Schieb Report

Ausgabe 2022.04

Drohnen: Verantwortungsvoll geflogen, eine gute Sache

In den USA beliefern Drohnen aus Deutschland abgelegene Krankenhäuser. Das ist ein cooles Projekt. Doch es gibt auch immer mehr Hobby-Drohnen. Aber längst nicht alle Piloten fliegen verantwortungsbewusst.

Drohnen – vor ein paar Jahren noch ein Begriff, bei dem vor allem ans Militär dachte. Heute hat man direkt das Summen und Fiepen von Hobby-Drohnen in den Ohren. Die leider häufig genau da aufsteigen, wo man sie gar nicht haben will. Für viele Menschen sind Drohnen nur noch Plagegeister, dabei könnten sie - richtig genutzt - nicht nur spektakuläre Bilder liefern.

Ein lautes Surren, wie eine Mücke, nur eben 1000x lauter: Ein Geräusch, das viele von uns kennen. Die einen hören begeistert hin, weil es sie an ihr Hobby erinnert. Bei vielen anderen steigt bei diesem Geräusch aber der Aggressionspegel.

Drohnen als potenzielle Spione

In meinem letzten Urlaub ist doch tatsächlich in der Abenddämmerung eine Drohne immer wieder an meinem Hotelzimmer vorbeigeflogen. Zum Greifen nah. Ob der – für mich unsichtbare! – Pilot hinter der Drohne nun Aufnahmen von der schönen Landschaft gemacht hat oder doch womöglich in die Zimmer blicken wollte – ich weiß es nicht.

Das sind zweifellos Momente, in denen Drohnen mächtig nerven können. Denn es ist dann nicht nur ihr Geräusch, das stört oder irritiert, sondern es kommt noch das diffuse Gefühl von Beobachtetwerden dazu. Wer weiß denn schließlich, was die Kamera gerade sieht und womöglich aufnimmt?

Hotelzimmer, Swimming-Pool oder der eigene Garten oder auch nur der Balkon sollten nicht von außen, besser gesagt oben beobachtet werden können. Leider gibt es solche Momente recht häufig und auch noch weitere Nerv-Faktoren. Wenn zum Beispiel Drohnen laut surrend durch unberührte Natur fliegen und Tiere aufschrecken. Und sie über dichte Menschenmengen fliegen... Da bekommt man

es sogar schon mal leicht mit der Angst zu tun.

Drohnen können helfen

Dabei können Drohnen richtig eingesetzt nicht nur jede Menge Spaß machen, sondern auch extrem hilfreich sein. Zum Beispiel, um Schäden an einem Dachstuhl von oben zu betrachten, einen Vermissten im Wasser mit Wärmebildkamera entdeckten oder Polizei und Feuerwehr bei Katastrophen einen schnellen Überblick verschaffen.

In den USA werden jetzt abgelegene Krankenhäuser mit Drohnen beliefert: Sie müssen nicht mal landen, sondern seilen die bis zu 6 Kg Fracht einfach ab. So lassen sich Blutproben, Impfstoffe, Arzneimittel oder dringend benötigtes Material zustellen – im Eiltempo.

Doch viele Hobby-Drohnen-Piloten nehmen es mit ihrer Verantwortung nicht so genau. Und halten weder etwas von ausreichend Abstand, noch von Anstand. Sie fliegen, wo sie wollen, egal, ob es andere stört. Solche Piloten sind verantwortlich für den schlechten Ruf, den Drohnen mitunter haben.

An dieser Stelle muss ich wohl gestehen: Ich fliege selbst gerne mit meinen Drohnen. Denn die Aufnahmen, Fotos wie Videos, die man mit so einer Drohne machen kann, sind wirklich spektakulär. Ungewöhnliche Perspektiven. Tolle Aufnahmen. Vor allem in der Natur.

Drohnen steuern bedeutet Verantwortung

Natürlich versuche ich, alles richtig zu machen, wenn ich meine Drohne steuere. Ich fliege nur da, wo es erlaubt ist, niemanden stört, niemanden gefährdet, Ich plane meine Drohnen-Flüge ganz genau. Da helfen einem spezielle Apps, die auch zeigen, wo man gar nicht fliegen darf. Etwa in der Nähe von Krankenhäusern, nahe Flughäfen oder in Naturschutzgebieten.

Umso mehr ärgere ich mich über Rüpel-Piloten, die fliegen wo sie wollen. Wie sie wollen. Es gibt mittlerweile Drohnen, die wirft man in die Luft – damit sie "schicke" Selfies machen.

Ganz ehrlich: Das halte ich für völlig verantwortungslos. Man sollte Leuten nicht einfach Drohnen in die Hand zu geben – und seien diese Drohnen noch so klein. Wer keine Ahnung hat, wie sich Drohnen steuern lassen und nur loslegen statt lernen will, stört und gefährdet sehr schnell auch ohne böse Absicht. Die Industrie erweckt den Eindruck, alles wäre kinderleicht. Aber: Eine Drohne korrekt zu fliegen ist durchaus eine Herausforderung.

Ich finde: Nicht jeder sollte Drohnen fliegen dürfen. Zum Glück haben sich die Vorschriften durch die EU-Drohnenverordnung verschärft. Piloten müssen heute mindestens 16 Jahre alt sein – wer jünger ist, darf nur völlig harmlose, kleine Spielzeugdrohnen fliegen. Und: Wer Drohnen fliegen will, muss sich registrieren. Und zumindest ein Minimum an Flugkenntnis nachweisen.

Das bewahrt uns zwar nicht vor Verrückten, die ganz bewusst ihre Drohnen in Flugverbotszonen steuern, um gegen Flugverkehr zu protestieren – wie in London Heathrow schon geschehen --, aber es macht die Fliegerei mit Drohnen sicherer.

Anlegen verschlüsselter Ordner in BoxCryptor

BoxCryptor verschlüsselt nicht die Dateien im Cloud-Service selbst, das würden die Anbieter nicht zulassen. Da Sie aber in den meisten Fällen Ihre Daten zwischen der Cloud und Ihrer Festplatte synchronisiert haben, ist das kein Problem: Verschlüsseln Sie einfach in Ihrem Dropbox-Ordner auf der lokalen Festplatte!

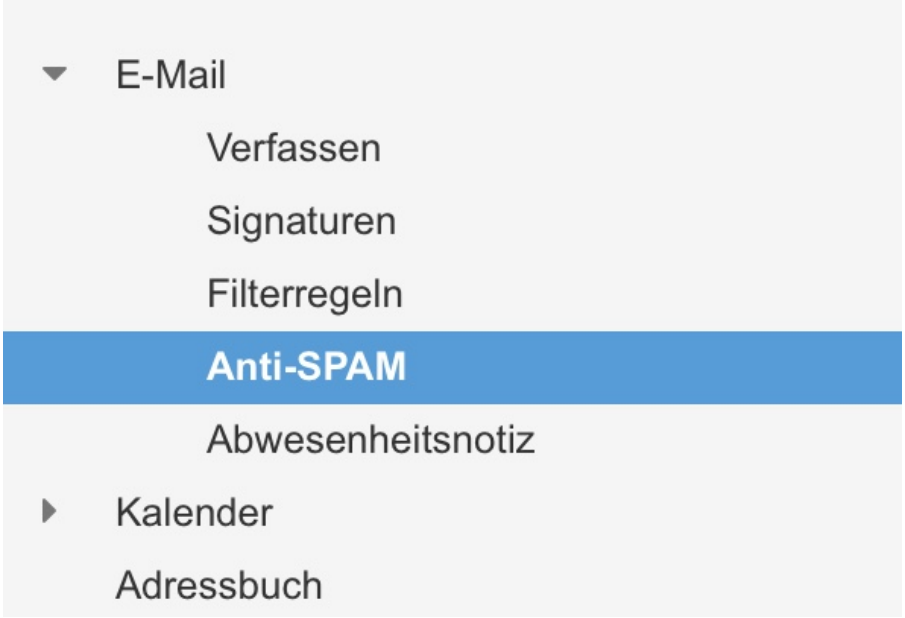
Die Verschlüsselung findet im synchronisierten Ordner statt, der Ordner wird auf Bit- und Byte-Ebene zur Dropbox übertragen und ist dort dann für Fremde unlesbar.

1. Öffnen Sie im Explorer/Finder den BoxCryptor-Ordner und darin den Cloud-Speicher, in dem Sie einen neuen, verschlüsselten Ordner anlegen wollen.
2. Sobald Sie über **Neu** > **Ordner** einen neuen Ordner anlegen, fragt die App Sie, ob Sie diesen verschlüsseln wollen.
3. Stimmen Sie dem zu, dann werden alle Dateien und Verzeichnisse, die Sie in diesem Ordner ablegen, ebenfalls verschlüsselt.
4. Die so für Unberechtigte unleserlichen Dateien werden dann auf den Cloud-Server hochgeladen. Ihr Anbieter kann damit überhaupt nichts anfangen, auch ein Hacker findet nur eine zufällige Ansammlung von Bits und Bytes, nicht aber Ihre Daten und Informationen.
5. Wenn Sie eine Datei öffnen, dann wird diese automatisch entschlüsselt, einen Unterschied zur einer unverschlüsselten Datei spüren Sie im Normalfall nicht.

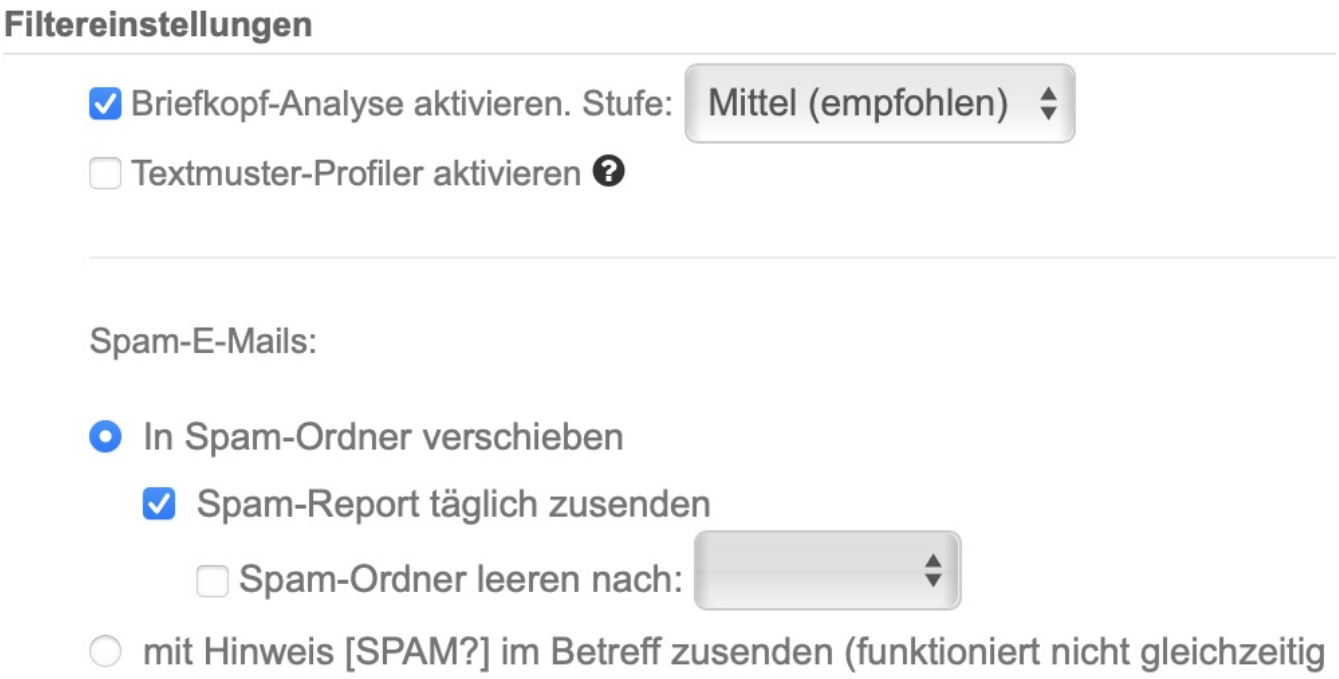
Anti-SPAM-Filter bei 1&1/IONOS konfigurieren

Wenn Sie Ihr E-Mail-Postfach bei einem externen Anbieter haben, dann übernimmt dieser auch die zentrale Verwaltung der Postfachsicherheit. Einige Anbieter wie beispielsweise 1&1/IONOS übernehmen auch die erste Schwelle des SPAM-Schutzes für Sie. Wir zeigen Ihnen, wie Sie diese beeinflussen können.

Wenn Sie den SPAM-Schutz mit Ihrem E-Mail-Programm erledigen, dann haben Sie die E-Mails immer noch auf Ihrer Festplatte im Posteingang. Die Regeln des E-Mail-Programms verschieben diese dann in die entsprechenden SPAM-Ordner. Änderungen an den Regeln, die Klassifizierung einer E-Mail als SPAM oder das Aufheben des Kennzeichens können Sie lokal machen.



Bei serverbasierten Regeln bei 1&1/IONOS müssen Sie stattdessen den Webmailer im Browser aufrufen. Klicken Sie dann oben rechts auf das **Zahnrad**, dann links auf **E-Mail** > **Anti-SPAM**. Ein Kompromiss zwischen lokaler SPAM-Behandlung und dem Ablegen auf dem 1&1/IONOS-Mailserver ist **mit Hinweis im Betreff zusenden**. Die Mails landen dann in Ihrem Mailprogramm im Posteingang und Sie können Sie anhand einer Regel selber wegsortieren.



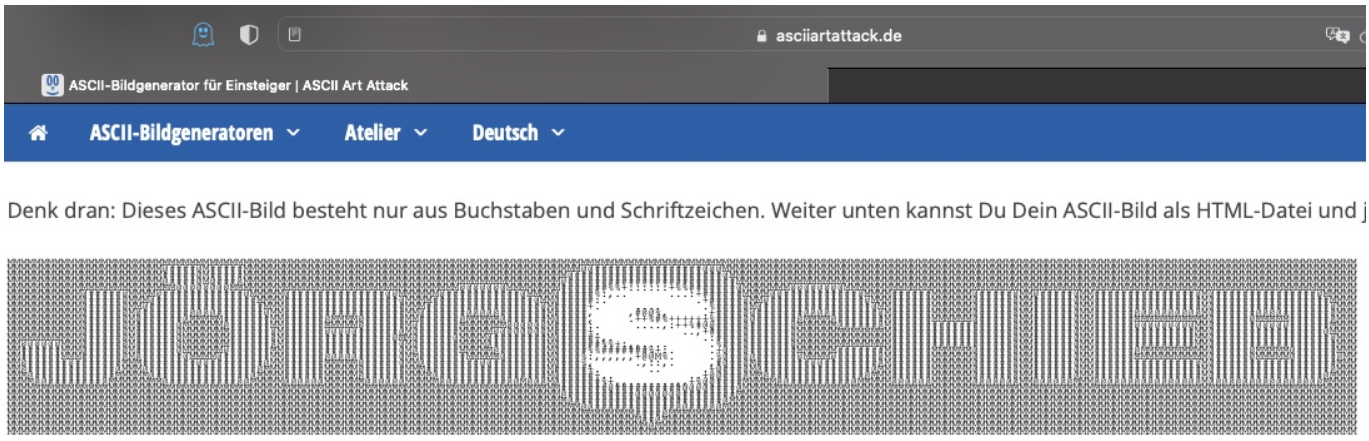
Wenn Sie den SPAM-Ordner von 1&1/IONOS verwenden wollen, dann aktivieren Sie SPAM-Report täglich zusenden. Damit haben Sie einen täglichen Überblick über die als SPAM identifizierten Nachrichten. Sie können mit wenig Aufwand Mails identifizieren, die doch kein SPAM sind und diese "befreien".

Fotos und Bilder in ASCII-Bilder umwandeln

So digital wir sind, so reizvoll wird manchmal das Analoge. Manchmal finden auf Webseiten oder in E-Mails Bilder aus Textzeichen, so, wie es früher mangels technischer Möglichkeiten oft vorkam. Diese müssen Sie nicht manuell erstellen, sondern können Webseiten wie ASCII Art Attack nutzen.

Mit dem kostenlosen Dienst können Sie Bilddateien der Formate .GIF, .JPG und .PNG, die nicht größer als 10MB sind, bearbeiten. Klicken Sie auf Bild auswählen und selektieren Sie das Bild, dass Sie in Zeichen umwandeln möchten. Geben Sie dann unter **Zeichen pro Zeile** die gewünschte Breite des ASCII-Bildes ein. Diese ist auf der einen Seite anhängig von dem Platz, den Sie haben: Je kleiner die Breite, desto eher passt das Bild auch in eine E-Mail, ohne durch einen Zeilenumbruch unleserlich gemacht zu werden.

Auf der anderen Seite bedeutet eine geringere Breite gleichzeitig auch weniger Bildinformationen, vergleichbar zur Auflösung eines JPG-Bildes. Dadurch, dass statt Bildpunkten Zeichen benutzt werden hat dies einen größeren Einfluss als man zunächst erwarten würde. Experimentieren Sie mit den Einstellungen!



Setzen Sie einen Haken bei **Ich bin kein Roboter** und klicken Sie dann auf **ASCII-Bild erstellen**. Das Bild wird jetzt in ASCII-Zeichen umgewandelt und angezeigt. Wenn Sie die Zeichen kopieren und weiterverwenden wollen, markieren Sie diese mit der Maus und kopieren sie in die Zwischenablage. Alternativ können Sie es als HTML-Datei oder JPG herunterladen, die entsprechenden Links finden Sie unten auf der Seite.

Wenn Sie sich fragen, warum Sie ein Bild aus einer Grafik in Text umwandeln sollten, um es dann wieder als Grafik zu speichern: Der künstlerische Effekt bleibt in der JPG bestehen, Windows und die Apps verwenden das Bild aber als ein Objekt, was eine einfache Handhabung und Größenveränderung erlaubt.

Apples Shot on iPhone Challenge: Teilt jetzt die besten iPhone Makrofotos

Apple lädt iPhone 13 Pro und iPhone 13 Pro Max Nutzer dazu ein, kleine Dinge ganz groß einzufangen – mit der Shot on iPhone Makrofotografie Challenge. Der Wettbewerb beginnt heute und läuft bis zum 17. Februar 2022. Die Gewinner werden im April bekannt gegeben.

Die iPhone 13 Pro Familie verfügt über das bisher fortschrittlichste Kamera-System in einem iPhone. Zum ersten Mal können Nutzer:innen scharfe, beeindruckende Nahaufnahmen von Motiven machen, die nur zwei Zentimeter entfernt sind. Um die Makrofotografie zu würdigen, lädt Apple dazu ein, die schönsten Makrofotos, die mit dem iPhone 13 Pro und iPhone 13 Pro Max aufgenommen worden sind, auf Instagram und Twitter mit den Hashtags #ShotoniPhone und #iPhonemacrochallenge zu teilen, um an der Challenge teilzunehmen.

Eine Jury aus Expert:innen der Fotobranche und Apple wird die weltweiten Einsendungen bewerten und zehn Fotos auswählen. Die Aufnahmen der Gewinner:innen werden in einer Galerie über Apple Newsroom, apple.com, Apple Instagram (@apple) und anderen offiziellen Apple Accounts vorgestellt. Sie können auch in digitalen Kampagnen, in Apple Stores, auf Plakaten oder in einer öffentlichen Fotoausstellung gezeigt werden.

Das Pro Kamera-System des iPhone 13 Pro und des iPhone 13 Pro Max verfügt über neue Ultraweitwinkel-, Weitwinkel- und Teleobjektive, die alle von der unübertroffenen Leistung des von Apple entwickelten A15 Bionic angetrieben werden. Die neue Ultraweitwinkel-Kamera hat eine deutlich größere ƒ/1.8 Blende und ein neues Autofokus-System für eine um 92 Prozent verbesserte Leistung in Umgebungen mit wenig Licht, das Bilder noch heller und schärfer werden lässt.

Das neue Design der Objektive, die Autofokusfunktion, die zum ersten Mal in der Ultraweitwinkel-Kamera des iPhone zum Einsatz kommt, und die fortschrittliche

Software ermöglichen es Anwender:innen, beeindruckende Makroaufnahmen zu machen, bei denen die Motive riesig erscheinen.

Einige der beeindruckendsten Beispiele für Makrofotografie sind Aufnahmen von scheinbar alltäglichen Gegenständen wie einer Haarbürste, Lebensmittel oder Naturmotiven wie Eis, Schnee, Federn, Blumen, Insekten oder Haustieren. Das Schöne an der Makrofotografie ist, dass sie das Gewöhnliche in etwas Außergewöhnliches verwandeln kann.

Tipps für die Makrofotografie mit einem iPhone 13 Pro:

- Minimaler Abstand zum Objekt — man kann sich bis auf zwei Zentimeter an das Motiv annähern.
- Hauptfokuspunkt in der Mitte des Bildes — dort ist die Schärfe bei Makroaufnahmen mit dem iPhone am höchsten.
- Einen Bereich im Bildausschnitt antippen — so legt man einen bestimmten Fokuspunkt.
- Mit Faktor 0,5x aufnehmen, um ein Ultraweitwinkel-Sichtfeld zu erfassen, oder mit Faktor 1x für einen engeren Bildausschnitt — das iPhone schaltet beim Annähern automatisch die Kamera um und behält dabei den Bildausschnitt mit Faktor 1x bei.

Der Unterschied zwischen Microsoft 365 Privat und Business

Microsoft 365 (früher: Office 365) findet immer mehr Verbreitung. Viele Beschreibungen der Funktionen kranken aber daran, dass sich die Privat- und die Business-Pläne funktional deutlich unterscheiden. Wir zeigen Ihnen, wie Sie den richtigen Plan für Sie identifizieren können!

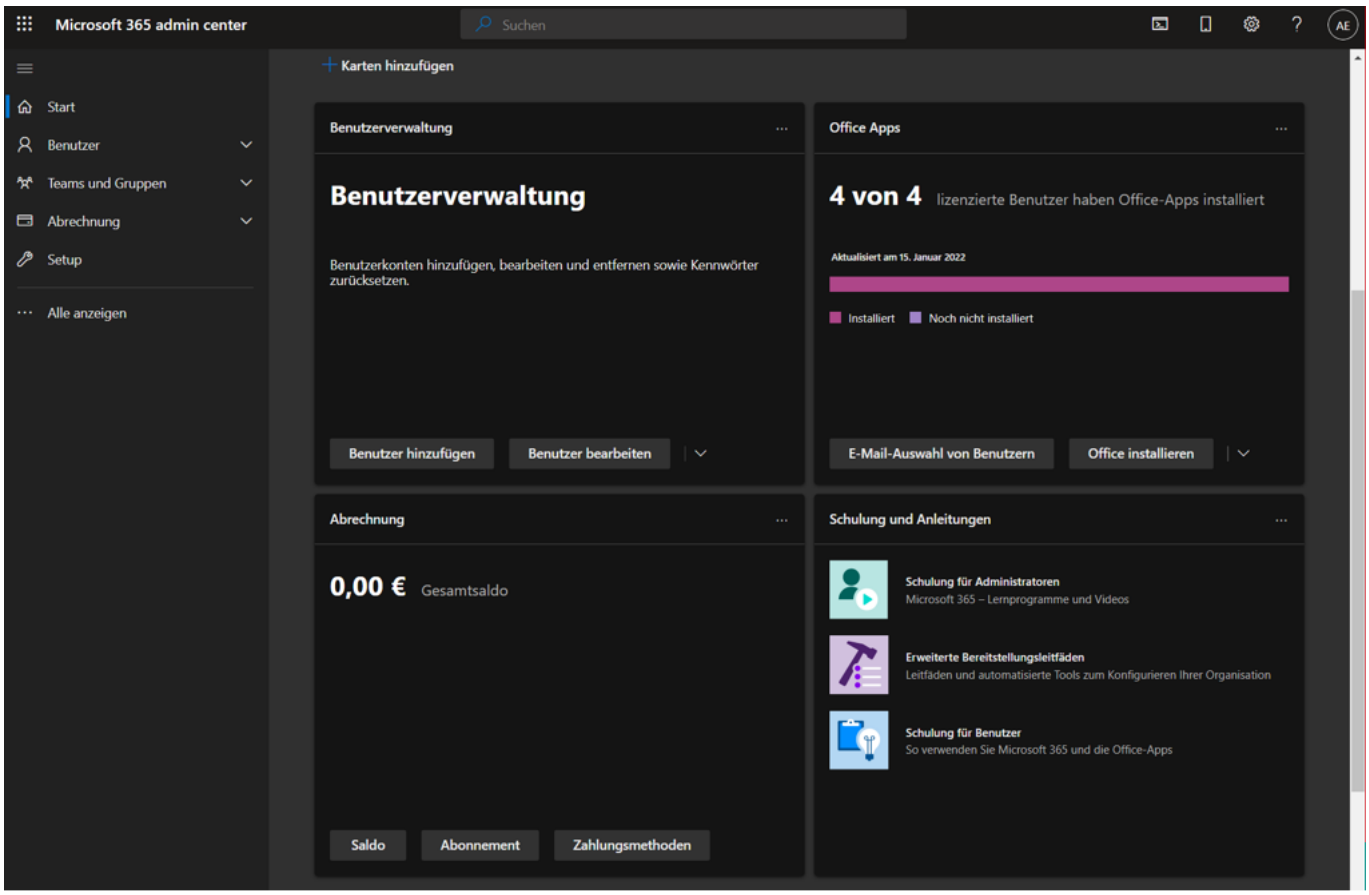
Was ist nun das richtige Modell für Sie? Die Frage lässt sich kaum allgemein beantworten. Microsoft unterscheidet zwei Arten von Plänen für Microsoft 365:

- **Für Zuhause:** Diese Pläne richten sich an Einzelpersonen (Microsoft 365 Single) oder Familien mit 2-6 Personen (Microsoft 365 Family), die hauptsächlich die am meisten genutzten Office-Apps nutzen wollen, ohne die erweiterten Möglichkeiten der Zusammenarbeit über Apps und Organisationen zu nutzen.
- **Für Unternehmen:** Hier kommen neben der Nutzung der Office-Apps noch die Möglichkeiten zur Zusammenarbeit über die Vollversion von

Teams, die Einrichtung eigener Organisationen und weitere Office-Programme wie beispielsweise Access und Publisher hinzu.

Einen Überblick über die jeweils aktuellen Pläne finden Sie hier.

Wie immer ist die Abgrenzung nicht so scharf, wie Sie auf dem Papier dargestellt wird. Nicht umsonst wir eine Familie oft mit einer kleinen Firma gleichgesetzt! Wenn Sie die Familie zentral verwalten wollen, dann macht es durchaus Sinn, einen der Pläne für Unternehmen zu verwenden. Ob Sie Mitarbeiter oder Familienmitglieder verwalten, die Tätigkeiten sind nahezu dieselben!



Hier hilft oft die Antwort auf eine einfache Frage zu finden: Wollen oder müssen Sie alles zentral verwalten, oder überlassen Sie das jedem Benutzer? In der Handhabung ist der große Unterschied zwischen den Privatanwender- und den Businessversionen, dass Sie bei Letzteren ein zentrales Administrationsportal zur Verfügung haben.

Die Zuweisung von Lizenzen, die Vergabe von Passwörtern/das Entsperren von Konten, Vorgaben an die Passwortsicherheit und vieles mehr können Sie darin

zentral verwalten. Besonders, wenn in der Familie minderjährige Anwender vorhanden sind, ist das sehr empfehlenswert. Für Firmen natürlich sowieso!

Festlegen der Rechte von Besprechungsteilnehmern in Teams

Teams ist zum Standard-Programm für Zusammenarbeit geworden, in Windows 11 ist es sogar direkt ins Betriebssystem integriert. Die Nutzung wird deutlich effizienter, wenn Sie im Vorfeld festlegen, was Teilnehmer an einer Besprechung dürfen!

In den meisten Fällen erstellen Sie erst einen Termin in Outlook, der dann den Link zur Teams-Besprechung enthält. In einem solchen Fall haben Sie noch die Möglichkeit, die Rechte zum Zugang zum Termin wie auch zum Verhalten während der laufenden Besprechung zentral festzulegen. Klicken Sie dafür im Termin-Fenster in der Symbolleiste auf **Besprechungsoptionen**.

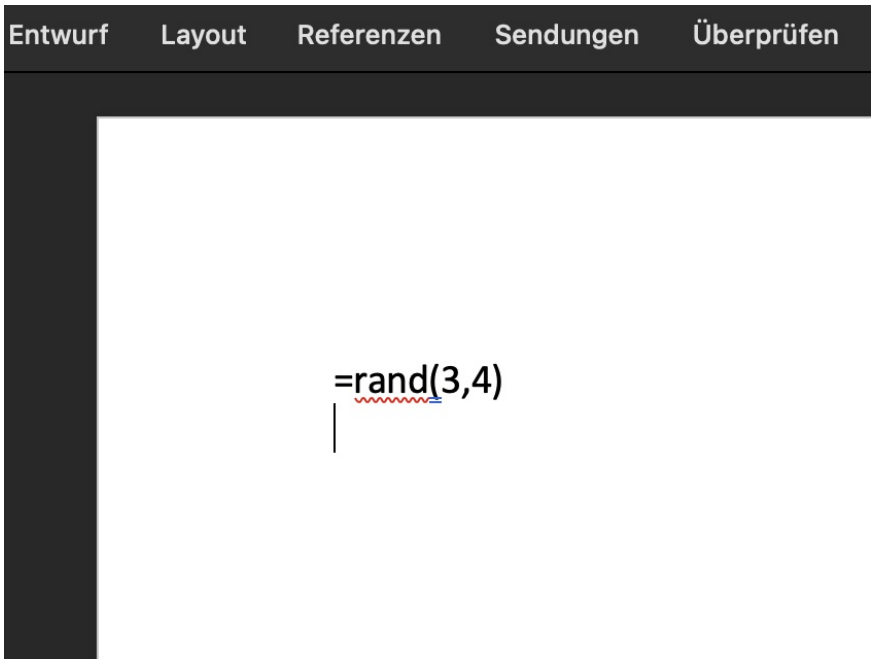
Unter **Wer kann den Wartebereich umgehen?** können Sie festlegen, welche Teilnehmer vorher im Wartebereich auf Einlass warten müssen und welche direkt in den Termin kommen. Das macht Sinn, wenn sich zwei Parteien in dem Termin treffen und nur bestimmte Inhalte für alle zugänglich sein sollen.

Mit den Einstellungen unter **Wer kann präsentieren?** legen Sie fest, wer das Recht hat, den Bildschirm zu teilen. Hier können Sie auch das **Mikrofon** und die **Kamera** sperren. Je restriktiver Sie die Einstellungen wählen, desto mehr Ordnung bekommen Sie in den Termin. Gleichzeitig aber schränken Sie die Möglichkeit der Mitwirkung der Teilnehmer massiv ein. Wägen Sie also schon im Vorfeld ab, welchen Charakter Ihr Meeting haben soll.

Einfügen von Blindtext in Word

Normalerweise füllen Sie Ihre Word-Dokumente mit sinnvollem Text. Manchmal geht es aber darum. vorab das Format zu bestimmen und abzustimmen, ohne die konkreten Inhalte zu kennen. Word erlaubt Ihnen das schnelle Einfügen von Blindtext, ohne diesen manuell eingeben zu müssen.

Oft ist die Word-Datei nur die Grundlage für das Endprodukt: Ein Flyer, ein Handbuch, eine Diplomarbeit gehen an eine Druckerei oder eine Marketing-Agentur. Die brauchen einen gewissen Vorlauf und möchten möglichst schnell ein Dokument mit dem erwarteten Umfang und Format haben. Ob darin der finale Text steht oder ungeordnete Zeichen, ist im ersten Schritt egal.



Um Bereiche Ihres Word-Dokumentes zu füllen, geben Sie als Text **=rand(x,y)** ein. An Stelle des **x** setzen Sie die gewünschte Zahl der Absätze und an Stelle des **y** die Zahl der Sätze pro Absatz und drücken Sie die **Eingabetaste**.

Video bietet eine leistungsstarke Möglichkeit zur Unterstützung Ihres Standpunkts. Wenn Sie auf "Onlinevideo" klicken, können Sie den Einbettungscode für das Video einfügen, das hinzugefügt werden soll. Sie können auch ein Stichwort eingeben, um online nach dem Videoclip zu suchen, der optimal zu Ihrem Dokument passt. Damit Ihr Dokument ein professionelles Aussehen erhält, stellt Word einander ergänzende Designs für Kopfzeile, Fußzeile, Deckblatt und Textfelder zur Verfügung.
Beispielsweise können Sie ein passendes Deckblatt mit Kopfzeile und Randleiste hinzufügen. Klicken Sie auf "Einfügen", und wählen Sie dann die gewünschten Elemente aus den verschiedenen Katalogen aus. Designs und Formatvorlagen helfen auch dabei, die Elemente Ihres Dokuments aufeinander abzustimmen. Wenn Sie auf "Entwurf" klicken und ein neues Design auswählen, ändern sich die Grafiken, Diagramme und SmartArt-Grafiken so, dass sie dem neuen Design entsprechen.
Wenn Sie Formatvorlagen anwenden, ändern sich die Überschriften passend zum neuen Design. Sparen Sie Zeit in Word dank neuer Schaltflächen, die angezeigt werden, wo Sie sie benötigen. Zum Ändern der Weise, in der sich ein Bild in Ihr Dokument einfügt, klicken Sie auf das Bild. Dann wird eine Schaltfläche für Layoutoptionen neben dem Bild angezeigt Beim Arbeiten an einer Tabelle klicken Sie an die Position, an der Sie eine Zeile oder Spalte hinzufügen möchten, und klicken Sie dann auf das Pluszeichen.

Word füllt die Zahl der Absätze dann mit halbwegs sinnvollem Text, der durchschnittliche Satz- und Wortlängen enthält. Die so gefüllten Bereiche werden

im Durchschnitt denen entsprechen, die Sie später mit ihrem eigenen Inhalt füllen, entsprechen.

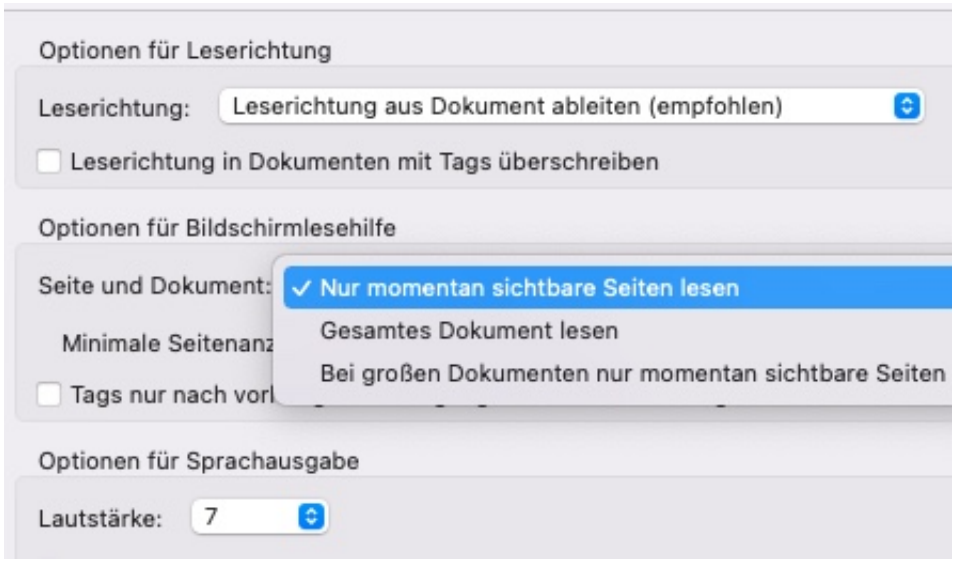
Ausschalten der Inhaltsvorbereitung beim Adobe Reader

Viele Dokumente werden nicht im ursprünglichen Format, sondern als PDF-Datei ausgetauscht. Das soll die Arbeit schneller machen. Dumm nur, wenn Sie konsequent von einer Fehlermeldung aufgehalten werden!

In bestimmten Konstellationen von Systemeinstellungen und PDF-Dateien kann es vorkommen, dass der Reader im Fenster **Inhaltsvorbereitung - Status** stehenbleibt. Die Funktion an sich ist wichtig, bereitet sie doch das Dokument für Menschen vor, die es sich über einen Screenreader vorlesen lassen. Beispielsweise, weil ihr Sehvermögen eingeschränkt ist.

Diese Funktion ist im Standard in den Adobe-Programmen aktiviert und so eingestellt, dass ein Dokument immer komplett verarbeitet wird, bevor die Meldung verschwindet. Das muss nicht sein: Wenn Sie keinen Screenreader verwenden, dann schalten Sie die Inhaltsvorbereitung aus.

Dazu klicken Sie im Reader auf **Einstellungen** > **Barrierefreiheit** und deaktivieren Sie **Unterstützung von Hilfstechnologien aktivieren**.



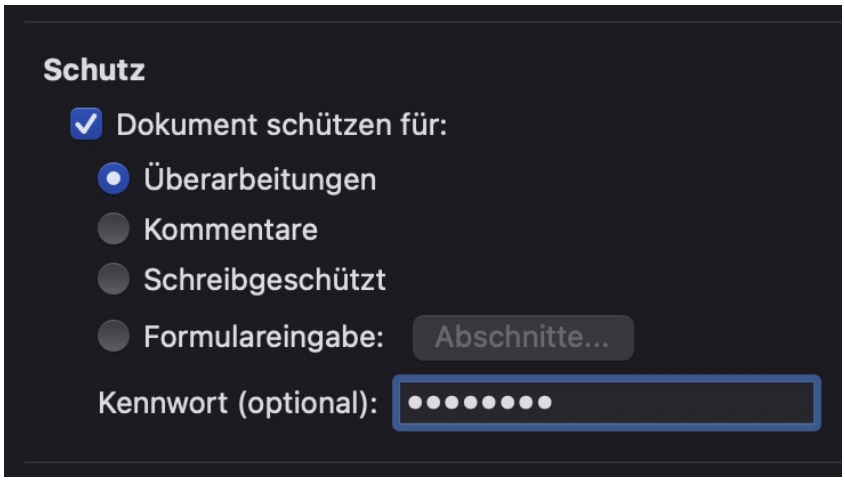
Wenn Sie die Funktion aktiviert halten wollen, aber beschleunigen wollen, dann klicken Sie in den Einstellungen unter **Lesen** > **Optionen für Bildschirmlesehilfe** bei **Seite und Dokument** auf **Nur momentan sichtbare Seiten lesen**. Damit

bereitet der Reader nur eine Seiten, eben die aktuell sichtbare Seite, auf und nicht das ganze Dokument. Das spart eine Menge Zeit.

Zugriff auf passwortgeschützte Word-Dokumente ohne Passwort

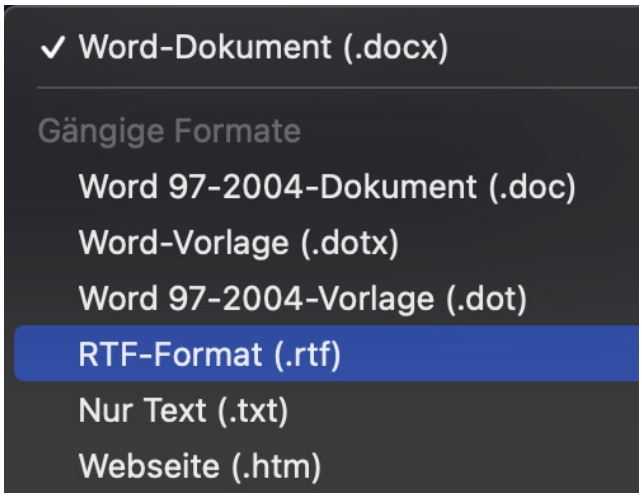
Wenn Sie Word-Dokumente mit einem Passwort schützen, dann ist diese vermeintlich vor unerwünschter Veränderung geschützt. Was aber, wenn Sie das Passwort vergessen? Wir zeigen Ihnen, wie Sie die Änderungen trotzdem vornehmen können!

Um ein Dokument zu schützenn klicken Sie unter Windows auf **Datei** > **Dateiinformationen** > **Dokument schützen**, bei aktuellen Word-Versionen für macOS auf **Überprüfen** > **Dokument schützen**. Wählen Sie dort die Art des Schutzes aus und geben Sie das Passwort ein, mit dem die Datei auf Wunsch freigeschaltet werden muss.



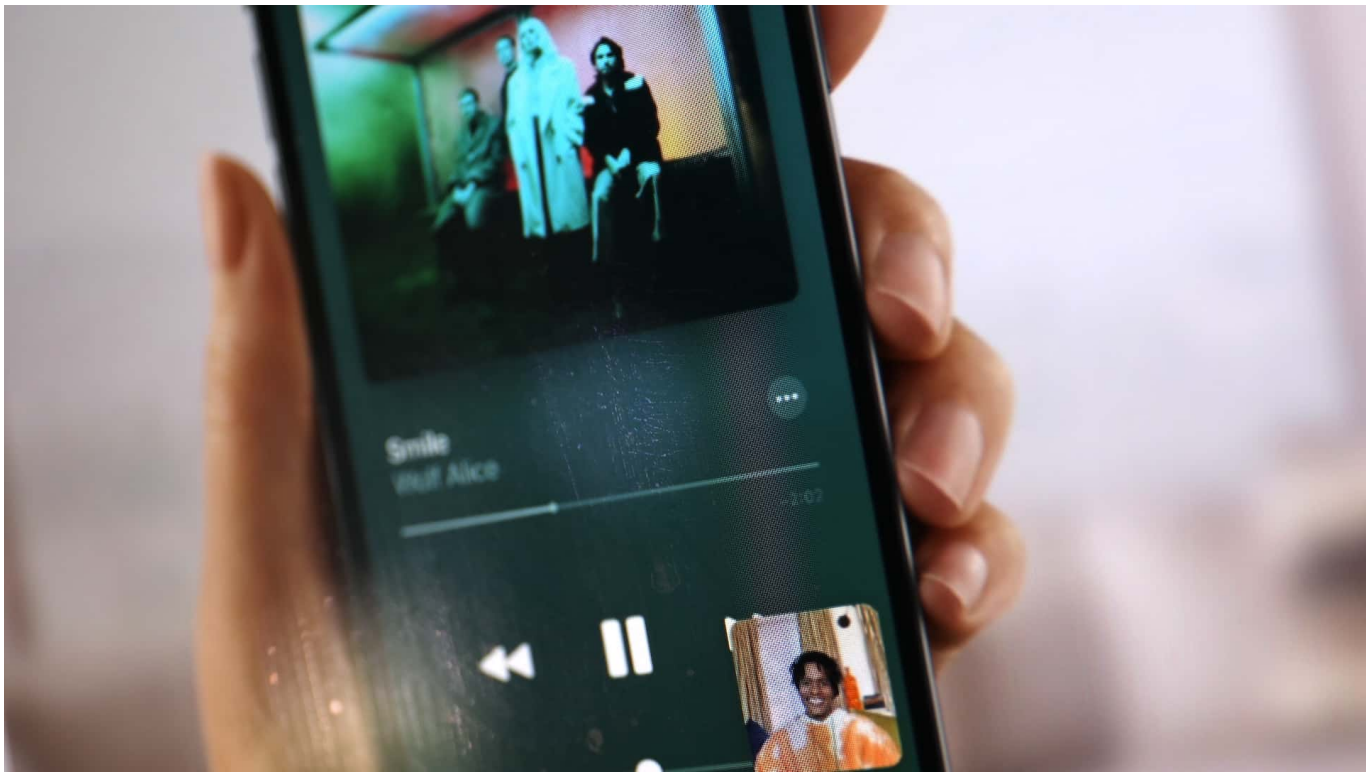
Wenn Sie Änderungen speichern möchten, dann brauchen Sie dieses Passwort. Ist das nicht vorhanden, dann verweigert Word nicht nur das Speichern der Änderungen in der bestehenden Datei, sondern auch das Speichern in eine neue Word-Datei.

Der Ausweg: Speichern Sie die Datei im RTF-Format, indem Sie auf **Datei** > **Speichern unter...** klicken und unter **Dateiformat RTF-Format (.rtf)** auswählen. Da diese Dateien die Word-Schutzfunktionen nicht unterstützen, ist der Schreibschutz automatisch entfernt.



Das RTF-Format heißt nicht umsonst ausgeschrieben "Rich Text Format", denn es ist in der Lage, die meisten Elemente eines Word-Dokumentes darzustellen. Wenn Sie also keine ganz speziellen Funktionen von Word nutzen, sollte die neue Datei dem Original zum Verwechseln ähnlich sein. Auf Wunsch können Sie die RTF-Datei dann natürlich wieder im Word-Format abspeichern.

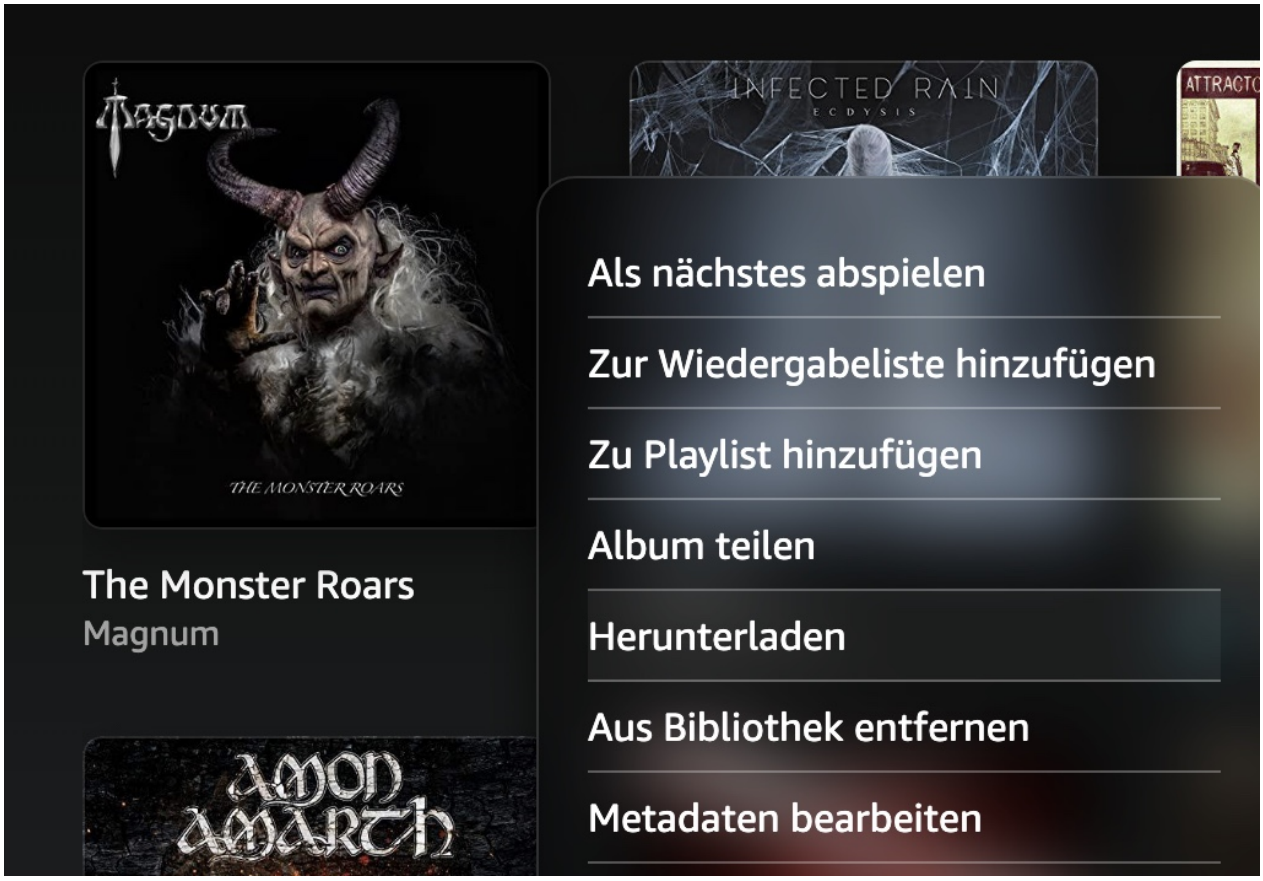
AutoRip und Herunterladen von Musik im Amazon Music



Wenn Sie Amazon Prime-Kunde sind, dann ist darin mit hoher Wahrscheinlichkeit auch der Streaming-Dienst Amazon Music enthalten. Der hat einen versteckten Vorteil: Für die meisten der physischen CDs und Vinyls, die Sie kaufen, können Sie direkt nach Versand die zugehörigen MP3-Dateien herunterladen!

Ein Grund, warum der Umsatz von CDs immer weiter zurückgeht, ist das veränderte Hörverhalten der meisten Käufer: Stationär auf der Couch Musik zu hören ist nur selten möglich dazu sind wir zu viel unterwegs. Musik muss also auch auf mobilen Geräten verfügbar sein. Wer nicht zu Streaminganbietern gewechselt hat oder unterwegs Daten sparen will, der wandelt die Musik manuell von der CD in MP3-Dateien um und kopiert diese auf das mobile Gerät. Dieser Vorgang wird auch rippen genannt.

Den automatisiert Amazon bei vielen Alben automatisch für Sie. Die Alben, bei denen das möglich ist, erkennen Sie schnell: Sie sind mit dem Hinweis **AutoRip** versehen. Die so zur Verfügung gestellten MP3s können Sie über die Amazon Music-App herunterladen.



Klicken Sie darin auf **Bibliothek** > **Alben** > **Sortieren nach: gekauft**. Die App zeigt Ihnen Ihre Alben in chronologischer Reihenfolge an, die neuesten ganz vorne. Wenn Sie den Mauszeiger über ein Cover bewegen, dann erscheinen darin **drei Punkte.** Klicken Sie darauf und dann auf **Herunterladen**. Die App lädt die MP3s nun in das Standard-Musikverzeichnis Ihres Rechners herunter. Von dort aus können Sie sie frei weiterverwenden, ein Kopierschutz wird nicht angewendet!

Amoklauf Heidelberg: Falscher Mann verdächtigt

Kurz nach Bekanntwerden des Amoklaufs vom Montag in Heidelberg wurde ein junger Mann als Täter verdächtigt. Der hatte mit der Sache aber gar nichts zu tun.

Anfang der Woche hatten wir wieder einen folgenreichen Amoklauf in Deutschland. Diesmal an der Uni in Heidelberg. Ein totes Opfer, ein toter Täter. Solche Ereignisse sind immer sehr schnell ein großes Thema. „Eilmeldung!“, steht dann im Handy-Display, weil Journalisten über den Fall berichten.

Man weiß ja nicht, wie sich so ein Amoklauf ausweitet. Aber auch im Netz geht’s dann los: Berichte, Spekulationen – Denunziationen. Schnell werden Personen verdächtigt. Gerne auch schon mal die Falschen... Und das kann im Zeitalter von WhatsApp, Facebook und Twitter schnell Folgen haben...

Das Netz fahndet nach Fakten - und Schuldigen!

Wir wollen nicht über den Amoklauf selbst berichten, sondern was im Netz passiert ist, nachdem die Polizei den Amoklauf gemeldet hat.

Es ist eigentlich immer derselbe Vorgang zu beobachten: Kaum ist die Meldung in der Welt, dass ein Amoklauf in Gang ist, gehen die Menschen ins Netz, um sich zu informieren. Die Radionachrichten kommen bestenfalls zur nächsten halben Stunde wieder – das Internet hat immer auf. Und da kursieren dann auch schon mal gerne Augenzeugenberichte... Was die Menschen aber immer besonders interessiert: Wer ist der Täter? Im Netz kursierte da am Montag relativ schnell ein Verdacht: Tobias L. aus Baden-Württemberg könnte es sein.

Es gab sogar ein Foto als Beweis: Der 25-jährige mit Gewehr auf einem Filmset. „Klar, der war's!“, denkt die Community... Das Handy des Betroffenen stand nicht mehr still. Es gingen unentwegt Nachrichten auf Instagram ein – und der aus verständlichen Gründen völlig verstörte Tobias L., mit der Sache nicht das Geringste zu tun, sah sich in der Situation, sich in einem „Reel“ – einem Video auf Instagram – öffentlich zu erklären, er sei es nicht gewesen und habe damit nichts zu tun. Aber der Mob war kaum noch zu halten.

Wie konnte das passieren?

Schrecklich, sich das vorzustellen: Man wird einfach zum Täter erklärt und im Netz bedrängt. Wie konnte denn das passieren?

Nun, da kommen immer verschiedene Dinge zusammen: Die Dynamik des Internet – und jemand, der entweder verrückt genug ist, einfach so etwas in die Welt zu setzen oder sogar ganz bewusst jemandem schaden möchte. In dem Fall könnten es Ex-Freunde von Tobias gewesen sein, die das wie einen „Streich“ betrachtet haben könnten. Einfach mal behaupten: Die Meute wird sich drauf stürzen. Und so ist es auch gewesen. Die Menschen suchen im Internet nach Fakten, Hintergründen und Erklärungen. Und alles, was da angeboten wird, geht viral.

Egal aus welcher Quelle es kommt. Ein Verdacht ist immer besser als nichts und verbreitet sich explosionsartig im Netz, ohne jede Kontrolle. Eine Polizei würde einen Verdacht prüfen, Journalisten ebenso und nie einen Verdächtigen nennen oder ein Foto zeigen. Im Netz gibt es solche Regeln nicht. Die einen wollen Informationen, die anderen freuen sich über die Aufmerksamkeit. Wer in einer solchen Situation eine Falschnachricht streut, kann sich der Aufmerksamkeit

gewiss sein: So viele Likes und Sternchen gibt es sonst nirgendwo. Auch wenn man anonym bleibt.

Phänomen oder Trend?

Man muss von einem Mechanismus sprechen. Schon Journalisten werden ja gerne und durchaus zu Recht als „Meute“ beschrieben, die sich alle gleichzeitig auf etwas stürzen. Im Netz ist es schlimmer: mehr Menschen, aber gar keine Anstandsregeln. Manche wollen anderen schaden, andere aber auch was Gutes tun: Ich, der Privatdetektiv, kriege doch bestimmt was raus... Und dann wird recherchiert. Online. Sie machen sich keine Gedanken, dass Spekulationen Panik auslösen oder Schaden verursachen können. Man muss aber auch von einem Trend sprechen.

Vor allem in den USA gibt es eine riesige Community, mit Zehntausenden von Menschen, die nicht aufgeklärte echte Verbrechen aufklären wollen. Der „**True Crime**“ Trend – etwa minutiös in Podcast nacherzählte echte Verbrechen – beflügeln diesen Trend. Es gibt sogar ein Portal: websleuths.com. Hier werden Dutzende von Kriminalfällen von Hobby-Sherlock-Holmes debattiert, Mutmaßungen ausgesprochen und Fälle gelöst. Solche Menschen kontaktieren sogar Angehörige von Opfern, obwohl sie das nicht wollen. Es gibt ihnen ein gutes Gefühl, sebst an einer „echten“ Sache dran zu sein, kann aber eine Menge Schaden anrichten.

Wie geht man damit um?

Nun ist es ja eine Sache, in einem Forum mit Gleichgesinnten über Fälle zu sinnieren oder öffentlich in Social Media Spekulationen auszustoßen.

Tobias L. – er ist Autist – war verständlicherweise unglaublich aufgeregt, hat das Video auf Instagram als Statement veröffentlicht und sich bei der Polizei Mannheim gemeldet. Sicher eine gute Idee, damit die Behörde Bescheid weiß. Denn die Polizei mag es gar nicht, wenn Spekulationen öffentlich kursieren. Das bindet Kapazitäten, verunsichert, muss manchmal wieder eingefangen werden. Da wir aber heute alle mehr oder weniger viel von uns in den Sozialen Medien preisgeben, können wir alle zum Opfer werden.

Es ist leichter als früher, etwas über Menschen in Erfahrung zu bringen. Das mag es manchmal leichter machen, den echten Täter zu ermitteln. Auch im

vorliegenden Fall war schnell bekannt, dass der echte Täter die Tat angekündigt hat. Aber es können eben auch Spekulationen sich viral verbreiten. Wir alle sind gut beraten, schnell kursierende Informationen aus dem Netz nicht einfach zu trauen, sondern darauf zu warten, dass sie professionell eingeordnet werden.

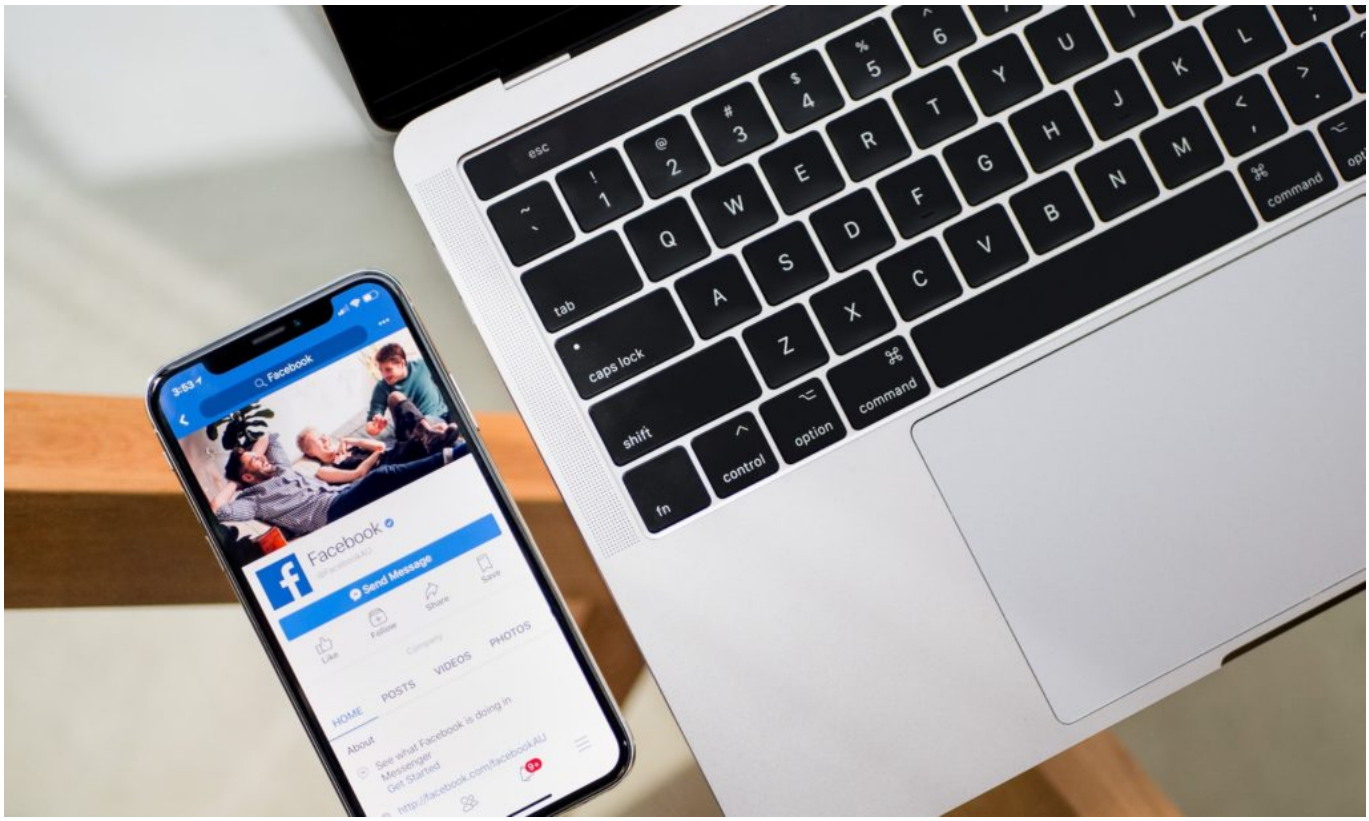
Streit um Klarnamenpflicht: Facebook verliert vor dem BGH

Der Bundesgerichtshof stellt klar: Facebook kann bestimmt User nicht dazu zwingen, Klarnamen zu verwenden. Alle User, die sich vor Mai 2018 beim Netzwerk angemeldet haben, dürfen auch Pseudonyme verwenden. Was das im Alltag bedeutet – nicht nur für Facebook-User.

Facebook schreibt seinen Nutzern in den Allgemeinen Nutzungsbedingungen vor, im Netzwerk einen Klarnamen zu verwenden, den sie „auch im alltäglichen Leben gebrauchen“. Das soll laut Betreiber die „Hemmschwelle für Hassrede und Mobbing erhöhen“ (was durchaus umstritten ist).

Immer wieder halten sich User nicht daran und verwenden Pseudonyme wie „Snoopy123“. Tatsächlich verpflichtet das deutsche Telemediengesetz Anbieter, die Nutzung ihrer Dienste „anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist“.

Trotzdem fordert Facebook Nutzer regelmäßig auf, einen Klarnamen zu verwenden, sollten sie ein Pseudonym im Einsatz haben. Weigern sich die Nutzer, sperrt Facebook die Konten.



„Alte“ Facebook-Konten dürfen Pseudonyme verwenden

Dagegen hatten ein Mann und eine Frau geklagt, deren Konten von Facebook gesperrt wurden. Bis zum Oberlandesgericht hat Facebook Recht bekommen. Doch der Bundesgerichtshof (BGH) hat heute (27.01.2022) entschieden: Dieses Recht auf die Verwendung eines Pseudonyms wirkt schwerer als die Formulierungen in den Nutzungsbedingungen. Facebook muss die gesperrten Konten freigeben und dort Pseudonyme zulassen. Die Kläger haben Recht bekommen.

Allerdings – und das macht die Sache für Konsumenten ein wenig kompliziert – gilt das nur für „Altfälle“ –, für Menschen, die ihre Konten schon vor Mai 2018 bei Facebook eröffnet haben. Denn seit Mai 2018 gilt die europäische Datenschutzgrundverordnung (DSGVO), die kein solches Recht auf Pseudonyme mehr vorsieht. Deshalb kann Facebook Nutzer, deren Konten nach Mai 2018 eröffnet haben, dann zum Verwenden eines Klarnamens verpflichten.

Prinzipiell gilt die Entscheidung auch für andere Netzwerke. Sollte ein Netzwerk die Nutzerinnen und Nutzer in den Geschäftsbedingungen zur Verwendung eines Klarnamens verpflichten – so wie Facebook –, so steht dem rechtlich aktuell nichts entgegen.

Debatte: Klarnamenpflicht oder Recht auf Pseudonyme?

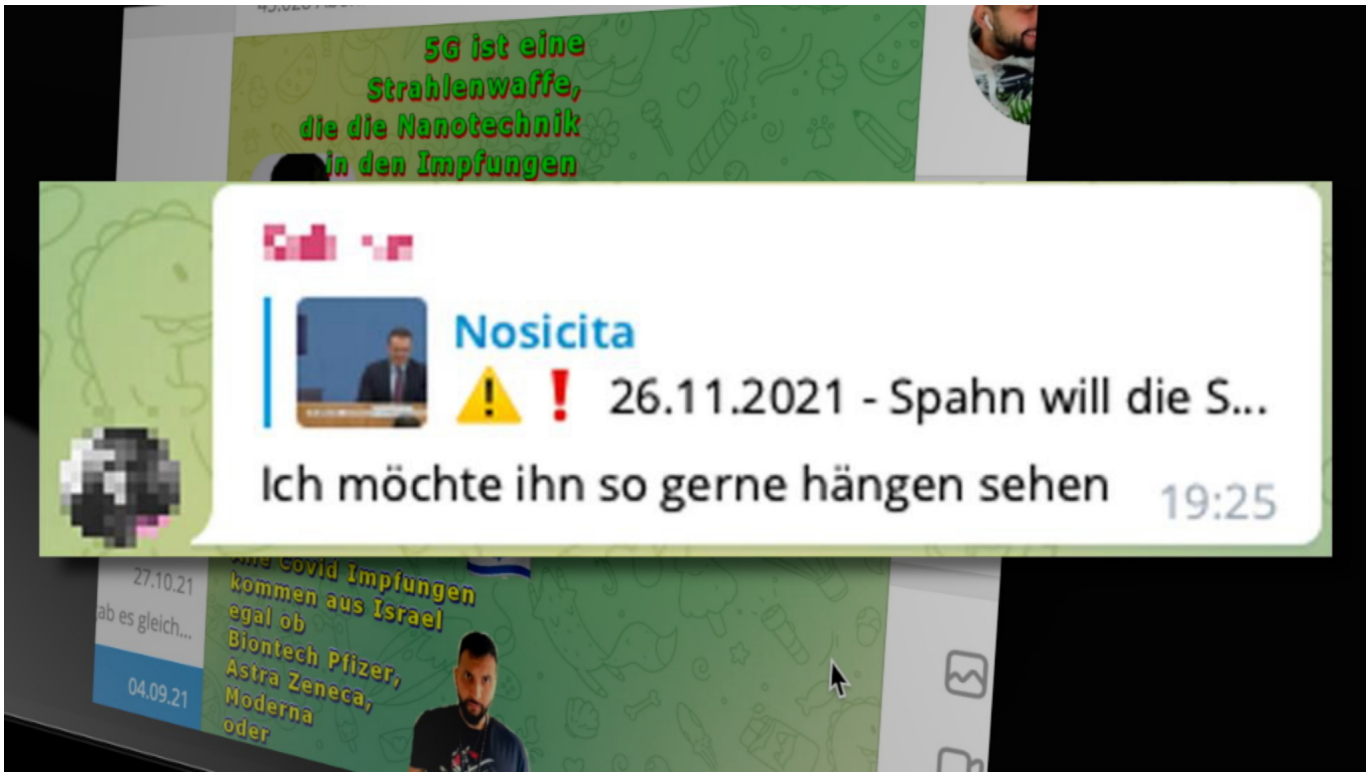
Schon lange gibt es eine Debatte darüber, was besser ist: Pseudonyme ermöglichen es Menschen öffentlich ihre Meinung zu sagen, ohne Belästigungen oder Repressalien befürchten zu müssen. Wenn unter Pseudonym Hass oder Hetze verbreitet werden, erschwere das eine Rechtsverfolgung und/oder senke die Hemmschwelle, sagen andere.

Allerdings gibt es auch eine Studie von der Universität Zürich, die belegt: Anonyme Nutzer kommentieren weniger aggressiv als User, die mit Klarnamen unterwegs sind.

In der Tat scheint Klarnamenpflicht kein Allheilmittel zu sein. In Südkorea wurde die Klarnamenpflicht eingeführt – und nach einigen Jahren auch wieder aufgehoben, da sie nicht den gewünschten und erwarteten Effekt gebracht hat.

Wirkung und Zusammenhang einer Klarnamenpflicht und der Bereitschaft zu aggressivem Verhalten im Netz sind also nicht so offensichtlich, wie es auf den ersten Blick erscheint.

Warum das BKA eine Task-Force für Telegram einrichtet



Das Bundeskriminalamt (BKA) richtet eine Task-Force zur Strafverfolgung von Straftaten auf Telegram ein. Der Messenger entwickle sich nach Einschätzung der Behörden zu einem „Medium der Radikalisierung“.

Bedrohungen, Beleidigungen, Mordaufrufe: Der Messengerdienst Telegram entwickelt sich nach Einschätzung der deutschen Sicherheitsbehörden zunehmend zu einem Medium der Radikalisierung. Das liegt vor allem an der offenen Architektur des Messengers: Hier kann jeder User „Kanäle“ einrichten, denen beliebig viele Menschen folgen können.

Telegram ist ein Massenkommunikationsmittel

An diesem Punkt ist Telegram kein Messenger mehr, sondern ein Massenkommunikationsmittel. Trotzdem rutscht Telegram durchs Raster – und wird durch das Netzwerkdurchsetzungsgesetz (NetzDG), das Hass und Hetze eindämmen soll und Anbieter von Plattformen diverse Pflichten auferlegt, nicht

erfasst. Eine Lücke, die Hassprediger und die einschlägige Szene missbrauchen.

Hinzu kommt, dass die Betreiber des Messengers mit Sitz in Dubai nicht mit den Behörden kooperieren.

Dafür aber den Messenger verantwortlich zu machen, ist falsch. Ebenso falsch ist es, wenn Bundesinnenministerin Nancy Faeser ankündigt, die App aus den App-Stores von Apple und Google werfen zu lassen. Zum einen würde das in der Android-Welt ohnehin wenig bringen (weil sich da – anders als beim iPhone – auch Apps aus anderen Quellen laden und installieren lassen), zum anderen und vor allem aber würde auch die Mehrheit der User bestraft, die Telegram einfach nur als Messenger benutzen. Abgesehen davon würden jene User, die man behindern möchte, schnell ein anderes Vehikel finden. Das Problem wäre also nicht wirklich aus der Welt.

User „Kanäle“ einrichten, denen beliebig viele Menschen folgen können.

Straftaten gezielt verfolgen

Deshalb ist die aktuelle Ankündigung (26.01.2022), nun im Bundeskriminalamt (BKA) eine eigene Task-Force einzurichten, der einzig richtige Weg. Denn Straftaten bleiben auch im Netz Straftaten – und müssen unbedingt zeitnah und konsequent strafrechtlich verfolgt werden. Anderenfalls werden es nicht nur immer mehr Straftaten im Netz, sondern auch immer aggressivere.

"Insbesondere die Corona-Pandemie hat dazu beigetragen, dass sich Menschen auf Telegram radikalisieren, andere bedrohen oder sogar Mordaufrufe veröffentlichen" sagt BKA-Präsident Holger Münch. "Der Rechtsstaat muss dieser besorgniserregenden Entwicklung entschlossen begegnen. Wir streben die Zusammenarbeit mit Telegram an, treffen unsere Maßnahmen aber auch, wenn Telegram nicht kooperieren sollte."

Cyberkriminologe rät: generell mehr Polizeipräsenz im Netz

Natürlich muss streng unterschieden werden zwischen den öffentlich zugänglichen Bereichen und privaten Bereichen. Aber ein öffentlicher Raum bleibt

ein öffentlicher Raum, auch wenn er online existiert.

Mehr Polizeipräsenz im Netz: Das fordert schon lange auch der Cyberkriminologe Dr. Thomas Rüdiger aus Brandenburg. „Menschen, die Normen verletzen, wägen nach der Routine-Activity-Theorie ab: Was bringt mir der Regelverstoß und welche Risiken drohen mir?“ Schließlich bekommt auch nicht jeder gleich einen Strafzettel, der bei Rot über die Ampel geht. Aber es gibt eben eine gewisse Wahrscheinlichkeit, dass ein Rotlichtverstoß im Auto verfolgt wird.

Diese Wahrscheinlichkeit gibt es im Netz bislang nicht. Im Gegenteil. Das Vakuum, dass Staat und Behörden hier bislang hinterlassen, ist eine regelrechte Einladung. Da das Strafverfolgungsrisiko online bei den meisten Delikten im Netz massiv niedriger ist als bei vergleichbaren analogen Delikten, von Hetze bis zur Androhung sexueller Gewalt.

Ein Besuch bei Europas schnellstem Quantencomputer – in Jülich

Im Forschungszentrum Jülich steht der leistungsfähigste und schnellste Quantencomputer Europas. Er kann komplexe Rechenaufgaben in kürzester Zeit lösen – und hebt die Forschung auf ein neues Level. Ich war neugierig - und habe mir den Quantencomputer angeschaut.

Einer der schnellsten Quantencomputer der Welt steht jetzt im Forschungszentrum Jülich. Als ich davon erfahren habe, gab es für mich nur einen Impuls: „Den musst Du Dir anschauen“.

Denn so ein Quantencomputer ist ein wahres Wunderwerk der Ingenieurskunst. Wer sich mit den technischen Konzepten hinter so einem Quantencomputer beschäftigt, kann nur staunen, was heute alles möglich ist. Quantencomputer funktionieren aber nicht nur in punkto Hardware ganz anders als "klassische" Computer, sondern auch in der Art und Weise, wie man sie nutzt. Zumindest die Art von Quantencomputer, die in Jülich steht.

Technisch extrem aufwändig, so etwas aufzubauen und zu realisieren: Das Innenleben muss auf den absoluten Nullpunkt (-273 Grad Celsius) heruntergekühlt werden. Anders als bei anderen Computern aber nicht, weil sich

die Anlage beim Rechnen erhitzt, sondern weil die Atome im Inneren des Kerns zum Stillstand kommen müssen. Denn es sind die Atome, die beim Rechnen helfen.

Sensibel: Erschütterungsfreier Untergrund erforderlich

In Jülich haben sie ein eigenes Gebäude dafür gebaut. Denn das Fundament muss solide sein: Jede noch so geringe Erschütterung führt unweigerlich zu Rechenfehlern. Deshalb muss die Millionen Euro teure Anlage auf erschütterungsfreiem Grund stehen. Doch wen man drin ist in dem Raum, in dem die Anlage steht, hört man nur ein dröhnendes Rauschen – viel mehr nicht. Weniger laut als ein übliches Rechenzentrum – und nichts deutet darauf hin, dass diese Maschine millionenfach schneller rechnet als andere Computer.

Die Physikerin Prof. Kristel Michielsen hat mir die Anlage gezeigt. Sie leitet das Projekt und ist sichtlich stolz auf die Neuanschaffung. Als ich sie frage, ob der „Juniq“ – so heißt die Anlage in Jülich – mich in „Tic Tac Toe“ schlagen kann, lacht sie nur laut und sagt: „Diese Maschine spielt kein Tic Tac Toe“. Nicht nur, weil der Quantencomputer in Jülich dafür viel zu teuer ist, sondern auch, weil die Maschine für ganz andere Aufgaben entwickelt wurde.

Es gibt bislang nur zwei Anlagen dieser Art vom kanadischen Hersteller D-Wave. Der Quantencomputer in Jülich ist einer der schnellsten seiner Art. Er kann vor allem Optimierungsaufgaben lösen: Fahrtpläne der Bahn optimieren, ökonomische Prozesse durchspielen, Klimamodelle kalkulieren oder die Wirkung pharmazeutischer Wirkstoffe simulieren. Und das so schnell, dass jeder Supercomputer alt aussieht.

So ein Quantencomputer – man verzeihe mir das unvermeidliche Wortspiel – ist ein Quantensprung in der Computerei. Quantencomputer heben die Möglichkeiten, etwa bei der Künstlichen Intelligenz (KI), auf ein völlig neues Level.

Qubits statt Bits

Denn Quantencomputer arbeiten völlig anders als herkömmliche Computer, wie wir sie bislang kennen. Quantencomputer arbeiten so extrem schnell, weil sie

Tausende Aufgaben gleichzeitig bearbeiten können. Wenn sich zum Beispiel 100 Lösungen für ein Problem anbieten, kann ein Quantencomputer sie alle gleichzeitig durchspielen und findet so viel schneller die beste Lösung.

Quantencomputer verwenden Bits und kennen nur 1 und 0. Strom an oder Strom aus. Quantencomputer hingegen arbeiten mit Quanten-Bits, kurz Qubits. So ein Qubit kann 1 oder 0, aber auch 1 und 0 gleichzeitig oder alles dazwischen sein. Also 80% ja und 20% nein, zum Beispiel. Ein völliges neues Prinzip. Mit 5000 Qubits ist der Juniq in Jülich üppig ausgerüstet.

Er hat seine Arbeit aufgenommen und wird für Forschungszwecke, aber auch für andere Aufgaben eingesetzt. Wer mit Juniq Probleme beackern möchte, muss erst mal einen Antrag stellen: Eine Kommission entscheidet, ob die Maschine dafür hergegeben wird – und ob es überhaupt eine Aufgabe ist, für die Juniq geeignet ist.

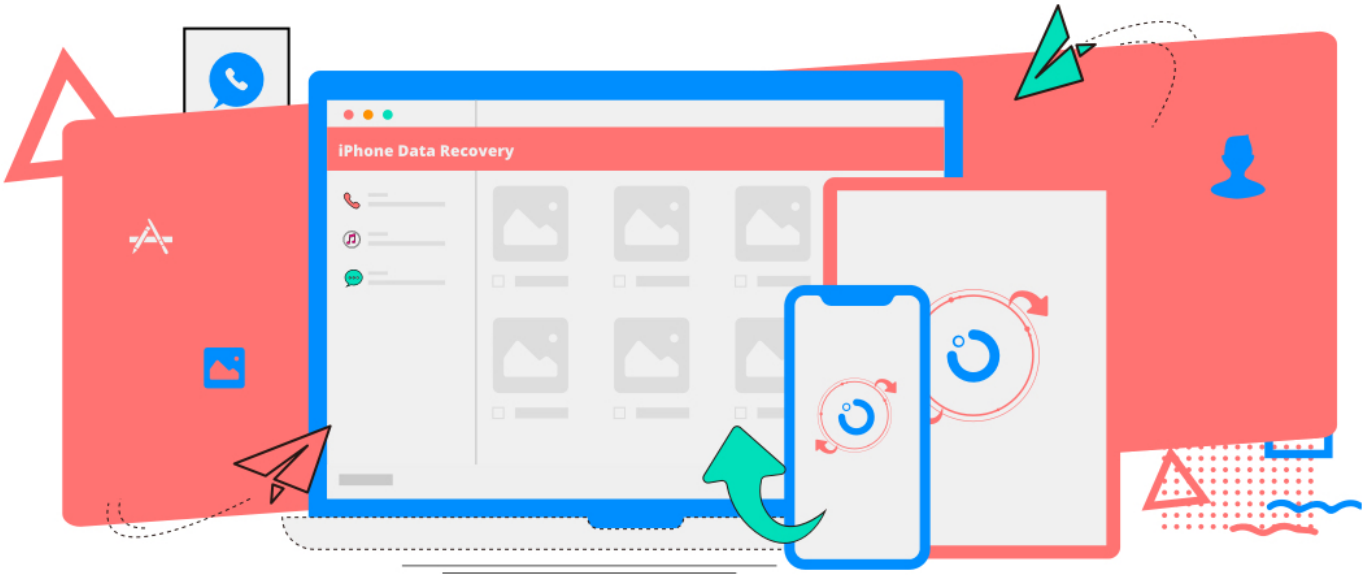
„Juniq“ erwartet eine spezielle Programmierung

Wer selbst über Programmierkenntnisse verfügt, etwa Basic, Pascal, C++ oder PHP beherrscht, darf sich bei Juniq keine Hoffnung darauf machen, von Juniq verstanden zu werden. So ein Quantencomputer wird aufgrund seiner Beschaffenheit völlig anders programmiert. Probleme müssen in mathematische Aufgaben runtergebrochen werden. Es ist eine völlig andere Herangehensweise erforderlich. Aber wer das beherrscht – wie das Team in Jülich –, darf mit deutlich schnelleren Ergebnissen rechnen.

So ein Quantencomputer stellt potenziell aber durchaus auch eine Bedrohung dar. Beispiel: Verschlüsselung wie wir sie heute kennen, um unsere Chats, Dokumente oder Kommunikation abzusichern, ließe sich in einem Quantencomputer knacken. Da wo Supercomputer Monate bräuchten, hätte ein Quantencomputer in Sekunden das Ergebnis. Neue Möglichkeiten bedeuten auch neue Herausforderungen. Verschlüsselung muss in Zukunft zum Beispiel anders aussehen, wenn sie wirklich sicher sein soll.

All das macht eins klar: In Jülich ist ein neues Zeitalter angebrochen – und es ist gut, dass wir in Deutschland Erfahrungen und Erkenntnisse sammeln können.

So gelingt Datenrettung auf dem iPhone



Zack - da ist es passiert: Aus Versehen ein Foto, eine Notiz, einen Kontakt oder etwas anderes ganz wichtiges auf dem Apple iPhone gelöscht. Mit einer speziellen Software lassen sich die Daten meist erfolgreich zurückholen.

Es passiert jedem irgendwann einmal, dass wichtige Dokumente, Bilder, Termine oder was auch immer verloren gehen. Etwa durch einen dummen Zufall, eine Fehlbedienung - oder durch versehentliches Zurücksetzen auf die Werkseinstellungen. Denkt man darüber nach, gibt es eine ganze Reihe von möglichen Gründen, warum man nicht mehr auf Daten auf dem iPhone zugreifen kann:

- Versehentlich gelöscht
- Auf Werkseinstellungen zurückgesetzt
- Systemprobleme
- Code vergessen
- Gestohlenes iPhone
- Wasserschaden
- Display defekt
- Jailbreak

Gut: Hat man ein Foto bewusst gelöscht, steht es noch eine Weile im Ordner "Kürzlich gelöscht" zur Verfügung. Aber in allen anderen Fällen hat man ein Problem.

Das Tool kann Daten sogar aus der iCloud retten

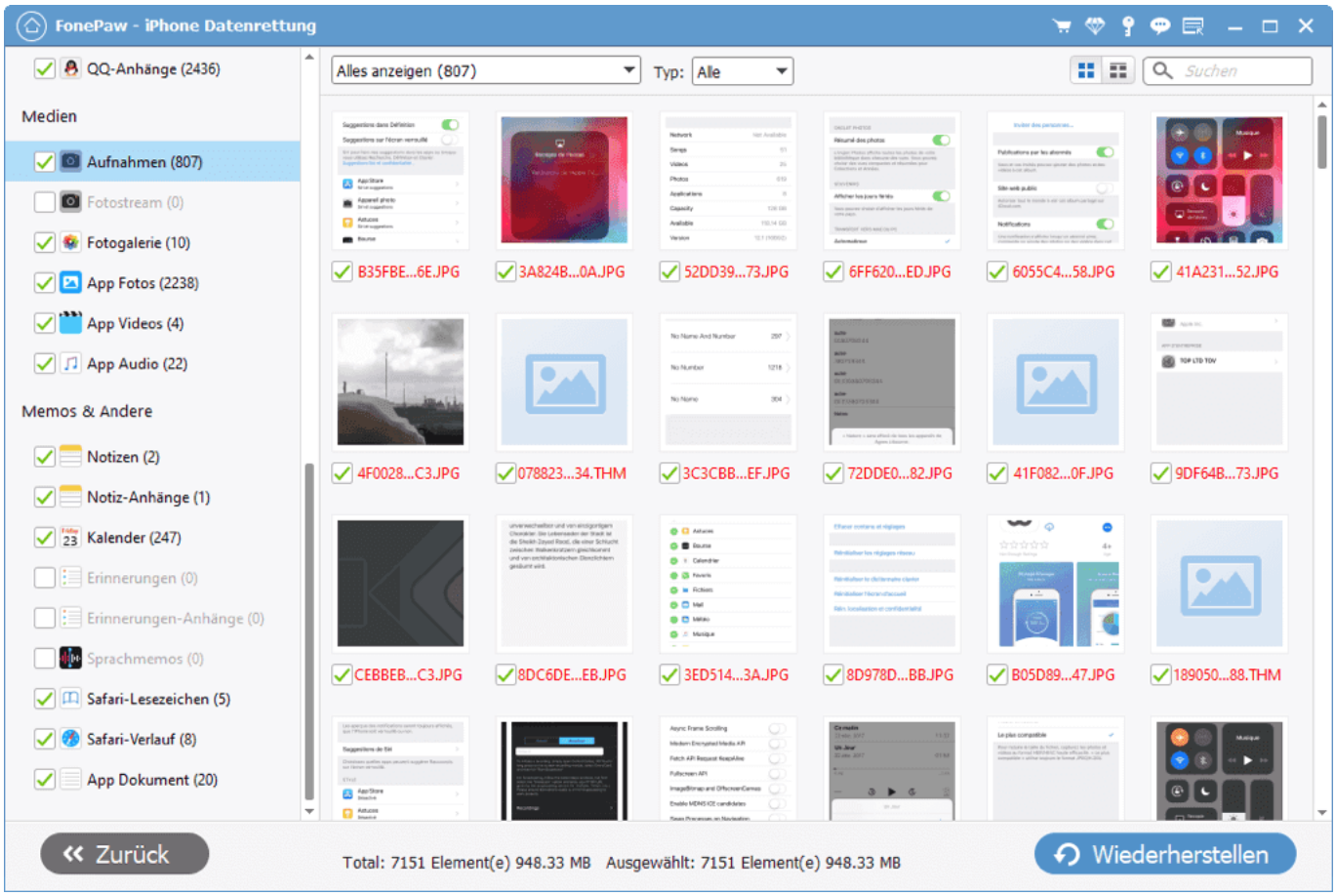
Was also tun? Wer regelmäßig Backups anfertigt, etwa mit Hilfe von iTunes oder iCloud, kann natürlich den zuletzt gesicherten Zustand wieder auf dem iPhone installieren. Das ist allerdings mühsam.

Viel praktischer sind in solchen Momenten, sich auf die Hilfe einer Spezial-Software zu verlassen. Für das iPhone habe ich eine Software entdeckt, die wirklich nützlich sein kann: Die iPhone Datenrettung von Fonepaw. Es gibt die Software für Windows und Mac. Mit der kostenlosen Version sind die Möglichkeiten zur Rekonstruktion eingeschränkt, aber wenn es sich um wirklich wichtige und/oder viele Daten handelt, die gerettet werden müssen, lohnt sich möglicherweise die Investition in die Kaufversion (ab 54 EUR).

Wie kann die Software helfen? Ganz einfach: Es gibt drei mögliche Wege, wie sich verloren gegangene Daten wiederherstellen lassen.

1. Vom Gerätespeicher wiederherstellen
2. Aus iTunes Backup zurückholen
3. Aus iCloud wiederherstellen

Besonders praktisch finde ich Möglichkeit (3). Denn das iCloud-Backup ist bequem - einmal eingeschaltet, läuft es mehr oder weniger automatisch. Deswegen haben die meisten iPhone-Nutzer ein iCloud-Backup. Ein Backup mit iTunes, das machen die meisten dann doch eher selten, weil es mit einem gewissen Aufwand verbunden ist. Vorteil hier: Die Daten liegen nicht in der Cloud, sondern auf der eigenen Festplatte.



Über 30 Dateitypen lassen sich retten

Die Datenrettung von Fonepaw bietet die Möglichkeit, aus allen drei möglichen Quellen versehentlich gelöscht oder verloren gegangene Dateien oder Informationen wiederherzustellen. Am bequemsten ist wie gesagt die Möglichkeit, aus dem iCloud-Backup zu rekonstruieren. Dazu einfach mit der iCloud verbinden, das Backup scannen lassen (das kann je nach Umfang durchaus 20 Minuten dauern) - und anschließend die Fotos, Dokumente oder Dateien markieren, die rekonstruiert werden sollen.

Das ist wirklich extrem bequem!

Über 30 Datentypen können mithilfe der iPhone Datenretung auf diese Weise wiederhergestellt werden auf dem iPhone, iPad und iPod Touch. Alle Dateien lassen sich problemlos aus iTunes- oder iCloud-Backup zurückholen. Egal, ob eine SMS gelöscht, eine WhatsApp-Gruppe entferne, ein Kalendereintrag gelöscht oder eine wichtige Fotoaufnahme oder Notiz gelöscht wurde: Die Software kann helfen.

Wichtig: Schnell reagieren

Ganz wichtig ist in solchen Situationen aber: Hat man bemerkt, dass wichtige Dateien oder Dokumente verloren gegangen sind, sollte auf dem Gerät nichts mehr gespeichert werden. Am besten sofort alle anderen Arbeiten beenden, damit keine Daten mehr gespeichert werden - das bedeutet nämlich ein Risiko, dass die verloren gegangen Daten überschrieben werden. Anschließend sofort das Rettungs-Tools aufrufen und starten und die Rettungsaktion starten!

Sicherheitspakete boomen: Was bringt Surfshark One?

Für Cyberkriminelle ist eine einfache Rechnung: Je mehr Menschen online sind und je mehr Zeit sie dort verbringen, desto mehr Gelegenheiten ergeben sich, User zu Opfern zu machen. Die Angriffsmethoden und Tricks nehmen zu - und deshalb müssen User auch immer aufmerksamer werden.

Ganz prinzipiell bin ich kein Freund davon, jedes Problem mit zusätzlicher Software zu lösen. Denn je mehr Software man installiert hat, desto mehr Programme muss man einrichten, pflegen und auch auf dem neuesten Stand halten.

Wenn es um die eigene Sicherheit geht, kommt man heute aber beinahe nicht umhin, sich mit Schutz-Software einzudecken. Sei es, um Viren und Würmer abzuwehren (vor allem auf Windows-Rechnern), Angriffsmethoden zu erkennen und zu blockieren, sich vor Schnüffelangriffen zu schützen und vieles anderes mehr.

Programmpakete (Suiten) bieten Vorteile

Aber auch die Werbeindustrie wird immer aggressiver. Deshalb wollen sich viele Menschen auch davor schützen, etwa indem sie ihre Identität verschleiern - oder

wenigstens ihre IP-Adresse, um nicht so leicht getrackt und damit eindeutig identifiziert werden zu können.

Für jede einzelne dieser Herausforderungen gibt es spezielle Software. Kostenlose Programme - aber natürlich auch kostenpflichtige Programme. Wenn man sich dazu entschließt, sich mit Software gegen all diese akuten Bedrohungen zu wehren, empfehle ich eine Suite zu installieren. Also ein Programmpaket, das alle wesentlichen Bereiche abdeckt. Denn zumindest weniger erfahrene Benutzer haben es dadurch einfacher: Alles an einer zentralen Stelle einrichten, konfigurieren und überwachen.

Praktisch alle großen Anbieter haben heute solche "Suiten" im Angebot. Diesmal habe ich mir Surfshark One angeschaut. Ein Programmpaket, bestehend aus Antiviren-Schutz, VPN, Alert und sichere Suchfunktion.

[av_button label='Mehr Infos über Surfshark One' link='manually,https://get.surfshark.net/aff_c?offer_id=87&aff_id=8832&url_id=1080' link_target='' size='large' position='center' label_display='' icon_select='yes' icon_hover='aviaTBicon_hover' icon='ue83f' font='entypo-fontello' color='theme-color' custom_bg='#444444' custom_font='#ffffff' av_uid='av-1ac3u9c' admin_preview_bg='']

Wichtigstes Werkzeug: VPN

Surfshark One enthält im Wesentlichen vier Pakete: VPN, Antivirus, Search und Alert.

Ein Virtual Private Network (VPN) kann für jeden sinnvoll sein. Denn in einem VPN wird auf Knopfdruck ein sogenannter Datentunnel eröffnet - und über diesen Datentunnel findet die komplette Kommunikation im Web und generell statt. Alles

ausnahmslos verschlüsselt, so dass selbst in einem offenen WLAN niemand irgendetwas abgreifen kann. In einem VPN zu surfen, zu chatten oder E-Mails auszutauschen ist generell sicherer. Erreicht wird das, indem jede Form von Kommunikation über eine Zwischenstelle läuft, die für die Verschlüsselung sorgt.

Doch ein VPN bietet noch mehr Vorteile. Nutzer können damit ihre Identität verschleiern, denn Aufenthaltsort und eigene IP werden dadurch für Anbieter im Netz unsichtbar (stattdessen erscheint die IP-Adresse der Zwischenstelle). Das braucht man keineswegs immer. Aber wer zum Beispiel sensible Themen recherchiert, sich in Foren politisch äußern möchte oder andere gute Gründe für eine Verschleierung der eigenen IP-Adresse hat, kann das mithilfe von Surfshark und anderen VPN-Anbietern sehr einfach. Im wahrsten Sinne des Wortes auf Knopfdruck.

Weiterer Aspekt: In einem VPN-Netzwerk kann man sogar seinen Aufenthaltsort verschleiern. Das kann sinnvoll sein, wenn man auf Inhalte zugreifen möchte, die nur für Menschen in einem bestimmten Land beschränkt sind. Eine Netflix-Folge aus den USA sehen? Mit einem VPN in der Regel kein Problem. Einfach im VPN einen Netzwerkknoten in den USA auswählen - fertig. Schon befindet Ihr Euch für die Anbieter im Netz in den USA.

Last not least lassen sich in einem VPN aber auch die Begehrlichkeiten von Werbetreibern einschränken: Sie bekommen weniger persönliche Daten von Euch - und können so auch weniger präzise Profile anfertigen.

Antivirus: Schutz vor Viren und Würmern

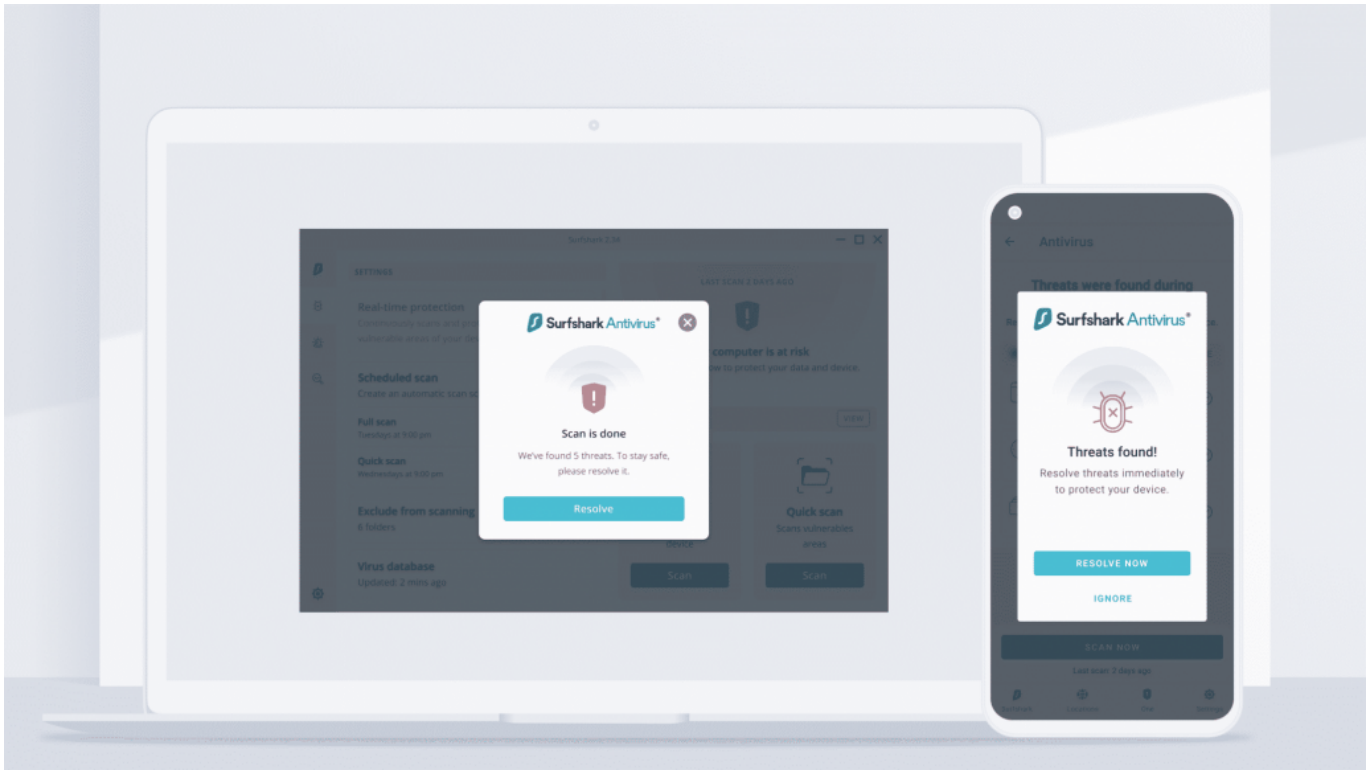
Bloß weil heutzutage seltener über Viren und Würmer berichtet wird, bedeutet leider nicht, dass es sie nicht mehr gäbe. Windows-Benutzer sind nach wie vor stärker betroffen. Aber auch die Mac-Welt ist mittlerweile häufiger Ziel von Viren und Würmern. Früher haben sich Apple-Geräte weniger für Angriffe geeignet, weil es zu wenige Nutzer gibt. Das ist längst nicht mehr der Fall. Deswegen entwickeln Cyberangreifer auch mehr Viren und Würmer für Apple-Systeme. Die Gefahr ist zwar nach wie vor vergleichsweise gering, aber sie ist leider nicht null.

Mit einem Virenschutz erfährt man wenigstens, wenn man sich einen Virus oder Wurm eingefangen hat - und kann dann Maßnahmen ergreifen, die Schädling auch wieder loszuwerden. Ein Virenschutz wie der von Surfshark bietet aber natürlich auch aktiven Schutz an. Auf Wunsch lässt sich der gesamte Rechner überwachen - oder Ihr führt gezielte Scans von Festplatten oder auch nur ausgewählten Ordnern durch. Auf diese Weise erfahrt Ihr, ob es bereits infizierte Dokumente oder Dateien gibt.

Natürlich werden auf Wunsch auch Downloads auf mögliche Infektionen hin untersucht. Das ist besonders wichtig.

Kurz: Surfshark Antivirus ist ein Antivirus-Tool für Windows- und Android-

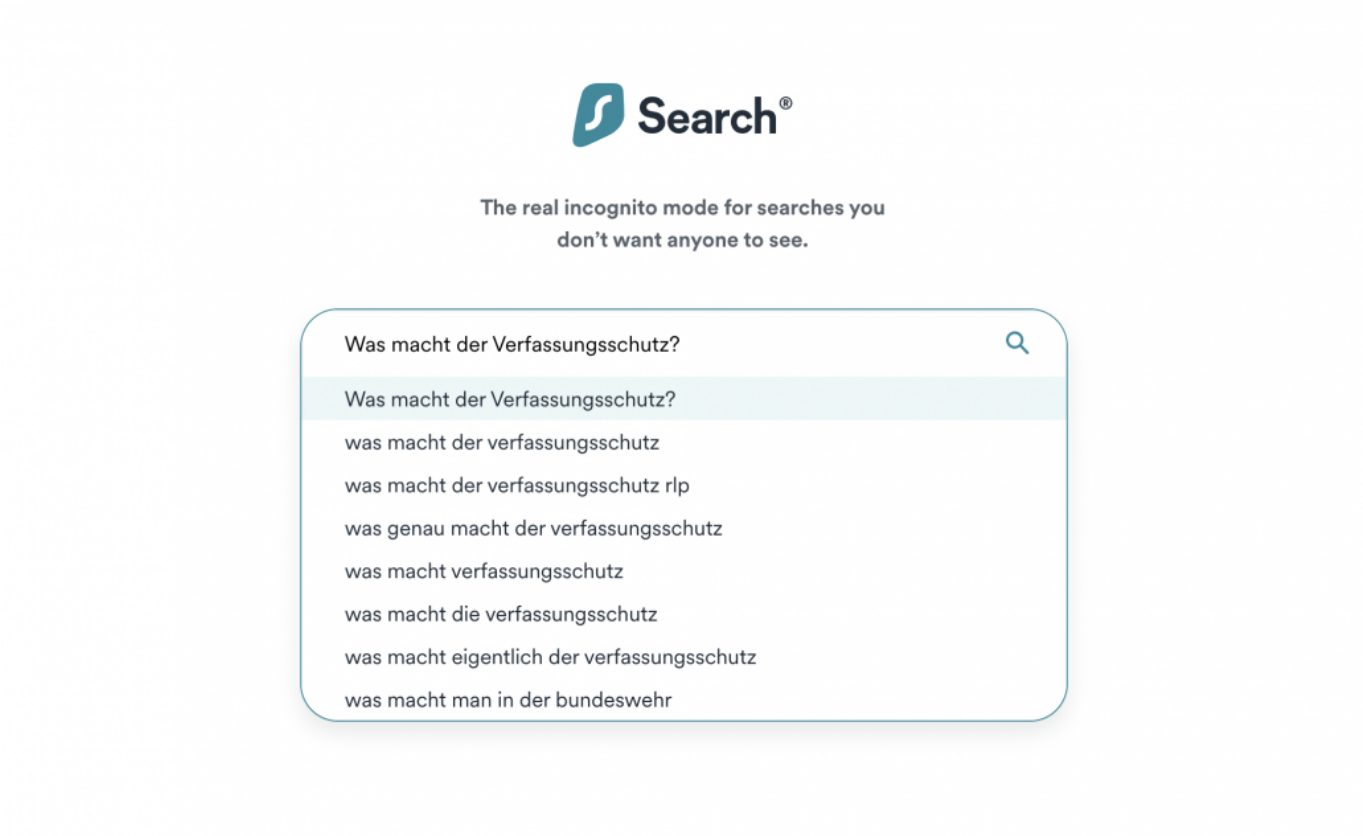
Plattformen (erst demnächst auch für MacOS), das Geräte vor Malware, Viren und in die Privatsphäre eingreifende Apps schützt. Die App schützt also auch vor Apps, die ohne Erlaubnis auf Daten zugreift. Surfshark Antivirus arbeitet in Echtzeit, bemerkt unzulässige Zugriffe also, während sie passieren. Die Geräte sind so immer geschützt.



Search und Alert

Wie Ihr vermutlich wisst, gebt Ihr bei jeder Suchanfrage auf Google, Bing oder andere führenden Suchdiensten private Daten an die Suchdienste weiter. Es erscheinen personalisierte Anzeigen. Die können praktisch sein, etwa man nach Angeboten oder Produkten sucht. Es gibt aber auch Situationen, da möchte man anonym surfen und keine privaten Daten weitergeben. Wann und wie oft das der Fall ist, hängt natürlich von den individuellen Nutzungsgewohnheiten und Empfindungen ab.

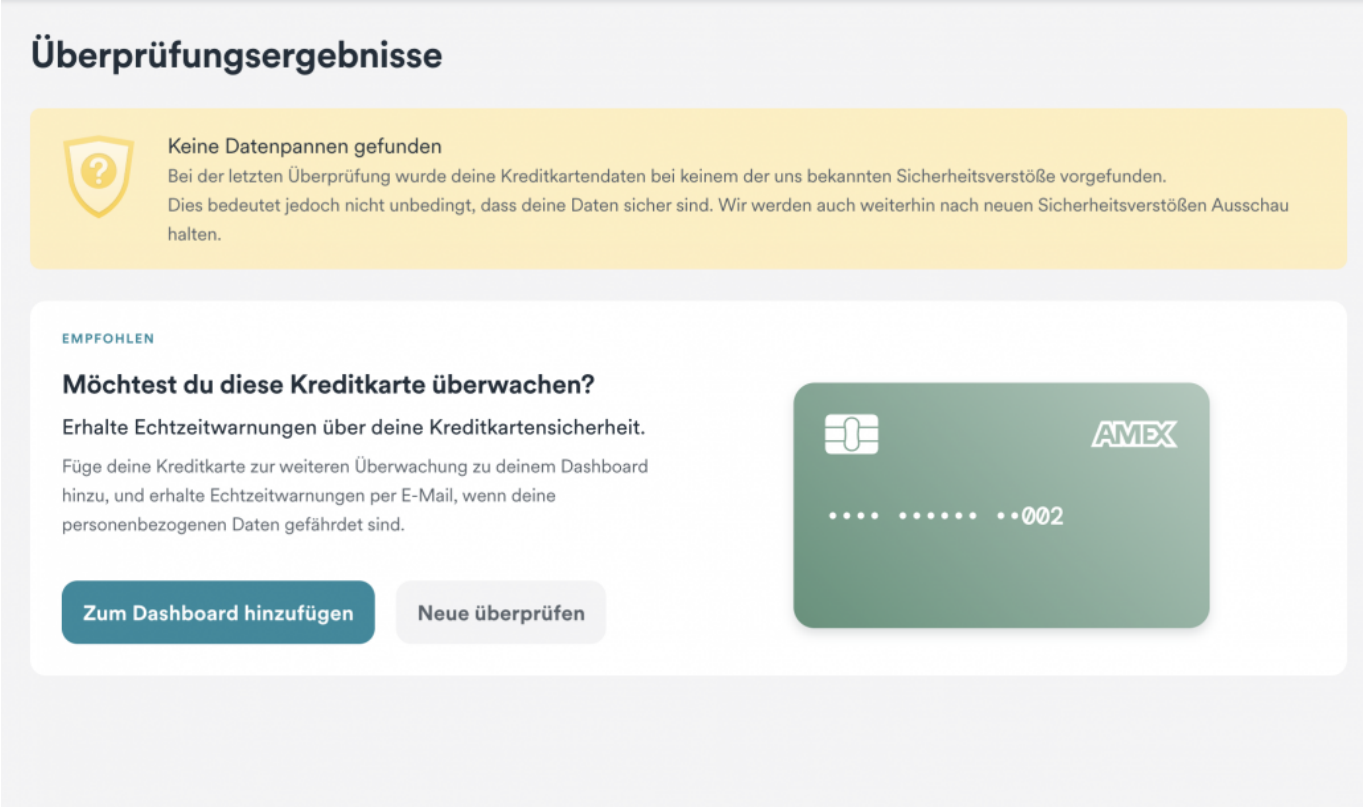
Surfshark One bietet einen völlig anonymen Suchdienst: Wollte Ihr anonym suchen, ruft Ihr aus dem Surfshark-Konto die Suchfunktion auf - und könnt dort wie gewohnt die Suchanfrage eingeben. Dabei werden keinerlei private Daten erfasst oder weitergegeben. Die Ergebnisse erscheinen ohne Online-Ads oder personalisierte Ergebnisse. Ganz schlicht.



Last not least gibt es noch eine Alert-Funktion. Hier könnt Ihr Euch darüber informieren, ob im Darknet Zugangsdaten von Euch auftauchen. Das ist in Surfshark etwas unglücklich übersetzt mit "Datenschutzverstößen" oder "Datenpannen". In Wirklichkeit geht es um entwendete persönliche Daten. Wenn Hacker sich zum Beispiel in einen Server hacken und dort Hunderttausende persönliche Daten stehlen, landen die in der Regel früher oder später im Darknet. So etwas wird heute von Spezialiseren überwacht. Mithilfe von Surfshark könnt Ihr "nachschauen", ob es schon Datenleaks gegeben hat, die auch Euch betreffen.

Surfshark informiert ausführlich, was entdeckt wurde - und auch, welche Daten dabei erbeutet wurden. Das ist wichtig zu wissen, um ggf. sofort die Passwörter der betreffenden Konten zu ändern und/oder andere Sicherheitsmaßnahmen zu ergreifen (etwa: Zwei-Faktor-Authentifizierung aktivieren).

Auf Wunsch durchsucht Surfshark diese Datenbanken auch nach Eurer Kreditkarte: Wurde die Kreditkartennummer schon mal irgendwo "abgegriffen" oder erbeutet?



Nützliche Hilfen auf Desktop und Mobilgeräten

Wer Surfshark One abonniert (derzeit gibt es ein preislich sehr günstiges Angebot für die ersten 12 Monate), kann mehrere Geräte schützen und mit VPN und anderen Schutzmechanismen ausrüsten. Wichtig: VPN und Viren-Scan funktionieren auch auf Mobilgeräten. Vor allem auf Android-Geräten sollte man darauf nicht verzichten, denn anders als iPhones sind Android-Geräte durchaus gefährdet.

[av_button label='Mehr Infos über Surfshark One' link='manually,https://get.surfshark.net/aff_c?offer_id=87&aff_id=8832&url_id=1080' link_target='' size='large' position='center' label_display='' icon_select='yes' icon_hover='aviaTBicon_hover' icon='ue83f' font='entypo-fontello' color='theme-color' custom_bg='#444444' custom_font='#ffffff' av_uid='av-8rbv8kw' admin_preview_bg='']