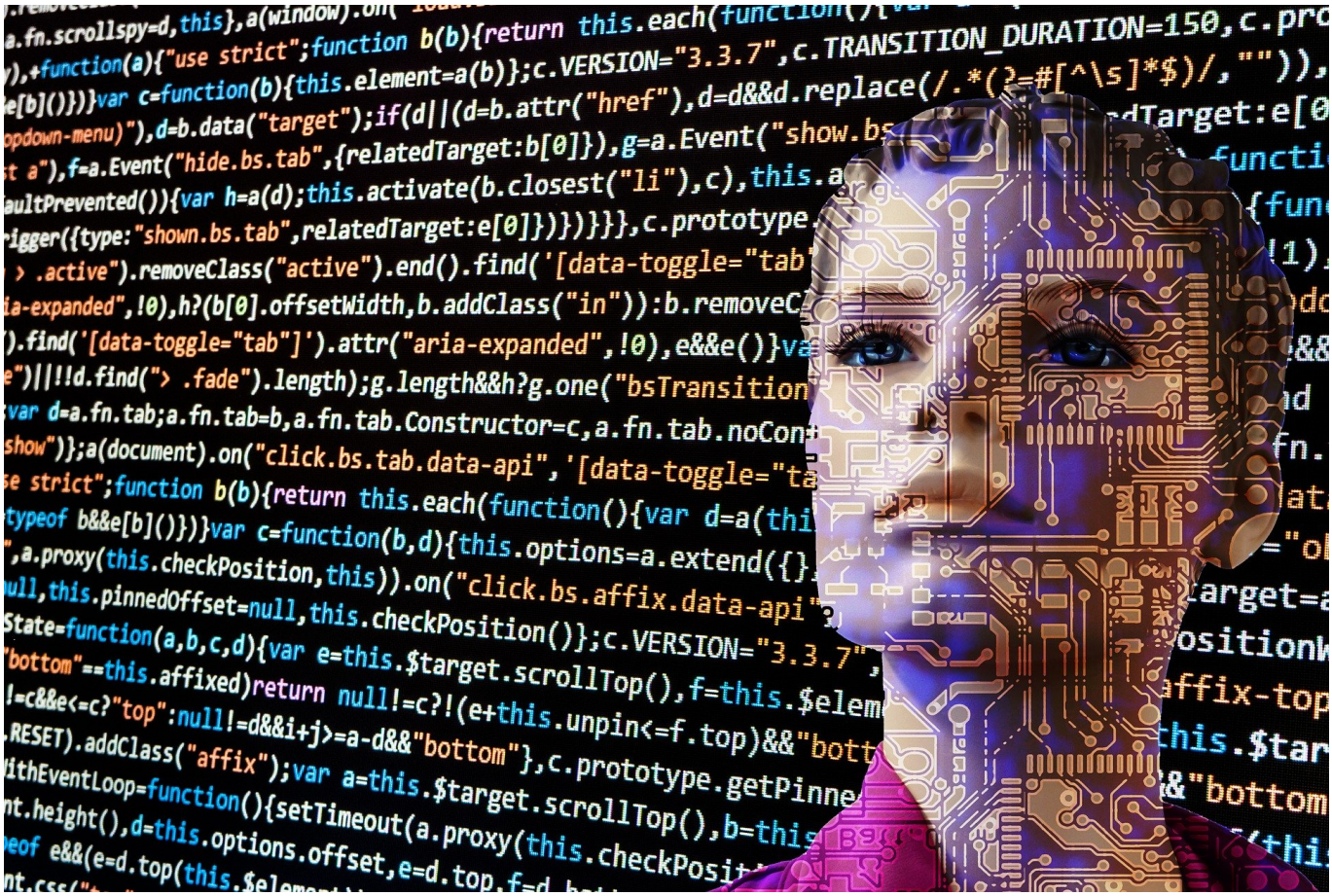
Schieb Report

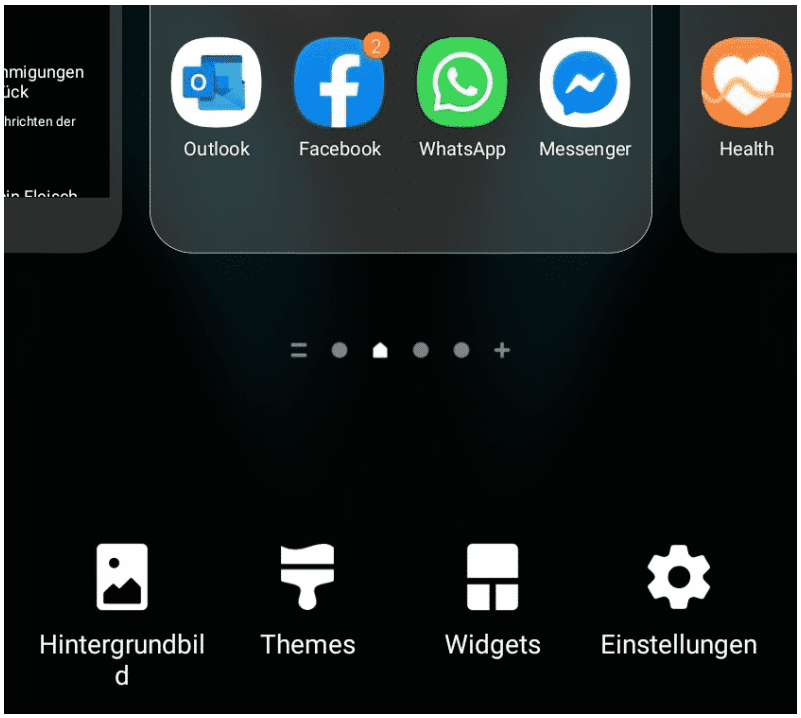
Ausgabe 2020.43

Neue Widgets auf dem Android-Homescreen anlegen

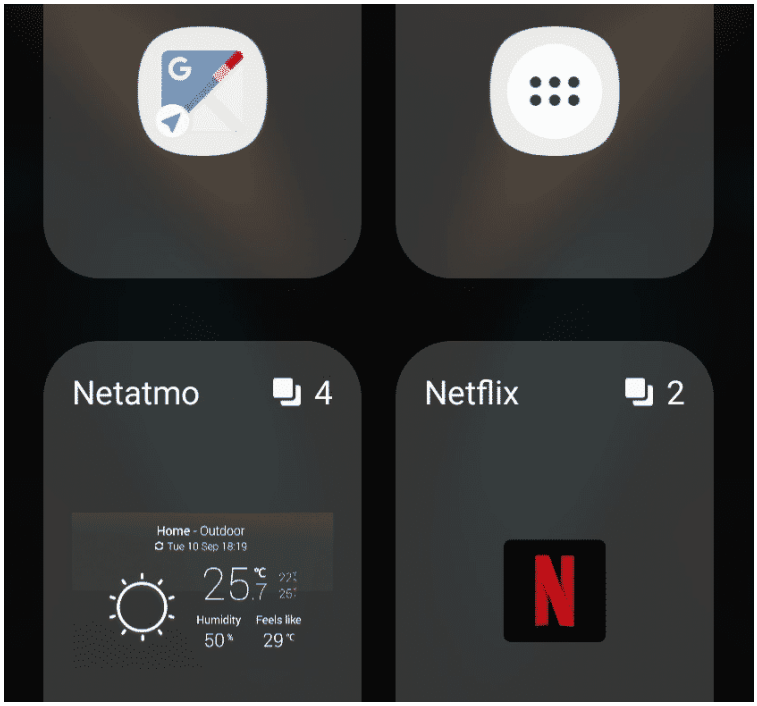


Widgets: Fast könnte man meinen, dass Apple diese kleinen Informationsfenster erfunden hat. Fakt ist aber, dass Apple erst 2020 mit iOS 14 auf die Idee gekommen ist, Android aber schon seit jeher Widgets auf dem Homescreen unterstützt hat. Wir zeigen Ihnen, wo und wie Sie diese auf Ihrem Smartphone verwenden können.

Sie müssen bei den Widgets zwei Kategorien unterscheiden: Es gibt zum einen die, die Android ab Werk mitbringt und die auf Geräten mit dem selben Launcher und der selben Android-Version gleich sind. Jeder App-Anbieter kann für seine App festlegen, ob er ein oder mehrere Widgets anbietet. Beide Widget-Arten finden sich in einer Übersicht. Dazu klicken Sie auf eine freie Stelle des HomeScreens und halten den Finger einen Moment darauf gedrückt. Die HomeScreens werden nun als kleine Ansicht angezeigt, darunter finden Sie eine neue Symbolleiste. Tippen Sie darin auf **Widgets**.



Für jede Funktion/jede App finden sie in einer alphabetisch geordneten Liste die Übersicht der Widgets. Oft gibt es derer gleich mehrere, dann finden Sie in dem Widget-Fenster eine kleine Zahl. Diese gibt die Anzahl der unterschiedlichen Widgets an.



Halten Sie den Finger auf das gewünschte Widget gedrückt und ziehen sie es nach oben in den entsprechenden HomeScreen. Wichtig: Auf dem muss auch

genug Platz sein, damit das Widget dort hinpasst. Ist das nicht der Fall, dann wählen Sie ein anderes Widget oder legen Sie einen neuen HomeScreen an!

Was ist ein Quadrocopter - und wann ist einer sinnvoll?

An den Anblick von "Drohnen" haben wir uns gewöhnt: Viele Menschen steuern die kleinen Fluggeräte mit den vier Rotoren aus Hobby. Denn es kann Spaß machen, die wendigen Flugkörper per Fernbedienung durch die Luft zu steuern - und gleichzeitig auch noch Fotos oder Videos aufzunehmen.

Die meisten sagen "Drohne", meinen aber Quadrokopter (oder Multikopter). So ein Quadrokopter hat vier Rotoren. Zwei drehen sich mit, zwei gegen den Uhrzeigersinn. Das hält das kleine Fluggerät stabil in der Luft. Die Wendigkeit ist enorm, denn so ein Quadrokopter lässt sich blitzschnell starten - steil nach oben.

Riesige Auswahl an Drohnen

Die Auswahl an entsprechenden Geräten ist heute wirklich riesig. Es gibt winzig kleine, die auch in einer Wohnung fliegen können, doch die sind in der Regel eher ein Spielzeug. Interessant wird es bei den Geräten ab 100 bis 300 Gramm, die sich präzise steuern lassen: Meist mit Hilfe einer App im Smartphone und einem Controller.

Die beiden Geräte verschmelzen dann. Die Drohne lässt sich steuern - und im Display des Smartphones ist das Live-Kamerabild zu sehen. Auf Wunsch lassen sich Fotos machen oder Videos drehen. Einige Quadrokopter haben heute exzellente Kameras an Bord, teilweise sogar mit einer Optik von Zeiss. Damit lassen sich gestochen scharfe Aufnahmen herstellen, die auch im Profibereich zum Einsatz kommen.

Eine schöne Übersicht über solche Quadrokopter, die preislich erschwinglich sind,

gibt es bei drohne.net. Das Portal informiert auch generell sehr ausführlich über alles, was man über Drohnen oder Multikopter zu wissen braucht.

Auch Profis fliegen mit Drohnen

Aber nicht nur Laien fliegen und steuern Drohnen, sondern auch viele Profis.

Zum Beispiel fliegen Profi-Kameraleuten mit Drohnen, um Aufnahmen zu machen. Die Polizei setzt Drohnen ein, um sich einen Überblick zu verschaffen, etwa bei großen Unfällen. Die Stadt Duisburg plant sogar, die Feuerwehr mit Drohnen auszustatten. Wird ein Brand gemeldet, könnte die Feuerwehr eine Drohne losschicken, die dann Live-Bilder an die Zentrale schickt. Die könnte dann sehen, was vor Ort los ist.

Wie schwierig ist es, eine Drohne zu fliegen?

Ich habe großen Respekt vor den Geräten, denn es sind fliegende Geschosse, das muss man schon sagen. Einige von ihnen schaffen im Sport Mode bis zu 70 km/h. Das ist schon was. Und es ist auch anspruchsvoll, so ein Gerät zu steuern. Es gibt eine Menge zu beachten, man will nirgendwo gegen fliegen, die optimale Route fliegen, schöne Bilder machen. Dazu verwendet man in der Regel ein Steuergerät, den Controller, der mit einem Smartphone gekoppelt wird. Im Display

gibt es dann live zu sehen, was die Kamera in der Drohne sieht.

Die Kamera will gesteuert werden. Wohin schauen wir? Wann auslösen? Gleichzeitig will auch die Drohne gesteuert werden. Es gibt eine Menge zu beachten: Akkustand, Windgeschwindigkeit, Abstand zu Objekten – da kommt schnell Stress auf. Das ist garantiert nicht für Kinder. Man muss ein hohes Maß an Verantwortungsbewusstsein haben.

Wer darf denn überhaupt eine Drohne fliegen – und muss man das anmelden?

Ein offizielles Mindestalter gibt es nicht. Manche Versicherungen schreiben aber ein Mindestalter vor. Drohnen ab 2 kg Gewicht setzen ein Mindestalter von 16 Jahren voraus. Das sind aber auch schon keine Hobbydrohnen mehr, die werden im Profibereich eingesetzt, etwa für hochwertige Filmaufnahmen.

Einen sogenannten **Drohnen-Führerschein**, eine Art Kenntnisnachweis, gibt es ebenfalls erst ab einem Gewicht von 2 kg. Die meisten Hobbydrohnen liegen deutlich darunter, so bei etwa 1 kg – und lassen sich daher ohne Führerschein und Genehmigung fliegen.

Wo darf man denn fliegen?

Die Vorschriften sind sehr strikt. Grundsätzlich nicht im Bereich von Flughäfen, auch Einflugschneisen sind ausgeschlossen. Krankenhäuser sind tabu. Oder Militäranlagen. Die Bereiche um Landtage oder Bundestag. Absolut tabu. Auch darf man nicht über Menschenmengen fliegen, man muss Abstand von 100 Metern zu Autobahnen und Schnellstraßen, Industrieanlagen und Unglücksorten einhalten und darf auch nur über bebaute Grundstücke fliegen, wenn man das Einverständnis der Besitzer hat.

Es gibt spezielle Apps, die helfen einem, zu erkennen, ob und wo man Drohnen aufsteigen lassen kann. Das ist vor allem im Bereich von Flughäfen sehr wichtig und sinnvoll. Auch die maximale Flughöhe ist limitiert: 100 Meter – mehr ist nicht erlaubt, jedenfalls nicht ohne explizite Genehmigung, die sich Profis durchaus einholen können. Auch bei Nacht darf man nur mit Genehmigung fliegen. Und: Der Pilot muss seine Drohne immer sehen können. Ohne Sichtkontakt ist Fliegen verboten. Eine Menge Einschränkungen also.

Starke Kundenauthentifizierung: Was ist das?

Dass das Passwort alleine kein wirklich ausreichender Schutz ist, dass haben Sie unter anderem bei unseren Artikeln rund um die Zwei-Faktor-Authentifizierung festgestellt. Viele Unternehmen sprechen jetzt sogar von der SCA, der "Strong Customer Authentication" oder übersetzt: Der "Starken Kundenauthentifizierung". PayPal beispielsweise fordert seine Kunden gerade reihenweise dazu auf, diese zu aktiveren. Doch was ist der Grund?

Die zweite Zahlungsdiensterichtlinie (PSD2) sieht vor, dass bei Zahlungsdienstleistern - zu denen PayPal gehört - weitere Sicherheitsmechanismen greifen müssen. Damit wird für bestimmte Transaktionen zwingend vorgeschrieben, dass neben dem ersten Faktor Passwort noch mindestens ein weiterer abgefragt werden muss. Die Faktoren teilen sich in drei Klassen:

Das Wissen: Das klassische Passwort ist etwas, das der Benutzer wissen muss, um sich einloggen zu können. Hat jemand anderes es erraten, dann ist dieses Wissen natürlich auch bei demjenigen vorhanden und der Schutz ist erloschen. Darum ergänzt man das Wissen um den Besitz.

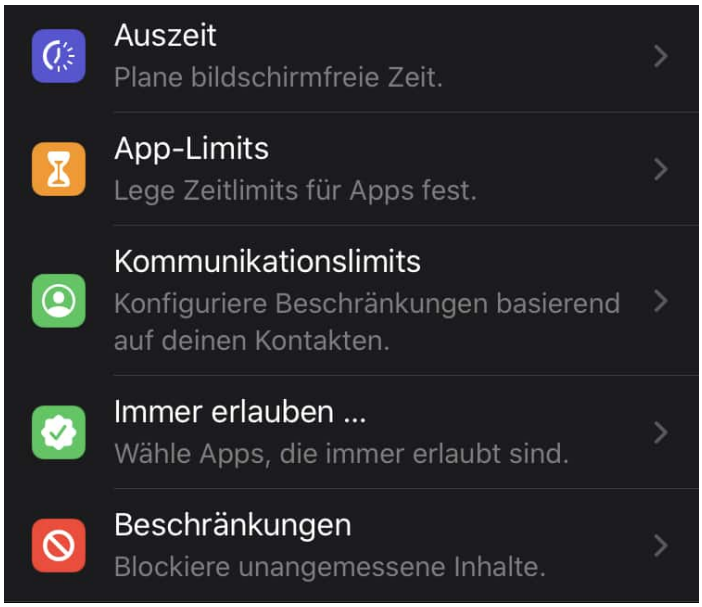
Der Besitz: Wenn Sie zusätzlich zum korrekten Passwort noch einen immer wechselnden Code eingeben müssen, der per SMS auf Ihr Smartphone kommt oder auf einem Token angezeigt wird, dann bedeutet dies zusätzlichen Schutz. Ein Angreifer muss nicht nur das Passwort bekopmmen, sondern auch noch in den Besitz des Gerätes kommen: Sonst kann er den Zahlencode nicht kennen und eingeben.

Einen Schritt weiter noch geht **die Inhärenz**: Auch ein Smartphone oder Token kann verloren gehen oder gestohlen und damit kompromittiert werden. Biometrische Merkmale können das nicht: Ihr Fingerabdruck, ihre Stimme, die Iris, das sind Eigenschaften, die fest mit Ihnen verbunden sind. Wenn diese als zusätzlicher Faktor verwendet werden, ist ein Kontenzugriff für einen Fremden kaum möglich!

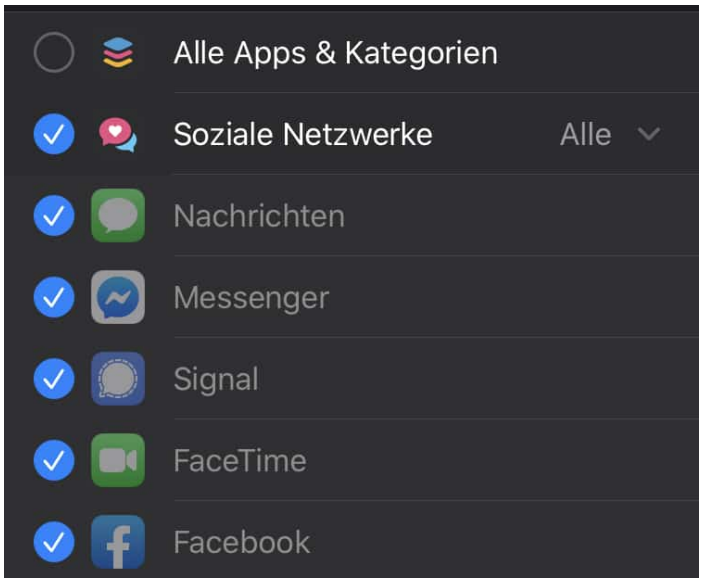
Digitale Auszeit: App-Zeiten einschränken bei iOS

Unsere Smartphones werden immer mehr zu einem mobilen Arbeitsplatz. Vorbei sind die Zeiten, in denen der Entertainment-Faktor mi Vordergrund stand. Durch die immer leistungsfähigere Hardware und die zunehmende Cloud-Verfügbarkeit Ihrer Daten ist das Arbeiten unterwegs einfach und verleitet so, kein Ende zu finden. Wir zeigen Ihnen, wie Sie sich Freiraum schaffen.

Der Begriff des "Digital Detox", der digitalen Auszeit, wird immer mehr diskutiert. Durch die Verfügbarkeit einer funktionierenden Arbeitsumgebung unterwegs sind sie verleitet, den Feierabend immer weiter zu verschieben. Und selbst dann sind Facebook, Ihr Lieblingsspiel und andere Apps immer noch eine Versuchung. iOS versucht, Ihnen über die Funktion der Bildschirmzeit Kontrolle darüber zu geben. eigentlich kommt diese Funktion aus den Einstellungen, die Eltern für das Gerät eines Kindes vorgeben können. Unter **Einstellungen** > **Bildschirmzeit** können Sie verschiedene Optionen wählen:



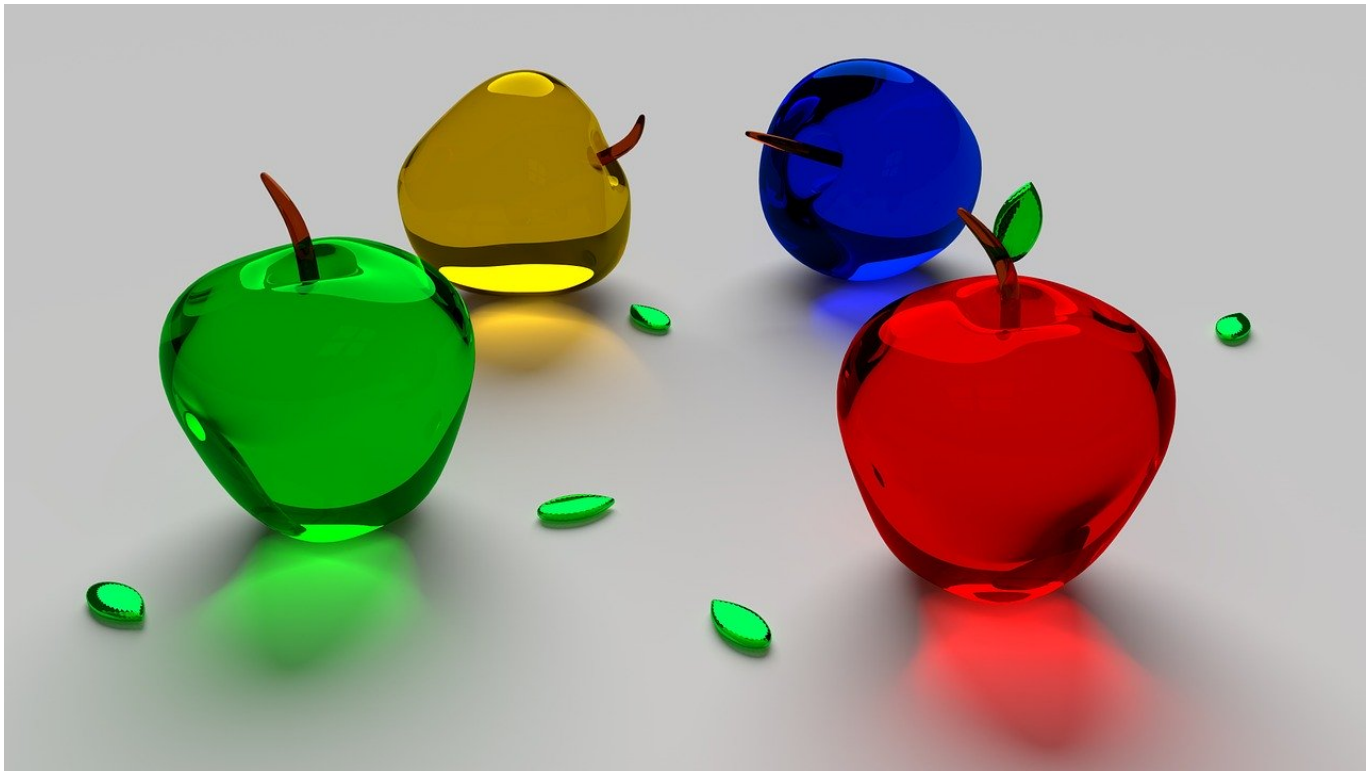
Unter **Auszeit** legen Sie tatsächlich eine bildschirmfreie Zeit fest. In der sind nur von Ihnen explizit freigegebene Apps und eingehende Anrufe verfügbar, alles andere wird verweigert. Unter **App-Limits** legen Sie fest, wie lange am Tag Sie bestimmte App-Kategorien zulassen wollen. Durch ein Tippen auf eine Kategorie öffnen Sie die von iOS automatisch zugeordneten Apps und können ein Limit auf Basis einzelner Apps vergeben. Nach Ablauf der Nutzungszeit wird die App geschlossen und lässt sich an dem Tag auch nicht mehr öffnen. Wenn die die Bildschirmzeit deaktivieren, dann fällt diese Beschränkung weg. Wenn bestimmte Apps generell von den Beschränkungen ausgenommen sein sollen, dann können Sie diese unter **Immer erlauben...** festlegen.



Auch die **Kommunikation** können Sie einschränken. Idealerweise definieren Sie

hier Kontakte, die davon ausgenommen sind, damit Sie im Notfall erreichbar sind.

iTunes Guthaben direkt vom Gerät verschenken



Viele Menschen verwenden iOS-Geräte und sind damit an den Apple App Store gebunden. Da bietet es sich als kleine Anerkennung oder als Geburtstagsgeschenk an, einen Gutschein für eben diesen zu verschenken. Oft dann, wenn es schnell gehen muss. Die Läden haben zu, die Tankstelle ist ausverkauft, dann ist guter Rat teuer. Wussten Sie, dass Sie das ganz bequem direkt von Ihrem iOS-Gerät machen können?

Dazu klicken Sie auf Ihrem iOS-Gerät auf **App Store** > **Ihr Kontobild** > **Karte per E-Mail senden**. der App Store öffnet eine Ansicht, die schon direkt an eine E-Mail erinnert. Geben Sie die E-Mail-Adresse des Beschenkten ein, korrigieren Sie den angegebenen Namen, der als Absender verwendet werden soll, wenn es nötig ist. Sie können einen kurzen Text eingeben, der dem Beschenken sagt, warum er bedacht wurde.

Zu guter Letzt legen Sie den Betrag fest, den Sie verschenken wollen. Der App Store erzeugt nun einen Gutscheincode für den angegebenen Wert und zieht den Betrag von Ihrer Standard-Zahlmethode ein. Im gleichen Moment wird der Gutscheincode an die angegebene E-Mail-Adresse versendet und ist vom Beschenkten direkt einlösbar. Einfacher geht es nicht!

Staatstrojaner für alle Geheimdienste?

Auch Kriminelle nutzen moderne Messenger wie WhatsApp oder Telegram. Clan-Kriminelle, islamische Terroristen, organisiertes Verbrechen. Für Polizei und Behörden ist das eine schwierige Sache, denn sie müssen auch observieren können, Gespräche belauschen, Kontakte ermitteln. Diese Woche hat die Bundesregierung beschlossen, den 19 Geheimdiensten den Einsatz von Staatstrojanern zu erlauben. Doch der Vorstoß ist alles andere als unumstritten. Auch Journalisten fürchten, möglicherweise abgehört zu werden.

Bundesinnenminister Seehofer hat den Gesetzentwurf vorgelegt – und setzt sich für das Vorhaben ein.

Es geht darum, dass Bundesverfassungsschutz, MAD sowie die 16 Landesbehörden des Verfassungsschutzes die Möglichkeit der sogenannten Quellen-TKÜ bekommen. TKÜ = Telekommunikationsüberwachung.

Die Schlapphüte sollen verschlüsselte Gespräche oder Video-Calls sowie Chats abhören dürfen – und zwar mit Hilfe eines Trojaners. Der aufgrund seiner Herkunft "Staatstrojaner" genannt wird. Der nistet sich dann im Gerät ein. Und weil der Trojaner direkt im Gerät aktiv ist, kann er die unverschlüsselte Kommunikation abhören und mitlesen – ein großer Vorteil.

Wie kommt ein Staatstrojaner aufs Gerät?

Das ist gar nicht so einfach. Dazu müssen die Behörden entweder kurz Zugriff auf das abzuhörende Gerät haben, damit sie die Software installieren können. Oder sie schicken der abzuhörenden Person eine Mail oder eine Message, die einen Anhang enthält. Durch Ausnutzen von Sicherheitslücken wird der Staatstrojaner dann auf das Gerät aufgebracht.

Das ist schon sehr aufwändig. Denn die Behörde muss wissen, welches Gerät verwendet wird, welche Software drauf installiert ist – und welche Sicherheitslücken ausgenutzt werden können, um den Staatstrojaner unbemerkt zu installieren. Im Grunde dieselbe Vorgehensweise wie bei Cyberkriminelle, die

Phishing-Mails verschicken... Allerdings müssen Internet-Provider im Zweifel beim Aufbringen des Staatstrojaners behilflich sein.

Das klingt nicht nur nach einer Menge Aufwand, sondern ist es auch. Zur Massenüberwachung taugen Staatstojaner daher auf keinen Fall, das muss niemand befürchten. Sowohl das Aufbringen des Staatstrojaners ist aufwändig – und das Auswerten des Materials natürlich auch. Man kann schon davon ausgehen, dass dieses Werkzeug nur eingesetzt wird, wenn es wirklich was zu holen gibt.

Kritik am Gesetzentwurf

Trotzdem gibt es erhebliche Kritik am Gesetzentwurf. Die Netzaktivisten von netzpolitik.org sprechen von einem "krassen Überwachungsgesetz"...

Das finde ich dann doch übertrieben. Denn: Der Aufwand ist hoch. Da kann wirklich nicht von einer breiten Überwachung die Rede sein. Gespräche, Telefonate oder Post mitzulesen, was schon immer die Aufgabe von

Sicherheitsbehörden und Geheimdiensten.

Dennoch argumentieren manche: Durch den Staatstrojaner wäre unser aller IT-Sicherheit gefährdet.

Das Argument trifft leider zu. Es ist ein altes Problem: Eigentlich soll uns der Staat schützen vor Bedrohungen jeder Art. Es sollte seine Pflicht sein dafür zu sorgen, dass zB Sicherheitslecks möglichst zeitnah gemeldet und gestopft werden. Wenn der Staat aber auch selbst Trojaner einsetzt, ist er darauf angewiesen, dass etliche Sicherheitslecks eben **nicht** gestopft werden, denn sonst lassen sich Trojaner nicht unbemerkt aufspielen.

Das ist ein klarer Interessenskonflikt. Und wir wissen: Wenn es Sicherheitslecks gibt und die bestehen bleiben – weil der Staat sie braucht –, dann werden diese Lecks auch von Cyberkriminellen ausgenutzt. Und davon sind wir dann alle betroffen. Das ist ohne jeden Zweifel eine Tatsache.

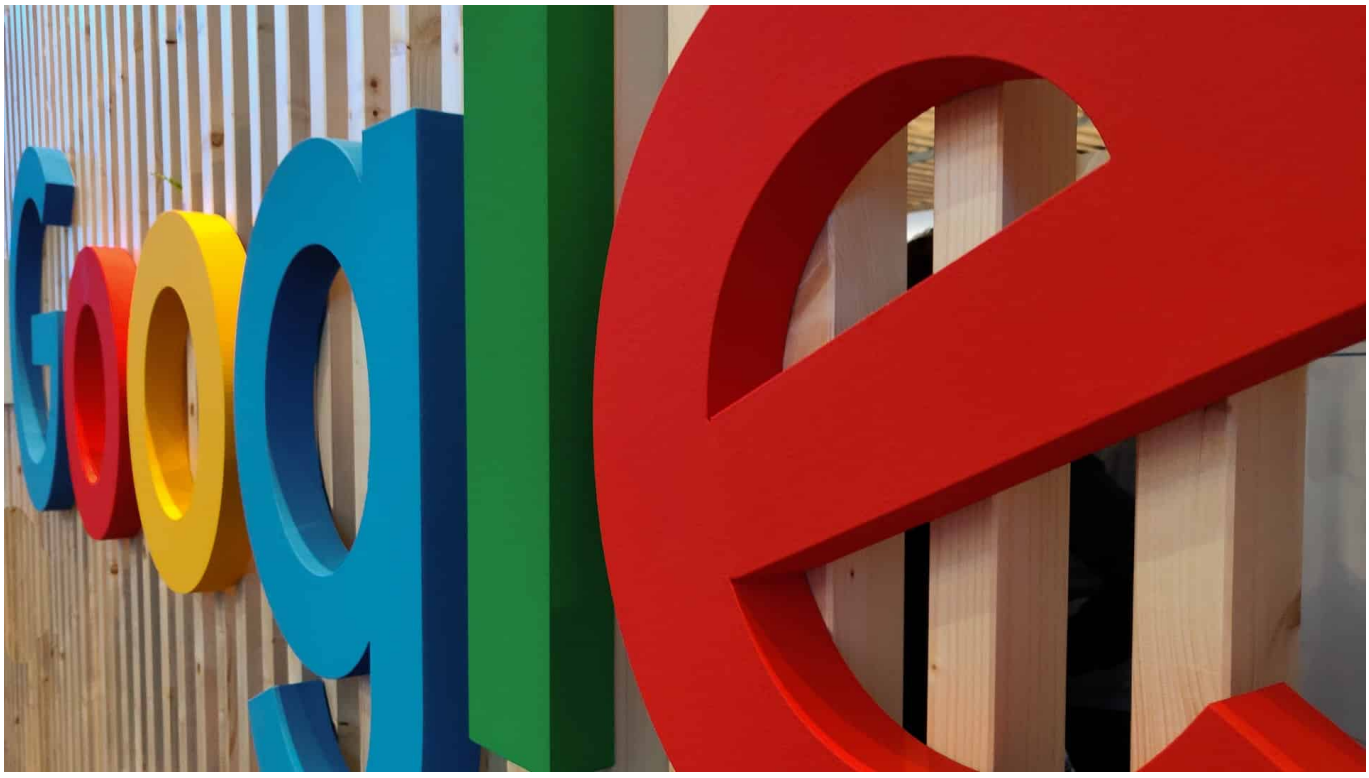
Auch Journalisten ausspähen?

"Reporter ohne Grenzen" beklagt, dass der Staatstrojaner auch gegen Journalisten eingesetzt werden darf. Welche Folgen hat das?

Journalisten unterliegen – wie einige andere Berufsgruppen auch – einem besonderen Schutz und dürfen nicht einfach so abgehört werden. Ist das anders, ist der Quellenschutz und die Vertraulichkeit der Kommunikation gefährdet.

Allein die Tatsache, dass zB ein Informant befürchten muss, abgehört zu werden, kann dazu führen, dass keine Informationen fließen. Das muss natürlich unbedingt vermieden werden. Gleichzeitig darf es natürlich nicht sein, dass sich islamische Terroristen nun einen Presseausweis besorgen und dann vor Abhöraktionen per Staatstrojaner geschützt sind.

Klage in den USA: Ist Google zu mächtig?



Das US-Justizministerium hat Klage gegen Google eingereicht. Der Vorwurf: Ausnutzen der Marktmacht zum Nachteil der Verbraucher. Denn Google bezahlt nicht nur Hardware- und Softwarehersteller dafür, auf ihren Geräten und in ihren Programmen die Nummer 1 Suchmaschine zu sein, sondern verdrängt möglicherweise auch im Werbeumfeld den Wettbewerb. Das wird ein interessanter Prozess!

Es gibt viele Suchmaschinen im Netz. Zumindest Theoretisch. Aber nur eine kennen alle - und zwar so gut, dass ihr Name weltweit zum Pseudonym für "Suchen im Netz" geworden ist: Google.

Das allein verleiht einer Suchmaschine ungeheure Macht. Die beeindruckenden Marktanteile, die Googles Suchdienst vorweisen kann, bestätigen den Erfolg.

US-Justizministerium - und elf US-Staaten

Doch nun hat das US-Justizministerium Klage eingereicht in den USA - und elf Bundesstaaten haben sich bereits angeschlossen. Der Vorwurf: Google habe seine Marktmacht missbraucht, den Wettbewerb unterdrückt und dadurch die Verbraucher geschädigt. In der Klageschrift wird das auch ausführlich begründet.

Die Klage ist kein Pappenstil, denn das US-Justizministerium ist mächtig. Gerichte werden sich nun ganz genau anschauen, wie die Mechanismen bei Google sind. Und es geht dabei nicht um die Suche selbst, sondern um die Art und Weise, wie Anzeigen präsentiert werden - auf den Suchseiten von Google, aber auch bei Android.

Der Vorwurf: Marktmacht ausgenutzt

Denn das darf man nicht vergessen: Google ist nicht nur die führende Suchmaschine, sondern stellt auch das mit Abstand populärste mobile Betriebssystem. Der konkrete Vorwurf: Google habe Milliardenbeträge an Hardwarehersteller wie LG, Motorola, Samsung oder Apple gezahlt, um als präferierte Suchmaschine eingetragen zu sein. Ebenso beim Browser Firefox: Auch hier erscheint Google an erster Stellt - und das lässt sich der Konzern eine Menge kosten.

Google habe sich zudem eine außerordentliche Stellung als "Gatekeeper" verschafft: Wenn alle alles googeln, bekommt Google nicht nur alles mit (und sammelt Daten), sondern verkauft auch jede Menge Anzeigen. Und die sind deutlich teurer, wenn es keinen Wettbewerb gibt. Mehr gefunden werden will, muss dafür bezahlen.

Prozess könnte reinigendes Gewitter sein

Natürlich ist die Sache deutlich komplexer - aber das in etwa ist der Knackpunkt. Google weist in einer ersten Reaktion darauf hin, dass kein Mensch **gezwungen** würde, Google zu nutzen. Das stimmt natürlich - und Google ist wirklich eine exzellente Suchmaschine.

Aber Google unternimmt alles, dass es keine Konkurrenz gibt - und nutzt dafür die bereits vorhandene Macht, dass es auch so bleibt. Das lässt sich nun wirklich nicht bestreiten.

Der Prozess wird groß werden. Es gibt Experten, die davon ausgehen, dass der Prozess gegen Microsoft vor 20 Jahren im Vergleich dazu klein war. Die gute Nachricht aber: Microsoft gibt es nach wie vor. Und die Wettbewerbssituation war nach dem Prozess fairer - im Interesse der Verbraucher.

Cyberbunker: Die Sache mit dem Provider-Privileg

Illegale Geschäfte im Netz abzuwickeln - ist ein riesiges Geschäft. In Deutschland wird aktuell ein besonders großer Fall verhandelt: Ein komplettes Rechenzentrum - unterirdisch in einem Bunker platziert - wurde für kriminelle Machenschaften und illegale Deals verwendet. Der Cyberbunker war ausschlielich für illegale Geschäfte im Darknet im Einsatz.

So etwas geht in Zeiten von Corona leider unter, aber Deutschland hat gerade ein aufsehenerregendes Gerichtsverfahren: Gegen die Betreiber von zahllosen kriminellen Darknet-Angeboten.

Der Prozess am Landgericht Trier ist äußerst kompliziert und komplex - und soll womöglich bis Ende 2021 dauern. Denn es wird gegen die Betreiber eines Rechenzentrums verhandelt, über das massenhaft kriminelle Geschäfte abgewickelt wurde. Bekannt als der "Cyberbunker".

Mindestens 249.000 Straftaten nachgewiesen

Angeklagt ist ein Niederländer sowie sieben weitere Personen (einige davon Familienmitglieder, also eine Art Family Business), die gemeinsam in einer Bunkeranlage in Traben-Trarbach ein Rechenzentrum betrieben haben. Die Mannschaft hat über Jahre hinweg die Infrastruktur für Angebote im Darknet bereitgestellt. Meint: Im Cyberbunker wurden vor allem Server betrieben, über die kriminelle Geschäfte abgewickelt wurden. Die Anklage spricht von mindestens 249 000 Straftaten.

Der Prozess dauert so lange, weil es grundsätzlich schwierig ist, Aktivitäten im Darknetz nachzuweisen. In diesem Fall ist es den Behörden gelungen. Sie haben keine Klitsche ausgehoben, sondern einen regelrechten Platzhirschen. Besonders schwierig, beklagt Oberstaatsanwalt Jörg Angerer in der Süddeutschen Zeitung, sei das sogennante "Providerprivileg".

> "Der Provider muss nicht prüfen, was auf seiner Plattform passiert, das kann er oft gar nicht. Nur wenn er Kenntnis von kriminellen Geschäften

hat, muss er aktiv werden.“

Provider-Privileg: Wichtig - aber reformbedürftig

Ob es wirklich gelingt, dem Unternehmen (Provider) Beihilfe zu Cyber-Straftaten nachzuweisen - zumal in diesem Umfang! -, ist derzeit leider noch völlig offen. Das Rechtswesen ist manchmal sehr kompliziert. Dabei ist es augenscheinlich, dass das komplette Rechenzentrum für allein diesen Zweck gebaut und betrieben wurde. Kein "Cyberbunker" - dieser Begriff ist viel zu harmlos und verniedlichend! -, sondern eher ein virtuelles "Sodom und Gomorra".

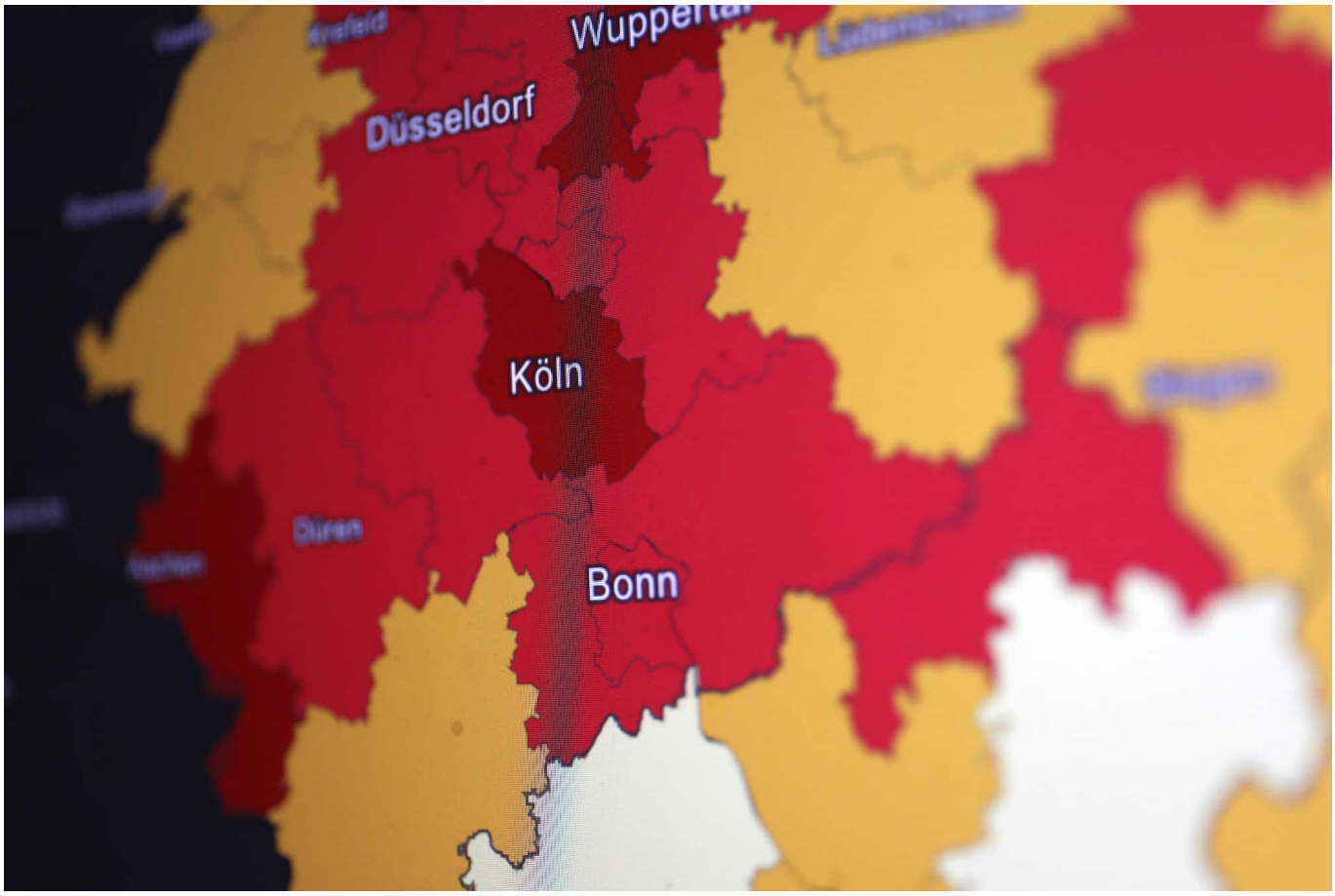
Das Provider-Privileg ist wichtig. Denn natürlich kann ein gewöhnlicher Provider nicht wissen, ob jemand zum Beispiel über einen gemieteten Server Canabis verhökert - oder IT-Infrastruktur angreift. Nur: Die seriösen Provider versuchen, Missbrauch zu erkennen - und reagieren entsprechend, wenn etwas Auffälliges passiert.

Mehr Sorgfaltspflichten wünschenswert

Ein Rechenzentrum, das praktisch ausschließlich Darknet-Angebote betreibt und in dieser "Branche" ganz offensichtlich einen guten Ruf genießt, kann wohl kaum behaupten, nichts davon gewusst zu haben.

Das Privileg ist meiner Ansicht nach reformbedürftig. Es ist an der Zeit, das Provider-Privileg präziser zu formulieren: Keine unangemessene Einmischung - aber angemessene Sorgfaltspflichten. Denn einen weiteren "Cyberbunker" brauchen wir garantiert nicht.

Corona PLZ Checker: Wo gibt's ein Risikogebiet?



Die offiziellen Zahlen der an Corona bzw. Covid-19 Erkrankten nimmt in Deutschland derzeit leider dramatisch zu. Besonders wichtig in diesem Zusammenhang: die Inzidenzzahlen. Wer eine Reise plant, kann jetzt bequem durch Eingabe der Postleitzahl erfahren, ob es sich um ein Risikogebiet handelt.

Der Corona PLZ Checker ist wirklich praktisch: Einfach die PLZ eingeben - schon zeigt das Tool die aktuellen Zahlen an. Die kommen aus der aktuellen Statistik des RKI. Das Tool präsentiert nicht nur die aktuelle Inzidenzzahl (also Fälle auf 100.000 Einwohner), sondern auch die Fälle insgesamt und die Todesfälle (allerdings alles auf Kreisebene bzw. je Stadt).

Schneller geht's wirklich nicht: Das Tool macht es überflüssig, eine lange Liste zu durchsuchen oder in einer Online-Karte den passenden Ort zu finden. Die Postleitzahl als Schlüssel - das ist clever.

Mit Hilfe des PLZ-Corona-Checkers könnt Ihr Eure Reisen besser planen. Hoteliers können aber auch einfach nachschauen, ob ein Gast aus einem

aktuellen Risikogebiet kommt. Das Tool bietet also wirklich für viele eine nützliche Funktion an.

Der Quellcode liegt auf GutHub, kann also von jedem eingesehen werden. Maximale Transparenz.

Kinder- und Jugendschutz im Netz wird verbessert

Das Bundeskabinett beschließt ein weiter entwickeltes, in den Augen der Politiker strengeres Jugendschutzgesetz für mehr Kinder- und Jugendschutz im Netz. Durchaus sinnvoll, denn der Jugendschutz wird im Netz mit Füßen getreten. Es braucht dringend ein energisches Durchgreifen. Doch es gibt bereits Kritik an der geplanten Umsetzung. Und auch die ist berechtigt.

Im Internet gibt es so ziemlich alles, was man sich vorstellen kann. Nein, nicht so ziemlich: Es gibt alles. Seriöse Informationen. Filme. Serien. Artikel. Fotos. Videos. Aber auch jede Menge Inhalte, die nicht für Kinder und Jugendliche geeignet sind. Gambling. Casinos. Erotik. Pornografie. Brutalität.

Eben alles. Die Bundesregierung will nun etwas dagegen unternehmen, den Jugendschutz im Netz verbessern. Das Kabinett hat Mittwoch eine Reform des Jugendschutzes beschlossen. Der Entwurf von Bundesfamilienministerin Franziska Giffey verspricht einen besseren Jugendschutz und sieht eine Menge Auflagen und auch Bußgelder vor.

Eins gleich vorweg: Weniger Jugendschutz geht auch kaum. Denn bislang hat sich die Politik darum praktisch gar nicht gekümmert. Kinder und Jugendliche sind sich im Netz bislang selbst überlassen. Die Eltern lässt man im Regen stehen. 41 Prozent der Kinder und Jugendlichen fühlten sich bei ihren Internet-Aktivitäten gemobbt, beschimpft oder bedrängt.

Das zeigt, wie dringend etwas passieren muss.

Das Paket sieht Auflagen vor allem für die großen Plattformen ab 1 Mio. Nutzer vor, also konkret Facebook, Youtube, Whatsapp, Instagram, aber auch Games-Plattformen, die häufig vergessen werden, aber bei Jugendlichen eine Rolle spielen. Ziel ist, die Minderjährigen vor Belästigung, Mobbing und Abzocke zu schützen. Die Plattformen müssen geeignete Maßnahmen ergreifen und es drohen hohe Bußgelder bis zu 50 Mio. EUR.

Konkretere Altersangaben - und Schutz vor Abzocke

Am einfachsten und klarsten sind noch die Regeln, was die Altersangaben betrifft, etwa bei Spielen. Die sollen klarer werden – und auch strenger kontrolliert und

eingehalten. Wichtig auch, dass mehr bei Abzockfallen in Spielen passiert.

Da gibt es in vielen Games und Apps ja diese „Lootboxen“, also Schatzkisten, die erzeugen einen regelrechten Suchtcharakter: Noch mal probieren, mehr, Glücksppiel.

Oft sind die auch kostenpflichtig, müssen also bezahlt werden. Bislang halten sich viele Spiele und Game-Entwickler nicht an die geltenden Regeln und sprechen auch gezielt Kinder und Jugendliche an. Dass sich hier etwas ändert, ist gut und richtig. Wir können nur hoffen, dass das schnell kommt, weil es wirklich wahnsinnig viele dreiste Abzock-Fallen in Games gibt.

Mobbing und Belästigung

Aber auch ein anderes, leider zunehmendes Problem wird angegangen: Mobbing und Belästigung in Sozialen Netzwerken und Foren.

Zumindest die großen Portale sollen geeignete Maßnahmen für Beschwerden und Meldungen vorsehen. Das verhindert kein Mobbing, bietet Betroffenen aber zumindest eine Hilfe und einen Ausweg an. Außerdem müssen die großen Konzerne Ansprechpartner für die Behörden bestimmen.

Es ist traurig, dass man so etwas überhaupt fordern muss. Aber Google, Apple, Facebook und Co. haben so etwas in der Regel nicht. Sie haben manchmal nicht mal eine Telefonnummer oder eine Postadresse, um juristische Dokumente zuzustellen. Mobbing und Belästigung werden damit natürlich nicht beseitigt, aber es sind erste wichtige Schritte.

Wer ist Ansprechpartner und zuständig?

Es gibt erste Reaktionen auf den Entwurf – auch aus der Games-Branche. Und die sind nicht begeistert.

Der Plan für mehr Kinder- und Jugendschutz wird vom Branchenverband grundsätzlich begrüßt. Allerdings kritisiert er auch, dass nicht klar sei, welche Aufsichtsbehörden denn zuständig seien. Und das stimmt auch: Wir haben in Deutschland ein völlig chaotisches System.

Das ist auch meine Erfahrung: Nie fühlt sich jmd zuständig. Denn wir haben die Landesanstalten für Medien, das ist auf Landesebene, und wir haben die Bundesprüfstelle für jugendgefährdende Medien, die zu einer Bundeszentrale ausgebaut werden soll. Wer ist wann zuständig?

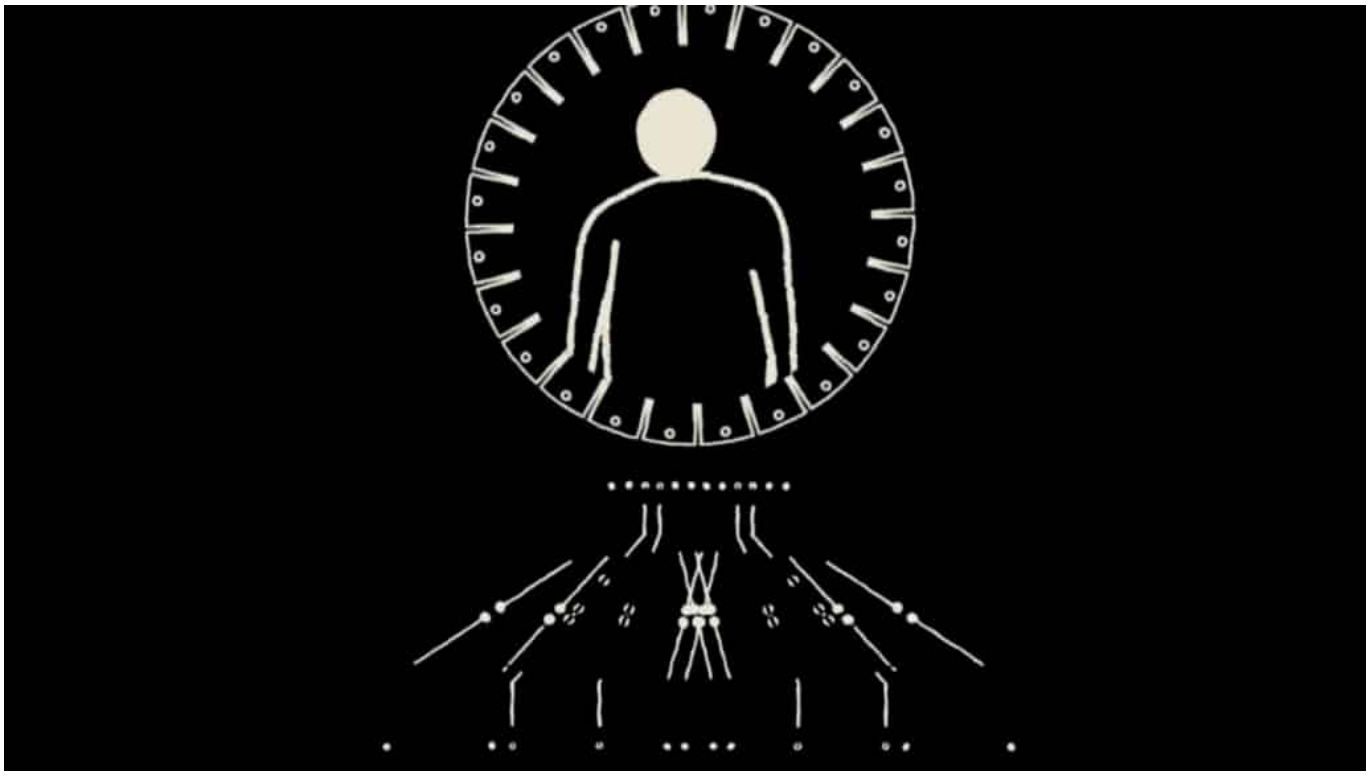
Keiner weiß es. Denn es kann doch wohl kaum der Firmensitz einer Onlinefirma eine Rolle spielen. Es wäre wohl zweifellos viel besser, alles zentral zu bündeln, mit maximaler Kompetenz und Autorität, damit auch wirklich eine Schlagkraft damit verbunden ist. Sonst passiert wieder nichts – wie in der Vergangenheit.

Jetzt macht uns KI auch noch unsterblich...

Ein neuer Trend im Silicon Valley: Wer mag, kann mit Hilfe von KI unsterblich werden. Aber nicht im körperlichen Sinn. Die KI hält die Erinnerung aufrecht: Indem Gedanken, Geschichten und Eigenheiten über Chat-Bots weiter bestehen. Hinterbliebene können mit Verstorbenen weiter im Dialog stehen - oder sich begegnen. Auch virtuell.

Künstliche Intelligenz (KI) ist für die meisten eher eine Art "Black Box": Wie neuronale Netze funktionieren, was KI-Systeme können und was nicht - davon haben viele keine konkrete Vorstellung.

Und weil die Industrie den Begriff mittlerweile überall verwendet, regelrecht inflationär (selbst Kaffee-Automaten wird KI untergejubelt), scheint auch das nicht unmöglich: KI soll uns unsterblich machen. Natürlich nicht im wahrsten Sinne des Wortes, aber doch im übertragenen Sinn.



KI entscheidet, was erinnerungswürdig ist

Das Silicon Valley bietet tatsächlich mittlerweile Dienste an, die eine Form von dauerhafter Erinnerung und Vermächtnis erlauben. Eine neue Form von Weiterexistieren. KI-Systeme werden entsprechend trainiert, damit sie wie Menschen reagieren, die bereits verstorben sind. Kein Blättern in Fotoalben oder Anschauen von Videos, sondern Interaktion.

Beispiel: Das amerikanische Startup Hereafter. Wer hier Kunde wird, kann sein Vermächtnis vorbereiten. Er oder sie kann Geschichten erzählen, Erinnerungen hinterlassen. Algorithmen analysieren dann alles. Auf diese Weise entsteht ein digitaler Klon. Eine Kopie.

Zwischen Trost und spooky

Das Versprechen: Angehörige können nach dem Tod noch mit den Verstorbenen sprechen. Das geht sogar per Alexa. Oder Google.

"Was war Dein schönster Urlaub?" Zu hören sind nicht nur die Erinnerungen der verstorbenen Person, sondern sogar ihre Stimme. Das kann manch einem vielleicht Trost spenden, ist aber vor allem eins: spooky.

Digitale Seele - Arten des "Weiterlebens"

Moritz Riesewieck und Hans Block haben darüber ein Buch geschrieben: "Die Digitale Seele". Sie berichten von diversen solcher Projekte. Denn es scheint ein Trend zu sein: Viele wollen digital weiter existieren.

Doch es gibt Risiken. Wer soll zum Beispiel bestimmen können, dass so ein digitaler Klon entsteht? Die Algorithmen entscheiden schon, was erinnerungswürdig ist. Und vor allem: Was macht so etwas mit den Hinterbliebenen?

Risiken inklusive

Manche mögen es genießen. Andere könnte es verstören. Wie das Beispiel aus Korea zeigt: Hier hat eine Mutter in der Virtual Reality ihre verstorbene zehnjährige Tochter wiedergetroffen, die nach vorhandenen Fotos, Videos und Tonaufnahmen rekonstruiert wurde.

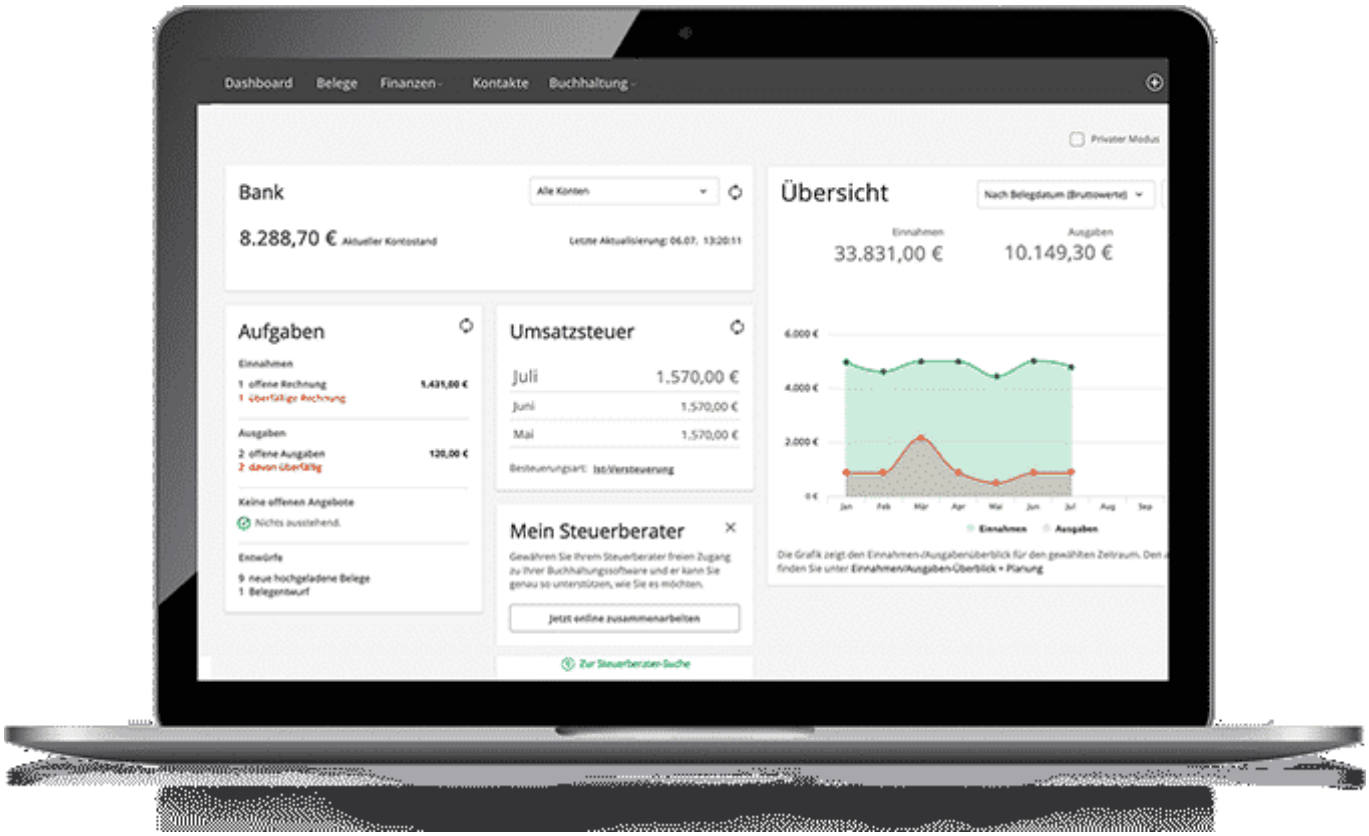
Da einige Anbieter auch das analysieren, was wir im Netz und in den Sozialen Netzwerken hinterlassen, braucht es wohl dringend Regeln - moralische, ethische und auch juristische. Denn eins hat das Silicon Valley gezeigt: Womit die Startups einmal anfangen, das hört nicht wieder auf. Wir sind gut beraten, rechtzeitig

Regeln aufzustellen.

Digitalisierung im Rechnungswesen 2020

Der Trend zum Home Office ändert eine Menge. Es werden nicht nur mehr Videokonferenzen abgehalten, sondern es landen auch viele andere Aufgaben in der Cloud. Die Digitalisierung schreitet voran - auch in der Buchhaltung und im Rechnungswesen.

Klar: Auch die Buchhaltung wird zunehmend digitalisiert - auch ohne Corona. Doch Corona beschleunigt die ohnehin vorhandene Entwicklung. Nicht jeder kleine Beleg muss heute noch auf Papier eingereicht und mit drei Stempeln und vier Unterschriften versehen werden. Es reicht häufig, den Beleg zu scannen oder zu fotografieren, um ihn dann digital zu verbuchen.



Digitalisierung hilft Kosten zu sparen

Ist so etwas erst einmal vernünftig und durchgängig eingerichtet, lassen sich damit Kosten sparen. Denn die Vorteile liegen auf der Hand: Jede(r) kann auf Belege und Buchungen zugreifen, unabhängig vom Aufenthaltsort. In Zeiten von vermehrtem Homeoffice ist das natürlich schon allein ein enormer Vorteil.

Selbstverständlich müssen dann die nötigen Rechte eingerichtet werden, damit nur die Personen Belege und Buchungen einsehen, genehmigen und ändern dürfen, die dazu auch wirklicj berechtigt sind. Entsprechend spezialisierte Software erledigt das mit geringem Aufwand.

> Der Begriff Buchhaltung bezeichnet die **Abteilung im Unternehmen**, die sich mit der Buchführung befasst. Diese bezeichnet also die eigentliche Tätigkeit sowie die dahinterstehende Methodik. Die Buchhaltungs-Abteilung besteht aus einem oder mehreren Buchhaltern. Der umfassendere Begriff Rechnungswesen findet hierfür ebenfalls oft Verwendung.

Prozesse automatisieren und Dokumente erzeugen

Es zieht auch zunehmend Künstliche Intelligenz (KI) ins Rechnungswesen ein: Die Programme von Lexware zum Beispiel sind vielseitig und lernfähig. Wer als Selbständiger oder Freiberufler regelmäßig Angebote schreiben muss, kann sie mit der Software Lexoffice auf Knopfdruck in eine Auftragsbestätigung und später in eine Rechnung umwandeln. Diese im PDF-Format, denn Rechnungen als Word-Dokument oder Excel-Datei sind verboten.

Sollte kein Zahlungseingang zu verzeichnen sein, kann die Software ebenso automatisch auch Mahnungen verschicken. Ein nahtloser Übergang der verschiedenen Arbeitsschritte. Vollständig automatisierte Prozesse. Das hilft nicht nur in großen Unternehmen weiter, sondern eben auch bei Freiberuflern und Selbständigen.

Dashboards: Übersicht über Einnahmen und Ausgaben

Genauso einfach lässt sich eine praktische Übersicht über Einnahmen und anstehenden Ausgaben erstellen: Auf Wunsch werden auch ausstehende

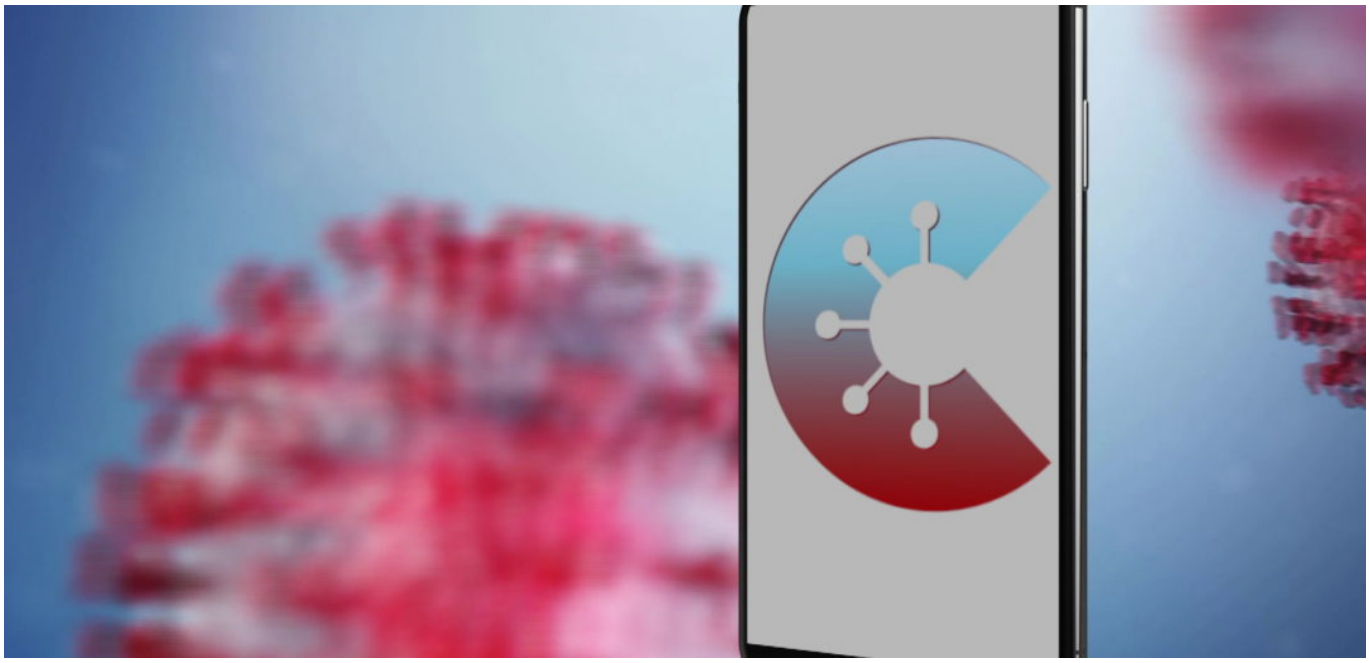
Zahlungen und sogar Steuertermine berücksichtigt. Ideal, um für Liquidität zu sorgen. Das Dashboard in Lexoffice zeigt auf Wunsch offene Rechnungen an, präsentiert aktuelle Kontostände und Zahlungsflüsse.

Lexware ist bekannt für seine Steuer-Software: Damit kann jeder einfach und bequem seine individuelle Steuererklärung anfertigen - und zum zuständigen Finanzamt senden. Lexoffice geht sehr viel weiter. Auf Knopfdruck lassen sich alle nötigen Formulare erstellen und erzeugen, auch die zur Umsatzsteueranmeldung und vieles andere mehr. Wenn alle Dokumente - auch Belege - lückenlos erfasst und gesoeichert werden, geschieht das nahezu ohne weiteres Zutun.

Aber auch, wer einen Steuerberater hat und braucht, erspart sich - und auch dem Steuerberater - Aufwand und Zeit. Denn mit der Software lassen sich die Belege erfassen, zuordnen und schon vorbuchen. Das erleichtert die nachfolgenden Arbeitsschritte und Prozesse enorm.

Der Nutzen liegt auf der Hand - und der Spareffekt ist erheblich.

Corona Warn App Version 1.5 ist nun EU-tauglich



Es gibt ein Update für die Corona Warn App, die über die Update-Funktion in den App-Stores von Apple und Google geladen werden kann. Version 1.5 bietet im Wesentlichen zwei neue Funktionen: Die Corona Warn App funktioniert nun auch über die Grenzen Deutschlands hinaus - und es gibt eine Protokollfunktion für Personen, die infiziert sind.

Besonders wichtig in einem vereinigten Europa ist, dass die EU in den letzten Wochen ein **EU Federation Gateway Service (EFGS**) aufgebaut hat. Ein Netzwerk, das es allen dezentral arbeitenden Warn-Apps in Europa die Zusammenarbeit erlaubt. Dadurch sind Kontakte mit als Infizierten auch über die Landesgrenzen hinaus erkennbar. Kostenpunkt: 13 Mio. EUR.

Ein wichtiger Schritt, der schon viel früher hätte gegangen werden müssen. Denn auch, wenn durch Corona weniger gereist wird als normalerweise: Menschen überschreiten nach wie vor die Grenzen. Im grenznahen Gebiet wie selbstverständlich, auch, um arbeiten zu gehen. Das zentrale Gateway sorgt dafür, dass internationale Kontakte registriert und gemeldet werden.

Ziel: 16 Apps von EU-Mitgliedsstaaten kooperieren

Deutsche User müssen dafür gar nichts machen - außer das Update installieren. User in anderen Ländern müssen die Funktion mitunter freischalten. In einem ersten Schritt tauschen die Warn-Apps aus Deutschland, Irland, und Italien länderübergreifend Daten aus. Schon bald soll es auch in Dänemark, Lettland und Spanien funktionieren.

Weitere Mitgliedsstaaten wie die Niederlande, Österreich, Polen und Tschechien folgen voraussichtlich im November, berichtet die Wirtschaftswoche.

Frankreich bleibt außen vor, weil sich Frankreich für eine zentrale Lösung entschieden hat - die ist nicht kompatibel.

Ebenfalls neu: Symptomtagebuch

Darüber hinaus - und das ist die zweite neue Funktion! - können positiv Getestete freiwillig auch Krankheitssymptome in ein Symptomtagebuch eintragen. Auf diese Weise soll die Risikobewertung bei Kontaktpersonen verbessert werden. Denn es macht einen Unterschied, ob ein milder Verlauf vorliegt - oder ein schwerer.

Da wir uns eindeutig auf eine zweite Welle vorbereiten müssen - oder bereits

mitten drin stecken! -, kommt der Warn-App nun wieder eine größere Bedeutung zu. Leider meinen immer noch viele, sie müssten nicht mitmachen. Zwar verzeichnet die App mittlerweile 19,5 Mio. Downloads in Deutschland. Doch es könnten deutlich mehr sein. Richtig eingesetzt, kann die App helfen, Infektionsketten schneller zu durchbrechen.

Allerdings müssen aber auch unbedingt die Gesundheitsämter besser unterstützt werden. Denn die Arbeit haben die Mitarbeiterinnen und Mitarbeiter der Gesundheitsämter, die im Falle einer Infektion mühsam die möglichen Kontakte nachvollziehen müssen. Hier hilt die Warn-App leider nicht weiter.

CleverPDF: Praktische PDF-Funktionen online

Wer mit anderen Dokumenten austauschen will, verwendet dazu in der Regel PDFs. Denn praktisch jede(r) kann ein PDF öffnen und drucken. Selbst auf dem Smartphone ist das in der Regel kein Problem. Aber nicht jeder hat ein voll funktionsfähiges PDF-Programm zur Hand, mit dem sich Dokumente erstellen lassen. Hier kann CleverPDF weiterhelfen.

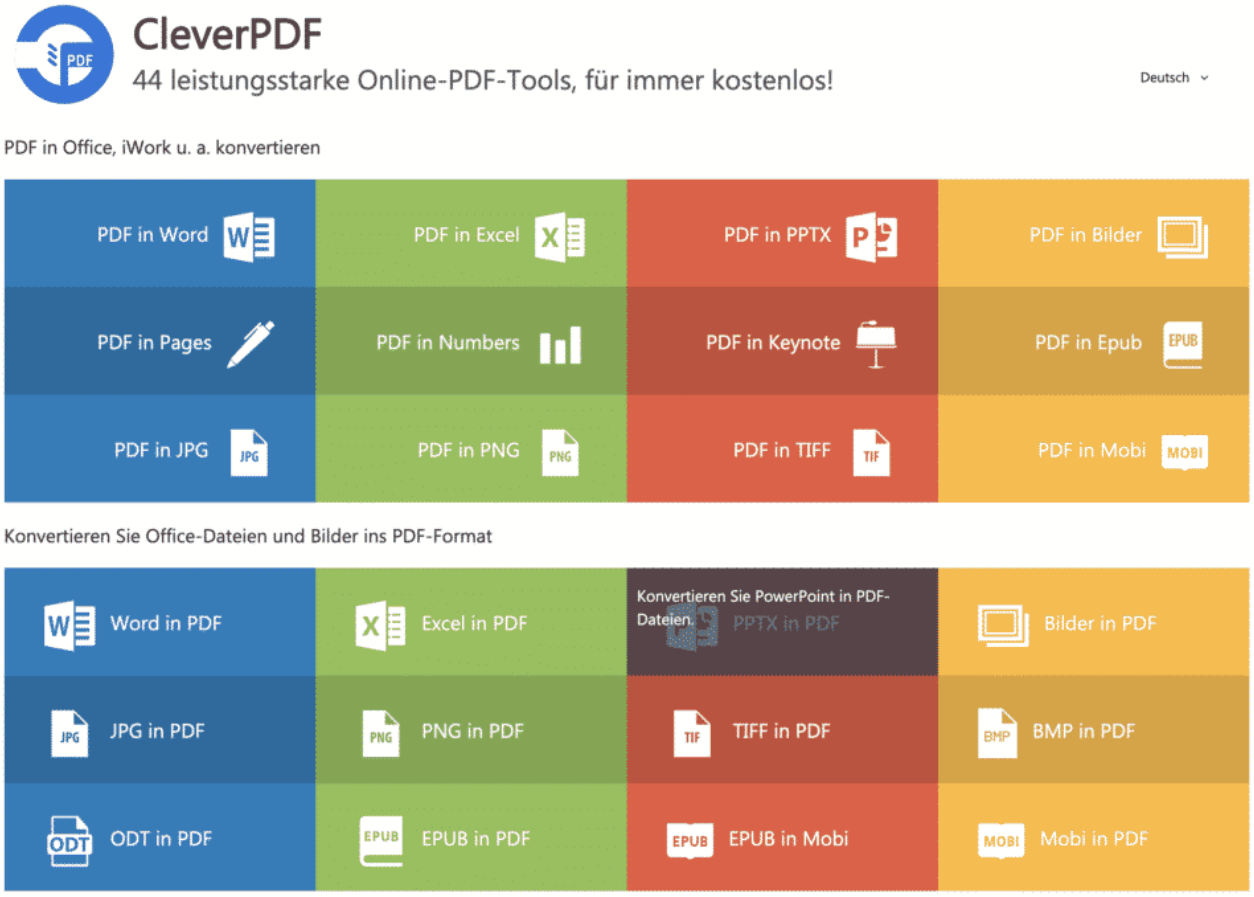
Viele Apps und Programme bieten die Möglichkeit, ein vorhandenes Dokument als PDF zu exportieren - oder "in" eine PDF-Datei zu drucken. Viele - aber nicht alle. Deshalb ist es gut zu wissen, dass es im Web einen praktischen Onlinedienst gibt, der praktisch alle nur denkbaren und nötigen Funktionen kostenlos anbietet - und alles online!

Viele nützliche Funktionen - alle an einem Platz

So ist es weder ein Problem, aus einem Word-Dokument ein PDF zu erzeugen - noch umgekehrt! CleverPDF kann aus vorhandenen Office-Dokumenten auch ohne Zugriff auf Microsoft Office ein PDF-Dokument erstellen. Aber umgekehrt

besteht auch die Möglichkeit, aus einem PDF wieder eine Excel-Datei zu machen (nur ein Beispiel).

Praktisch ist, dass CleverPDF auch mobile Dateiformate wie .ePub oder .Mobi unterstützt. Auf diese Weise lassen sich vorahndene PDFs oder andere Dokumente leicht und bequem in ein Dateiformat wandeln, das auch eBook-Reader verstehen. Wichtig!



Dokumente verschlüsseln, komprimieren oder zusammenführen

Doch CleverPDF kann noch viel mehr - und wird dadurch spätestens hier auch für alle User interessant, die ihre PDF-Dokumente mit Anwendungen oder Apps erzeugen. Denn CleverPDF kann auf Wunsch auch PDFs zusammenführen, Seitenzahlen in PDFs einfügen, PDF-Dokumnte verschlüsseln (oder entschlüsseln), Seiten löschen oder umordnen und vieles andere mehr.

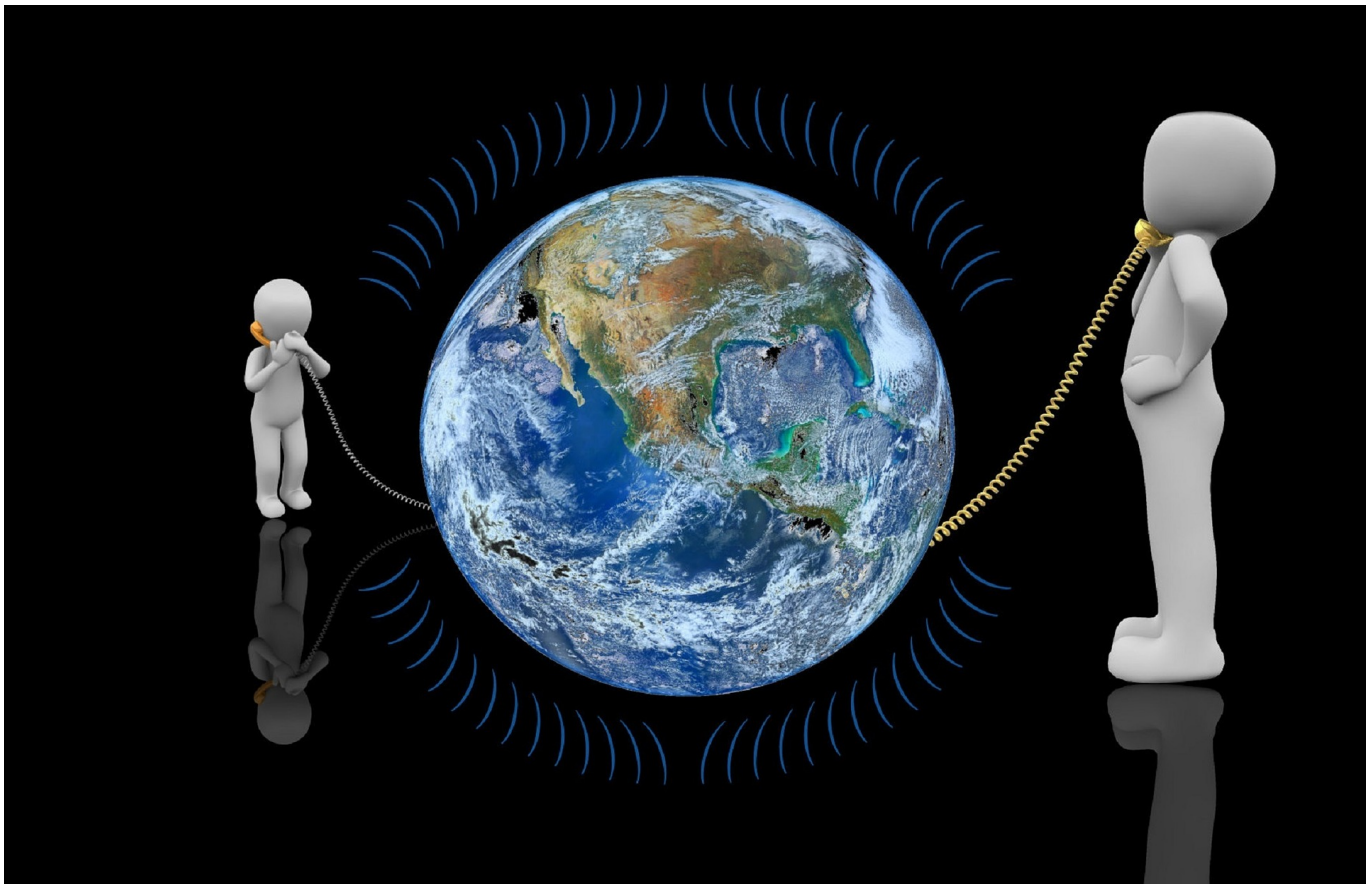
Sollte ein PDF zu umfangreich werden, ist auch ein Kompriminieren von PDFs möglich (weniger Speicherplatz nötig) - oder das Aufteilen eines PDFs auf

mehrere Dokumente.

Online kostenlos - und auf dem Desktop sicher

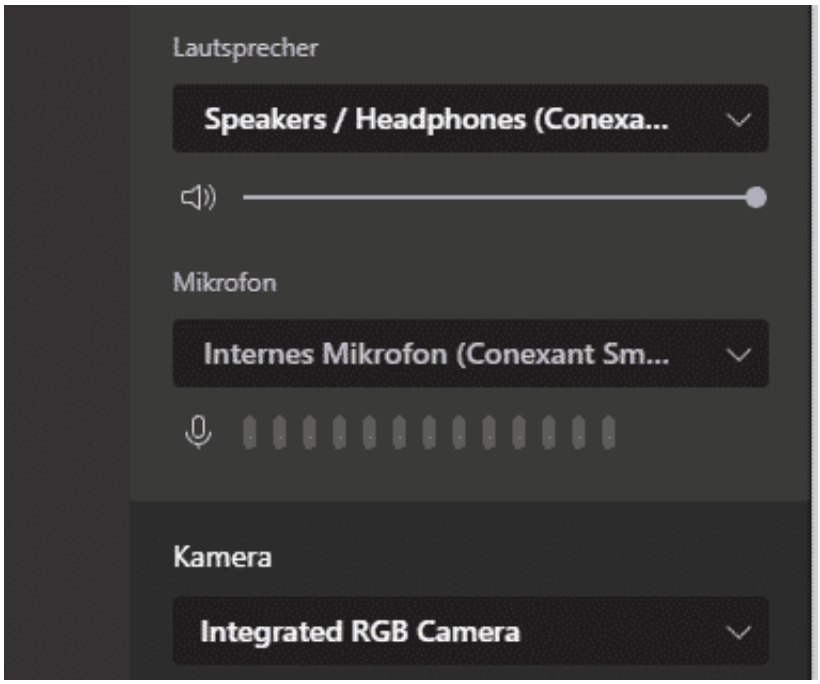
Wer das online erledigt, kann die Funktionen kostenlos nutzen - muss dafür aber die Dokumente hochladen. Das ist und bleibt Vertrauenssache. Auch wenn der Anbieter keinen Anlass zur Sorge bietet: Besser ist es natürlich, all diese Aufgaben auf dem eigenen Desktop zu erledigen. Für relativ kleines Geld (unter 20 EUR) lassen sich Desktop-Versionen für MacOS und Windows 10 kaufen.

In Teams an Meetings mit einem Raumsystem teilnehmen



Die Nutzung von Teams oder Zoom ist mittlerweile immer mehr zum Standard geworden. Unternehmen sind immer mehr dazu übergegangen, Räume mit entsprechender Hardware auszustatten. Allerdings ist es oft so, dass Sie Medien oder Dokumente von Ihrem eigenen PC teilen wollen und entscheiden müssen: Raumsystem oder lokaler PC. Das müssen Sie aber nicht!

Um das Meeting bedienen zu können, müssen Sie sich ganz normal mit Ihrem PC anmelden. Im einfachsten Fall können Sie sich mit den externen Geräten wie Kamera, Mikrofon und Lautsprecher verbinden. Dann können Sie diese in Teams direkt verwenden. Dazu klicken Sie im Meeting auf die **drei Punkte**, dann auf **Geräteeinstellungen**. hier können Sie dann unter **Lautsprecher** aus den angeschlossenen Ausgabegeräten, unter **Mikrofon** die Eingabegeräte und unter **Kamera** die Kameras.

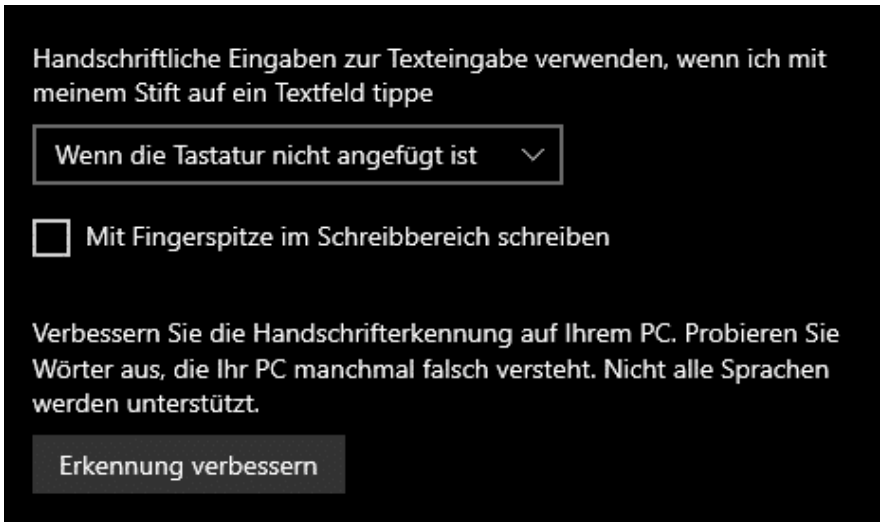


Manchmal sind die Geräte aber komplett autark und lassen sich nicht mit Ihrem PC verbinden, beispielsweise Konferenzspinnen mit Mikrofon und Lautsprecher. Wenn Sie in einem solchen Umfeld sind, dann fahren Sie einfach zweigleisig: Wählen Sie sich sowohl mit der Konferenzspinne ins Meeting ein als auch mit Ihrem eigenen Gerät. Bei letzterem schalten Sie sowohl den Lautsprecher als auch das Mikrofon aus. Die nutzen Sie ja mit den Anderem im Raum über die Konferenzspinne.

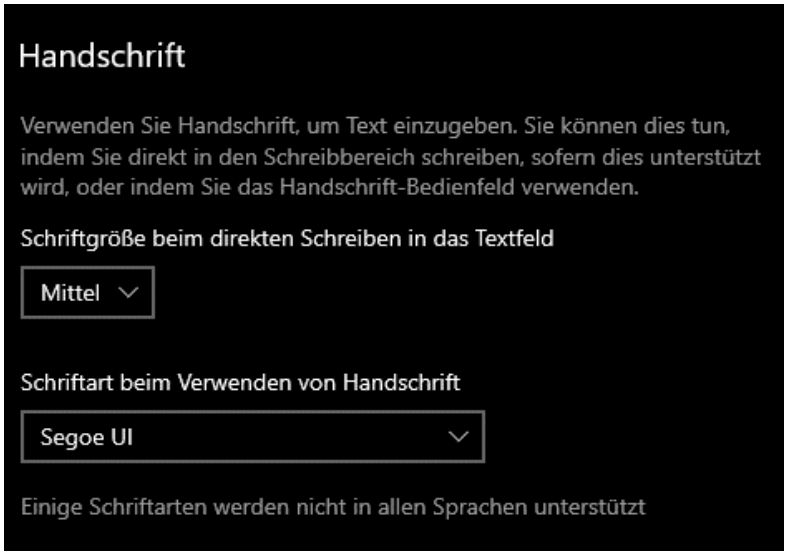
Handschrifterkennung bei Windows effektiv nutzen

Den Traum gibt es schon seit Jahrzehnten: Für die Texteingabe ist die Tastatur das Standard-Eingabegerät, was nicht der natürlichen Schreibart des Menschen entspricht. Von Kindesbeinen an sind wir darauf getrimmt, mit einem Stift auf Papier zu schreiben. Das ist erst seit einigen Jahren eine echte Option am PC, und Windows 10 unterstützt dies schon in der Standardinstallation. Wir zeigen Ihnen, wo Sie Einfluss nehmen können.

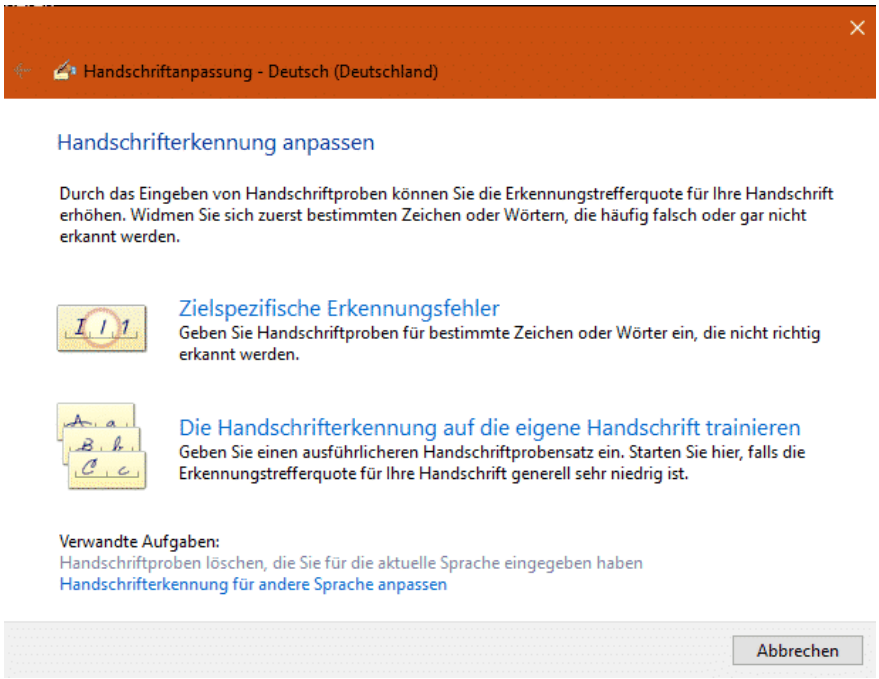
Unter **Einstellungen** > **Windows Ink** können Sie die Einstellungen für die Handschrifteingabe bei Windows verändern. Wenn Sie ein Gerät wie ein Microsoft Surface Pro oder ein anderes Tablet mit abnehmbarer Tastatur haben, dann sollen Sie unter **Handschriftliche Eingaben zur Texteingabe verwenden, wenn ich mit meinem Stift auf ein Textfeld tippe** festlegen, ob der Stift auch verwendet werden soll, wenn die Tastatur angeschlossen ist. Normalerweise nutzen Sie entweder Tastatur oder Stift!



Unter **Handschrift** können Sie einstellen, in welcher Schriftart und in welcher Größe der Text angezeigt werden soll, der aus der Handschrifteingabe erzeugt wird.



Um die Handschrifterkennung stärker auf Ihre persönlichem individuelle Handschrift anzupassen, können Sie die Erkennung trainieren. Dazu klicken Sie auf **Erkennung verbessern** und dann auf die **Handschrifterkennung auf die eigene Handschrift trainieren**. Die hier investierte Zeit ist gut verwendet: Schon mit wenigen Durchläufen wird die Erkennung spürbar besser!

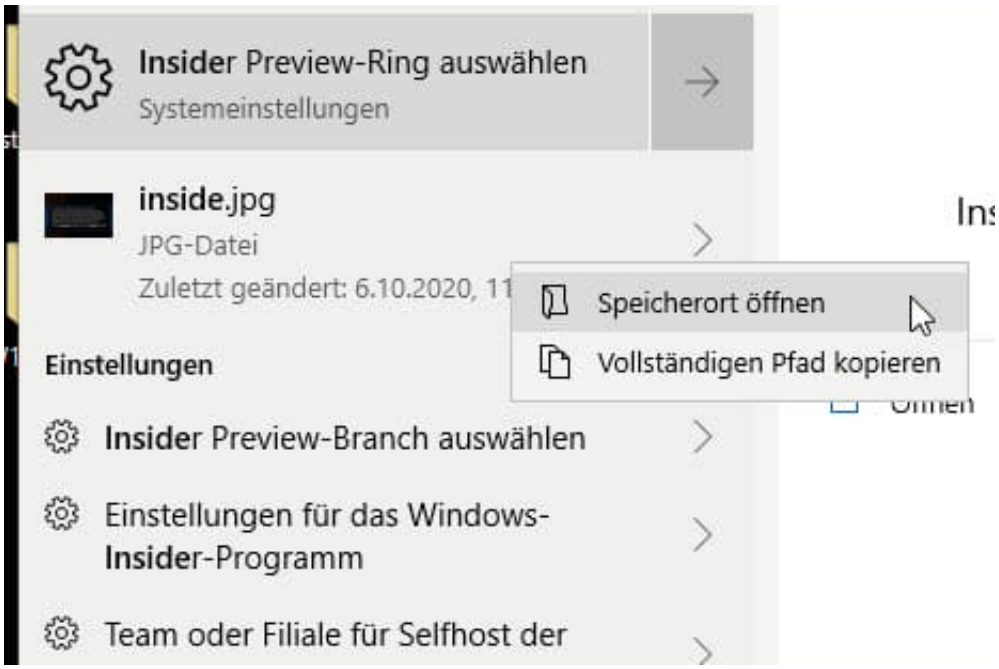

Handschriftanpassung - Deutsch (Deutschland)
Handschrifterkennung anpassen
Durch das Eingeben von Handschriftproben können Sie die Erkennungstrefferquote für Ihre Handschrift erhöhen. Widmen Sie sich zuerst bestimmten Zeichen oder Wörtern, die häufig falsch oder gar nicht erkannt werden.
Zielspezifische Erkennungsfehler
Geben Sie Handschriftproben für bestimmte Zeichen oder Wörter ein, die nicht richtig erkannt werden.
Die Handschrifterkennung auf die eigene Handschrift trainieren
Geben Sie einen ausführlicheren Handschriftprobensatz ein. Starten Sie hier, falls die Erkennungstrefferquote für Ihre Handschrift generell sehr niedrig ist.
Verwandte Aufgaben:
Handschriftproben löschen, die Sie für die aktuelle Sprache eingegeben haben
Handschrifterkennung für andere Sprache anpassen
Abbrechen

Wo sind meine Dateien?

Selten haben Sie Ruhe, um eine Arbeitssitzung an Ihrem PC in Ruhe zu absolvieren. Das führt schnell dazu, dass Sie Dateien erzeugen und speichern, und diese später nicht wiederfinden. Auf Speichern klicken geht schnell, den Pfad, in den die Datei gespeichert wird, zu kontrollieren, kostet mehr Zeit und geht schnell unter. Keine Sorge, die Datei finden Sie trotzdem schnell wieder!

Ganz einfach ist das, wenn Sie ein Office-Programm verwenden: Wenn sie darin auf **Datei** > **Öffnen** > **Zuletzt verwendet** klicken, dann bekommen Sie die letzten Dateien angezeigt und können diese durch einen Klick öffnen. Auch viele andere Windows-Programme bieten diese Funktion.

Wenn das Programm, mit dem Sie gearbeitet haben, diese Funktion nicht hat, dann hilft folgendes Vorgehen: Klicken Sie in das Suchfeld unten links in der Taskleiste und heben Sie den Namen (oder einen Teil davon) ein. Windows zeigt Ihnen nun die Datei als Suchergebnis an.



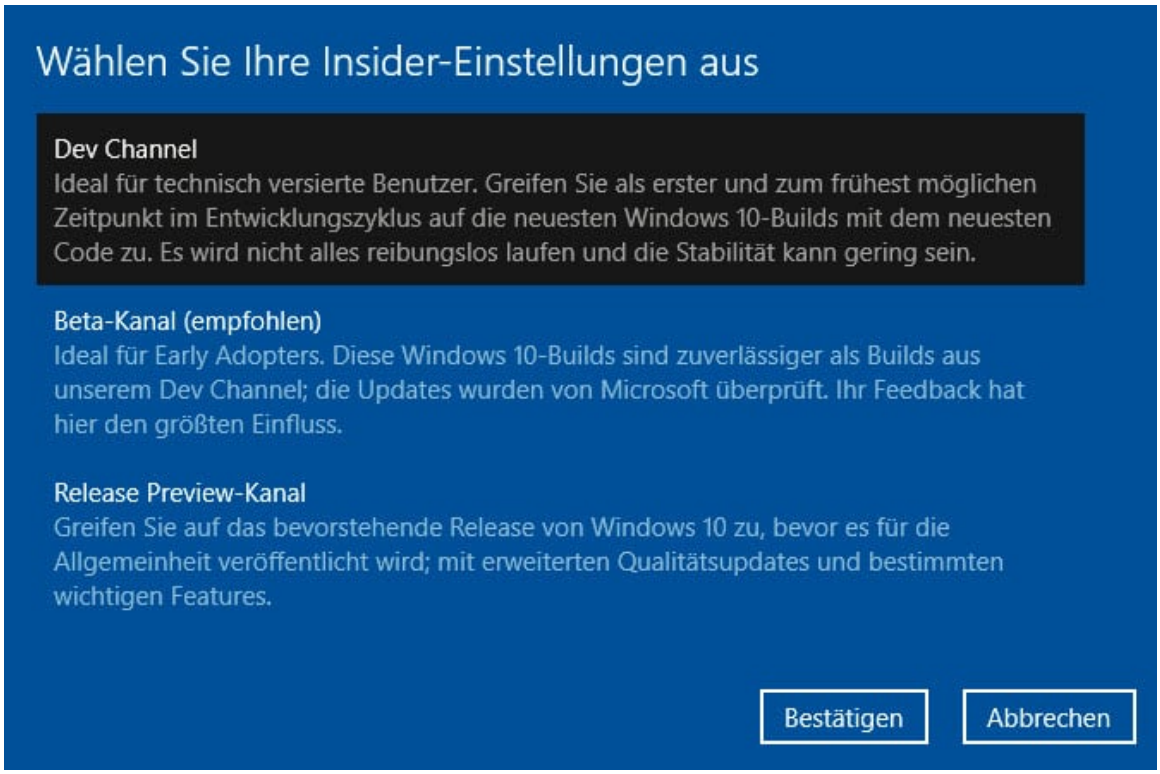
Klicken Sie mit der rechten Maustaste auf den Dateinamen und dann auf **Speicherort öffnen**. Windows öffnet das Verzeichnis, in dem die Datei sich befindet. Sie können die Datei dann an einen anderen Ort verschieben oder öffnen. Das Verzeichnis finden Sie im Explorer-Fenster ganz oben in Klarschrift.

Windows-Versionen früher bekommen: Das Insider-Programm

Windows 10 unterliegt stetigen Änderungen. Neue Funktionen kommen hinzu, Fehler werden behoben, alles wird - hoffentlich - besser. Manche der schon im Vorfeld kommunizierten Änderungen erwarten Sie ungeduldig, müssen aber warten, bis Microsoft diese freigibt und das Update an die Endbenutzer ausrollt. Das müssen Sie nicht: Mit wenig Aufwand können Sie schon vorab neue Versionen installieren!

Diese mittlerweile fest in Windows 10 integrierte Funktion heißt Windows-Insider-Programm. Sie finden Sie in den Einstellungen von Windows unter **Update und Sicherheit** > **Windows-Insider-Programm**. Um sie nutzen zu können, müssen Sie bei den Diagnosedaten auswählen, dass alle Daten an Microsoft gegeben werden - schließlich soll ja Microsoft auch das Verhalten Ihres Systems überwachen können. Ist das nicht der Fall, dann bekommen sie einen Hinweis und können dies einschalten.

Nach der Anmeldung können Sie dann den Kanal auswählen, aus dem Sie die Vorab-Versionen beziehen wollen. Der **Dev Channel**, der **Beta-Kanal** und der **Release-Preview-Kanal** unterscheiden sich im Hinblick auf die Stabilität: Im Dev Channel bekommen Sie sehr frühe Versionen, die gegebenenfalls noch instabil sind. Im Release-Preview-Kanal bekommen Sie neue Versionen erst später. Diese sind aber deutlich besser getestet und stabiler.


Wählen Sie Ihre Insider-Einstellungen aus
Dev Channel
Ideal für technisch versierte Benutzer. Greifen Sie als erster und zum frühest möglichen Zeitpunkt im Entwicklungszyklus auf die neuesten Windows 10-Builds mit dem neuesten Code zu. Es wird nicht alles reibungslos laufen und die Stabilität kann gering sein.
Beta-Kanal (empfohlen)
Ideal für Early Adopters. Diese Windows 10-Builds sind zuverlässiger als Builds aus unserem Dev Channel; die Updates wurden von Microsoft überprüft. Ihr Feedback hat hier den größten Einfluss.
Release Preview-Kanal
Greifen Sie auf das bevorstehende Release von Windows 10 zu, bevor es für die Allgemeinheit veröffentlicht wird; mit erweiterten Qualitätsupdates und bestimmten wichtigen Features.
Bestätigen
Abbrechen