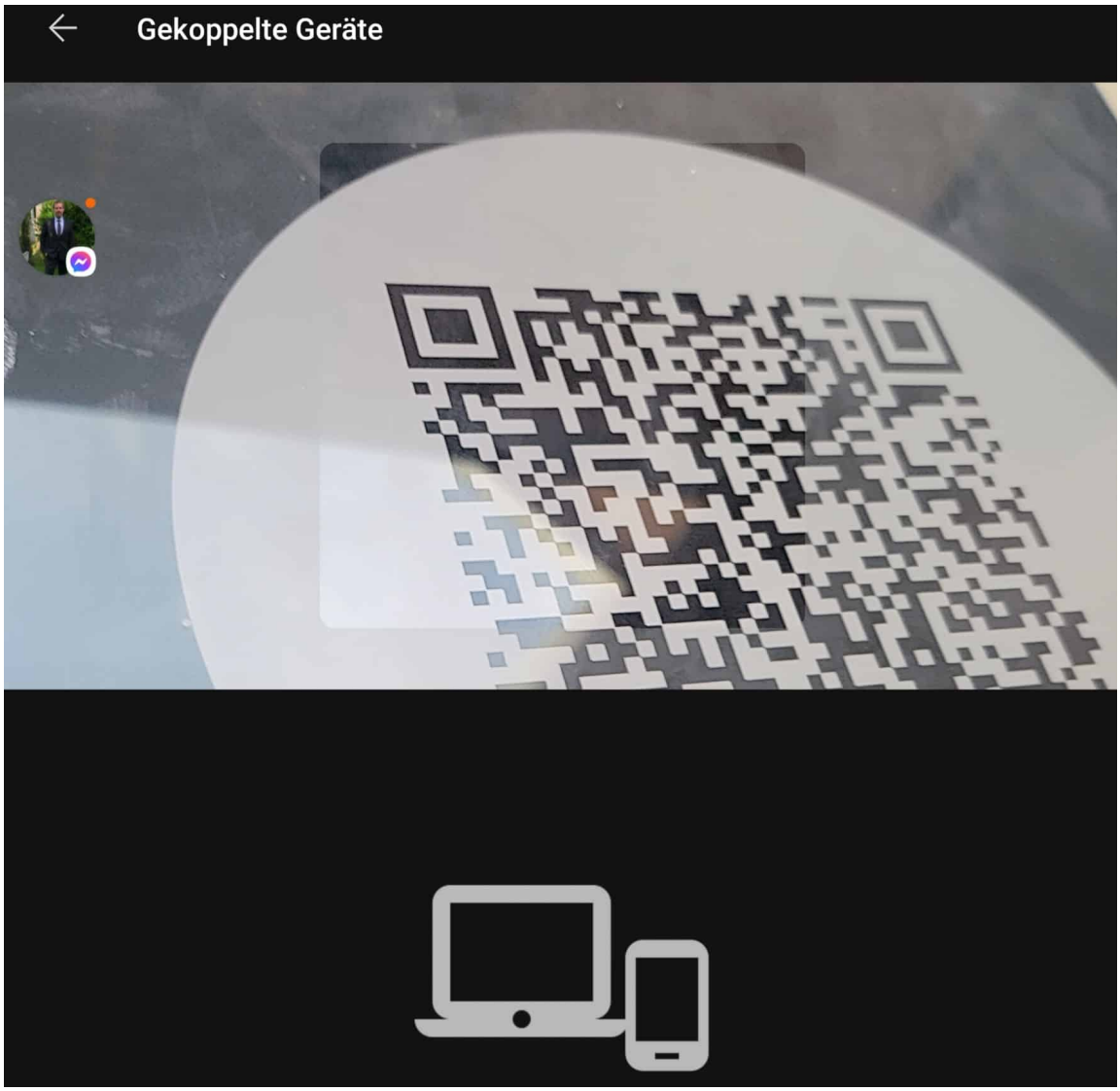


Unter Überlauf in der Taskleiste können Sie festlegen, welche Apps und Funktionen unten rechts neben der Uhr auf jeden Fall immer sichtbar vleiben sollen. Die deaktivierten Elemente werden dann nach einer gewissen Zeit ausgeblendet.

Mit dem Tablet auf den Signal-Messenger zugreifen

Signal hat sich in den vergangenen Monaten mehr und mehr zur Alternative zu WhatsApp etabliert. Wo andere Messenger daran krankten, dass nicht genug der eigenen Kontakte ihn nutzten, hat Signal hier deutlich mehr Erfolg. Einen Nachteil gegen den Platzhirschen gibt es aber leider: Es gibt keinen Webclient, mit dem Sie auch über ein Tablet oder einen beliebigen Browser darauf zugreifen können. Auf dem Tablet gibt es aber eine Alternative!

Sowohl für Android- als auch für iOS-Tablets gibt es eine spezielle Version, die die Registrierung per SMS überspringt und sich als Client installiert. Den können Sie dann wie die Web-Version von WhatsApp registrieren. Auf dem Tablet wird Ihnen beim Start ein QR-Code angezeigt. Um diesen zu scannen, tippen Sie in der Signal-App auf Ihrem Smartphone auf **Einstellungen** > **Gekoppelte Geräte**.

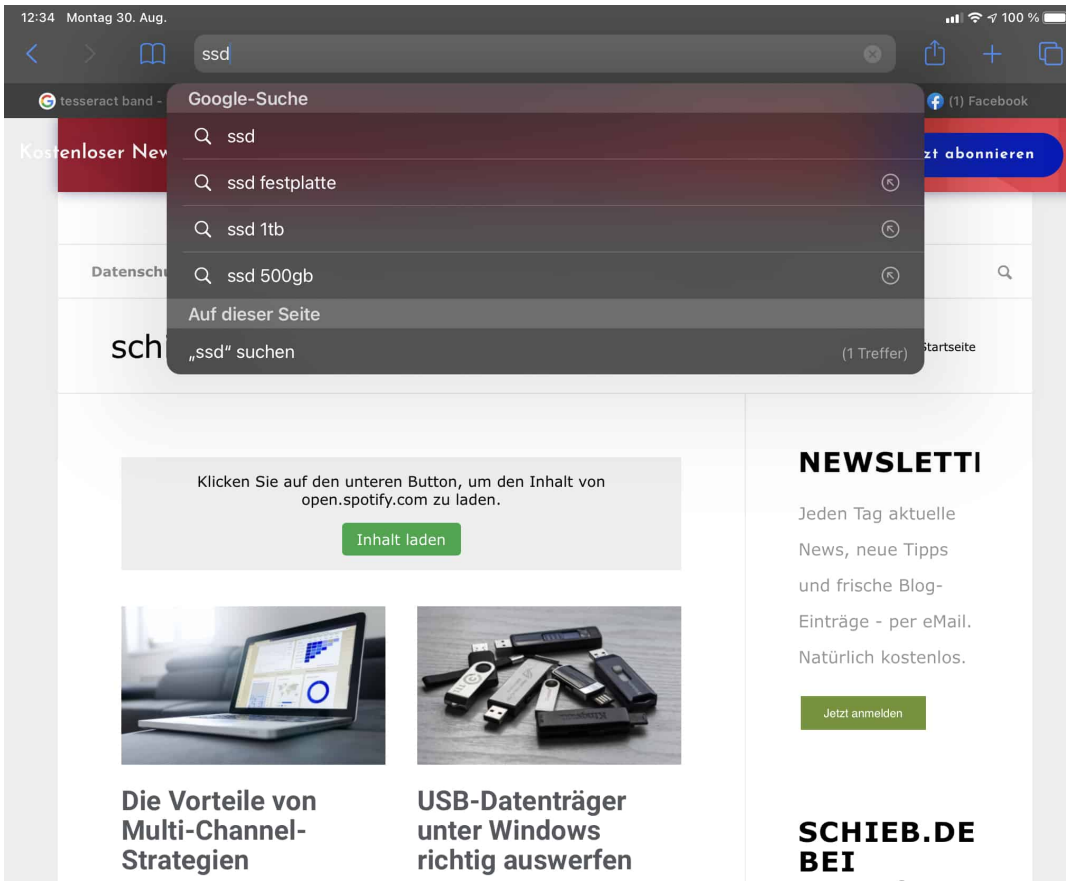


In der Liste zeigt Ihnen Signal nun die bereits gekoppelten Geräte an, um ein neues Gerät hinzuzufügen, tippen Sie auf das **Plus-Zeichen**. Nachdem Sie der App Berechtigungen auf die Kamera erteilt haben, können Sie den QR-Code scannen. Signal gibt die Freigabe, die Tablet-Version fragt Sie nach einem Namen für das Tablet und gewährt dann Zugriff auf die Nachrichten.

Suchen in einer Webseite in Safari

Safari ist als Browser nicht so verbreitet wie Chrome und Firefox, für alle Nutzer von macOS und iOS ist er aber der Standard. Gerade bei den mobilen Geräten wie dem iPad und iPhone gehen Ihnen einige Funktionen verloren, die auch in der Anwendung unterwegs wichtig sind. Auf einer umfangreichen Webseite ein bestimmtes Thema zu finden beispielsweise scheitert an der fehlenden Suchmöglichkeit. Es sei denn, Sie lesen weiter!

Bei einem Desktop-Browser können Sie im Regelfall die Tastenkombination **Strg+F** nutzen, um ein Suchfenster aufzurufen und auf der aktuellen Webseite nach einem Begriff zu suchen. Das funktioniert bei den mobilen Versionen anders, ist aber auch genauso möglich.



Tippen Sie auf der Seite, die Sie durchsuchen wollen, in die Adressleiste und geben Sie den Suchbegriff ein. Safari ergänzt diesen wie gewohnt mit möglichen Webergebnissen. In dieser Liste sehen Sie ganz am Ende die Rubrik **Auf dieser Seite**. Darunter finden Sie die Zahl der Vorkommen des Suchbegriffes aus der Seite. Tippen Sie darauf.

Die Vorteile von Multi-Channel-Strategien

30. Aug. 2021

Wer etwas zu verkaufen hat – egal ob Ideen, Dienstleistungen oder Produkte – nutzt heute das Internet. Für Marketing und Vertrieb. Wer dabei erfolgreich sein

Weiterlesen »

USB-Datenträger unter Windows richtig auswerfen

30. Aug. 2021

Die Festplatten oder SSDs eines PCs sind mittlerweile großzügig bemessen und reichen für so manche Datei und viele Programme vollkommen aus. Trotzdem haben Sie immer

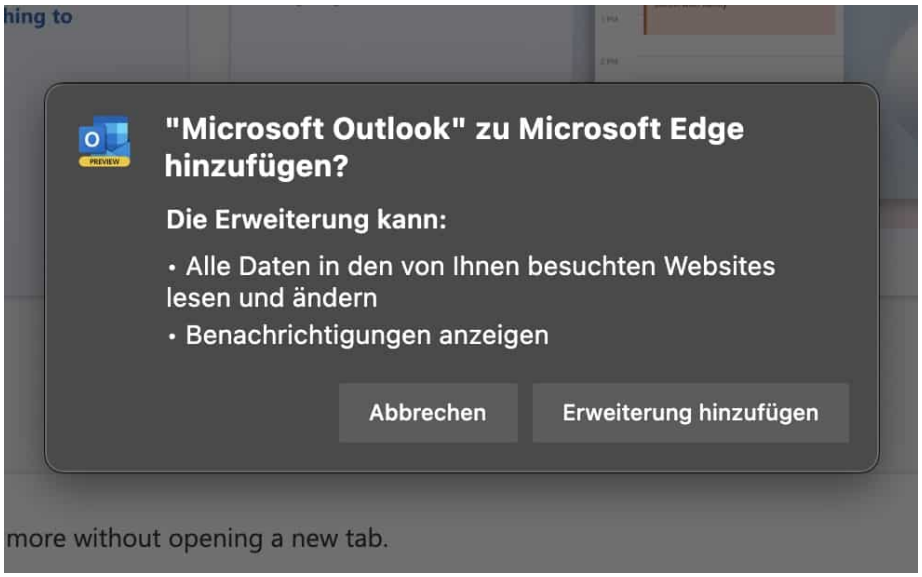
Weiterlesen »

Safari springt jetzt zum ersten Suchergebnis und markiert dieses gelb. Sollten weitere gefunden worden sein, dann haben Sie am Ende der Seite einen Pfeil, mit dem Sie jeweils zum nächsten Vorkommen auf der Seite gelangen können.

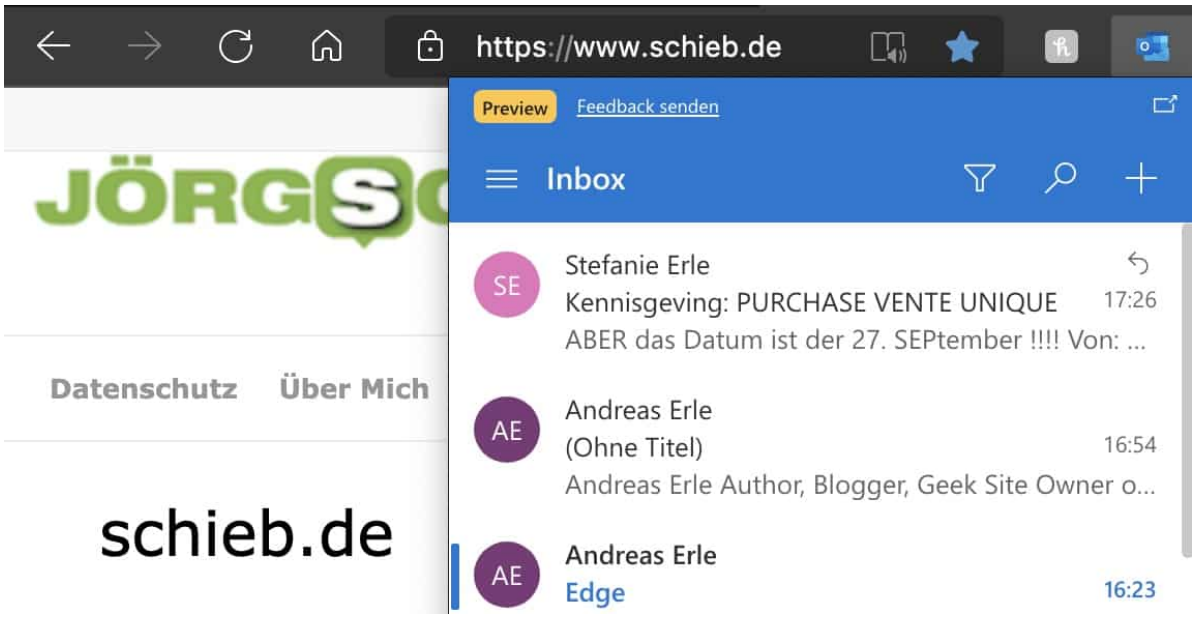
Microsoft Outlook als Erweiterung in Edge laufen lassen

Wenn Sie intensiv an Ihrem PC arbeiten, dann ist jeder unnötige Klick ein Klick zu viel. Einen guten Teil Ihrer Zeit verbringen Sie im Browser. Wenn Sie dann auf Ihre E-Mails zugreifen sollen, dann müssen Sie immer wieder erneut den Webmailer aufrufen oder in Outlook als App wechseln. Wenn Sie ein Microsoft-E-Mail-Konto wie Outlook.com oder Microsoft/Office 365 verwenden, dann geht das viel einfacher!

Die einzige Voraussetzung ist die Verwendung von Microsoft Edge, der in Windows 10 und 11 der Standardbrowser ist. Für den gibt es nämlich eine Browsererweiterung, die Outlook in Edge integriert. Laden Sie sich diese kostenlos hier herunter. Bestätigen Sie dann die Berechtigungen, die die Erweiterung benötigt:



Nach erfolgreicher Installation haben Sie in der Symbolleiste von Edge ein zusätzliches Symbol für Outlook zur Verfügung. Wenn Sie das erste Mal darauf klicken, dann müssen Sie sich mit dem E-Mail-Konto anmelden, das Sie verwenden wollen. Leider geht das immer nur mit einem Konto gleichzeitig!



Nach dieser ersten Einrichtung können Sie dann mit einem Klick auf das Symbol Ihren Posteingang öffnen, Mails anklicken und lesen und sogar darauf antworten. All das, ohne die aktuelle Webseite zu schließen oder zu verlassen!

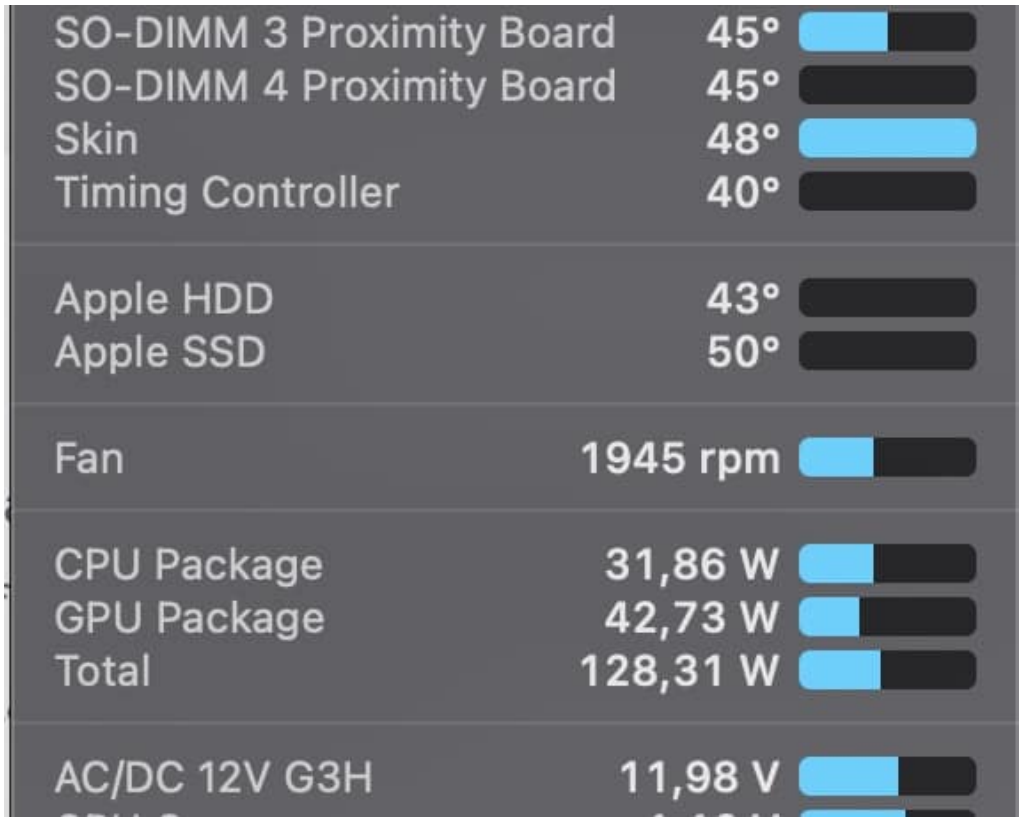
Laptopkühler: Placebo oder Hilfe?

Sie stellen Ihren Laptop auf den Schoß, und er verbrennt Ihnen die Oberschenkel. Alternativ können Sie den Ton des Films, den Sie gerade ansehen, nicht mehr hören, weil der interne Lüfter so laut ist. Ist ein Laptop-Lüfter nötig, oder helfen auch Bordmittel? Wir forschen nach!

Die immer wieder empfohlene Lösung ist der Laptop-Lüfter, wie Sie ihn bei allen großen Online-Shops bekommen. Eine echte Lösung ist der aber nicht unbedingt, er versucht nur, die Symptome des Problems zu lindern. Wir zeigen Ihnen, wo Sie nachschauen sollten!

Zuerst: Der Lüfter Ihres Notebooks wird automatisch gesteuert und sollte immer so schnell laufen, dass die Wärme von den Komponenten abgeführt wird. Das funktioniert aber nur, wenn dieser auch frei ist. Vermeiden Sie also, die Lüftungsschlitze zu verdecken. Kontrollieren Sie, ob diese frei sind und nicht beispielsweise durch Staub oder andere Gegenstände verstopft. Unter Windows können Sie mit der App SpeedFan, unter macOS mit den iStat Menus den Status

des Lüfters sehen und über die Temperaturen der einzelnen Komponenten identifizieren, welche für die Wärme verantwortlich ist.



Ist beispielsweise beim Notebook der rechte Thunderbolt-Port deutlich wärmer als der andere, dann ist dort mit hoher Wahrscheinlichkeit ein Zubehör angeschlossen, das viel Strom zieht. Gönnen Sie diesem beispielsweise einen Hub mit eigenem Netzteil, dann wird das Notebook weniger belastet und in der Folge weniger warm.

Ebenfalls hilfreich: Schauen Sie sich an, welche Apps und Dienste laufen. Oft sind das viel zu viele, die einfach nur CPU-Kapazität in Anspruch nehmen, den PC warm machen, Ihnen aber nicht wirklich einen Vorteil bringen. Beenden Sie diese und ändern Sie die Konfiguration, sodass sie gar nicht mehr automatisch gestartet werden!

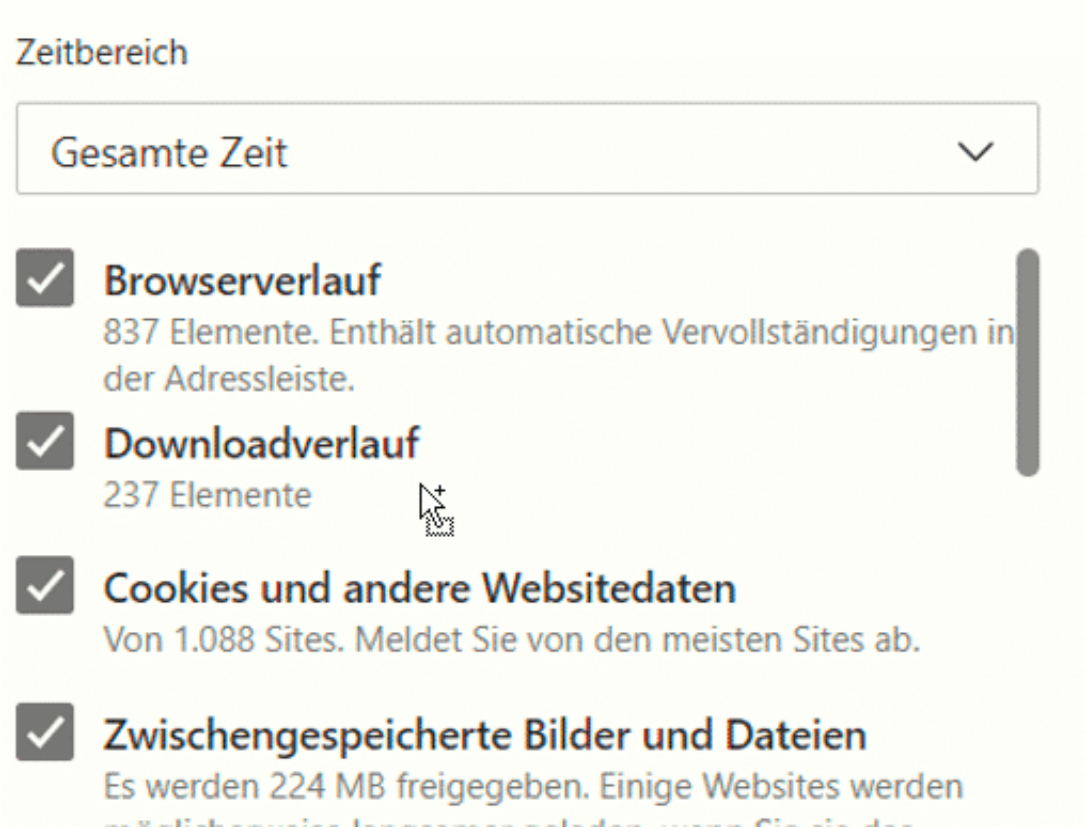
Bleibt Ihr Gerät dann immer noch warm, dann können Sie sich Gedanken über einen Lüfter machen, der die Wärme wegtransportiert.

Löschen des Verlaufs in Microsoft Edge

Der Verlauf im Browser zeigt Ihnen über eine lange Zeit an, welche Seiten Sie besucht haben. Wenn Sie im Eifer des Gefechts von einer auf die nächste Seite gewechselt sind und später wieder dahin zurückwollen, dann geht das über den Verlauf ohne große Anstrengungen. Auf der anderen Seite: Manchmal wollen Sie bestimmte Seiten einmal aufrufen, aber verhindern, dass diese in Ihrem Verlauf auftauchen. Dann können Sie diese auch wieder löschen!

Der Verlauf gibt einen guten Überblick über das, was Sie im Internet gemacht haben. Sowohl die Seiten an sich als auch der Zeitpunkt des Aufrufs sind für Unberechtigte eine tolle Informationsquelle, was Ihnen nicht recht sein dürfte. Es macht also Sinn, diese Daten regelmäßig durchzuschauen und zu löschen.

Dazu klicken Sie im Verlauf auf die **drei Punkte** und dann auf **Browserdaten löschen**. Edge zeigt Ihnen nun eine Übersicht der gespeicherten Informationen in Edge. Unter **Zeitbereich** können Sie auswählen, für welchen Zeitraum Sie die Browserdaten löschen wollen.



Um nicht gespeicherte Daten zu verlieren, die Sie noch verwenden wollen, achten Sie auf die Häkchen: Im Standard sind alle Kategorien aktiviert, wenn Sie nur den Verlauf löschen wollen, dann entfernen Sie die anderen Haken!

Neben dem Verlauf können Sie noch den Downloadverlauf, die Cookies, zwischengespeicherte Dateien und Kennwörter löschen. Wenn Sie auf einem fremden Rechner gesurft haben, dann macht das Löschen aller Kategorien Sinn!