Schieb Report

Ausgabe 2019.21

Wachsende Gefahren durch Hacker

Wir wissen es insgeheim: Durch die zunehmende Vernetzung von Geräten machen wir uns insgesamt angreifbarer. Denn in jedem einzelnen Gerät, in jeder Software schlummern Sicherheitslecks. Die Telekom beobachtet sehr genau, welche Angriffe erfolgen - und erstellt Statistiken. Der aktuelle Bericht ist besorgniserregend.

Die Telekom macht auf wachsende Gefahren durch Hacker aufmerksam. Anfang April hatte der Konzern 46 Millionen tägliche Angriffe auf seine "Honeypots" (Lockangebote für Hacker, damit sich ihr Verhalten messen und beobachten lässt).

Dies ist ein neuer Spitzenwert. Im Schnitt gab es im letzten Monat (April 2019) 31 Millionen Angriffe pro Tag. Im April 2018 waren es durchschnittlich noch 12 Millionen. Der April-Wert 2017 lag noch bei 4 Millionen. Die Angriffszahlen steigen exponentiell. Dies gab der Konzern im Vorfeld der morgen beginnenden Potsdamer Sicherheitskonferenz bekannt.

Honeypots: Virtuelle Fallen für Hacker

Honeypots sind digitale Fallen im Internet. Vergleichbar sind sie Honigködern für Bären. Der Konzern lockt damit absichtlich Angreifer an. Die Telekom analysiert die Attacken und macht aus den Erfahrungen eigene Systeme und die von Kunden sicherer. Knapp 3.000 verschiedene Fallen hatte die Telekom im April im Internet ausgelegt. Angriffszahlen auf die Köder der Telekom-Unternehmen gelten in der Branche als Haltepunkt für Cybersicherheit. Sie zeigen wie umtriebig Hacker im Internet sind.

Dirk Backofen, Leiter Telekom Security, sagt: „Fünfzig Milliarden Geräte werden wir nächstes Jahr im Internet sehen. Jeder und alles ist vernetzt und braucht Cyber-Security. Dies schafft niemand allein.

Wir brauchen die Armee der Guten. Dafür teilen wir unser Wissen für eine Immunisierung der Gesellschaft gegen Cyber-Attacken. Nur im Schulterschluss zwischen Politik, Wissenschaft und der Privatwirtschaft werden wir erfolgreich die Hacker in die Schranken weisen können."

Mehr als ein Viertel der Hacker zielt auf Kontrolle über fremde Rechner.
Die Telekom veröffentlicht auch eine Statistik zu Angriffen auf Lockfallen. Danach zielten 51% der Attacken auf die Netzsicherheit. Hacker konzentrierten sich dabei auf Schnittstellen für die Fernwartung von Computern.

In 26% der Fälle ging es dem Angreifer um die Kontrolle über einen fremden Rechner. Rund 7% der Attacken zielten auf Passwörter. 5% der Angriffe galten Internetseiten. Die Telekom Security beobachtet täglich drei bis acht unbekannte Angriffstaktiken. Aus den im Schnitt monatlich 250 neuen Hacker-Tricks lernt der Konzern Abwehr für sich selbst und seine Kunden.

Sorge vor Datendiebstahl

Passwort-Diebstahl beschäftigt den Kundenservice der Telekom intensiv. Rund 110.000 Kunden hatten im April diese Sorge und riefen bei der Hotline an. Immer wieder fallen Kunden auf das sogenannte Phishing herein. Ausgangspunkt solcher Angriffe sind gefälschte E-Mails. Sie sehen denen von Banken, Sparkassen, Online-Versendern oder Telekom-Firmen täuschend ähnlich. Sie zielen auf Betrug ab. Opfer geben darüber Kundenkennwort oder Zugangsdaten heraus. Diese nutzt der Angreifer für seine Zwecke aus.

[caption id="attachment_762791" align="alignnone" width="500"]

Double exposure of businessman touch padlock virtual currency with technology background, Cyber Security Data Protection Business Technology Privacy concept.[/caption]

Angriffe durch gekaperte Computer massiv gestiegen

Heftiger werden auch die Angriffe auf Fest- und Mobilfunknetz der Telekom. So feuerten im April Botnetze 5,3 Billionen Datenpakete auf die Telekom. Im Vorjahr waren es noch 330 Milliarden. Botnetze bestehen aus einer großen Zahl gekaperter Computer oder Smartphones. Fremdgesteuert senden diese gemeinsam Datenpakete auf ein Ziel.

Verträgt das Ziel den Ansturm der Daten nicht, bricht es zusammen. An den Übergängen von ihrem Netz zum Internet hat die Telekom Sensoren installiert. Diese fanden heraus: Botnetze nutzen Internetsurfer von Unternehmen aus. Sie greifen an, wo Firmen zwangläufig Datenwege freihalten. Dort schützen keine Firewalls. Wo der Internet-Browser seine Datenpakete aus dem Netz bekommt, lauern die gekaperten Zombie-Rechner.

KI setzt Cyber-Abwehr unter Druck

Neben exponentiell steigenden Zahlen registriert die Telekom Security grundsätzliche Trends bei Cyber-Attacken. So entsteht seit Jahren eine Hacker-Industrie. Gruppen spezialisieren sich auf bestimmte Angriffstypen und bieten diese an.

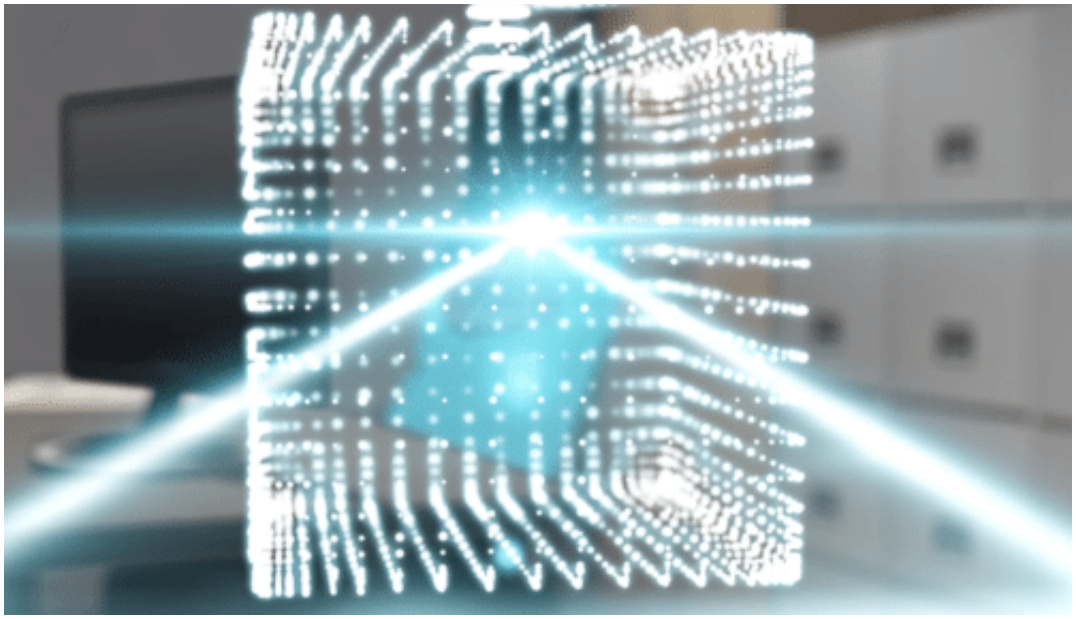
Ein Kunde stellt sich die Services verschiedener Gruppen dann je nach Bedarf und Ziel zusammen. Nach wie vor kommen die meisten Hacker-Gruppen aus China und Russland. Dabei steigt der Anteil von Attacken mit künstlicher Intelligenz. Angriffe sind daher heute viel schneller erfolgreich. Die Cyberabwehr setzt das unter Druck. Sie kontert immer mehr mit Gegenmaßnahmen in Echtzeit.

Legaler Hack: Daten sammeln und durchleuchten

Immer wieder gibt es Sicherheitskonferenzen, auf denen alle möglichen Aspekte diskutiert werden - vor allem Cyber- und Hackangriffe. Absolut realistische Szenarien, die ernst genommen werden müssen. Dabei geraten allerdings alltägliche Hacks ein wenig aus dem Sichtfeld: Konzerne sammeln Daten - und erstellellen messerscharfe Profile. Und dagegen wird nichts unternommen.

So lautet das jüngste Motto des BSI (Bundesamt für Sicherheit in der Informationstechnik): “IT-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung".

Da will ich unbedingt zustimmen. Mehr Sicherheit führt zu mehr Akzeptanz. Vor allem aber zu mehr Sicherheit - und das ist das Wichtigste. Denn noch immer werden die möglichen Probleme von vielen unterschätzt. "Unwahrscheinlich", "fast unmöglich", "schwer vorstellbar" - und dann passiert es eben doch. Aus Zufall. Oder weil Kriminellen oder Geheimdiensten selbst die winzigsten Lücken ausreichen, um zuzuschlagen und/oder um sich zu bedienen.



Legaler Hack: Daten sammeln und analysieren

Doch viel bedrohlicher erscheint mir der legale Hack - in unsere Köpfe. Unternehmen sammeln Daten in nie gekanntem Ausmaß und machen sich im wahrsten Sinne des Wortes ein Bild von uns.

Die Schwierigkeiten, die mit der dreisten Datenanhäufung einhergehen, werden gerne übersehen oder kleingeredet. Daten, die große Onlinedienste völlig legal einsammeln und KI-mäßig verarbeiten - so dass rasiermesserscharfe Waffen entstehen.

Denn wenn Onlinedienste oder Soziale Netzwerke zum Beispiel die Psyche eines Nutzers extrem treffsicher einschätzen können, dann ist das nicht nur unangenehm für den Betroffenen, sondern eben auch bedrohlich bis sogar gefährlich.

Doch was passiert? Nichts. Wir haben uns daran gewöhnt, dass Amazon uns bestens kennt - weil unser Kaufverhalten penibel untersucht wird. Wir finden nichts mehr dabei, dass auch Google, Facebook und große Werbenetzwerke ungeniert alle Daten sammeln, derer sie habhaft werden können.

Profiling durch Streamingdienste und mehr

Datenschutzexpertin Katharina Nocun hat mir auf der re;publica19 gezeigt, welche Daten zum Beispiel Netflix hat. Weil der Streamingdienst genau registriert, was wir schauen, wann wir schauen, wo wir anhalten, welche Szenen wir überspringen oder wiederholen - das erlaubt konkrete Aussagen, in welcher seelischen Verfassung jeder einzelne von uns ist.

Erst Recht, wenn diese Daten noch mit anderen kombiniert werden - was ununterbrochen und immer häufiger geschieht. Amazon hält ein Patent darauf, die Stimmung einer Person zu erkennen, die gerade mit Alexa spricht. Anhand der Stimmlage. Husten oder Trennung? Vorfreude auf den Geburtstag oder generell gute Laune? Amazon könnte es schon bald wissen...

Wenn das nicht spooky ist. Es sind also keineswegs nur die möglichen Cyber- und Hackangriffe, die problematisch sind. Die Daten-Absauge-und-Analyse-Wut ist viel schlimmer. Vor allem, da sie meist legal erfolgt - und völlig intransparent ist.

https://vimeo.com/337513137

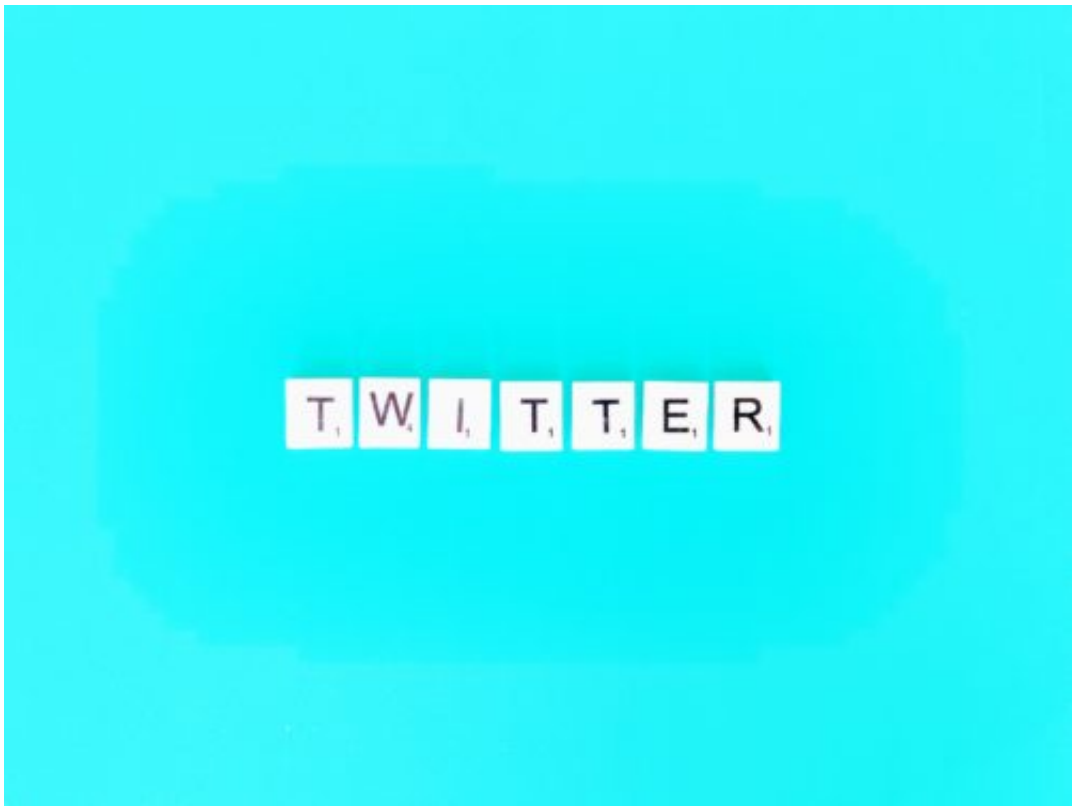
Streamingdienste sammeln unbemerkt selbst psychologische Daten

Was Twitter gegen Desinformation macht

Weil die Sozialen Medien immer wieder genutzt werden, um gezielt Falschinformationen zu verbreiten, Stimmung zu machen oder sogar Wahlwerbung zu betreiben, hat die EU die Regeln für die Sozialen Netzwerke verschärft. Bei Twitter geht es aber derzeit drunter und drüber.

Soziale Netzwerke müssen transparent machen, wer Werbung schaltet – und gegen gezielte Desinformation oder Hetze vorgehen. Nicht nur Facebook und YouTube, sondern auch Twitter. Doch bei Twitter hat es irritierende Maßnahmen gegeben: Sperrungen, Blockaden... Algorithmen entscheiden eben nicht immer zuverlässig. Im Gegenteil.

Für politische Debatten ist Twitter besonders wichtig. Denn hier ist nicht nur der US-Präsident eifrig aktiv, sondern mittlerweile die meisten Parteien und Politiker. Und auch wir Journalisten.



Auf Twitter wird Meinung gemacht

Auf Twitter wird Meinung gemacht – und deshalb ist der Zwitscher-Dienst natürlich unwiderstehlich für alle, die – aus womöglich unlauteren Motiven – die öffentliche Meinung beeinflussen wollen.

Oft genug mit Hetze, Pöbeleien, dreisten Falschbehauptungen – und Manipulationsversuchen. Deswegen hat die EU-Kommission auch Twitter in die Pflicht genommen: Twitter verbietet deshalb ausdrücklich das "Posten und Teilen von Inhalten, die sich negativ auf die

Wahlbeteiligung auswirken oder falsche Angaben zum Termin, zum Ort oder zum Ablauf der Wahl machen".

Damit kann man doch arbeiten. Wer also schreibt: "Geht nicht zur Wahl" – oder "die Spanier wählen erst am 1. September", der muss damit rechnen, dass Twitter den Tweet löscht. Zu Recht, wie ich finde.

Twitter blockiert Tweets und Account grundlos

So weit, so klar. Doch in jüngster Zeit wurden jede Menge Twitter-Accounts von Institutionen und Personen blockiert, die gegen keine dieser Regeln verstoßen haben. Die Jüdische Allgemeine zum Beispiel, die Berliner Staatssekretärin Sawsan Chebli – die gerne schon mal mit spitzer Zunge formuliert -, der Schriftsteller Tom Hillenbrand, auch einige offizielle Kandidaten fürs EU-Parlament.

Alle Betroffenen wollten auf keinen Fall die Wahl beeinflussen – einige Tweets hatten nicht mal was mit der Wahl zu tun.

Was zeigt: Das gewünschte Ziel wird nicht erreicht – es wird sogar die Meinungsfreiheit gestört.

Deshalb müssen unbedingt verlässliche Regeln her, vom Gesetzgeber – glasklar formuliert. An die müssen sich die Sozialen Netzwerke dann klar halten.

Nur vage Vorgaben: Politik muss besser werden

Doch die Vorgaben sind vage – die Art und Weise, wie Twitter die Probleme in den Griff bekommen will, sind ungeeignet, teilweise sogar schädlich.

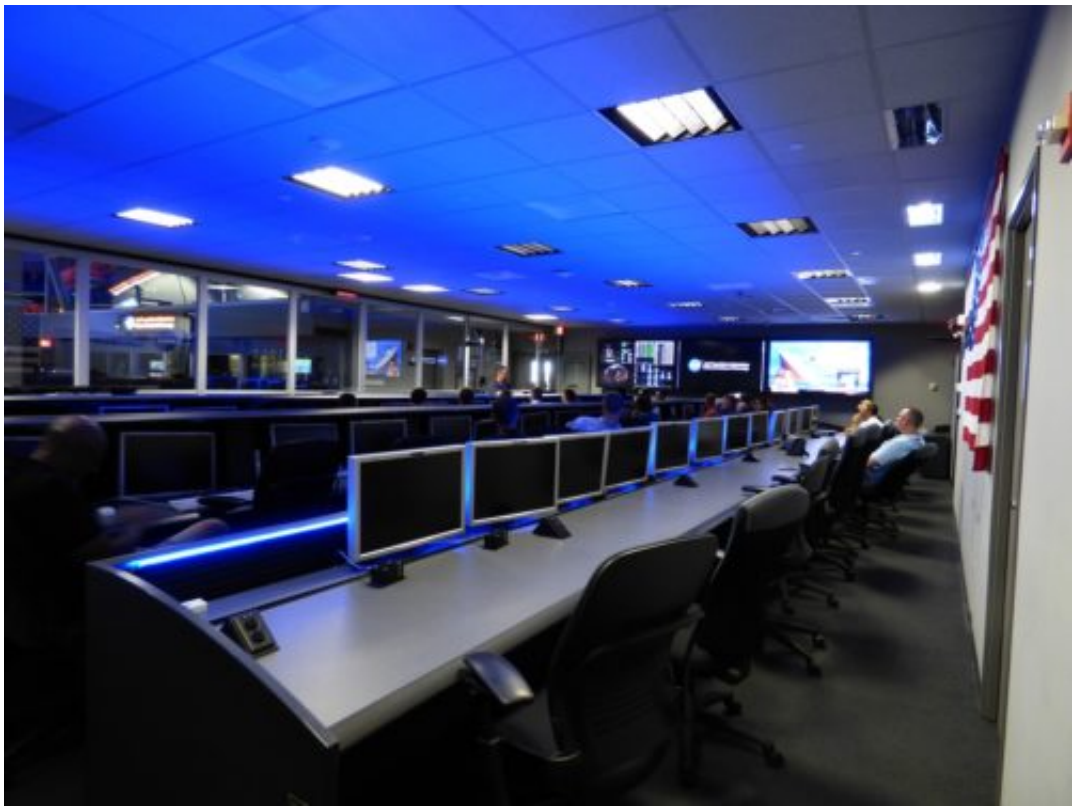
Nicht Algorithmen entscheiden bei Twitter, ob ein Tweet gelöscht oder ein Account gesperrt wird, sondern Mitarbeiter aus Fleisch und Blut. Immerhin. Aber die sitzen überall auf der Welt und sind offensichtlich nicht besonders gut geschult. Vermutlich werden auch nicht nur Muttersprachler mit der Aufgabe betraut.

Vorsicht bei Satire

Satire ist bei Twitter jedenfalls nicht erlaubt. Wer einen Scherz macht, etwa sagt: „Unterschrift unter dem Wahlzettel nicht vergessen“, der wird gesperrt. Obwohl es juristisch unbedenklich ist.

Ein anderes Problem: Tweets melden! Es gibt offensichtlich vor allem im sogenannten rechten Spektrum des politischen Geschehens den Trend, verstärkt die Accounts von eher linken User zu melden. Immer wieder. Bis sich ein Prüfer erbarmt – und sperrt.

Ein Chaos. Es gibt keine klaren Regeln. Entsprechend miserabel ist das Ergebnis: Manchmal sperrt Twitter Tweets oder Accounts, die sich nichts haben zu schulde kommen lassen, dann bleiben Tweets online, die glasklar das Kriterium Hetze oder Manipulation erfüllen.



Unzureichend geschulte Mitarbeiter

Mit Algorithmen lässt sich dem Problem nicht beikommen. Auch mit Hilfskräften nicht, die in Sekundenbruchteilen entscheiden sollen, was in Ordnung geht und was nicht – wofür Juristen sich oft stundenlang streiten können.

Onlinedienste wie Twitter, Facebook oder Youtube verdienen Milliardenbeträge. Jeden Monat. Investieren aber nur absurd geringe Summen in solche Projekte. Sie nehmen ihre Verantwortung nicht ernst. Da können sie behaupten, was sie wollen.

Allerdings lassen sich einige Probleme auch nicht wirklich lösen. Der Staat kann unmöglich die Entscheidungsgewalt darüber, was öffentlich geäußert werden darf und was nicht, in die Hände von auf Gewinnmaximierung optimierte Konzerne geben. Auch das ist ein Armutszeugnis – der Politik.

Es braucht also klare Regeln – und nicht nur wachsweiche Formulierungen wie "Wahlbeeinflussung ist zu unterbinden". Wie genau? Diese Frage muss die Politik beantworten.

https://soundcloud.com/user-999041145/ttb-netzdenker-twitter

Google sperrt Android für Huawei

Google stellt die Zusammenarbeit mit Huawei ein. Bis auf weiteres bekommen die Chinesen keine Hard- und Software mehr. Mit Folgen für alle, die ein Smartphone mit Huawei-Logo benutzen.

Der chinesische Hersteller Huawei ist mittlerweile der zweigrößte Handyhersteller der Welt - nach Samsung und vor Apple.

US-Präsident Trump hat ein Dekret unterschrieben.

"Telekommunikationsnotstand" genannt. Das verbietet US-Konzernen die Zusammenarbeit mit chinesischen Unternehmen, die auf einer "schwarzen Liste" der Regierung stehen, etwas weil sie unter Spionageverdacht stehen – unter anderem Huawei. Vermutlich ist auch die Marke Honor betroffen, die zum Huawei-Konzern gehört. Google ist also praktisch gezwungen, solche Maßnahmen zu ergreifen.

Google hat die Folgen konkretemn bekanntgegeben: Der US-Konzern beendet die Zusammenarbeit mit Huawei. Die Chinesen bekommen keine Hard- und vor allem auch keine Software mehr von Google. Das hat Folgen für die ganze Welt, denn wenn Huawei keine Software bekommt, können die Mobilgeräte auch nicht entsprechend ausgerüstet werden.

Die konkreten Folgen für Kunden

Huawei-Kunden können ihre Geräte erst mal normal weiter benutzen. Bereits verkaufte Geräte können auch weiterhin auf Google Play und Google Protect zugreifen, sich also mit Apps

versorgen. Auch Google Mail und Google Maps können weiterhin benutzt werden.

Das Android-Betriebssystem sorgt auch weiterhin für Viren-Scans und allem, was dazu gehört. Auch sollen Sicherheits-Updates erst mal weiter ausgeliefert werden. Allerdings wird Huawei nicht mit neuen Versionen vom Android-Betriebssystem versorgt – die bleiben den Kunden also versperrt.

Nicht nur in den USA, sondern überall auf der Welt. Bei künftigen Geräten sind die Folgen heftiger. Künftige Geräte dürfen nicht mehr mit Android ausgestattet sein, Dienste wie Google Maps, Google Mail oder Google Play sind gesperrt.

[caption id="attachment_762722" align="alignnone" width="500"]


Auch Marke Honor betroffen[/caption]

Künftige Geräte müssen ohne Android auskommen

Wichtig zu wissen ist erst mal: Im Augenblick sieht es so aus, als ob künftige Huawei-Geräte nicht mehr mit Android und Google-Diensten arbeiten dürfen. Wer also seiner Marke treu bleiben möchte – was viele ja gerne tun –, dürfte in Zukunft Schwierigkeiten haben. Denn ein Umstieg auf ein Huawei-Betriebssystem? Das werden die meisten nicht wollen. Die Apps funktionieren dann nicht mehr.

So kommt es natürlich nur, falls der Handelsstreit nicht beigelegt werden kann. Das könnte durchaus passieren. Huawei wird ein eigenes mobiles Betriebssystem entwickeln müssen, um seine Handys künftig verkaufen zu können. Denn iOS von Apple steht nicht nur Auswahl – und andere Alternativen gibt es nicht. Für asiatischen Markt würde das sicher akzeptiert — aber im Rest der Welt eher nicht.

Handelskrieg auf dem Rücken der Nutzer

Die USA haben Huawei und damit auch die Tochter Honor auf eine schwarze Liste gesetzt – weil sie Spionage befürchten. Gibt da Beweise, dass eine konkrete Gefährdung vorliegt? Muss ich als Nutzer dankbar sein, dass hier ein Schutz aufgebaut wird. Oder wird hier aus Ihrer Sicht ein Handelsstreit auf dem Rücken der Nutzer ausgetragen?

Die Frage ist schwierig zu beantworten. Ich denke: Von allem ein bisschen. Konkrete Belege, die überzeugend wären, dass Huawei spioniert, gibt es bislang nicht. Es besteht lediglich der Verdacht. Den halte ich allerdings auch für ausgesprochen begründet.

Denn in China sind alle chinesischen Unternehmen zur Zusammenarbeit mit Staat und Regierung verpflichtet. Wenn sie spionieren können, dann werden sie es auch tun – und Daten ausliefern. In China wird die eigene Bevölkerung schließlich sehr umfassend ausspioniert.

Der Handelskrieg zwischen USA und China ist auch nicht völlig unbegründet. Die Methoden, mit denen hier vorgegangen wird, sind allerdings fraglich. Und deshalb: Ja, der Handelskrieg wird durchaus auf den Rücken der Konsumenten ausgetragen. Aber auch US-Konzerne könnten spionieren. Das wissen wir seit Snowden. Generell müsste mehr Transparenz herrschen.

https://vimeo.com/337240636

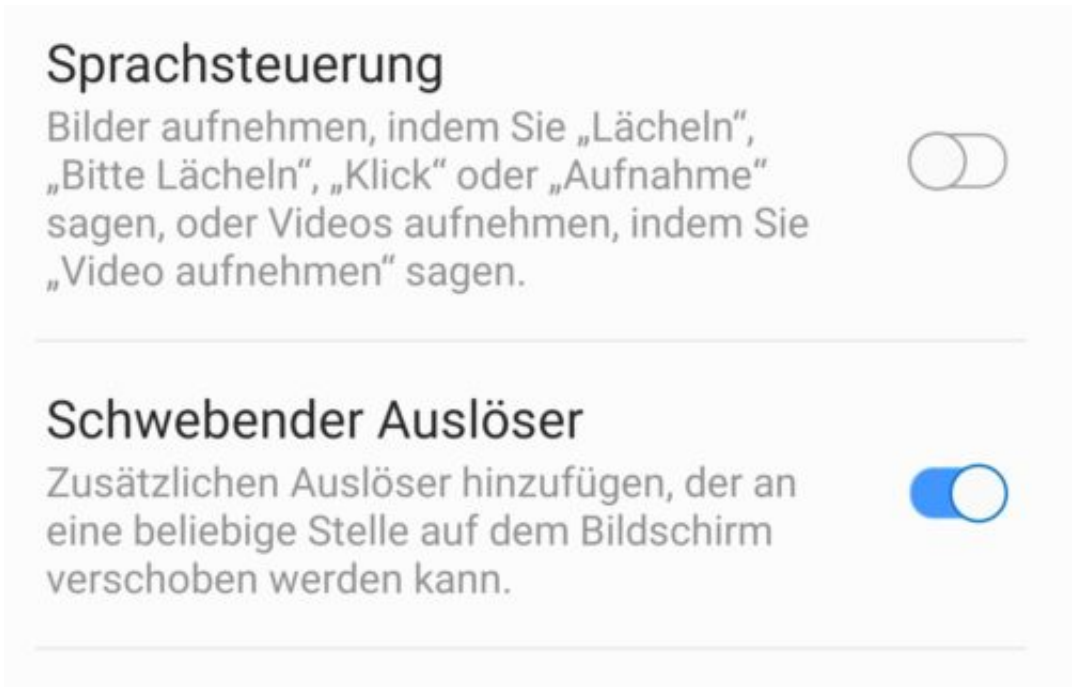
Variablen Auslöser in der Kamera-App aktivieren

Unser Smartphone ist der perfekte Kamera-Ersatz: Die Bilder haben mittlerweile eine hohe Qualität, der Speicher ist groß und nachrüstbar, es ist immer mit dabei und kann dazu noch Bilder schnell auf sozialen Netzwerken teilen. Einzig seine Form kann eine Herausforderung sein: Es ist nicht so griffig wie eine Digitalkamera, und damit manchmal schwer einhändig zu bedienen. Samsung hat bei den S10 und S10+ eine softwareseitige Anpassung vorgenommen.

Das Problem ist meist der Auslöser, der sich mittig am unteren Bildschirmrand auf dem Display befindet und nicht so ganz einfach zu erreichen ist. Eher wackelt das Telefon, was wiederum der Schärfe der Bilder nicht zuträglich ist.

Dafür können Sie einen zweiten Auslöser auf den Bildschirm bringen und diesen so platzieren, dass Sie ihn leicht erreichen können. Die optimale Position ist von vielen Faktoren abhängig: Der Größe des Gerätes, der Größe Ihrer Finger, der Positionierung des Displays im Gerät. Hier müssen Sie also ausprobieren.

Aktivieren können Sie diesen "Schwebenden Auslöser" in der Kamera-App unter **Einstellungen** > **Schwebender Auslöser**. Ist dieser aktiviert, dann können sie Ihn durch Schieben mit dem Finger an die richtige Position bringen.


Sprachsteuerung
Bilder aufnehmen, indem Sie „Lächeln“, „Bitte Lächeln“, „Klick“ oder „Aufnahme“ sagen, oder Videos aufnehmen, indem Sie „Video aufnehmen“ sagen.
Schwebender Auslöser
Zusätzlichen Auslöser hinzufügen, der an eine beliebige Stelle auf dem Bildschirm verschoben werden kann.

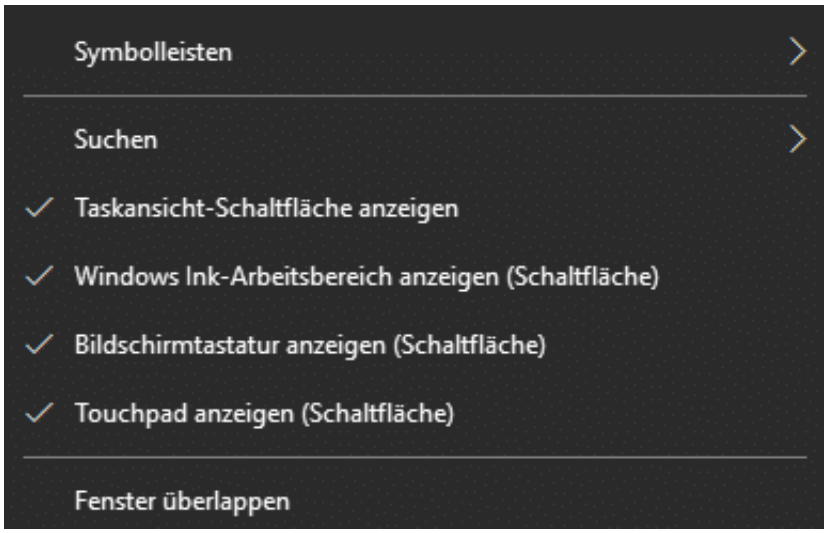
Optimieren der Task-Leiste unter Windows 10

Die Task-Leiste ist mit ihrer definierten Position unten am Bildschirm ist eines der prominentesten Bedienelemente in Ihrer Arbeit mit Windows 10. Im Standard blendet das System hier die Suchleiste für Cortana und den Shortcut für die Taskansicht/Zeitleiste an. Diese beiden Felder nehmen Platz auf dem Bildschirm weg, die Sie für das schnelle Auffinden von laufenden Apps dringend benötigen. Darum schalten Sie diesen Platz einfach frei!

[caption id="attachment_762692" align="alignnone" width="500"]

Free-Photos / Pixabay[/caption]

Klicken Sie mit der rechten Maustaste auf die Taskleiste, dann entfernen Sie den Haken bei **Taskansicht-Schaltfläche anzeigen**. Damitr entfernen Sie "nur" den Shortcut zur Zeitleiste, bei dem engen Platzangebot ist das aber schon einmal ein erster Schritt, ein weiteres Programmsymbol sichtbar zu halten.

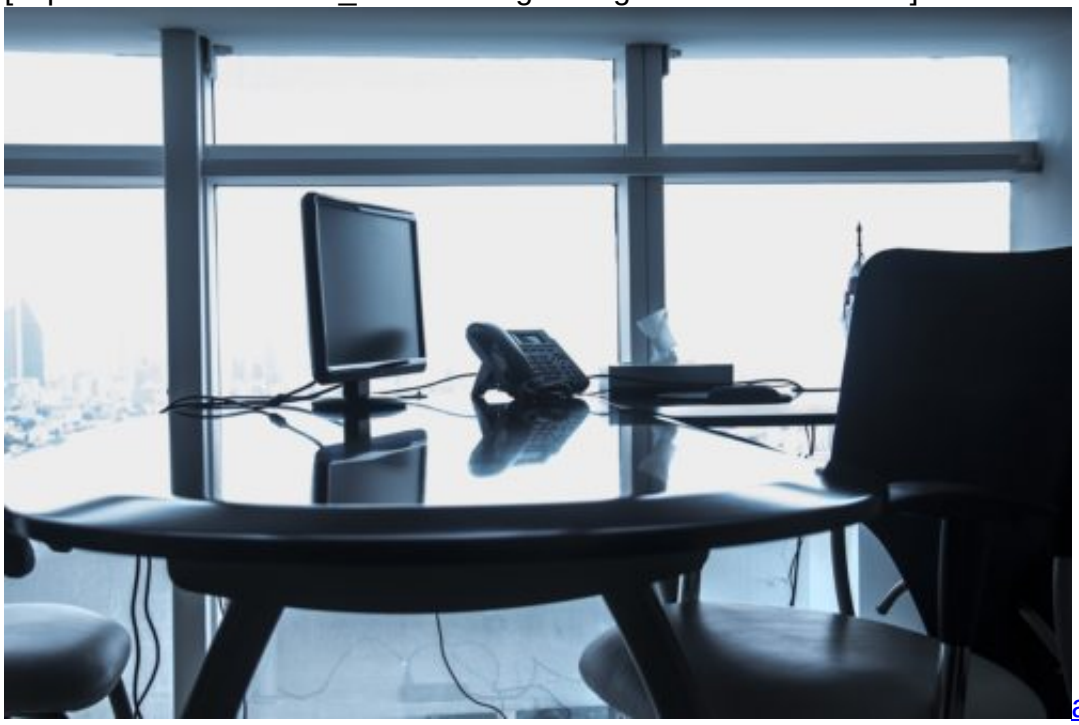


Über denselben Weg wählen Sie unter **Cortana** > **Cortana-Symbol anzeigen** (statt **Suchfeld anzeigen**). Statt der breiten Eingabefläche für Suchbegriffen haben Sie dann nur das Cortana-Symbol sichtbar, ein Klick darauf öffnet aber ein ganz normales Suchfeld und nutzt Cortana weiter.

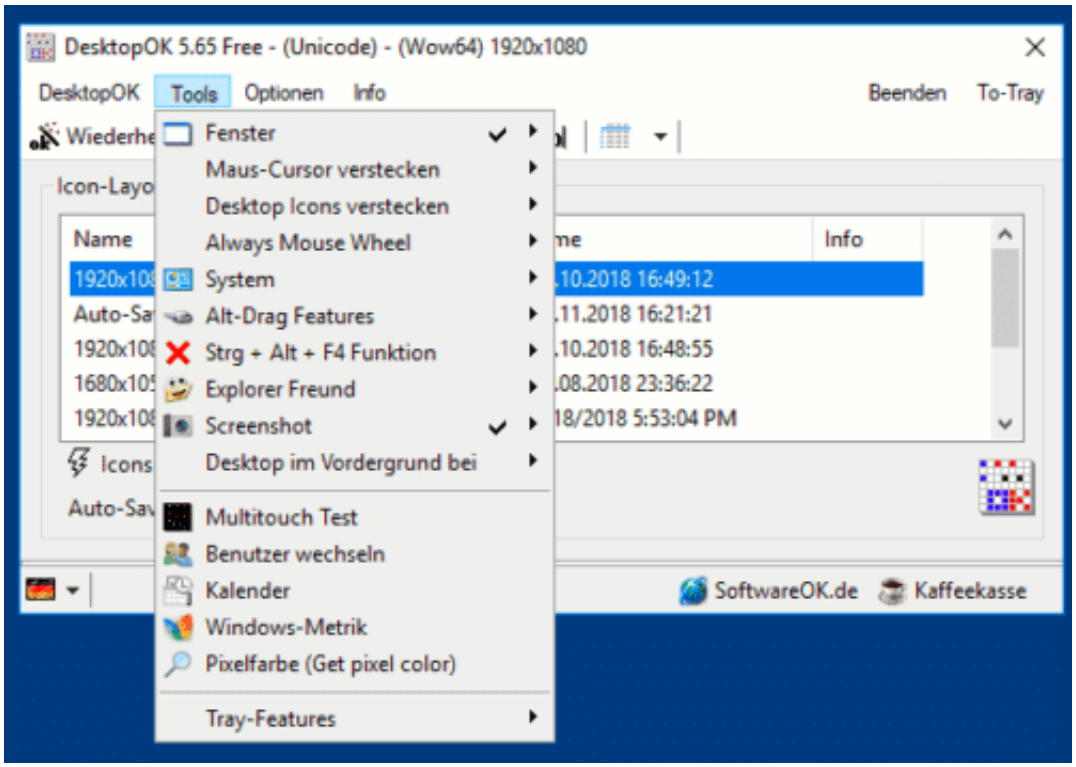
Wenn Sie den Cortana-Eintrag nicht zur Vefügung haben, dann liegt das wahrscheinlich daran, dass Sie Cortana in den Datenschutzeinstellungen Cortana deaktiviert haben.

Speichern der Desktop-Symbole

Der eine Anwender nutzt den Desktop gar nicht, der andere nach einem ausgeklügelten System. Egal zu welchem Anwendertypus Sie gehören: Die Anordnung der Symbole sollte möglichst gleich sein, sonst verschwenden Sie Zeit mit der Suche. Windows 10 bietet hier von Haus aus wenig Möglichkeiten, lässt sich aber durch Programme erweitern.

[caption id="attachment_762659" align="alignnone" width="500"]

aracelymitsu / Pixabay[/caption]

Einzig die automatische Anordnung der Symbole wird systemseitig unterstützt. Klicken Sie mit der rechten Maustaste auf den Desktop, dann auf **Ansicht** > **Symbole automatisch anordnen**. Damit werden die Symbole zumindest vor versehentlichem leichtem Verschieben geschützt.



Eine leistungsfähigere Alternative ist die Freeware DesktopOK (https://www.softwareok.de/?seite=Freeware/DesktopOK). Mit dieser kleinen Software können Sie die Anordnung der Symbole auf dem Desktop mit ihren Größen und Positionen sichern. Das sogar regelmäßig. Ist Ihr Desktop in Unordnung, dann können Sie die gespeicherte Position der Symbole schnell wiederherstellen.

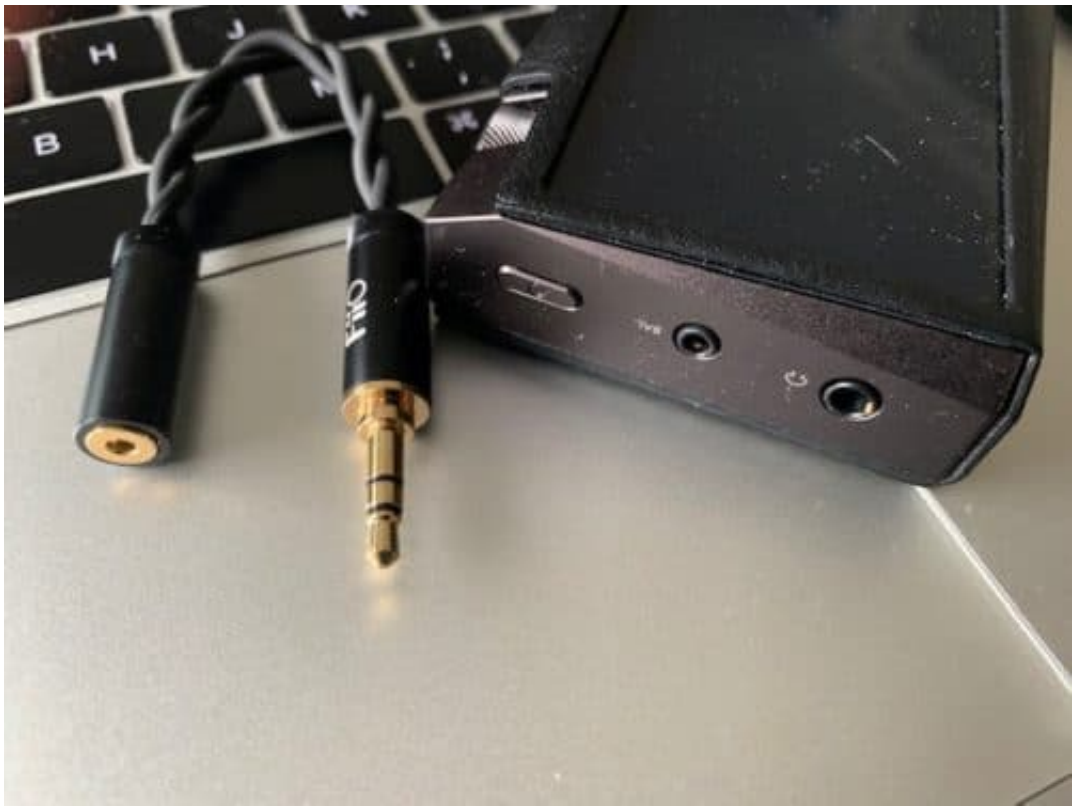
Symmetrische Kopfhöreranschlüsse auf 3,5mm Klinke adaptieren

Audiophiler Musikgenuss ist vor allem abhängig von der Hardware, mit der Sie Ihre hochauflösenden Musikdateien anhören. Die HiRes-Player der verschiedenen Hersteller wie Onkyo, Fiio, Astell&Kern und anderer versuchen oft, durch zwei Wandler die Qualität der beiden Stereokanäle zu erhören. Dafür wird dann ein symmetrischer Kopfhöreranschluss verwendet, der statt einem 3,5mm- einen 2.5mm-Klinkenanschluss verwendet. Kopfhörern liegen dann meist zwei Kabel bei. Wenn Sie aber nicht andauernd zwischen dem Player-Kabel und dem 3,5mm-Kabel für den Anschluß des Kopfhörers an Ihren PCs wechseln wollen, macht ein Adapter Sinn. Leider gibt es auf dem Markt eine riesige Menge an Adaptern aus Fernost, bei denen es aber Glücksspiel ist, ob sie funktionieren oder nicht.

[caption id="attachment_762715" align="alignnone" width="500"]

OpenClipart-Vectors / Pixabay[/caption]

Wichtig ist dabei, dass zum einen die Kombination aus Stecker (3,5mm) und Buchse (2,5mm) die richtige ist, zum anderen aber eben auch die interne Verdrahtung des Kabels. Wenn die Pole nicht richtig mit einander verbinden sind, dann können im schlimmsten Fall Teil der Soundkarte beschädigt werden.



Die Lösung kommt markenübergreifend vom Hersteller Fiio. Das Fiio BL35 ist ein kleines Adapter, das von dem symmetrischen 2,5mm-Klinkenanschluss auf den 3,5mm-Anschluss Ihres Notebooks oder Tablets adaptiert und klanglich einwandfrei funktioniert.

Der God Mode unter Windows 10

Wenn Sie Ihr Windows 10 System unter Kontrolle haben und effektiv verwalten wollen, dann benötigen Sie eine Vielzahl von Einstellungen und Funktionen. Diese verstecken sich an den verschiedensten Stellen des Systems und sind nicht schnell an einer zentralen Stelle zu erreichen. Abhilfe schafft hier der „God Mode“. Für diesen brauchen Sie keine langen, komplexen Einstellungen, es reicht ein kleiner Trick.

[caption id="attachment_762654" align="alignnone" width="500"]

pixel2013 / Pixabay[/caption]

Legen Sie an einer beliebigen Stelle einen neuen Ordner an, dem Sie dann den kryptischen Namen

GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}

geben. Statt **GodMode** können Sie natürlich auch einen beliebigen anderen Namen wählen. Das Symbol springt sofort von dem eines Ordners zu dem der Systemeinstellungen um. Wenn Sie den Ordner Doppelklicken, dann erhalten Sie ein zentrales Menü mit allen wichtigen Einstellungen.

Dies ist deutlich umfangreicher als das über **Windows** + **X** aufzurufende Shortcut-Menü. Der GodMode richtet sich vor allem an Administratoren, die Zugriff auf Systemtools benötigen. Wenn Sie diesen Trick nutzen, dann seien Sie sich bewusst, dass viele dieser Tools Ihr System durcheinander bringen können, wenn Sie nicht genau wissen, wie diese anzuwenden sind.

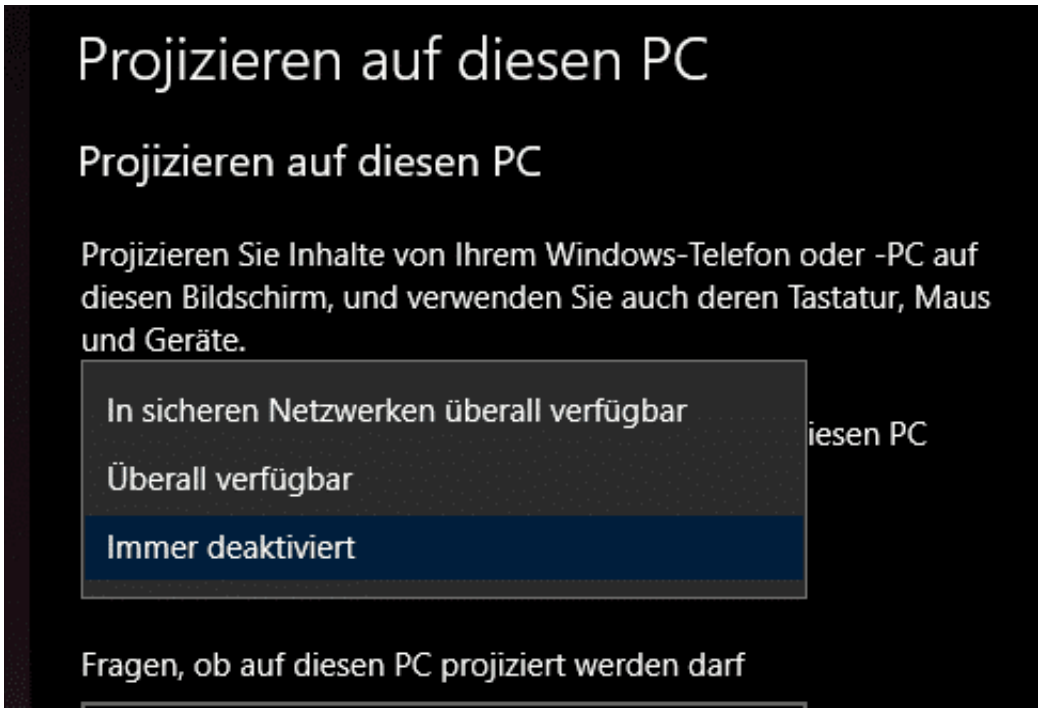
Projizieren auf einen PC unter Windows 10

In der Zusammenarbeit mit anderen Benutzern können Sie sich immer besser Dinge veranschaulichen, wenn Sie sie sehen und gezeigt bekommen statt nur eine Kopie oder einen Ausdruck in der Hand zu haben. Damit Sie sich dazu nicht einmal von Ihrem Platz wegbewegen müssen, hat Windows die Funktion der Projektion auf PCs mit an Bord..

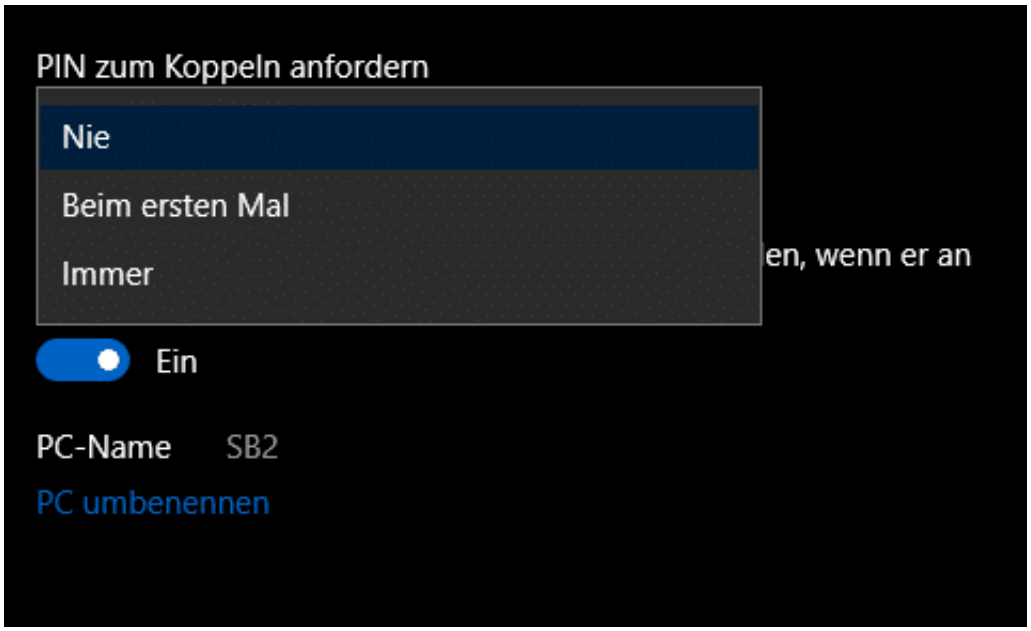
[caption id="attachment_762702" align="alignnone" width="500"]


LoboStudioHamburg / Pixabay[/caption]

Als Erstes müssen Sie den PC, auf dem Sie Inhalten anzeigen lassen wollen, dazu ermächtigen. Unter **Einstellungen** > **System** > **Projizieren** auf diesen PC können Sie festlegen, ob dieser PC immer zur Projektion zur Verfügung steht, nur auf Nachfrage oder gar nicht.

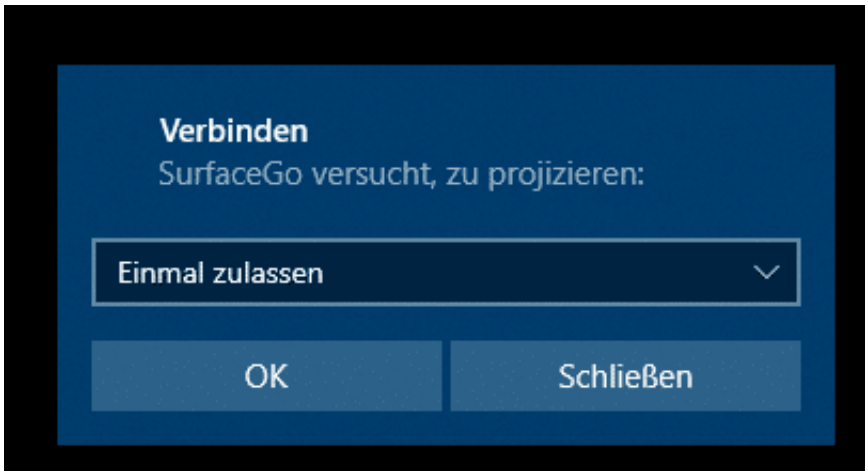


Haben Sie die Anzeige aktiviert, dann können Sie noch eine PIN anfordern lassen, damit zumindest ein gewisser Schutz besteht.



Nun können Sie mit einem anderen Windows-Gerät im Infocenter auf **Projizieren** klicken. Suchen Sie nach einer drahtlosen Anzeige, dann wird Ihnen das soeben freigeschaltete Gerät angezeigt und kann als kabelloses Display angewählt werden.

Auf diesem wird dann (je nach Einstellung) eine Nachfrage angezeigt, ob es zur Projektion freigegeben werden soll. Bejahen Sie das, dann wird das Display umgeschaltet auf den Inhalt des projizierenden Gerätes.


Verbinden
SurfaceGo versucht, zu projizieren:
Einmal zulassen
OK
Schließen

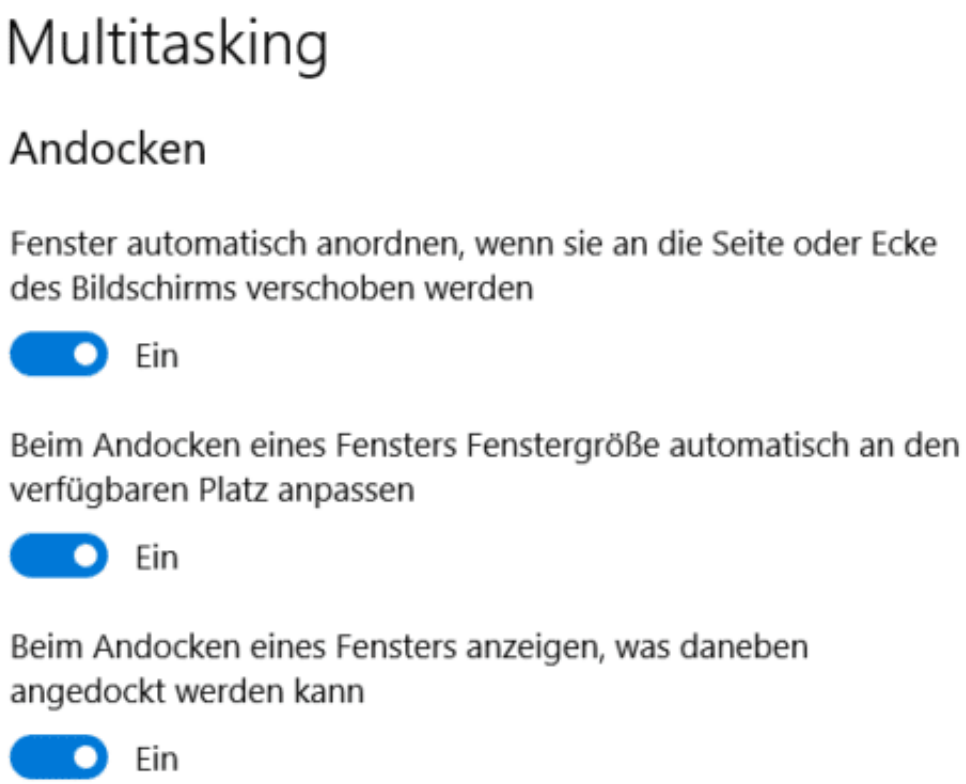
Ausschalten des automatischen Andockens von Fenstern

Ein wunderschöner visueller Effekt von Windows 10 ist das automatische Andocken von Fenstern. Ziehen Sie ein Fenster beispielsweise in die obere, rechte Ecke des Bildschirms, dann wird es genauso skaliert, dass es das obere rechte Viertel einnimmt. Was in manchen Situationen großartig ist, nervt bei anderen. Statt ein Fenster in einer benutzerspezifischen Größe zu akzeptieren greift Windows 10 ein und macht es genau viertelgroß. Das kostet Zeit und Nerven, lässt sich aber schnell ausschalten.

[caption id="attachment_762651" align="alignnone" width="500"]

ChristopherPluta / Pixabay[/caption]

Klicken Sie auf **Einstellungen** > **System** >**Multitasking** und schalten Sie dann die **Einstellung Fenster automatisch anordnen, wenn sie an die Seite oder Ecke des Bildschirms verschoben werden** aus. Damit können Sie Größe und Position eines Fensters auf dem Bildschirm ohne automatischen Einfluss von Windows 10 festlegen. Natürlich können Sie die Funktion jederzeit wieder einschalten.



Das bietet sich vor allem dann an, wenn Sie zwei Monitore nebeneinander stehen haben. Das Schieben von Fenstern über die Monitorgrenzen hinaus ist einfacher, wenn die Automatismen zum automatisch Skalieren von Fenstern ausgeschaltet sind.

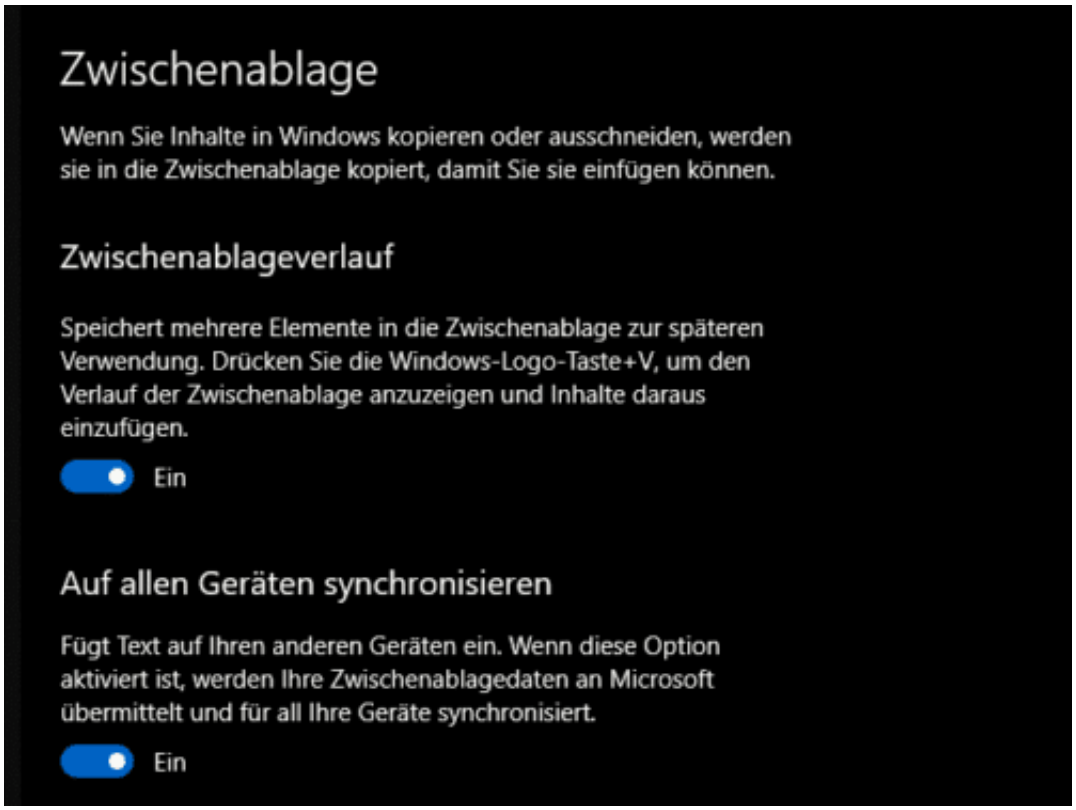
Nutzen der Cloud-Zwischenablage

Die Zwischenablage ist seit Jahren die schnellste und komfortabelste Möglichkeit, Daten zwischen Programmen hin und her zu kopieren. Oft vermissen Sie dann aber ein Element, dass Sie durch ein neues überschrieben haben, und auch die Möglichkeit der Synchronisation von Elementen zwischen Geräten wäre toll? Windows 10 hat diese Funktion ganz versteckt nachgeliefert!

[caption id="attachment_762697" align="alignnone" width="500"]

FotografieLink / Pixabay[/caption]

Über **Einstellungen** > **System** > **Zwischenablage** können Sie den **Zwischenablageverlauf** einschalten. Sie können hier mit geeigneten Apps auch die Synchronisation mit einem Smartphone aktivieren. Dazu benötigen Sie für Android die SwiftKey-App, die Sie sich direkt als Link per SMS zusenden lassen können.



In nahezu jedem Windows-Programm können Sie dann durch Drücken von **Windows** + **V** auf die erweiterte Zwischenablage zugreifen. Die zeigt Ihnen die zuletzt kopieren Elemente an. Durch einen Klick auf einen Eintrag fügen Sie diesen an die aktuelle Cursor-Position ein.

Auf Wunsch können Sie übrigens auch manuell festlegen, welche Einträge in der Zwischenablage synchronisiert werden sollen. Dazu schalten Sie **Meinen kopierten Text nie automatisch synchronisieren** ein. Sie können dann in der Zwischenablage auswählen,

welches Element synchronisiert wird.

Abschalten des virtuellen Arbeitsspeichers

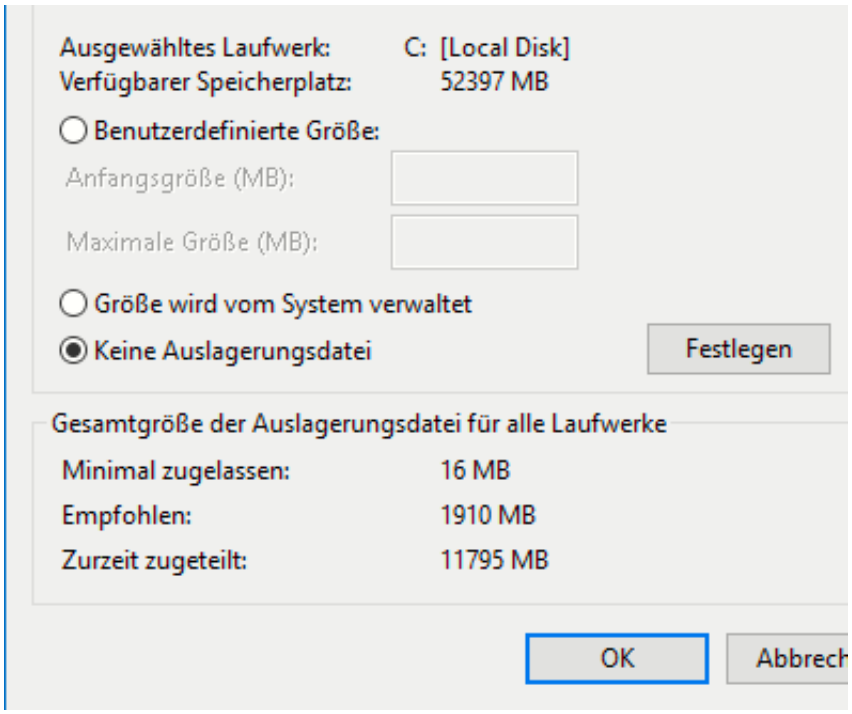
Im Gegensatz seinen Benutzern kann Windows 10 sein Gedächtnis nahezu unbegrenzt erweitern. Das Zauberwort heißt „virtueller Arbeitsspeicher“. Wird der interne – sehr schnelle – Arbeitsspeicher knapp, dann verwendet Windows 10 einfach die Festplatte zur Erweiterung. Das Problem: eine Festplatte ist im Gegensatz zu dem elektronischen Hauptspeicher oder einer SSD sehr langsam, und damit wird das System gebremst. Es kann also Sinn machen, diesen auszuschalten.

[caption id="attachment_762646" align="alignnone" width="500"]

stevepb / Pixabay[/caption]

Das Ausschalten des virtuellen Arbeitsspeichers ist relativ leicht:

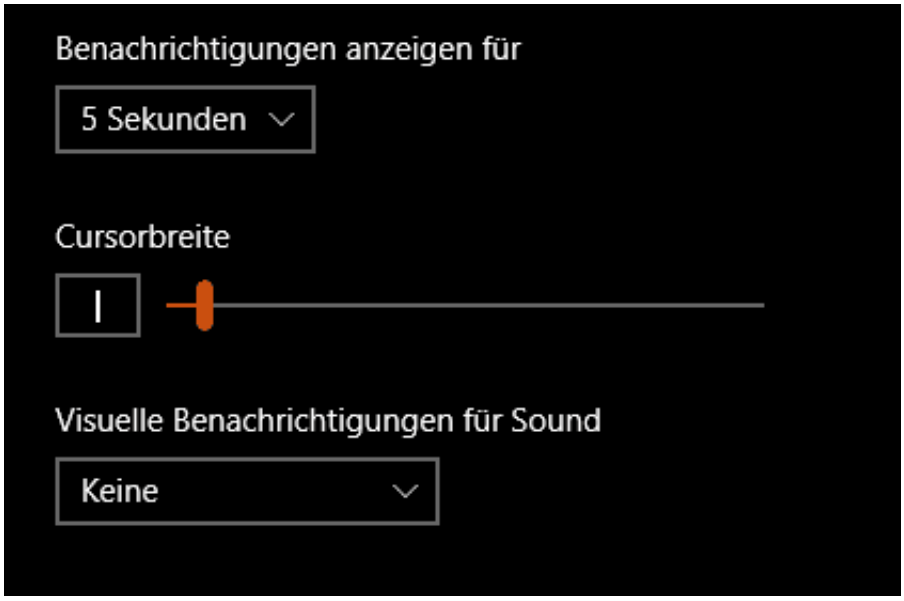
1. Geben Sie im Startmenü **Systeminfo** ein und klicken Sie dann auf **Erweiterte Systemeinstellungen**.
2. Unter dem Reiter **Erweitert** klicken Sie unter **Leistung** auf **Einstellungen**.
3. Bei **Erweitert** klicken Sie auf **Ändern**.
4. Entfernen Sie den Haken bei **Auslagerungsdateigröße für alle Laufwerke automatisch verwalten**.
5. Weiter unten wählen **Keine Auslagerungsdatei**.
6. Ein Klick auf **OK** wendet die Einstellungen an.



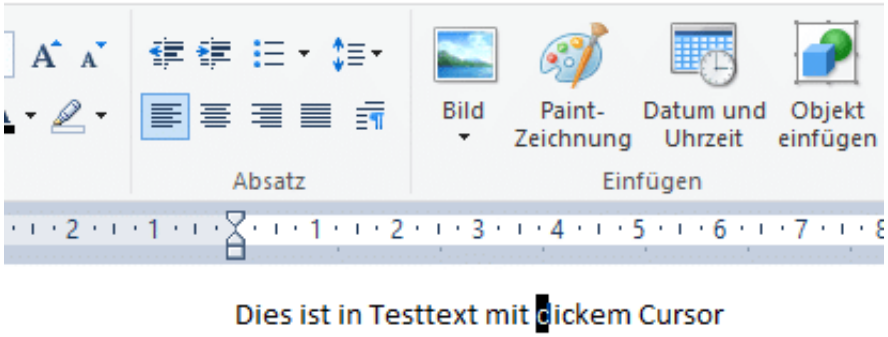
Hilfreich kann es alternativ sein, eine zusätzliche SSD einzubauen. Diese ist deutlich schneller als eine Festplatte. Wenn Sie die virtuellen Arbeitsspeicher auf die SSD auslagern, dann ist dies zwar immer noch langsamer als bei "echtem" Arbeitsspeicher, aber deutlich schneller als eine Festplatte.

Änderung der Cursorbreite unter Windows 10

Die Eingabe von Text ist eine der Standardaufgaben unter Windows 10. Wenn sie dann mit mehreren Eingabefenstern arbeiten oder mehrere Monitore einsetzen, dann wird das Suchen des Cursors manchmal zur Sisyphusarbeit. sowohl für den Text- als auch für den Mauszeiger. Windows 10 kann Ihnen dabei aber helfen!

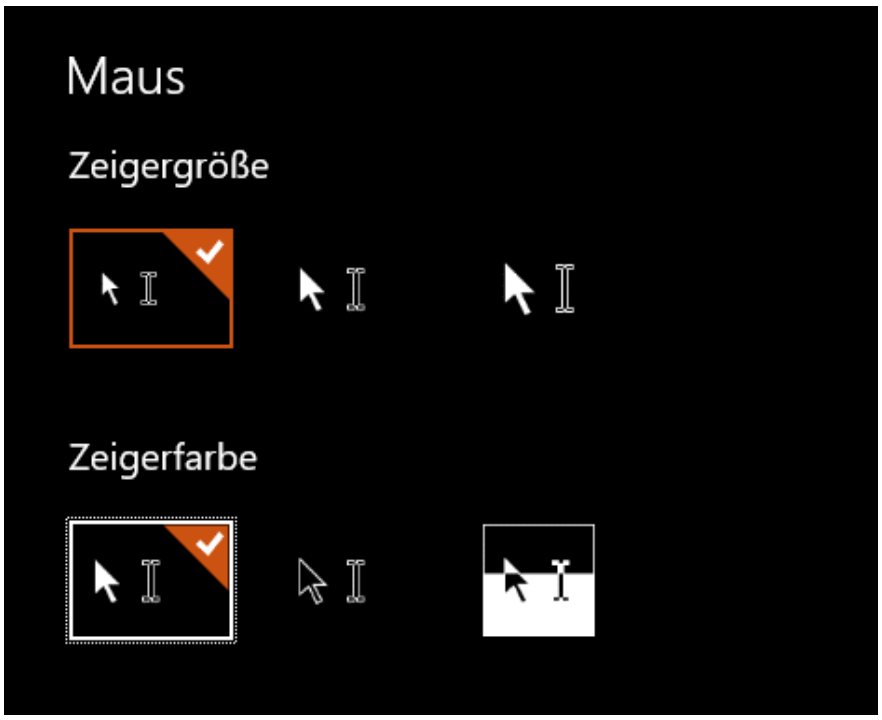


Unter **Einstellungen** > **Erleichterte Bedienung** > **Weitere Optionen** können Sie unter Cursorbreite die Breite des im Standard ein Pixel breiten Textcursors verbreitern. Lassen Sie sich nicht verunsichern: je breiter sie ihn wählen, desto eher erscheint er wie ein markiertes Zeichen.



Wenn Sie den Mauszeiger nicht sehen können, dann können Sie eine ähnliche Einstellung auch für diesen vornehmen: Unter **Einstellungen** > **Erleichterte Bedienung** > **Weitere**

Optionen > Maus können sie verschiedene hervorgehobene Darstellungen des Mauszeiger aktivieren.



diese Einstellungen haben keine weiteren Auswirkungen auf das System, Sie können also frei herumprobieren und die für Sie Beste wählen.