Schieb Report

Ausgabe 2019.04

Smart-TVs verraten Nutzerdaten - und die Hersteller verdienen daran

Kaum einer fragt sich, was so ein Smart-TV eigentlich alles macht, wenn man auf der Fernbedienung die bunten Tasten drückt. Jetzt hat ein Branchen-Insider zugegeben: Die Hersteller von Smart-TVs sammeln Nutzungsdaten und verkaufen diese an Interessemten. Damit werden erhebliche Summen verdient - und die TV-Nutzer wissen nichts davon.

Alles wird teurer? Stimmt nicht. Fernseher zum Beispiel werden zunehmend günstiger. Und das, obwohl sie immer flacher, größer und smarter werden. Während wir 2005 für einen Fernseher in Deutschland noch durchschnittlich rund 1.600 EUR ausgegeben haben, waren es 2017 nur noch 600 EUR.

Ein Minus von satten 60 Prozent. Die Hersteller verdienen an den Geräten. Aber nicht mehr so sehr an der Ladenkasse, sondern indem sie ihre Kundschaft ausspionieren und die ermittelten Daten verkaufen.

Insider berichten über die Details der Datensammelei

Viele Smart-TVs schauen ihren Nutzern sprichwörtlich rund um die Uhr über die Schulter. Was wird geschaut? Von wem, wann und wie lange? Daten, die für viele Unternehmen wertvoll sind - und deshalb von den Fernsehherstellern verkauft werden. Zwar in anonymisierter Form, aber trotzdem: Die Sehgewohnheiten werden sogar mit Angaben wie Alter, Geschlecht, Einkommen und Bildungsstand angereichert - und so attraktiver gemacht.

Rund 90 Prozent aller Smart-TV-Nutzer stimmen dieser Nutzeranalyse zu - ohne zu wissen,

was mit den Daten passiert. Das hat der der technische Chef (CTO) des US-Herstellers Vizio dem US-Dienst The Verge erklärt.

Demnach ist das Einsammeln, Auswerten und Weiterverkaufen der Nutzerdaten mittlerweile das eigentliche Geschäft bei Smart-TVs. Die Preise für die Geräte fallen. Die Verkaufsmargen belaufen sich nur noch auf magere 6 Prozent. Viel mehr wird mit dem klammheimlichen Verhökern der Nutzerdaten verdient.

https://vimeo.com/312404733

Kaum einer weiß davon

Das wäre so weit ein legitimes Geschäftsmodell - schließlich funktioniert genau so der Großteil des Internets -, wenn es da nicht ein erhebliches Problem gäbe: Die Nutzer wissen nichts davon. Offensichtlich sammeln die meisten Hersteller von Smart-TVs unbemerkt und in der Regel ungefragt Nutzerdaten, ob Vizio, Samsung, LG, Sony oder Philips, um nur einige Beispiele zu nennen. Die Nutzer stimmen beim Einrichten der Geräte zwar eine Erfassung der Daten zu, wissen aber nicht mal ansatzweise, was damit passiert.

Bei einem Smart-TV gehen die Leute nicht davon aus, dass Daten erfasst und weitergegeben werden. Viele Fernsehgeräte haben heute Google Android eingebaut und können die Daten so direkt bei Google abliefern. Ich bin sicher: Den meisten Smart-TV-Zuschauern dürfte das weder geheuer, noch Recht sein.

Bedeutet was? Dass sich jeder, der sich heute ein Smart-TV zu Hause hinstellt, bewusst darüber sein sollte, dass hier anfallende Daten weitergegeben werden. Das passiert sogar mit an Sicherheit grenzender Wahrscheinlichkeit, es sei denn - und das ist auch eine Möglichkeit! -,

man widerspricht der Auswertung der Daten ausdrücklich, meist in den Optionen. Aber auch der Gesetzgeber ist gefordert: Derart klammheimliche Datensammelei und -auswertung sollte auf keinen Fall erlaubt sein.

Collection#1: Millionen User von Hack betroffen

Ein austalischer Sicherheitsexperte lässt die Alarmglocken läuten: Er hat im Netz eine sorgfältig zusammengestellte Liste mit 773 Millionen E-Mail-Adressen samt Passwörtern gefunden. Das größte jemals entdeckte Paket mit Zugangsdaten. Für die User ist das ein Weckruf.

Das Jahr fängt wirklich nicht gut an. Erst der Daten-Leak, von dem Promis und Politiker betroffen waren. Und jetzt meldet ein australischer Sicherheitsexperte: Im Netz sind ungeheuer große Datenbanken mit Nutzerdaten aufgetaucht, die mehr oder weniger jeder laden und nutzen kann. Insgesamt 773 Millionen unterschiedliche Mail-Adressen sind in dieser Datenbank gespeichert.

Was ist genau passiert

Es handelt sich nicht um einen neuen Hack, sondern um eine Sammlung von erbeuteten Zugangsdaten, die aus Hackaktionen aus der Vergangenheit stammen. „Collection#1“ ist das Paket überschrieben. Also ausdrücklich eine Sammlung. Der australische Sicherheitsexperte Troy Hunt hat das ungeheuer große Paket in Untergrund-Foren im Netz gefunden.

Irgend jemand hat sich die Mühe gemacht, und öffentlich kursierende Zugangsdaten, die aus Hackangriffen kommen, fein säuberlich in einer Datenbank zusammenzutragen.

Es sind 773 Millionen Mail-Adresse darin enthalten und 21 Millionen unterschiedliche Passwörter – alle in Klartext! Das ist alarmierend, denn das ist natürlich ein Leckerbissen für jeden, der im großen Stil Mail-Konten übernehmen oder andere Straftaten begehen will. Einfacher war es noch nie, irgendwo einzubrechen.

Was können Cyberkriminelle dami anrichten?

Cyberkriminellen werden praktisch auf dem Silbertablett valide Zugangsdaten übergeben: E-Mail-Adresse und Passwort. 773 Millionen Mal. So ist es kinderleicht, diese Zugangsdaten auszuprobieren. In Mail-Diensten, in Cloud-Diensten, bei Facebook, Twitter, überall.

Besonders gefährdet sind alle, die ihr Passwort selten ändern und vor allem all jene, die dasselbe Passwort in mehreren Diensten verwenden. Denn wenn dieselbe Kombination aus Nutzername und Passwort überall funktioniert, dann haben es Hacker besonders einfach.

Bin auch ich betroffen?

Das ist leicht. Es gibt einen Dienst, der sich „Have I been Pawned“ nennt – einfach mal googeln. Zu deutsch: Bin ich erwischt worden. Da gibt man seine Mail-Adresse ein und erfährt dann schnell, in welchen Hackangriffen bereits Daten erbeutet wurden – und auch welche.

Wenn hier „Collection#1“ auftaucht, stehen die eigenen Zugangsdaten in dieser gigantischen und nun sehr populären Datenbank drin. Übrigens: Wer nicht so gut Englisch spricht: Es gibt auch eine deutsche Übersetzung mittlerweile. In meinem Blog Digitalistan auf wdr.de beschreibe ich, wo man diese deutsche Übersetzung findet und benutzt.

Was unternehmen?

Wichtig ist, dass man die Ratschläge der Experten ernst nimmt: Nie dasselbe Passwort in mehreren Diensten verwenden. Komplexe Passwörter wählen. Passwort-Manager wie Dashlane, 123password oder lastpass können helfen.

Wenn man in der Liste steht, unbedingt die Passwörter überall(!) ändern, zumindest aber schon mal bei Mail-Postfach und Cloud-Diensten. Und: Die Zwei Faktor Authentifizierung einsetzen. Das sichert Online-Konten gut ab. Selbst wenn ein Hacker das Passwort in die Hände fällt, hat er kaum eine Chance.

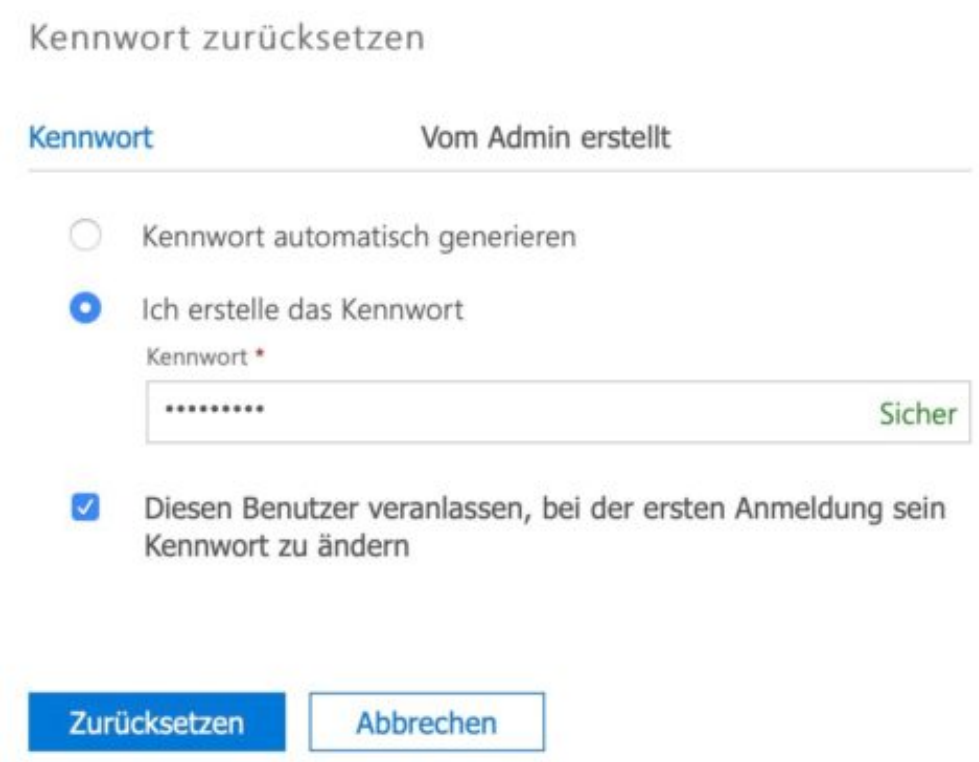
Zwei Faktor Authentifizierung

Alle sowieso nicht. Von ganz kleinen Onlineshops kann man das nicht unbedingt erwarten. Die großen Onlinedienste wie Apple, Amazon, Google, Twitter, Facebook, Microsoft und viele andere bieten es an. Allerdings sehr versteckt – und nicht proaktiv.

Man muss schon wissen, dass es das gibt und es dann auch selbst aktivieren. Ein regelrechter Skandal ist, dass die drei großen Mail-Dienste GMX, Web.de und Telekom die Zwei Faktor Authentifizierung bislang nicht anbieten. Überhaupt nicht. Ich habe nachgefragt, wieso. Auskunft: Ab 2. Quartal 2019 soll es so weit sein. Dafür gibt es keine guten Noten im Fach Datensicherheit.

Passwortwechsel bei Office 365 erzwingen

Passwörter (und die Benutzer, die sorglos mit den ihren umgehen) sind eines der Hauptübel, wenn es um die Sicherheit eines PCs oder Dienstkontos geht. Wenn Sie Office 365 verwenden, dann können Sie mehr tun, als sich auf einen regelmäßigen Passwortwechsel Ihrer Anwender zu verlassen: Vergeben Sie einfach ein neues Passwort und zwingen Sie Ihre Benutzer, dieses sofort zu ändern!



Der Weg dahin ist ganz einfach: Rufen Sie die Office 365-Administrationskonsole auf. Dazu melden Sie sich unter admin.microsoft.com mit Ihrem Office 365-Konto an.

Unter **Benutzer**, **Kennwort zurücksetzen** bekommen Sie eine Übersicht all Ihrer Benutzer angezeigt und können den oder die bequem markieren, im Extremfall gleich alle. Klicken Sie nun auf **Auswählen**.

Entweder lassen Sie Office 365 nun ein **Kennwort automatisch generieren** oder Sie erstellen das Kennwort selbst. Wichtig ist nun der Haken neben **Diesen Benutzer veranlassen, bei der ersten Anmeldung sein Kennwort zu ändern**. Damit wird der Passwortwechsel erzwungen. Nach der ersten Anmeldung kennen Sie als Administrator das Kennwort dann nicht mehr.

Windows-Sicherheitsfunktionen nutzen

Sicherheit wird groß geschrieben, nicht erst seit den letzten Datenlecks. Es gibt eine Menge an Zusatzprogrammen, die Ihnen helfen können, aber wie so oft im Leben: Warum in die Ferne schweifen, wenn das Gute liegt so nah? Windows 10 selbst bietet eine Vielzahl von Sicherheitsfunktionen, die Sie ohne Zusatzkosten nutzen können!

[caption id="attachment_761234" align="alignnone" width="500"]

Free-Photos / Pixabay[/caption]

Das Windows-Sicherheitscenter finden Sie in den Einstellungen unter **Update und Sicherheit**, **Windows-Sicherheit**. Dieses ist in verschiedene Schutzbereiche gegliedert, die die unterschiedlichen Gefahrenquellen für Ihren PC (wie Virenschutz, Kontoschutz, Netzwerkschutz und vieles mehr) umfassen.

Klicken Sie einen der Schutzbereiche an, um weitere Einstellungen und Einflussmöglichkeiten angezeigt zu bekommen. Bei all diesen Schutzfunktionen können Sie auswählen, ob Windows eine potenzielle Bedrohung direkt blockiert oder Sie davor nur warnt. Hier gilt es gut abzuwägen: Die Blockierung ist ohne Frage sicherer, auf der anderen Seite ist Windows 10 recht vorsichtig. So genannte "False Positives", also Fehlalarme, bei denen Ihnen eine Bedrohung angezeigt wird, die gat keine ist, sind wahrscheinlich.

Wir empfehlen Ihnen die mittlere Einstellung: Eine Warnung vor einer identifizierten Bedrohung schützt Sie auf der einen Seite, auf der anderen Seite blockiert sie nicht automatisch Programme, die keine Bedrohung sind, sondern gebraucht werden.

Was an Facebooks Charme-Offensive faul ist

Facebooks Top-Managerin Sheryl Sandberg ist nach Deutschland gekommen, um mit Charme für das Unternehmen zu werben. Selbst ein paar Millionen Euro für einen deutschen Lehrstuhl für KI hat sie mitgebracht. Doch was sich konkret ändern soll, ist kein Thema.

Wer kann noch "Facebook" sagen, ohne an all die Skandale, die Lügen und nicht eingehaltenen Versprechen zu denken? Sicher kaum einer von uns. Man kann wohl mit Fug und Recht behaupten, dass das Unternehmen nicht nur einen katastrophalen Führungsstil aufweist, sondern auch noch ein miserables Krisenmanagement. Was aber daran liegt, dass der Kopf des Unternehmens - Mister Mark Zuckerberg - nicht sonderlich lernwillig zu sein scheint.

Guter Schachzug: Sandberg statt Zuckernerg

Zuckerberg hat viele Sympathien verspielt. Nicht nur deshalb war es eine gute Idee, nicht Zuckerberg, sondern Sheryl Sandberg zur DLD-Konferenz nach München zu schicken. Sie ist nicht so "verbrannt" wie Zuckerberg.

Im Gegenteil: Die zweite Frau im Unternehmen gilt vielen als Vorbild und soll nach den zahlreichen Skandalen und Problemen sogar versucht haben, im Unternehmen etwas zu verändern. Gegen den Widerstand von Zuckerberg.

In München verkündet die Top-Managerin dann allerlei Verbesserungen im Unternehmen. Die Rhetorik ist mehr oder weniger dieselbe wie die von Zuckerberg. Aber geschickter verpackt.

Sandberg gelobt in München medienwirksam Besserung. Man habe verstanden. Es soll etwas passieren. Man unternehme etwas gegen Hate Speech und Manipulation der öffentlichen Meinung. Wunderbar. Aber was ist gemeint? Konkret wird Sandberg auch nicht.

https://vimeo.com/302911841

Lauter bedeutungslose Bekundungen

Von wegen: "Wie sind nicht mehr dasselbe Unternehmen wie 2016 oder vor einem Jahr!" Alles Rhetorik. Es gibt immer noch Verstöße gegen den Datenschutz - und gegen die Interessen der User. Wenn gebetsmühlenartig behauptet wird, die Privatsphäreeinstellungen würden besser, so mag das stimmen. Aber warum werden sie nicht einfach mal gut? Oder spitze?

Weil Facebook das alleine gar nicht kann. An dem größten Problem, dem Business-Modell, will Facebook nämlich nichts ändern. Deshalb bleibt alles Flickschusterei. Facebook könnte nur überzeugend besser werden, wenn sich das Unternehmen Hilfe von außen holt.

[caption id="attachment_758940" align="alignnone" width="500"]

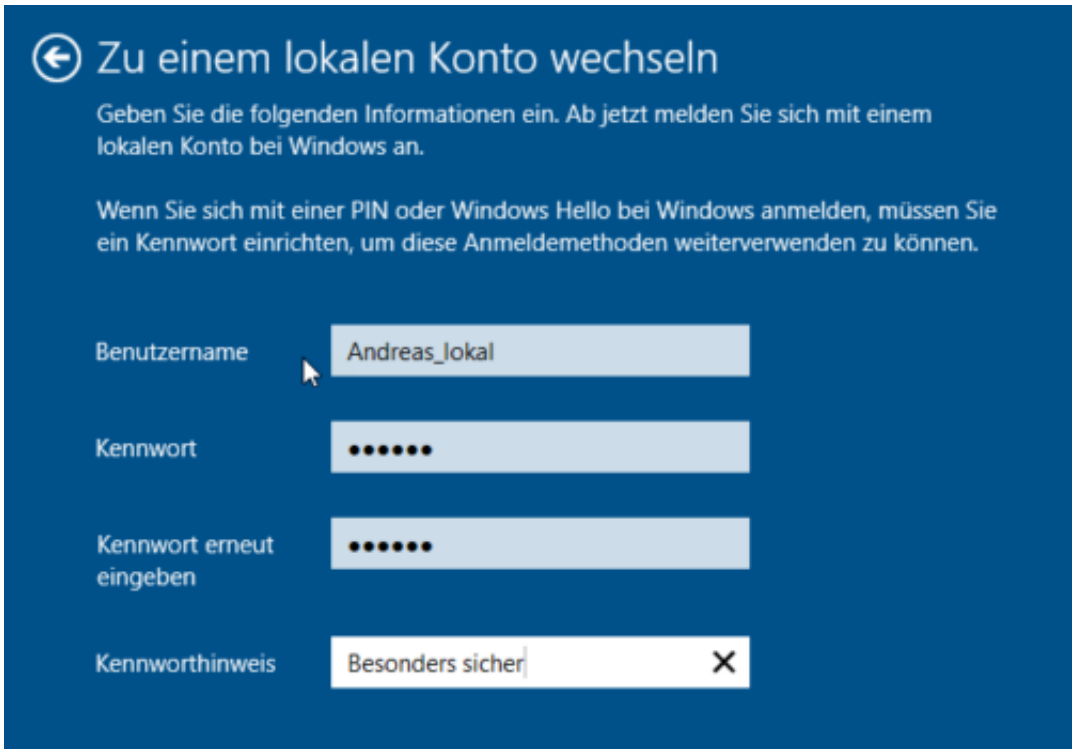

geralt / Pixabay[/caption]

Unabhängige Expertise und Beratung - und die Empfehlungen dann auch gnadenlos befolgt, auch wenn es Umsatz kostet. Anderenfalls bleiben die Beteuerungen von Sandberg, Zuckerberg oder wem auch immer unglaubwürdig und meist folgenlos.

Die 7,5 Millionen Dollar, die Facebook nun in Deutschland für KI-Forschung und Ethikfragen investiert, sind ein nettes Mitbringel. Mehr eine Geste - denn 7,5 Millionen Dollar verdient Facebook innerhalb von drei Stunden. Ethik ist dem Unternehmen also 0,036% des Jahresumsatzes wert. Beeindruckend, oder?

Wechseln zwischen lokalem und Microsoft-Konto unter Windows 10

Nicht jeder Anwender möchte seine Daten in der Cloud haben, und so ist die Verwendung eines lokalen Kontos, bei dem alle Daten auf der Festplatte Ihres Windows 10-PCs bleiben, durchaus eine gängige Alternative. Der Wechsel zwischen den beiden Kontotypen ist kinderleicht und vor allem dann empfehlenswert, wenn Sie weniger Daten in der Cloud haben möchten.



Klicken Sie in den Einstellungen von Windows 10 auf Konten, dann unter Ihrem Namen auf **Stattdessen mit einem lokalen Konto anmelden**.

Geben Sie nun einen lokalen Benutzernamen ein (diese muss keine E-Mail-Adresse sein wie es beim Microsoft-Konto der Fall ist), dann ein Passwort für das neue Konto, das Sie dann noch einmal bestätigen müssen. Zu guter Letzt können Sie noch einen Kennworthinweis eingeben, um sich besser an das Passwort erinnern zu können. Dieser sollte natürlich so kryptisch sein, dass er einem Fremden keinen Hinweis auf das tatsächliche Kennwort gibt.

Wenn Sie nun bei einem lokalen Konto das Passwort ändern wollen, dann drücken Sie gleichzeitig die Tasten **Strg**, **Alt** und **Entf**, und dann auf **Kennwort ändern**. Der Prozess ist wieder derselbe: Geben Sie das alte und dann zweimal das neue Passwort ein, und schon haben Sie die Passwortänderung durchgeführt.

Wiederherstellung eines vergessenen Passwortes

Während Sie bei der Anmeldung mit dem Microsoft-Konto ein vergessenes Passwort

wiederherstellen können, ist der Prozess bei einem lokalen Konto leider nicht so einfach. Hier sind einige Eingriffe ins System nötig, die zeitaufwändig sind. Für den Notfall finden Sie durch eine Suche nach „Kennwort lokales Konto vergessen“ diverse Anleitungen im Internet.

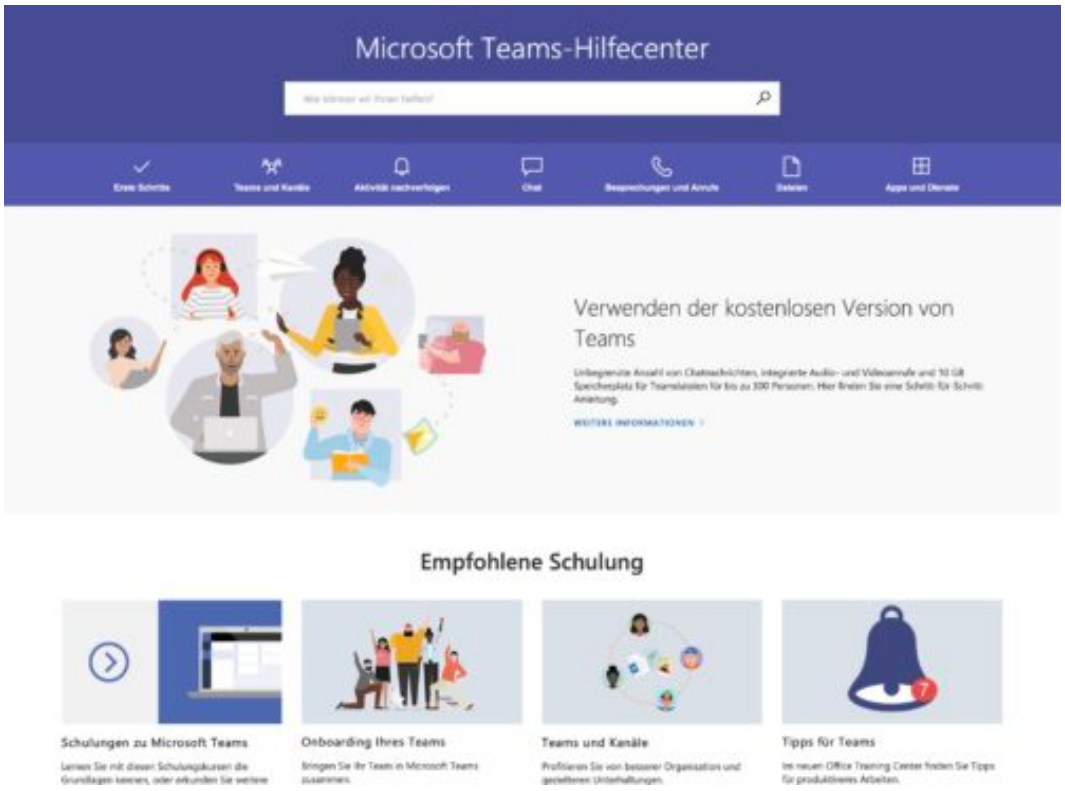
Es ist empfehlenswert, bei der Passwortänderung auf **Kennwortrücksetzdatenträger erstellen** zu klicken. Damit können Sie auf einem USB-Stick verschlüsselt Ihr Kennwort hinterlegen, um im Notfall damit die Passwortänderung ohne Eingabe des alten Passworts durchführen zu können. Diesen Datenträger sollten Sie allerdings wie Ihren Augapfel hüten: Was Sie können, kann auch derjenige, der den USB-Stick in seine Hände bekommen hat!

Automatische Migration auf Microsoft Teams

Microsoft hat schon seit einiger Zeit angekündigt, Skype for Business und die zugehörigen Kommunikationsdienste auf Microsoft Teams umzustellen. Ziel ist es hier, die Unternehmen (und natürlich auch die Privatnutzer von Office 365) auf eine neue, einheitliche Infrastruktur zu bringen. Die Umstellung wird automatisch vorgenommen, Sie bekommen eine Info-E-Mail, wenn diese abgeschlossen ist.

Einen klaren Plan, wann wer mit der Umstellung dran ist, kann man zwar nicht erkennen. Berichten von Betroffenen nach aber sind Sie früher an der Reihe, wenn Sie bisher Skype for Business nicht oder nur selten genutzt haben. Das macht Sinn: Der Umstellungsaufwand ist geringer, Sie können sich bei Bedarf gleich an die zukünftige Oberfläche gewöhnen.

Keine Sorge: Sie sind nicht ohne Hilfestellung: Microsoft bietet hier eine umfangreiche Sammlung von Informationen und Schulungen an, mit denen Sie den Start mit Teams ohne großen Aufwand realisieren können.


Microsoft Teams-Hilfecenter
Verwenden der kostenlosen Version von Teams
Empfohlene Schulung
Schulungen zu Microsoft Teams
Onboarding Ihres Teams
Teams und Kanäle
Tipps für Teams

Import von Textdateien in Excel

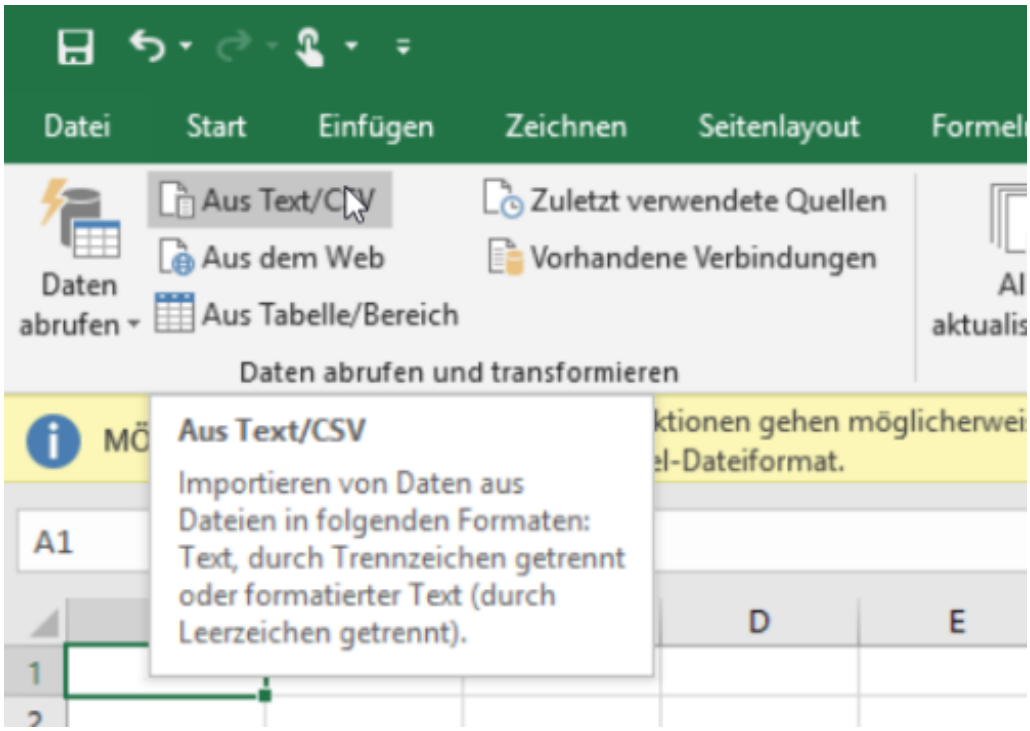
Es mgibt wenig Alternativen, wenn Sie Daten auswerten und visualisieren wollen: Tabellenkalkulationen wie Excel (oder Calc aus dem kostenlosen LibreOffice-Paket) gehören zum Standardhandwerkszeug der meisten PC-Benutzer. Spannend wird es, wenn Ihre Quelldaten in einer Textdatei und damit einem anderen Dateiformat vorliegen. Die Tabellenkalkulationen sind allerdings in der Lage, solche Dateien komfortabel zu importieren.

[caption id="attachment_761151" align="alignnone" width="500"]

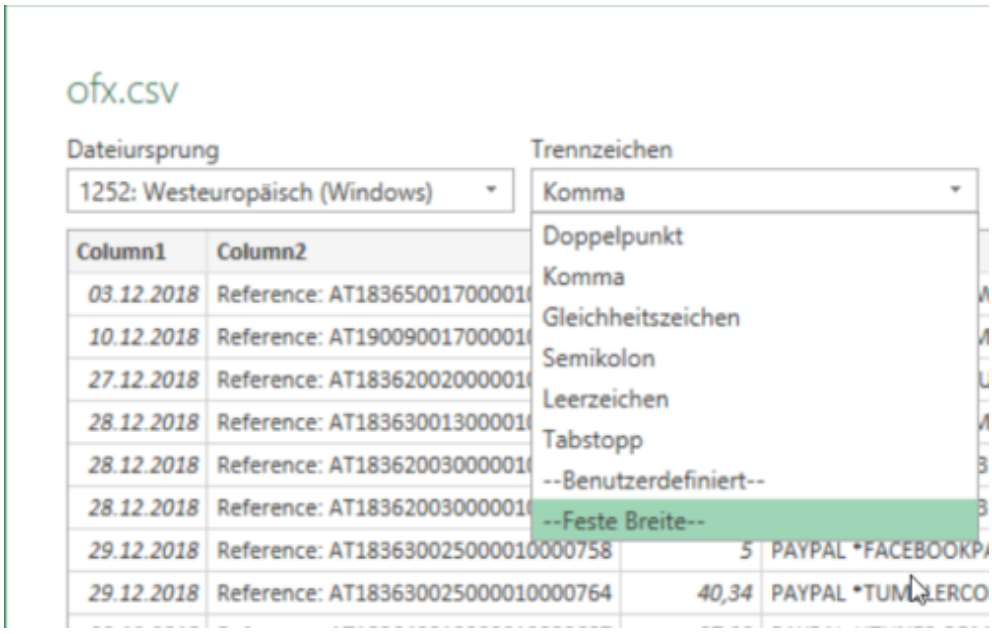
StockSnap / Pixabay[/caption]

Wichtig ist, daß in den Zeilen der Textdatei die einzelnen Datenfelder, die später die Spalten der Tabelle darstellen sollen, durch irgendein eindeutiges Trennzeichen voneinander getrennt sind. Das kann ein Leerzeichen, Komma, Semikolon sein. Hauptsache, die Tabellenkalkulation kann anhand dieses Zeichens eine Aufteilung vornehmen. Die Datei muss dazu die Erweiterung .TXT oder .CSV haben.

In Excel (das Verfahren ist bei allen verbreiteten Tabellenkalkuklationen ähnlich) dürfen Sie diese Datei nun nicht einfach öffnen, sonst wird jede Zeile ungetrennt in eine einzige Spalte geschrieben. Stattdessen legen Sie eine neue Excel-Datei an, dann klicken Sie auf **Daten**, **Aus Text/CSV**.



Excel versucht nun automatisch, die Trennzeichen zu erkennen und stellt die Tabelle in einer Voransicht dar. Sollte die Zuordnung der Daten in Spalten nicht funktionieren, dann klicken Sie unter Trennzeichen auf das verwendete Trennzeichen in der Textdatei. Wenn dieses nicht in der Liste dargestellt wird, klicken Sie auf **Benutzerdefiniert**. Danach können Sie das Trennzeichen (bei Bedarf sogar Zeichenketten) manuell festlegen. Alternativ geben Sie unter **Feste Breite** die feste Breite der Spalten an, wenn es eine gibt.



Schon wird die Textdatei importiert und kann mit den Bordmitteln Ihrer Tabellenkalkulation ausgewertet, in Diagramme umgewandelt werden und vieles mehr.

Verwenden eines Passwortgenerators

Passwörter sollten sicher sein, hier haben wir Ihnen schon beschrieben, wie Sie im Kopf gute Passwörter erzeugen können. Eine weitere Alternative ist die Verwendung eines Passwortgenerators, also eines Programms bzw. einer Webseite, die Ihnen nach bestimmten Vorgaben sicher Passwörter generiert. Kostenlos finden Sie dies beispielsweise unter https://www.lastpass.com/de/password-generator

Wählen Sie gewünschte Passwortlänge ein, wählen Sie ob Großbuchstaben, Kleinbuchstaben, Ziffern und/oder Sonderzeichen verwendet werden sollen. Auf Wunsch können Sie dann das Passwort noch für das Lesen oder Sprechen optimieren, diese Einstellungen beeinflussen die Verwendung von Sonderzeichen bzw. leicht verwechselbaren Zeichen im Passwort.

Aus LastPass können Sie das Kennwort dann über das Symbol mit den beiden Seiten oben rechts in die Zwischenablage kopieren und vor dort aus weiterverwenden.

Das sichere Passwort: Wenige Schritte zu mehr Sicherheit

Eigentlich ist der Begriff irreführend. Ein „sicheres“ Passwort ist ebenso theoretisch wie ein Perpetuum Mobile, denn mit genügend Rechenpower und Zeit lässt sich wohl jedes Passwort irgendwann herausfinden. Sie können den Aufwand aber zumindest so hochtreiben, dass die Wahrscheinlichkeit, dass das passiert, gegen Null geht.

Was ist nun ein sicheres Passwort? Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt unter https://www.bsi-fuer-buerger.de im Bereich Passwort einige Hinweise:

1. **Es sollte einfach zu merken sein:** Je schwerer ein Passwort zu merken ist, desto höher ist die Wahrscheinlichkeit, dass sie es sich aufschreiben. Das widerspricht dem Anspruch, dass es nur Ihnen selbst bekannt sein soll. Das so beliebte kleine, gelbe PostIt als
   Zwischenspeicher ist eben nicht sicher!
2. **Es sollte mindestens 8 Zeichen haben**: Mehr (an Buchstaben) ist hier tatsächlich mehr (an Sicherheit). Bei den Passwörtern für Ihr WLAN werden gar 20 Zeichen empfohlen.
3. **Nutzen Sie Sonderzeichen, Groß- und Kleinschrift und Ziffern**: Je komplexer das Passwort ist, desto schwerer ist er herauszubekommen. Wichtig dabei auch:
4. **Verwenden Sie keine über sie bekannten oder herauszufindenden Daten als Passwort**: Namen von Familienmitgliedern, Haustieren, Freunden, Geburtstage, Hochzeitstage etc. eignen sich nicht als Passwort. Auch keine Wörter, die in einem Wörterbuch vorkommen, oder Zeichen- oder Ziffernfolgen, die auf- oder absteigend sind wie 123456 oder abcdef.

Verlieren Sie nicht den Mut: Diese Anforderungen lassen sich tatsächlich umsetzen.

Passwörter müssen nicht lesbar sein oder aus tatsächlich vorhandenen Begriffen bestehen, damit Sie sich daran erinnern können. Der Ausgangspunkt zu einem guten Passwort kann beispielsweise ein für Sie ganz persönlich leicht zu merkender Satz oder eine Zeile aus einem Lied. „Ich habe im Sommer 2018 den Motorradführerschein gemacht!“ beschreibt ein Ereignis, an das Sie sich sicherlich noch lange erinnern werden. Nehmen Sie davon nur die Anfangsbuchstaben (unter Beachtung der Groß- und Kleinschrift) und lassen Sie Ziffern und Satzzeichen an ihrem Platz, und schon haben Sie *IhiS2018dMg!* als Passwort. Dieses Passwort errät niemand, der nicht Ihren speziellen Satz kennt.

Löschen von Ereignissen aus der Timeline

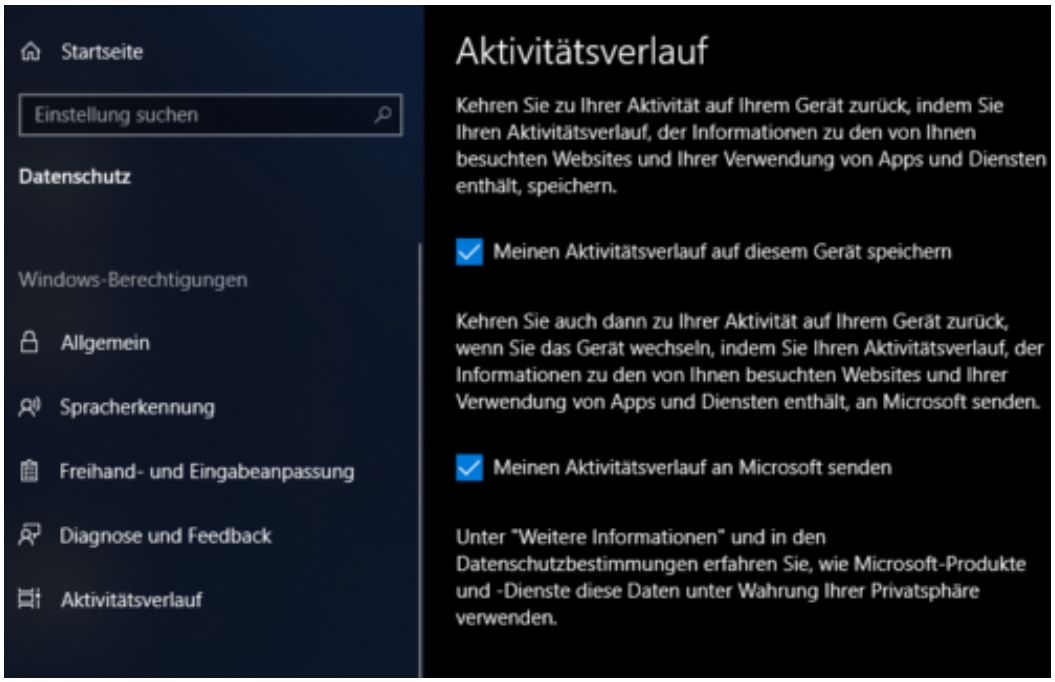
Die Timeline von Windows 10 ist eine wunderbare Hilfe, wenn Sie eine Webseite oder ein Dokument eines vergangenen Tages benötigen und wieder aufrufen möchten. Manche Tage aber sind einfach zum Vergessen und sollten aus der Erinnerung gelöscht werden. Besonders, wenn Sie Ihrem PC mit mehreren Leuten nutzen und nicht möchten, dass diese bestimmte Informationen wie aufgerufene Webseiten nutzen. Wir zeigen Ihnen, wie das ganz einfach geht.

Für ganz spezielle Tage oder einzelne Webseiten oder Dokumente, die aus der Zeitleisten-Ansicht entfernt werden sollen, öffnen Sie zuerst die Zeitleiste durch das Symbol neben der Suchleiste:

In der Übersicht der Ereignisse klicken Sie dann mit der rechten Maustaste auf das Miniaturbild des Ereignisses. Darin können Sie dieses durch **Entfernen** aus der Liste entfernen oder gar **Alle von (Datum) löschen**,um die Einträge des kompletten Tages zu entfernen.

Löschen der Timeline über die Datenschutzeinstellungen

Wenn Sie komplett mit Ihrer Vergangenheit abgeschlossen haben und die ganze Timeline löschen wollen, hilft nur noch der Holzhammer: Unter **Einstellungen**, **Datenschutz**, **Aktivitätsverlauf** können Sie die Zeitleiste ausschalten bzw. die Speicherung bei Microsoft unterbinden.



Über **Aktivitätsdaten zu meinem Microsoft-Konto verwalten** können Sie dann über die Microsoft Webseite die gespeicherten Ereignisse komplett löschen.

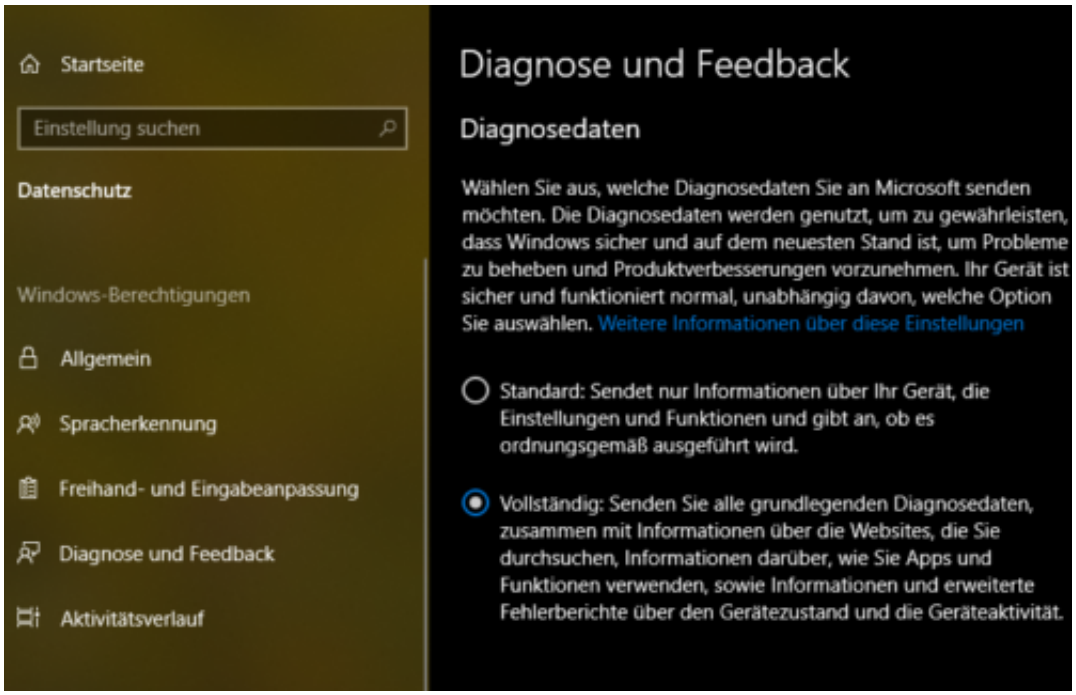
Windows besser machen: Diagnose und Feedback

Windows 10 hat eine schier unübersehbare Zahl von Funktionen und Apps, die universell für alle Hard- und Software lauffähig sein sollen. Sie haben sicherlich auch schon das ein oder andere Mal geflucht, wenn etwas nicht so funktionierte, wie es sollte. Programme beenden sich, stürzen ab, ruckeln, eine bestimmte Hardwarekomponente funktioniert nicht: Ärgerlich, aber es kommt vor. Um diese Erfahrung anderen Benutzern zu ersparen, können Sie Ihren Beitrag leisten.

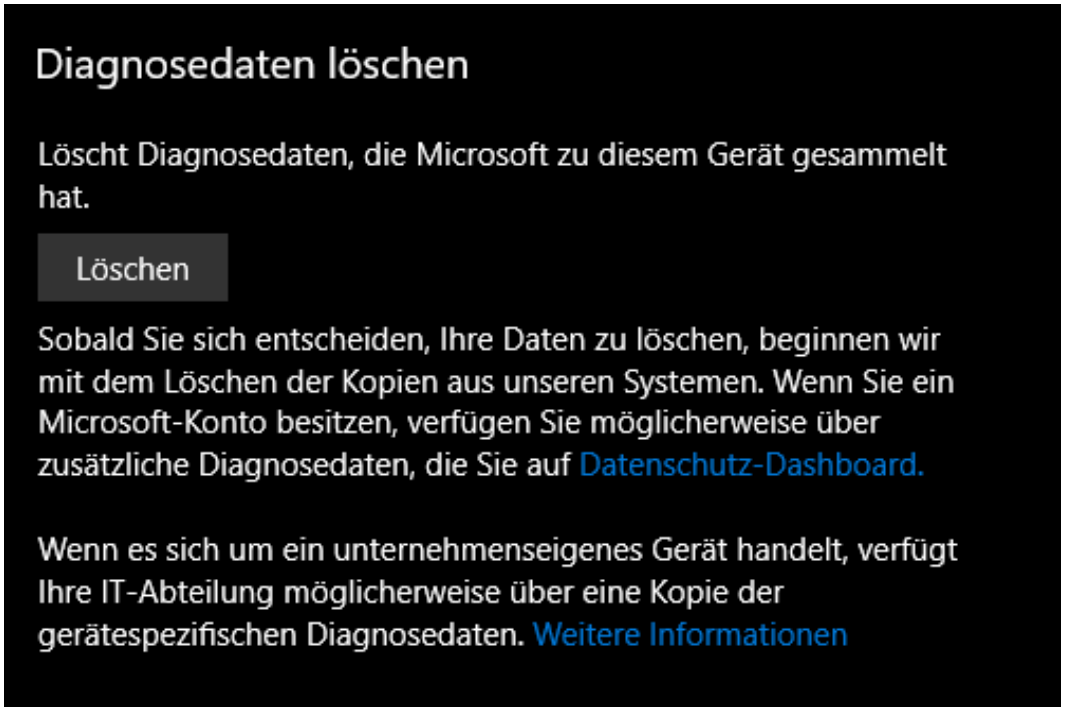
[caption id="attachment_761174" align="alignnone" width="489"]

RyanMcGuire / Pixabay[/caption]

Microsoft bietet unter **Datenschutz**, **Diagnose und Feedback** ein eigenes Dashboard für Ihre Beteiligung an der Verbesserung von Windows an. Im Standard sendet Windows nur Informationen über Ihr Gerät, die Einstellungen und Funktionen und den Status, ob das Gerät ordnungsgemäß ausgeführt wird, an.



Wenn Sie stattdessen **Vollständig** auswählen, dann wird die Menge der an Microsoft übertragenen Daten deutlich erhöht: Diagnosedaten, angesurfte Webseiten, Ihre verwendeten Apps und vieles mehr sind dann für Microsoft auswertbar.



Wenn Sie die Daten löschen möchten, dann rollen Sie auf der Einstellungsseite nach unten: Unter **Diagnosedaten löschen** können Sie den Prozess starten. Da die Daten auf den Servern von Microsoft liegen, kann dies allerdings etwas dauern.

Zurück in der Zeit: Die Windows Timeline

Wünschen Sie sich auch manchmal eine Zeitmaschine, mit der Sie nochmal an wichtige Zeitpunkte Ihres Lebens zurückkehren können? Wo Sie beispielsweise noch die eine, spezielle und plötzlich unauffindbare tolle Webseite mit dem Supertrick sehen? Oder das später veränderte Dokument noch im Urzustand haben? Im ersten Fall empfehlen wir schieb.de. Für die anderen können wir Ihnen aber auch helfen!

[caption id="attachment_761161" align="alignnone" width="500"]

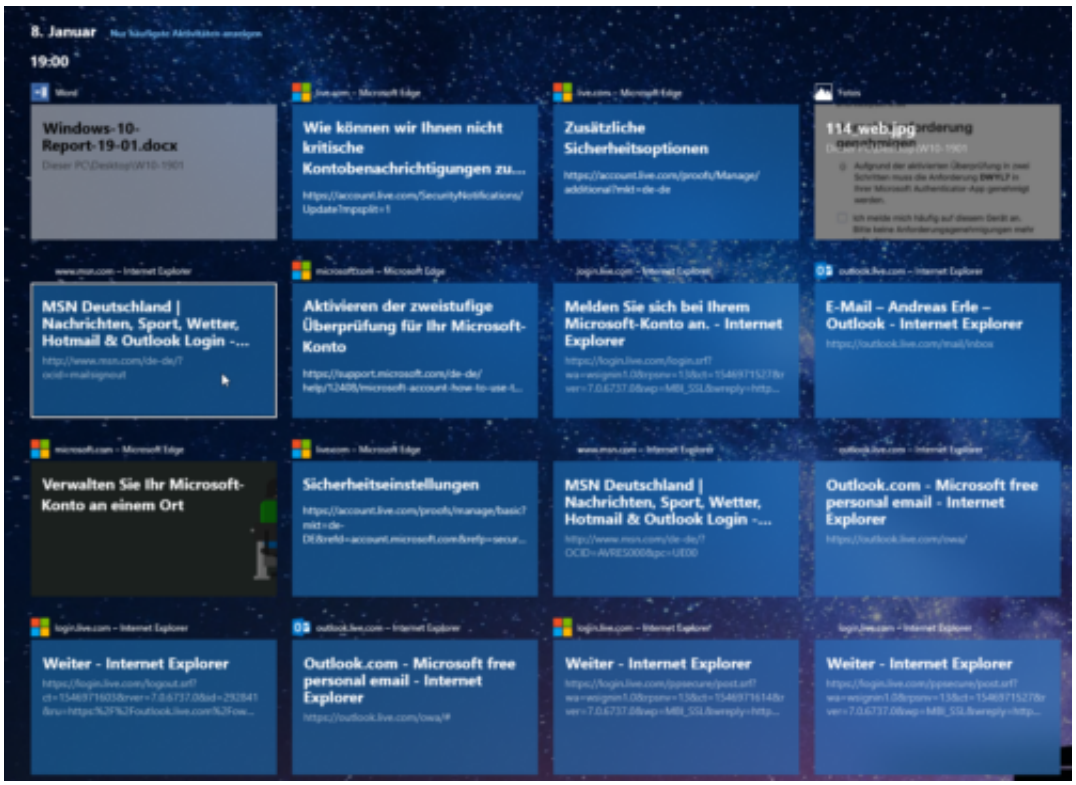

spirit111 / Pixabay[/caption]

Seit einigen Versionen bietet Windows 10 die Timeline, in der deutschen Version auch "Zeitleiste" genannt. Diese bietet Ihnen die Möglichkeit, an einen beliebigen Tag der ausgezeichneten Historie Ihres Windows 10-PC zurück zu gehen und Dokumente, Webseiten, Einstellungen zu dem Stand an diesem Tag anzusehen und wiederherzustellen.

Öffnen Sie die Zeitleiste durch einen Klick auf das kleine Symbol neben dem Suchfeld in der Taskleiste.

Windows 10 zeigt Ihnen nun eine Übersicht der Tage, die in der Zeitleiste gespeichert sind, und

wiederherstellbarer Momentaufnahmen. Klicken Sie auf eine davon , um das zugehörige Dokument oder die Webseite zu öffnen.



Wenn Sie einen produktiven Tag hatten, dann wird eine Vielzahl von Dokumenten und Webseiten gespeichert sein. Nicht alle zeigt Windows 10 Ihnen direkt an. Klicken Sie dazu auf **Alle Aktivitäten von XX anzeigen** (wobei XX die Zahl der Aktivitäten ist, die für dieses Datum gespeichert sind.

Support für Windows 10 Mobile geht zuende

Das Ende kam schleichend, aber unwiderruflich: Nach den klaren Aussagen von Microsoft-Chef Satya Nadella und "Mr. Windows Phone" Joe Belfiore, dass Windows 10 Mobile nicht mehr weiterentwickelt würde, kommt nun das offizielle Ende. Ab dem 10. Dezember 2019 bekommen die "aktuellsten" Windows Phones keine Sicherheitsupdates mehr.

Geräte, die die Version 1709 haben, werden noch zwei Updates bekommen, allerdings tatsächlich nur Fehlerbehebungen und Sicherheitsupdates. Ältere Geräte, bei denen die Version 1703 installiert ist (und die die 1709 nicht bekommen haben), erreichen das Support-Ende schon im Juni 2019. Eine genauere Auflistung nach Gerät finden Sie hier.

Neben den ausbleibenden Updates stellt Microsoft schrittweise auch die Möglichkeit der Gerätebackups (bis März 2020) und des Restores aus einem Backup (Ende 2020) ein.

Die offizielle Empfehlung von Microsoft selbst ist nun, entweder ein Android oder ein iOS-Gerät zu verwenden. Positiv betrachtet: Eine Vielzahl der Microsoft Apps bekommen Sie für beide der angegebenen Plattformen....

- **What does end of support mean for customers?**
- **Will my apps continue to be supported?**
- **Are Lumia or Microsoft devices supported differently?**
- **I just purchased a Windows 10 Mobile phone; can I return the phone for reimbursement?**
- **What should Windows 10 Mobile customers do now?**

  With the Windows 10 Mobile OS end of support, we recommend that customers move to a supported Android or iOS device. Microsoft's mission statement to empower every person and every organization on the planet to achieve more, compels us to support our Mobile apps on those platforms and devices.

  Customers who expect to continue using their Windows 10 Mobile device after December 10, 2019 are encouraged to manually create a backup using the **Settings->Update & security->Backup->More Options** and then tapping **Back up now** before that date.

- **Will existing updates for Windows 10 Mobile continue to be available, and for how long?**
- **Will I still be able to recover my device image?**
- **Will my device still work after December 10, 2019?**
- **How do I know if I have a Windows 10 Mobile?**

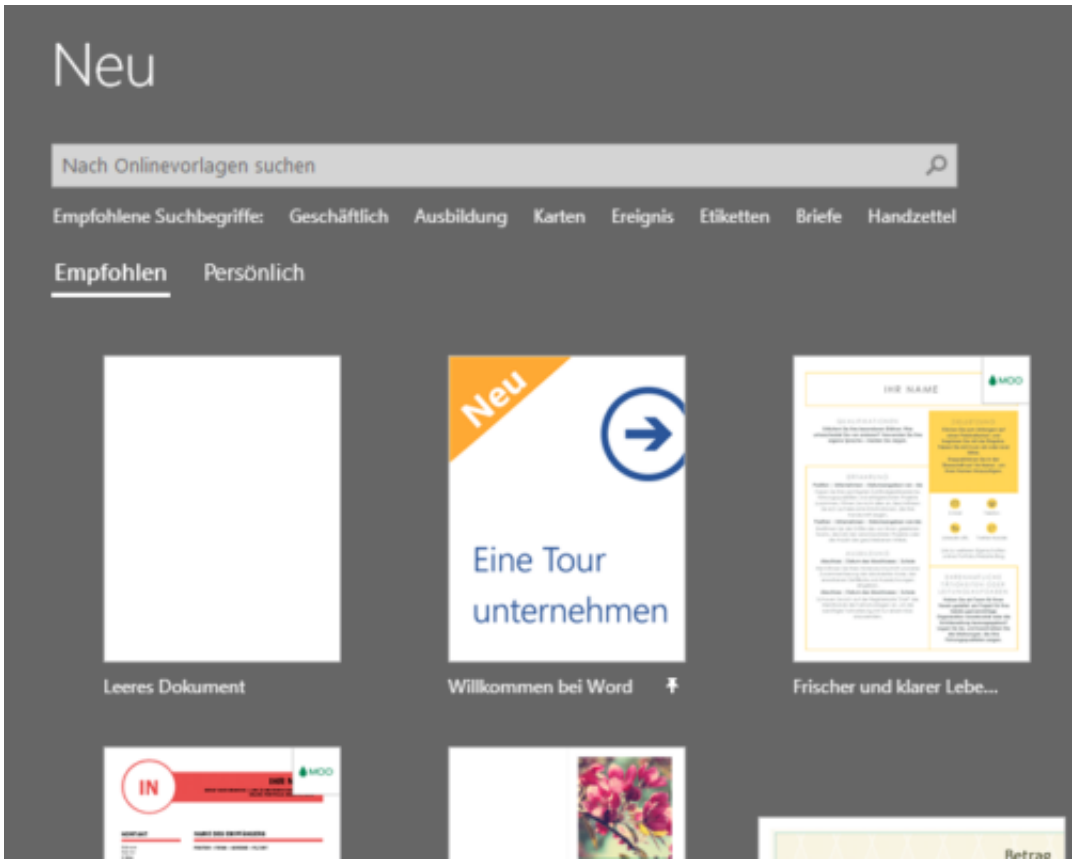
Wenn die eigenen Dokumentvorlagen verschwunden sind

Dokumentvorlagen sind das Salz in der Suppe der Office-Programme. Mit wenigen Handgriffen können Sie Ihre elektronisches Briefpapier erstellen. Wenn Sie dann den PC wechseln, dann sind diese Vorlagen leicht kopierbar. Dumm nur, wenn Word diese Vorlagen dann nicht anzeigen mag. Keine Sorge, das ist in den meisten Fällen nicht Ihre Schuld, sondern ein Fehlverhalten von Word, das sich leicht beheben lässt.

[caption id="attachment_761198" align="alignnone" width="500"]

RobinHiggins / Pixabay[/caption]

In einem solchen Fall hat Word nämlich nicht die Motivation, nach Ihren benutzerdefinierten Dokumentvorlagen zu schauen, auch wenn diese physisch vorhanden sind. Es fehlt schlicht die Kategorie **Persönlich** unter den angebotenen Vorlagen.

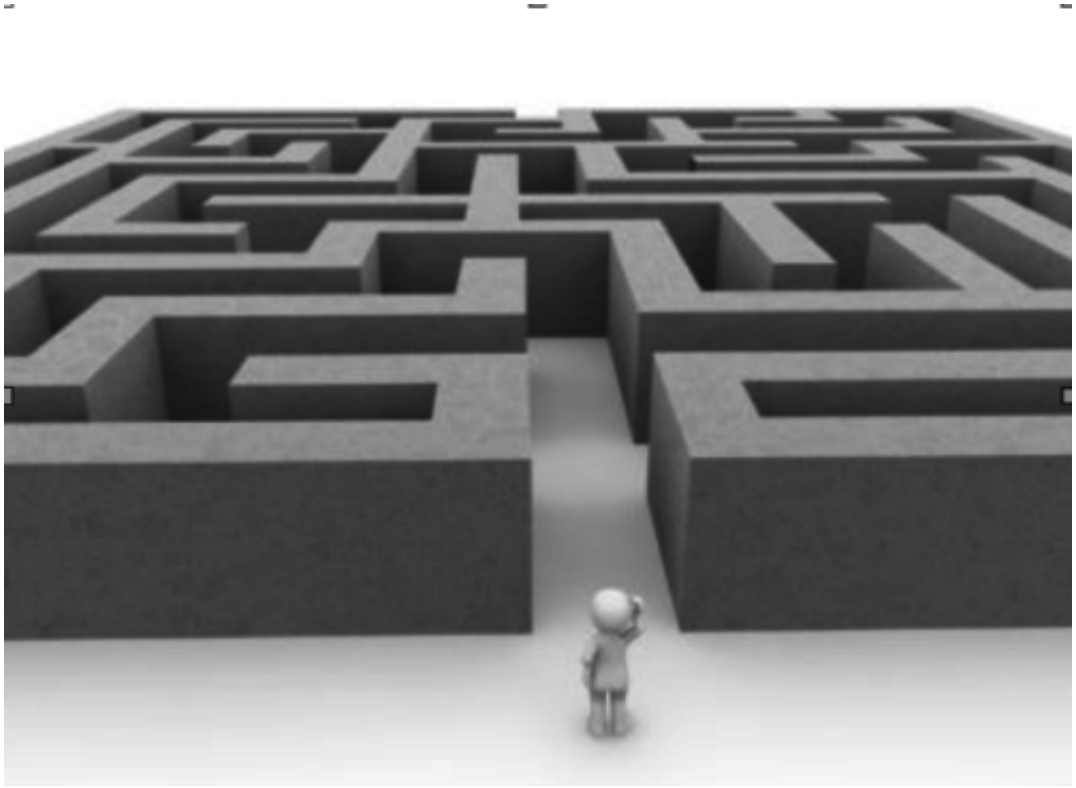


Die Lösung ist einfach: Erzeugen Sie ein **Leeres Dokument**, dann speichern Sie dieses als Dokumentvorlage ab: Unter **Datei**, **Speichern unter**, **Durchsuchen** wählen Sie als **Dateityp** Word-Vorlage (*.dotx) aus.

Speichern Sie die Dummy-Vorlage ab, und plötzlich fällt Word wieder ein, dass Sie ja auch eigene Vorlagen haben. Beim nächsten Anlegen eines neuen Dokumentes bekommen Sie dann alle Vorlagen, die in *\Dokumente\Benutzerdefinierte Office-Vorlagen* stehen, zur Auswahl angeboten.

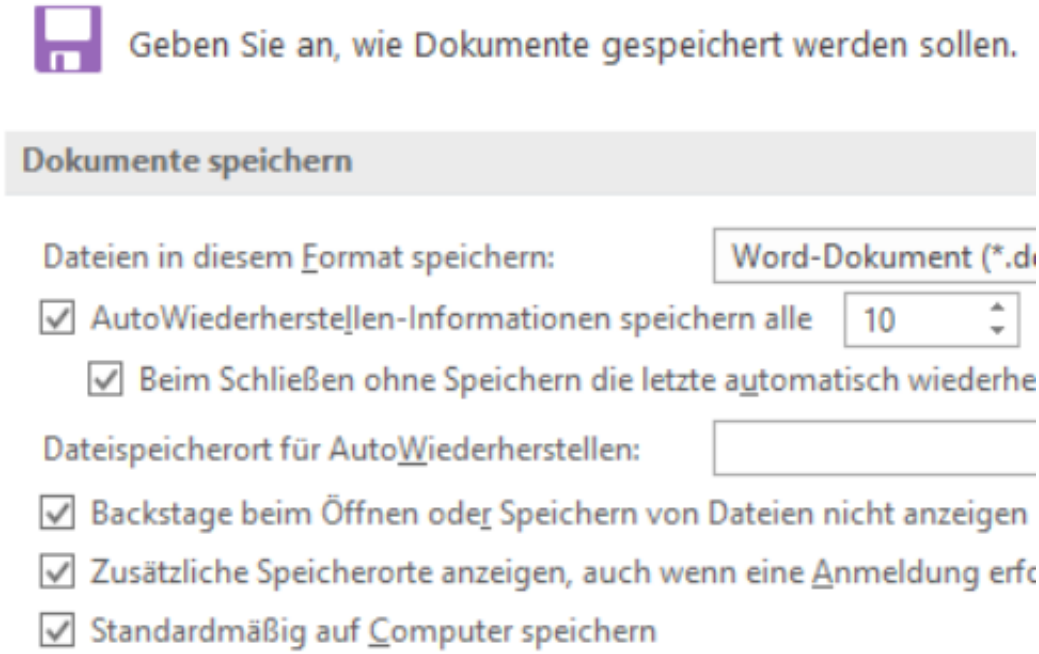
Dateien in Word automatisch direkt auf die Festplatte speichern

Über die Jahre hat sich der Dialog zum Speichern von Dateien in Word der Tatsache angepasst, dass es immer mehr potentielle Speicherorte gibt: Die Festplatte, die Cloud, geteilte Dateien anderern Benutzer.So muss sich der Anwender mittlerweile mühsam durch einen Zwischendialog quälen, statt direkt Ordner und Datei auswählen zu können. Das lässt sich aber ganz einfach beheben!



viele Anwender sind immer noch nicht gewillt, ihre Dateien der Cloud zu übergeben und wollen eine Speicherung auf einem lokalen Datenträger wie der internen Festplatte des eigenen PCs. Da macht es Sinn, diese auch direkt als Standard-Speicherort in Word zu definieren.

Unter **Datei**, **Optionen** muss dazu auf den Eintrag **Speichern** geklickt werden. Im nun erscheinenden Wirrwarr der Optionen für die Speicherung von Dateien müssen Sie dann den Haken neben **Standardmäßig auf Computer speichern** setzen.



Diese Einstellung erspart Ihnen das manuelle Anklicken von Auf diesem PC im Speichern-Dialog. Nur ein Klick, aber jeder Klick zählt schließlich!

Schutz vor Makro-Viren in Word-Dokumenten über das Trust-Center

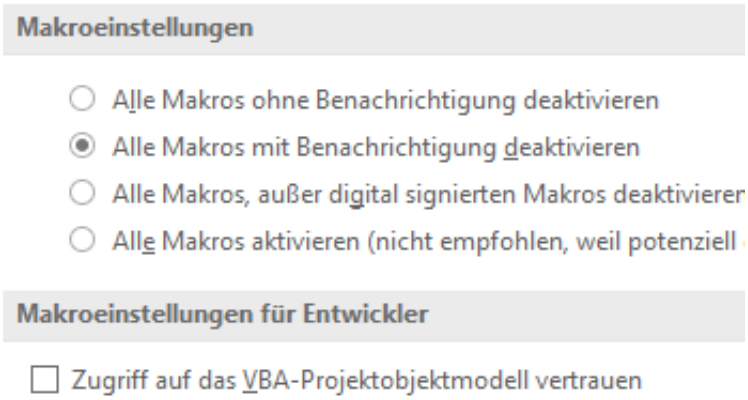
Nicht nur Programme können Viren entthalten, auch Dokumente, die Sie beispielsweise in Microsoft Word öffnen. Der Hintergrund: Makros, im Hintergrund laufende Prozesse, die beispielsweise Daten aus anderen Dokumenten ziehen und im Dokument aktualisieren und vieles mehr. Auch wenn Makros in Word als Funktionen geliefert werden, sind sie in einer Programmiersprache geschrieben. Eine Kontrolle der Makroausführung ist also wichtig und gar nicht schwer.

[caption id="attachment_761114" align="alignnone" width="368"]

geralt / Pixabay[/caption]

Auch wenn eine Textverarbeitung als Programm eher unkritisch erscheint: sie hat eine Menge an Zugriffen auf das System, kann Dateien öffen, auf Peripheriegeräte zugreifen und vieles mehr. In der praktischen Arbeit als Anwender werden Dokumente mit Makros aber eher die Ausnahme sein, in sofern bremst die Einschränkung der Ausführung von Makros Ihre Arbeit normalerweise nicht wirklich aus.

Unter Word klicken Sie auf **Datei**, **Optionen**, **Trust Center** und dann auf **Makro-Einstellungen**.



Hier können Sie einstellen, ob Makros komplett blockiert werden sollen (Alle **Makros ohne Benachrichtigung deaktiveren**) oder immer automatisch aktiviert werden sollen (**Alle Makros aktivieren**). Beide Einstellungen sind nicht empfehlenswert: Die erste gibt Ihnen keine Information, wenn ein Dokument einen Makro hat (der ja gegebenenfalls sinnvoll und wichtig sein kann). Die zweite nimmt Ohnen die Möglichkeit, aufmerksam zu werden, wenn ein Dokument plötzlich einen Makro enthält, der gegebenenfalls bösartig ist.

Wählen Sie am besten **Alle Makros mit Benachrichtigung deaktivieren**: damit müssen Sie die Ausführung von Makros in einem Dokument explizit freigeben und können sich so gegebenenfalls noch beim Ersteller erkundigen, ob das seine Richtigkeit hat. Nach manueller Freigabe in einem Infotext am oberen Rand des Dokumentes werden Makros dann aber ganz normal und ohne Einschränkung ausgeführt.

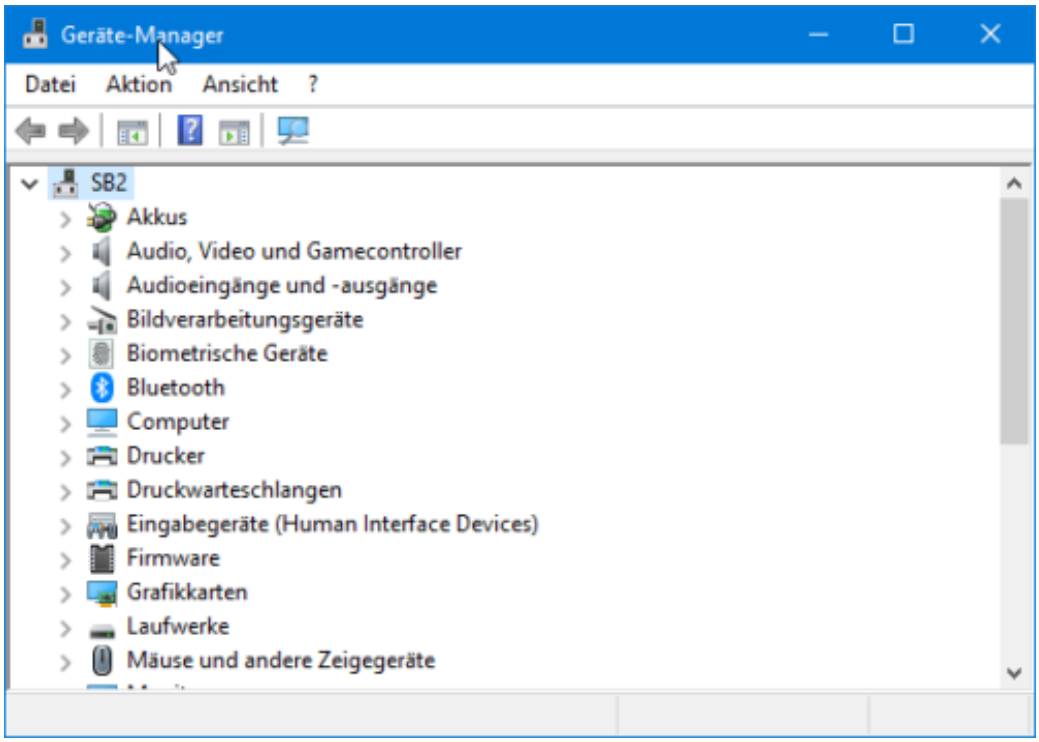
Aktivieren und Deaktivieren von Geräten unter Windows 10

Windows besteht nicht nur aus der reinen Software, mit der Sie Ihren PC verwenden. Jede einzelne Hardwarekomponente im System benötigt zusätzlich einen Treiber, ein kleines Stück Software. Dieser teilt Windows mit, wie es Daten mit dem Zubehörgerät austauschen soll. Nun sind Treiber leider oft Ursache für Hakler im Systembetrieb. Wir zeigen Ihnen wie Sie hier Abhilfe schaffen können.

[caption id="attachment_761133" align="alignnone" width="500"]

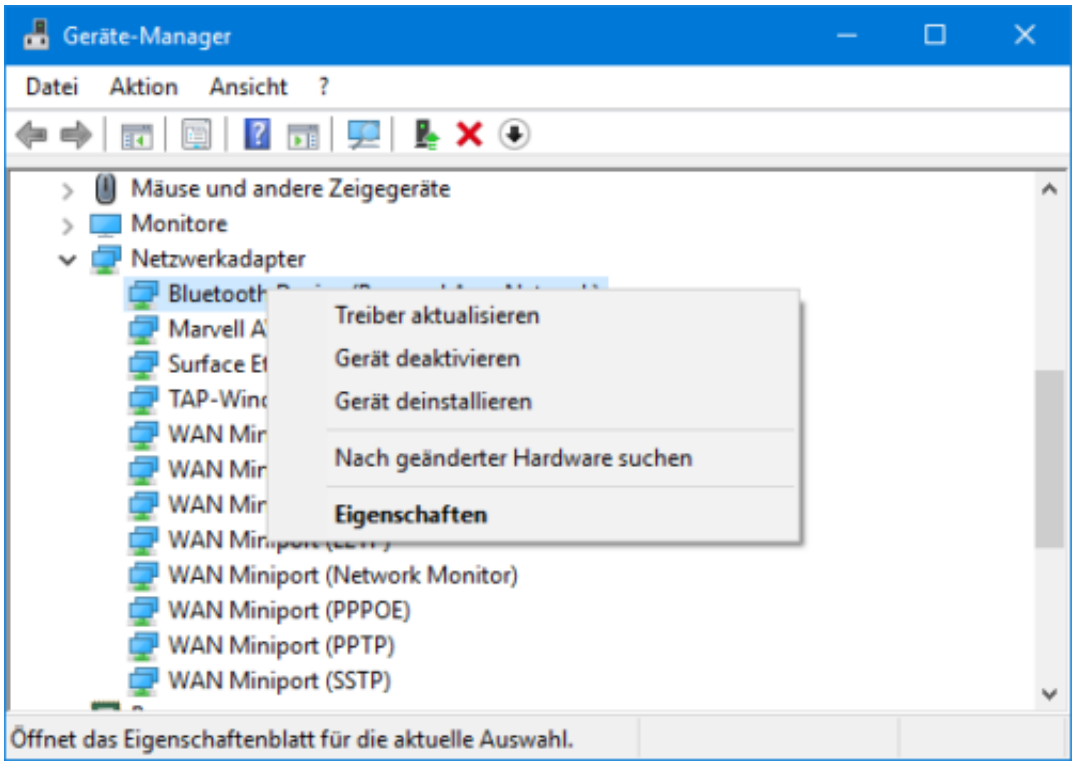

tookapic / Pixabay[/caption]

Die Gerätesteuerung ist quasi der Maschinenraum Ihres Windows 10-PCs. Öffnen Sie sie, indem Sie im Suchfeld in der Taskleiste **Geräte-** eingeben und dann auf das entsprechende Suchergebnis klicken.



Sie erhalten nun eine Auflistung aller Geräte, die Windows erkennt, nach Kategorien geordnet. Öffnen Sie eine Kategorie, indem Sie auf das **>-Zeichen** neben der Kategorie klicken. Nicht funktionierende Geräte sind mit einem Ausrufezeichen markiert.

Um ein Gerät zu deaktivieren, klicken Sie mit der rechten Maustaste auf **Gerät deaktivieren**. Damit wird das Gerät natürlich nicht physisch entfernt, wohl aber aus dem Zugriff von Windows genommen. Ein defektes oder mit einem störenden Treiber betriebenes Gerät, das Probleme bereitet, ist damit für Windows nicht mehr vorhanden.



In manchen Fällen ist die Ursache einer Störung ein veralteter Treiber. Vor der Deaktivierung eines Gerätes können Sie versuchen, über **Treiber aktualisieren** einen aktuelleren Treiber herunterzuladen und zu installieren.