Schieb Report

Ausgabe 2018.52

Amazon Echo verrät vertrauliche Gespräche

Sie liegen dieses Jahr ziemlich häufig unterm Tannenbaum. Diese mehr oder weniger kleinen smarten Boxen, mit denen man sprechen kann. "Alexa, sag mir, was Du über mich weißt?" Darauf bekommt man keine Antwort. Aber der Mini-Lautsprecher von Amazon erfährt auf Dauer so einiges über die Familie, in der er wohnt. Jetzt hat es aber eine riesige Datenpanne gegeben. Amazon hat Gesprächsfetzen von Alexa-Nutzern an Fremde übergeben. Was ist da los? Ist Alexa indiskret?

Ein Kunde aus Deutschland hat von seinem Recht Gebrauch gemacht, das es seit der DSGVO gibt, und Amazon aufgefordert, ihm genau mitzuteilen, welche Daten das Unternehmen über ihn gespeichert hat. Kaum zwei Monate später ist ein umfangreiches Dossier eingetroffen, mit vielen Infos über Einkäufe und Produktsuchen.

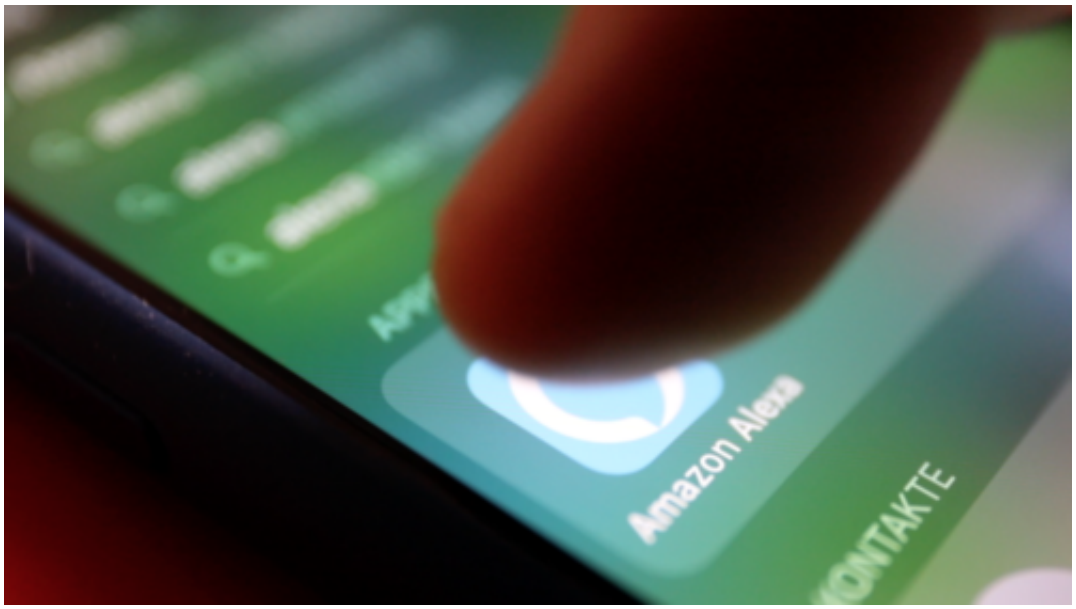
Aber auch über Alexa, was der Kunde also Alexa gefragt hat. Das Problem: Dieser Kunde hat gar kein Alexa. Das hat ihn natürlich besonders neugierig gemacht. 1700 Audiodaten wurden geliefert. Er hat reingehört – und Fremde gehört. Fremde, die mit Alexa gesprochen haben. Aber auch Gesprächsfetzen, die eindeutig zufällig mitgeschnitten wurden. Davon hat der Fachverlag Heise erfahren und das veröffentlicht.

Mitschnitte bei Alexa

Dass ein Fremder die Mitschnitte bekommen hat, war ein Versehen. Das ist der Anfrage geschuldet, da haben Mitarbeiter bei Amazon Mist gebaut. Aber dass die Gespräche aufgezeichnet werden, ist üblich – das wissen die meisten nur nicht. Es ist so: Wenn ich mit Echo/Alexa spreche, geht das an Server von Amazon und wirt dort analysiert.

Nicht im Gerät. Das ist bei allen Assistenten so, auch bei Siri, Cortana, Google etc. Amazon

speichert die Anweisungen oder Fragen aber dauerhaft! Man kann sie sich selbst auch anhören. Dazu muss man nur ins Profil gehen. Da sieht man genau: Wann habe ich mit welchem Gerät wo welche Fragen gestellt – und sich die Audios anhören.



Vertrauliche Gespräche aufgezeichnet

Aber offensichtlich sind nicht nur Anfragen wie "Wir wird das Wetter morgen" dabei, sondern auch vertrauliche Gespräche. Wie kommt das?
Es ist ja so: Normalerweise aktiviert man Alexa, indem man "Alexa" sagt. Auch das ist bei allen anderen Assistenten genauso.

Was danach kommt, ist relevant – und wird an die Server zur Analyse geschickt. Nun kann es aber passieren, dass sich Alexa verhört. Wenn in einem Gespräch von einer "Alex" die Rede ist, geht das Mikrofon auf. Im Radio nuschelt einer "alles", und das Mikrofon geht auf.

Die Maschine glaubt also, das Schlüsselwort sei gefallen – und beginnt mit der Aufzeichnung, überträgt alles auf die Server, das wird dort gespeichert. Das passiert häufiger als man glaubt. Davon kann sich jeder selbst überzeugen, indem er/sie mal in sein Amazon-Profil schaut oder besser: rein hört.

Wann hören die Geräte mit?

Nun, das Mikro selbst hört die ganze Zeit zu, wenn nicht gerade manuell auf Stumm geschaltet. Denn es könnte ja jederzeit sein, dass ich "Alexa" oder "Google" oder "Siri" oder "Cortana" sage. Zu den Servern geschickt wird das Gesagte aber normalerweise aber nur, wenn das Schlüsselwort vorher fällt. Aber kann man sich darauf verlassen? Theoretisch lassen sich die Geräte hacken und manipulieren, dann lässt jederzeit alles mitschneiden.

Im schlimmsten Falle schon, wenn sie manipuliert werden oder einen Defekt aufweisen. Das gilt übrigens sogar für sprachgesteuerte Fernseher. Deshalb verzichten viele bewusst darauf, sich solche Technologie ins Haus zu holen. Im aktuellen Fall war das aber nicht das Problem. Hier haben wir das Problem, das aufgezeichnete Daten in **fremde Hände geraten**.

https://vimeo.com/307502420

Wie häufig passiert das?

Das soll nicht passieren. Ist aber passiert. Wer will sicherstellen, dass die eigenen Aufzeichnungen nicht von Amazon-Mitarbeitern mitgehört oder weitergegeben werden? Dass ein Datenleck entsteht, und jeder kann reinhören?

Der Fall zeigt: Sowas kann passieren. Und das sollte jeder wissen. Die Kollegen von Heise haben mit Hilfe der Daten, also was wurde gesagt, welche Namen sind gefallen, nach welchen Wetterinfos wurde gefragt etc., sogar die betroffene Familie ermitteln können. Sie haben sie informiert. Das zeigt, dass es möglich ist, im Fall eines solchen Datenlecks Rückschlüsse zu ziehen.

Dateien futsch: So könnt Ihr die Daten retten

Es kommt in den besten Familien vor: SD-Karte versehentlich formatiert, Ordner in den Papierkorb gezogen und gelöscht oder ein Programm hat Unsinn angestellt. Weg sind die wichtigen Fotos, Videos oder Dokumente. Was tun? Wichtig sind: Ruhe bewahren und mit den passenden Tools vorgehen.

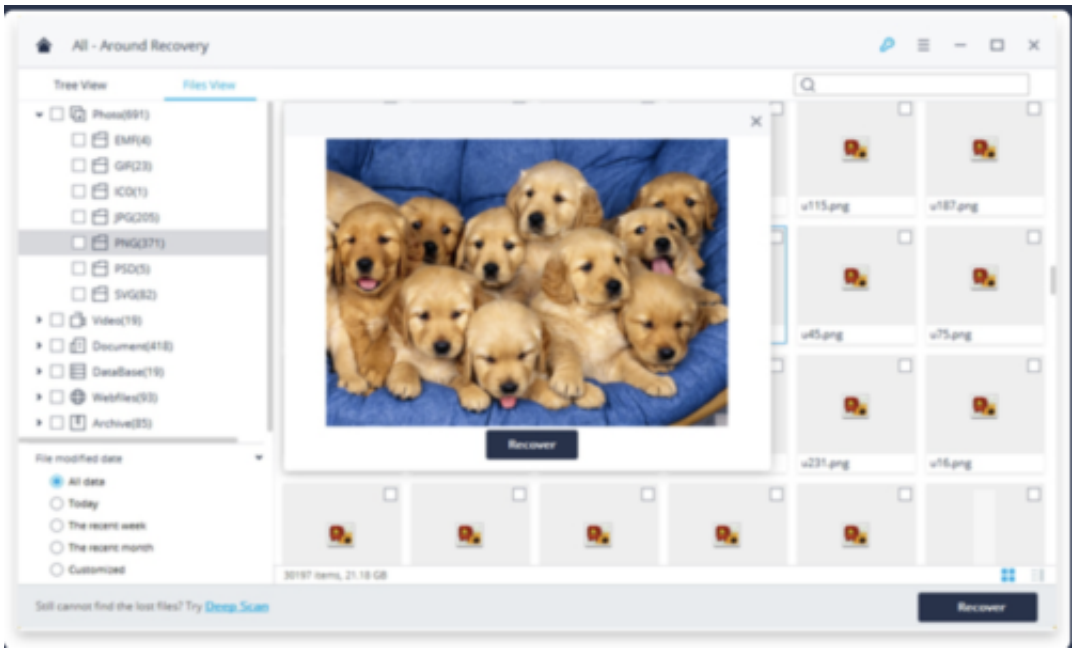
Ich bekomme regelmäßig Mails von Leserinnen und Lesern, die versehentlich irgend etwas gelöscht haben - oder wo die Technik verrückt spielt und deshalb stehen bestimmte Daten nicht zur Verfügung.

Ich fühle mich da oft immun, da ich wichtige Dateien und Dokumente in der Cloud sichere. Wenn Ihr das auch macht: Checkt, ob der Cloud-Dienst nicht eine Backup-Funktion anbietet für versehentlich gelöschte Dateien. Bei Dropbox ist so etwas möglich.

Daten retten, wenn sie verschwinden

Aber jetzt hat es mich auch erwischt: Wichtige Fotos und Videos auf einer SD-Karten waren plötzlich verschwunden. Als wären sie nie aufgenommen worden. Ich habe da mehrere Recovery-Apps probiert. Geholfen hat mit Recoverit von Wondershare. Hier gibt es Spezialprogramme für Windowsd und Mac, um gelöschte Dateien aufzuspüren und den Rettungsversuch zu starten.

Wichtig: Falls Euch das mal passiert, dass Dateien plötzlich weg sind, am besten sofort handeln und wenn möglich, auf dem betreffenden Datenträger keine weitere Daten speichern. Erst mal die Rettungsaktion starten. Das erhöht die Chance, dass Ihr an die Daten kommt.



Recoverit kommt mit den meisten Datenformaten klar

Recoverit müsst Ihr laden und installieren. Danach geht es auch schon los, und Ihr könnte auswählen, welches Laufwerk/welcher Datenträger gescannt werden soll. Die Software ist clecer programmiert: Sie durchforstet selbst komplexe Datenstrukturen, sogar nach einer Neuformatierung oder Partionierung, und versucht, die Daten zu retten.

Dabei werden sogar die Eigenheiten verschiedener Dateiformate berücksichtigte. All das geht sogar vergleichsweise schnell, bedenkt man, welche ungeheuren Speicherkapazitäten moderne Datenträger haben.

Ich konnte meine plötzlich verschwundenen Fotos und Videos jedenfalls mühelos wieder rekonstruieren - und bin dafür sehr dankbar.

Recoverit kann man kostenlos testen. Aber wenn es zur Sache geht und man Dateien retten will, dann muss man dafür bezahlen. Etwa 80 EUR. Sofern es sich nicht um irgendwelche unwichtigsten Daten handelt, sondern Daten, die relevant sind, ist das zweifellos gut investiertes Geld.

Deep Fakes: Erstellen, erkennen und abwehren

Alle reden gerade über die gefälschten, erfundenen und manipulierten Geschichten, die im SPIEGEL erschienen sind. Dass sich Texte verfremden lassen, das kann sich jeder vorstellen. Aber Fotos, Audios und Videos? Doch, das geht auch. Sogar vergleichsweise einfach - und sehr effektiv. Wir brauchen geeignete Mittel, um uns gegen so etwas zu wehren.

Jeder kann mit einer App wie Mug Life Fotos bearbeiten. Mit wenigen Handgriffen und ein paar Mal Tippen lassen sich realistisch wirkende Bewegungen ins Gesicht zaubern, etwa das Hochziehen einer Augenbraue. Das Ergebnis: eine Bildmanipulation.

Nur wenige EUR teure Apps erlauben so etwas. Ein Lächeln hinzaubern, wo eigentlich gar kein Lächeln ist. Auch das geht. Mit dieser App hier kann man praktisch jeden Gesichtsmuskel beeinflussen – in jedem Foto!

Manipulationen für wenige EUR

Beeindruckend, oder? Aber auch ein bisschen spooky, finde ich.

Es gibt Dutzende solcher Apps, mit denen selbst Laien Fotos geschickt manipulieren – und aus Fotos bewegte Bilder machen können. Auf diese Weise entstehen Videos, die Dinge zeigen, die so nicht passiert sind.

So lange solche kleineren Manipulationen im Privatbereich oder schlichtweg als Gag zum Einsatz kommen, ist alles OK. Problematisch wird es, wenn woanders manipuliert wird. Wenn wir nicht mehr erkennen können, ob wir zum Beispiel einen echten Präsidenten sehen – oder einen manipulierten Clip. Hier ein Beispiel.

https://www.youtube.com/watch?v=cQ54GDm1eL0

Dem Präsidenten alles in den Wort legen

Wie bitte? Barack Obama sagt hier offiziell im Fernsehen: "President Trump is a total and complete dipshit". Also: Präsident Trump ist ein Vollidiot. Das ist eigentlich nicht die Art von Obama, sieht doch aber täuschend echt aus, oder etwa nicht?

Doch das ist ein Fake. Ein so genannter Deep-Fake. Weil Inhalt, Bild und Ton gefälscht sind – und wir können es praktisch nicht erkennen. Denn wenn simple Apps fürs Smartphone schon beeindruckende Effekte hinbekommen, dann ist im Labor natürlich noch mehr möglich.

Entstanden ist das Obama-Video an der University of Washington. Grundlage ist ein Original-Video. Eine Ansprache von Obama. Danach hat sich Künstliche Intelligenz, KI, das Material angeschaut. Alles analysiert. Jedes Wort. Jede Gesichtsbewegung. Die Mimik. Es reichen einige Minuten Videomaterial. Danach kann die KI-Software den Menschen alles sagen lassen.

Ein Schauspieler spricht den Text. Das Video ist fertig. Oder aber, man legt einen komplett anderen Text unter das Video. Die KI-Software erzeugt dann das passende Video. Mit den typischen Bewegungen. Der üblichen Mimik. Das alles ist noch nicht unbedingt perfekt. Aber doch täuschend echt. Ausreichend, um im Netz oder auch im Fernsehen Millionen Menschen zu überzeugen.

Oder zu erschrecken. Zu manipulieren.

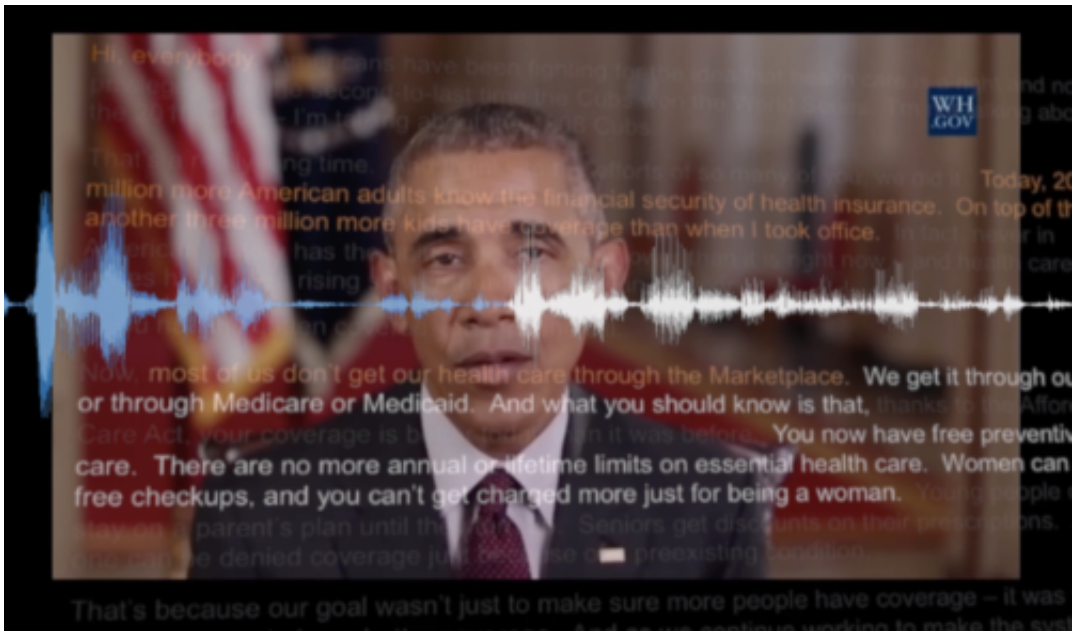
Künstliche Videos erzeugen und mit fremden Stimmen sprechen

Man kann also künstlich Videos erzeugen, die täuschend echt aussehen. Das will uns das University of Washington sagen. Sie will das nicht nutzen. Sie will uns warnen. Denn wenn die Uni das kann, dann können das Geheimdienste auch. Mühelos.

Was man wissen muss: Auch Stimmen lassen sich heute perfekt animieren.

Es gibt KI-Systeme, die lernen mit der Stimme einer jeden Person zu sprechen. Die KI-Software untersucht vorhandene Sprechtexte, 20 Minuten reichen. Schon spricht man jeden Text mit der Stimme jeder Person. Die perfekte Täuschung ist fertig.

Wir dürfen sicher sein, dass amerikanische, russische oder chinesische Geheimdienste so etwas können.



Quellen prüfen

Was bedeutet das? Das bedeutet, es wird immer wichtiger, die Quellen zu prüfen. Wir hier im Fernsehen machen das. Was im Internet kursiert, kann von überall kommen – und eben nicht nur Fake-News, sondern auch Deep-Fake sein.

Es wird immer schwieriger, wahr von falsch zu unterscheiden. Echt von unecht. Es wird bereits an Methoden entwickelt, die Fotoaufnahmen und Videos „versiegeln“. Methoden wie TruePic oder Serelay. Fotos und Videos bekommen eine Art Siegel, wenn sie gemacht werden. Jede Art von Veränderung oder Manipulation lässt sich so erkennen.

Fotos und Videos versiegeln

Funktioniert aber nur, wenn Fotos und Videos von Anfang an entsprechend behandelt und versiegelt werden. Eine offizielle Ansprache des Präsidenten oder der Bundeskanzlerin zum Beispiel könnte man so unterscheiden von einem Fake. Immerhin.

Es gibt also viele gute Gründe, skeptisch zu sein, wenn wir im Netz etwas sehen oder hören.

Facebook 2018: Ein Jahr mit vielen Sünden

Wie waren wir dieses Jahr? Diese Frage stellen sich viele Unternehmen am Ende eines Jahres. Aus gutem Grund, denn irgendwann muss man doch mal Bilanz ziehen. Wir wissen nicht, ob auch bei Facebook ein kritischer Blick zurück erfolgt. Aber eins steht fest: Das Jahr 2018 war für Facebook ein Jahr voller Sünden, Skandale und Katastrophen. Gut möglich, dass es genauso weitergeht - denn Mark Zuckerberg scheint nicht sonderlich lernbereit.

Kennt Ihr diese kleinen Botschaften, die in der Facebook-Timeline regelmäßig aufpoppen: Irgend etwas, das vor zwei, drei oder sechs Jahren passiert ist? Oder die niedliche Zusammenfassung des zurückliegenden Jahres in Bildern und Videos?

Wenn die Algorithmen gut funktionieren, müsste Mark Zuckerberg eine niederschmetternde Zusammenfassung für 2018 erhalten. Eine Aneinanderreihung von Hiobsbotschaften. Denn 2018 war für Facebook ein katastrophales Jahr.

Dutzende von Skandalen und Skandälchen

Was ist 2018 nicht alles ans Tageslicht gekommen. Der Cambridge-Analytica-Skandal mit seinen 87 Millionen potenziellen Opfern ist den meisten sicher noch am besten in Erinnerung geblieben. Der Vorfall hat hohe Wellen geschlagen. Nicht nur, weil Facebook Daten weitergegeben (=veruntreut) hat, sondern auch und besonders, weil diese Daten - möglicherweise - bei der US-Wahl missbraucht wurden.

Apropos Wahlen: Russische Quellen haben auf Facebook im großen Stil manipulative Anzeigen

geschaltet. Zur gezielten Desinformation. Und Facebook hat das nicht nur nicht verhindert, sondern sogar prächtig daran verdient.

Ein Vorgang, der selbst in den USA für Empörung gesorgt hat. Es gibt noch viele andere Verfehlungen: Die Weitergabe der Nutzerdaten an 150 große Onlinedienste, eine Datenpanne bei User-Fotos, die mehrfache Verletzung der Datenschutzbestimmungen durch WhatsApp, diverse Datenlecks. Und, und, und ...

https://vimeo.com/261094792

Mark Zuckerberg: Jedes Vertrauen verspielt

Niemand kauft Mark Zuckerberg noch ab, wenn er Mea-Culpa-ausrufend durch die Lande zieht und wie ein kleiner Junge den Kopf senkt. Von wegen: Fehler! Sorry! Kommt nicht mehr vor... Alles gelogen. Es handelt sich nicht um Pannen, jedenfalls eher selten.

Es ist das Prinzip Facebook: Daten sammeln, bis es nicht mehr geht - und Geld rausquetschen, so viel wie möglich. Ohne jede Moral. Ohne jeden Anstand. Kontrolliert wird nur beim Thema "Nacktheit": Da werden dann auch gerne schon mal Kunstwerke aus dem Angebot entfernt. Nackte Brust auf einem Bild? Das geht ja gar nicht ...

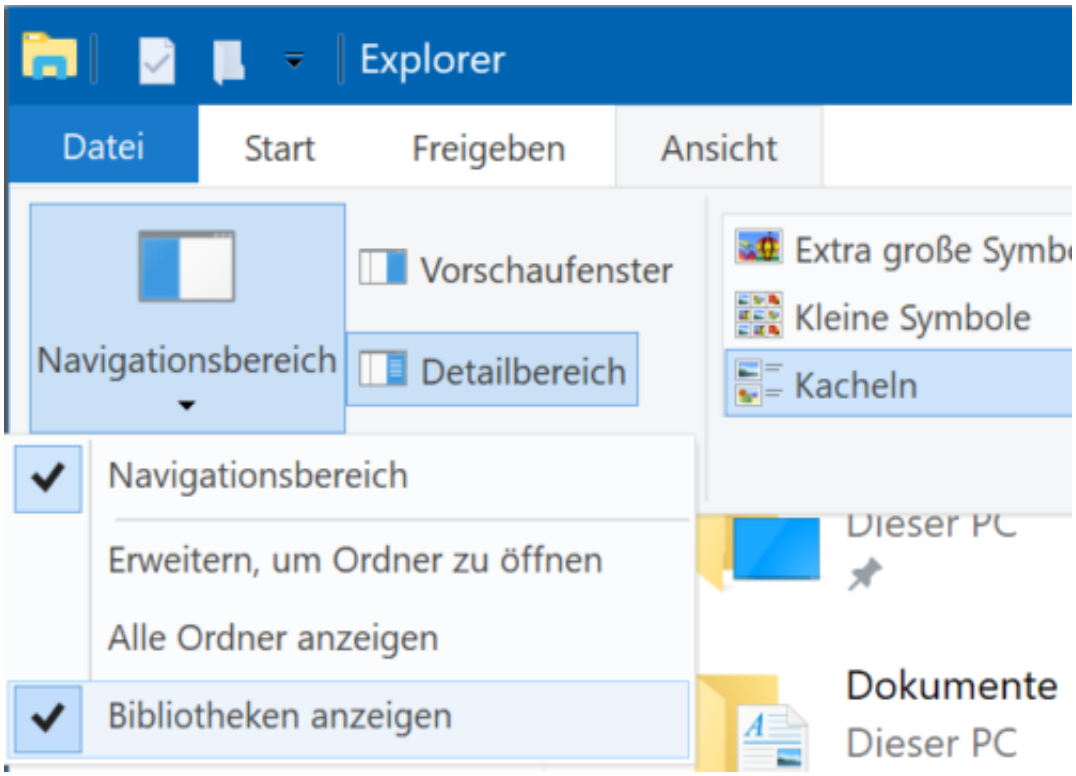
Die Sündenliste ist lang. Doch niemand weist Mark Zuckerberg ernsthaft in die Schranken. Weder sitzt er im Gefängnis, wo er meiner Ansicht nach hingehört (nicht dass wir uns missverstehen: Er sollte sich die Zelle mit vielen anderen Managern teilen), noch wird sein Vermögen beschlagnahmt, noch ändert sich irgend etwas Wesentliches.

Zuckerberg darf weitermachen wie bisher - und weil ihn niemand stoppt, wird er auch so weitermachen. Nur der Aktienkurs ist etwas eingebrochen. Was soll's.

Keine guten Aussichten für 2019.

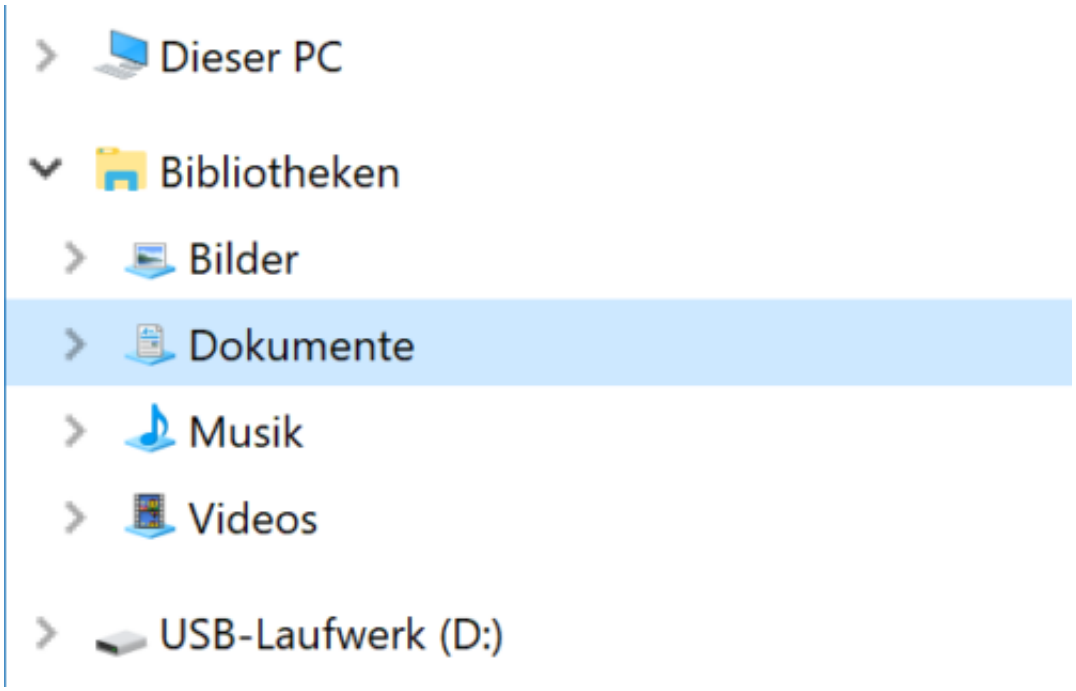
Anzeigen der Bibliotheken in Windows 10

Windows bietet die so genannten „Bibliotheken“ an, die nach verschiedenen Datei- und Medientypen (Dokumente, Bilder, Musik, Videos) getrennt als zentraler Speicherort angelegt sind und von den meisten Windows-Programmen automatisch verwendet werden. Diese dienen dazu, möglichst einfach verschiedene Dateitypen sortiert aufzubewahren:Dokumente in der einen, Musik in der anderen, Videos und Bilder wieder ein eigenen. Im Standard sind diese allerdings im Explorer ausgeblendet, was sich leicht korrigeren lässt.



In drei Schritten zu den Bibliotheken

1. Starten Sie auf Ihrem Windows 10-PC den Windows Explorer, indem Sie gleichzeitig die **Windows-Taste und E** drücken.
2. Wählen Sie **Ansicht, Navigationsbereich, BiBliotheken anzeigen,** um die Bibliotheken in der Ordneransicht des Explorers angezeigt zu bekommen.
3. Sie finden die Biliotheken dann als separaten Eintrag in der linken Spalte des Explorers


Dieser PC
Bibliotheken
Bilder
Dokumente
Musik
Videos
USB-Laufwerk (D:)

Recovery Keys für Bitlocker finden

"Eigentlich" sollte der Ottonormalanwender gar nicht damit konfrontiert werden, aber "eigentlich" ist bekanntermassen der beste Freund von "fast", und so kommt es unter anderem manchmal bei der Installation eines BIOS-Updates zu folgender Situation: Windows erkennt eine Veränderung der Hardware eines Notebooks oder Tablets und fordert den Anwender auf, den Recovery Key für die Festplattenverschlüsselung Bitlocker einzugeben.

Erst nach erfolgreicher Eingabe wird die Festüplatte freigegeben und Windows kann starten. Nun macht sich der Normalanwender meist wenig Gedanken über siene Festplattenverschlüsselung, im schlimmsten Fall ist er sich derer nicht einmal bewusst. In der Folge existieren auch keine Sicherheitskopien der Schlüssel auf einem USB-Stick, die hier zu verwenden wären.

Bitlocker Schlüssel auf dem OneDrive

Microsoft hat dieses Problem in der Vergangenheit bereits erkannt und speichert die Schlüssel automatisch auf dem OneDrive, dass zum Microsoft-Konto auf dem Gerät gehört. Es bleibt dem geschockten Anwender nicht viel mehr übrig, als sich einen anderen PC oder Tablet zu suchen und dort https://onedrive.live.com/recoverykey aufzurufen.

WICHTIG: Die URL, die Windows selber anzeigt, ist manchmal nicht mehr gültig und führt auf das Hauptverzeichnis des OneDrives, zeigt aber nicht die Schlüssel an!

Der Bitlocker-Dialog zeigt auf dem betroffenen Gerät dessen Kennung an, die sich in der Liste auf dem OneDrive findet. Diese muss eingegeben werden und damit die Festplatte wieder freigeschaltet.

Neue E-Mails in Outlook auf China-Smartphones stabil per Push benachrichtigen lassen

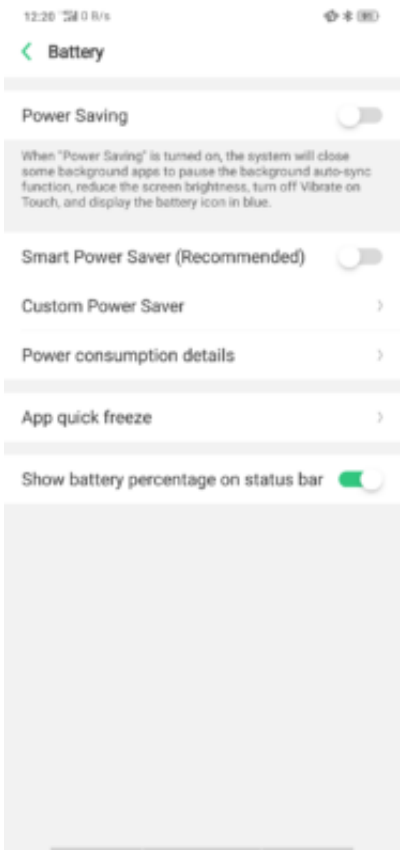
Mittlerweile ist die Beschaffung von nicht direkt in Deutschland vertriebenen Smartphones verschiedener Hersteller aus China ein Kinderspiel. Verschiedene Internet-Shops beschaffen diese und schicken sie kostengünstig nach Deutschland, sogar mit passendem Strom-Adapter. Was aber bei den China-Geräten immer eine Herausforderung ist: Die Geräte haben einen solch aggressiven Stromsparmodus, dass Push-Nachrichten wie auch Benachrichtigungen auf Wearables Glückssache sind: Anfangs funktionieren sie, und nach kurzer Zeit im Standby-Modus sind die Apps eingefroren, beendet oder reagieren nicht mehr... und schon werden keine neuen Nachrichten mehr abgerufen und eben auch nicht benachrichtigt. Die Lösung versteckt sich in den Einstellungen von Android.

Für das Nubia Z17 (und andere Geräte des Herstellers) findet sich hier ein Lösungsansatz. Bei OPPO (und anderen) Herstellern ist die Lösung leider nicht so einfach, weil keine eigene App dafür existiert, sondern die Einstellungen im System vorgenommen werden müssen.

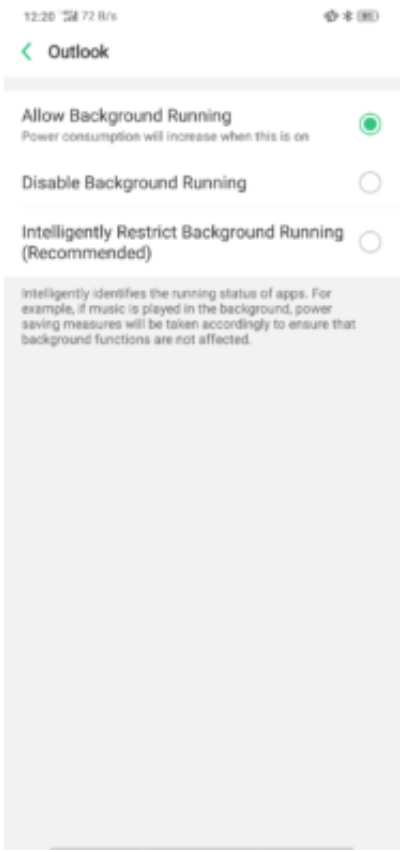
Die Beschreibungen beziehen sich auf die englische ROM-Version. Wenn die entsprechenden Einstellungen nicht einer etwaigen internationalen Version auffindbar sind, dann macht es Sinn, das Gerät kurzzeitig auf Englisch umzustellen.

Einstellungen für den Stromsparmodus

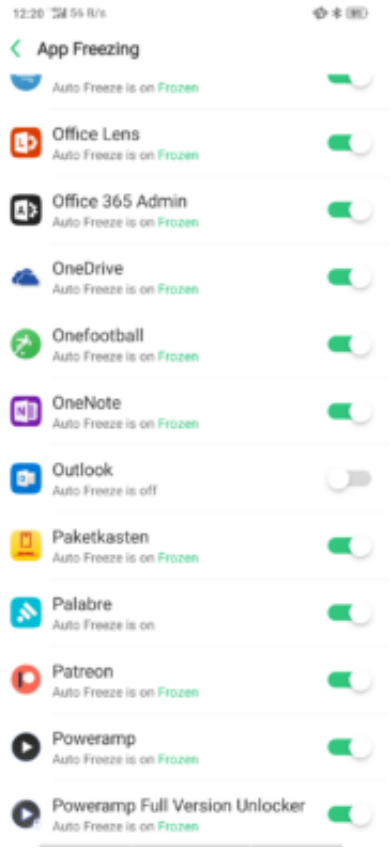
Die generellen Stromspareinstellungen finden sich unter **Settings**, **Battery**. Hier ist wichtig, dass erst einmal der generelle Stromsparmodus (**Power Saving**) ausgeschaltet ist.



Hier finden sich noch zwei weitere wichtigeEinstellungen: Unter **Customs Power Saver** wird für die einzelnen Apps festgelegt, ob diese im Hintergrund laufen dürfen, intelligent gesteuert werden (und damit bei "Nichtaktivität" gestoppt werden) oder gar nicht im Hintergrund laufen können. Für alle Apps, die Push-Nachrichten schicken sollen, muss hier angewählt werden, dass sie immer im Hntegrund laufen dürfen. Das "intelligente" Verfahren führt dazu, dass die Apps schnell abgeschossen werden, um Energie zu sparen.

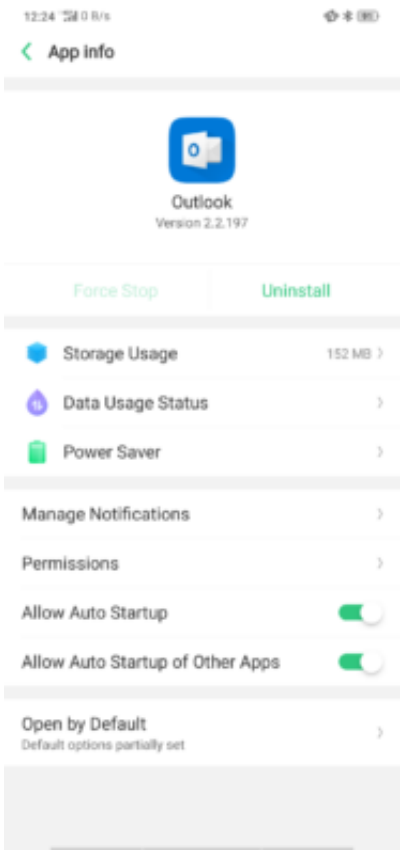


Unter **App Quick Freeze** muss für jede dieser Apps die Möglichkeit, sie einzufrieren (ein weiterer Schritt des Stromsparens), deaktiviert werden:



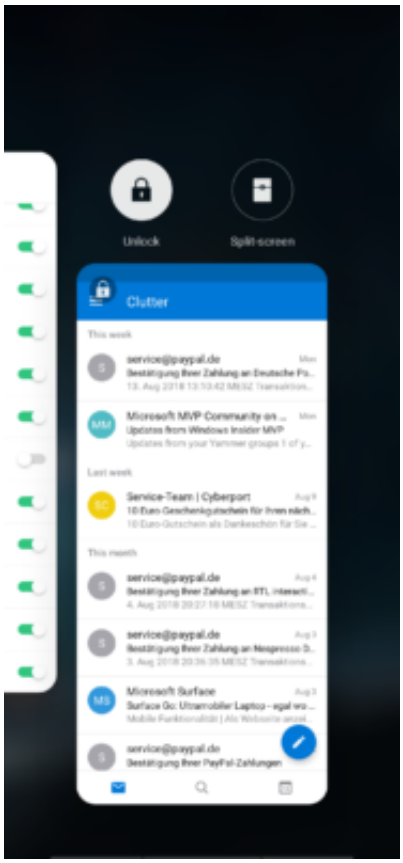
App Management/Auto StartUp

Kein echtes Stromsparthema, aber damit mim Zusammenhang: Im Standard wird Push nur dann aktiv, wenn die App auch läuft. Gerade bei Outlook (sicherlich aber auch bei anderen) muss die App im Hintergrund automatisch starten, und das muss in den Systemeinstellungen von Android explizit freigegeben werden: Unter **Settings**, **App Management** muss separat für jede App **Allow Auto Startup** aktiviert werden. Dort finden sich auch die Benachrichtigungsoptionen (unter **Notification Settings**), die für die stabile Verwendung einer Smartwatch wichtig sind und aktiviert werden müssen.



Verriegeln von Apps

Ein weiterer Schritt, um Apps vor der automatischen Beendigung zu schützen, ist die Möglichkeit, sie in der Übersicht (**Recents**) zu "verriegeln". Dazu muss in die Übersicht der laufenden Apps von Android gewechselt werden (per Hard- oder Software-Taste, beim OPPO duerch die Geste "mit dem Finger vom Rand nach oben über das Display streichen und das Display kurz gedrückt halten"). Dann das Fenster der entsprechenden App nach unten ziehen und **Lock** auswählen. Die App bekommt dann ein kleines Schloss im Symbol oben links. Beim Oppo find X allerdings lassen sich nur 5 Apps so "schützen".

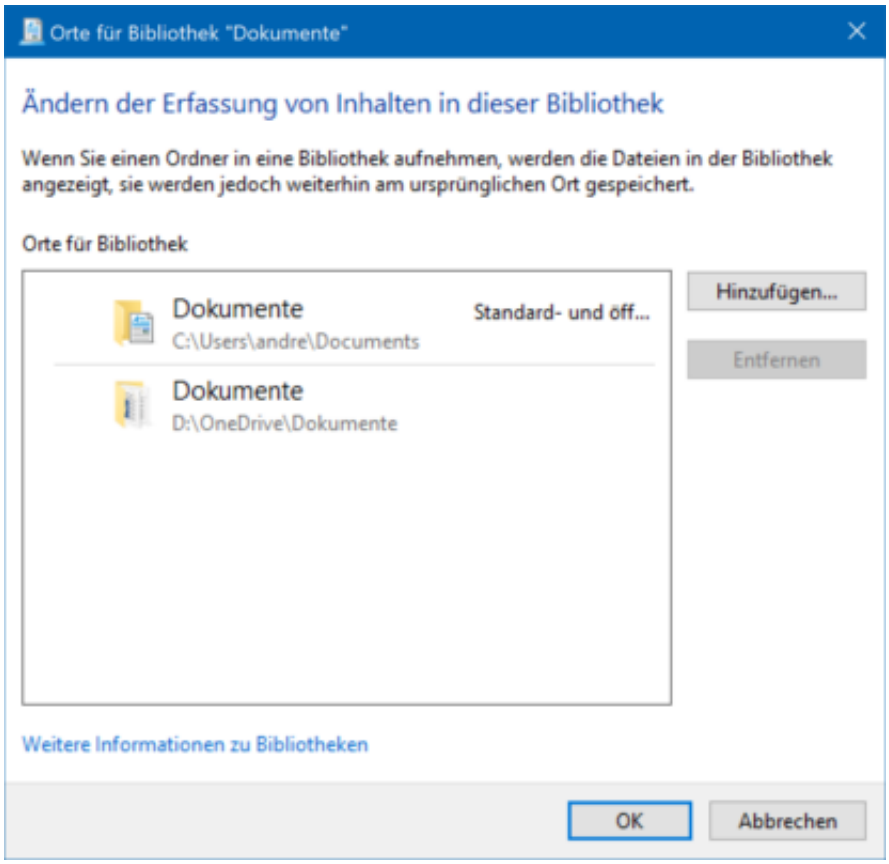


Tipp für Smartwatch-Benutzer

Damit die Smartwatch durchgängig verbunden bleibt, sollte die entsprechende App (Garmin connect, Samsung Gear, Android Wear, ...) ebenso mit den oben beschriebenen Schritten davor geschützt werden, beendet zu werden. Sonst funktionieren die Benachrichtigungen auch nur kurzfristig.

Anpassen der Bibliotheken-Ordner unter Windows

Wie fast alles unter Windows 10 sind auch die Bibliotheken frei anpassbar. Musik kann sich auf der Festplatte wie auch auf einer Speicherkarte befinden, Dokumente in einem lokalen Verzeichnis und zusätzlich im Onedrive, und so ist es kein Problem, Ordner auf unterschiedlichen Laufwerken den Bibliotheken hinzuzufügen. Windows-Bibliotheken können also verschiedene Speicherorte haben. Windows genau das mitzuteilen, ist denkbar einfach!



1. Im Windows Explorer klicken Sie auf die Bibliothek, der Sie einen weiteren Speicherort hinzufügen wollen, Dann erscheint in der Menüleiste ein neuer Eintrag **Verwalten.**
2. Wählen Sie nun in der Symbolleiste **Bibliothek verwalten,** dann sehen Sie die Verzeichnisse, die aktuell in der Bibliothek zusammengefasst sind.
3. Klicken Sie dann auf **Hinzufügen,** um einen weiteren Ordner zu der Bibliothek hinzuzufügen. Es ist egal, ob dieser sich auf der lokalen Festplatte oder einer Speicherkarte befindet.
4. Klicken Sie auf **Entfernen,** um einen Speicherort zu entfernen.
5. Wenn Sie einen der Speicherorte mit der rechten Maustaste anklicken, dann können Sie festlegen, ob dieser der **Standardspeicherort,** also der, in dem die Dateien standardmäßg gespeichert werden sollen, sein soll.

SD-Karten als Bibkliotheks-Speicherorte

Sie können auch eine SD-Karte als Bibliotheks-Speicherort festlegen. Das macht vor allem bei

mobilen Geräten wie Notebooks und Tablets Sinn, wo zum einen der Speicherplatz knapp ist, zum anderen ein Wechseldatenträger ein zweites Laufwerk bietet, das unabhängig von der internen Festplatte ist.

Power Throttling beim Surface GO und anderen Geräten unterbinden

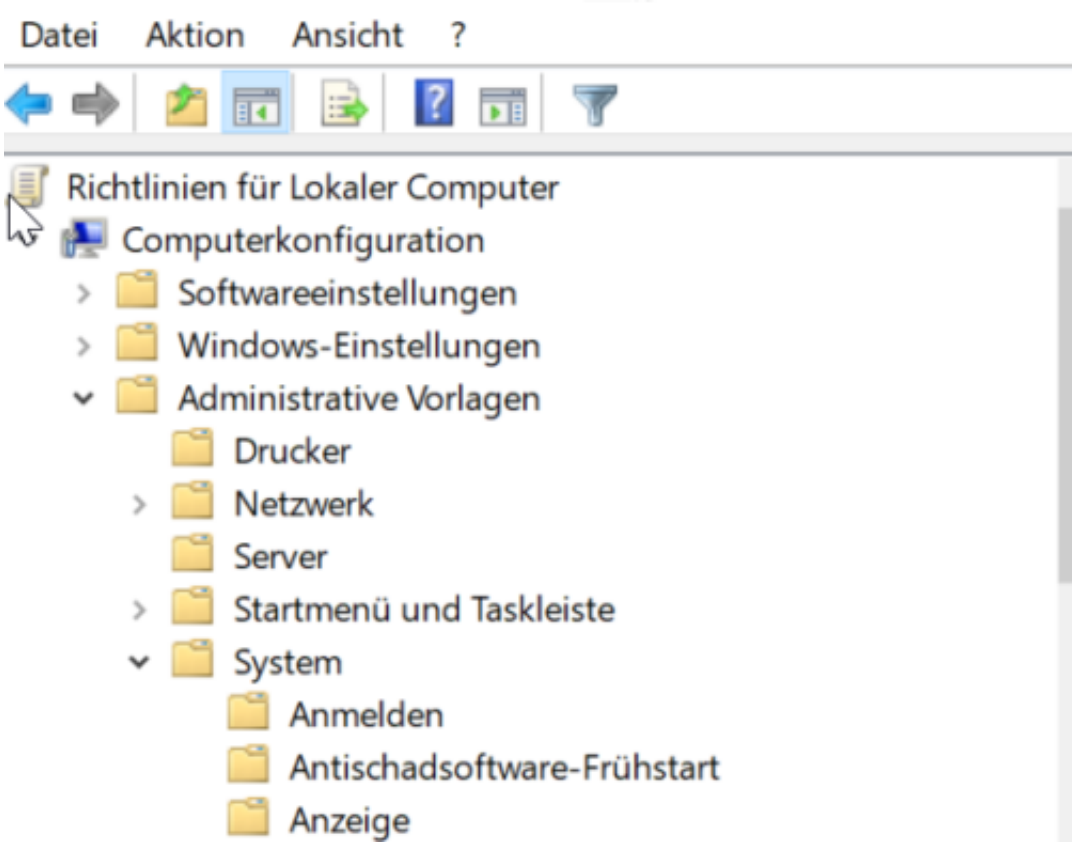
Power Throttling ist für den einen Anwender Segen, für die anderen Fluch: Die Idee dabei ist, dass Dienste/Programme ausgebremst werden, wenn sie nicht benötigt werden, und so durch geringere Prozessorlast Energie gespart und die Laufzeit eines Notebooks/Tablets verlängert werden. Wie Automatismen es so an sich haben: sie funktionieren mal besser, mal schlechter, und besonders beim Surface GO führen sie immer wieder dazu, dass das Gerät Apps/Programme spürbar verzögert startet bzw. verlangsamt. Beim eh schon nicht überbordend leistungsfähigen Pentium Gold keine schöne Situation.

Die Lösung (oder zumindest ein Teil davon) ist relativ einfach: per Group Policy kann das Throttling komplett ausgeschaltet werden. Einen Überblick über den Status des Power Throttlings bekommt man, indem man den Tsatk Manager startet, auf den Reiter "Details" klickt, dann mit der rechten Taste in die Spaltenüberschriften und dann auf "Spalten auswählen" klickt. Durch Einblenden der Spalte "Leistungseinschränkung" wird für jeden Prozess angezeigt, ob Power Trottling für ihn aktiviert oder deaktiviert ist.

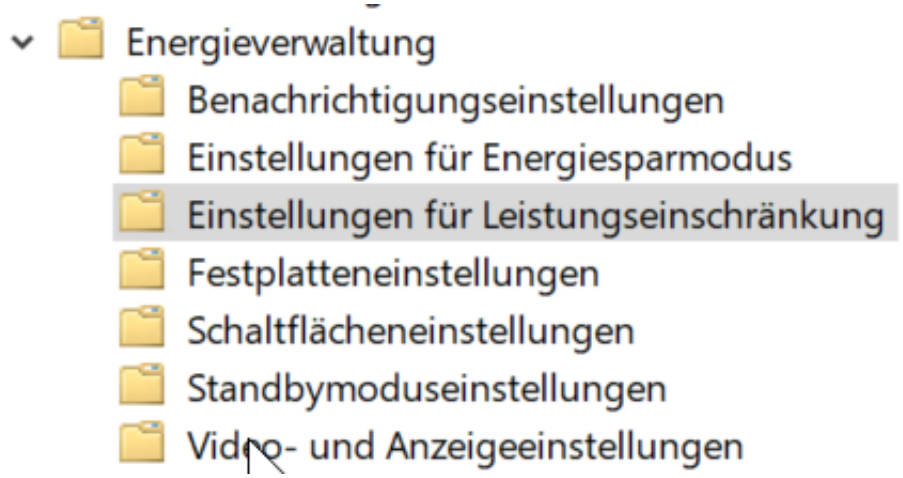
Änderung per Gruppenrichtlinie

Zum Ausschalten der Funktion muss die Verwaltung für Gruppenrichtlinien gestartet werden: Erst muss die Windows-Taste gleichzeitg mit "R" gedrückt werden, dann **gpedit.msc** eingegeben werden.

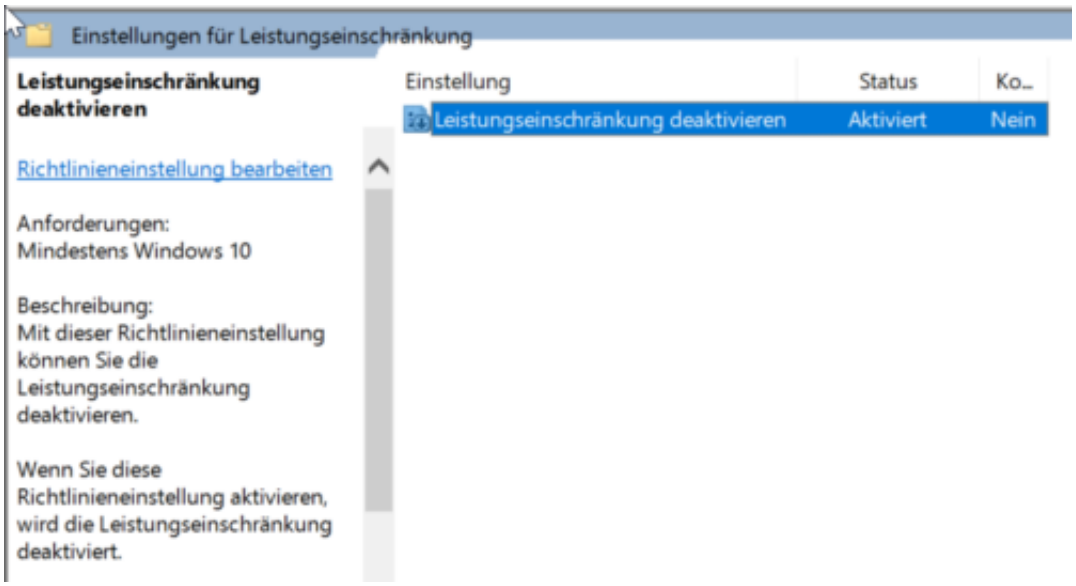
Im Verzeichnisbaum dann unter "Computerkonfiguration" und "System":



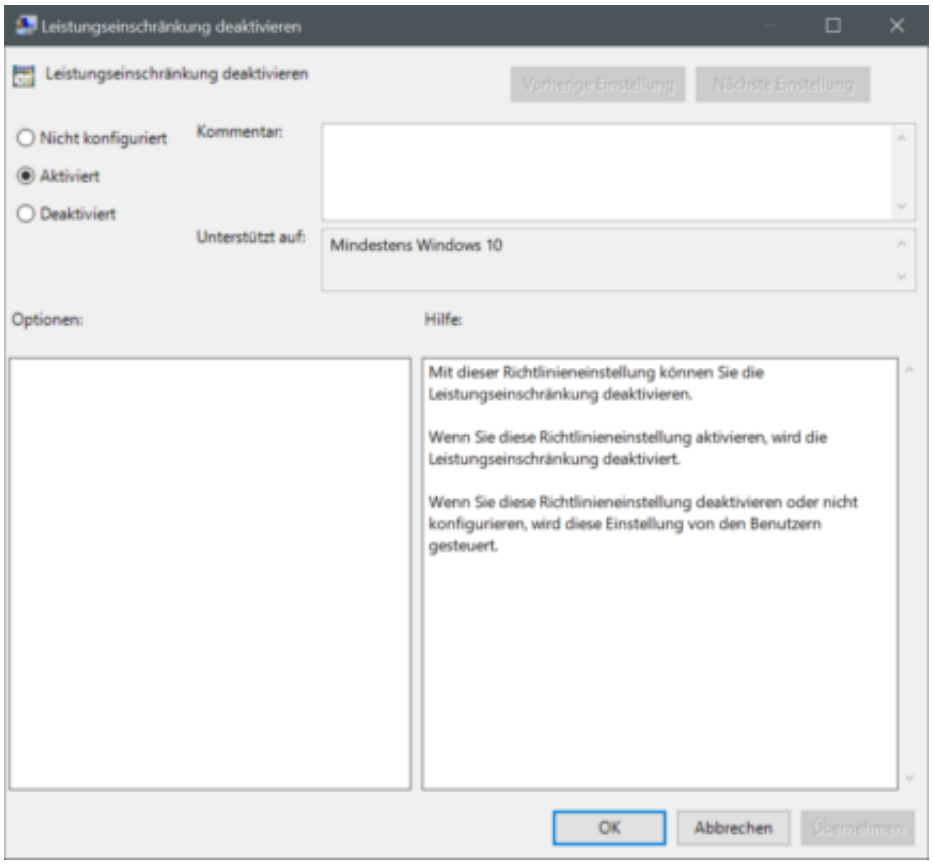
Dann unter "Energieverwaltung" und "Einstellungen für Leistungseinschränkung":



Wie im Registry Editor findet sich darin ein Key, den man Doppelklicken kann:



Im sich nun öffnenden Fenster muss "Deaktiviert" angeklickt werden und die Änderung durch einen Klick auf OK bestätigt werden.



Nach einem Neustart des Rechners wird die Änderung dann angewendet. Der Energieverbrauch wird leicht höher, was sich der Erfahrung mit einem Surface GO nur im Minutenbereich bemerkbar macht. Gefühlt ist die Arbeit aber spürbar flüssiger geworden.

Importieren einer Liste von SPAM-Absendern

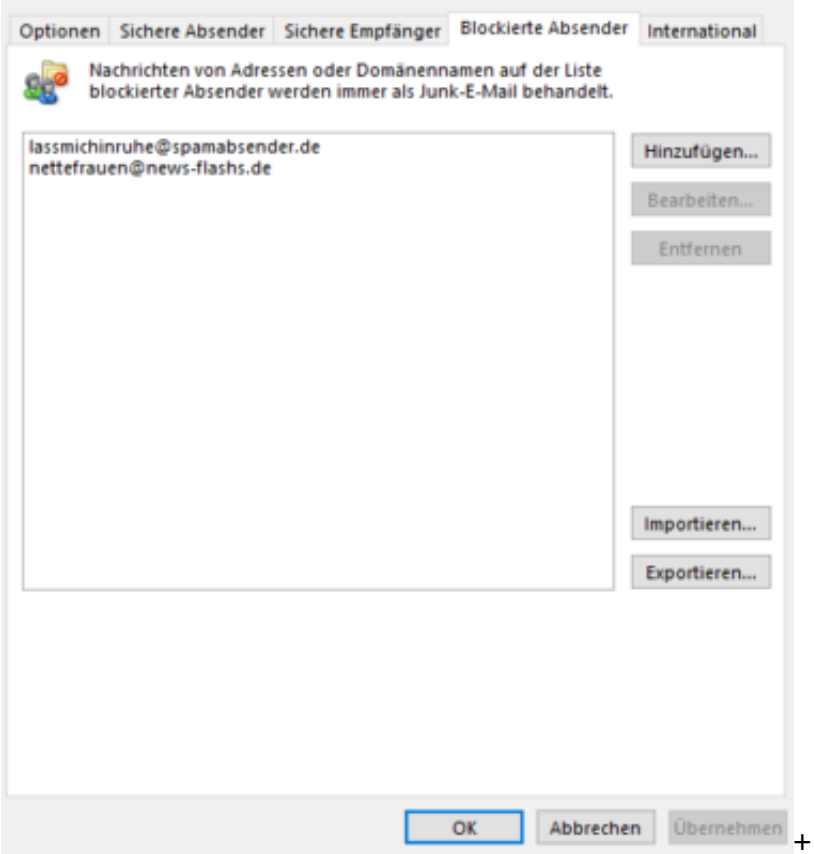
SPAM ist eine der Plagen der Neuzeit: Ohne geeignete Software und Dienste ist es kaum noch möglich, die wichtigen E-Mails von den unwichtigen Werbe- und Phishing E-Mails zu trennen. Der Aufbau einer eigenen Liste unerwünschter (oder erwünschter) Absender ist eine mühsame Angelegenheit, zumal es keine wirklichen Anbieter dieser Listen gibt: Dienste, die Mails gegen eigene Absenderlisten abgleichen, lassen sich gut bezahlen. Zumindest im Freundes- und Bekanntenkreis können Sie aber mit einem kleinen Trick Ihre SPAM-Adresslisten austauschen!

[caption id="attachment_760914" align="alignnone" width="500"]


geralt / Pixabay[/caption]

Export und Import in Outlook

Klicken Sie der rechten Maustaste auf eine beliebige E-Mail und dann auf **Junk-E-Mail**, **Junk-E-Mail-Optionen**. Je nach der Liste, die Sie bekommen haben oder weitergeben möchten, klicken Sie auf **Sichere Absender** oder **Blockierte Absender** (letzteres ist hier die sinnvollere Wahl, denn SPAMmer treffen die meisten Anwender gleichermaßen, während jeder Anwender unterschiedliche "sichere" Absender haben wird).



Klicken Sie nun auf **Exportieren**, um Ihre Liste der Absender in eine Textdatei exportieren zu können. diese Datei können Sie per E-Mail oder auf einem USB-Stick an Bekannte weitergeben, wenn Sie das möchten. Wenn Sie eine Liste bekommen haben, die Sie importieren wollen, dann klicken Sie auf **Importieren**.

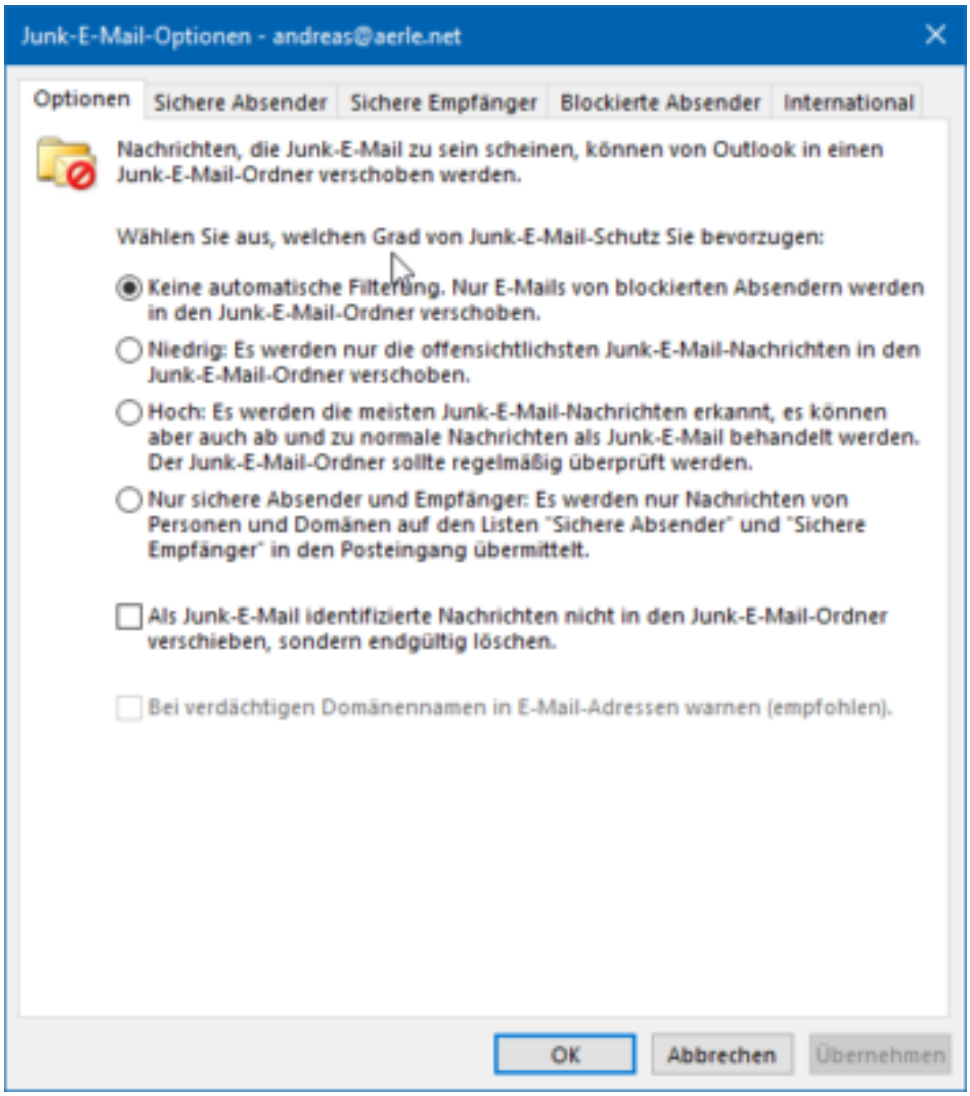
Konfiguration der automatischen Mailfilterung von Outlook

Microsoft Outlook bringt ein breites Instrumentarium an Filtermechanismen mit, die automatisiert versuchen, die Spreu im Weizen Ihrer E-Mails zu trennen. Der Ordner Junk Email enthält alle als SPAM qualifizierten E-Mails. Allerdings kann es durchaus sein, dass die automatischen Filterregeln zu streng oder zu weich sind und dadurch entweder Mails Ihrer Aufmerksamkeit entgehen oder doch noch zu viele unerwünschte Mails im Posteingang landen. Das muss nicht sein!

Klicken Sie der rechten Maustaste auf eine beliebige E-Mail und dann auf **Junk-E-Mail**, **Junk-E-Mail-Optionen**.

Blacklist, Whitelist, Internationale E-Mails

In mehreren Reitern bietet Outlook verschiedene Filtermechanismen: Unter Optionen können Sie einstellen, wie streng Outlook Mails als SPAM identifiziert: Von geringer Strenge (nur explizit als unerwünscht festgelegt Absender werden verschoben) bis hin zu der genauen Festlegung der Empfänger/Absender, die in den Posteingang gelassen werden können Sie frei wählen. Es macht Sinn, mit den Einstellungen zu experimentieren und das Ergebnis zu kontrollieren!



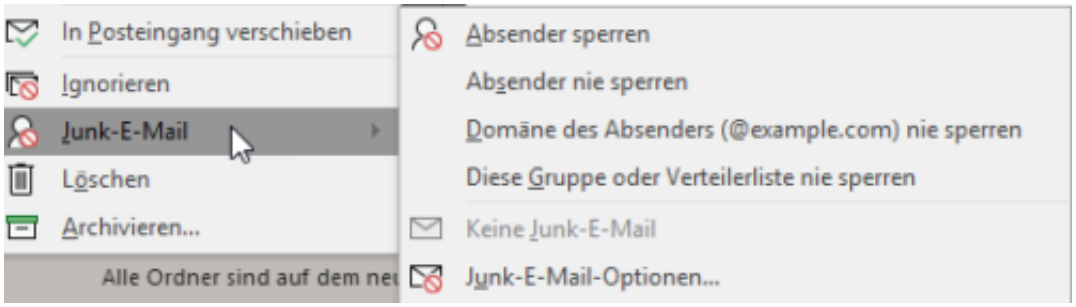
Sie können sichere Absender definieren, deren E-Mails immer in den Posteingang gelangen, Absender immer blockieren und sogar Mails aus bestimmten Ländern blockieren (beispielsweise alle Emails mit der Kennung .ru für Russland).

Befreien von Mails aus den Junk-E-Mails

Der Junk-E-Mail-Filter und die automatische Sortierung von "unwichtigen" E-Mails in das Clutter-Verzeichnis bei Outlook und Office 365 ist ein hilfreicher Automatismus, der Ihnen eine Menge an Arbeit sparen kann. Allerdings nur dann, wenn er richtig funktioniert. Es kommt immer wieder vor, dass so genannte "False Positives", also E-Mails, dee fälschlicherweise als SPAM identifiziert wurden, auftreten. Wir zeigen Ihnen, wie Sie diese von ihrer Markierung als unerwünschte Post befreien können.

Einzelne E-Mails als erwünscht kennzeichnen

Um eine einzelne E-Mail zu kennzeichnen, dass sie wider der Einschätzung von Outlook doch erwünscht ist, klicken Sie sie mit der rechten Maustaste an, dann auf **Junk-E-Mail** und auf **Absender nie sperren**.



Wenn Sie gleich allen Absendern der zugehörigen Mail-Domäne (zum Beispiel schieb.de) Vertrauen schenken, dann können Sie auf **Domäne des Absenders (@example.com) nie sperren**.

Wichtig zu wissen: Damit wandern die E-Mails zwar nicht mehr in den Junk-E-Mail-Ordner. Wenn Sie diese aber öfter ungeöffnet löschen oder ein einen Ordner verschieben, dann kann es durchaus sein, dass diese im Clutter landen!