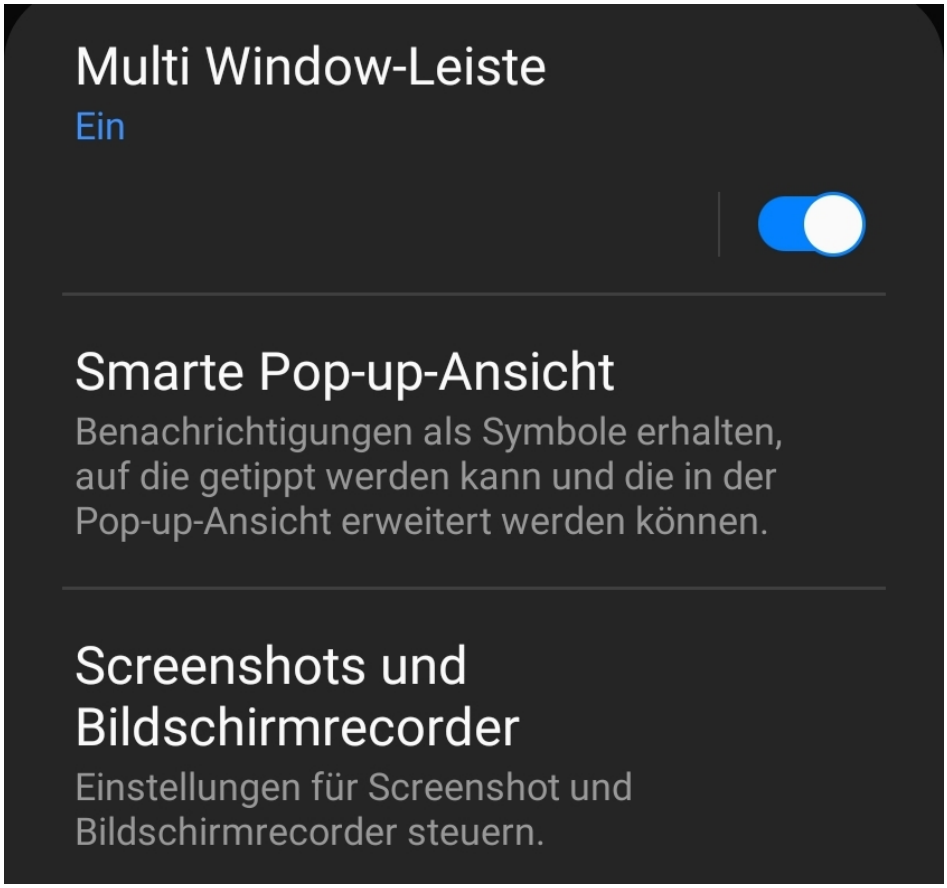
Schieb Report

Ausgabe 2020.21

Benachrichtigungen als PopUps bei Android 10

Sie verlassen sich auf die Benachrichtigungen Ihres Android-Smartphones. Oft nicht nur auf die Information, dass es neue Elementen, Nachrichten oder Kontakte gibt. Neben der Information ist die schnelle Reaktion darauf ein wichtiger Punkt. Der Benachrichtigungsbereich ist nur eine der Stellen, an der Sie auf Benachrichtigungen reagieren können. Wir zeigen Ihnen einen effektiveren Weg!

Um auf eine Benachrichtigung zu reagieren, streichen Sie mit dem Finger vom oberen Bikdschirmrand nach unten. Dann tippen Sie die Benachrichtigung an. Android öffnet jetzt die zugehörige App. In der können Sie das neue Element dann öffnen und darauf regieren. Beispielsweise durch eine Antwort, ein Like oder eine andere Aktion. Das sind allerdings recht viele Schritte. Bei Apps, die eine Unterhaltung erlauben (der Messenger, Nachrichten, WhatsApp) geht das auch schneller.



Die Smarte Pop-up-Ansicht ist eine Funktion vieler neuerer Android-Geräte, die Sie für bestimmte Apps einschalten können. Sie finden Sie unter **Einstellungen** > **Erweiterte Funktionen** > **Smarte Pop-up-Ansicht**. Sie finden im Einrichtungsmenü eine Liste der vorgeschlagenen Apps und können diese noch erweitern. Aktivieren Sie für jede in Frage kommende App den Schalter neben ihrem Eintrag.

Die Benachrichtigung erscheint dann nicht als Eintrag in der Benachrichtigungsliste, sondern als kleines Pop-up-Symbol direkt auf dem Bildschirm. Das tippen Sie an und sind direkt in der Benachrichtigung in der zugehörigen App. Dort können Sie ohne Zeitverzug direkt darauf reagieren.

iOS und Android sind nun Corona-Warn-App-tauglich

Apple und Google haben sich vor einigen Wochen gemeinsam verpflichtet, eine Schnittstelle für den diskreten Datenaustausch per Bluetooth Low Energy in die mobilen Betriebssysteme einzubauen. Ein wichtiger Bestandtteil für Corona-Warn-Apps wie die der Bundesregierung. Jetzt haben die beiden US-Konzerne die Schnittstelle fertig - und in ihre mobilen Betriebssysteme eingebaut.

Damit die Corona Warn App der Bundesregierung funktionieren kann (wie viele andere Warn-Apps in Europa auch), müssen Apple und Google eine neue "Schnittstelle" (Fachbegriff für: Erweiterung, die auch von Apps genutzt werden kann) vorsehen. Die beiden US-Konzerne haben diese Aufgabe jetzt zeitgkeich erledigt. Mittwoch abend (21.05.20) hat Apple iOS 13.5 und iPad iOS 13.5 zum Download freigegeben. Auch Google hat eine neue Version ausgerollt.

Man könnte diese Aktualisierung auch Corona-Update taufen, denn die Neuerungen stehen im Zeichen der Pandemie. Im Zentrum steht die gemeinsam entwickelte Schnittstelle, die für die Corona Warn App der Bundesregierung wichtig ist.

Nur ausgewählte Apps können die Funktion nutzen

Die "Exposure Notification API" erlaubt es ausgewählten Apps, auf Mobilgeräten auch im Hintergrundbetrieb unbemerkt und energiesparsam per Bluetooth IDs auszutauschen. Die Nutzer müssen diese Funktion allerdings ausdrücklich im Gerät aktivieren. Eine Deaktivierung ist jederzeit möglich.

Nur ausgewählte, von Apple manuell freigegebene Apps von Gesundheitsbehörden in aller Welt haben Zugriff auf diese Funktion, betont Apple-Chef Tim Cook in einem Tweet. Warn-Apps aus 22 Ländern. Nur eine App pro Land. Das ist sehr wichtig zu wissen, denn anderenfalls hätten sich blitzschnell auch andere Apps diese Funktion "geschnappt". Zum Beispiel Partnerschafts-Apps, Kontakt-Apps wie Tinder oder ganz sicher auch die Werbeindustrie. Durch diese Sicherheitsmaßnahme bleibt die sinnvolle Funktion nur den Warn-Apps vorbehalten.

Bald kommt noch eine eigene Plattform von Apple und Google

Die eigentliche Datenverarbeitung der Kontakte und auch die Warnung, wenn ein möglichner Kontakt mit einer infizierten Person vorgelegen haben könnte, erledigt nicht Apple (iOS) oder Google (Android), sondern die jeweilige Warn-App. Noch, denn Apple und Google wollen in einigen Wochen eine gemeinsame Plattform vorstellen, dann reicht ein einfaches Opt-In im Smartphone, um die Kontaktverfolgung zu ermöglichen. Auch ohne eine Warn-App installiert haben zu müssen.

Es gibt noch eine weitere Corona-spezifische Neuerung in iOS 13.5: Wenn Nutzer/innen Maske tragen, funktioniert die Gesichtserkennung nicht mehr. Es entfallen zu viele wichtige Punkte im Gesicht. Erkennt das Betriebssystem das Tragen einer Maske, erscheint nun schneller das Eingabefeld für die PIN.

Maske tragen und Gesichtserkennung

Die Wartezeit wird verkürzt. Eine Kleinigkeit, aber wer nun plötzlich 20x am Tag die PIN eingeben muss, spart so einiges an Zeit. Auch bei Bezahlvorgängen, im App-Store - überhaupt immer, wenn die Gesichtserkennung zur Authentifizierung zum Einsatz kommt.

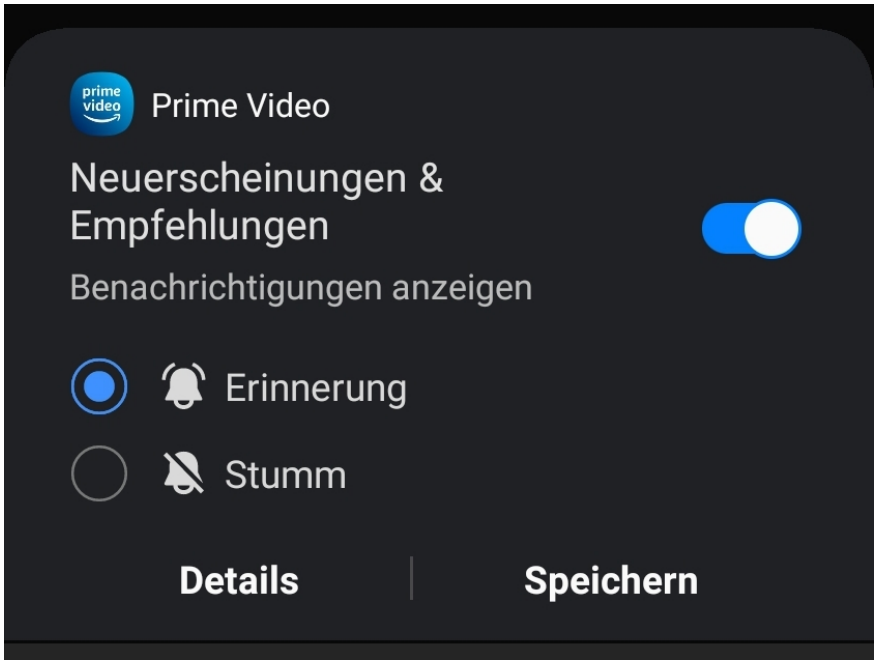
Eine Standortverfolgung (Tracking) ist mit der neuen Schnittstelle nicht möglich. Außerdem haben beide Unternehmen darauf geachtet, dass die Nutzung der Kontaktermittlung mit Bluetooth im Hintergrund so wenig Energie wie möglich verbraucht - also akkuschonend erfolgt.

Benachrichtigungen bei Android schnell stummschalten

Benachrichtigungen auf dem Smartphone sind das Salz in der Suppe. Dem einen versalzen sie die Suppe, weil sie zu sehr ablenken, dem anderen können Sie gar nicht oft genug angezeigt werden. Irgendwo zwischen dieses beiden Extremen werden Sie sich bewegen und müssen sehen, wie Sie diese umsetzen. Android ist da relativ flexibel, mit unserem Tipp geht es aber noch einfacher als auf den ersten Blick zu vermuten!

Die Benachrichtigungseinstellungen von Android finden Sie unter **Einstellungen** > **Benachrichtigungen**. Hier können Sie ganz in Ruhe festlegen, ob Sie überhaupt Benachrichtigungen angezeigt bekommen wollen. Ebenso, wie diese in der Nachrichtenleiste dargestellt werden sollen. Sie können an dieser Stelle die Benachrichtigungen für die letzten drei Apps direkt deaktivieren. App für App können Sie schließlich festlegen, wie die Benachrichtigungen für diese App jeweils erfolgen sollen.

Dieser Prozess ist toll für die Ersteinrichtung, weil Sie damit strukturiert einmal alle Apps durchgehen können. Oft aber sind es spontane Einsätze: Eine App nervt Sie mit einer Benachrichtigung, die wollen Sie zukünftig nicht mehr sehen. Dann streichen Sie mit dem Finger vom oberen Bildschirmrand herunter, um die Liste der Benachrichtigungen angezeigt zu bekommen.



Halten Sie dann den Finger auf die Benachrichtigung, um die es geht. Direkt am oberen Rand des Fensters sehen Sie den Schalter, mit der Sie diese ab sofort deaktivieren können. Dazu müssen Sie nicht einmal mehr ins Einstellungsmenü gehen!

HPI Identity Leak Checker: Passwortcheck deluxe

Passwörter können Sie in Ihrem eigenen System gut schützen, denn da haben Sie die Kontrolle. Anders sieht es bei den Anbietern aus: Wenn diese Opfer eines Cybereinbruchs sind, dann sind Ihre Benutzerdaten schnell im Internet verfügbar. Das können Sie zumindest prüfen: Das Hasso-Plattner-Institut bietet mit dem kostenlosen Identity Leak Checker unter https://sec.hpi.de/ilc/ einen entsprechenden Service.

Geben Sie auf der Seite die E-Mail-Adresse ein. Sie bekommen an genau diese E-Mail-Adresse eine Liste der Leaks, in denen diese sich befindet. In dieser E-Mail finden Sie noch detailliertere Informationen als in der Datenbank von HaveIBeenPwned: Sie sehen auch, welche Daten abgeflossen sind.

Wenn Sie betroffen sind, dann ändern Sie so schnell wie möglich das Passwort. Führen Sie die Abfrage regelmäßig durch. Auch wenn Sie das nach dem Vorfall wissentlich oder unwissentlich schon gemacht haben: Besitzer der erbeuteten Daten wissen zumindest, dass die Benutzernamen und E-Mail-Adressen existieren. Sie müssen sich so nur noch darauf konzentrieren, das Passwort herauszufinden.

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse andreas@ taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf.
Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozial-versicherungsnr.	IP-Adresse
Combolist	Jan. 2019		1.247.433.080	Betroffen	–	–	–	–	–	–	–	–
	Der Ursprung der Daten ist unklar. Auch ist nicht bekannt, wie alt die Daten sind bzw. wo genau diese erlangt wurden. Vermutlich handelt es sich aber um eine Zusammenstellung zahlreicher älterer Leaks und Daten aus Phishingkampagnen.											
Unknown (Collection #1-#5)	Jan. 2019		2.191.498.885	Betroffen	–	–	–	–	–	–	–	–
	Dieser Datensatz wurde im Januar 2019 veröffentlicht und enthält riesige Listen von Zugangsdaten unbekannter Herkunft, ältere Leaks und kleinere Datenbankabzüge.											
Onliner Spambot (Spamlist)	Aug. 2017		128.471.704	–	–	–	–	–	–	–	–	–
WHOIS Database (NET-Domains)	Mär. 2017	✓	7.572.808	–	–	–	–	–	–	–	–	–
WHOIS Database (NET-Domains)	Mär. 2017	✓	7.572.808	–	Betroffen	–	–	Betroffen	–	–	–	–
Phishing Data (LKA)	Feb. 2017		4.713.404	Betroffen	–	–	–	–	–	–	–	–
	Dieser Datensatz wurde vom LKA bei einem Ermittlungsverfahren beschlagnahmt und stammt aus verschiedenen Phishingkampagnen im deutschen Sprachraum. Das LKA hat dem HPI die betroffenen E-Mail-Adressen ausgehändigt.											
Unknown (Anti-Public Combolist Jan. 2017)	Jan. 2017		948.385.599	Betroffen	–	–	–	–	–	–	–	–
Unknown (Anti-Public Combolist)	Dez. 2016		541.567.187	Betroffen	–	–	–	–	–	–	–	–

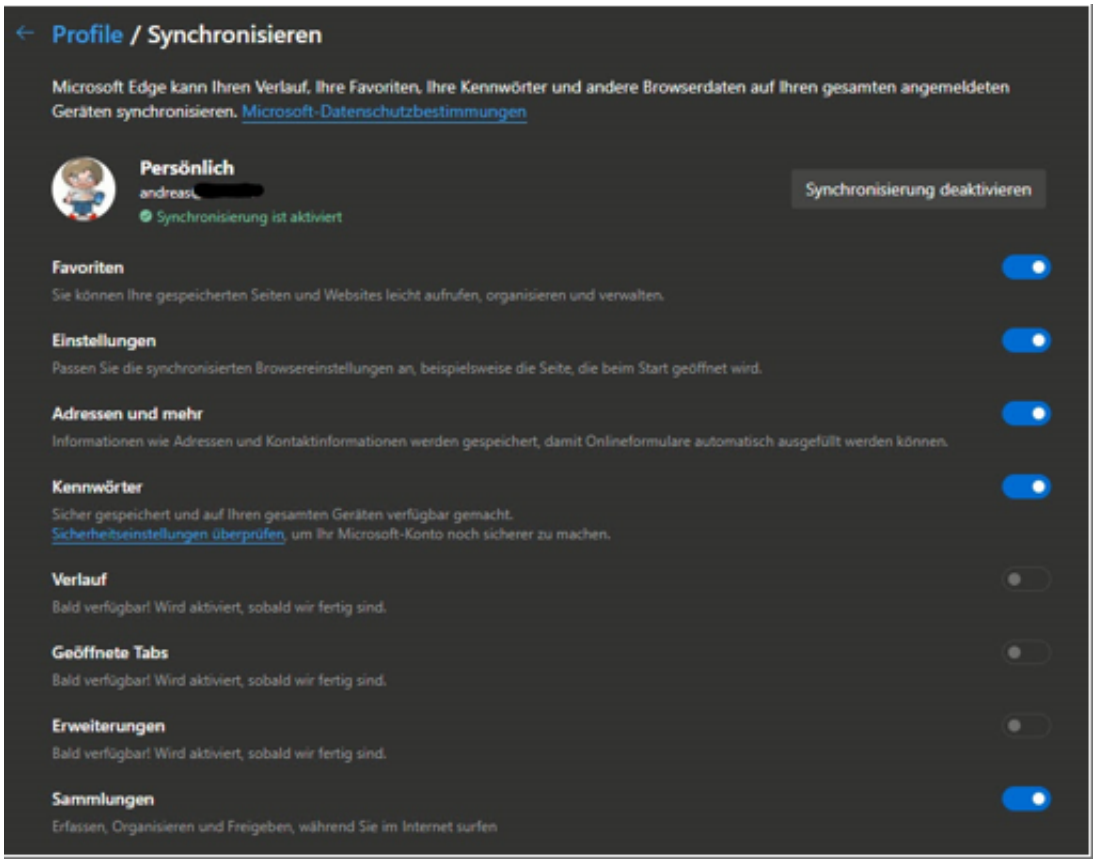
Keine dieser Datenbanken erhebt natürlich Anspruch auf Vollständigkeit. Nur, weil Ihre E-Mailadresse nicht als betroffen gekennzeichnet wird, können damit zusammenhängende Kombinationen aus Benutzername und Kennwort trotzdem in die falschen Hände gelangt sein!

Echten Schutz dagegen gibt es nicht. Natürlich macht es Sinn, Ihre Kennwörter auch ohne konkreten Anlass regelmäßig zu ändern. Dabei sollten Sie eben keine erkennbare Systematik zu verwenden. Ab dem Zeitpunkt der Änderung ist der Zugang für einen Fremden mit den erbeuteten Passwörtern nicht mehr möglich.

Synchronisieren der Passwörter in Edge

In der Praxis verwenden Sie meist mehrere Geräte, mit denen Sie auf das Internet zugreifen. Damit können Sie auch die Anmeldungen an Webseiten und Diensten durchführen. Die meisten Browser haben einen eigenen zugehörigen Dienst (Microsoft das Microsoft-Konto, Google den Google-Account etc.). Darüber können Sie die Kennwörter dann synchronisieren. Die bisher gespeicherten Passwörter sind verfügbar und neu hinzugefügte oder veränderte Passwörter werden auf die anderen Geräte übertragen. die Voraussetzung: Sie haben auf allen Geräten den selben Browser installiert.

Um die Synchronisation in Edge zu aktivieren, klicken Sie auf das Symbol mit dem Kopf oben rechts in Edge und dann auf **Anmelden**. Geben Sie die Zugangsdaten Ihres Microsoft-Kontos ein und bestätigen Sie die Anmeldung. Wenn Sie die Zwei-Faktor-Authentifizierung aktiviert haben, müssen Sie noch den Zahlencode eingeben.



Wenn Sie dann auf **Einstellungen** > **Profile** > **Synchronisierung** klicken, können Sie ganz fein einrichten, welche Elemente mit der Cloud synchronisiert werden sollen. Darunter eben auch die Passwörter.

Hier hat der neue Edge-Browser im Gegensatz zu seinen Vorgängern einen Vorteil: Er ist auch auf dem Mac verfügbar und wurde sogar für Linux angekündigt. Somit können Sie ihn auf allen gängigen Systemen benutzen.

Automatische Updates beim Mac aktivieren

Auch wenn das manchmal nicht so offensichtlich ist: Auch ein Gerät mit macOS benötigt Updates. Dabei geht es nicht nur um die neuen Versionen von macOS, die nahezu im Jahresrhythmus veröffentlicht werden, sondern viel mehr um die vielen kleineren Patches. Die beseitigen kleinere Fehler bis hin zu gefährlichen Sicherheitslücken. Es macht Sinn, diese zeitnah zu installieren. Warum nicht gleich automatisch?

Das Vorliegen von Updates finden Sie auf dem Mac am schnellsten, wenn Sie auf den Apfel oben links ab Bildschirm klicken. Neben **Systemeinstellungen** finden Sie die Zahl der mac-OS-Updates, unter **App Store** die Zahl der Apps, für die es ein Update gibt. Ein Klick auf einen der beiden Einträge führt direkt zu den Updates und deren manueller Installation.

Für macOS-Updates können Sie direkt im Update-Bildschirm (oder unter **Einstellungen** > **Softwareupdate**) einen Haken neben **Meinen Mac automatisch aktualisieren setzen**. MacOS prüft dann regelmässig auf Updates und installiert diese.

Für App-Updates starten Sie den App Store, klicken Sie in der Menüleiste auf **App Store** > **Einstellungen**. Aktivieren Sie dort **Automatische Updates**. Auch hier sucht Ihr Mac automatisch nach Updates und installiert diese. Er informiert Sie nur, wenn er die Zustimmung für Lizenzbedingungen oder ähnliches benötigt.

Die gute Nachricht des BND-Urteils

Die Skepsis ist groß in der Bevölkerung: Will die Regierung die Bürgerinnen und Bürger mit der Corona-Warn-App lückenlos überwachen? Es spricht zwar so ziemlich alles dagegen - trotzdem lassen sich viele nicht überzeugen. Etwas Beruhigendes gibt es aber: Das Bundesverfassungsgericht (BVG) achtet sehr genau darauf, dass die Grundrechte eingehalten werden. Auch jetzt wieder. Das BVG hat dem Bundesnachrichtendienst (BND) strengere Grenzen für seine Überwachungsarbeit gesteckt.

Das Bundesverfassungsgericht hat sich genau angeschaut, welche Rechte der Gesetzgeber dem Bundesnachrichtendienst (BND) eingeräumt hat - um Ausländer im Ausland zu überwachen. Die Antwort der Richter ist an Klarheit nicht zu überbieten: Die Internet-Überwachung des BND ist in seiner jetzigen Form in Teilen verfassungswidrig. Grundrechte gelten auch im Ausland. Deshalb muss der Gesetzgeber nachbessern - und hat dafür bis Ende 2021 Zeit.

Viele hören vielleicht weg, wenn sie eine solche Meldung lesen. Denn der Bundesnachrichtendienst - der darf ja sowieso keine Bundesbürger belauschen. Schon gar nicht im Inland. Betrifft also nur die anderen. Ausländer. Im Ausland.

BND überwacht gezielt den Internet-Traffic

Aber so einfach ist das nicht. Denn der BND klinkt sich am größten Internetknoten der Welt (De-Cix) in Frankfurt ein, um gezielt Informationen aus diesem gigantischen Datenstrom zu ziehen. Das Argument: Fast alle Daten, die aus Deutschland ins Ausland gehen oder umgekehrt aus dem Ausland nach Deutschland kommen, passieren diesen Netzknoten.

Theoretisch kann der BND auf diese Weise täglich bis zu 1,2 Billionen sogenannte Verbindungen analysieren und auf Auffälligkeiten untersuchen. Die Frage ist aber: Schaut sich der BND nur die Verbindungen an, die er von Rechts wegen auch anschauen darf?

Nahezu unmöglich, keine Fehler zu machen

Praktisch alle Verbindungen, die wir mit dem Ausland herstellen - egal, ob E-Mails, Videos, Webseiten, Chats - laufen über den Knoten in Frankfurt. Eine sensible Sache, wenn ein Geheimdienst hier abhören darf. Denn am Ende - da sind sich alle Experten einig - ist es praktisch unmöglich, präzise wie ein Neurochirurg genau die Informationshäppchen herauszuschneiden, die den BND wirklich etwas angehen - und alle anderen unangetastet zu lassen.

Die Tatsache, dass Geheimdienste - allen voran die NSA - Menschen in aller Welt ausspionieren, lässt viele glauben, auch sie würden rund um die Uhr komplett überwacht. Und auch im Falle der NSA ist leider eine Menge dran, wie wir seit den Enthüllungen von Edward Snowden wissen.

Das erklärt meiner Ansicht nach zum Teil das große Misstrauen, das viele Menschen gegenüber dem Staat hegen. Motto: "Die überwachen uns doch sowieso."

Signalwirkung für Corona-App

In diesen diffusen Strudel des Misstrauens wird auch die Corona-Warn-App gezogen. Hier hat zwar der BND nichts zu melden, da die App nur im Inland eingesetzt wird. Aber das Misstrauen bleibt. Nicht wenige glauben ja, es handele sich dabei um ein Spionagewerkzeug. Eine App, die einen auf Schritt und Tritt überwacht - obwohl die Fakten klar dagegen sprechen.

Doch in Deutschland wird die Gewaltenteilung ernst genommen: Das Verfassungsgericht

schaut ganz genau hin - und setzt dem Gesetzgeber klare Grenzen. Ein vertuschtes Abhören aller Bürger wird es nicht geben.

#Crowdless App: Wo kann man gerade bequem einkaufen gehen?

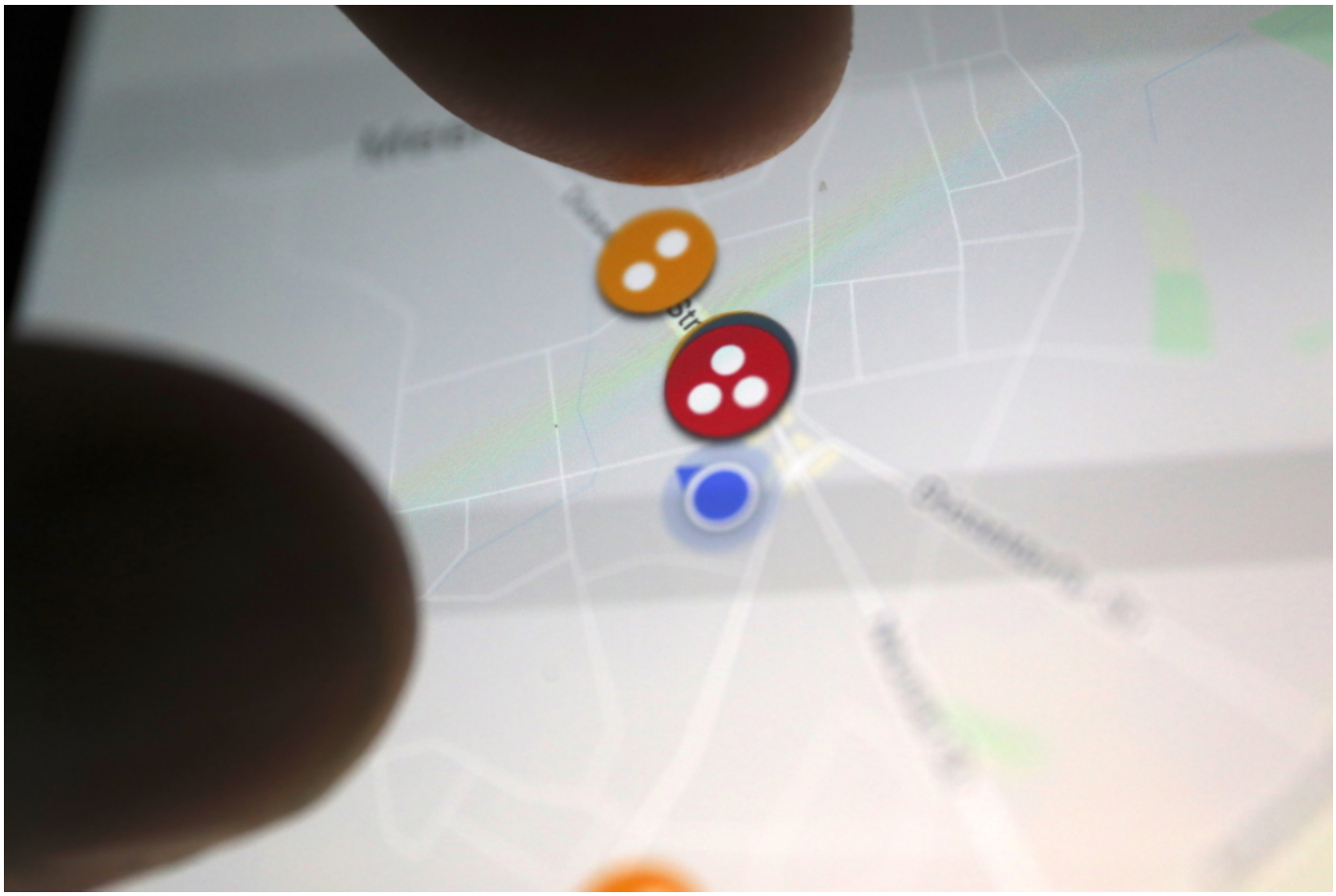
Eine der großen Herausforderungen derzeit ist: Wann sollte ich einkaufen gehen, damit die Warteschlangen möglichst kurz sind? Eine neue App namens Crowsless kann da helfen. Sie "weiß", wie voll es gerade in einem Geschäft oder Restaurant ist - oder zu einer bestimmten Zeit sein wird.

Durch die Lockerungen bei den Corona-Beschränkungen ergeben sich mitunter schwierige Situationen: Eben mal ein Eis essen gehen? Denkbar. Aber die Sitzplätze innen sind geblockt, draußen gibt es eine Schlange vor dem Verkaufsstand. Und vor der Apotheke steht man sich die Beine in den Bauch - obwohl die um die Ecke total leer ist. Hätte man das doch nur vorher gewusst...

Elegant Hot Spots vermeiden?

Die App Crowdless, entwickelt in Großbritannien, kostenlos auch bei uns nutzbar, will Abhilfe schaffen. Sie zeigt per Ampel-System, wo es sich gerade knubbelt und wo nicht. So lassen sich Einkaufszeiten bequem und zuverlässig planen.

Wie macht Crowdless das? Ganz einfach: Google hat längst 100 Mal mehr Daten, als es die offizielle Corona Warn-App je wollte. Deshalb weiß Google Maps auch ganz genau, wann die Pizzeria öffnet, wie viele Leute gerade da sind - und wie es im Wochendurchschnitt aussieht. Auf diese Daten greift Crowdless zurück. Keine Hexerei, die Daten lassen sich auch in Google Maps direkt abrufen.



Daten aus unterschiedlichen Quellen genutzt

Die App nutzt verschiedene Quellen: Google Maps, GPS/GNSS sowie die aktiven Meldungen der Crowdless-User. Daraus ergibt sich ein Bild über die aktuelle Besuchersituation. Selbst ob Parkplätze vor Einkaufszentren aktuell gut besucht sind, lässt sich auf diese Weise ermitteln.

Das alles funktioniert vom Start weg. Wichtig sind aber natürlich auch die Daten, die die User selbst liefern: Sie können via App melden, wie voll es ist. Auf diese Weise kann die App errechnen, ob in einem Geschäft, einer Ladenpassage, einem Restaurant, einem Bistro mit Menschenmengen zu rechnen ist.

Könnte kommen: Virtuell anstellen

Eine gute Idee: Die Daten haben die Menschen sowieso schon "gespendet" (via Google Maps und ohne Proteste) - nun lassen sich diese sinnvoll nutzen. Ich habe die App ausprobiert: Die Angaben stimmen häufig - aber nicht immer. Es ist und bleibt eben Statistik und keine reale Abbildung der Wirklichkeit.

Die App ist kostenlos und anonym. Es ist keine Anmeldung erforderlich. Die Entwickler sagen, zurzeit werde die App von der europäischen Raumfahrtbehörde ESA, der Oxford University und der London School of Economics finanziert.

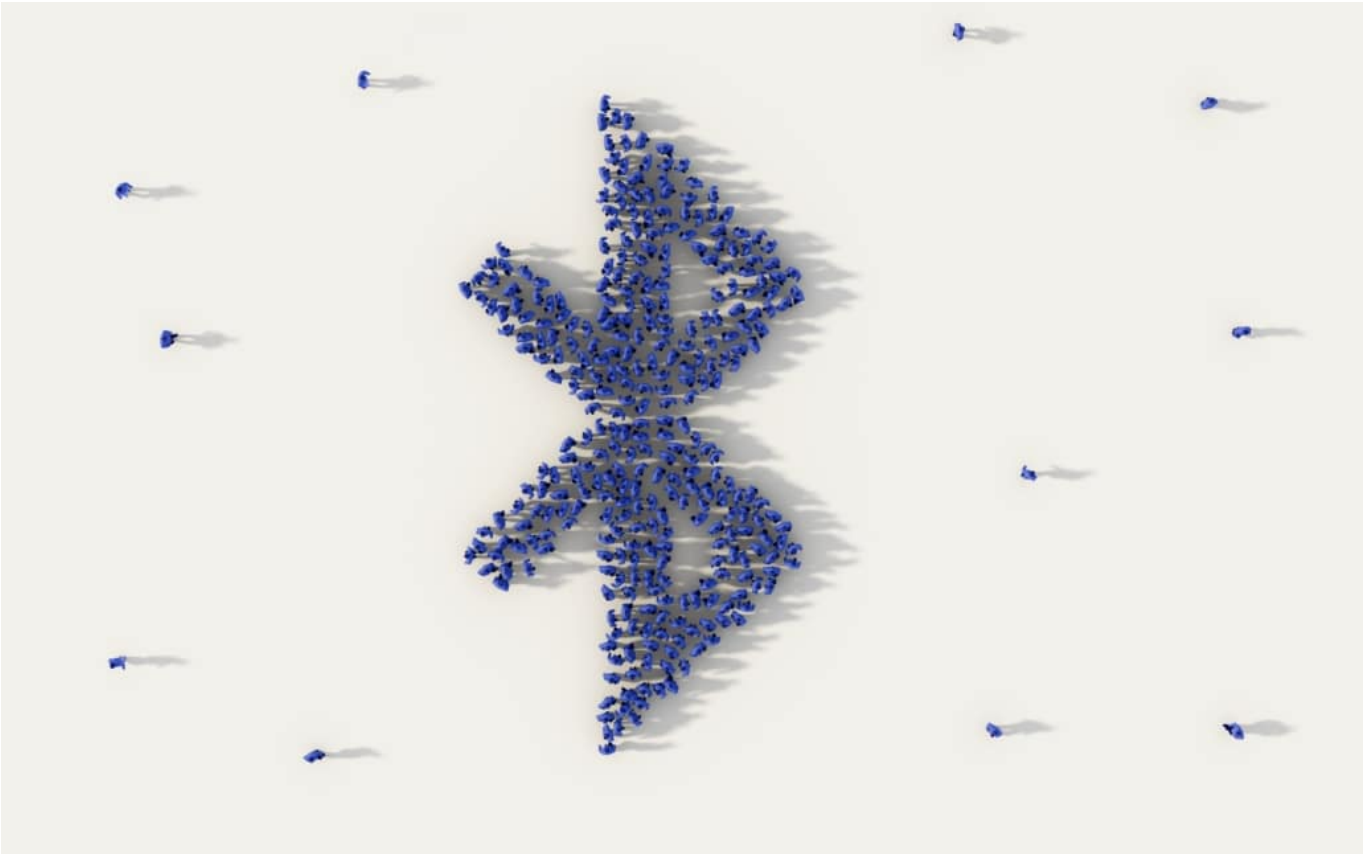
In Zukunft könnte mit der App Geld verdient werden, etwa indem sich die User "virtuell anstellen" können. Also schon zu Hause in die Reihe stellen - und zu einem bestimmten Zeitpunkt tatsächlich eintreten. Oder, indem die App die Menschen zu einer Filiale einer Kette in der Nähe schickt, in der weniger los ist.

Corona: Europaweit reisen dank Corona App? Äh, eher nein...

Seit Wochen ist die Corona Warn App – so soll sie offiziell nun heißen – in der Diskussion. Manche halten sie für das wichtigste Instrument überhaupt, um Infektionsketten zu unterbrechen. Andere halten sie für Teufelswerk, weil sie eine komplette Überwachung befürchten. Die Wahrheit liegt wahrscheinlich – wie meistens – irgendwo in der Mitte. Fest steht aber: Die Reisebeschränkungen werden gelockert. Grenzen sollen sich öffnen. Welche Rolle kann die Corona App da spielen – es ist doch eine deutsche App. Was ist, wenn man im Ausland unterwegs ist oder wenn man auf Ausländer im eigenen Land trifft?

Die EU-Kommission hat klare Regeln veröffentlicht, die für eine Öffnung der Grenzen und einen wieder zunehmenden Reiseverkehr unerlässlich sind. Neben Virustests und Quarantäne-Maßnahmen setzt Brüssel vor allem auf die Möglichkeit zur Nachverfolgung von Kontaktpersonen. Tracing-Apps könnten da hilfreich sein. Das EU-Paket enthält klare Leitlinien, wie die Apps miteinander Daten austauschen sollen.

Per Bluetooth Low Energy – wie bei „unserer App“. Das soll grenzüberschreitend, freiwillig und plattformunabhängig funktionieren. Technische Details müssen noch erarbeitet werden, wie das funktionieren soll, auch auch wirklich datenschutzkonform zu sein.



Kann die deutsche Corona App europaweit Daten tauschen

Die Corona App in Deutschland befindet sich bereits in der Entwicklung. Wird sie den Anforderungen genügen?

Das wird sie müssen. Erste Dokumente und Code-Auszüge sind jetzt öffentlich als OpenSource einsehbar, also als Quellcode, in den jeder reinschauen darf. Die Experten werden prüfen, ob alle Anforderungen eingehalten werden. Aber die grenzüberschreitende Kommunikation ist noch nicht vorgesehen – dafür braucht es erst mal die verabschiedeten Standards.

Es hat schon mal einen Versuch gegeben, den paneuropäischen Standard PEPP-PT. Aber der ist gescheitert. Deswegen braucht es eine neue Lösung. Es kann also noch was dauern. Der offizielle Starttermin der App ist bereits schon wieder verschoben worden: auf den 15. Juni.

Das ist nötige für europaweites Tracing

Was braucht es denn, damit mögliche Kontakte von Europäern untereinander und mögliche Infektionssituationen erkannt werden können?

Da es keine EU-App geben wird, müssen die Apps aller einzelner Länder untereinander und über die von Google und Apple entwickelten Corona-Schnittstellen kommunizieren können. Das wird aber schwierig, weil zum Beispiel Frankreich auf eine zentrale Lösung setzt, die es in Deutschland nicht geben wird. Aber Google und Apple unterstützen zentrale Lösungen nicht.

Es wird also richtig schwierig, da dadurch selbst der Umweg über Google und Apple versperrt bleibt. Auch haben Datenschützer Bedenken, die eigentlich anonymen IDs, die in den Smartphones ständig erzeugt werden, mit einer Länderkennung zu versehen.

Das wäre aber nötig, um grenzüberschreitende Begegnungen zu erkennen – und nachvollziehen zu können. Weil Franzosen, Schweizer, Niederländer oder Spanier in anderen Corona-App-Netzen unterwegs sind als wir, müsste ja „Meldung“ gemacht werden, wenn eine Infektion vorliegt, anderenfalls erfahren die Kontakte nichts davon. Eine sehr schwierige Situation.

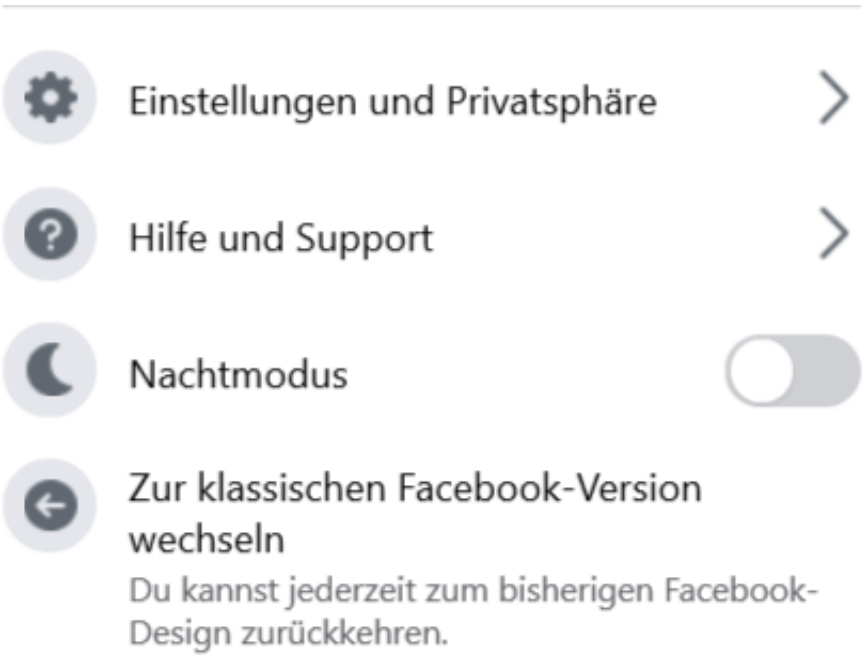
Klingt so, als wären wir noch weit entfernt von einer EU-weiten Lösung?

Allerdings. Es müssen noch etliche Nüsse geknackt werden, bevor es los geht. Und selbst wenn diese Probleme gelöst werden: Die Zustimmung für eine Corona App nimmt ab. Laut einer aktuellen Studie der Uni Erfurt würden sich nur noch 44% der Bundesbürger so eine App installieren. Vor einigen Wochen waren es weit über 60%. Die mögliche Wirkung solcher Apps schwindet also von Woche zu Woche.

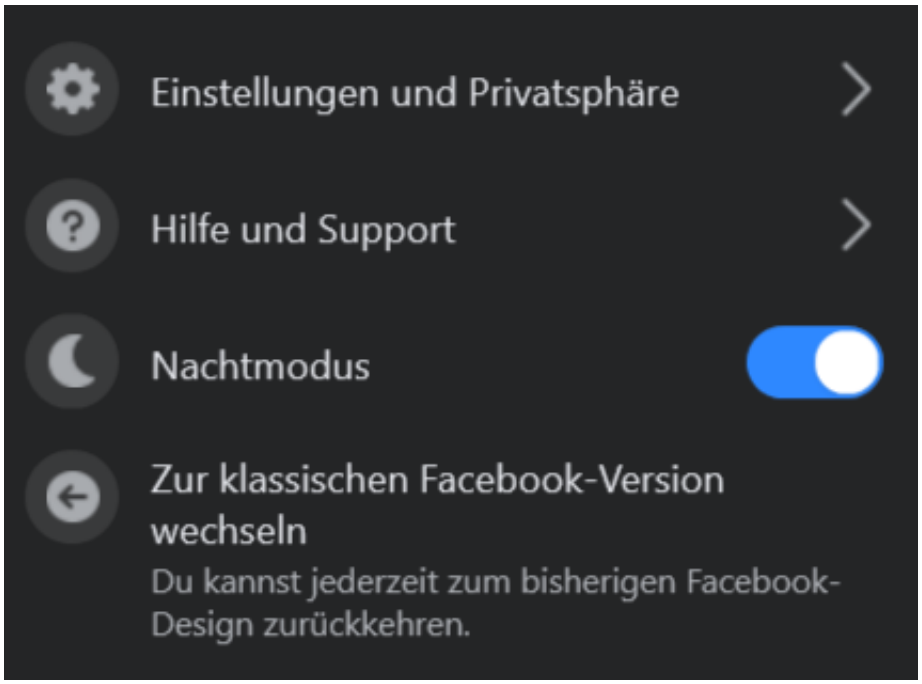
Wechsel zwischen neuem und altem Facebook-Design

Die Web-Version von Facebook ist schon ein wenig in die Jahre gekommen. Folgerichtig hat Facebook damit begonnen, eine neue, modernere Version der Oberfläche auszurollen. Die wird nicht unbedingt für jeden Anwender optimal sein. Wir zeigen Ihnen, welche Einstellungen Sie kenne sollten!

Die Veränderungen der neuen Facebook-Version sind vor allem kosmetischer Natur: Die Farben sind angepasst, die Symbole ein wenig moderner, die Hinweis-Bubbles auffälliger. Das "Look and Feel" passt sich also dem aktuellerer Software an. Dazu gehört auch, dass der allgegenwärtige Nachtmodus eingeführt wird. iOS und Android, macOS und Windows haben es vorgemacht: Für viele Anwender ist es angenehmer, wenndie Grundfarbe der Oberfläche Schwarz (statt Weiß) ist.



Um dies umzustellen, klicken Sie auf Ihr Kontobild und schalten Sie den **Nachtmodus** ein. Auf dem selben Weg können Sie den Nachtmodus auch wieder ausschalten.



Um zwischen der alten und der neuen Version von Facebook zu wechseln, klicken Sie auf Ihr Kontobild und dann auf **Zur klassischen Facebook-Version wechseln** oder **Zum neuen Facebook wechseln**. Der Wechsel ist jederzeit während einer Sitzung möglich. Daten gehen dabei nicht verloren.

Anforderungen an Passwörter: Die Qual der Wahl

Ihr Passwörter sind von der Relevanz her wie ein Schlüssel. Nur die Personen, die Zugang benötigen, haben einen, und benutzen ihn auch. Lassen Sie den Schlüssel einfach mal so rumliegen? Eher nicht, der ist am Schlüsselbund und der Schlüsselbund immer in Ihrer Nähe. Ähnlich verhält es sich mit Passwörtern. Ein gutes und sicheres Passwort alleine hilft Ihnen gar nichts, wenn Sie es nicht geheim halten. Und dazu zählt mehr, als es nicht laut auszusprechen!

Wir Menschen sind manchmal noch sehr analog. Was wir uns merken wollen, das schreiben wir lieber mal auf. Man weiß ja nie, wann man die Information wieder braucht und wie es dann um die Erinnerung bestellt ist! Das ist leider auch nicht selten bei Passwörtern der Fall. Viele der Vorfälle, bei denen Passwörter bekannt geworden sind oder Unbefugte mit gestohlenen Zugangsdaten in Rechner und Systeme eingebrochen sind, haben keine technischen Ursachen.

Der Anwender ist das Problem.

Sie ändern das Passwort, das aber meist nicht in Ruhe, sondern „mal eben“ zwischendurch., Nur ist „mal eben“ der kleine Bruder von „unkonzentriert“. Sie schreiben das neue Passwort auf einen Klebezettel. Den packen Sie dann bevorzugt unter die Schreibtischunterlage. Oder an die Rückseite des Monitors. Es gibt sogar Untersuchungen, dass diese Zettel immer an der jeweils anderen Seite Ihrer Schreibhand kleben. Weil Sie sich anstrengen müssen, einen solchen Zettel als Rechtshänder an der linken Seite des Monitors zu befestigen, kommt auch kein anderer Mensch darauf.

Unnötig zu sagen, dass diese Orte genau die sind, an denen Unholde als erstes nach einem Passwort suchen. Die elektronische, sichere und damit deutlich empfehlenswertere Version des Klebezettels ist der Passwort-Manager. Mehr dazu später!

Vermeiden Sie Muster

Die meisten Menschen denken strukturiert und entwickeln Systeme, auch bei Passwörtern. Das ist auf den ersten Blick eine gute Idee, trägt es doch zur besseren Merkbarkeit bei. Genauer betrachtet aber machen Sie damit ein eigentlich gutes Passwort schnell zunichte.

Das aus dem Satz „Ich habe im Sommer 2018 den Motorradführerschein gemacht!“ abgeleitete Passwort *IhiS2018dMg!* ist super. Wenn Sie als nächstes dann aber einfach die Jahreszahl ändern, wenn Sie zur Änderung des Passwortes aufgefordert werden, dann nimmt die Sicherheit rapide ab.

Bei gestohlenen Passwörtern werden automatisch auch „Weiterentwicklungen“ ausprobiert. *IhiS20**19**dMg!* und *IhiS20**20**dMg!* sind da auch für den einfachsten Cyberkriminellen allzu naheliegend. Das selbe trifft dann auch Passwörter wie *Passwort2005!*, Kombinationen aus einem festen Text und wechselnden Jahres- und Monatsziffern. Auch wenn diese einmal mehr bei einem Passwortcheck als gut (weil aus Klein- und Großbuchstaben,

Ziffern, Sonderzeichen bestehend) bewertet werden würden.

Die Quintessenz: Das für sie beste Passwort ist immer eine Kombination aus vielen Faktoren: Technische Anforderungen, persönliche Präferenzen und das menschliche Auge für alle nicht technisch zu erkennenden Schwächen müssen hier zusammenspielen.

Besser kein Zusammenhang zur eigenen Person

Einfache Zahlen- und Ziffernfolgen sind keine gute Idee, das haben Sie mittlerweile schon häufiger gelesen und auch schon vorher selber so gesehen. Was im ersten Moment weniger einsichtig ist: Auch Ihnen bekannte Daten und Begriffe sind keine guten Passwörter. Der BVB-Fan, der *BorussiaBVB09!* als Passwort wählt, hat zwar rein formal ein sicheres Passwort gewählt. Wenn Ihr Schreibtisch aber voll mit BVB-Devotionalien steht, dann ist auch das mit wenig Aufwand zu erraten. Auch persönliche Daten wie Geburts- und Hochzeitstage, Namen von Haustieren und andere sind eher ungeeignet. Wenn Sie sich nur ein wenig in sozialen Netzwerken bewegen, dann sind diese Daten auf Ihren Posts oft ableitbar. Noch schlimmer: Facebook & Co. lieben Kettenbrief-Beiträge.

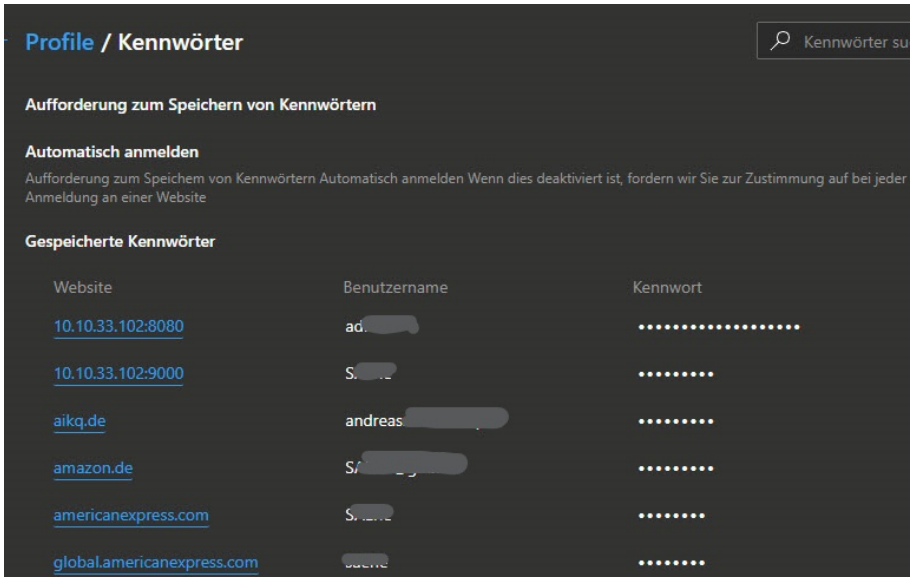
„Jetzt nehme ich das einfach mal auf: Otto Ottensen hat mich eingeladen, 12 Fragen über mich zu beantworten. Ich nominiere Petra Petersen, das auch zu machen."

Ganz zufällig sind diese 12 Fragen dann darauf ausgelegt genau solche Informationen über Sie zu erfragen. Was Facebook weiß, weiß die Welt. Abgesehen davon: Genau diese Informationen werden oft dazu verwendet, ein vergessenes Passwort wiederherstellen zu lassen beziehungsweise ein neues anzufordern: Viele Anbieter lassen Sie beim Anlegen des Kontos genau solche Fragen beantworten und speichern die Antworten. Wer diese Antworten kennt, der kann leichter auf Ihre Daten zugreifen!

Herausfinden vergessener Kennwörter in Microsoft Edge

Es gibt eine Vielzahl von Webseiten, auf denen Sie sich anmelden müssen. Amazon, eBay, Ihre Bank, Facebook und viele mehr schützen Ihr Daten durch die Eingabe von Benutzernamen und Passwort. Wenn Sie den Schutz so stark wie eben möglich haben wollen, dann verwenden Sie unterschiedliche Kombinationen für die Anwendung. Das hat den Nachteil, dass Sie sich viele Informationen merken müssen. Edge bietet hier eine tolle, aber auch mit Vorsicht zu genießende Hilfe.

Sie kennen die Situation bestimmt: Da Gehirn ist noch wach, das Gedächtnis gut und so können Sie sich alle Kombinationen von Benutzernamen und Kennwort merken. Bis Sie dann eine Seite länger nicht mehr besucht haben und in der Folge genau deren Zugangsdaten vergessen haben. Wenn Sie keinen Passwort-Manager verwendet haben, dann ist guter Rat teuer. Es sei denn, Sie verwenden den neuen Edge-Browser. Der erlaubt nämlich den Export der darin gespeicherten Passwörter.



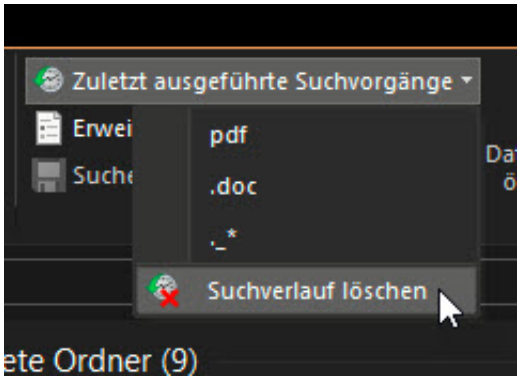
Klicken Sie auf die drei Punkte oben rechts am Bildschirm, dann auf **Einstellungen** > **Profile** > **Kennwörter** zeigt Edge Ihnen alle Webseiten an, auf denen Sie ein Passwort gespeichert haben. Ein Klick auf das Augen-Symbol rechts von einem Eintrag ändert die angezeigten Sternchen dann in das gespeicherte Passwort.

Um alle Passwörter in einer Excel-Tabelle zu erhalten, klicken Sie auf die drei Punkte neben **Gespeicherte Kennwörter** und wählen Sie dann **Kennwörter exportieren**. Vorsicht: Diese Excel-Tabelle in den Händen eines Unbefugten verursacht größtmöglichen Schaden: Darin stehen die Webseiten-URLs und die Kennwörter in Klarschrift!

Löschen der Suchhistorie im Explorer

Der Windows Explorer ist Ihr Tor zu den Dateien auf Ihrem PC. Das führt dazu, dass Sie ihn zum einen oft benutzen, zum anderen aber auch oft Suchen nach Dateien darin durchführen. Windows 10 speichert diese Suchen automatisch. Das ist hilfreich, gibt anderen Benutzern des PCs aber auch viele Informationen über Ihre Arbeit. Das können Sie aber unterbinden!

Eine Suche im Explorer starten Sie, wenn Sie den Suchbegriff in dem Eingabefeld rechts unter **Schnellsuche** eingeben. Sobald Sie das getan haben, wechselt der Explorer auf die Registerkarte **Suchtools**. Darin finden Sie unter anderem die **zuletzt ausgeführten Suchvorgänge**. Diese sind eine Historie der Suchen, die Sie bisher durchgeführt haben.



Um diese zu löschen, klicken Sie auf das nach unten zeigende Dreieck neben **Zuletzt ausgeführte Suchvorgänge** und dann auf **Suchverlauf löschen**. Die Liste der Suchbegriffe wird damit gelöscht und steht nicht mehr zur Verfügung. Damit werden aber natürlich keine Dateien auf einem der Datenträger gelöscht. Sie verlieren nur die Möglichkeit, bereits eingegebene Suchanfragen direkt wiederverwenden zu können.

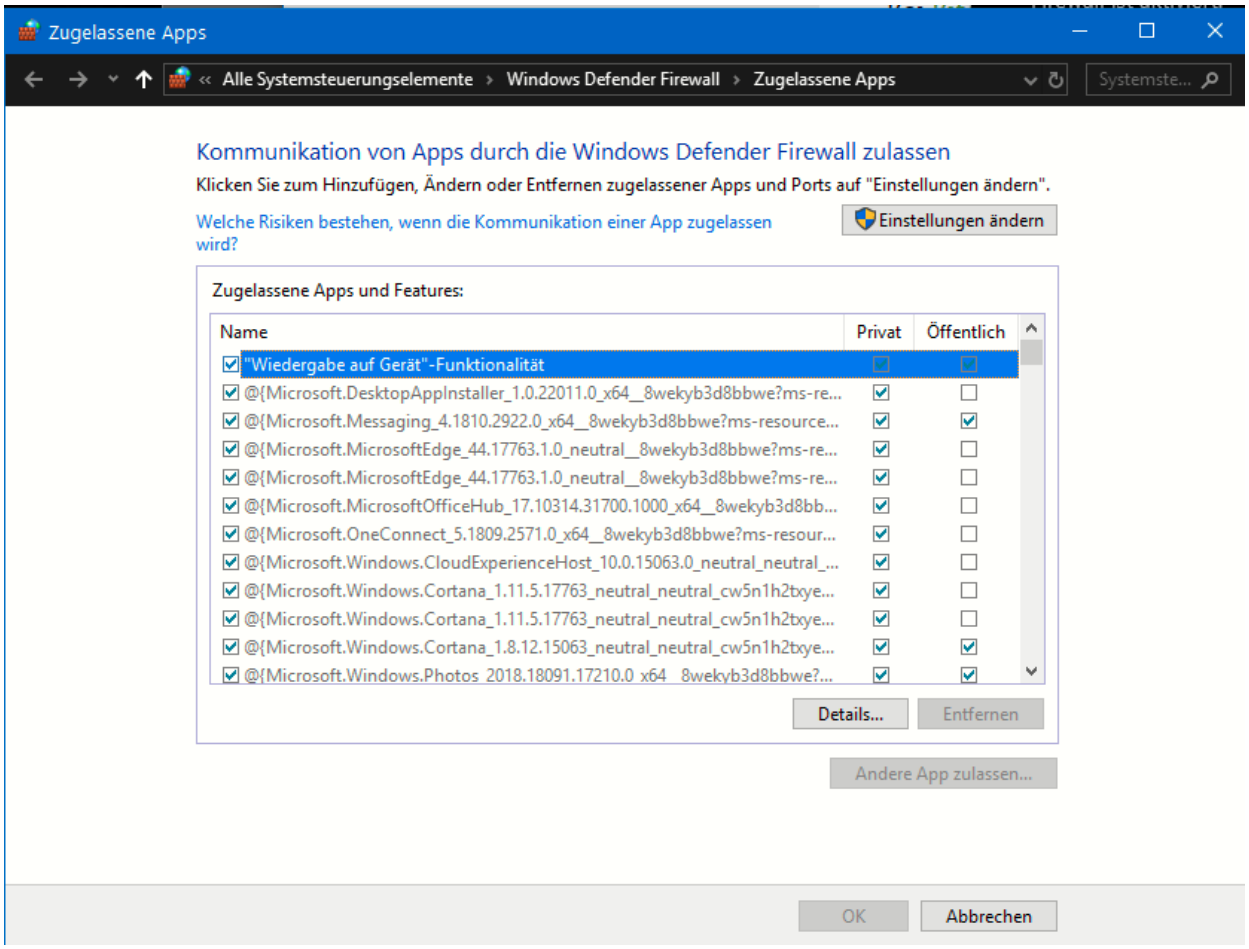
Konfigurieren einer Firewall

Eine Software-Firewall ist sinnvoll: Sie schützt sie vor ungewollten Datenübertragungen von oder auf Ihren Rechner. Die Funktionsweise ist ein wenig vergleichbar mit der eines Antivirenprogramms. Die Firewall erkennt Angriffsmuster, die verdächtig erscheinen. Den entsprechenden Datentransfer blockiert sie dann. Manchmal aber meint sie es zu gut. Wenn bestimmte Programme nicht mehr laufen, dann kontrollieren Sie die Firewalleinstellungen.

Windows 10 hat schon eine recht gute Firewall mit an Bord. Die Öffnen Sie, indem Sie in der Suchleiste **Firewall** ein geben und auf **Firewall- und Netzwerkschutz** klicken. Windows unterscheidet drei Arten von Netzwerken: **Domänennetzwerke** (die meist in Firmenumgebungen vorkommen), **Private Netzwerke** (das sind Netzwerke, bei denen Sie den Standort kennen und unter Kontrolle haben) und **Öffentliche Netzwerke**.

Für alle drei Netzwerktypen sollten Sie die Firewall aktivieren. Windows überprüft dann selbständig, ob eine App versucht, irgendwelche Verbindungen aufzubauen, die verdächtig sind. Das können Würmer sein, Viren, Hardwarekomponenten, die Daten irgendwo hinschicken. Nicht immer ist das ein Schädling, manchmal meldet die Firewall einen Einbruchsversuch, wenn ein echtes Programm seine Arbeit verrichten will. Solche „False Positives“ genannten Fehler können Sie selber korrigieren: Die Firewall meldet Ihnen jede blockierte Verbindung durch eine PopUp-Meldung auf dem Bildschirm Das führt dazu, dass die Verbindung erst einmal nicht zugelassen wird. Wenn Sie dann aber in die Firewalleinstellungen oben gehen und auf **Zugriff**

von App auf durch Firewall zulassen anklicken, dann zeigt Ihnen Windows 10 eine Liste der Apps an, die über die Firewall gehe. Hier können Sie für private wie öffentliche Netzwerke einzeln festlegen, ob die App die Verbindung aufbauen darf oder nicht.

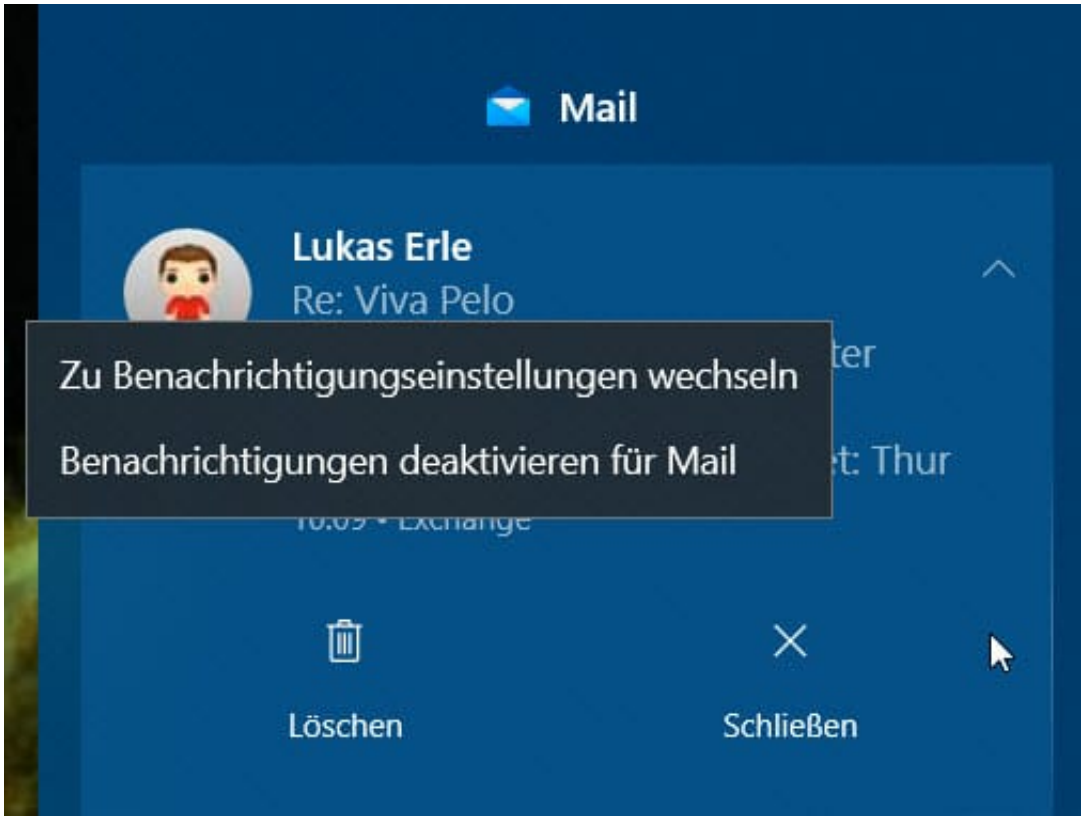


Aktivieren Sie die gerade noch blockierte App einfach, dann bauen Sie die Verbindung erneut auf. Schon sollte sie funktionieren. Findet sich die App, die Sie für die Firewall zulassen wollen, nicht in der Liste, dann können Sie sie manuell hinzufügen. Klicken Sie dazu auf die Schaltfläche **Andere App zulassen** und geben Sie deren Pfad auf der Festplatte an. Schon wird auch diese App nicht mehr blockiert!

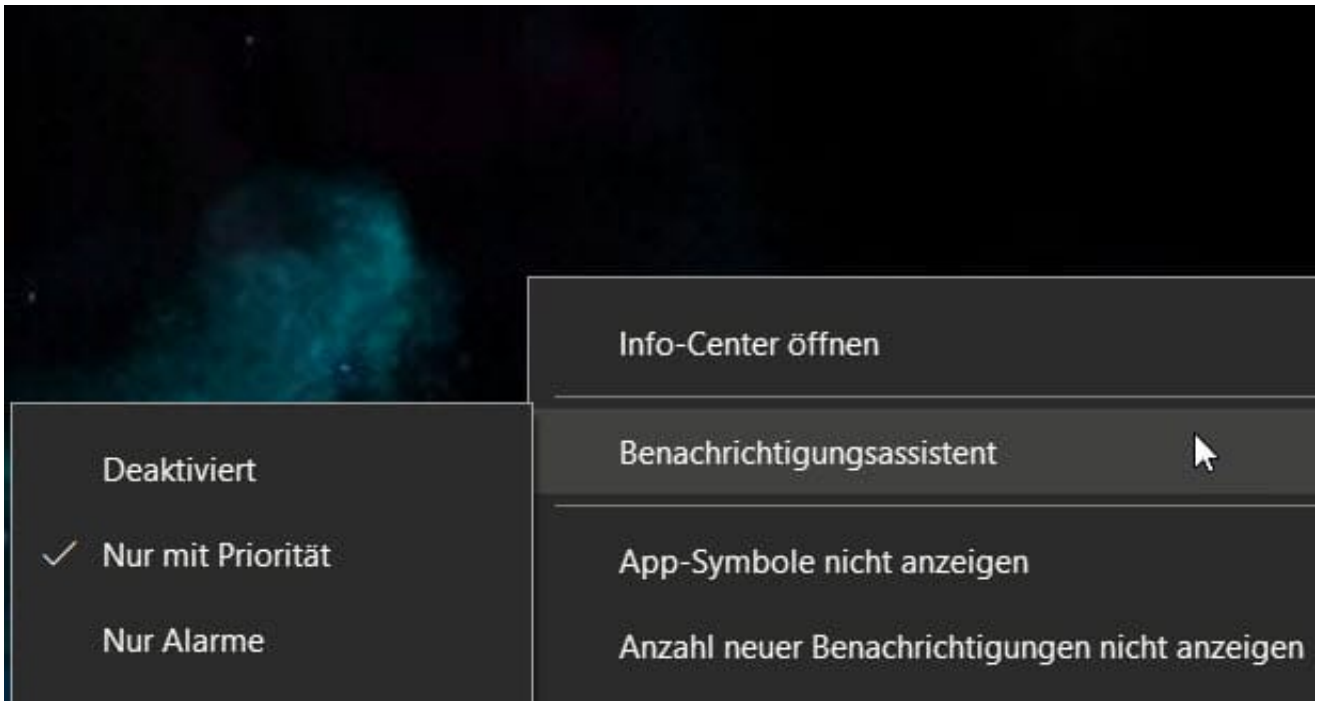
Windows-Benachrichtigungen steuern

Die Benachrichtigungen unter Windows 10 sind hilfreich und detailliert. Sobald eine E-Mail eingeht, ein Termin fällig wird oder neue Nachrichten des bevorzugten News-Dienstes verfügbar sind, werden diese direkt als kleine Nachricht im Info-Center angezeigt. Die Kehrseite: Je mehr Benachrichtigungen erfolgen, desto häufiger lassen Sie sich ablenken. Das geht auf Kosten der Produktivität. Hier einige kleine Tipps, wie Sie dem entgegenwirken können.

Die Nachrichtenblase am unteren, rechten Bildschirmrand ist der zentrale Zugang zum Info-Center. Klicken Sie mit der linken Maustaste darauf, dann öffnet sich die Seitenleiste mit allen Benachrichtigungen. Wenn Sie eine Benachrichtigung gar nicht sehen wollen, dann klicken Sie mit der linken Maustaste darauf Dann klicken Sie auf **Benachrichtigungen deaktivieren für . Die Benachrichtigungseinstelllungen, in denen Sie dann Einstellungen für alle Benachrichtigungen von Apps vornehmen können, erreichen Sie über den ersten Link in diesem Fenster.**



In Situationen, in denen Sie pauschal die Benachrichtigungen einschränken wollen: Klicken sie stattdessen mit der rechten Maustaste auf die Nachrichtenblase am unteren, rechten Bildschirmrand. Ein Klick auf Benachrichtigungsassistent öffnet denselben. Hier können Sie festlegen, wie die Benachrichtigungen einschränken können, Prioritäten für Apps und Kontakte setzen etc.


Info-Center öffnen
Benachrichtigungsassistent
App-Symbole nicht anzeigen
Anzahl neuer Benachrichtigungen nicht anzeigen
Deaktiviert
Nur mit Priorität
Nur Alarme