

A portrait of a man with short brown hair and blue eyes, wearing a teal button-down shirt. He is looking slightly to the right of the camera with a subtle smile. His arms are crossed, and he is wearing a watch on his left wrist. The background is dark and out of focus.

# Schieb Report

**Ausgabe 2018.10**

## Was ist eigentlich “USB-Debugging”?

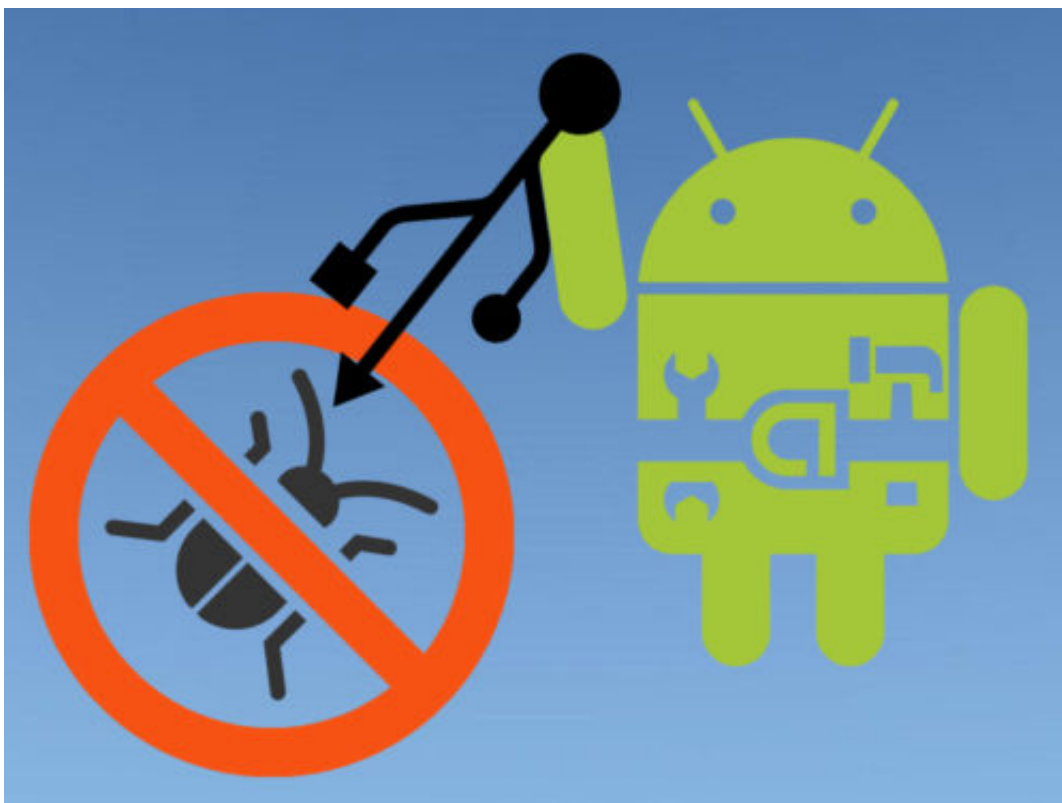
Von dem Begriff “USB-Debugging” dürfte so ziemlich jeder Smartphone-Nutzer schon einmal gehört haben. Was das aber genau ist oder wofür die Funktion gebraucht wird, ist den wenigsten klar. Wir klären auf, was es mit USB-Debugging auf sich hat.

Die ersten drei Buchstaben verraten schon, dass die Einstellung etwas mit den USB-Anschlüssen des Computers zu tun haben könnte. Bei aktiviertem USB-Debugging wechselt das Smartphone automatisch in eine Art Entwicklermodus, sobald es über die USB-Verbindung angeschlossen wird.

So lässt sich auf bestimmte Systemfunktionen und Einstellungen zugreifen, die für normale Nutzer eigentlich unzugänglich wären. Der Begriff “Debugging” kommt daher, weil Entwickler diesen Modus nutzen, um Fehler (engl. Bugs) in ihren Apps nachzuverfolgen und zu entfernen.

Der Modus kann aber auch für normale Nutzer hilfreich sein, etwa wenn ein Backup erstellt oder wiederhergestellt werden soll. Manche Apps benötigen dann Zugriff über USB-Debugging, um auf die tief liegenden Systemdateien zugreifen zu können.

Der Modus bringt aber auch Risiken mit sich. Zum einen können Systemdateien durch falsche Anwendung beschädigt werden. Außerdem lässt sich ein gestohlenes Smartphone, bei dem USB-Debugging dauerhaft aktiviert ist, leicht von Dieben entsperren. Der Modus sollte also nur dann aktiviert werden, wenn er unbedingt gebraucht wird.



## Alexa kann lachen, auch Dich auslachen

Der smarte Lautsprecher Amazon Echo ist mittlerweile recht populär. Viele haben ihn zu Hause stehen. Durch einen von Amazon mittlerweile offiziell eingeräumten Bug kann es passieren, dass Alexa schallend lacht. Es klingt, als ob Echo seinen Besitzer auslacht. Was ist da los?

[Alexa](#) ist die Siri von Amazon - und die hat eine ziemlich dreckige Lache. Hat Alexa wirklich. Das Problem ist, dass immer mehr Alexa-Nutzer davon aufgeschreckt werden. Sogar mitten in der Nacht.

<https://vimeo.com/259121001>

*So klingt das, wenn Alexa einen unvermittelt auslacht*

### Dreckige Lache erschallt unvermittelt

Offensichtlich fängt Alexa unvermittelt an zu lachen. "Ich habe mich total erschrocken", berichtet [einer auf Twitter](#). "Ich dachte, ein Kind steht hinter mir!" Weil das auch mitten in der Nacht passieren kann, kann das ausgesprochen erschreckend sein. Doch Alexa lacht einen nicht aus wegen der Unterhosen, wie Jimmy Kimmel vermutet, sondern weil ein technischer Fehler vorliegt.

"Alexa, Lache" reicht als Befehl, um Amazons Lautsprecher dazu zu bewegen, loszulachen. Offensichtlich wird dieser Befehl häufig unterstellt, auch wenn nichts gesagt wurde. Darum korrigiert Amazon den Sprachschatz: Jetzt muss man schon "Alexa, kannst Du lachen?" fragen. Auch soll der vor allem in den USA populäre Lautsprecher dann nicht mehr einfach loslachen, sondern vorher sagen: "Natürlich kann ich lachen! Hahahaha".

<https://www.youtube.com/watch?v=tMJm4cZ9yxQ>

*Jimmy Kimmel macht sich in seiner Show lustig über den Effekt*

### Nicht witzig, sondern ein großes Problem

Die Geschichte wirkt heiter. Man kann gut drüber lachen. Aber sie hat auch eine äußerst ernste Seite. Im Grunde ist der Vorfall besser als jede erfundene Geschichte. Sketch-Schreiber hätten sich das nicht besser ausdenken können. Aber: Die Sache ist real. Sie ist ernst. Es zeigt: Wenn wir uns Technik ins Haus holen, die mit Künstlicher Intelligenz ausgestattet und mit vielen Aufgaben betraut ist und über die wir keine wirkliche Kontrolle haben, kann eine Menge schiefgehen.

Mit Alexa kann man nicht nur Musik abspielen oder Infos aus dem Netz holen, sondern auch das Smart Home steuern. Wenn aber eine solche Schaltzentrale nicht macht, was sie soll, sondern eigenmächtig agiert, können tragische Dinge geschehen. Die Polizei wird irrtümlich alarmiert. Oder die Feuerwehr. Oder das Licht ausgeschaltet, während eine betagte Person die

Treppe runtergeht. Im Schlafzimmer wird die Heizung hochgedreht oder der Kühlschrank abgetaut.

Vielleicht lacht Alexa deswegen so laut und dreckig: Das System freut sich schon auf all den Unsinn, der in Zukunft angestellt werden kann.

## Nachtmodus für Google Home aktivieren

Sprachassistenten und intelligente Lautsprecher wie Google Home haben sich in den letzten Jahren konstant weiterentwickelt. Nicht nur erkennen sie Sprachbefehle zunehmend zuverlässig, sie antworten mittlerweile auch wesentlich verständlicher.

Die Sprach-Software lässt sich auf dem Google Home sogar so modifizieren, dass sie sich der Tageszeit anpasst. Heißt, wenn es auf die Abendstunden zugeht, antwortet Google Assistant leiser, um nicht zu stören.

Dieser sogenannte **Nachtmodus** lässt sich folgendermaßen aktivieren.

1. **Google Home App** öffnen
2. Auf das **Lautsprecher-Symbol** oben rechts tippen
3. Auf **Geräte** tippen und den verbundenen **Google Home Lautsprecher** auswählen
4. Das erweiterte **Menü** über einen Tap auf das **Symbol** oben rechts öffnen
5. **Geräteeinstellungen** anwählen
6. Den **Schieberegler** neben **Nachtmodus** aktivieren

Im folgenden Menü lässt sich nun genau festlegen, an welchen **Wochentagen** und zu welcher **Uhrzeit** der Lautsprecher in den Nachtmodus wechselt. N

eben der **Lautstärke der Sprache**, lässt sich hier außerdem die **Helligkeit der LEDs** einstellen und der **Bitte nicht stören-Modus** aktivieren. Dieser verhindert, dass störende Benachrichtigungs-Töne oder Erinnerungen über den Lautsprecher abgespielt werden.



## Equalizer für Musik-Streaming auf dem Apple HomePod

Mit iPhone und iPad lässt sich sehr bequem Musik abspielen - auch streamen. Mit Hilfe des Equalizers kann jeder den Sound auf seine individuellen Vorstellungen anpassen.

Immer mehr Menschen stellen sich smarte Lautsprecher in die Wohnung. Mit ihrer Hilfe kann man nicht nur die Hilfe Digitaler Assistenten in Anspruch nehmen, sondern auch Musik hören. Die Klangqualität der Lautsprecher ist sehr unterschiedlich, Apples HomePod zeichnet sich allerdings durch eine sehr hohe Wiedergabequalität aus.

Apples HomePod erlaubt sogar, den Klang an den persönlichen Geschmack anzupassen. HomePod bietet einen Equalizer: Ob dunkle Bässe oder präsenzte Höhen, das kann hieder jeder User nach eigenem Geschmack einstellen. Das geht auf iPhone oder iPad. Die Einstellungen werden auf den Lautsprecher übertragen.

Dazu zunächst auf dem iPhone oder iPad die **Musik-App** öffnen und einen Song abspielen. Nun über **Einstellungen** --> **Musik** etwas runterscrollen und auf **EQ** tippen. Im Equalizer nun einfach ein **Preset** auswählen oder die **Frequenzregler** händisch anpassen. Als Nächstes einfach die Musik über **AirPlay** an den HomePod streamen.

Die Einstellungen für den Equalizer werden auf dem iOS-Gerät gespeichert und automatisch aktiviert, wenn Musik über AirPlay übertragen wird.

Wer Musik über **Spotify** statt über die Musik-App wiedergibt, kann den Equalizer auch direkt dort einstellen. Dazu einfach in Spotify im Bereich **Bibliothek** die **Einstellungen** öffnen, **EQ** antippen und ein **Preset** auswählen.





## Firefox: URL in neuem Tab öffnen

Wer im Firefox-Browser eine Internet-Adresse aufrufen möchte, kann diese einfach oben in die Leiste eingeben. Beim Druck auf [Enter] wird dann die aktuell geöffnete Seite durch die neue URL ersetzt. Wer das nicht will, wendet einen Trick an.

Auf Wunsch kann Mozilla Firefox neu aufgerufene URLs nämlich auch in einem neuen, separaten Browser-Tab öffnen. Der Vorteil: Die zuvor geladene Webseite bleibt erhalten und kann noch gelesen werden.

Um im Firefox-Browser beim Aufrufen einer URL einen neuen Tab zu erstellen, folgende Schritte ausführen:

1. Zunächst die Adresse eingeben, wie gewohnt.
2. Nun beim Drücken auf [Enter] auf der Tastatur zusätzlich die [Alt]-Taste gedrückt halten. Dadurch legt Firefox einen neuen Tab an.



## Dropbox-Links in Gmail

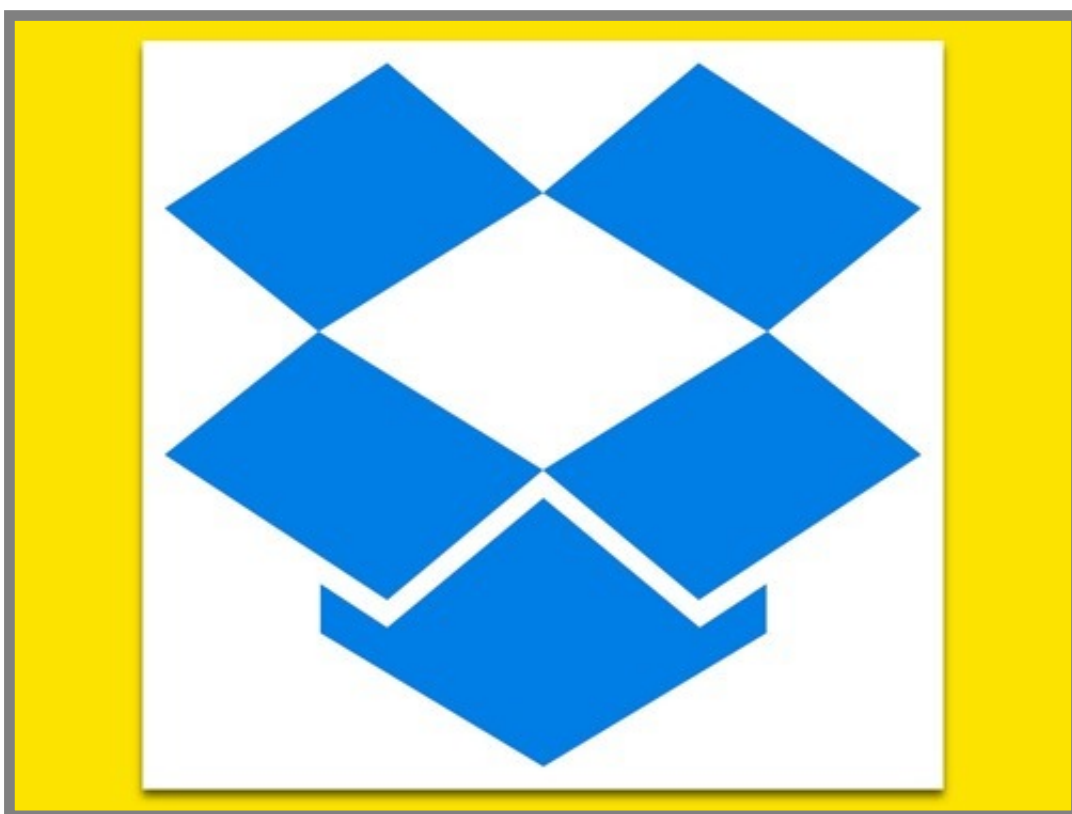
Große Dateien lassen sich über den Web-Dienst Google Mail nicht versenden. Bei Gmail gilt zum Senden von Anlagen ein Limit von 25 MB. Wer mehr Inhalte anhängen möchte, muss auf Cloud-Speicher zurückgreifen.

Besonders beliebt ist der Anbieter Dropbox mit seinen mehreren Gigabyte kostenlosem Speicher – je nach Paket und Anzahl eingeladener Freunde. Dieser Speicher lässt sich auch für eMail-Anlagen nutzen. Dann wird in der Nachricht nur noch ein Link mitgesendet.

Die einfache Einbindung der Dropbox in Gmail gelingt mit einer Chrome-Erweiterung, die Dropbox selbst entwickelt hat. Hier kann der Nutzer vor dem Einfügen eines Links in eine neue eMail auch Vorschauen der gewünschten Dateien einfügen – auch für Bilder.

Das Dropbox-Add-On für den Google Chrome-Browser lässt sich direkt aus dem Chrome Web Store herunterladen:

<https://chrome.google.com/webstore/detail/dropbox-for-gmail/dpdmhfocilnekecfjgimjdeckachfbc?hl=de>



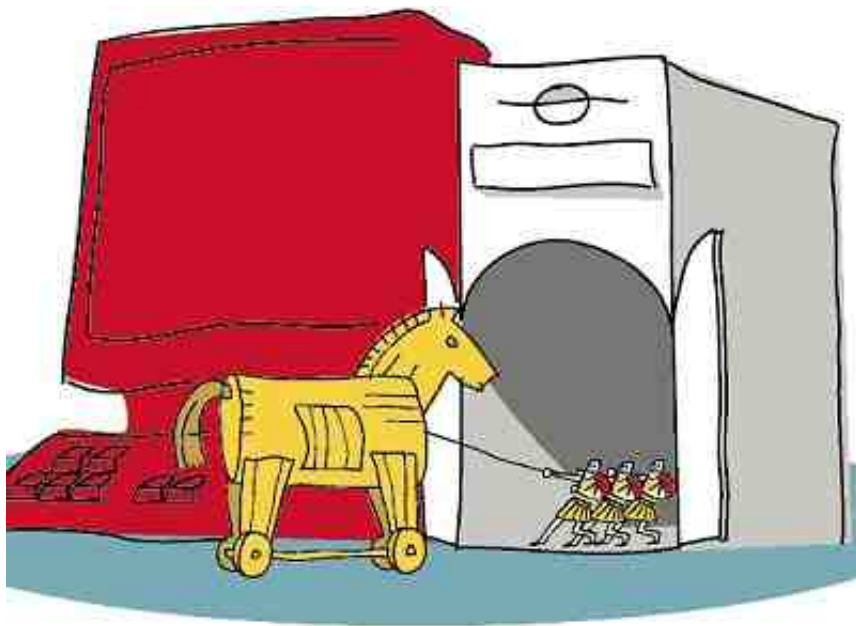
## Microsoft blockt Staatstrojaner FinFisher

Die Hack-Aktion in unserem Regierungsnetzwerk war in den letzten Tagen immer wieder Thema. Mit Hilfe eines über Sicherheitslücken eingeschleusten Trojaner konnten die Hacker auf das Netzwerk zugreifen. Ein Trick, den durchaus auch Behörden und Regierungen verwenden.

Zum Beispiel, wenn sogenannte Staatstrojaner zum Einsatz kommen. Klappt aber nur, wenn die Schnüffelprogramme nicht entdeckt werden. Microsofts Schutz-Software jedoch warnt jetzt vor einem Staatstrojaner – sowas ist neu.

Trojaner sind Schnüffelprogramme. Sie werden in der Rege über Sicherheitslücken in Betriebssystemen oder wichtigen Programmen eingeschleust. Trojaner verstecken sich im Speicher, bleiben unentdeckt und beobachten den Benutzer.

Sie merken sich Passwörter oder sensible Daten – und übermitteln sie an die Hacker. Genau so sind auch die Hacker beim [jüngsten Regierungshack vorgegangen](#). Es braucht also ein Sicherheitsleck, nur dann kann ein Trojaner aufgespielt werden. Wenn Schutz-Software zum Einsatz kommt, muss sie den Trojaner "kennen", um ihn zu entdecken und zu blocken.

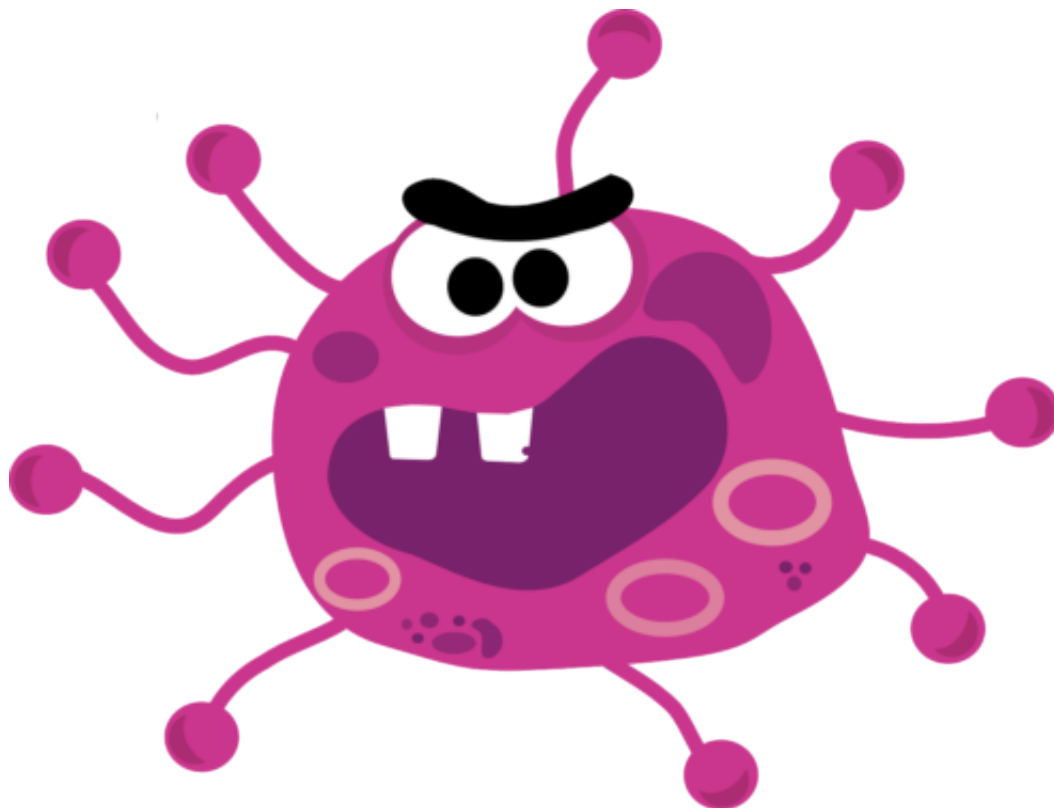


### Staatstrojaner FinFisher

Auch Staatstrojaner sind also Trojaner – kommen aber vom Staat. Behörden entwickeln solche Malware in der Regel nicht selbst, mit Ausnahme der NSA. Die Deutschen kaufen solche Schnüffelprogramme, zum Beispiel beim deutsch-britischen Unternehmen FinFisher. Der Staatstrojaner heißt genauso. Er nutzt Sicherheitslücken im Betriebssystem Windows aus.

Er kann genutzt werden, um Rechner fernzusteuern: Behörden können sensible Daten mitlesen, den Benutzer überwachen und ausspionieren und teilweise auch Mikrofon und

Kamera einschalten, wann immer sie es wollen. Geht aber nur, wenn der Trojaner unentdeckt bleibt. Auch deutsche Behörden setzen FinFisher ein.



## Trickreich programmierter Trojaner

Der Staatstrojaner FinFisher ist sehr trickreich programmiert und für Anbieter von Schutz-Software eine harte Nuss. Microsoft kennt die verschiedenen Versionen des Trojaners schon länger und kämpft auch schon lange dagegen, etwa durch Stopfen von ausgenutzten Sicherheitslecks.

Nun haben sich die Ingenieure bei Microsoft den Trojaner noch genauer angeschaut, um Windows und Outlook entsprechend abzusichern ([hier mehr Infos dazu](#)). Microsoft hat sich sogar öffentlich dazu geäußert: FinFisher sei sehr komplex und schwierig zu knacken. Doch es ist offenbar gelungen. Die sogenannte "Advanced Thread Protection" (ATP) im Schutzprogramm Windows Defender ist deutlich verbessert worden.

[caption id="attachment\_757264" align="alignnone" width="500"]



[joffi /](#)

Pixabay[/caption]

## Bedeutet für Computerbenutzer?

Wer den Windows Defender einsetzt und vor allem die erweiterte Schutzfunktion, der ist nicht nur vor dem FinFisher geschützt, sondern auch besser gegen vergleichbare Schadprogramme geschützt. Es gibt noch andere Malware, die ähnliche Techniken und Tricks einsetzt wie FinFisher. Durch die aufwändigen Analysen ist die Schutz-Software Windows Defender also besser geworden.

Theoretisch kann FinFisher auch künftig eingesetzt werden, praktisch aber nein. Denn wenn die Erkennungsfahr für einen Staatstrojaner derart hoch ist, wird er kaum noch zum Einsatz kommen. Sicher wird das Unternehmen eine neue Version entwickeln, die andere Sicherheitslecks ausnutzt – und andere Techniken einsetzt.

## Chrome säubern

Wenn Google [Chrome](#) sich nur noch langsam öffnet und ständig abstürzt, ist guter Rat teuer. Spätestens beim ungewollten Ändern der Startseite oder Such-Funktion sollten aber die Alarmglocken läuten. Abhilfe schafft ein Tool, das von Google selbst stammt.

Unerwünschte Pop-ups, Änderungen an den Einstellungen sowie mangelhafte Performance können auf Malware hinweisen, die sich im Chrome-Browser breit gemacht hat. Solche schädliche Software lässt sich oft mit dem [Chrome Software Cleaner](#) beseitigen.

Nach dem Download des Tools von der Google-Webseite lässt sich der „Software Cleaner“ direkt starten. Danach beginnt auch gleich die Suche nach Malware, die man sich beim Chrome-Browser eingefangen hat.

Schließlich fragt das Tool auch noch, ob die Einstellungen des aktuell genutzten Browser-Profiles zurückgesetzt werden sollen. Das kann nämlich weitere Fehler verhindern. Dabei werden auch alle bisher installierten Erweiterungen gelöscht.

**Wichtig:** Den Chrome Software Cleaner gibt es momentan nur für Windows-Nutzer.

<https://www.google.com/chrome/cleanup-tool/>



## Warum haben sie geklappt, die Hackangriffe auf das Regierungsnetzwerk

Hackangriff auf die Datennetze der Regierung: Diese Woche haben sich die Schlagzeilen überschlagen. Kein Wunder, ist schließlich kein Pappenstil, wenn Hacker sich Zugang zu Netzwerken des Auswärtigen Amtes verschaffen und dort vertrauliche Daten entwenden. Mittlerweile wissen wir: Es wurden wochenlang sensible Daten abgegriffen. Nun wird nach den Verantwortlichen gefahndet.

Hacker sind in das als besonders sicher geltende Datennetz der Regierung eingedrungen, das sich "IVBB" nennt: Informationsverbund Bonn-Berlin. Darüber sind Ministerien, Bundeskanzleramt, einige Bundesbehörden wie der Bundesrechnungshof und andere Bundesbehörden vernetzt.

Eingedrungen sind die Hacker über eine Hochschule des Bundes, um dann 17 Rechner im Auswärtigen Amt anzugreifen. Offenbar sind die Hacker vor allem an Dokumenten und Informationen interessiert, die sich mit der Ostpolitik beschäftigen. Schon seit Monaten sind die Hacker im Netz.



### Erst spät informiert

Als das Leck entdeckt wurde, wollte man nicht gleich an die Öffentlichkeit, um die Hacker nicht zu warnen. Man wollte sich die Zeit nehmen, herauszufinden, wie die Hacker vorgehen – und vor allem, wohin die Daten geschickt werden. Das braucht Zeit. Aber offensichtlich hat es nicht nur ein Leck im Datennetz gegeben, sondern auch ein Leck im Kreise der Verantwortlichen.

Die Öffentlichkeit wurde informiert. Wer das war, das soll möglicherweise ermittelt werden. Die Bundesregierung sucht den Informanten – vielleicht wird sogar Strafantrag gestellt. Warum die zuständigen Gremien nicht informiert wurden, ist eine ganz andere Frage – und eine sehr berechtigte Frage.



## Vermutlich steckt "Snake" dahinter

Man geht davon aus, dass ein Hackerverbund namens "Snake" (Turla) dahinter steckt. Eine bekannte Truppe hoch-spezialisierter Experten, gut vernetzt und gut bezahlt. Man vermutet Verbindungen zum russischen Geheimdienst FSB.

Fest steht: Es braucht nicht nur eine enorme Expertise, um einen solchen Angriff durchzuführen, sondern auch eine Menge Geld, denn Angriffe auf diesem Niveau sind recht kostspielig. Das spricht für Snake.

## Die Analysemethoden

Jeder Hacker und auch jede Hackertruppe hat einen bestimmten Stil, eine Art Handschrift, die bei einem Hackangriff hinterlassen wird. Außerdem kann man auch versuchen festzustellen, woher die Angriffe kommen oder wohin die Daten gehen. So etwas lässt sich zwar verschleiern, aber wenn man lange und intensiv genug analysiert, lässt sich auch das sagen. Aber sicher sein kann man sich nicht. Es wird viel getäuscht, es werden viele falsche Fährten gelegt.

Das [BSI](#) macht in der Regel eine gute Arbeit. Doch hundertprozentigen Schutz gibt es leider



nicht, egal wie sehr man sich anstrengt. Oft gibt es Schwierigkeiten in der Infrastruktur: Wo liegen Daten, wer darf darauf zugreifen, halten sich auch alle an die Regeln? Es gibt wohl mehrere Sicherheitsstufen im Auswärtigen Amt, aber offensichtlich haben die nicht ausgereicht, hat es zumindest den Anschein. Größtes Sicherheitsrisiko ist der Mensch. Menschen machen Fehler.

[caption id="attachment\_757264" align="alignnone" width="500"]



[joffi /](#)

Pixabay[/caption]

## Was macht das Cyber-Abwehrzentrum?

Das nationale [Cyber-Abwehrzentrum](#) gehört zum BSI. Es koordiniert verschiedene Sicherheitsstellen auf Bundesebene. Sie alle kümmern sich getrennt, aber eben über das Abwehrzentrum koordiniert um etwaige Angriffe aus dem Netz. Doch das Abwehrzentrum ist keine eigene Behörde, sondern lediglich eine Koordinierungsstelle.

Zu den Kernaufgaben gehören "Prävention und Frühwarnung von Cyber-Angriffen". Nun, man kann wohl sagen, das ist in diesem Fall definitiv nicht gelungen. Selbst die sensiblen Netzwerke der Regierung können nicht geschützt werden, das lässt nichts Gutes hoffen für sensible Daten in der Wirtschaft – die von den Behörden praktisch gar nicht aktiv geschützt werden –, und

schon gar nicht wir normale Bürger.

## **Kein Einzelfall**

Offensichtlich wurden auch die Systeme anderer Länder angegriffen. Und gerade wurde bekannt, dass auch die Stiftung Wissenschaft und Politik gehackt wurde, die unter anderem das Auswärtige Amt berät. Offenbar wurde einem Mitglied der Stiftung bei einem Moskau-Besuch Schnüffel-Software aufs Handy installiert, über das WLAN des Hotels, in dem er sich aufgehalten hat. Das ist Stoff für Spionage-Thriller.

Natürlich muss man wissen, dass ein enormer Aufwand betrieben wird, um an Regierungsinformationen zu kommen. Ein solcher Aufwand wird nicht für mich oder Dich betrieben.

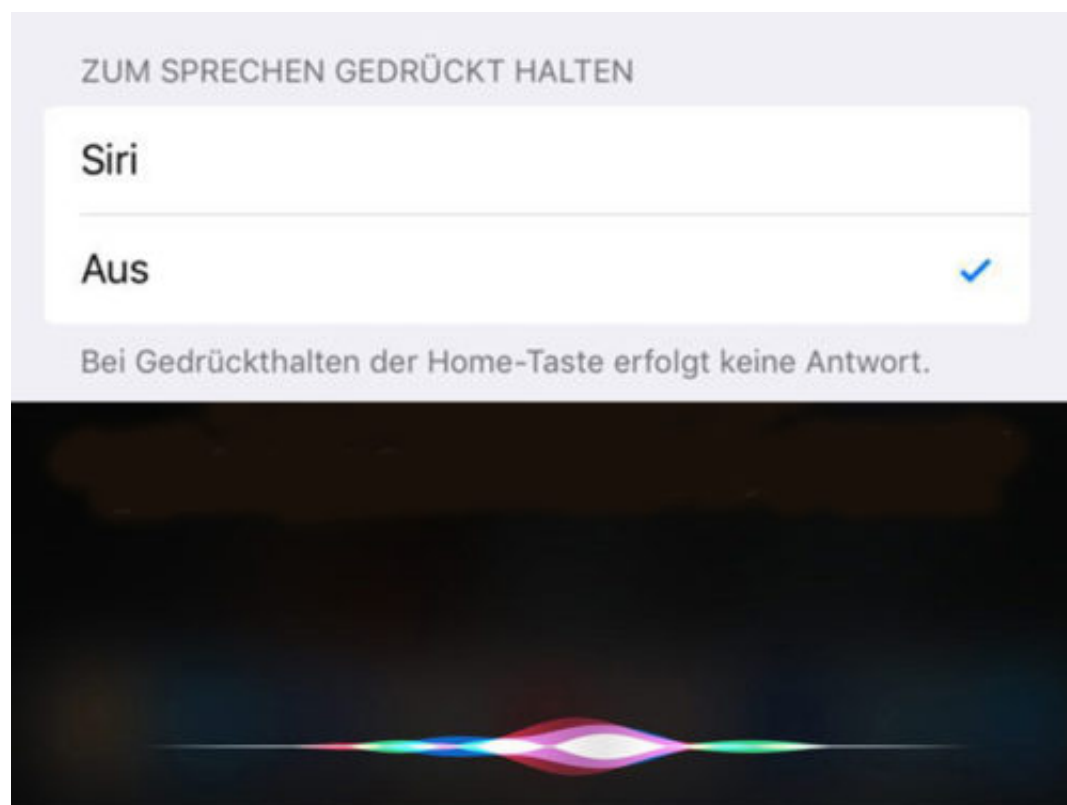
Aber wir lernen daraus: Hundertprozentigen Schutz kann es unmöglich geben, egal welchen Aufwand wir betreiben. Wir sollten also angemessenen Schutz betreiben, etwa ständige Updates und je nachdem auch Schutz-Software einsetzen, aber mehr können wir auch nicht machen, wenn wir Onlinedienste nutzen wollen.

## Siri auf der Seitentaste des iPhone X deaktivieren

Den meisten iPhone-Nutzern dürfte es schon mal passiert sein, dass der Sprachassistent Siri aus Versehen aktiviert wurde. Das geschieht ganz leicht, etwa wenn die Seitentaste am iPhone X versehentlich etwas länger gedrückt wird.

Wer auf Siri in der Regel verzichten kann und die nervige Aktivierung ausschalten möchte, kann das ganz leicht in den Einstellungen tun.

Dazu zunächst in **Einstellungen** auf **Allgemein** tippen und unter **Bedienungshilfen** den Punkt **Seitentaste** auswählen. Hier nun eine der Optionen wählen, um festzulegen, was passieren soll, wenn die Taste gedrückt gehalten wird. Neben Siri lässt sich lediglich die Sprachsteuerung aktivieren oder beides komplett ausschalten.

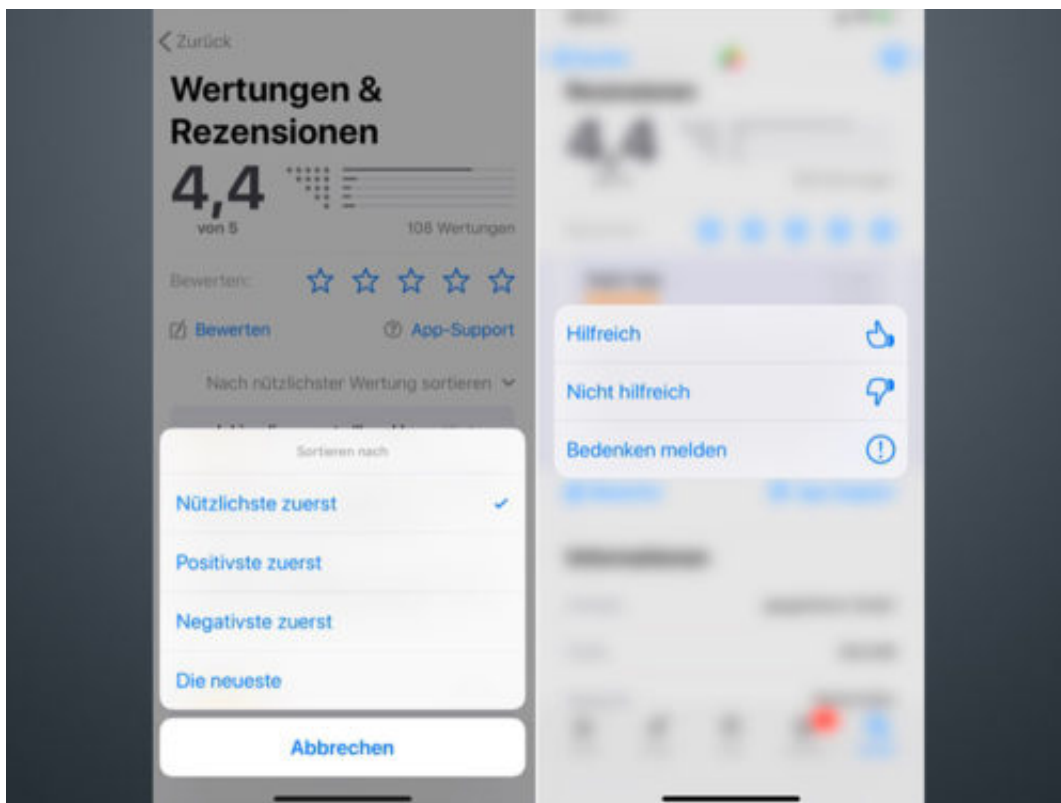


## Apps auf iPhone und iPad Apps nach Bewertungen filtern

Niemand möchte einen kostenpflichtigen Download später bereuen. Doch oft halten heruntergeladene Apps nicht das, was sie versprechen. Was natürlich besonders ärgerlich ist, wenn sie kostenpflichtig sind. Rückgabe der gekauften App? In der Regel gar nicht oder nur unter ganz bestimmten Umständen möglich.

iPhone-User können sich die Entscheidung erleichtern, bevor sie einen Kauf tätigen: Wer mag, kann seit iOS 11.3 Bewertungen im App Store nach verschiedenen Kriterien sortieren lassen. Auf diese Weise ist es möglich, bequem wichtige Beurteilungen zu studieren.

Dazu im **App Store** einfach die gewünschte App auswählen. Hier werden standardmäßig die **nützlichsten** Rezensionen und Bewertungen angezeigt. Um den Filter auf **Positivste**, **Kritischste** oder **Neueste** zu setzen, einfach auf **Alle anzeigen** tippen und die gewünschte Option auswählen. Anschließend muss man die Bewertungen natürlich noch lesen - aber das kann sehr hilfreich sein.



## iPhone: SMS-Weiterleitung reparieren

SMS-Nachrichten, die an einem iPhone empfangen werden, lassen sich auch direkt am Mac lesen. Auf Wunsch können sie nämlich an Computer weitergeleitet werden, die mit der gleichen Apple-ID bei iMessage angemeldet sind. Manchmal funktioniert diese Weiterleitung allerdings nicht wie gewünscht.

Wenn das iPhone eingehende SMS-Nachrichten nicht mehr an Macs über iMessage weiterleitet, liegt das oft an der Internet-Verbindung des mobilen Geräts. Beispielsweise könnte es sein, dass das iPhone zwar mit dem Mobilfunknetz verbunden ist, aber nicht über eine Verbindung ins Internet verfügt – die Weiterleitung funktioniert nämlich über Apple-Server.

Außerdem sollte beachtet werden: Die SMS-Weiterleitung über iMessage funktioniert nur über das mobile Datennetz – hat der Nutzer kein Datenpaket gebucht, sondern surft ausschließlich über WLAN, funktioniert die Weiterleitung der SMS-Nachrichten nicht.



## Mac: App-Fenster zu Tabs machen

Tabs lassen sich grundsätzlich leichter verwalten als separate Fenster. Bestes Beispiel dafür ist der Browser. Ab macOS Sierra unterstützen auch viele System-Apps Tabs. Sind zum Beispiel mehrere Fenster von TextEdit oder der Vorschau geöffnet, lassen sie sich mit wenigen Klicks in ein einzelnes Fenster mit mehreren Tabs zusammenführen.

Über die Tastatur ist das Feature bislang nicht zu erreichen, nur über das Menü:

1. Wir starten mit mehreren Fenstern des gleichen Programms, im Beispiel ist die Vorschau-App zu sehen.
2. Jetzt eines dieser Fenster in den Vordergrund holen, sodass oben am Bildschirm das Menü erscheint.
3. Dort folgen Klicks auf **Fenster, Alle Fenster zusammenführen**.

Schon werden alle offenen Dokumente als Tabs in ein einzelnes Fenster verstaat.



## Leseliste in Safari leichter nutzen

Mit der Leseliste können im Safari-Browser Internetseiten gespeichert werden, wenn sie später gelesen werden sollen. Dabei archiviert das Programm nicht nur die jeweilige URL, sondern kopiert auch die Inhalte der Seite auf die Festplatte. Der Vorteil: Später können sie auch ohne Verbindung zum Internet gelesen werden.

Die Leseliste im Safari-Browser ist über die Seitenleiste jederzeit erreichbar. Dazu befindet sich oben in der Kopfzeile des Fensters ein eigener Button, mit dem sich diese seitliche Leiste ein- und ausblenden lässt. Innerhalb der Seitenleiste dann auf das Brillen-Symbol klicken, um zur Leseliste umzuschalten.

Hier ein weiterer Clou: Hat man eine bestimmte Webseite aus der Leseliste geöffnet und zu Ende gelesen, genügt es, weiter nach unten zu scrollen. Dann öffnet Safari automatisch die nächste archivierte Webseite aus dieser Liste. So spart man sich das einzelne Anklicken der archivierten Seiten.

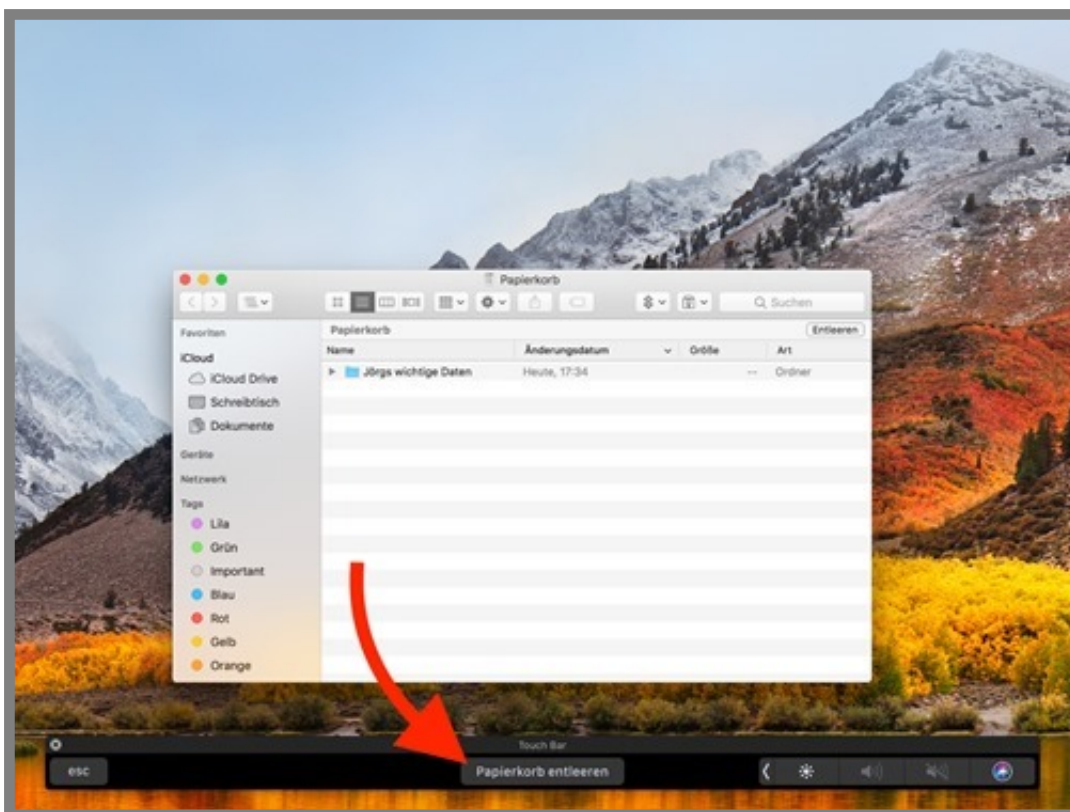


## Papierkorb leichter leeren am Mac

Auf der rechten Seite unten am Bildschirm von Mac-Computern erscheint immer der Papierkorb. Hier werden bereits gelöschte Dateien und Ordner noch vorübergehend aufbewahrt. Am MacBook lässt sich der Papierkorb nicht nur über die rechte Maustaste leeren, es geht auch einfacher.

Eine Möglichkeit besteht beispielsweise darin, zuerst mit dem Mauszeiger auf das Papierkorb-Symbol zu zeigen. Dann fest auf das Force Touch-Trackpad drücken, sodass das Kontextmenü erscheint. Hier findet sich der Eintrag zum Leeren des Papierkorbs.

Verfügt das eigene MacBook Pro über eine Touch Bar, genügt zum Löschen der Inhalte des Papierkorbs auch ein normaler Klick auf das Papierkorb-Symbol im Dock. Daraufhin wird in der Touch Bar ein Button sichtbar, der zum Leeren des Papierkorbs nur angetippt werden muss.





## In Excel leere Zellen löschen

Bei der Arbeit mit großen Tabellen im Tabellen-Programm Excel kommt es öfter vor, dass einzelne oder mehrere Werte gelöscht werden müssen. Übrig bleiben leere Zellen. Die kann man leicht auch noch loswerden.

Anstatt alle leeren Zellen in einer Excel-Tabelle manuell einzeln zu entfernen, geht dies auch viel einfacher, was Zeit spart:

1. Im ersten Schritt einen Rahmen um den Bereich ziehen, der unter anderem die leeren Zellen enthält.
2. Jetzt oben im Menü auf **Start, Suchen und Auswählen, Gehe zu...** klicken.
3. Im erscheinenden Dialogfeld folgt ein Klick auf den Button **Inhalte...**
4. Hier den Eintrag **Leerzellen** markieren und mit **OK** bestätigen.
5. Zum Schluss oben im Menü bei **Start** auf **Löschen** klicken – fertig!

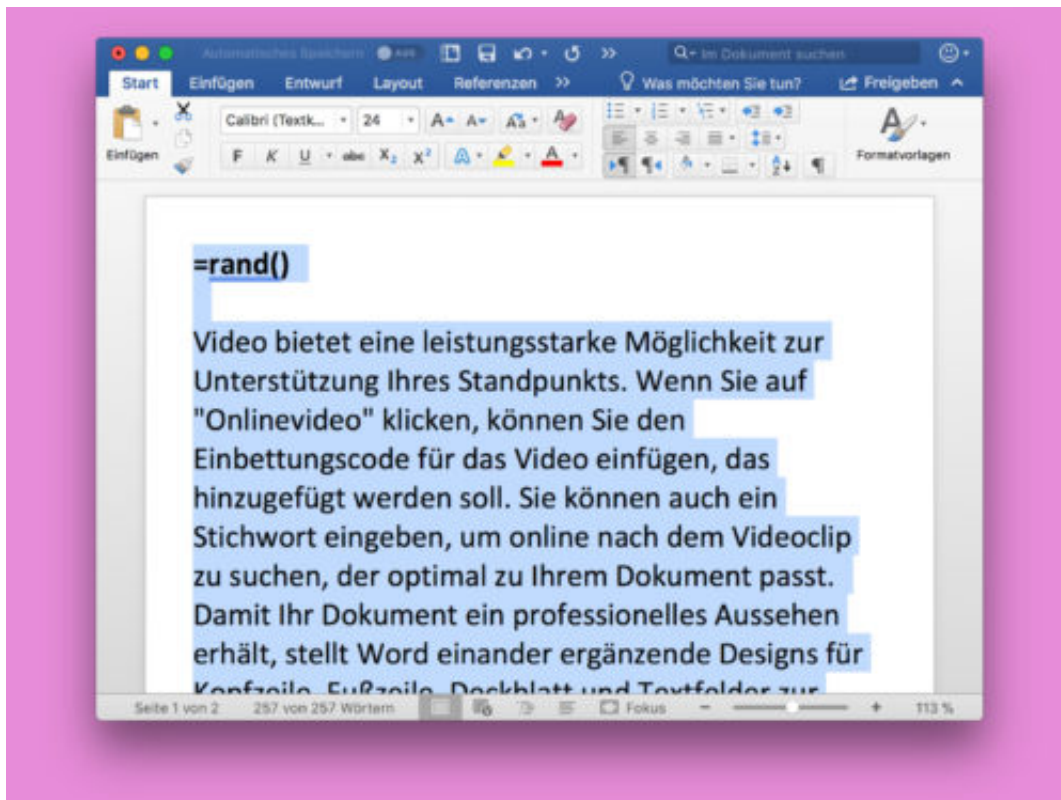


## Zwei Arten Fülltext in Word einfügen

Mit Microsoft Word lässt sich auf Wunsch Text erzeugen, der die Rolle eines Platzhalters übernimmt. Neben dem klassischen Lorem-ipsu-Text können Word und PowerPoint auch sinnvolleren Text einfügen. Das ist praktisch, wenn das Layout einer Datei überprüft werden soll.

In Word 2016 für Windows kann ein Text im Lorem-ipsu-Still eingefügt werden, indem folgendes Kommando eingegeben und mit Druck auf die [Enter]-Taste bestätigt wird:  
**=lorem()**

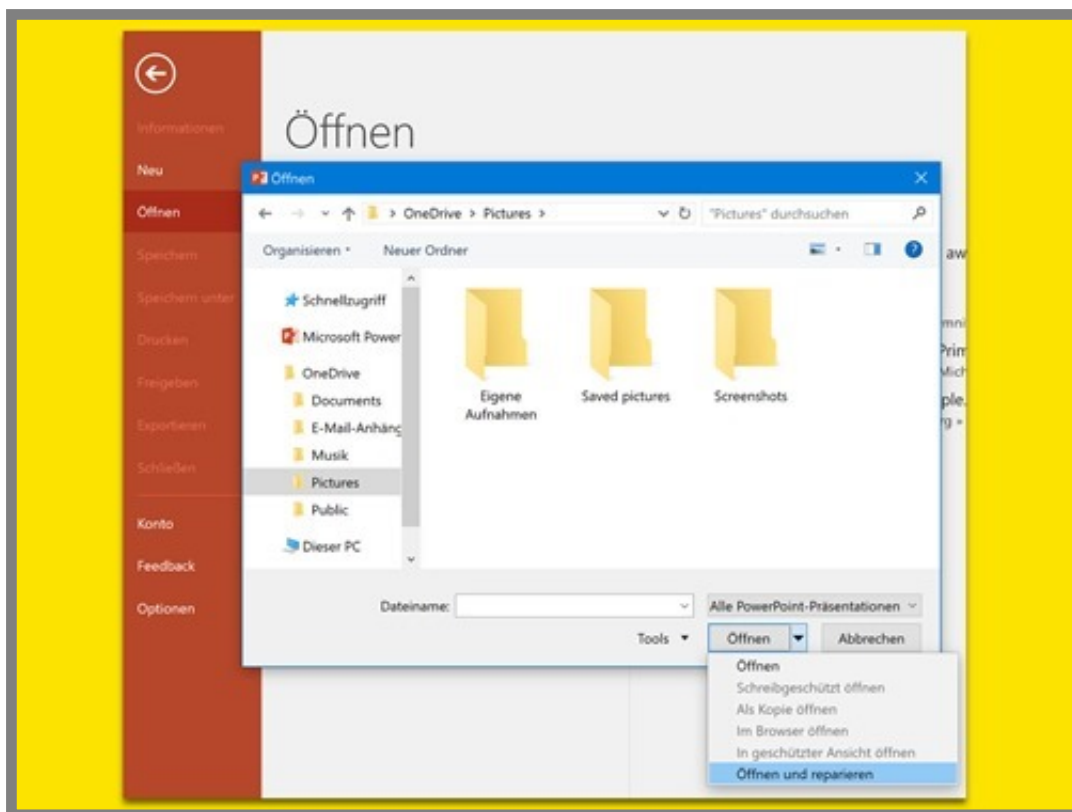
Auf ähnliche Weise funktioniert auch das Einfügen von Fülltext:  
**=rand()**



## Beschädigte Office-Dokumente reparieren

Wenn der Computer abstürzt oder ein anderes unerwartetes Ereignis eintritt, können Word-Dokumente, Excel-Tabellen und Co. beschädigt werden. Dann lassen sich die Dateien nicht mehr problemlos auf jedem Gerät öffnen. Oft lassen sich die Fehler mit der integrierten Reparatur-Funktion korrigieren.

1. Um ein beschädigtes Office-Dokument zu reparieren, wird als Erstes die zugehörige Office-Anwendung gestartet. Im Beispiel nutzen wir Microsoft PowerPoint.
2. Jetzt oben links auf **Datei** und dann auf **Öffnen, Durchsuchen** klicken.
3. Nun auf der Festplatte die gewünschte Datei herausuchen und markieren.
4. Als Nächstes unten auf der rechten Seite des Öffnen-Buttons auf den kleinen Pfeil klicken, sodass ein Menü eingeblendet wird.
5. Hier findet sich unter anderem auch die Funktion **Öffnen und reparieren**.

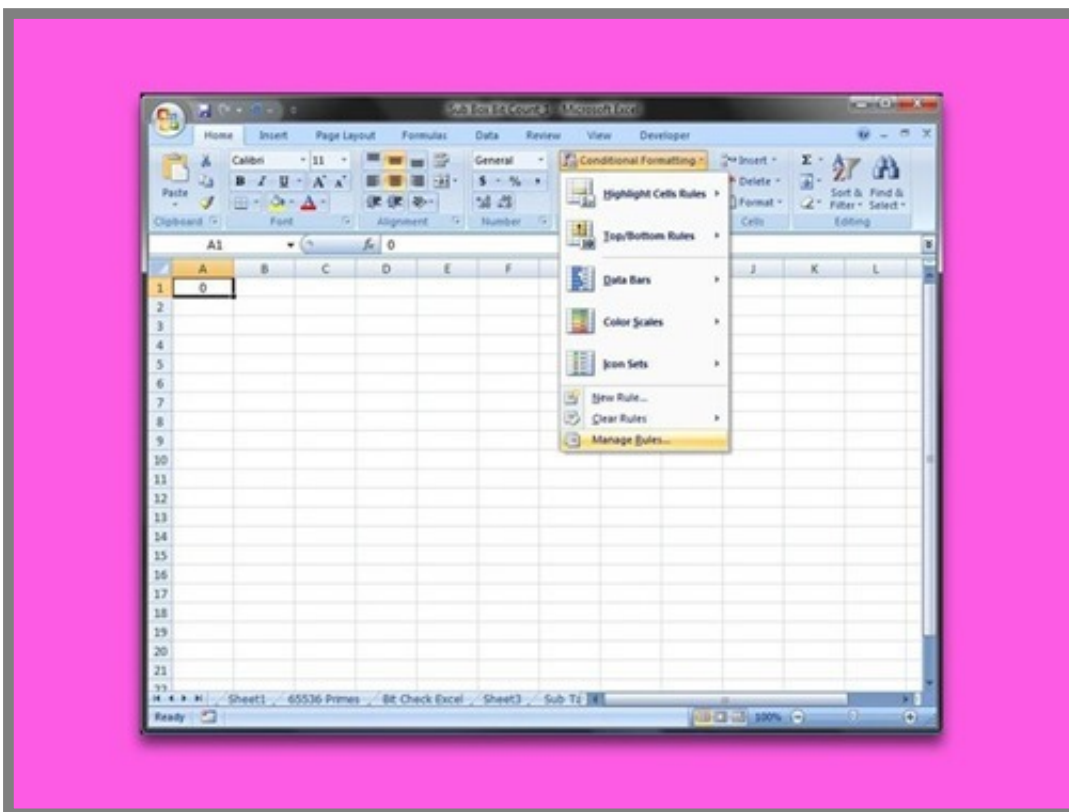


## Excel: Zellen mit bestimmten Wörtern hervorheben

Die Funktion zum Suchen und Ersetzen kennt jeder aus Microsoft Word. Tatsächlich funktioniert sie auch in Microsoft Excel – allerdings nur dann, wenn eine Tabelle nicht zu viele Zellen enthält. Doch selbst in diesem Fall lassen sich Zellen, die bestimmte Begriffe enthalten, wenigstens farblich markieren. So findet man sie schneller.

Die bedingte Formatierung lässt sich wie folgt einrichten:

1. Zunächst oben im Menü auf **Start, Bedingte Formatierung, Regeln verwalten** klicken.
2. Es folgt ein Klick auf den Button **Neue Regel**.
3. Hier die Option **Formel zur Ermittlung der zu formatierenden Zellen verwenden** auswählen.
4. Im Feld darunter wird jetzt folgende Formel eingetragen:  
**=ISTZAHL(SUCHEN("Begriff", C1))**  
Dabei verweist C1 auf die Zelle, in der der Begriff enthalten ist.
5. Jetzt bei **Format, Füllung** die gewünschten Farben festlegen.
6. Zum Schluss noch den Zellbereich hinterlegen, für den diese Formel gelten soll.



## Facebook-Namen auf iPhone und Android ändern

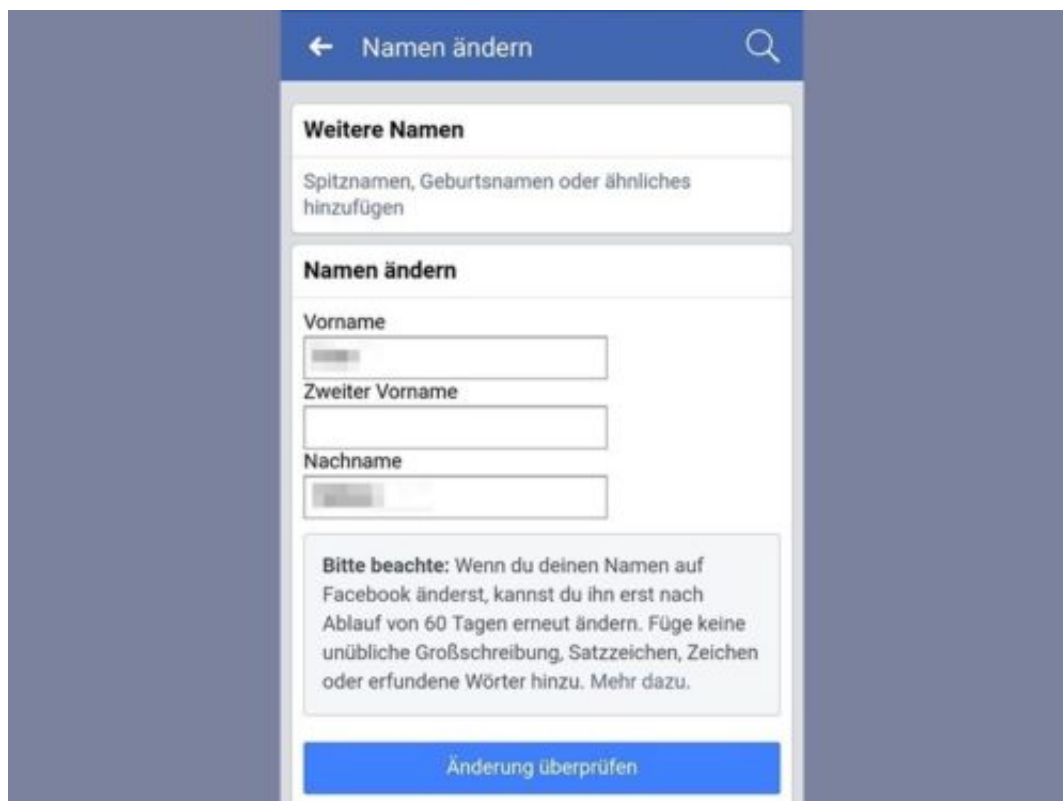
Wer sich in einem sozialen Netzwerk anmeldet, gibt bei der Erstellung des Profils für gewöhnlich seinen Namen an und/oder wählt einen Profilnamen. Den Namen sollte man sorgfältig wählen, denn ihn nachträglich zu ändern, ist bei den meisten Plattformen eher schwierig.

Bei Facebook gibt es für Account-Namen strenge Regeln. Um Fake-Accounts zu vermeiden, ist die Umbenennung hier nur alle 60 Tage möglich. Wer trotzdem seinen Namen Facebook-Namen ändern möchte, kann das über folgende Einstellungen tun:

1. **Facebook-App** öffnen
2. Den **Menü-Button** antippen
3. **Einstellungen** auswählen
4. **Kontoeinstellungen** wählen
5. Den Punkt **Allgemein** antippen

Unter **Name** nun den Vor- und Nachnamen eingeben. Zusätzlich können auch zweite Vornamen, Spitznamen oder Geburtsnamen im Profil angegeben werden. Ist der Name gespeichert, einfach auf **Änderung überprüfen** tippen.

Facebook wird die gewünschte Namensänderung jetzt kontrollieren und eine Benachrichtigung abschicken, sollte der gewünschte Name unzulässig sein. Bei einem positiven Ergebnis wird von nun an der neue Name in Facebook angezeigt.



## Verschwommene Bilder in WhatsApp

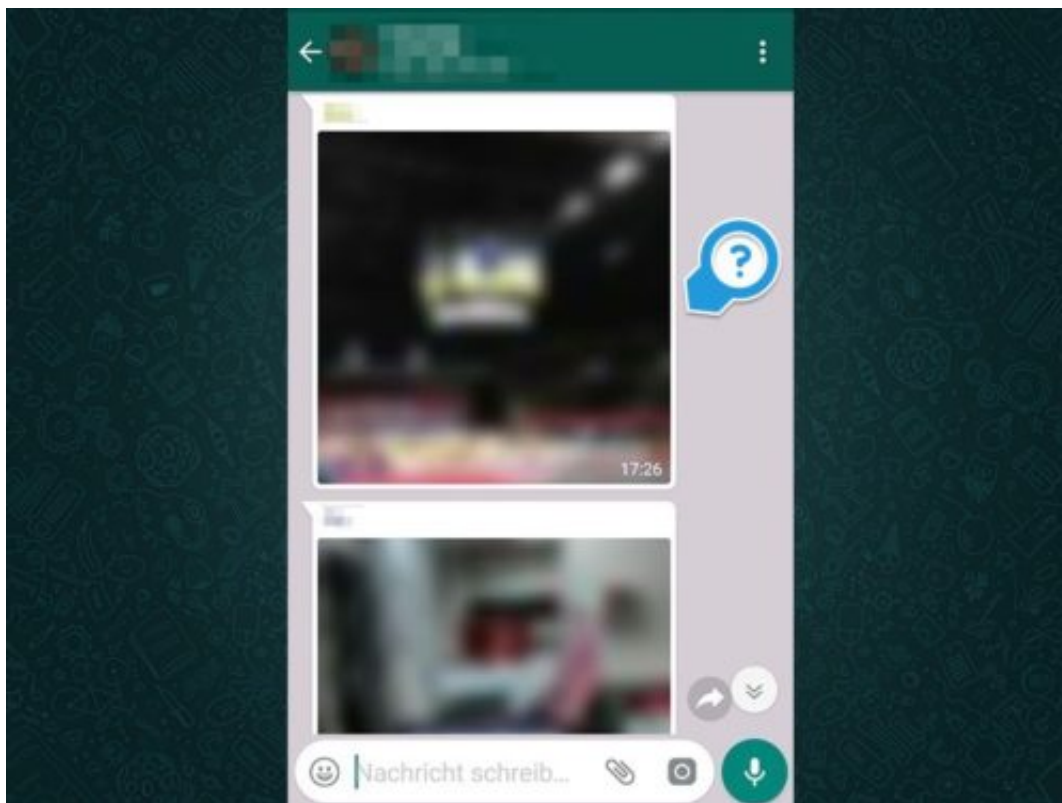
Über WhatsApp lassen sich nicht nur Texte austauschen, sondern auch Bilder, Videos, GIFs oder Audio-Dateien. User können sie verschicken und empfangen. Dem ein oder anderen dürfte es schon einmal passiert sein, dass Bilder in einem Chat nur noch stark verschwommen erscheinen. Das ist allerdings kein Softwarefehler und auch das Handy ist nicht defekt.

Einer der Gründe, warum ein Bild im Chat undeutlich dargestellt wird, ist, dass es noch gar nicht heruntergeladen wurde. In diesem Fall liegt das Bild zwar auf dem WhatsApp-Server, wurde allerdings nicht an das Smartphone übertragen.

Das kann eventuell daran liegen, dass keine stabile Internetverbindung möglich war, als das Bild über den Server ging. Erkenne lässt sich das an dem Pfeil-Symbol, welches im Bild angezeigt wird. Durch einen Tap auf den Pfeil wird das Bild dann nachträglich heruntergeladen und korrekt angezeigt.

Ein weiterer Grund könnte sein, dass das entsprechende Bild zwar heruntergeladen wurde, aber nachträglich aus dem Speicher des Smartphones gelöscht wurde. Das kann schnell ungewollt bei der Speicherbereinigung passieren, die das Smartphone schneller machen soll.

Ein gelöscht Bild lässt sich leider nicht einfach wiederherstellen oder erneut herunterladen, da [WhatsApp](#) die Daten nach der Übertragung von seinen Servern löscht. Um das Bild wieder auf das Smartphone zu bekommen, muss es vom Chat-Partner erneut versendet werden.

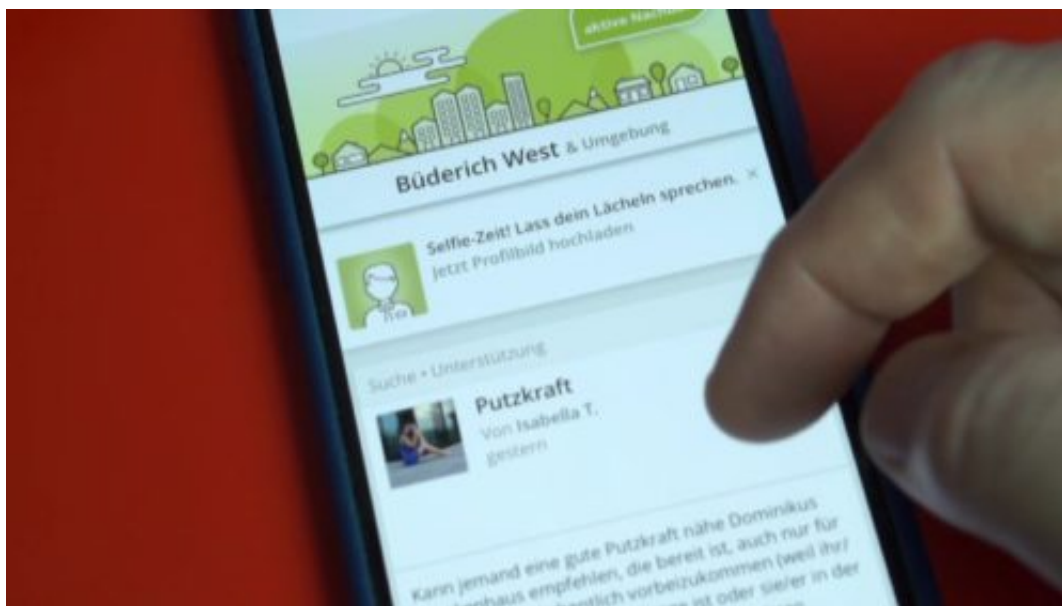


## Das Soziale Netzwerk für die Nachbarschaft: nebenan.de

Die meisten sogenannten Sozialen Netzwerke machen die Welt zum Dorf: Jeder ist gleich nah - egal, ob guter Freund oder Fremder, ob direkter Nachbar, in derselben Stadt wohnend oder am anderen Ende der Erde. Doch es gibt Themen, die interessieren nur Menschen in der unmittelbaren Nachbarschaft. Deshalb gibt es nebenan.de: Hier kann man nur mit Menschen kommunizieren, die gleich um die Ecke wohnen.

[nebenan.de](https://www.nebenan.de) ist das genaue Gegenteil von der großen weiten Welt. nebenan.de ist ein Soziales Netzwerk für die unmittelbare Nachbarschaft. Wer hier seine Postleitzahl eingibt, sieht gleich, was das Netzwerk unter Nachbarschaft versteht – welches Gebiet. Man kann sich nur mit Personen in diesem Bereich austauschen. Und man muss seine Wohnadresse belegen.

Hier sieht man, was in der Nachbarschaft los ist. Ob jemand Hilfe braucht oder etwas abgeben will. Alltägliche Dinge. Aber die Leute betreffen, die man kennt – oder die in der Nähe wohnen. Ein charmantes Konzept, das Aufmerksamkeit verdient.



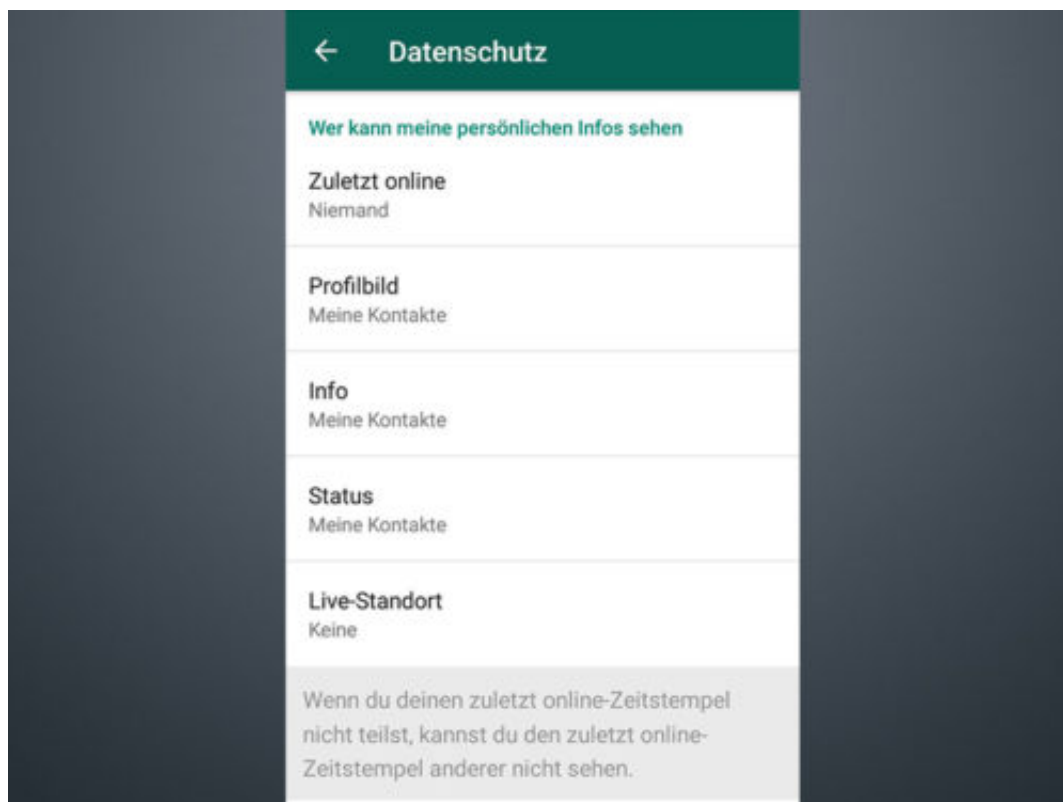
## Profilbild und Status in WhatsApp verbergen

WhatsApp-Nutzer können ein Profilbild hinterlegen, das jeder in WhatsApp sehen kann. Dasselbe gilt für den aktuellen Status. Wer nicht möchte, dass jeder Foto und Status sehen kann, kann in WhatsApp nach Bedarf einstellen, wer diese Informationen sehen darf.

WhatsApp ist zweifellos einer der bequemsten Wege, via Smartphone mit anderen zu kommunizieren. Wer mit anderen kommunizieren möchte, braucht lediglich seine (oder ihre) Mobilfunknummer. Schon lässt sich das WhatsApp-Profil einsehen. Das funktioniert natürlich in beide Richtungen.

Wer seinen [WhatsApp](#)-Account personalisiert, hinterlegt zum Beispiel ein Profilbild oder den aktuellen Status, den dann jeder sehen kann. Um zu verhindern, dass jeder diese Angaben/daten direkt sieht, sollten folgende Einstellungen vorgenommen werden.

Zunächst **WhatsApp** öffnen und über **Einstellungen** den eigenen **Account** aufrufen. Hier **Datenschutz** auswählen und für die jeweiligen Punkte entweder die Option **Jeder**, **Meine Kontakte** oder **Niemand** festlegen.





## Alte Snapchat-Version wiederherstellen

Viele Nutzer ärgern sich derzeit über das letzte Update für Snapchat, das die Benutzeroberfläche radikal verändert. Unter iOS gibt es allerdings die Möglichkeit, die alte Version über einen kleinen Umweg wiederherzustellen.

Dieser Weg dürfte auf kurz oder lang allerdings von den Entwicklern abgeschafft werden, da es bisher keine Absicht gibt, die Änderungen für Snapchat rückgängig zu machen. Wer ein iPhone besitzt und sich die alte Version zurückwünscht, sollte die Möglichkeit also nutzen, solange sie funktioniert.

Zunächst die Snapchat-App vom iPhone deinstallieren und alle verknüpften Daten löschen. In **Einstellungen** nun **iTunes und App Store** öffnen und die **automatischen Updates für Apps deaktivieren**. Nun Snapchat aus dem App Store **neu herunterladen**, allerdings nicht einloggen.

Stattdessen nur die **E-Mail-Adresse** eingeben, auf **Passwort vergessen** tippen und die Option **Passwort-Reset** auswählen. Nun den zugesendeten Reaktivierungscode nutzen, um ein neues Passwort festzulegen und mit diesem jetzt bei Snapchat anmelden. Hat alles geklappt, sollte jetzt wieder die alte Snapchat-Version vor dem Update laufen.

Ein Nachteil des Umweges ist allerdings, dass künftig keine Updates und Verbesserungen mehr in die App geladen werden, was sie auf lange Sicht eventuell unbrauchbar macht.



## Sicherheitsnummer in WhatsApp anzeigen

Bei Messengern ist Sicherheit das A und O. Um seine Chats besser abzusichern, hat WhatsApp vor einiger Zeit die End-zu-End-Verschlüsselung eingeführt. Das bedeutet, dass jede einzelne Unterhaltung ihre eigene 60-stellige Sicherheitsnummer hat, die alle Chat-Partner verwenden, um die Chats sicher zu verschlüsseln.

Wer in seinem Chat die Nachricht "Sicherheitsnummer wurde geändert" sieht, muss sich deswegen nicht gleich Sorgen machen. In den meisten Fällen bedeutet das lediglich, dass der Chat-Partner entweder ein neues Smartphone oder WhatsApp neu installiert hat.

Wer trotzdem ganz sicher gehen und seine Sicherheitsnummer mit dem Chatpartner abgleichen will, findet sie folgendermaßen:

1. **WhatsApp** öffnen
2. **Chatfenster** des Kontaktes öffnen
3. Auf den **Account-Namen** des Chatpartners tippen
4. **Verschlüsselung** auswählen

Hier wird nun der komplette **60-stellige Sicherheitscode** für den Chat angezeigt. Außerdem findet sich hier auch ein **QR-Code**, der vom jeweiligen Chat-Partner gescannt werden kann, um sicherzugehen, dass der Chat verschlüsselt ist.



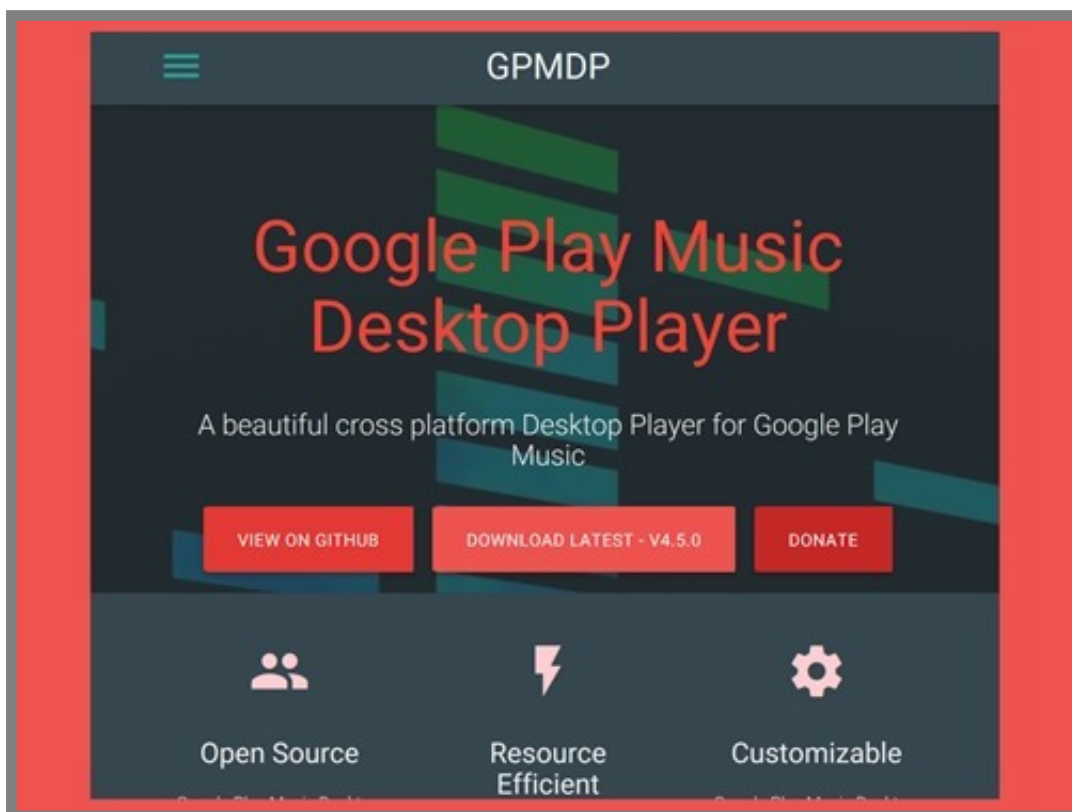
## Desktop-App für Google Music

Wer am Computer seine [Google Music-Bibliothek](#) abspielen möchte, muss das über den Browser machen – etwa mit dem zugehörigen Add-On für den Chrome-Browser. Ein Entwickler hat jetzt eine eigenständige App entwickelt: den Google Play Music Desktop Player.

Nach dem Download und Start der App ist eine Anmeldung beim eigenen Google-Konto nötig. Mit Abonnement kann man auf sämtliche Musik-Funktionen von Google Play zugreifen, während kostenlose User sich mit der eigenen Bibliothek sowie dem Zugriff auf Internet-Radios begnügen müssen. Wichtig: Adobe Flash Player muss installiert sein.

Weitere Einstellungen, etwa die Steuerung der Wiedergabe über den Mini-Player-Modus, sind übrigens nach Klick auf das Zahnrad-Symbol erreichbar. Dort kann auf Wunsch auch eine Verbindung zu einem Last.fm-Account hinterlegt werden. Angehörte Musik wird dann auch gleich automatisch gescrobelt.

<https://www.googleplaymusicdesktopplayer.com/>



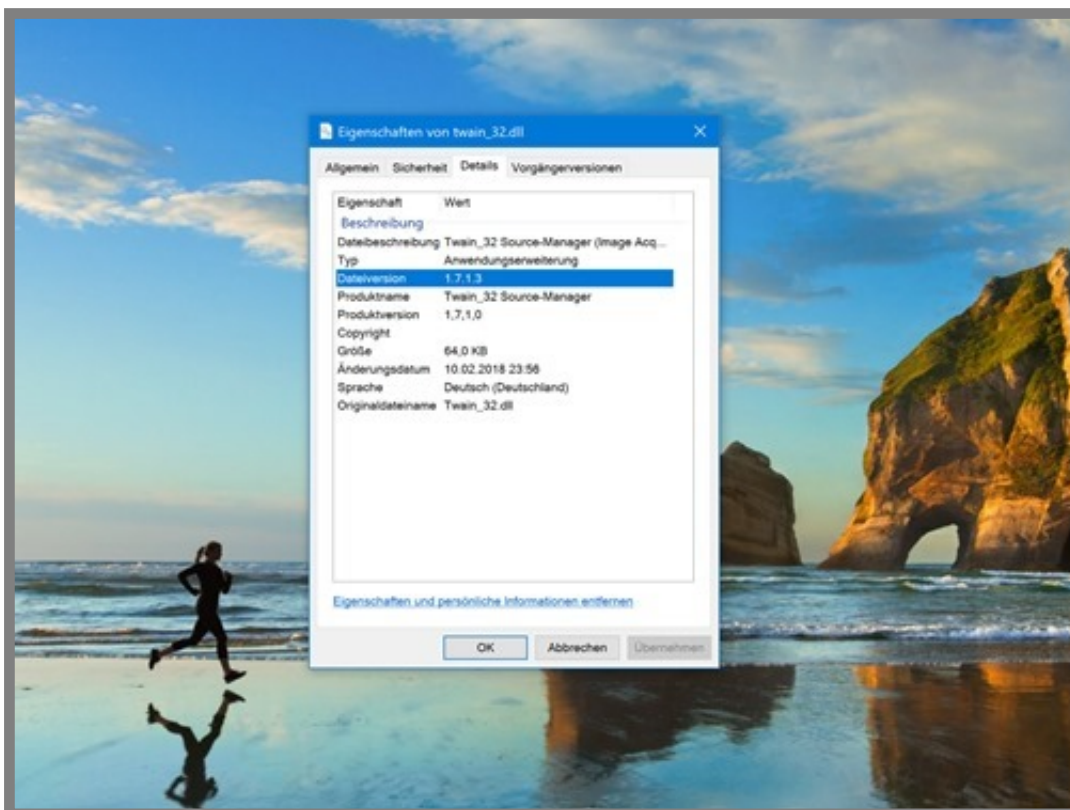
## DLL-Version herausfinden

Manche Programme greifen bei der Ausführung auf zusätzliche Funktionen zurück, die in separaten Dateien gespeichert sind. Dabei handelt es sich oft um DLL-Dateien. Und nicht selten funktionieren die Programme nur mit einer bestimmten DLL-Version. Welche Version eine DLL-Datei hat, lässt sich in Windows 10 schnell ermitteln.

Um die Version einer bestimmten DLL-Datei herauszufinden, führt man folgende Schritte aus:

1. Zunächst unten in der Task-Leiste auf das gelbe Ordner-Symbol klicken, sodass ein neues Fenster des Datei-Explorer erscheint.
2. Jetzt in den entsprechenden Ordner navigieren, der die DLL-Datei enthält.
3. Jetzt mit der rechten Maustaste auf die DLL-Datei klicken, worauf ein Menü eingeblendet wird.
4. Hier die **Eigenschaften** aufrufen und zum Tab **Details** wechseln.

Die Version der ausgewählten DLL-Datei kann jetzt hier abgelesen werden.



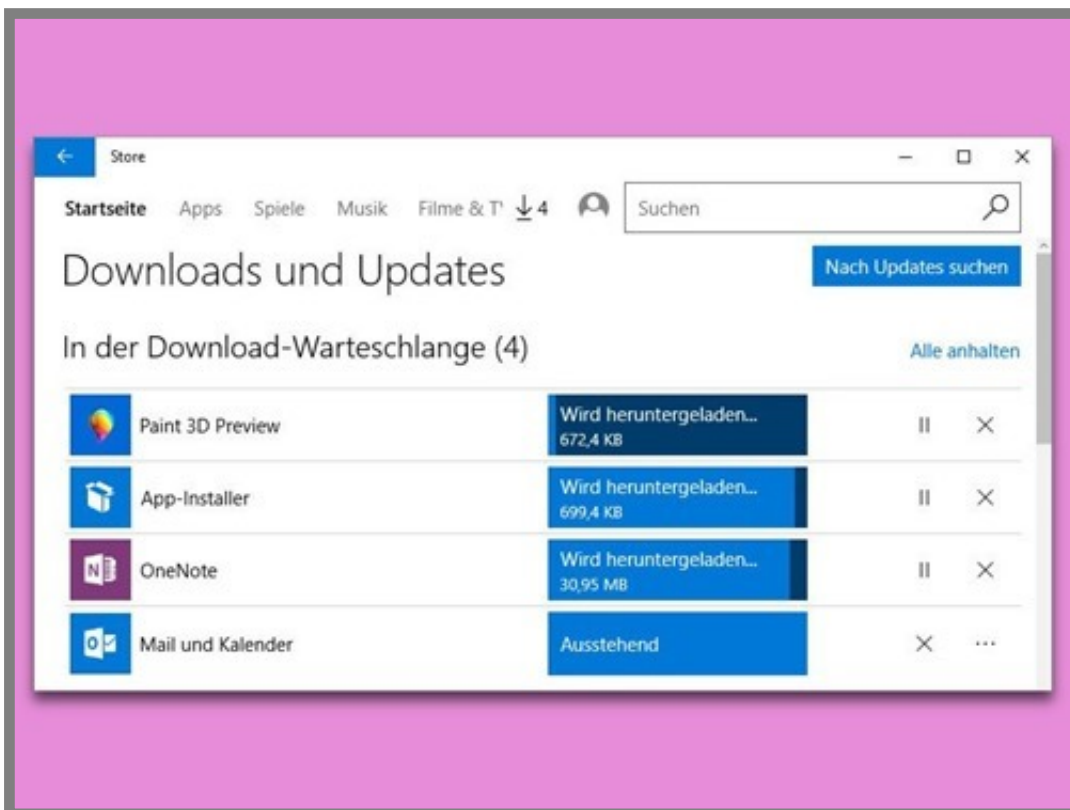
## Windows 10: Letzte App-Updates einsehen

Alle neueren Windows-Versionen aktualisieren aus dem Microsoft Store installierte Programme automatisch, wenn der Anbieter eine neue Version freigibt. Auch Microsoft-eigene Apps werden auf diese Weise selbsttätig auf dem neuesten Stand gehalten. Über den Microsoft Store lässt sich die Liste der zuletzt aktualisierten Apps jederzeit anzeigen.

Hier die nötigen Schritte, um in Windows 10 die zuletzt installierten App-Updates einzusehen:

1. Zunächst unten auf **Start, Microsoft Store** klicken. Ist das Store-Symbol noch in der Task-Leiste angeheftet, genügt natürlich auch ein Klick auf dieses Icon.
2. Im Store-Fenster jetzt oben rechts auf den Button mit den drei Punkten klicken, sodass ein Menü erscheint.
3. Hier die Rubrik **Downloads und Updates** aufrufen.

Daraufhin blendet der Store eine Liste sämtlicher kürzlich installierte Apps und Aktualisierungen ein. Diese Liste ist dabei absteigend chronologisch sortiert. Neben dem Datum der Installation erscheint hier auch die zugehörige Versionsnummer.



## Ändern des Wallpapers verhindern

Wer anderen sein Notebook ausleiht, sollte eigentlich davon ausgehen, dass das Wallpaper, also der Hintergrund auf dem Desktop, unverändert bleibt. Mit einem Eingriff in die Registrierung lässt sich effektiv verhindern, dass der Desktop-Hintergrund geändert wird.

Dazu den Pfad zu einer JPG- oder BMP-Datei (!) in die Zwischenablage kopieren. Jetzt gleichzeitig [Windows] + [R] drücken, **regedit** eingeben und mit **OK** bestätigen. Dann links zum Schlüssel **HKEY\_CURRENT\_USER, Software, Microsoft, Windows, CurrentVersion, Policies** wechseln.

Existiert hier noch kein Schlüssel namens **System**, wird dieser über die rechte Maustaste angelegt. Anschließend auf der rechten Seite eine neue Zeichenfolge erstellen, diese wird **Wallpaper** genannt. Als Wert dann den kopierten Pfad einfügen. Mit einer weiteren Zeichenfolge namens **WallpaperStyle** lässt sich das Aussehen anpassen – **0** steht für ein zentriertes Bild, **1** für eine gekachelte und **2** für eine gestreckte Grafik.

