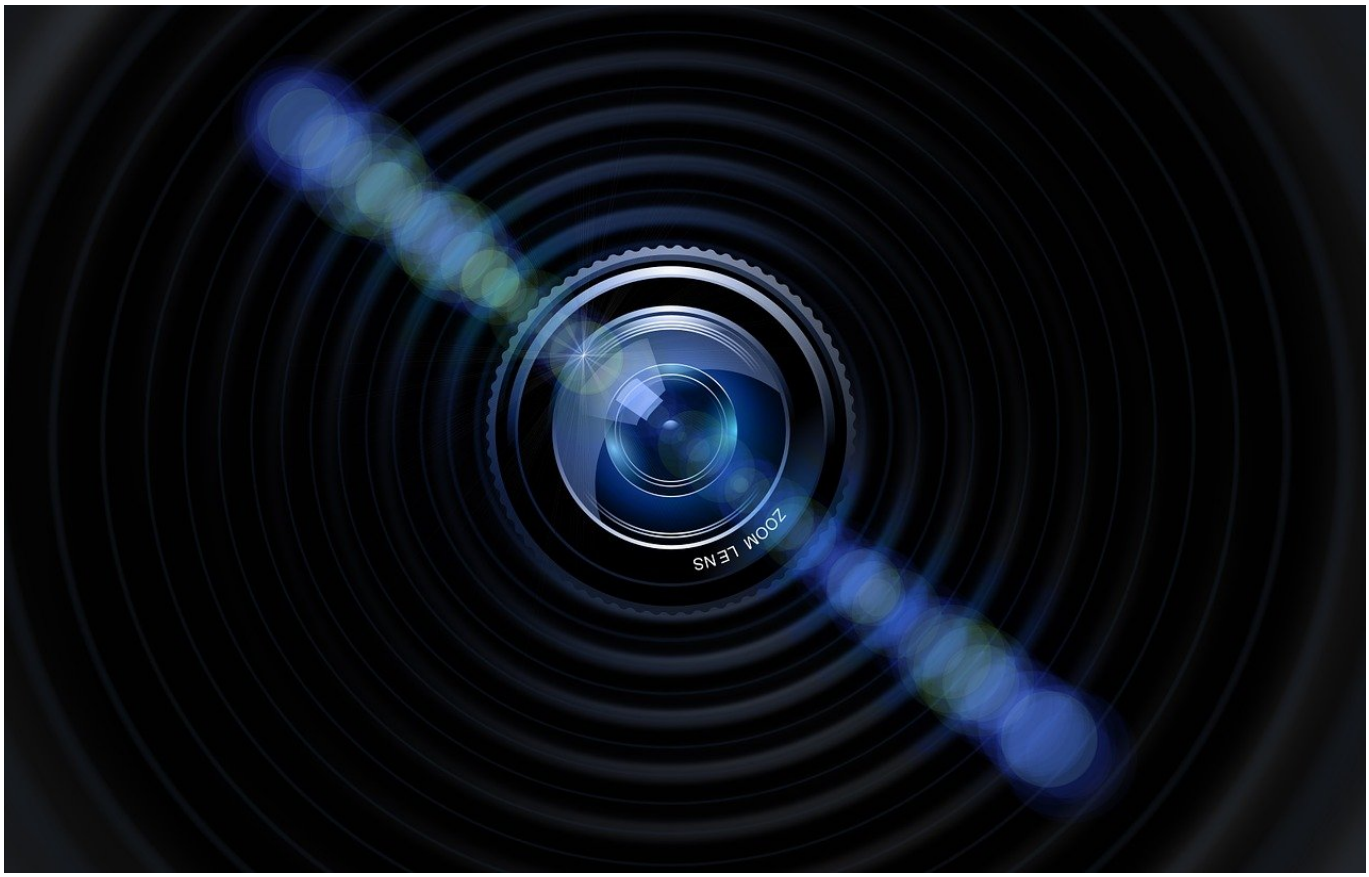
Schieb Report

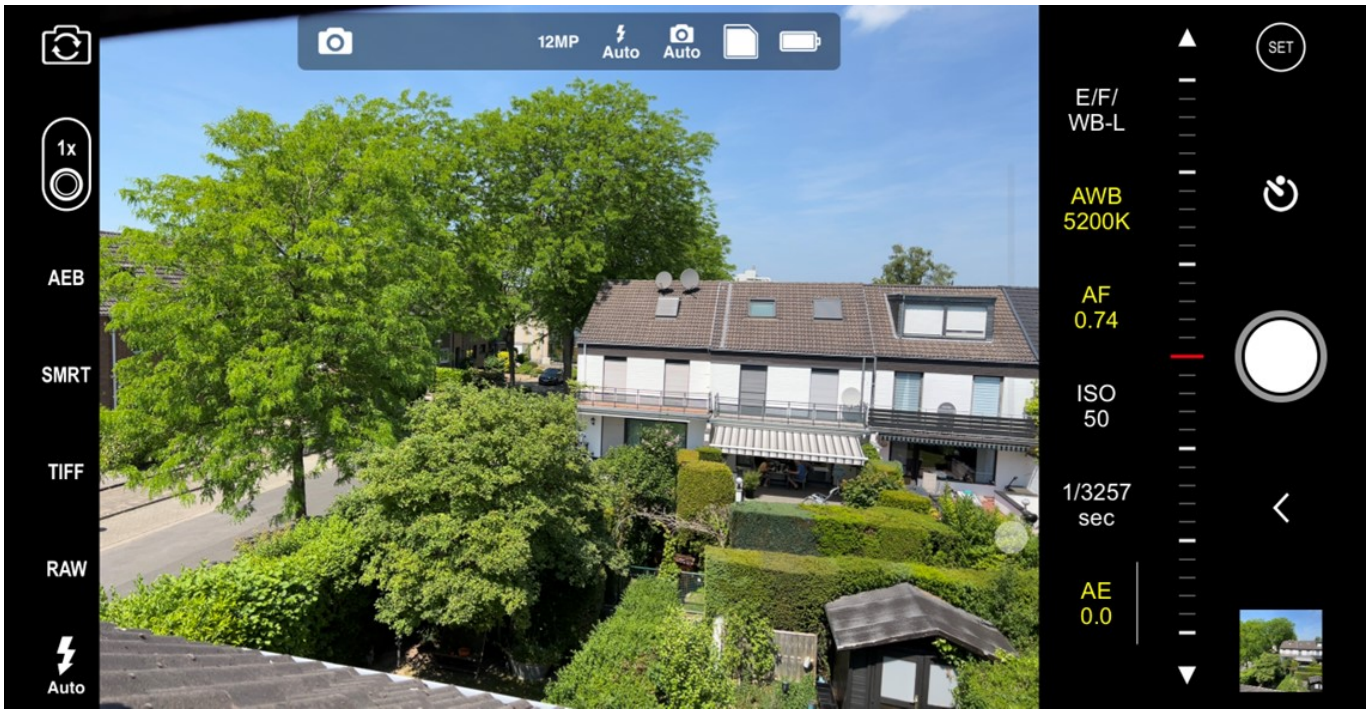
Ausgabe 2022.21

Tipps für bessere Fotos mit dem Smartphone



Das Smartphone ist Eure Immer-dabei-Kamera. Auch wenn Ihr meist Schnappschüsse macht, könnt Ihr Einstellungen beeinflussen. Wir zeigen Euch, was dabei wichtig ist!

Die Kamera ist bei einem Foto nur einer der Faktoren, die das Endergebnis bestimmen. Auch mit einer Smartphone-Kamera der Mittelklasse könnt Ihr tolle Fotos machen. Vor allem dann, wenn Ihr manchmal von den Standardeinstellungen abweicht. Dazu solltet Ihr entweder den Profi Modus bei Android aktivieren oder bei einem iPhone die App ProCam installieren.



Die technischen Werte

Die Blende: Je größer die Öffnung im Objektiv ist, desto mehr Licht kann einfallen. Wenig logisch: Je kleiner die Öffnung, desto größer der Blendenwert. Viele Smartphone-Kameras haben eine feste Blende von f2.8, bekommen also viel Licht auf den Sensor. Verstellbare Blenden haben meistens nur die klassischen Digitalkameras.

Die Einstellung der Blende unter anderem auch Auswirkungen auf die Schärfentiefe. Je größer der Blendenwert ist, desto größer ist der Bereich, der scharf dargestellt wird. Das ist wichtig, wenn Ihr das Motiv gleichmäßig scharf haben wollt. Bei einem kleinen Blendenwert ist das schwieriger zu erreichen.

Die Verschlusszeit: Diese regelt, wie lange der virtuelle Film (der Sensor der Kamera/des Smartphones) Licht bekommt. Die Verschlusszeit hat vor allem bei bewegten Objekten Auswirkungen. Am Beispiel eines Wasserstrahls: Bei kurzer Verschlusszeit erkennt Ihr einzelne Tropfen, bei längerer Verschlusszeit den Wasserstrahl als Ganzes. Bei Fotos von sich bewegenden Objekten entsteht bei längerer Belichtungszeit eine Bewegungsunschärfe, die durchaus als künstlerischer Effekt genutzt werden kann.

Auch für Nachaufnahmen ist die Verschlusszeit entscheidend: Detail-Fotos vom Mond – der ja sehr hell ist – gelingen nur mit ganz kurzer Verschlusszeit,

Aufnahmen der Sternenhimmels nur mit langer.

Die Verschlusszeit lässt sich auch bei den meisten Smartphones manuell verändern, bei Digitalkameras dann, wenn Ihr den automatischen Modus ausschaltet.

Der ISO-Wert: Früher ein Qualitätsmerkmal für die Empfindlichkeit der Filme at der ISO-Wert hat er auch bei Digitalkameras seinen Sinn: Je höher der Wert, desto mehr reduziert sich die notwendige Belichtungszeit. Das hat allerdings auch Auswirkungen auf die Bildqualität, das Rauschen des Bildes nimmt mit höherem ISO-Wert zu. Auch der ISO-Wert lässt sich manuell auf den meisten Smartphones und Digitalkameras einstellen.

Ihr merkt schon: Viele manuelle Einstellungen, die natürlich auch Wechselwirkungen haben. Am Beispiel des Mondfotos: Die Verkürzung der Belichtungszeit reicht nicht aus, wenn Vollmond am klaren Himmel fotografiert werden soll, der Mond ist so hell, dass er auch bei der kürzesten Belichtungszeit noch grell und ohne Details aufgenommen wird. Wenn Ihr dazu aber noch den ISO-Wert reduziert, den virtuellen Film also unempfindlicher macht, dann gelingt ein tolles Foto auch mit einem Smartphone.

Probiert mit den Einstellungen in verschiedenen Situationen, um Erfahrungen zu gewinnen. Wenn Ihr spezielle Fotos machen wollt, dann findet Ihr im Internet eine Vielzahl von Artikeln, die Euch einen Überblick geben welchen Wert Ihr in welche Richtung verändern müsst!

Das Motiv: Auswahl und Schärfe

Die beste Optik, die professionellsten Einstellungen nützen wenig, wenn das Motiv das nicht hergibt. Das hat zwei Dimensionen: Zum einen ist die Auswahl des Motivs wichtig. Was lohnt sich, zu fotografieren, und was nicht? Wie groß ist das Motiv im Bildausschnitt? Wo im Bild befindet es sich?

Eine pauschale Einschätzung ist schwer, einige Tipps, die auch auf einem Smartphone leicht umsetzbar sind, können wir Euch aber geben:

- Verwendet den Goldenen Schnitt für die Position von Objekten: Teilt Euch im Kopf den Bildschirm in drei horizontale und drei vertikale Bereiche auf. Objekte sollten immer an den Schnittpunkten der Linien sein. Das hat

etwas mit der realistischen Darstellung zu tun: Es wirkt authentischer, wenn das Objekt nicht genau in der Mitte ist, sondern ein wenig davon abweichend.

- Stellt sicher, dass das Motiv scharf ist. Die meisten Smartphone-Kameras erlauben es, durch Antippen auf dem Bildschirm das Objekt festzulegen, das scharf gestellt wird.
- Haltet die Kamera ruhig, um Verwacklungen zu vermeiden.
- Haltet die Kamera gerade. Vor allem bei Schnappschüssen geht das leicht unter. Auch wenn der schiefe Horizont im Hintergrund nicht schadet, der Betrachter merkt das aber trotzdem.

Apples App-Store unterstützt laut Hersteller 400.000 Arbeitsplätze in Deutschland

Apple hat zum ersten Mal detaillierte Zahlen über den App-Store auch für Deutschland bekannt gegeben. Danach hängen an Apples App-Store rund 400.000 Arbeitsplätze in Deutschland - zumindest teilweise.

Mehr als 250 deutsche Entwickler haben bislang am **App Store Foundations Programm** teilgenommen. Ein Programm, das vor allem kleineren Unternehmen hilft zu wachsen und erfolgreich zu sein

Die iOS App-Economy hat sich auch im Jahr 2021 als ein Motor für wirtschaftliches Wachstum und ein Quelle für Chancen erwiesen. Sie unterstützt in Deutschland mehr als 400.000 Arbeitsplätze — ein Plus von 11 Prozent seit 2020. Dabei hat sie kleinen Unternehmen zu mehr Erfolg denn je verholfen. Dieses Wachstum spiegelt einen ähnlichen Trend in Europa wider, wo die iOS App-Economy auf 2,2 Millionen Arbeitsplätze gewachsen ist — ein Anstieg von 7 Prozent seit dem letzten Jahr.

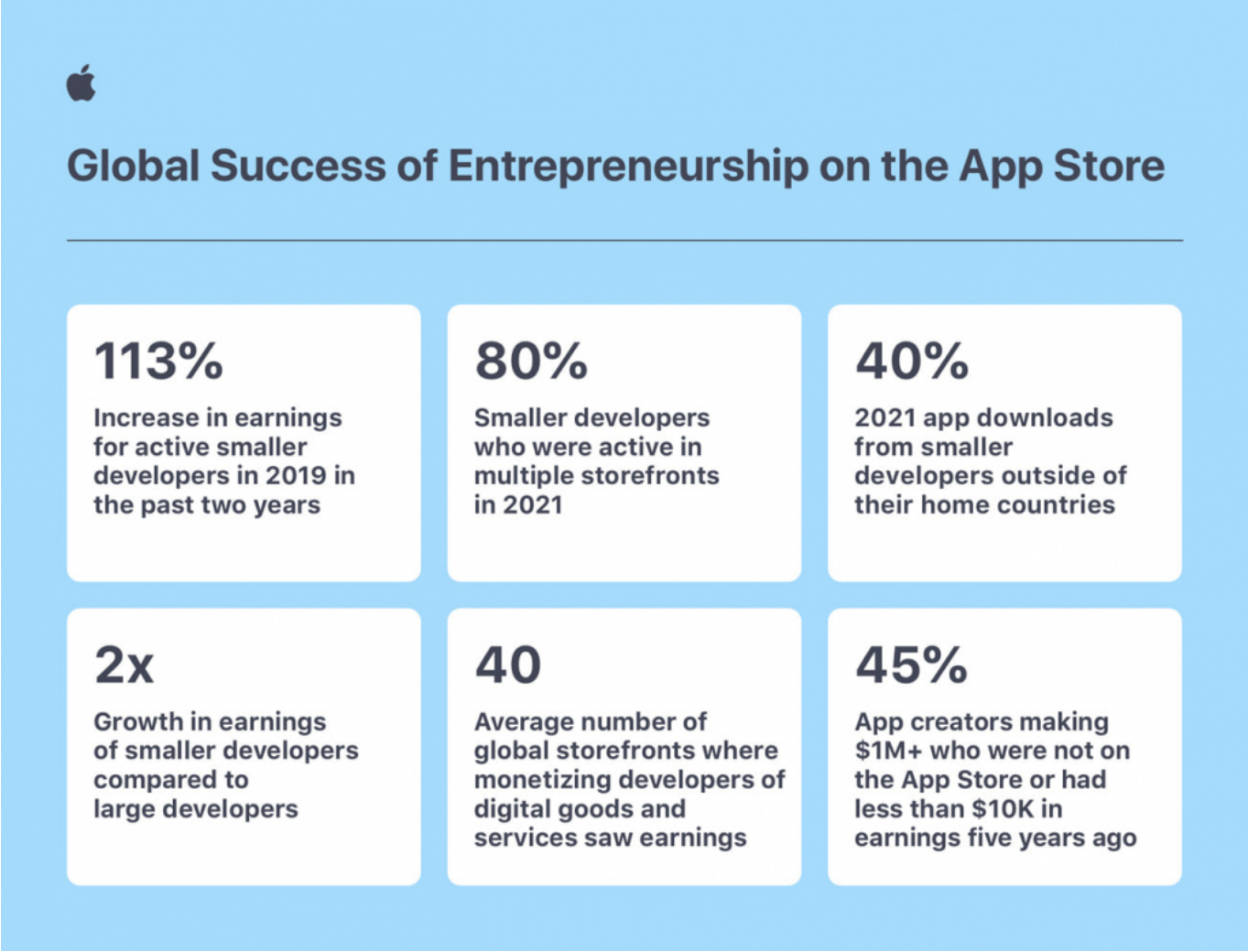
Studien belegen den Effekt

Zwei neue Studien zeigen, dass die iOS App-Economy Unternehmer:innen hilft, neue Firmen zu gründen, innovativ zu sein, Kund:innen auch während der Pandemie zu erreichen sowie ihre Teams von Programmierer:innen, Designer:innen und Kreativen zu vergrößern. So sind sie Teil eines der erfolgreichsten und innovativsten Marktplätze auf der Welt.

Eine neue Studie mit dem Titel „Spotlight on Small Business & App Creators on the App Store“, die von unabhängigen Ökonomen der Analysis Group durchgeführt worden ist, hat ergeben, dass die Einnahmen von Entwickler:innen in den letzten zwei Jahren deutlich gestiegen sind. Während die Umsätze aller Entwickler:innen angewachsen sind, sind besonders die Einnahmen kleinerer Entwickler:innen, die seit 2019 im App Store aktiv sind, in den letzten zwei Jahren um 113 Prozent gestiegen. Damit haben sie das Umsatzwachstum großer Entwickler:innen um mehr als das Doppelte übertroffen. In Deutschland verzeichneten diese kleineren Entwickler:innen, die per Definition einem Umsatz von bis zu eine Million US-Dollar und weniger als eine Million Downloads pro Jahr erzielen, einen Anstieg der Einnahmen um 76 Prozent seit 2019.

Darüber hinaus beleuchtet eine weitere, neue Studie des Progressive Policy Institute die Schaffung von Arbeitsplätzen in der iOS App-Economy. Diese Studie untersucht, wie die iOS-App Economy beigetragen hat, Millionen von Arbeitsplätzen zu schaffen — in Bereichen wie Softwareentwicklung, Vertrieb, Design und mehr.

Zusammengenommen zeigen diese Studien, dass in den letzten zwei Jahren immer mehr Unternehmen Apps eingesetzt haben, um Kunden auf innovative Weise zu erreichen. Diese digitalen und hybriden Trends haben sich auch dann fortgesetzt, nachdem die COVID-bedingten Einschränkungen in vielen Teilen der Welt aufgehoben worden sind. Die Entwickler:innen und ihre Apps haben Menschen geholfen, neue und oft dauerhafte Wege zu finden, um mit Kolleg:innen zusammenzuarbeiten, Unterhaltung zu finden, Kreativität weiterzuentwickeln und mit Freund:innen und Familie in Kontakt zu bleiben.



Unterstützung deutscher Entwickler durch das App Store Foundations Programm

Apple hat inzwischen mehr als 250 deutsche Entwickler:innen durch das App Store Foundations Programm unterstützt. Das Programm ist 2018 erstmals eingeführt worden und bietet ausgewählten Entwickler:innen zusätzliche Unterstützung bei der Entwicklung noch besserer Apps. Die Entwickler:innen lernen, wie sie ihr Geschäft am besten ausbauen und die Reichweite ihrer Apps vergrößern können, wie sie die innovativen Technologien und APIs von Apple nutzen, wie sie ihre Inhalte stärken, um bei Nutzer:innen höhere Resonanz zu erzielen, und wie sie ihre Präsenz im App Store optimieren können.

„Deutschland ist die Heimat so vieler brillanter und kreativer Entwickler:innen, und wir freuen uns sehr, dass der Bereich weiter wächst und eine Rekordzahl von

Arbeitsplätzen unterstützt“, sagt Christopher Moser, Senior Director App Store bei Apple. „Menschen weltweit nutzen Apps, die von talentierten und innovativen deutschen Entwickler:innen entwickelt werden, um ihnen das Leben, Arbeiten und Spielen zu erleichtern. Apple ist stolz darauf, einen Teil zu diesem Erfolg beizutragen, und wir freuen uns darauf, Entwickler:innen dabei zu unterstützen, neue Ziele zu erreichen."

Vectornator ermöglicht es Anwender:innen unterwegs anspruchsvolle Illustrationen, spektakuläre Layout-Mockups und ausdrucksstarke Schriftzüge zu erstellen. Der Gründer Vladimir Danila ist ein Gewinner des Student Scholarships zur Worldwide Developer Conference (WWDC) von Apple gewesen, und die App ist in einer Keynote von Apple vorgestellt worden.

Eigenes App-Ökosystem

In ihrer Studie „Spotlight on Small Business & App Creators on the App Store“ untersuchen die Ökonomen der Analysis Group, wie Unternehmer:innen in der iOS App-Economy weiterhin innovativ sind und wachsen. Insgesamt zeichnet die Studie das Bild eines wachsenden und dynamischen App-Ökosystems, in dem sich Chancen bieten und Innovationen entwickeln.

Im Jahr 2021 sind Tausende von kleinen Unternehmen und neuen App-

Entwickler:innen aus der ganzen Welt in den App Store dazugekommen. Von diesen neuen Entwickler:innen stammen etwa 24 Prozent aus Europa, 23 Prozent aus China, 14 Prozent aus den USA, 4,3 Prozent aus Japan und 34 Prozent aus anderen Regionen wie Korea, Indien und Brasilien. In den letzten zwei Jahren ist die Zahl der kleineren und aufstrebenden Entwickler:innen im App Store gestiegen - in Großbritannien beispielsweise ist die Zahl kleiner Entwickler:innen, die neu in den App Store kommen, seit 2019 um fast 40 Prozent gestiegen, in Deutschland um über 25 Prozent.

Da diese Entwickler:innen die Möglichkeiten des App Stores nutzen, die den Vertrieb von Apps in 175 weltweiten Märkten erleichtern, sind im Jahr 2021 etwa 40 Prozent aller Downloads von Apps kleiner Unternehmen und aufstrebender App-Entwickler:innen von Nutzer:innen außerhalb der Heimatmarkts der Entwickler:innen erfolgt.

Die Studie zeigt auch, dass der App Store Unternehmer:innen geholfen hat, neue Apps auf den Weg zu bringen und ihre Unternehmen schnell zu vergrößern. Um die Wachstumsmethoden von Entwickler:innen zu analysieren, die im Jahr 2021 mehr als 1 Million Dollar im App Store verdient haben, haben die Ökonomen einen längeren Zeitraum beobachtet und festgestellt, dass 45 Prozent der heutigen großen Entwickler:innen vor fünf Jahren entweder gar nicht im App Store vertreten gewesen sind oder weniger als 10.000 US-Dollar verdient haben.

Die vollständige Studie der Analysis Group zu Small Business & App Creators on the App Store ist ab sofort verfügbar.

Der App Store wurde 2008 gestartet und gilt als sicherer und dynamischer App-Marktplatz. Er umfasst derzeit 1,8 Millionen Apps und wird jede Woche von mehr als 600 Millionen Menschen besucht. Apple stellt den mehr als 30 Millionen registrierten Entwickler alle Tools, Ressourcen und Unterstützung zur Verfügung, die sie benötigen, um Software für über eine Milliarde Kund:innen auf der ganzen Welt auf Apple-Plattformen zu entwickeln und bereitzustellen. App Unternehmer:innen können sich zusätzlich für das App Store Small Business Program qualifizieren, das ihnen eine auf 15 Prozent reduzierte Provision gewährt. Es unterstützt kleine und individuelle Entwickler:innen, die bis zu 1 Million US-Dollar Umsatz erzielen und die Innovationen für die nächste Generation an Apps vorantreiben.

Wenn der Finder in macOS nicht mehr läuft

Wenn Apps nicht mehr funktionieren, dann ist das schon ärgerlich. Wenn eine App aber gleichzeitig integraler Teil des Systems ist, dann sind die Auswirkungen meist noch schlimmer. Beim Finder gibt es diverse Ansätze, das zu lösen.

Dateien öffnen nicht mehr, die Dock ist statisch und nicht mehr bedienbar, Apps aber laufen immer noch? Das lässt darauf schließen, dass der Finder von macOS sich aufgehängt hat. Der ist - wie der Explorer bei Windows - nicht nur die interne App zur Verwaltung von Dateien, sondern auch der Hintergrundprozess, der die komplette Oberfläche des Systems steuert.

Wenn gerade ein größeres Update von macOS verfügbar ist und noch auf seine Installation wartet, dann installiert dies erst und probiert nach dem Neustart ob das Problem nicht dadurch sowieso schon gelöst ist. Manchmal ist das aber nicht der Fall.

In einer solchen Situation habt Ihr verschiedene Optionen:

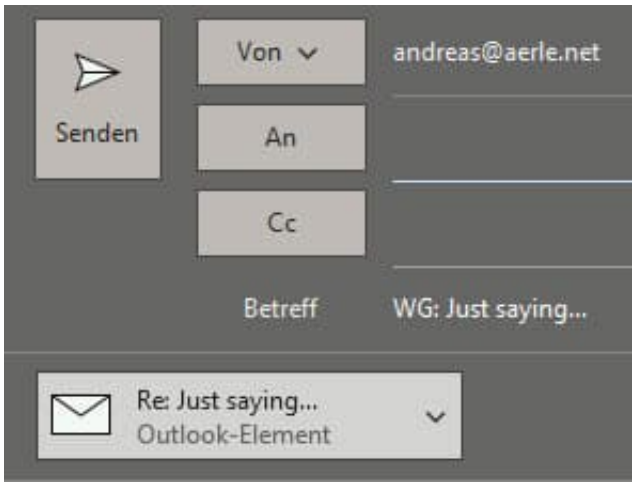
1. Klickt auf den Apfel oben links auf der Oberfläche, dann auf **Sofort beenden**. Sucht den Finder heraus, klickt ihn an und dann auf **Neu starten**. Der Finder sollte neu starten und wieder funktionieren.
2. Hilft das nicht, dann startet den Mac neu, gegebenenfalls sind es mehrere Prozesse, die sich blockieren. Ein Neustart startet sie alle erneut.
3. Wenn das immer noch nicht hilft, dann ist die letzte einfache Möglichkeit das Löschen der Einstellungen des Finders: Ruft mit einem Administrator-Konto das Terminal auf, dann verwendet als Befehl *sudo rm ~/Library/Preferences/com.apple.finder.plist*. Ihr müsst dann die Einstellungen des Finders (Wie Sortierungm anzuzeigende Elemente etc.) wieder neu vornehmen, das ist aber ein kleiner Preis dafür, dass alles andere wieder funktioniert.

Emails mit allen Inhalten weiterleiten in Windows 11

Eine E-Mail weiterleiten ist keine große Kunst. Dabei die Quellinformationen wie den tatsächlichen Absender und Server zu erhalten, schon. Unser Hack hilft Euch dabei!

Normalerweise klickt Ihr eine E-Mail an, dann auf **Weiterleiten** und schon habt Ihr Text und Anhänge in einer neuen E-Mail. Allerdings fehlen dann die gesamten Verwaltungsinformationen. Die sind wichtig, wenn Ihr eine SPAM- oder Virus-E-Mail analysieren lassen wollt.

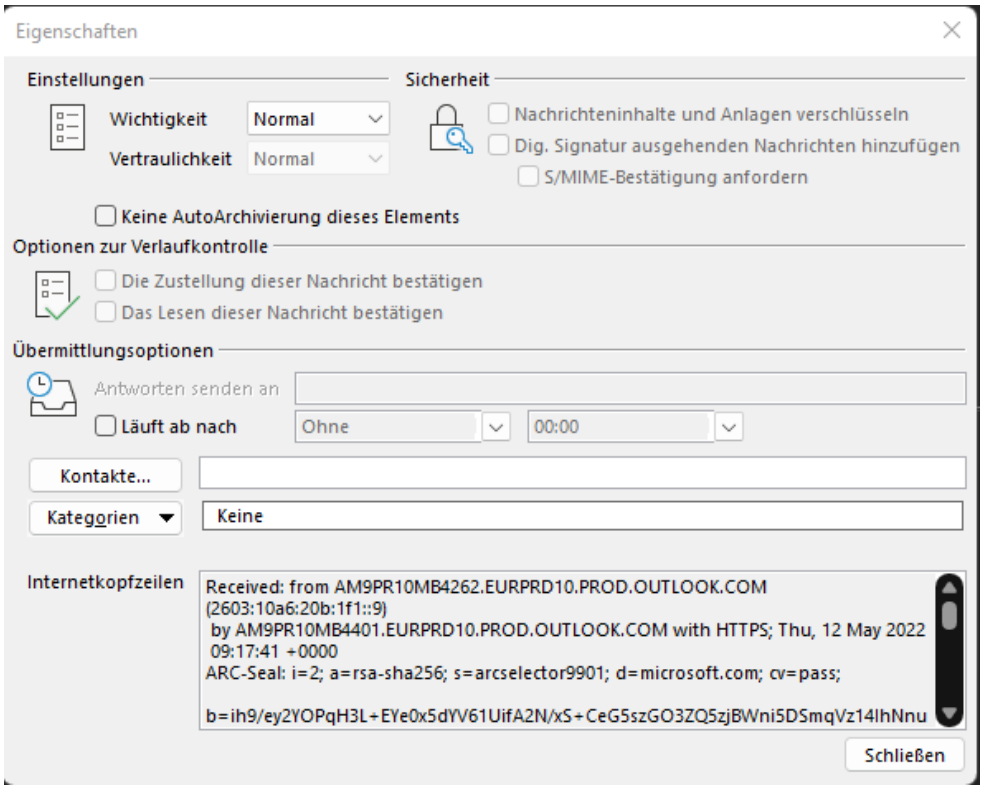
Viel von dem, was von einer E-Mail im Posteingang angezeigt wird, ist aufbereitet. Die Informationen wie der Absendername und der Betreff lassen sich leicht verfälschen, gerade bei SPAM- und Virus-E-Mails ist das ein Problem.



Dazu müsst Ihr diese unverändert komplett (und nicht nur als Textzitat) weiterleiten.

1. Dazu klickt sie im Posteingang von Outlook an und drücken dann gleichzeitig die Tasten **Strg** + **Alt** + **F**.
2. Outlook erzeugt eine neue E-Mail, die die vorher markierte als Dateianhang enthält.
3. Der Empfänger kann diese dann öffnen, als wäre sie direkt an ihn gegangen.

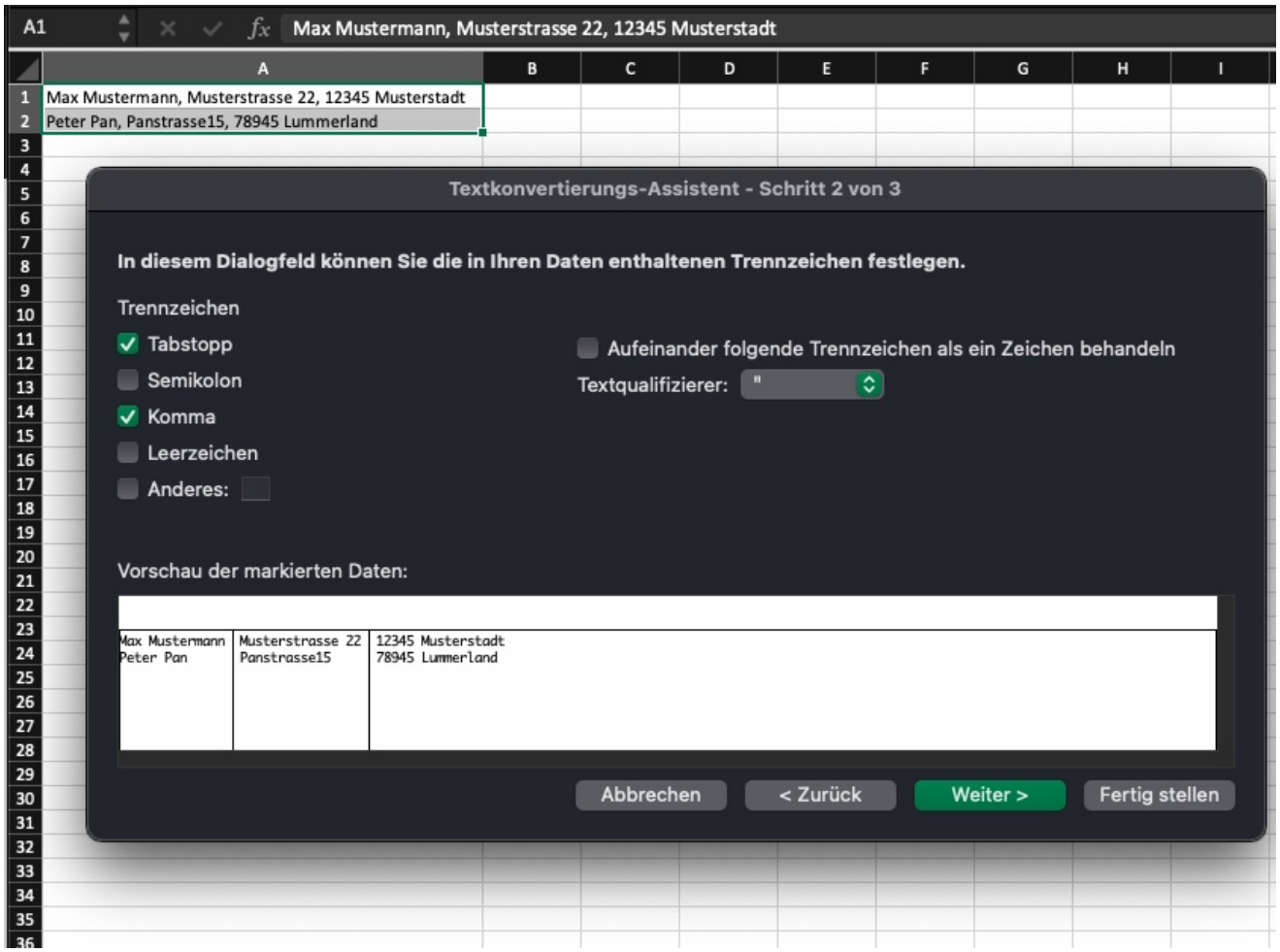
Um die Verwaltungsinformationen zu sehen, öffnet die E-Mail aus dem Posteingang durch einen Doppelklick, dann klickt auf **Datei** > **Eigenschaften**. Im Detailfenster seht Ihr unten unter Internetkopfzeilen all die Metainformationen, die die E-Mail auf ihrem Weg zu Euch mitbekommen hat. Die enthalte die echten Absender und Server, was Euch bei der Analyse helfen kann.


Eigenschaften
Einstellungen
Wichtigkeit
Normal
Vertraulichkeit
Normal
Sicherheit
Nachrichteninhalte und Anlagen verschlüsseln
Dig. Signatur ausgehenden Nachrichten hinzufügen
S/MIME-Bestätigung anfordern
Keine AutoArchivierung dieses Elements
Optionen zur Verlaufkontrolle
Die Zustellung dieser Nachricht bestätigen
Das Lesen dieser Nachricht bestätigen
Übermittlungsoptionen
Antworten senden an
Läuft ab nach
Ohne
00:00
Kontakte...
Kategorien
Keine
Internetkopfzeilen
Received: from AM9PR10MB4262.EURPRD10.PROD.OUTLOOK.COM
(2603:10a6:20b:1f1::9)
by AM9PR10MB4401.EURPRD10.PROD.OUTLOOK.COM with HTTPS; Thu, 12 May 2022
09:17:41 +0000
ARC-Seal: i=2; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=pass;
b=ih9/ey2YOPqH3L+EYe0x5dYV61UifA2N/xS+CeG5szGO3ZQ5zjBWni5DSmqVz14lhNnu
Schließen

Text in Excel in Spalten bekommen

Daten einer Excel-Tabelle werden oft in Dateien geliefert oder finden sich in einer E-Mail. Mehrere Daten-Spalten werden dann schnell zum Problem. Es sei denn, Ihr kennt unseren Hack!

Oft nutzten Datenlieferanten Textdateien im CSV-Format. Darin finden sich die Datensätze in separaten Zellen, die einzelnen Datenfelder (die später in einzelnen Spalten der Excel-Tabelle landen sollen) sind durch Trennzeichen getrennt. Das kann ein oder mehrere Leerzeichen sein, das können aber auch andere Zeichen wie Komma, Semikolon oder Punkt sein. Wenn Ihr die aber kopiert und in Excel einfügt, dann sind sie komplett in einer Spalte.



Wichtig dabei: Ein Zeichen kann nicht mal als Trennzeichen zwischen Spalten, mal als Teil eines Spalteninhalts verwendet werden. An einem Beispiel: Wenn das Leerzeichen ein Trennzeichen sein soll, dann dürfen einzelne Wörter in einer Spalte nicht auch durch ein Leerzeichen getrennt sein. Dann würden sie nämlich als neue Spalte erkannt.

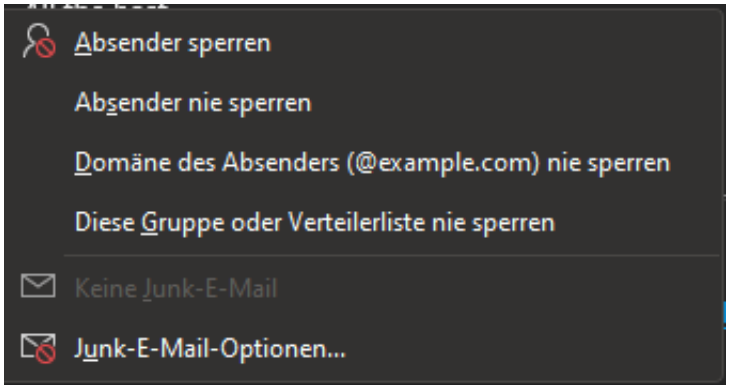
Markiert die Spalten, die getrennt werden sollen, dann klickt in der Registerkarte **Daten** auf **Text in Spalten**. Excel startet den Textkonvertierungs-Assistenten und lässt Euch festlegen, ob die Spalten im Text eine **feste Breite** haben oder ein **Trennzeichen**.

Nach einem Klick auf **Weiter** könnt Ihr dann festlegen, welche Zeichen als Trennzeichen erkannt werden sollen. Excel erzeugt nach jedem Trennzeichen eine neue Spalte.

Junk oder nicht Junk? Es liegt in Eurer Hand!

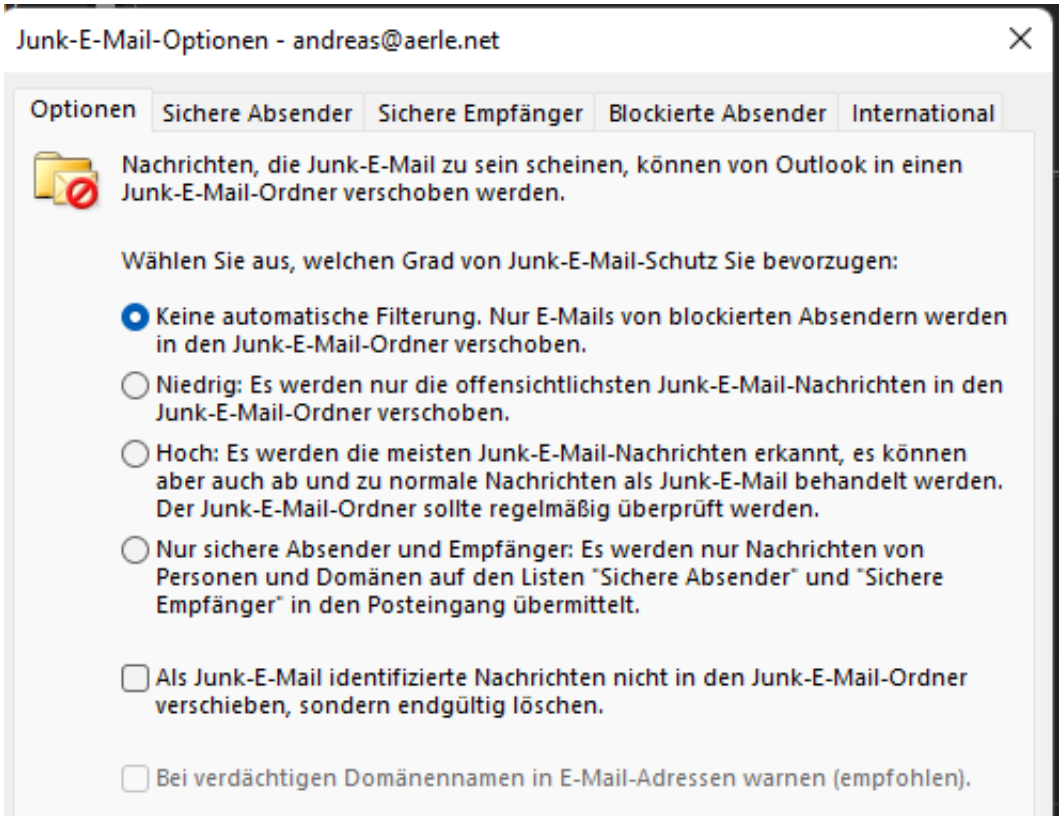
SPAM-Mails nerven. Genauso aber auch die manchmal abstruse Behandlung durch Outlook Wenn Ihr Euren Junk-Filter in Outlook verbessern wollt, dann können wir Euch helfen!

Windows und Outlook versuchen, möglichst viele Dinge zu automatisieren. Dazu gehört auch die Identifikation von E-Mails als unerwünschte Werbung. Das geht in den meisten Fällen gut, immer mal wieder aber auch schief. Wenn Ihr vermehrt Fehlerkennungen in die eine oder andere Richtung habt, dann solltet Ihr die Einstellungen in Outlook kontrollieren:



Klickt mit der rechten Maustaste auf eine E-Mail, auf **Junk-E-Mail** und dann auf

Absender sperren (wenn eine unerwünschte E-Mail durchgekommen ist oder auf **Absender nie sperren**, wenn eine Mail eines Absenders fälschlicherweise als SPAM identifiziert wurde. Das muss gegebenenfalls nochmal wiederholt werden, danach aber werden E-Mails dieses Absenders im Normalfall verlässlich richtig einsortiert.



Wenn das noch nicht ausreicht oder Ihr eine Einstellung detaillierter anpassen wollt, dann klickt mit der rechten Maustaste auf eine E-Mail und dann auf **Junk-E-Mail-Optionen**. Hier könnt Ihr unter **Sichere Absender**, **Sichere Empfänger** und **Blockierte Absender** einzelne Absender klassifizieren.

Manchmal reicht auch das nicht, weil die Absenderadressen wechseln. Oft lassen sich diese aber an den Ländern der Domains erkennen. Dazu klickt auf die Registerkarte **International. Hier könnt Ihr Top-Level-Domains** blockieren, alternativ auch die Codierungen der Nachrichten (die dann vielleicht von einer deutschen Adresse kommen, aber trotzdem russisch codiert sind).

Xingjiang Police Files: Der chinesische Überwachungsapparat

Die Xinjiang Police Files rütteln die Welt auf: Nun kann niemand mehr die Gräueltaten verleugnen. Chinas Überwachungssystem ist zudem gnadenlos - und sollte uns allen eine Warnung sein.

Die **Xinjiang Police Files**: Mehr als 10 GByte an chinesischen Regierungsdaten, als „vertraulich“ klassifiziert – und trotzdem, irgendwie, an die Öffentlichkeit geraten. Die Medien berichten seit Tagen davon. Fotoaufnahmen von Tausenden Gefangener, geheime Reden, Schulungsunterlagen und vieles andere mehr. All das ist in westliche Hände geraten und macht das Grauen sichtbar. Es wird aber auch deutlich, wie engmaschig die Überwachungssysteme in China sind. Nichts und niemand bleibt unbeobachtet, alles wird gesehen und ausgewertet. Ob im Netz – oder in der „echten Welt“.

Quelle des Datenleak unbekannt

Das Datenmaterial, das den Journalisten zugespielt wurde, ist erstaunlich

umfangreich – und vor allem detailreich.

Die eigentliche Quelle der geleakten Daten ist nicht bekannt. Aber irgendjemand hat entweder aus internen Kreisen in China oder – wahrscheinlicher! – durch Hackangriffe in die Computersysteme der chinesischen Sicherheitsbehörden Zugriff auf große Datenmengen des chinesischen Überwachungsapparats bekommen und diese Daten unbemerkt abgezogen. Die Daten wurden dem deutschen Anthropologen Adrian Zenz zugespielt – der schon der Vergangenheit geheime Informationen der verschiedenen Straflager veröffentlicht hat und dem Datenleaker damit vertrauensvoll erschienen ist.

Der Anthropologe hat nach eigenen Angaben nichts dafür bezahlt, es wurden auch keine Bedingungen für die Übergabe gestellt. Er hat die Daten nach große Nachrichtenanbieter weitergegeben, darunter WDR und SZ. Außerdem kann sich jeder die aufbereiteten Daten im Internet anschauen unter www.xinjiangpolicefiles.org. Der Datenleak enthält über 2.800 Fotos, 300.000 persönliche Datensätze von Menschen, 23.000 Datensätze von Häftlingen und auch noch einige genaue Beschreibungen, wie sich die Beamten in den Haftanstalten zu verhalten haben.

Strikte Überwachung und Kontrolle

Alle Bürger in China sind daran gewöhnt: Sie werden überall überwacht, von Kameras. Im Internet sowieso – es herrscht eine strenge Zensur.

Es gibt offensichtlich keinerlei Hemmungen. Im öffentlichen Raum sind praktisch überall Kameras montiert, die jede Bewegung aufzeichnen. Es ist bekannt, dass die Chinesen KI zur Gesichtserkennung einsetzen: Wer die Straße bei rot überquert, wird identifiziert, teilweise öffentlich angeprangert – und auch bestraft. Die KI erkennt jedes Gesicht. Es gibt einen Katalog mit erwünschtem und unerwünschtem Verhalten.

Die Menschen bekommen Punkte gutgeschrieben (**Social Score**), wenn sie sich aus Sicht der Regierung „richtig“ verhalten und Strafpunkte, wenn sie gegen den Regelkatalog verstoßen. Ein Versuch der totalen Kontrolle, der durch Digitalisierung möglich wird. Da es in China praktisch unmöglich ist, sich öffentlich zu wehren oder zu protestieren, entsteht der Eindruck, alle wären einverstanden. Hinzu kommt noch das Projekt „**Goldener Schild**“, das eine nahezu totale

Kontrolle und Überwachung im Internet bedeutet. Die Menschen bekommen viele Inhalte aus dem Ausland nicht zu sehen und werden gleichzeitig engmaschig überwacht. Man könnte sagen, dass die chinesische Regierung die Dystopie von „1984“ locker auf die Spitze getrieben hat. Das ist möglich, weil in China kein Widerspruch geduldet wird.

Auch Diplomaten und Ausländer

Die eigene Bevölkerung auszuspionieren, ist eine Sache. Aber auch Besucher und Gäste sind offenbar nicht davor gefeit, nicht mal Diplomaten.

Als einige Diplomaten sich 2018 die Situation der inhaftierten Uiguren anschauen wollten, wurden sie – obwohl Diplomaten – penibel überwacht. Die Diplomaten berichteten, dass ihre „Überwacher“ alles wussten über sie, wo sie herkommen, wo sie hin wollen, welche Geschichte sie haben. Das könnte man noch als mehr oder weniger normale Geheimdienstarbeit verbuchen – auch wenn die Einschränkungen der Diplomaten eindeutig gegen internationales Recht verstoßen.

Das chinesische Regime hat aber schon mehrfach gezeigt, dass es keine Hemmungen hat, selbst Ausländer zu überwachen. So waren Sportler, Journalisten und Gäste bei den Olympischen Spielen vor einigen Monaten gezwungen, eine offizielle App der chinesischen Regierung zu installieren. Angeblich, um alles besser zu organisieren. Aber in Wahrheit wohl, um die Menschen besser überwachen zu können. Zumindest, wo sie sich aufhalten – vielleicht aber auch mehr. Niemand kann ausschließen, dass solche Apps auch zur Spionage verwendet werden.

Russland setzt andere Schwerpunkte

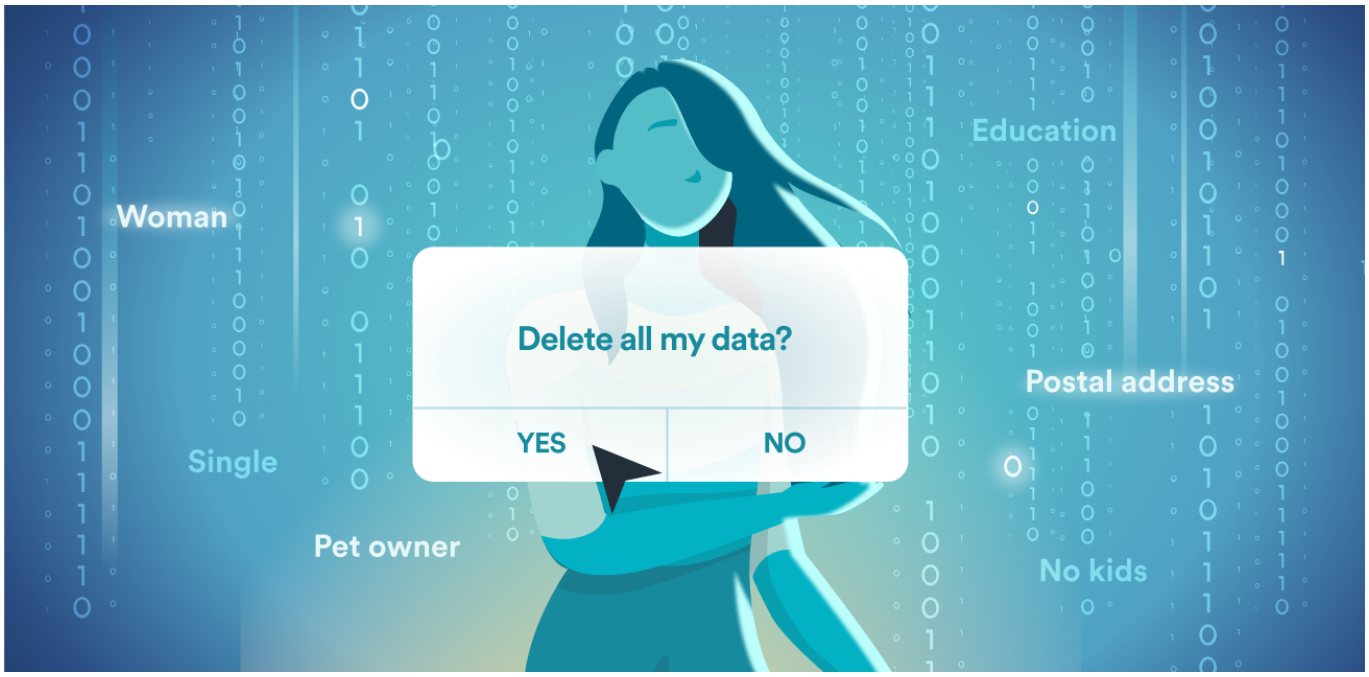
Auch Russland hat ja eine autokratische Regierung und starke Zensur im Netz.

Aber das lässt sich nicht vergleichen. Den Aufwand, den China aktiv betreibt für die Überwachung und Zensur im Netz – aber auch im öffentlichen Raum –, kann Russland gar nicht betreiben. Schon allein technisch nicht: Russland ist technologisch rückständig, China führend. In China wird alles entwickelt, auch KI-

Systeme zur Kontrolle, die rücksichtslos überall eingesetzt oder wenigstens getestet werden. Russland hat so etwas nicht, bzw. müsste solche Technologie teuer einkaufen.

China hat Heerscharen von Mitarbeitern, die das Netz nach unliebsamen Inhalten durchforsten. Nach allem, was wir wissen, hat Russland auch das nicht. Was Russland hat, ist zweifellos der entschlossene Wille zur Kontrolle: Da werden rigide ausländische Inhalte herausgefiltert zum Beispiel. Aber das ist nicht aufwändig. Auffallend aktiv sind vor allem russische Hackerverbunde, die direkt oder indirekt vom Kreml bezahlt werden. Hier liegt eine große Gefahr, vor allem für uns im Westen, weil diese Hackerkollektive rücksichtlos alles angreifen, auch kritische Infrastruktur und sogar Kliniken. Hier ist Russland viel stärker aufgestellt als China.

Incogni: So wehrt Ihr Euch effektiv gegen "Data Broker"



Recht zu haben ist nicht schwer, Recht zu bekommen allerdings schon: Incogni ist ein praktischer Service von Surfshark, der dafür sorgt, dass Data Broker über Euch gespeicherte Daten löschen.

Wir wissen es eigentlich alle - und ergeben uns viel zu häufig: Trotz DSGVO werden jede Menge Daten von uns erhoben und gespeichert. Keineswegs nur Daten, die wir selbst irgendwo eingeben, sondern auch und vor allem Daten, die Tracker in Apps, Anwendungen und auf Webseiten gnadenlos einsammeln und an sogenannte "Data Broker" verkaufen.

Wer die kostenlose App benutzt oder im kostenlosen Game daddelt, bemerkt nicht, dass im Hintergrund diverse Tracker aktiv sind und Daten sammeln. Diese Daten werden eingesammelt und an die Broker verkauft. In der Regel, ohne dass wir es wissen - und ohne unsere ausdrückliche Zustimmung. Wenn überhaupt, gibt es verquaste Paragrafen in den Datenschutzbestimmungen ("Dürfen wir Daten mit Dritten teilen"), die niemand in Frage stellt.

Schlimm genug, dass der Gesetzgeber das erlaubt.

Data Broker werfen ihre Krakenarme aus

Dieses Business ernährt Hunderte von Agenturen weltweit, die auf diese Weise (meist unbemerkt und leise) sensible Daten einsammeln, Datenbanken aufbauen, Profile erstellen und die Daten gewinnbringend verkaufen. Darunter persönliche Daten wie:

- Name
- Alter
- Adresse
- E-Mail-Adresse
- Bewegungsdaten
- Interessen
- Telefonnummer
- Beschäftigungsverhältnisse
- Finanzdaten
- Medizinische Daten

Oft werden diese persönlichen Daten mit der Advertising-ID verknüpft. Das ist eine unverwechselbare ID, die jedes Smartphone besitzt. Sind Datensätze mit dieser eineindeutigen Advertising-PC verknüpft, lassen sich Daten aus unterschiedlichen Quellen (von unterschiedlichen Brokern) mit vergleichsweise geringem Aufwand verknüpfen. Auf diese Weise sind Datenjournalisten und Ermittler zum Beispiel den Personen auf die Schliche gekommen, die im Januar 2021 das Capitol in Washington DC gestürmt haben.

Doch personalisierte Werbung ist nur das geringste Problem hierbei. Die unrechtmäßig eingesammelten Daten werden auch für Scamming (etwa fingierte Telefonanrufe), Identitätsdiebstahl oder Stalking missbraucht.

DSGVO: Recht auf Auskunft

Wir haben grundsätzlich ein Recht - das sieht vor allem die DSGVO vor - von jedem Anbieter oder Onlinedienst zu erfahren, welche Daten er über uns gespeichert hat. Ganz konkret. Das gilt keineswegs nur für die offensichtlichen Kandidaten wie Facebook, Google, Amazon, Microsoft und Co., sondern ganz allgemein. Jede(r) muss diese Auskunft erteilen. Und wir haben auch das Recht, die Löschung der Daten zu verlangen.

Nur: Wer macht das schon? Die meisten Verbraucher denken, die Daten landen

nur bei Google, Facebook, Twitter und Co. Da landen sie auch - aber eben auch bei Hunderten Brokern weltweit.

Hier kommt ein neuer Service ins Spiel, den ich wirklich klasse und sehr interessant finde: **Incogni** von Surfshark.

Wer sich hier anmeldet, kann Incogni damit beauftragen, bei Dutzenden von bekannten Data Brokern (aktuell sind es 130) ganz offiziell - formell und rechtskonform - die Löschung der eigenen persönlichen Daten zu beauftragen. Das macht Incogni vollkommen automatisch. Incogni erledigt sozusagen den "Papierkram": Der Dienst verschickt auf unseren Wunsch entsprechende Schreiben (in der Regel E-Mails) an die bekannten Data Broker dieser Welt. E-Mails. formal formuliert und juristisch korrekt, die - in unserem Namen - die entsprechende Auskunft verlangen.

Rund 130 solcher Broker hat Incogni bereits in seiner Datenbank. Weltweit soll es mindestens 1200 Broker geben. Die Liste der Broker, die Incogni automatisiert anschreibt, um unsere Interessen und Rechte durchzusetzen, wird stets länger und umfangreicher.

PRO

- Verschickt automatisch offizielle Lösch-Anforderungen an Data Broker
- Trackt die Antworten der Broker
- Wiederholtes Nachfragen, wenn nötig
- Vergleichsweise günstig

CONS

- Es gibt keine offiziellen Löschbestätigungen
- Bearbeitet (noch) keine People-Suchdienste

Vollautomatische Rechtspflege

Incogni funktioniert wie ein eifriger Rechtsbeistand, der formal Beschwerde einlegt, Daten abruft und Löschungen beauftragt. Das allein ist schon ein Fest, weil es die Data Broker beschäftigt. Sollten Sie nicht antworten, verhalten sie sich nichts rechtskonform - und ein solcher massenhafter Verstoß ließe sich dank

Incogni leicht belegen und ahnden.

Wer den Dienst bucht, sieht, welche Data Broker der Service schon angeschrieben hat - und ob es zu Reaktionen gekommen ist. Hier darf man nicht ungeduldig sein. Denn da diese Prozesse im Hintergrund per E-Mail erfolgen, kann es tagelang dauert, bis eine Antwort eintrifft. Incogni hakt nacht, sollte ein Data Broker der Ansicht sein, er müsse sich nicht bewegen.

Incigoni ist ein gebührenpflichtiger Service. Wer mag, kann monatsweise buchen - oder jahreweise. Verglichen mit Anwaltskosten sind die Gebühren gering. Mir ist es wert, für diesen Service zu bezahlen.

Aber eigentlich ist es eine Schande, dass der Gesetzgeber zulässt, dass so viele Daten unbemerkt gesammelt werden können - und dass wir als Konsumenten die Arbeit und die Kosten haben, um unser Recht in Anspruch zu nehmen.

[av_button_big label='Mehr Infos über Incogni von Surfshark' description_pos='' icon_select='yes-left-icon' icon='ue81f' font='entypo-fontello' link='manually,https://www.incogni.com' link_target='' title_attr='' color='theme-color' btn_custom_grad_direction='vertical' btn_custom_grad_1='#000000' btn_custom_grad_2='#ffffff' btn_custom_grad_3='' btn_custom_grad_opacity='0.7' custom_bg='#444444' color_hover='theme-color-highlight' custom_bg_hover='#444444' color_font='theme-color' custom_font='#ffffff' color_font_hover='white' custom_font_hover='#ffffff' border='' border_width='' border_width_sync='true' border_color='' border_radius='' border_radius_sync='true' box_shadow='' box_shadow_style='0px,0px,0px,0px' box_shadow_color='' hover_opacity='' sonar_effect_effect='' sonar_effect_color='' sonar_effect_duration='1' sonar_effect_scale='' sonar_effect_opac='0.5' id='' custom_class='' template_class='' av_uid='av-5cc2k0i' sc_version='1.0' admin_preview_bg=''][/av_button_big]

Wer sich für das Jahresabo entscheidet, spart 50%.

Unwetter: Wie gut warnen Warn-Apps wie Nina oder Katwarn?

Nach der Flutkatastrophe im vergangenen Jahr wurden zahlreiche Verbesserungen in den Warnsystemen versprochen: Bessere und schnellere Infos per Warn-App – und ein zügiger Ausbau von „Cell Broadcast“ (Warnungen aufs Handy). Viel passiert ist aber nicht.

Wir haben im Wesentlichen zwei Warn-Apps in Deutschland, die vor Unwettern, Katastrophen, großen Unfällen und sogar Terroranschlägen warnen: „Nina“ und „Katwarn“. Doch spätestens nach den Unwettern 2021 wurde Kritik laut, denn die Apps funktionieren nicht immer zuverlässig – und auch der Mobilfunk ist nicht so robust, wie er sein sollte.

Die bundesweit verfügbare und aktive Warn-App Nina vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) ist quasi die offizielle Warn-App des Katastrophenschutzes. Der ist allerdings Ländersache: Die nötigen Warnmeldungen müssen die nötigen Daten einstellen. Dann gibt es noch die von Fraunhofer Fokus entwickelte Katwarn-App.

Warum zwei Apps statt nur einer?

Nur rund 10% der Deutschen haben wenigstens eine der Warn-Apps installiert. Zwei Systeme: Wie soll sich ein Bürger entscheiden, welche er benutzen soll? Die offizielle App „Nina“ hatte im vergangenen Jahr die Bevölkerung gar nicht gewarnt, weil die lokalen Behörden keine Warnungen eingestellt haben. Da Katastrophenschutz Ländersache ist, liegt die Verantwortung in den Regionen, nicht bei der Bundesbehörde.

Deshalb ist die Idee, dass die beiden Apps kooperieren, damit mehr Warnungen zusammenkommen. Wenn Katwarn Warnungen hat, sollten die an Nina weitergegeben werden können – und umgekehrt.

Noch Anfang Mai gab es aber Kritik, dass nicht mal ein Test richtig möglich sei. Das Bundesamt für Katastrophenhilfe (BKK) hat die Anschuldigungen aber zurückgewiesen, für Nina existiere seit Jahren eine sogenannte „Testumgebung“. Nach einer wirklich konstruktiven Zusammenarbeit, die im Angesicht der Katastrophe im vergangenen Jahr mehr als nötig erscheint, klingt das nicht gerade.

Cell Broadcast soll kommen

Nach der Flutkatastrophe im vergangenen Jahr hat man ja auch auf das öffentliche Meldesystem geschaut. Sirenen – gibt es häufig nicht mehr. Der Begriff „Cell Broadcasting“ ist gefallen: In Japan, USA, Kanada, Neuseeland und auch die Niederlande längst im Einsatz. Das ist ein Verfahren, um gleichzeitig allen Menschen in einer Funkzelle eine offizielle Nachricht zu senden. Es bekommen alle dieselbe Nachricht, egal in welchem Mobilfunknetz sie unterwegs sind – und das funktioniert auch auf alten Handys.

Die Nachricht ist maximal 1395 Zeichen lang und kann alle Zeichen enthalten, somit auch Weblinks. Aber keine Bilder, das ist den Apps vorbehalten. Cell Broadcasting ist keine Massen-SMS, sieht aber so ähnlich aus. Praktisch alle Handys unterstützen „Cell Broadcasting“.

Das Problem: In Deutschland ist dieser Dienst bislang nach wie vor nicht vernünftig eingerichtet. Eigentlich schreibt eine EU-Verordnung vor, dass spätestens im Juni 2022 alles fertig sein müsste. Doch in Deutschland will man im September am Sirenentesttag die Technologie einsetzen – vor Januar 2023 wird

es nicht fertig. Das wurde mir von Manuel Atug von der AG Kritis mitgeteilt, die sich für den Schutz kritischer Infrastruktur einsetzt. Es kommt also viel zu spät.

Es dauert zu lange

Staat und die Behörden haben zwar eine Menge versprochen, aber man kann nicht behaupten, dass sie liefern. Sie sind zu langsam, zu träge, nicht ausreichend motiviert.

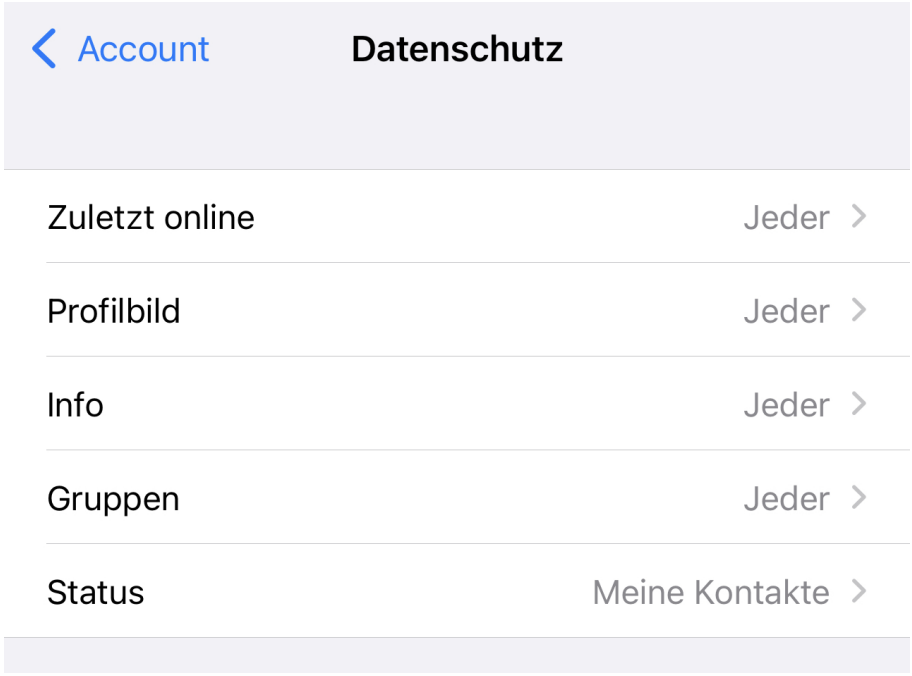
Bürger sind deshalb gut beraten, sich nicht auf eine App zu verlassen. Bürger sollten Nina, Katwaren und vielleicht auch noch den Regenradar installieren. Alles kostenlose Apps. Dort trägt man dann ein, wann man gewarnt werden möchte, etwa in seinem Wohngebiet oder dort, wo das Haus der Eltern steht – und lässt sich von allen Apps warnen.

User können auch einstellen, bei welchen Anlässen gewarnt wird. Lieber eine Warnung zu viel als eine zu wenig. Und wir sollten Druck machen, dass die Behörden endlich mal in die Pötte kommen.

Datenschutzeinstellungen bei WhatsApp

Die Nutzung von WhatsApp ist umstritten: Die Menge der Daten, die über die Leitung gehen, ist hoch. Wenn Ihr den Messenger-Dienst nutzen wollt, dann nutzt zumindest die Datenschutzeinstellungen!

WhatsApp hat so eine gewisse Widersprüchlichkeit: Auf der einen Seite will man es nicht nutzen, weil es ablenkt und Datenschutz-Bauchgrummen verursacht. Auf der anderen Seite verwendet si viele Menschen die App, dass eine wichtige Kommunikationsform fehlen würde. Da ist es zumindest schon mal positiv, dass Ihr in der App einige Einstellungen vornehmen könnt, die Euch mehr Selbstbestimmung über Eure Daten geben.



Diese findet Ihr unter **Einstellungen** > **Account** > **Datenschutz**.

- Unter **Zuletzt online** könnt Ihr festlegen, wer sehen kann, wann Ihr WhatsApp zuletzt genutzt habt. Das nimmt Euch den Druck, dass Gesprächspartner sich beschweren, dass Ihr nicht antwortet, obwohl Ihr online wart.
- Unter **Gruppen** könnt Ihr verhindern, dass Euch jeder beliebige Teilnehmer in eine Gruppe hinzufügen kann, ohne dass Ihr zustimmen müsst.
- **Profilbild** und **Info** gehören zu den allgemein verfügbaren Informationen und sind im Standard für alle Teilnehmer sichtbar. Auf der anderen Seite: Wer mit Euch Chatten soll, kennt Euch, die anderen müssen diese Informationen nicht haben. Gebt sie nur für Kontakte frei.
- Der **Status** wird von vielen Benutzern aktiv genutzt, um den aktuellen Gemütszustand, den Aufenthaltsort oder andere aktuelle Informationen zu kommunizieren. Der sollte auf jeden Fall nur Kontakten angezeigt werden.

WhatsApp: Ältere iPhones werden bald nicht mehr unterstützt

Im Oktober soll es so weit sein: WhatsApp wird durch eine ständige Weiterentwicklung auf einigen älteren iPhone-Geräten nicht mehr laufen. Entscheidend ist nicht das Alter des Geräts an sich, sondern welche Betriebssystem-Version im Einsatz ist.

Es ist ein völlig normaler Vorgang: Jede im Einsatz befindliche Software wird unentwegt weiter entwickelt. Neue Funktionen müssen her, mögliche Bugs beseitigt werden - und weil sich auch jedes Betriebssystem weiter entwickelt, sind auch deshalb häufiger Korrekturen oder Erweiterungen nötig. Das gilt auch für das beliebte (wenn auch alles andere als unumstrittene) WhatsApp.

Irgendwann kommt der Punkt, da müssen App-Entwickler aufgrund der Entwicklungen bei einem Betriebssystem eine Mindestversion voraussetzen. Das ist bei WhatsApp jetzt mal wieder der Fall: Im Herbst soll eine neue Version von WhatsApp herauskommen, die ältere iPhone-Modelle ausschließen wird - berichtet das Portal Wabetainfo.

Ab Herbst nicht mehr mit iOS 10 und 11

Die Prognose ist erstaunlich konkret: Stichtag für die Änderung soll danach der 24. Oktober 2022 sein. Während iPhone-Nutzer aktuell Version 15.4 einsetzen und Apple bereits an iOS16 arbeitet, werden ak Oktober wohl iPhones mit iOS10 und iOS11 nicht mehr unterstützt. Das kommt nicht so völlig überraschend, da WhatsApp schon heute wenigstens iOS12 **empfiehlt**. Lauffähig ist der Messengerdienst aber auch noch auf älteren iOS-Versionen.

Sollt es kommen wie prognostiziert und der Support für iOS 10 und 11 entfällt, betrifft das alle, die noch ein iPhone 5 oder 5c verwenden. Spätestens dann müssten sich die User nach einer Alternative umschauen: Entweder ein neueres Gerät (mit neuerem iOS) - oder ein anderer Messenger wie **Signal**.

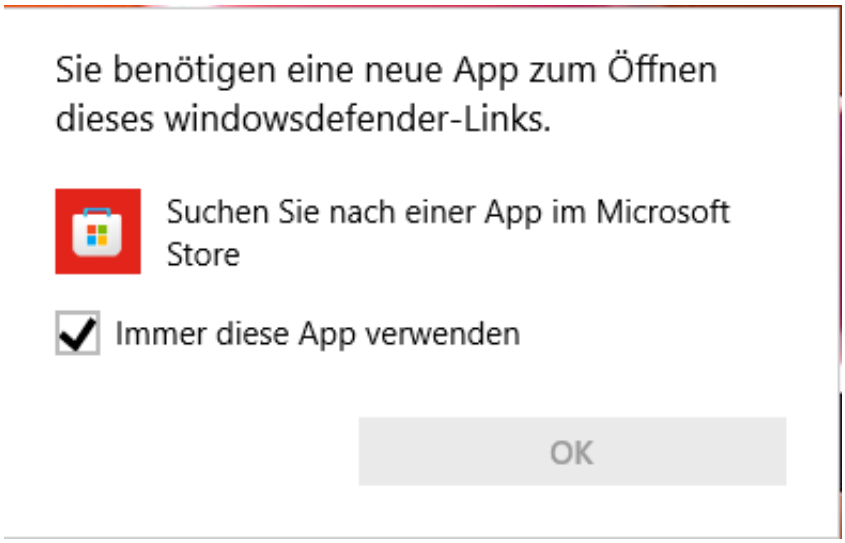
WhatsApp will die Nutzer aber rechtzeitig informieren, damit der Wechsel und damit das Support-Ende nicht aus heiterem Himmel kommt.

https://twitter.com/WABetaInfo/status/1528070057124843522?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1528070057124843522%7Ctwgr%5E%7Ctwcon%5Es1_c10&ref_url=https%3A%2F%2Ft3n.de%2Fnews%2Fwhatsapp-diese-iphones-bald-mehr-1474693%2F

Fehler bei Windows 11-Sicherheitseinstellungen lösen

Beim Öffnen einer der Sicherheitseinstellungen von Windows 11 kommt die Fehlermeldung "Sie benötigen eine neue App zum Öffnen dieses windowsdefender-Links"? Wir zeigen Euch, wie Ihr den Fehler behebt!

Windows kann manchmal komisch sein. Vor allem dann, wenn eine Standardaktion statt mit der Ausführung des Befehl mit einer abstrusen Fehlermeldung beantwortet wird. So bei Windows 11 aktuell immer wieder beim Umgang mit Sicherheitseinstellungen des Windows Defender. Ob Ihr im Benachrichtigungsbereich eine Warnung habt und darauf klickt oder über **Einstellungen** > **Datenschutz und Sicherheit** > **Windows Sicherheit** eine Einstellung ändern wollt, die Fehlermeldung bleibt die gleiche.



Sie weist darauf hin, dass der Windows Defender zwar installiert ist, Windows aber keine Befehle an ihn weitergeben kann. Das ist kein Hinweis auf einen Virebefall, sondern schlicht und einfach ein Bug. Den könnt Ihr im Handumdrehen beheben:

1. Klickt auf die Lupe unten in der Taskleiste, dann gebt **powershell** ein.
2. Klickt rechts auf **Als Administrator ausführen**.
3. Gebt an der Eingabeaufforderung den Befehl *Get-AppxPackage Microsoft.SecHealthUI -AllUsers* | *Reset-AppxPackage* ein.

Macht Euch nicht die Mühe, den Befehl abzutippen, sondern markiert ihn und kopiert ihn in die Zwischenablage. An der Eingabeaufforderung der Powershell könnt Ihr sie dann wieder einfügen und durch Drücken der Eingabetaste ausführen.

Nach dem Abschluss der Installation ist keine weitere Aktion nötig: Die Links zu den Windows Defender-Funktionen funktionieren sofort wieder.