

A portrait of a man with short brown hair and a slight smile, wearing a teal button-down shirt. He is positioned on the left side of the frame, with his arms crossed. The background is dark. The text 'Schieb Report' is overlaid on the right side in large white font.

Schieb Report

Ausgabe 2018.46

Berlin fördert KI mit drei Milliarden: Was steckt dahinter?

Drei Milliarden Euro will die Bundesregierung bereitstellen, um [die KI-Forschung in Deutschland zu fördern](#). "Hurra, ein Lebenszeichen!", will man da ausrufen. Denn das Thema Digitalisierung spielt in Berlin ansonsten nicht die geringste Rolle. Keine Visionen, nichts zur Abwehr von Gefahren. Es gibt schlichtweg kein ressortübergreifendes Konzept. Daran ändert auch die Tatsache wenig, dass nun drei Milliarden locker gemacht werden.

Das offiziell gesteckte Ziel: Deutschland zum führenden Forschungsstandort für Künstliche Intelligenz (KI) zu machen. Das ist ehrenwert. Allerdings wird sich das Ziel kaum erreichen lassen. Aus vielen Gründen. Unter anderem, weil die anderen schon viel weiter sind. Die Amerikaner natürlich. Aber vor allem die Chinesen.



Wo bleibt die Ethik?

Die geben richtig Gas - und stecken unfassbar hohe Beträge in die Entwicklung. Sie setzen ihre Systeme auch einfach so gegen ihre eigene Bevölkerung ein. Stichwort: Komplettüberwachung und Scoring-Systeme in China. Skrupel gibt es keine.

Wollen wir das hier auch? Es ist fast schon anrührend, wie begeistert und Wirtschaftsminister Peter Altmaier von der Kölner Firma DeepL berichtet, die ein fraglos ungeheuer gutes Übersetzungssystem entwickelt hat (ich habe [hier schon darüber berichtet](#)). Altmaier freut sich dann, ist stolz wie Oskar, wie ein Papa auf seine Kinder: Seht her, ja, das wurde tatsächlich in Deutschland entwickelt.

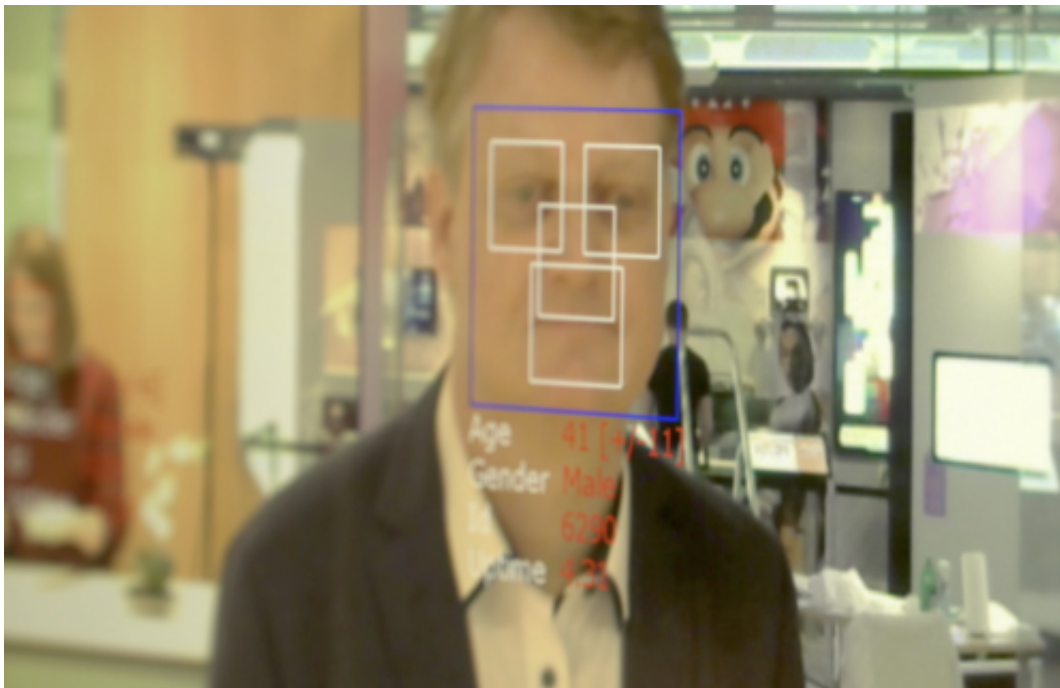
<https://vimeo.com/297276960>

Interview mit Dr. Viehoff zum Thema KI

Es fehlt an Visionen und Strategien

Allerdings sollte es nicht nur um die Weiterentwicklung dieser Systeme gehen. Das ist klug, aus wirtschaftlichen Gesichtspunkten. Es muss auch um ethische Fragen gehen: Was sollen Algorithmen allgemein dürfen, was KI im Besonderen? Welche Grenzen soll es geben? Wie bewertet man die Systeme, die uns bewerten? Wie lässt sich so etwas international aufhängen? Am besten sogar bei den Vereinten Nationen (UN)? Es gibt keinen einzigen Politiker, der an so etwas auch nur denkt, geschweige handelt.

Zwar heißt es auch in Berlin, dass im Sinne des "demokratischen Anspruchs" eine "verantwortungsvolle und gemeinwohlorientierte Entwicklung und Nutzung von KI" ermöglicht werden soll und in einem breiten gesellschaftlichen Dialog "ethisch, rechtlich und kulturell" debattiert werden soll. Immerhin.



Doch wie wäre es mit vorausschauender Politik? Mitdenken. Weiterdenken. Handeln. Nicht: Drei Milliarden Euro locker machen, weil es die anderen auch tun. Das ist keine Gestaltung. Das ist ein Sich-von-anderen-treiben-lassen. Sollte dieser Schritt jetzt ein "Awakening" sein, also nur eine Art erster Reflex, der Beginn für etwas für Neues, dann wäre ich zufrieden. Aber ich fürchte, genau das Gegenteil passiert: "Aber wir haben doch die KI gefördert", werden wir zu hören bekommen. Genug getan. Thema Digitalisierung abgeschlossen.

Google macht Werbung für seine Werbung

Google lebt vor allem von Werbung. Das wissen wir - und akzeptieren das zu einem großen Teil auch. Deshalb ist es für Google wichtig, dass wir dem Unternehmen vertrauen. Aber welche Daten werden eigentlich gespeichert, welche Daten erhoben - welche Schlüsse gezogen? Zumindest teilweise verrät uns Google das - im Dashboard. Eine aktuelle PR-Kampagne soll uns motivieren, unsere Daten zu kontrollieren und die passenden Einstellungen vorzunehmen.

Wenn Online-Konzerne wie Facebook oder Google Anzeigen in Zeitungen und Magazinen schalten oder sogar in der Öffentlichkeit Plakate aufhängen, dann fällt einem das einfach auf. Es wirkt ein bisschen ungewohnt, fast wie ein Fremdkörper. Denn was hat [Google](#) an meiner Bushaltestelle verloren? Die wissen doch sowieso, dass ich hier gerade stehe - und wohin ich will. Ja selbst, ob ich spät dran bin. Wieso auch noch ein Plakat?



Dashboard: Eine Art Regiezentrale der Privatsphäre

Ein Blick auf das Plakat verrät, warum Google das macht: Google will uns davon überzeugen, uns mehr für unsere Privatsphäre und unsere Belange einzusetzen. Schon seit Jahren bietet Google im sogenannten [Dashboard](#) die Möglichkeit, eine ganze Menge über sich selbst in Erfahrung zu bringen.

Was speichert Google eigentlich über mich? Und zu welchen Schlüssen kommt Google dadurch? Wer sich mal in die Untiefen des Dashboards begibt und im Angebot stöbert, staunt nicht schlecht, was er dort alles erfährt.



Etwa: Welche Suchbegriffe habe ich in die Suchmaschine eingegeben? Aber auch wann, wo und womit (welches Gerät)? Welche YouTube-Videos habe ich mir angeschaut und wie lange?

Welche Fragen habe ich Google Home oder dem Assistenten gestellt? (Das kann ich mir sogar anhören.) Wo habe ich mich wann und wie lange aufgehalten? Welche Google-Dienste habe ich benutzt? Es sind jede Menge Daten. Vor allem, wenn ich ein Android-Gerät verwende.

<https://vimeo.com/300493927>

Die eigene Datenpflege macht Aufwand

Gut ist, dass man als Benutzer auch einiges ändern kann. Einzelne Daten lassen sich löschen. Oder ich kann Google sagen, sich bestimmte Dinge nicht mehr zu merken, etwa welche Videos ich mir anschau oder welche Suchbegriffe ich eingebe.

Spannend wird es in der Abteilung "Werbeanzeigen". Denn hier sieht man, welche Themen Google mit einem verbindet, welche "auf die persönlichen Interessen zugeschnittene Werbeanzeigen" einem präsentiert werden. Lässt sich alles abschalten.

Die im Mai in Kraft getretene Datenschutz-Grundverordnung (DSGVO) zwingt Google dazu, solche Einblicke zu gewähren. Und einiges bot Google schon vor der DSGVO an. Ausreichend ist das zwar noch nicht (so sollten wir mehr über das Thema KI erfahren), aber ein Anfang. Allerdings machen nur vergleichsweise wenige Menschen von diesen Möglichkeiten Gebrauch. Denn die Datenpflege macht durchaus Mühe.

Doch jeder sollte es tun. So, wie man auch seinen Keller aufräumt. Oder seine Garage.

Wie gerecht ist das Internet?

Themenwoche [Gerechtigkeit in der ARD](#). Grund genug, sich mal zu fragen, ob das Internet die Welt eigentlich gerechter macht - oder ungerechter. Schließlich hat das Internet mittlerweile nahezu alle Bereiche unseres Lebens erobert. Das Internet hat die Herrschaft über uns - nicht umgekehrt.

Als sich das Internet Anfang der 90er-Jahre für die Allgemeinheit öffnete, waren die Hoffnungen groß: Das Wissen der Welt, für alle verfügbar – wie verlockend das klingt. Jeder ist mit jedem vernetzt, wenn er mag.

[caption id="attachment_756826" align="alignnone" width="500"]



[geralt](#) /

Pixabay[/caption]

Große Hoffnungen - wurden enttäuscht

Und: Jeder hat im Internet eine Stimme. Diese Ansätze lassen durchaus den Eindruck entstehen, das Internet könnte die Welt ein bisschen gerechter machen. Schon allein deswegen, weil die Mächtigen dadurch nicht mehr so mächtig sind. Weil sich jeder mitteilen kann. Zum Teil stimmt das auch.

Allerdings gibt es nun neue Mächte. Mächte, die nicht nur das Internet beherrschen, sondern in der gesamten Welt den Takt angeben. Unternehmen wie Google, Apple, [Facebook](#) und Amazon. An ihnen führt heute kaum ein Weg vorbei.

Selbst Regierungen haben mit diesen Unternehmen ihre liebe Not. Man muss nur sehen, wie Facebook die Regierenden am Nasenring durch die Arena führt. Doch Regierungen sind gewählt (meistens) - Unternehmen nicht.

Hat das Internet die Welt also gerechter gemacht? Ganz sicher nicht.

<https://vimeo.com/300251489>

Das Netz macht die Welt eher ungerechter

Das neue Analphabetentum

Wer keinen Zugang hat - und das ist weltweit fast die Hälfte der Bevölkerung -, hat schlechtere Bildungs- und Arbeitschancen. Das gilt sogar hierzulande für Betriebe auf dem Land, die nicht gut ans Netz angebunden sind. Kein Internet zu haben, das ist das neue Analphabetentum.

Selbst wer Zugang zum Netz hat: Es besteht das Risiko der Ausbeutung. Das Netz verschafft Unternehmen in reichen Ländern die Möglichkeit, Menschen in armen Ländern zu billigen Arbeitskräften zu machen. Stichwort: [Mechanical Turk von Amazon](#).

Für Centbeträge die Arbeit machen, die sonst keiner machen will. Oder noch günstiger. Das Internet ruiniert Arbeitsplätze in aller Welt - und drückt den Lohn. Beispiel: Amazon. Jeff Bezos' Onlinekonzern kann wohl mit Fug und Recht als Hinrichter von Millionen Arbeitsplätzen im Einzelhandel bezeichnet werden.

<https://soundcloud.com/user-999041145/macht-das-internet-die-welt-gerechter-nein>

Wie gerecht Algorithmen sind

Man darf sich nicht täuschen lassen: Kleinere Erfolge oder Vorteile machen die globale Entwicklung nicht wett. Das Internet fördert den Turbokapitalismus. Die Machtzentralen sitzen im Silicon Valley. Dort fließt das Geld hin - und wird kaum versteuert. Der Kommerz hat das Internet fest im Würgegriff. Nahezu alles im Netz ist dem Kommerz unterworfen. Deshalb machen Algorithmen sichtbar, was Klicks und Geld bringt - nicht das, was wahr ist und die Welt schlauer macht. Gerecht ist das nicht.

Heute schon gehackt worden? Bestimmt

Wir werden rund um die Uhr gehackt. Bots hacken uns. Hacker hacken uns. Und allzu oft klappt es auch – und wir merken es nicht einmal. Grund genug, der Sache mal auf den Grund zu gehen: Wie ist es um die eigene Sicherheit bestellt – und was kann ich unternehmen?

Wenn Hacker hacken, dann geschieht das in der Regel unsichtbar. Wir bekommen zumindest davon nichts mit. Doch die Hackangriffe lassen sich sichtbar machen. Sicherheitsfirmen registrieren Hackangriffe jeder Art weltweit – und zeigen sie zu Beispiel in [solchen Onlinekarten](#). Millionen von Angriffen jeden Tag. Rund um die Uhr.



Die Karten zeigen nicht jeden tatsächlichen Angriff, der gerade stattfindet, das geht gar nicht. Aber sie registrieren eine Menge davon – und so lassen sich Tendenzen erkennen. Wer hackt gerade besonders viel, welche Methoden werden angewandt, wer ist beliebtes Ziel.

Deutschland ist ein begehrtes Ziel

Deutschland ist auf Platz 2 der am häufigsten attackierten Ziele.

Und wenn ich Deutschland sage, dann meine ich nicht nur Behörden, Regierung und Firmen. Alle Ziele in Deutschland sind attraktiv. Auch unsere Rechner. Unsere Smartphones. Unsere vernetzten Geräte. Unsere Onlinekonten. Alles ist reizvoll und interessant.

Deshalb sollte man sich schützen. Wichtig ist zum Beispiel, regelmäßig zu prüfen, ob die eigenen Profile und Konten von Fremden benutzt werden. E-Mail. Facebook. Instagram. Google. Das kann man durchaus herausfinden.

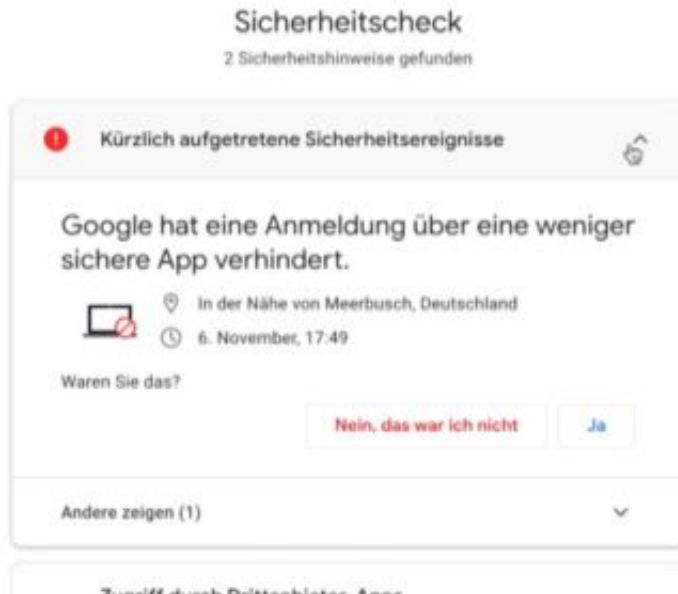


Google warnt auf Wunsch bei auffälligen Logins

Bei Google zum Beispiel kann man im [Google Dashboard](#) genau sehen: Wann wurde sich über das Konto eingeloggt – und wo? Bei Facebook und anderen Onlinediensten funktioniert das ganz ähnlich. Jeder kann sich selbst fragen: Passt das? War ich an diesem Tag in Köln? Oder – wie hier – Singapur? Falls da etwas nicht stimmt: Sofort die Zugangsdaten ändern, also vor allem das Passwort.

Mein Tipp: Man kann sich bei Google, Facebook, Twitter und Co. auch warnen lassen, wenn die eigenen Zugangsdaten an einem ungewöhnlichen Ort oder an einem neuen Gerät verwendet werden. Von einem Fremden, der die Daten geklaut hat zum Beispiel. Man bekommt dann eine Warn-Mail – und kann entscheiden, was man tun möchte.

Ich kann nur empfehlen, das zu machen. Denn niemand möchte, dass sich Fremde einfach so Zugang verschaffen und Onlinekonten missbrauchen.

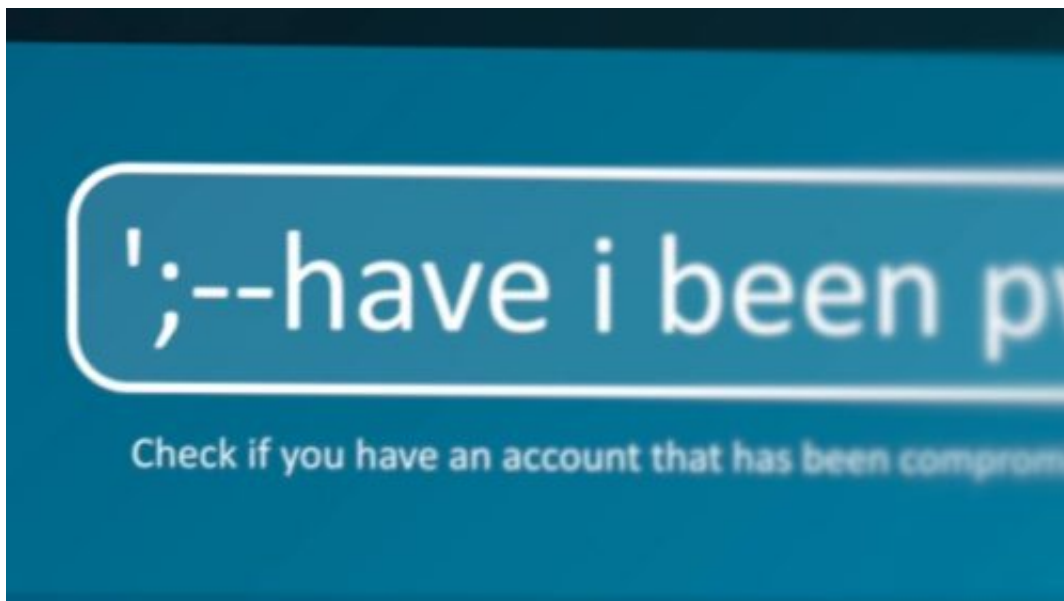


Wenn Hacker sich die Logindaten besorgen

Jetzt werden sich viele denken: Wie kommen denn Fremde überhaupt an meine Zugangsdaten?

Die Antwort: Das ist leider gar nicht so schwer – und kommt häufiger vor, als man denkt.

Zugangsdaten können auf den eigenen Geräten geklaut werden, etwa durch eingeschmuggelte Abhör-Software. Keylogger. Oder die Passwörter sind schlecht. Oder: Hacker brechen in die Server großer Unternehmen ein und holen sich die die Daten. Davon bekommt man als Betroffener in der Regel nichts mit, weil man nicht gewarnt wird.



Es gibt aber einen Weg, das herauszufinden. [Have I been Pwned](https://haveibeenpwned.com/). Eine Webseite, die einem verrät, ob man schon mal Opfer gewesen ist.

["Have I Been Pwned"](#) sollte jeder mal besuchen. Ein äußerst seriöser Dienst: Man gibt seine Mail-Adresse ein – und erfährt sofort, ob, wann und wo die eigenen Nutzerdaten schon mal in die Netze von Hackern gelangt sind. Mit detaillierten Infos. Spätestens jetzt sollte man das Passwort ändern

Unbedingt vorbereitet sein

Man muss nicht Bundeskanzlerin sein, um Opfer von Hackangriffen zu werden. Es kann jeden treffen. Ein paar Vorsichtsmaßnahmen können helfen. Deshalb bitte die eigenen Onlinekonten optimal absichern. Und regelmäßig überprüfen, dass Fremde sich nicht einloggen. Damit ist schon viel erreicht.

iPhone: App-Ordner ohne Namen

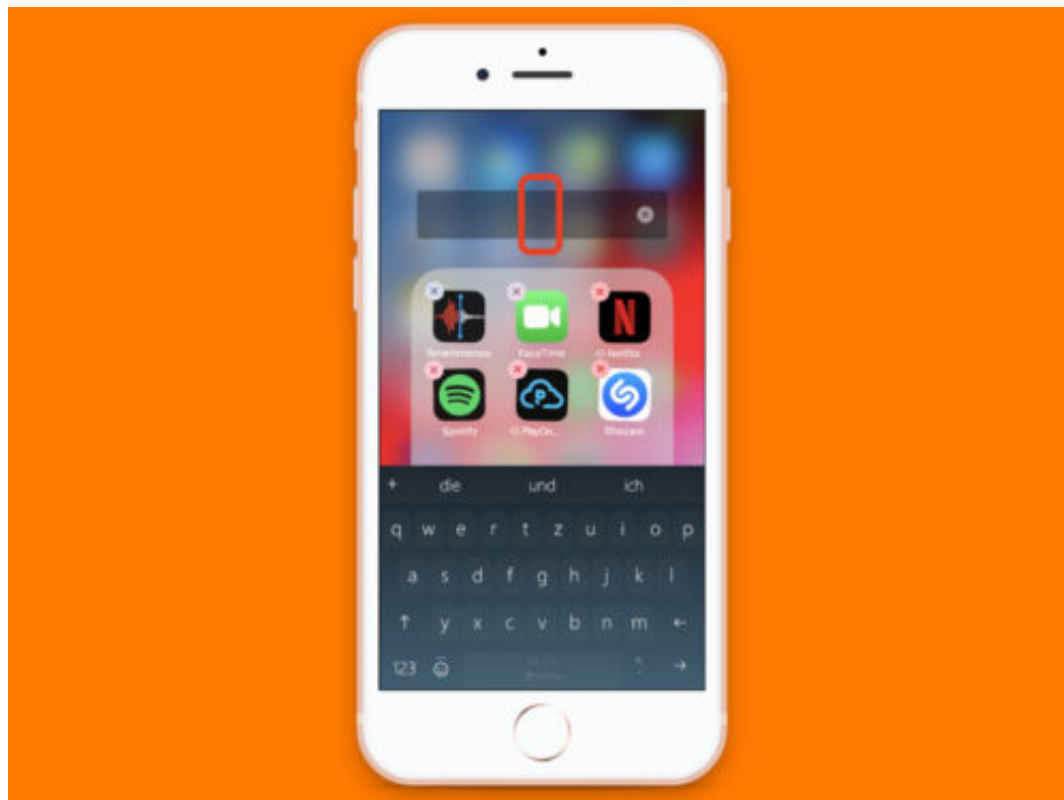
Wer keine Unordnung auf dem Home-Bildschirm von iPhone und iPad haben will, räumt auf. Besonders nützlich dafür sind die Ordner, die sich durch Aufeinanderziehen einzelner App-Symbole anlegen lassen. Allerdings müssen diese Ordner mit einem Namen versehen werden. Sauberer sieht's aber ohne Namen aus – das geht mit einem Trick.

Wird ein App-Icon mit dem Finger auf ein anderes gezogen, erstellt iOS aus den beiden Symbolen einen Ordner und legt sie hinein. Dieser Ordner kann benannt werden, indem er zunächst geöffnet wird, dann oben auf die Beschriftung tippen, sodass die Tastatur eingeblendet wird.

Wer hier aber keinen Namen für den Ordner eingeben möchte, kann stattdessen ein besonderes, transparentes Zeichen eingeben. Es lässt sich zwischen den beiden folgenden X-Zeichen kopieren:

X ?X

Wer dieses transparente Zeichen als Namen für den iOS-Ordner angibt, erhält damit effektiv einen namenlosen Ordner.



USB-Sticks verschlüsseln

USB-Sticks können leicht verloren gehen und/oder gestohlen werden. Das bedeutet, dass alles auf Ihren USB-Sticks eine Art Verschlüsselung haben muss, um Diebe und Schnüffler abzuschrecken. Mit VeraCrypt lässt sich das schnell einrichten.

Schließen Sie zunächst Ihren USB-Stick an Ihren Computer an. Als nächstes laden Sie VeraCrypt herunter, installieren und öffnen es. Klicken Sie auf **Volume erstellen**. Wählen Sie die zweite Option zum Erstellen eines Volumes innerhalb einer Partition/eines Laufwerks. Wählen Sie nun **Gerät auswählen**. Geben Sie Ihr Administrator-Passwort ein und wählen Sie das Gerät aus, das Sie verschlüsseln möchten.

Sie werden dann gewarnt, dass durch die Verschlüsselung des Laufwerks alles gelöscht wird, was sich derzeit auf dem Laufwerk befindet. Wenn Sie also etwas Wichtiges dabei haben, sichern Sie es zuerst, dann klicken Sie auf **Ja**.

Als nächstes kommen die Verschlüsselungsoptionen. Wenn Sie den Unterschied zwischen den einzelnen Verschlüsselungsprotokollen nicht kennen, entscheiden Sie sich für Standard-AES und den SHA-512-Hash-Algorithmus.

Passwort definieren

Nun zum wichtigsten Teil: Das Passwort. Erstellen Sie ein 25-30-stelliges Passwort, Großbuchstaben, Kleinbuchstaben, Zahlen, Symbole. Klicken Sie auf **Passwort anzeigen**, um sicherzustellen, dass Sie es richtig eingegeben haben.

Als nächstes generieren Sie starke Verschlüsselungscodes, indem Sie Ihre Maus zufällig durch das VeraCrypt-Fenster bewegen. Wenn der blaue Balken bis zum Ende geht, klicken Sie auf **Format** und beobachten Sie, wie VeraCrypt die Arbeit erledigt.

Sie sehen nun, wie Ihr USB-Gerät formatiert wird und wie viel Zeit noch bis zum Ende bleibt. Dann ist es erledigt! Klicken Sie auf **OK**, um den Formatierungsassistenten zu beenden.



Besser mobil mit 2 SIMs

Viele Angestellte haben eine private und eine geschäftliche Handy-Nummer. Wer auf beiden erreichbar sein will, ohne ständig zwei mobile Geräte mit sich herumzuschleppen, richtet entweder eine Ruf-Weiterleitung ein – oder nutzt ein Handy mit 2 SIM-Slots.

Wenn zwei SIM-Karten in einem Handy genutzt werden können, hat das noch weitere Vorteile: die eine kann zu einem normalen Smartphone-Tarif gehören, für die andere lässt sich auch ein Daten-Tarif mit passendem Inklusiv-Volumen nutzen. Auch im Nicht-EU-Ausland nützt das: So bleibt die eigene deutsche Nummer erreichbar, und trotzdem kann eine lokale Daten-SIM zum Surfen zum Einsatz kommen, um Roaming zu vermeiden.

Dual-SIM-Geräte gibt es im Moment nur von Android – bei Apple verstehen sich die neuen iPhones zwar auch auf Dual-SIM, eine davon ist allerdings eine eSIM, die sich über den Mobilfunk-Anbieter programmieren lassen wird.



Externe IP über die Konsole herausfinden

Die Eingabeaufforderung unter Windows 10 enthält ein nützliches Tool namens ipconfig, mit dem Sie IP-Adresse, Netzwerk-Infos und weitere Daten abrufbar sind. Die IP-Adresse, die hier zu sehen ist, ist jedoch nicht die externe IP-Adresse des Systems. Mit einem Trick kann in der Konsole auch die externe IP ermittelt werden.

Das ipconfig-Tool kann Ihnen nicht sagen, was Ihre externe IP ist. Das liegt daran, dass Sie meist nicht direkt mit dem Internet verbunden sind. Ihr Router fungiert als Vermittler, weshalb diese Informationen nicht nachgeschlagen werden können. Es gibt jedoch eine einfache Lösung.

Externe IP-Adresse aus der Eingabeaufforderung

Was Sie tun müssen, ist, Ihre externe IP von einem Server zu beziehen, der sie sehen kann. Ihre externe IP ist nicht vor Websites verborgen, es sei denn, Sie maskieren sie mit einem VPN unter Windows zum Schutz der Privatsphäre. Der Trick besteht darin, eine Website zu finden, die auch diese Informationen in der Eingabeaufforderung wiedergeben kann. Um dies zu tun, führen Sie den folgenden Befehl aus:

```
nslookup myip.opendns.com resolver1.opendns.com [Enter]
```

Dadurch wird Ihre externe IP-Adresse aus Sicht von opendns.com zurückgegeben. OpenDNS ist im Grunde genommen genau das; ein offenes und kostenloses DNS, das Sie verwenden können, wenn Sie wollen. Es ist ein Server, der, wie alle anderen Websites, Ihre externe IP-Adresse sehen kann und diese Informationen für Sie anzeigen kann.

Administrator: Eingabeaufforderung

```
C:\WINDOWS\system32>nslookup myip.opendns.com resolver1.opendns.com
Server: resolver1.opendns.com
Address: 208.67.222.222

Nicht autorisierende Antwort:
Name: myip.opendns.com
Address: 84.132.103.64

C:\WINDOWS\system32>
```

Word: Keine geschützte Ansicht

Wer aus dem Internet oder mit eMail ein Word-Dokument erhält und dieses dann auf dem eigenen PC öffnet, sieht zuerst die „Geschützte Ansicht“. Bearbeiten lässt sich die Datei damit allerdings nicht. Dazu muss immer erst oben auf „Bearbeiten aktivieren“ geklickt werden. Für einzelne Dateien lässt sich die Markierung auch dauerhaft abschalten.

Damit Word ein Dokument aus dem Internet nicht mehr in der geschützten Ansicht öffnet, folgende Schritte ausführen:

1. Zunächst ein neues Explorer-Fenster öffnen.
2. Nun den Ordner öffnen, in dem die Datei liegt.
3. Dann mit der rechten Maustaste auf das Dokument klicken und dessen **Eigenschaften** aufrufen.
4. Hier findet sich auf der Registerkarte **Allgemein** bei Internet-Dokumenten ein **Zulassen**-Kästchen, in das ein Haken gesetzt wird.

Sobald unten mit **OK** bestätigt wird, entfernt das System den NTFS-Hinweis, dass die Datei aus dem Internet stammt – und Word wechselt nicht mehr in die Geschützte Ansicht.



Text in Tabellen ausrichten

Texte in Word auszurichten ist eine Sache weniger Klicks: Einfach oben im Menü auf Start klicken, dann kann der markierte Text links, rechts, zentriert oder im Blocksatz ausgerichtet werden. Ähnlich klappt's auch in Tabellen.

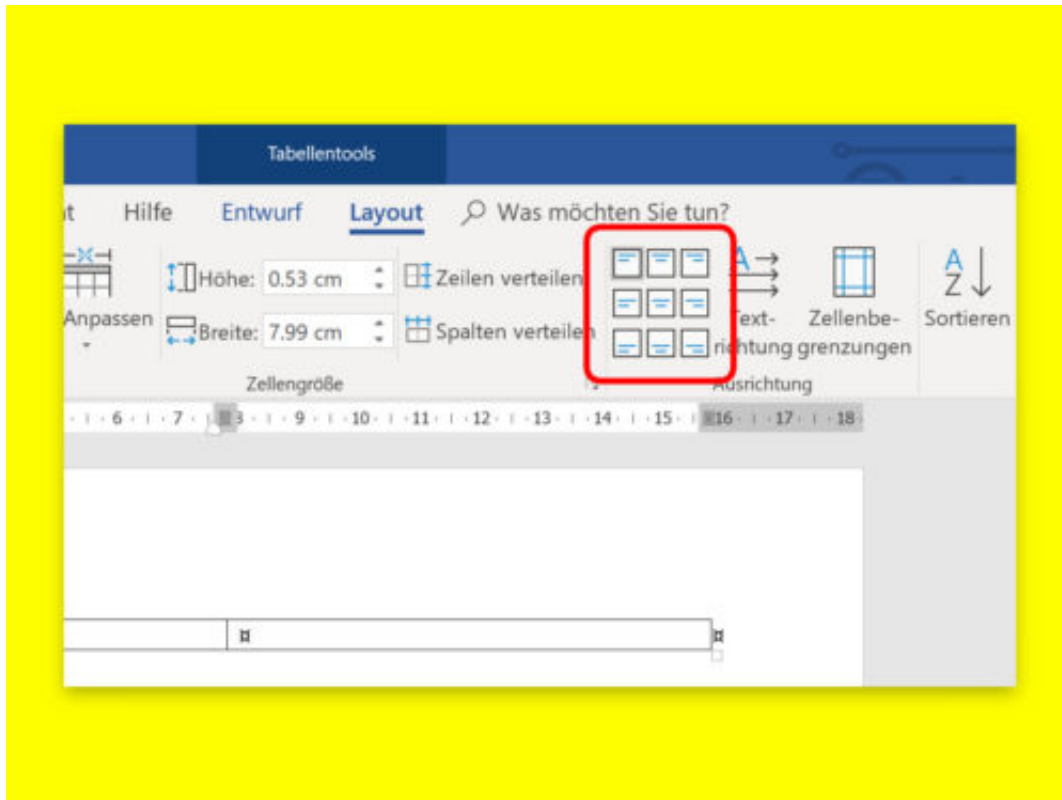
Wenn Sie eine Tabelle erstellen und Text in den verschiedenen Zellen eingeben, ist sie immer links ausgerichtet. Die Ausnahme ist, wenn Sie in einer Sprache schreiben, die von rechts nach links schreibt – in diesem Fall wird der Text immer nach rechts ausgerichtet.

Bei Tabellenzellen sind zwei Ausrichtungen zu berücksichtigen: die linke/rechte/zentrische Ausrichtung, die in Bezug auf den linken und rechten Rand der Zelle gemessen wird, und die obere/zentrische/untere Ausrichtung, die in Bezug auf den oberen und unteren Rand der Zelle gemessen wird. Standardmäßig ist der Text links und oben in der Zelle ausgerichtet.

Ausrichtung über Kontext-Tab im Menü

Um sie zu ändern, klicken Sie innerhalb der Zelle, für die Sie die Textausrichtung ändern möchten. Dadurch werden die beiden Registerkarten aktiviert, mit denen Sie die Tabelle anpassen können. Gehen Sie auf die Registerkarte Layout und Sie werden feststellen, dass es dort einen Bereich für die Ausrichtung gibt.

Die Alignment Toolbox verfügt über neun Schaltflächen zum Ausrichten von Text in einer Tabelle in Microsoft Word. Von links nach rechts und von oben nach unten können Sie mit den Schaltflächen den Text nach rechts und oben, nach oben, nach Mitte und oben sowie nach links und oben ausrichten. In der zweiten Zeile können Sie den Text nach rechts ausrichten, aber von oben zentrieren, den Text von rechts und oben zentrieren, den Text nach links ausrichten und von oben zentrieren. In der dritten Zeile können Sie den Text links und unten in der Zelle ausrichten, den Text von rechts und unten in der Zelle zentrieren und schließlich den Text links und unten in der Zelle ausrichten.



Symbol-Vorschau reparieren

Windows 10 zeigt für bestimmte Dateitypen im Datei-Explorer eine Vorschau an. Für andere Dateien verwendet das System ein generisches Symbol, z. B. das gelbe Ordnersymbol, um Ordner darzustellen. Windows 10 verfügt dafür über einen Icon-Cache. Leider kann dieser Icon-Cache beschädigt werden.

Wenn das passiert, fehlen Symbole an allen möglichen Stellen im System. Um dies zu beheben, müssen Sie die Datenbank des Icon-Cache neu erstellen. Hier ist die Vorgehensweise.

Icon-Cache neu aufbauen

Dies führt nicht zu einem Datenverlust, aber Sie sollten alle Anwendungen und Dateien schließen, die Sie geöffnet haben. Wenn es noch unfertige Arbeiten gibt, die gespeichert werden müssen, sollten Sie diese zuerst speichern.

Öffnen Sie die Eingabeaufforderung mit Administratorrechten und führen Sie die folgenden Befehle nacheinander aus. Sobald Sie den blinkenden Cursor in der Eingabeaufforderung sehen und ihn erneut eingeben können, können Sie den nächsten Befehl ausführen.

ie4unit.exe -show

taskkill /IM explorer.exe /F

DEL /A /Q "%localappdata%\IconCache.db"

DEL /A /F /Q "%localappdata%\Microsoft\Windows\Explorer\iconcache*"

Jetzt müssen Sie einen letzten Befehl ausführen, dieser Befehl wird Ihr System jedoch neu starten, sobald Sie auf Enter tippen. Speichern Sie daher alles, was Sie noch benötigen.

shutdown /r /f /f /t 00

Sobald Sie wieder auf Ihren Desktop booten, beginnt Windows 10 mit dem Neuaufbau des Symbol-Cache.

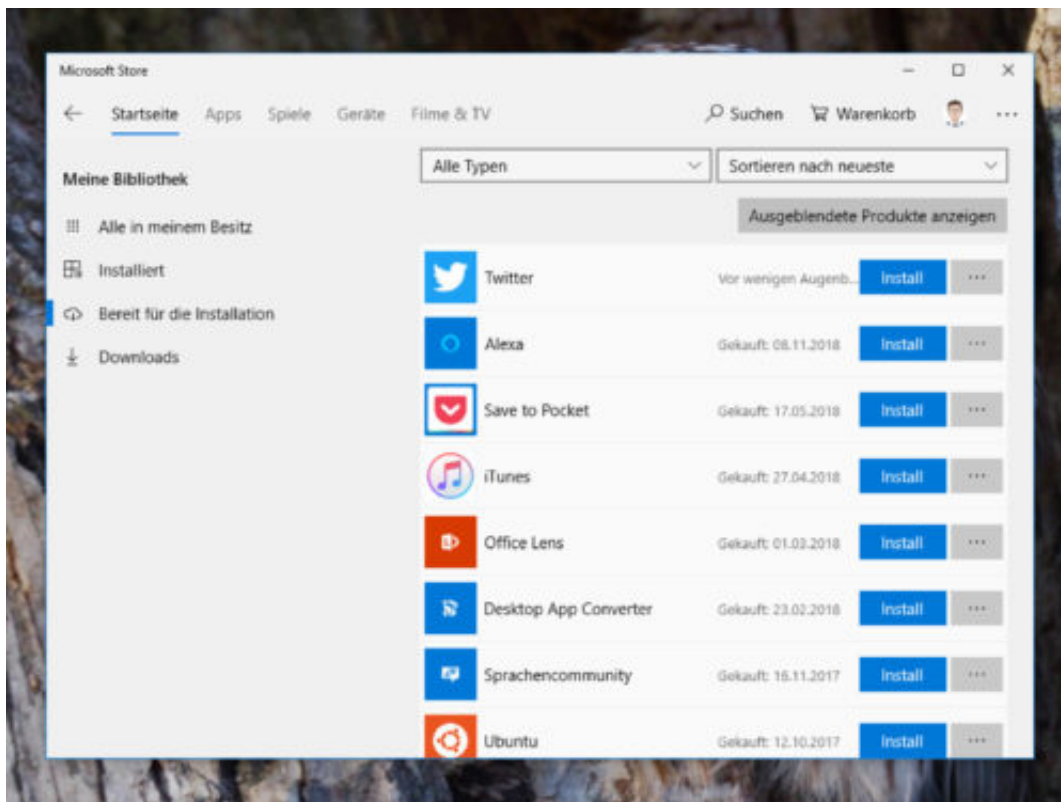


Apps neu installieren

Im Microsoft Store finden Nutzer von Windows 10 nützliche Programme, Tools und auch Spiele. Ob gekauft oder kostenlos nutzbar – Windows 10-Apps lassen sich auf mehreren Geräten laden und installieren. Welche Apps auf einem Gerät noch fehlen, kann mit wenigen Schritten überprüft werden.

Store-Programme, die bereits auf einem anderen Windows 10-PC installiert wurden, können wie folgt auch auf dem aktuell genutzten Computer eingespielt werden:

1. Zunächst unten auf den Start-Button klicken.
2. Im Startmenü dann die Kachel des **Microsoft Store** aufrufen. Die ist normalerweise schon angeheftet.
3. Jetzt oben rechts im Store-Fenster auf den 3-Punkte-Button und dann im Menü auf **Meine Bibliothek** klicken.
4. Apps, die noch nicht lokal auf dem System vorhanden sind, werden per Klick auf **Bereit für die Installation** aufgelistet – und können auch gleich per Klick installiert werden.



Mein eBook: Notfall-Stick für Windows 10

Es kann jederzeit passieren: Der Windows-Rechner startet (bootet) nicht richtig oder wichtige Dateien sind verschwunden oder das Passwort ist vergessen... Dann braucht man einen Notanker. Der Windows 10 Report zeigt, wie sich dieser USB-Notfallstick herstellen lässt. Optimal gerüstet also für den Fall f+r Fälle.

Wir alle vertrauen unserem [Windows-10](#)-Rechner eine Menge Daten an. Eigentlich alle Daten. Wir speichern Texte, Dokumente, Zahlen, Listen, Präsentationen, Fotos, Bilder, Videos und vieles mehr auf dem Gerät, Manches davon landet auch in der Cloud. Vorteil: Gut aufbewahrt und von überall nutzbar. Nachteil: Na ja, Cloud halt – da weiß man nie so recht.

[caption id="attachment_760383" align="alignnone" width="500"]



[EsaRiutta](#) /

Pixabay[/caption]

Deshalb lassen wir manche Dokumente und Dateien nur auf unserem Rechner und gehen davon aus, da seien sie sicher. Stimmt so weit ja auch. Allerdings nur für den Fall, dass der Rechner immer artig startet. Was aber, wenn es mal Probleme gibt? Windows 10 könnte sich zum Beispiel weigern, zu booten. Technische Probleme könnten den Start verhindern. Was tun?

Für solche Fälle sollte man ein Notfall-System parat haben. Einen USB- Stick, der den Rechner startet, damit man wenigstens an seine Daten herankommt. Wie man einen solchen USB-Stick zusammenstellt, erfahrt Ihr in meinem eBook: [Windows 10 - Notfallsystem einrichten](#).

Aus dem Inhalt:

- Vorbereitet auf den GAU
- Einrichten des eigenen Notfall-Stick
- Den Rechner auf das Booten mit Notfall-Stick vorbereiten

- Die richtigen Dateien kopieren
- Notfall-Stick benutzen und Daten retten
- Schneller surfen mit Microsoft Edge
- Die Cloud-Zwischenablage nutzen
- Sowie viele weitere Tipps und Tricks



OneDrive: Hohe CPU-Auslastung stoppen

Zu Windows 10 gehört auch die Microsoft-Cloud OneDrive. Wer den Dienst nicht braucht, kann ihn zwar vom System entfernen. Nutzt man OneDrive allerdings, schlägt das Programm öfter mal mit 100% CPU-Auslastung zu Buche. Gegen diesen Ressourcen-Hunger lässt sich etwas unternehmen.

Hinweis: Es kann andere Ursachen für die hohe CPU-Auslastung von OneDrive geben, und diese Lösung funktioniert nicht immer. Sie können jederzeit versuchen, die App zu deinstallieren und neu zu installieren. Dieser Fix gilt für die Desktop-Version von OneDrive und nicht für die UWP-App, die Sie im Microsoft Store herunterladen können.

Telemetrie-Werte löschen

1. Öffnen Sie als Erstes den Task-Manager und suchen Sie in der Liste der laufenden Prozesse nach **OneDriveSetup.exe**. Dieser Task muss beendet werden.
2. Jetzt zum Ordner **C:\Benutzer\Beispiel** wechseln, wobei der Benutzername immer anders lautet.
3. Nun im Explorer oben per Klick auf **Ansicht, Ausgeblendete Elemente** die versteckten Dateien anzeigen.
4. Hier bei **AppData\Local\Microsoft\OneDrive\OneDrive\setup\logs** die Dateien **UserTelemetryCache.otc** und **UserTelemetryCache.otc.session** löschen.
5. Danach drei Ebenen höher gehen, also zum übergeordneten Ordner **OneDrive**.
6. Dort im Verzeichnis **Update\Update** die Datei **OneDriveSetup.exe** starten.

Dies sollte das Problem der hohen CPU-Auslastung lösen. Starten Sie Ihr System zur Sicherheit neu.



Windows ist deaktiviert – was nun?

Viele Benutzer sehen aktuell einen Hinweis, ihre Windows-Kopie sei nicht aktiviert. Dabei spielt es keine Rolle, ob eine OEM-Lizenz, eine Softwarelizenz oder ein Upgrade von Windows 7 oder 8/8.1 zum Einsatz kommt. Wenn Sie sich fragen, warum Windows 10 plötzlich von selbst deaktiviert wurde, lautet die Antwort schlicht: Serverprobleme.

Microsoft ist das Problem bekannt. Es scheint von Servern verursacht zu werden, die für die Authentifizierung von Lizenzen und Produktschlüsseln verantwortlich sind. Es gibt viel Gerede darüber in den Foren und die folgende Erklärung wurde abgegeben:

Microsoft hat gerade eine Ankündigung über ein aktuelles Aktivierungsproblem im Zusammenhang mit der Pro-Edition veröffentlicht. Es tut mir sehr leid, Ihnen mitteilen zu müssen, dass es im Moment ein temporäres Problem mit dem Aktivierungsserver von Microsoft gibt und einige Kunden dieses Problem haben könnten, wenn Windows als nicht aktiviert angezeigt wird.

Unsere Ingenieure arbeiten unermüdlich daran, dieses Problem zu lösen, und es wird erwartet, dass es innerhalb von ein bis zwei Werktagen behoben wird.

Was ist zu tun?

Kurz gesagt: Abwarten und Tee trinken. Die Meldung kann jedenfalls – eine legale Windows-Kopie vorausgesetzt – getrost ignoriert werden. Das System wird weiterhin überprüfen, ob es sich um eine gültige Aktivierung handelt. Sobald Microsoft das Problem auf dem eigenen Server also repariert hat, zeigt auch das Windows-System wieder den korrekten Aktivierungsstatus an.

Schon seit Windows XP muss das System bei Microsoft aktiviert werden. So fing alles an:

