Schieb Report

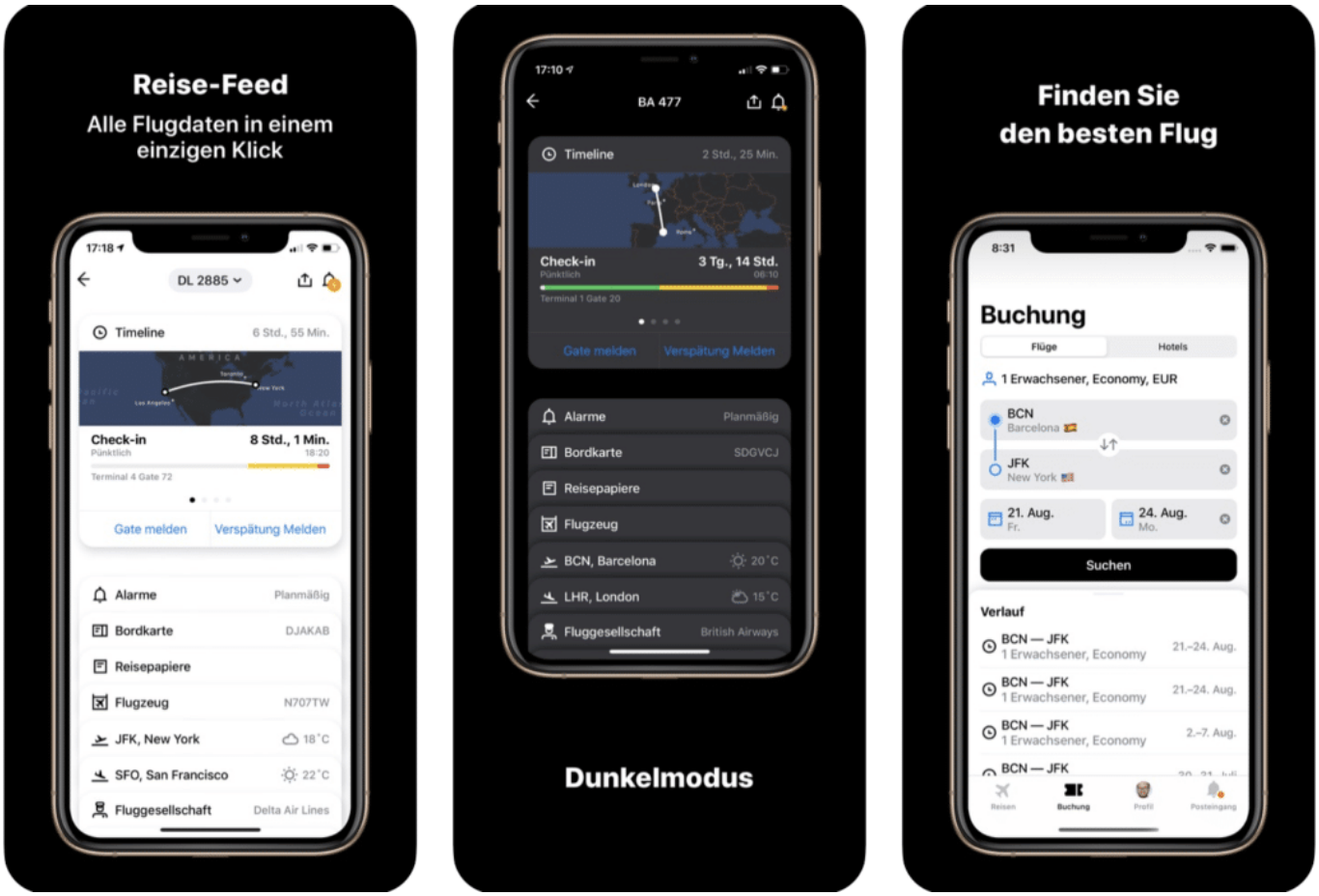
Ausgabe 2020.29

App in the air: Komfortabel Flüge im Blick behalten

In Corona-Zeiten wird nicht so viel geflogen - sonst aber schon. Und dann bekommt "App in the Air" ordentlich was zu tun. Die App hilft dabei, die eigenen Flüge zu überwachen - und einem während der Flüge beseite zu stehen. Eine App, nicht nur für die Reisezeit - aber auch.

App in the air
Von: AITA Limited
Kostenlos / InApp-Käufe für Premium
iPhone, iPad, Apple Watch

Vielflieger wissen Komfort zu schätzen – und brauchen stets Infos über den aktuellen Status der Flüge, Abflug-Gate, einzuplanende Wartezeiten an Sicherheitskontrollen und vieles mehr. Solche Infos liefert **App in the air**.



Die App versorgt den Nutzer mit allen wichtigen Daten der gebuchten Flüge – und checkt auf Wunsch sogar automatisch ein. Das leisten Apps der Fluggesellschaften auch. Doch App in the air bietet diesen Service für alle Airlines – in einer App. Das macht die Sache einfacher. Auf Wunsch importiert die App gebuchte Flüge aus Gmail – vollkommen automatisch.

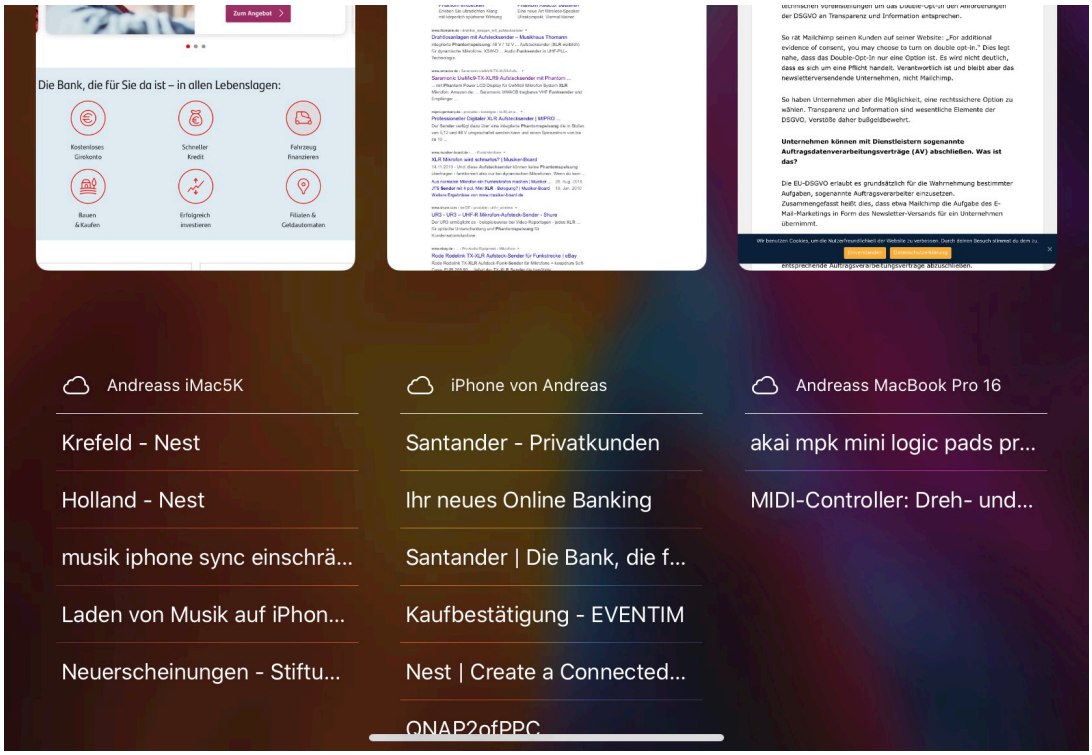
Praktisch sind Extras wie Navigationshilfen in Flughafengebäuden, Änderungsinfos per SMS

(also ohne Roaming und WLAN) und Flugprofile. Auch im Flug macht die App weiter: Es gibt Infos über aktuell überflogene Sehenswürdigkeiten oder Fitness-Übungen auf der Apple. Die Basisfunktion ist kostenlos. Wer auch komplett offline arbeiten und per SMS über Änderungen informiert werden möchte, braucht die Premium-Funktion (32,99 EUR im Jahr).

Webseiten teilen zwischen iOS-Geräten

Wenn Sie nicht nur mit einem Apple-Geräte arbeiten, sondern iPhone, iPad, MacBook und/oder iMac parallel benutzen, dann werden Sie auf all diesen Geräten immer mal wieder im Internet sein. Und dann passiert folgendes: Sie sind auf dem einen Gerät auf einer Webseite, legen es weg und denken irgendwann wieder daran. Nur haben Sie dann eines der anderen Geräte in der Hand und die Seite nicht zur Verfügung. Das ist bei iOS überhaupt kein Problem!

Vorab: Nicht nur für diese Anwendung empfiehlt es sich, die iCloud-Synchonisation einzuschalten. Dann können Sie nämlich folgende tolle Funktion nutzen: Alle Tabs, die Sie auf einem der Geräte offen haben, werden in die iCloud synchronisiert. Sie sind damit auf allen Geräten verfügbar, die das selbe Konto nutzen.

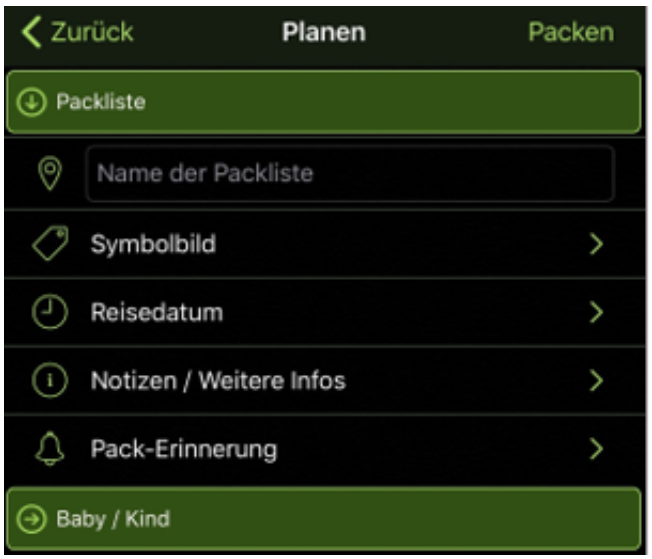


Für die Tabs in Safari öffnen Sie die App Safari, dann tippen Sie auf das Symbol mit den übereinander liegenden Seiten, das zu den geöffneten Tabs führt. Unter den auf dem aktuellen Gerät geöffneten Tabs sehen Sie die auf den anderen Geräten geöffneten Tabs. Tippen Sie einen Eintrag an, dann öffnet Safari die Seite.

Erstellen einer Packliste: Pack The Bag

Wenn einer eine Reise macht… dann vergisst er garantiert die Hälfte. Kennen Sie das? Sie haben an alles gedacht, aber unterwegs fällt Ihnen dann immer wieder etwas ein, das fehlt. Oder die Packliste ist nicht mehr auffindbar, wenn Sie die Koffer packen wollen. Das muss nicht sein: Pack the Bag ist eine tolle Hilfe, um (nahezu) alles mit dabei zu haben.

Dabei können Sie auf eine große Menge von thematisch vorbereiteten Gegenständen zugreifen. Alles rund ums Baby finden Sie unter *Baby/Kind*, die Dinge für den Hund unter *Haustier* und so weiter. Damit klicken sie sich im Handumdrehen Ihre Packliste zusammen und können diese dann später durch ein Tippen auf **Packen** abarbeiten.



Wenn Sie regelmäßig dieselben Sachen packen, dann investieren Sie einfach ein wenig mehr Aufwand: Legen Sie sich Ihre eigenen Gegenstände in der App ab und pflegen Sie auch das Gewicht. So haben Sie schnell im Blick, was Sie normalerweise einpacken und haben gleichzeitig dien Füllgrad und das Gewicht Ihres Koffers im Blick. Vorbei ist die Zeit, in der Sie am Flughafen panisch Koffer umpacken mussten, um teures Zusatzgebühren zu vermeiden.

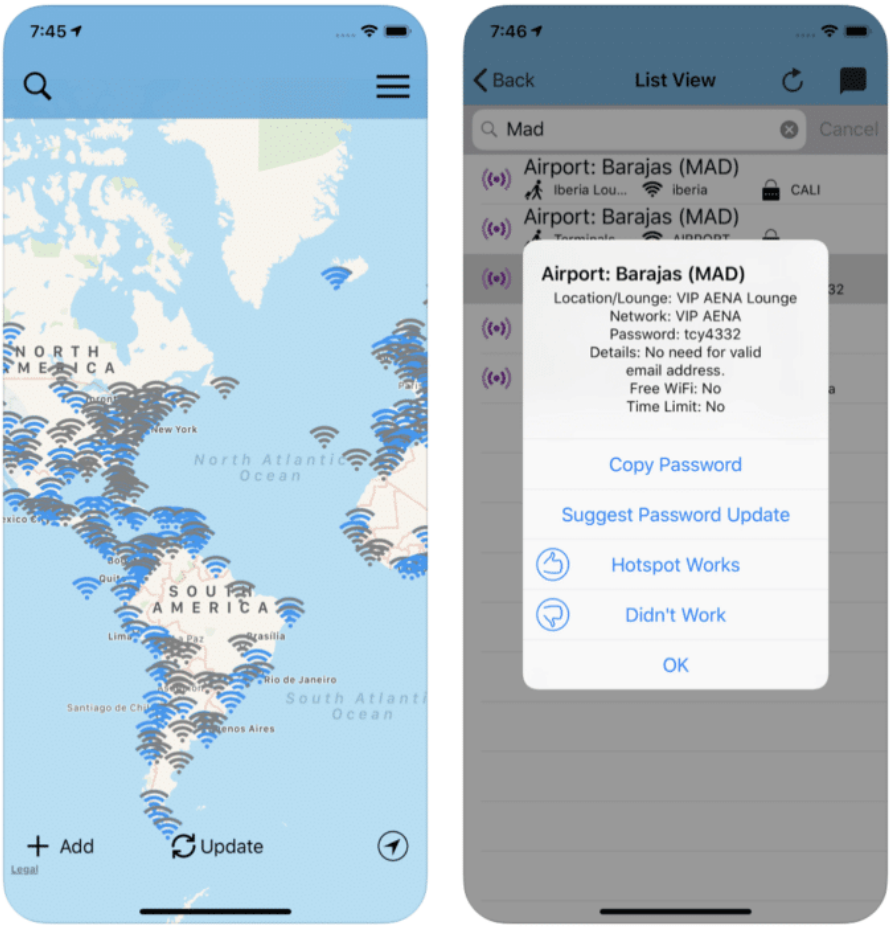
Natürlich können Sie aus jeder bereits abgearbeiteten Packliste wieder eine neue erstellen oder diese überarbeiten.

Pack the Bag gibt es kostenlos für iOS.

WiFox: Die App kennt die Passwörter für fast alle Flughafen-WLANs

Wer am Flughafen sitzt und sich in ein WLAN einloggen will, braucht manchmal Zugangsdaten - denn nicht alle WLANs sind offen und ohne Passwort zu erreichen. Das gilt vor allem für WLAN-Netzwerke aus Loungen oder speziellen Bereichen. Die App WiFox hilft weiter.

Nach Corona wird bestimmt wieder mehr geflogen. Und dann sitzen wir wieder am Flughafen, wollen ins kostenlose WLAN – und kennen die Zugangsdaten nicht. Klar, irgendwo stehen die oder man kann sie erfragen. Einfacher und schneller geht es, wenn die Zugangsdaten bereits bekannt sind.



Hier hilft **WiFox** weiter. Die praktische App kennt die Zugangsdaten und Passwörter von nahezu allen Flughäfen. Einfach in der Weltkarte den Flughafen auswählen (Daten sind offline verfpgbar!), schon erscheinen die zur Verfügung stehenden WLAN-Netzwerke. Auch die von Loungen, zu denen nur bestimmte Personen Zutritt haben. Doch die Funknetzwerke lassen sich oft auch außerhalb der Lounge erreichen.

Das WLAN wählen, das man gerade sieht – schon zeigt WiFox das Passwort, sofern nötig. Das lässt sich schnell und bequem per Tippen in die Zwischenablage übernehmen und so

übernehmen. Die App kostet 2,29 EUR und ist kostenlosen Apps in Sachen Bedienkomfort und Umfang überlegen.

Speicherplatz sparen bei Fotos auf dem Mac

iOS und macOS haben viele Dinge über die Integration von iCloud standardisiert. Dokumente, Lesezeichen, geöffnete Tabs sind auf allen Geräten mit der selben Apple ID gleichzeitig verfügbar. Die Foto-Bibliothek funktioniert ähnlich: Wenn Sie iCloud nutzen, dann können Sie die neuen Bilder hochladen und die komplette Bibliothek auf jedes Gerät heruntersynchronisieren. Was aber, wenn dafür kein Platz vorhanden ist?

Gerade bei MacBooks, bei denen der Speicher in den Einsteigermodellen arg limitiert ist, kann das zur Herausforderung werden. 128 oder 256GB lassen keinen Platz um eine umfangreiche Bildersammlung zu beherbergen. Das hat allerdings auch Apple erkannt: Sie können im System aktivieren, dass der Speicher optimiert wird.

Dazu gehen Sie in die Einstellungen von macOS und klicken dann auf Ihr Kontobild. Klicken Sie dann auf **iCloud**. Aktivieren Sie **iCloud-Fotos**. Wenn sie genügend Platz haben, dann wählen Sie **Originale auf den Mac laden**. Wenn nicht, dann aktivieren Sie stattdessen **Mac-Speicher optimieren**. macOS ersetzt dann die großen Bilder durch kleine Platzhalter, wen der Platz auf der Festplatte/SSD eng wird. Zoomen sie in ein Bild hinein, dann lädt macOS das große Bild automatisch aus iCloud nach.

Geht 5G auch ohne Huawei? Bestimmt!

Während Großbritannien auf Druck der USA den chinesischen Hersteller Huawei als Ausstatter der 5G-Infrastruktur ausgeschlossen hat, hält sich die Bundesregierung alles offen. Das Problem: Die europäischen Hersteller wurden nicht ausreichend gefördert. Nun ist das Problem da.

Das 5G-Netzwerk kommt. Für uns Verbraucher bedeutet das erst mal: Deutlich schnellere Datenübertragung. Aber auch nur, wenn wir früher oder später ein neues Smartphone-Modell kaufen, das auch 5G kann.

Nahezu alle bisher verkauften Geräte können nämlich kein 5G. Das zeigt schon: Es ist neue Technologie nötig, um den schnelleren Mobilfunkstandard nutzen zu können.

Huawei ist weltweiter Marktführer

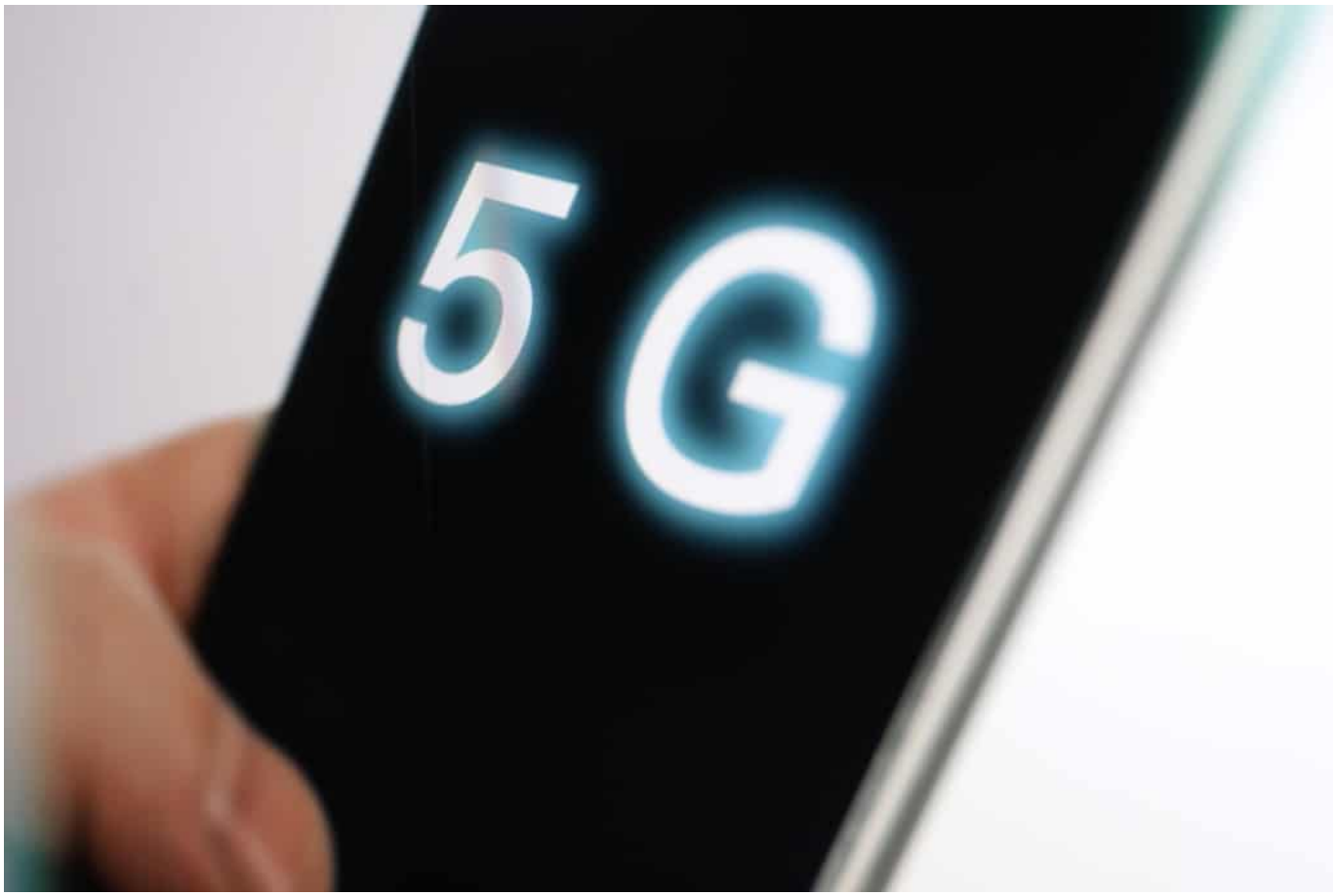
Das gilt auch und besonders für die Apparatur "hinter den Kulissen": Damit ein Mobilfunknetzwerk funktioniert, ist jede Menge moderne Technologie erforderlich.

Marktführer bei 5G ist der chinesische Hersteller Huawei. Ginge es nur darum, die beste Technologie zu verbauen, wäre die Wahl einfach: Huawei.

Spionage und Sabotage denkbar

Aber die Welt ist kompliziert(er). Huawei ist ein chinesischer Hersteller. Es ist allgemein bekannt und weitgehend unbestritten, dass chinesische Regierung und chinesische Wirtschaft alles andere als entkoppelt sind. Wenn die chinesische Regierung etwas will, dann passiert es auch.

Das macht zum Beispiel Spionage und Sabotage denkbar. Wie einfach wäre es, ein fremdes Land damit unter Druck zu setzen, dass ein einmal etabliertes Mobilfunknetz - bildlich gesprochen! - per Knopfdruck in Peking lahmgelegt werden könnte.



Daten rund um die Uhr abschöpfen

Schlimmer noch wäre unbemerkte Spionage. Als Laie kann man sich das nicht so einfach vorstellen. Aber es ist kaum möglich, so etwas mit 100%iger Sicherheit auszuschließen.

Niemand kann wirklich in die Geräte und vor allem Software reinschauen, die dann - im 5G-Netzwerk verbaut - rund um die Uhr Daten verarbeiten. Und womöglich unbemerkt interessante Daten abschöpft.

Aggressive Wirtschafts- und Außenpolitik

Chinas aggressive Wirtschafts- und Außenpolitik sprechen eine deutliche Sprache. Das Risiko der Spionage und Sabotage zu ignorieren, wäre fahrlässig. Das Risiko ist meiner Ansicht nach sehr real.

Großbritannien hat jetzt beschlossen: Huawei fliegt raus bei 5G. Das, was schon verbaut wurde, wird in den nächsten sieben Jahren ersetzt.

In den USA wettert Donald Trump seit Jahren gegen Huawei. Dort ist das Verbauen von Huawei mittlerweile aber wieder erlaubt.

Gleichzeitig gibt die USA Geld aus, damit in Brasilien keine Technologie von Huawei zum

Einsatz kommt. Die USA spielen alles andere als fair und konsequent.

EU muss eigene Technologie voranbringen

Was bleibt, ist ein enormes Risiko - und Problem. Das Dilemma haben wir dem Versagen der Politik zu verdanken. In Deutschland, in der EU. Sie sollte weniger von Digitalisierung reden, sondern mehr unternehmen.

In Nokia und Ericsson hatten wir Weltmarktführer für solche Technologie in Europa. Heute nicht mehr.

Der Digitalbereich muss besser politisch gefördert und begleitet werden. Es braucht auch hier mehr Unabhängigkeit - nicht nur von China, auch und vor allem von den USA.

Amazon und seine Algorithmen: Wissen ist Macht

Wer oder was Amazon ist, das müssen wir sicher niemandem erklären. Jeder kennt Amazon – als größtes Online-Warenhaus der Welt. Zwar ist Amazon längst sehr viel mehr als das. Aber eins lässt sich sagen: Das Unternehmen ist vor allem durch seine Algorithmen groß geworden. "Kunden, die das gekauft haben, die haben auch jenes gekauft". Das ist eine Erfindung von Amazon – auch wenn das heute viele nachmachen. Was aber steckt genau dahinter? Was kann Amazon sonst noch so alles?

Wie hat es Amazon geschafft, der größte Onlineshop der Welt zu werden?

Nicht mit niedrigen Preisen oder besonderem Service, sondern: Indem Amazon von Anfang an versucht hat, möglichst viel über die Käufer in Erfahrung zu bringen. Was interessiert sie? Was schauen sie sich an – und was kaufen sie?

Welche Produkte werden zusammen in einen Warenkorb gelegt? Jeff Bezos Unternehmen war das erste, das das Potenzial einer genauen Analyse erkannt und gnadenlos in Algorithmen umgesetzt hat. "Das könnte Ihnen auch gefallen" – basierend auf das eigene Einkaufsverhalten.

Das hat es vorher nicht gegeben und hat das Einkaufverhalten verändert. Hinzu kommen E-Mails mit Empfehlungen, die ebenfalls zum Kauf anregen. Amazon kennt seine Kunde bis ins Detail.

Auch interessant für Amazon: Bewerten und Rezensieren

Auch das Bewerten und Rezensieren gekaufter Artikel war eine Erfindung von Amazon, auch wenn wir das heute überall sehen.

Das spielt eine immense Rolle. Denn zum einen lieben wir es als Kunden, Rezensionen zu lesen und Bewertungen zu erfahren. Das beeinflusst unser Einkaufsverhalten enorm. Natürlich, das kann auch missbraucht werden, indem falsche Bewertungen eingestellt werden. Aber prinzipiell ist das ein guter Mechanismus.

Auch hier saugt Amazon aber jede Menge Informationen heraus – und kann die Kundschaft perfekt scannen und einschätzen. Wenn Google es geschafft hat, eine Netz-User perfekt zu kennen, um ihn oder ihr perfekt passende Werbung zu präsentieren, so hat es Amazon geschafft, im Onlineshop alles zu optimieren.

Wir sehen das, was uns interessiert. Amazon kennt uns so gut, dass es sogar ein Patent darauf hat, Ware schon bereitzustellen und zu verpacken, bevor wir selbst bestellt haben. Das sollten wir nicht unterschätzen: Amazon kennt uns nicht nur, sondern manipuliert uns auch.

Immer für den eigenen Vorteil: Was gut läuft, wird selbst hergestellt

Es gibt durchaus auch Kritik am intensiven Einsatz von Algorithmen bei Amazon. Mitunter werden Händler ausspioniert – und ausgebootet.

Amazon weiß ganz genau, was gut läuft. Was die Leute zum Beispiel bereit sind, für eine Tube Zahnpasta auszugeben, für eine Yoga-Matte oder einen Fernseher. Kann man schließlich alles bei Amazon kaufen. Heute ist Amazon nicht nur ein Onlineshop, sondern auch der größte **Marktplatz**. Wer Waren verkaufen will, muss hier fast zwangsweise vertreten sein, weil viele Menschen Amazon als Suchmaschine für Kaufprodukte sehen und verstehen.

Dadurch hat Amazon eine enorme Macht – basierend auf Daten. Die Händler müssen Provisionen für alles bezahlen: Wenn ein Kauf getätigt wird, wenn Amazon eine Zahlung bearbeitet, wenn Amazon Waren im Lager hält etc.

Aber Amazon geht sogar hin, und stellt immer wieder von besonders gut laufenden Produkten Eigenmarken her. Etwa Batterien oder Akkus. Handtücher. Geschirr. Messer. Körbchen für den Hund. Erst mal wartet Amazon, welche Waren gut laufen – und stellt sie dann unter eigener Marke selbst her, verdrängt die anderen Hersteller und verdient noch mehr.

Amazon ist ein Hai – verschluckt alle und jeden, ohne mit der Wimper zu zucken.

Amazon saugt auch aus anderen Quellen Daten - etwa Alexa

Amazon ist ein Meister darin, Daten zu sammeln und für sich und seinen unternehmerischen Erfolg zu nutzen. Amazon sammelt aber nicht nur Daten, wenn wir im Online-Store stöbern oder einkaufen.

Im Grunde immer, wenn wir mit Amazon in Verbindung stehen – und einen der vielen Dienste von Amazon nutzen. Bestes Beispiel ist zweifellos Alexa. Der Sprach-Assistent ist ein Eldorado für einen Datensammler wie Amazon.

Wer Alexa(s) zu Hause stehen hat, spricht mit dem Assistenten. So erfährt Amazon zum

Beispiel, wann ich zu Hause bin – auch wann ich zu Hause bin. Amazon erfährt auch, worüber ich mich im Web informiere, zumindest wenn ich Alexa befrage. Wann ich zur Arbeite starte. Wann ich mich wecken lassen. Welche Personen sonst noch zu Hause sind.

Sofern ich andere Geräte damit steuere, wann ich fernsehe und was, wann ich die Lampe dimme, die Türe verriegele – oder welche Musik ich höre. Das wiederum lässt nicht nur generell ein Profil über mich zu, sondern auch im Speziellen: Heute Kuschel-Rock, morgen Baladen – das sagt etwas über meine Stimmung aus.

Amazon hat sogar ein Patent darauf, zu erkennen, in welchem Gefühlsmodus ich befinde, allein anhand meiner Stimme. Es ist erschreckend. Wir wissen nicht, welche Daten konkret alle zum Einsatz kommen. Es sind viele.

Nachfragen: Welche Daten sammelt Amazon wirklich?

Wiele fragen sich: Lässt sich rausbekommen, welche Daten ein Konzern wie Amazon sammelt?

Theoretisch schon. Denn Amazon muss, wie jedes anderes Unternehmen auch, auf Nachfrage alle Daten rausrücken. Macht der Konzern aber nicht. Die Datenschützerin Katharina Nocun hat sich damit intensiv beschäftigt und musste mit Datenbehörden drohen, bevor Amazon überhaupt mal nennenswertes Material herausgerückt hat.

Da sieht man dann zum Beispiel den „Click Stream“: Amazon registriert ganz genau, wonach ich suche, auch wann, welche Bilder ich mir in groß anschaue, wie lange ich auf einer Produktseite verbleibe, ob ich etwas in den Warenkorb stecke oder auch wieder entferne. Das sind alles abenteuerlich konkrete Daten, die man im Zweifel nicht mal selbst über sich weiß.

Und wer viele Daten hat, kann gut vergleichen mit anderen Usern und so Schlüsse ziehen und ein Profil erstellen. Auch welche Musik ich mir bei Amazon anhöre, welche Serien ich schaue, ob ich mir eine Szene doppelt und dreifach anschaue oder schnell vorspule – wird alles registriert und in Informationen umgewandelt. Selbst Rückschlüsse auf das Schlafverhalten sind möglich...

Geld verdienen mit Cloud-Diensten

Was die meisten gar nicht wissen: Amazon ist auch ein Cloud-Dienst, ein sehr großer sogar.

Amazons Stärke sind seine Rechenzentren. Die sind ausfallsicher, super schneller, über die ganze Welt verteilt. Das hat Amazon zu einem Business gemacht. Nicht für uns Privat-User, aber für Firmen, Startups: Anstatt selbst ein Rechenzentrum aufzubauen, mietet man bei Amazon Server und Funktionen: Ob Datenbank, Web-Server, Speicherplatz, Gesichtserkennung, Sprachanalyse, was auch immer: Es gibt alles.

Viele Startups mieten diese Ressourcen bei Amazon – und zahlen dafür. Wenn sie wachsen, buchen sie einfach größere Dimensionen der Ressourcen bei Amazon. Deshalb sind auch viele Start-Ups von Amazon abhängig: Fallen deren Server aus oder gibt es in der Infrastruktur von Amazon Probleme, gibt es plötzlich viele Probleme in diversen Apps und Online-Anwendungen gleichzeitig. Die Abhängigkeit von Amazon ist riesig: Bei Verlagen, Industrie, Händlern und sogar Online-Unternehmen.

Siebter Himmel für Stalker: PimEyes ist ein Staubsauger für Fotos

Vor einigen Monaten ist das US-Unternehmen Clearvia AI damit aufgefallen, mehrere Milliarden Fotos und Personen aus dem Netz gezogen zu haben. Behörden konnten darüber nach Personen suchen. Jetzt gibt es einen ähnlichen Fall in Europa. Unterschied: Bei PimEye kann jeder die Datenbank durchforsten.

Warum lächeln wir eigentlich noch, wenn wir fotografiert werden? Die Chance, dass eine Aufnahme mit uns im Bild irgendwo in den diversen Sozialen Netzwerken auftaucht und zur Bereicherung derselben beiträgt, ist extrem hoch.

Das Risiko für Missbrauch ebenfalls, wie der aktuelle Fall PimEyes aus Polen zeigt: Wer das Angebot von PimEyes aufsucht, kann ein Porträtfoto hochladen und nach anderen Fotos dieser Person suchen. Sekunden später erscheinen die Treffer...

PimEyes geht weit über Google hinaus

Das geht weit über die Bilder-Suchfunktion von Google hinaus. Denn PimEyes "saugt" im großen Stil Fotos aus allen nur denkbaren Quellen, vor allem aus dem Web und Plattformen wie Facebook, Instagram, Twitter und Youtube.

(Noch) erscheinen nicht Name und Wohnort auf dem Bildschirm, sondern es werden "nur" Quellen präsentiert, die ein Bild mit der Person zeigen. Aber das reicht meist schon, um innerhalb weniger Sekunden herauszufinden, um wen es sich handelt.

Anonymität wird abgeschafft

Die Datenschutzexperten von netzpolitik.org haben sich das genau angeschaut - und kommen zum Schluss: Die polnische Firma schafft gerade unsere Anonymität ab. Rund 900 Milionen Aufnahmen sollen laut PR-Texten von PimEyes bereits in den Datenbanken gespeichert sein.

Ein ähnlicher Datenskandal wie Anfang des Jahres bei Clearwiew AI. Da hat ein US-Unternehmen das Netz abgegrast, eine Gesichtserkennung darübergelegt und den Service unter anderem an die Polizei verkauft.

Mit der DSGVO wohl kaum vereinbar

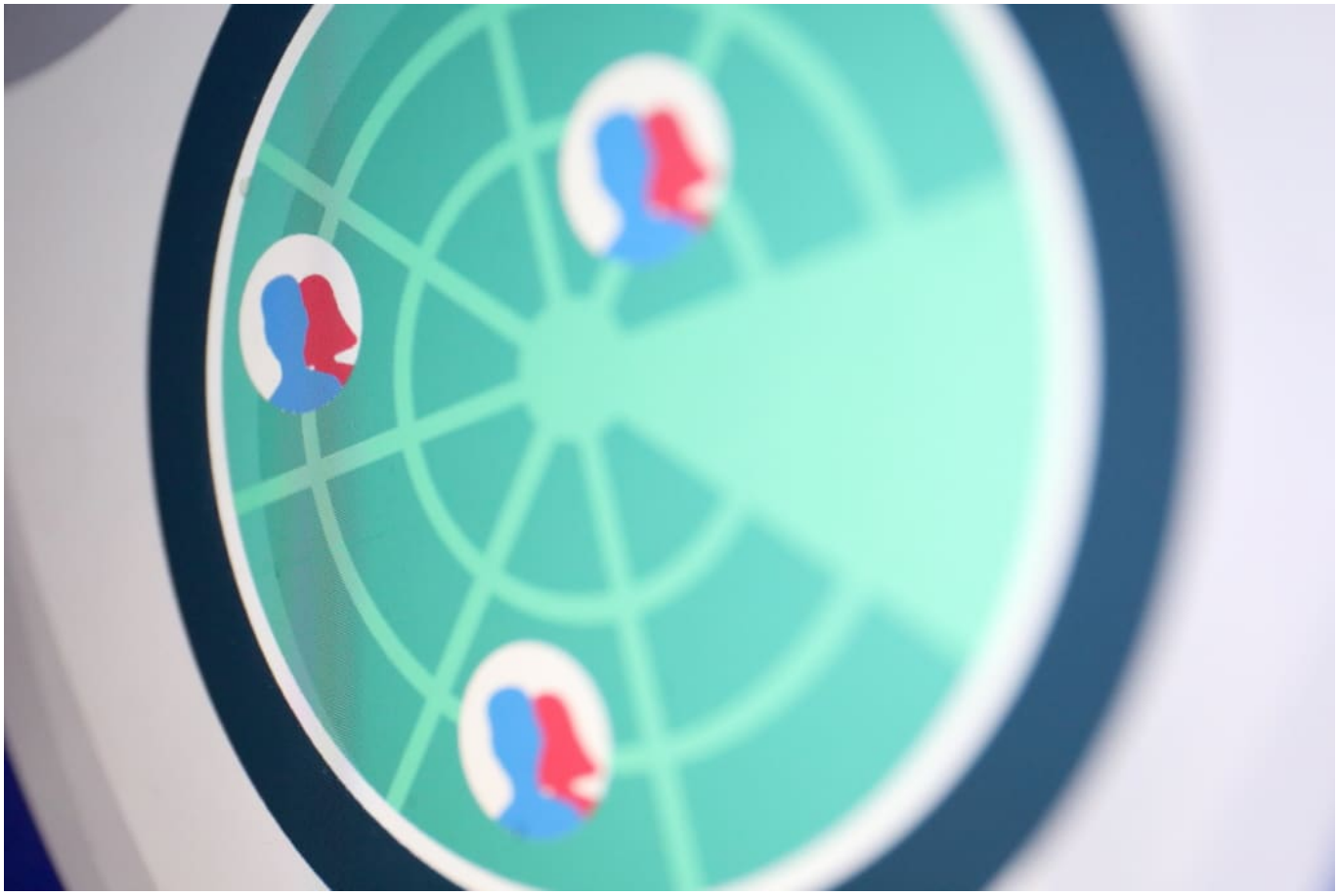
Doch PimEyes sitzt in Polen. In der EU! Unvorstellbar, dass es mit der DSGVO vereinbar ist, hunderte Millionen Fotos aus dem Netz zu ziehen, miteinander zu verbinden und eine Gesichtserkennung darüber laufen zu lassen - für die Allgemeinheit!

Anders als Clearview AI bietet PimEyes diesen Service nämlich jedem an. Der siebte Himmel für Stalker: Foto machen - und PimEyes verrät, wer er oder sie ist. Herzlichen Glückwunsch!

Wo sind Algorithmen, die das verhindern?

Laut Recherchen von netzpolitik.org hat PimEyes nachjustiert, einige Formulierungen und auch Verfahrensweisen geändert. So kann man derzeit - zumindest offiziell - nur noch eine Webcam-Bild hochladen. Angeblich, damit man herausfindet, auf welchen Webseiten und Fotos man selbst zu sehen ist und auftaucht. Nur: Das ist kein Geschäftsmodell - das kauft dem Unternehmen doch niemand ab, dass es darum geht.

Markus Beckedahl von netzpolitik.org fragt völlig zu Recht: Wieso ist es eigentlich möglich, dass Facebook, Twitter, Instagram und Co. hunderte von Millionen Fotos "herausgeben"? Warum lassen sie es zu, dass einzelne Unternehmen zig Millionen Fotos "ziehen", also laden? Es müsste doch Algorithmen geben, die das erkennen - und wirksam verhindern?



Verantwortung liegt bei Plattformen

Hier liegt ganz klar auch eine Verantwortung bei den Plattformen. Auch sollte es möglich sein, dass Fotos sich automatisch auflösen nach einer Weile. Und dass sie ausschließlich im jeweiligen Netzwerk angeschaut werden dürfen.

Aber ganz klar muss auch die Politik reagieren: Niemand sollte im großen Stil Daten absaugen dürfen. Unter gar keinen Umständen.

Mögliche Diskriminierung in Algorithmen

Seit dem Tod von George Floyd gibt es eine verstärkte Debatte für Diskriminierung und Rassismus. Es werden offensichtliche Fälle von Diskriminierung angesprochen und kritisiert, ebenso die Rassismus-Frage gestellt. Aber das nicht nur da, wo es jedem einleuchtet, sondern auch in Bereichen, die vielleicht überraschen. Zum Beispiel in der Digitalisierung. Auch da gibt es Diskriminierung – ja auch Rassismus. Denn auch Algorithmen sind nicht immer objektiv und gerecht.

Computer können super schnell rechnen? Stimmt. Computer haben keine Gefühle? Stimmt auch. Computer irren sich nicht? Doch, durchaus. Es gibt Fehler. Sicherheitslecks. Und objektiv sind Computer schon mal gar nicht. Denn Algorithmen tun das, wozu sie programmiert wurden. Und können daher durchaus auch diskriminieren.

Wir programmieren, Computer führen aus

Algorithmen, also Computerprogramme, sind nur so neutral, wie es die Programmierer vorgesehen haben.

Wer nur seine eigene Lebenswirklichkeit sieht und an den Computer weitergibt, will nicht zwingend diskriminieren oder hat sogar rassistische Motive, sondern denkt womöglich nicht weit genug – und erzeugt so einen Algorithmus, der diskriminiert.

Zeigt man einer Künstlichen Intelligenz zum Beispiel ausschließlich Fotos von schwarzen Katzen und weißen Hunden, dann „denkt“ der Algorithmus: Alle Katzen sind schwarz. Alle Hunde weiß. Ein schwarzer Hund wird von der KI dann womöglich für eine Katze gehalten, wegen seiner Fellbarbe.

Fatale Konsequenzen möglich

Solche unzureichenden Trainings können fatal sein. So wurde in selbstfahrenden Autos festgestellt, dass die auf hellhäutige Passanten tadellos reagierten. Dunkelhäutige Passanten aber wurden deutlich schlechter erkannt. Was ein erhöhtes Unfallrisiko mit sich bringt. Grund: Die Systeme wurden vor allem mit hellhäutigen Menschen trainiert.

Die Informatikerin Joy Buolamwini zeigt auf einer öffentlichen Veranstaltung, dass ihr Gesicht bei diversen Projekten, die sich mit Gesichtserkennung beschäftigen, gar nicht oder nicht richtig erkannt wird. Sie muss sich eine weiße Maske aufziehen, damit es funktioniert. Die Folge eines sogenannten „Bias“. Einer falschen Vorgehensweise.

Leider kein Einzelfall. Aber ist es diskriminierend oder sogar rassistisch, wenn Systeme derart schlecht programmiert sind – oder eher Nachlässigkeit?

Auch ungewollte Diskriminierung ist diskriminierend

Die Spanierin Lorena Jaume-Palasi, die sowohl die spanische Regierung wie die EU in Sachen Künstliche Intelligenz berät, sagt: Diskriminierung und Rassismus hat nichts mit Vorsatz oder Willen zu tun.

Lorena: "Wenn wir zum Beispiel Kiosken an Flughäfen bauen, die Weiße sehr gut erkennen, biometrisch erkennen und damit durchgehen lassen, aber Leute mit asiatischen Zügen schlechter erkennen können und diese damit länger in der Schlange stehen müssen, dann haben wir im Grund ein Speed-Boarding für Weiße kreiert. Und natürlich war das keine Absicht. Aber das ist der Effekt. Und selbstverständlich ist dieser Effekt rassistisch – und darauf kommt es an.“

So eine ungewollte Diskriminierung kann zu ganz konkreten Nachteilen führen: Bestimmte Personengruppen bekommen keinen Kredit, werden öfter von der Polizei kontrolliert oder angehalten, das ein oder andere Geschlecht hat schlechtere Chancen bei Bewerbungen...

Das fällt nur auf, wenn wir genauer hinschauen. Die Algorithmen auf mögliche Diskriminierung abklopfen.

Lösungsansätze: Buntere Teams

Es gibt viele Ansätze bzw. viele Sachen, die man machen kann. Man sollte die Teams diverser gestalten. Leute aus verschiedenen aus verschiedener Herkunft, aus verschiedenen Religionen und auch verschiedene Geschlechtern zusammenstellen. Und damit ist die Wahrscheinlichkeit, dass man etwas übersieht, deutlich geringer.

Also: Teams von Programmierern und KI-Systemen möglichst divers besetzen. Dann fallen Denkfehler schneller auf.

Selbst Experten sehen es Algorithmen nicht an, nach welchen Kriterien sie entscheiden – denn vor allem Künstliche Intelligenz besteht nicht aus Programmcode, sondern aus Erfahrungen. Es

muss also genau geprüft werden: Was wurde da eigentlich trainiert – und deckt das alle ab, ist das fair?

Höhere Sensibilität nötig

Nur selten werden Algorithmen oder Systeme ganz bewusst so programmiert, dass sie diskriminieren oder rassistisch sind. Algorithmen lernen von uns.

Wenn wir uns die Algorithmen oder die KI-Systeme näher anschauen und Probleme entdecken, gibt es dafür immer einen Grund in der Realität. In unserer Welt.

Algorithmen können uns also durchaus auch helfen, weil sie wie ein Brennglas funktionieren, Missstände zu entdecken. Und sie dann zu beseitigen. In der Gesellschaft. In der Art, wie wir leben.

Darf man das noch sagen: White Hat und Black Hat?

Die aktuelle Debatte über Diskriminierung und Rassismus reicht bis in die IT-Technologie. Auch hier gibt es Begriffe, an denen sich manche stören - oder die zumindest diskussionswürdig sein könnten.

Googles Sicherheitschef für Android David Kleidermacher hat gerade erst seinen Auftritt bei der bedeutenden Securitykonferenz "Black Hat" abgesagt. Seine Begründung auf Twitter: "Black Hat" wirke auf ihn diskriminierend.

https://twitter.com/DaveKSecure/status/1279194357116006400

Black and White: Guter Hacker, böser Hacker

"Black Hat": Ein Terminus für Insider. Hacker werden unterteilt in die Gruppe der "Black Hat" (schwarze Hüte) und "White Hat" (weiße Hüte). Die "White Hat" bewegen sich innerhalb von Gesetzen und Hackerethik, sie nutzen ihre Fähigkeite konstruktiv. Während die "Black Hat" ihre Fähigkeiten außerhalb des gesetzlichen Rahmens einsetzen - vor allem zum eigenen Vorteil, etwa um Daten zu kopieren, sich zu bereichern oder zu spionieren.

Nun flammt eine Diskussion darüber auf, ob diese Begriffe noch verwendet werden dürfen. Da "weiß" für gut steht und "schwarz" für schlecht. Es gibt noch andere Beispiele dafür, etwa "Blacklist" und "Whitelist": Auf einer "Blacklist" stehen etwa Mail-Adressen, die geblockt werden sollen, da schlecht/schädlich. Auf einer "Whitelist" hingegen Datensätze, die ausdrücklich willkommen sind.

Die Diskussion kann man führen - allerdings erscheint sie mir persönlich übertrieben. Denn "schwarz" und "weiß" werden hier nicht im Entferntesten mit der Hautfarbe von Menschen oder Kulturen verbunden. Sondern sie fußen auf alten Traditionen, die eher mit hell (Tag) und dunkel (Nacht) zu tun haben.

Das hat in diesen Fällen eher nichts mit Hautfarbe zu tun - sagen auch die Kritiker. In meinen Augen eine klare Überreaktion. Vielleicht gut gemeint, aber deswegen nicht richtig und gesund.

Master und Slave - oder Primary und Replica?

Aber die Diskussionen gehen weiter. Eigentlich spricht man in der IT von einer "Man-in-the-middle-Attack", wenn sich ein Hacker oder Betrüger gewissermaßen in einen Datenstrom klinkt und so Daten abgreift oder manipuliert. Eine häufig verwendete Hackmethode.

Auch dieser Begriff steht in der Kritik. Vorschlag: "Person-in-the-middle-Attack". Es könnte ja auch eine Frau sein, die den Angriff durchführt.

Klar, man könnte künftig von "Person-in-the-middle-attack" sprechen, auch von "Ethical Hacker" und "Unethical Hacker".

Ein anderes Beispiel sind die Begriffe "Master" und "Slave" in der IT. Der "Master" gibt den Takt vor, hält die Originale (etwa bei Servern), der "Slave" hat zu gehorchen, hält nur Kopien vor. Hier wären meiner Ansicht nach in der Tat andere Begriffe glücklicker, etwa "Primary" und "Replica". Oder von mir aus "Admiral" und "Cadet".

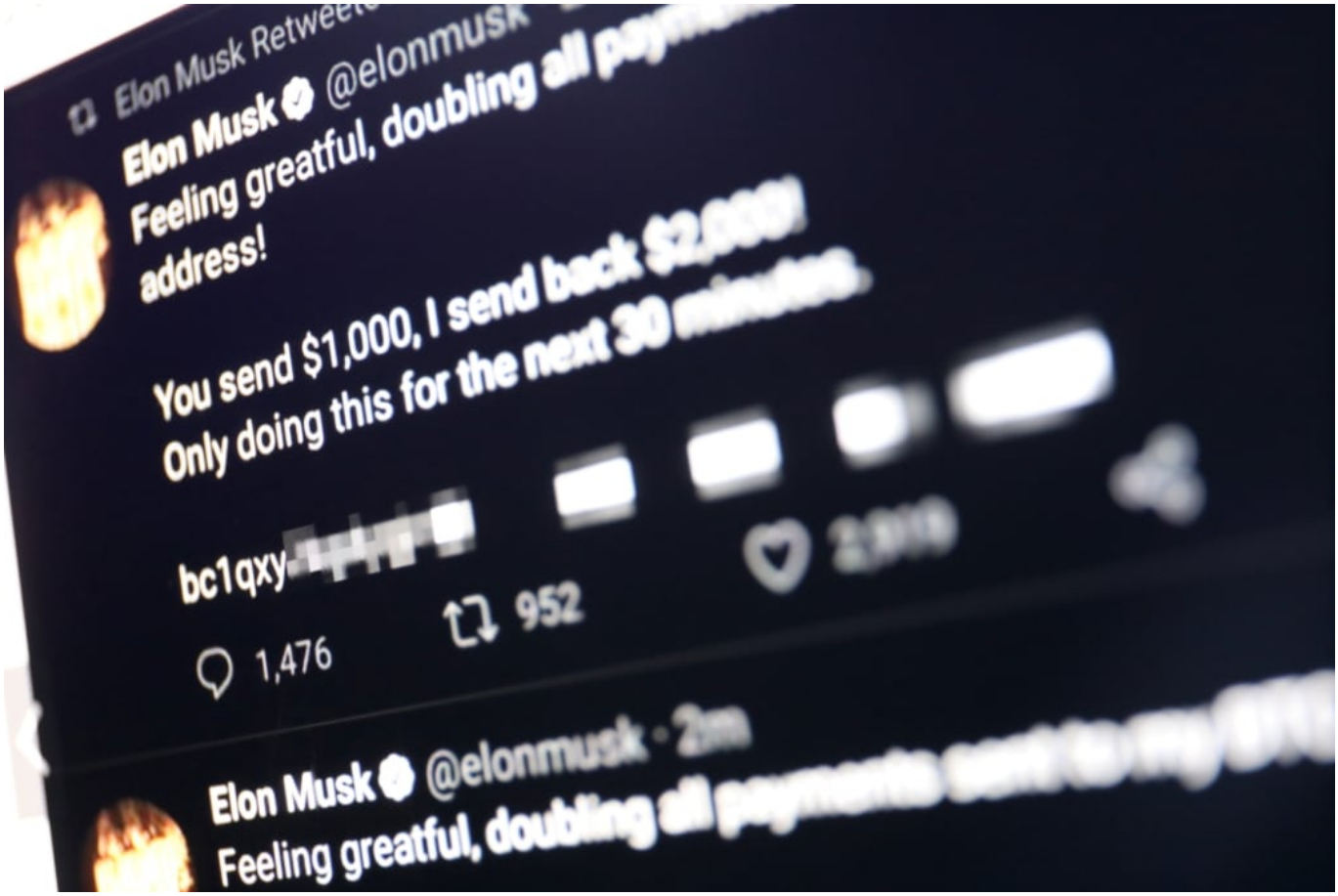
Es kommt Bewegung in die Welt der Begriffe.

Twitter-Hack: Es hätte noch viel schlimmer kommen können...

Durch einen gezielten Hack - indem Mitarbeiter bei Twitter ausspioniert und überrumpelt wurden - haben sich Angreifer Zugriff auf die internen Systeme von Twitter verschafft. Auf diese Weise konnten die Angreifer prominente Twitter-Accounts übernehmen - und im Namen dieser Menschen twittern... Das hätte auch ins Auge gehen können. Zeigt aber, sie verletzlich diese Systeme sind.

Jetzt ist es also passiert: Hacker haben offensichtlich ein ernsthaftes Sicherheitsleck entdeckt - und gnadenlos ausgenutzt.Der Imageschaden für Twitter ist erheblich.

Über die Accounts von Prominenten wie Barack Obama, Joe Biden, Jeff Bezos, Warren Buffet oder Kanye West wurden individuelle Tweets verschickt, die den Eindruck erwecken, man könne über eine Bitcoin-Börse praktisch sofort aus 1.000 Dollar 2.000 Dollar machen.



Gier funktioniert immer: Per Bitcoin Einsatz verdoppeln

Innerhalb weniger Stunden sind 100.000 Dollar auf dem Bitcoin-Konto eingegangen. Rund 100 Leute konnten also nicht widerstehen. Die Gier ist den Menschen nicht auszutreiben. Tja, und weil bei der Kryptowährung Bitcoin so ziemlich alles möglich erscheint - selbst eine sofortige

Verdopplung - greifen eben manche zu. Das haben die Täterinnen und Täter schon clever eingefädelt.

Doch eine wichtige Frage ist natürlich: Wie haben sie das gemacht? Von Anfang an war klar: Da so viele prominente Konten gleichzeitig betroffen sind, kann es nicht die Nachlässigkeit einzelner bei der Verwaltung von Zugangsdaten sein. Denn bei derart prominenten Konten kümmern sich in der Regel Experten um die Verwaltung der Konten, die nicht so ohne Weiteres zu überlisten sind - schon gar nicht so viele gleichzeitig.

Mittlerweile sind erste Details bekannt, woran es gelegen haben könnte. Vermutlich war Social Enginerring im Spiel - aber nicht im Dunstkreid der gekaperten Konten, sondern bei Twitter. Wahrscheinlich wurde ein Twitter-Mitarbeiter ausgetrickst - und ihm oder ihr durch Ausnutzen von Sicherheitslücken in Betriebssystem oder anderer Software ein Trojanter untegejubelt.

Auf diese Weise haben sich die Angreifer Zugriff auf die **internen Systeme von Twitter** verschafft. Und konnten nach Beliebgen Passwörter von Konten zurücksetzen - und dann loslegen.

Mängel im System: Abhängigkeit und mangelnde Absicherung

Der aktuelle Fall macht deutlich, wie sehr die Welt von einzelnen US-Konzernen abhängt. Und es ist noch glimpflich ausgegangen. Man stelle sich vor, es wäre das Konto des US-Präsidenten

gehackt worden. Der erste Präsident, der seine Befehle twittert - sozusagen. Hätten die Hacker hier eine Kriegserklärung gegenüber Nordkorea, einen Zoll von 100% auf Produkte aus China oder einen Austritt aus der NATO getwittert, hätte das zumindest für heillosen Schaden in der Diplomatie und für zusammenbrechende Börsen gesorgt.

Wir sollten also nicht nur darauf warten, welche Ursachen uns Twitter für dieses Desaster erklärt. Wir sollten Schlüsse daraus ziehen.

Ein US-Präsident sollte den Anstand haben, nicht über Twitter oder ähnliche Kanäle zu regieren. Journalisten sollten nicht annehmen, dass Twitter eine offizielle Nachrichtenquelle ist. Wir alle sollten Twitter und Co. weniger ernst nehmen. Und last not least braucht es endlich 100% sichere Mechanismen, um Onlinekonten abzusichern - zumindest jene, die verifiziert und damit besonders prominent sind.

Tipps zu einer Facebook Live-Übertragung

Facebook unterstützt wie andere soziale Netzwerke die maximal mögliche Unterstützung des Mitteilungsbedürfnisses seiner Mitglieder. Neben einfachen Posts und Medien-Uploads gehört dazu auch das Live-Video. Ungefiltert und so, wie es gerade passiert können Sie einen Video-Live-Feed veröffentlichen und Ihre Zuschauer am aktuellen Geschehen teilhaben lassen. Das sollten Sie aber geplant tun. Wir geben Ihnen Tipps, worauf Sie achten sollten!

Denken Sie daran: Live ist live. Die Übertragung verzeiht keine Fehler. Was passiert, sehen die Teilnehmer direkt. Natürlich sind Pannen immer lustig. Je nach dem Zweck Ihrer Übertragung aber können Sie die Zielgruppe auch verschrecken!

Kein Live Video ohne Konzept. Es gibt nichts Schlimmeres als einen stotternden Moderator, der sich verhaspelt. Machen Sie sich vorher ein Konzept und folgen Sie dem so weit es geht. Je spontaner Sie sind, desto eher verlaufen Sie sich. Eine Live-Übertragung soll spannend sein und die Zuschauer bei der Stange halten!

Geplant ist besser als spontan. Sicherlich gibt es Gelegenheiten, zu denen Sie keine andere Wahl haben, als die Übertragung direkt zu starten. Beispielsweise, wenn Sie über ein Ereignis berichten, das spontan passiert. In allen anderen Fällen weisen Sie in Ihrer Timeline vorher auf die Übertragung hin!

#TikTok wird politisch: Aktionen gegen Trump

Alle reden über Facebook, Twitter und YouTube - und lassen TikTok links liegen. Dabei ist TikTok eins der am schnellsten wachsenden Sozialen Netzwerke/Plattformen. Der Nachfolger der Tanz-Video-App Musically entwickelt sich zu einer politischen Plattform. So sind bereits mehrere erfolgreiche Aktionen gegen US-Präsident Donald Trump von TikTok ausgegangen.

TikTok ist eine App, die vor allem Kinder und Jugendliche benutzen - und auch junge Erwachsene. Aber was da passiert in TikTok, das bleibt meistens unter dem medialen Radar. Jede kleine Empörungswelle auf Twitter wird medial aufgebauscht - weil die meisten Journalisten sich bei Twitter umschauen. Doch TikTok ist wie ein blinder Fleck.

TikTok ist Plattform #1 bei jungen Menschen

Ein riesiger Fehler, denn TikTok ist unfassbar erfolgreich. Kein anderes "soziales Netzwerk" (ich sage ja lieber Plattform dazu) hat so schnell die 1-Milliarde-Nutzer-Marke geknackt wie TikTok. Das liegt zweifellos an der Herkunft: TikTok kommt aus China. Und in China - wie in Asien generell - stehen die Jugendlichen auf alles, was auf dem Mobilgerät passiert. Und alles, was neu ist.

Eigentlich ist TikTok eine Plattform, auf der die meist jungen User aufwändige Tanz-Moves präsentieren, oder Lip-sync-Videos, in denen sie populäre Songs nachsingen. Doch mehr und mehr entwickelt sich auch TikTok zu einer politischen Plattform. Die User nutzen sie für ihre Zwecke.

Mit Abstand populärster Hashtags ist #BlackLivesMatter - mit 13,3 Mrd. Videoaufrufen. Die Debatte über Rassismus hat also auch TikTok voll erfasst. Ein regelchter Star - aber im negativen Sinne! - ist US-Präsident Donald Trump. #Trump kommt auf 3,3 Mrd. Videoaufrufe. Es hat in der jüngsten Vergangenheit einige wirklich aufsehenerregende Aktionen auf TikTok gegeben.

Mit Tricks Online-Shops lahmgelegt und Stadien leer gemacht

So hat die Community zum Beispiel dazu aufgerufen, Tickets für die Wahlkampf-Veranstaltung von Donald Trump in Tulsa zu reservieren - aber dann nicht hinzugehen. Das hat Donald Trump eine ungeheure Schlappe eingebracht: Nur rund 6.000 Fans waren vor Ort, wo Trumps Wahlkampflager rund eine Million Besucher erwartet hatte.

Ein anderer Coup: Diese TikTok-Nutzerin hat eine Schwachstelle in Online-Shops entdeckt - und gegen Trump gewendet. Der Trick: Trump-Gegner sollten in Onlineshops mit Trump-Fan-Artikeln wahllos so viele Produlte wie möglich in den Warenkorb legen, zum Beispiel "Make America Great Again"-Cappys. Aber am Ende nicht kaufen. Die Wirkung: Waren, die im Warenkorb liegen, werden erst mal für diesen Nutzer geblockt - und bei vielen Shopsystemen nicht mehr freigegeben. Am Ende steht ein Ausverkauf - obwohl niemand kauft.

Die Macht der Masse: Trump dürfte sich ärgern

Ein anderer Trick: Das massenweise Schlecht-Machen von Trumps Hotels und Restaurants mit 1-Stern-Bewertungen.

Eine moderne Form von zuvilem Ungehorsam. Moralisch nicht über jeden Zweifel erhaben - aber ganz sicher ein Aufreger für Donald Trump, der auf diese Weise - über Bande! - die Macht des Volks zu spüren bekommt.

In China herrschen normalerweise strenge Regeln und Restriktionen. Aber Aktionen, die Donald Trump schaden - die lassen die Herrscher Peking derzeit ganz sicher kalt. Wohl aber nicht, dass man in den USA laut über ein Verbot von Plattformen aus China nachdenkt.

https://vimeo.com/360737213

Sogar interner Bericht belegt: Facebook schützt die Falschen

Vor zwei Jahren hat Facebook eine interne Studie in Auftrag gegeben. Das Ergebnis: Faceboom unternimmt viel zu wenig gegen Hass, Hetze und Falschmeldungen - und schützt die Falschen. Das geht auf Kosten von Bürgerrechten und Schutz vor Diskriminierung. Kritik aus dem eigenen Haus.

Das Ergebnis der über zweijährigen Untersuchung ist eine schallende Ohrfeige: Facebook stelle die Meinungsfreiheit über die Bürgerrechte und sogar gegen den Schutz vor Diskriminierung. Was alle wissen, das hat Facebook jetzt Schwarz auf Weiß.

Mark Zuckerbergs Konzern hat den Bericht nicht nur selbst in Auftrag gegeben, sondern nun auch veröffentlicht. Was Lob und Anerkennung verdient, da das Ergebnis der Untersuchung wirklich alles andere als schmeichelhaft ist.

Bürgerrechte sträflich vernachlässigt

Dem Abschlussbericht geht eine unabhängige, zweijährige Untersuchung von Facebooks Richtlinien und deren Umsetzung voraus. Die Autorinnen und US-Bürgerrechtlerinnen Laura Murphy und Megan Cacace von der Anwaltskanzlei Relman Colfax bescheinigen dem "f"-Netzwerk, bei weitem nicht genug für den Schutz der Nutzerrechte zu tun. Laut Bericht gibt es sogar "signifikante Rückschritte für die Bürgerrechte".

Klare Ansagen. Im Grunde müssten wir uns alle aus dem Netzwerk verabschieden. Die Politik hat in der Vergangenheit kaum etwas erreicht.

Mark Zuckerberg wiederholt wie ein Mantra, er wolle die Meinungsfreiheit nicht beschneiden - und redet sich so raus. Er will keine Verantwortung übernehmen und erst recht nicht die Kosten tragen, aus seinem Netzwerk einen angenehmen Ort zu machen.

Lasst Dollars sprechen - dann reagiert Facebook

Doch nun laufen ihm die Werbekunden davon. Das bedeutet Milliarden an Einnahmeverlusten für Facebook. Nun plötzlich passiert etwas: Vor einigen Tagen hat Facebook Dutzende Konten und Chat-Gruppen von rechten und rechtsradikalen Gruppierungen in den USA geschlossen.

Selbst politiknahe Akteure müssen nun mit Beschränkungen rechnen. Das Netzwerk hat jetzt sogar Accounts geschlossen, die Mitarbeitern des brasilianischen Präsidenten Bolsonaro gehören. Auch Konten von Roger Stone, Ex-Berater des US-Präsidenten Donald Trump, hat Facebook nun entschlossen gesperrt.

Politischer Druck bisher wirkungslos

Gute Argumente bringen bei Facebook nichts. Die Bemühungen von Bürgerrechtsverbänden verpuffen bei Facebook. Selbst politischer Druck ist bei Facebook weitgehend wirkungslos.

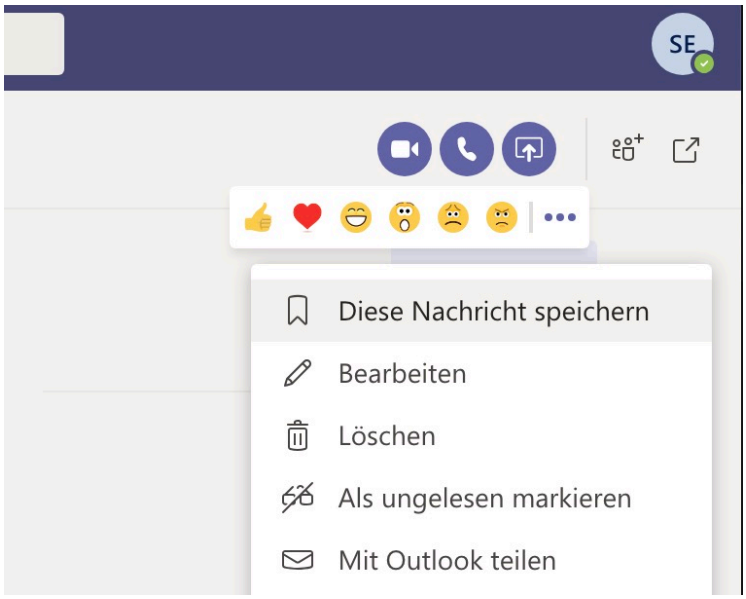
Einnahmeverluste durch den Werbeboykott ist die einzige Sprache, die Mark Zuckerberg und sein Team verstehen und respektieren. Wie armselig.

Facebook-Chefin Sheryl Sandberg behauptet in einem Posting, das alles würde nicht aufgrund des Werbedrucks geschehen, sondern "weil es das Richtige ist". Wer soll das denn bitte glauben?

Gespeicherte Nachrichten in Teams

Nicht erst die Corona-Krise hat dazu geführt, dass Kollaborations-Tools wie Microsoft Teams immer weitere Verbreitung finden. Was auf der einen Seite eine tolle Entwicklung ist, hat auch Auswirkungen auf die Arbeitsprozesse: Die Zahl der Nachrichten nimmt immer mehr zu. Immer weitere Teams werden hinzugefügt. Wichtige Nachrichten zu finden kann zur Herausforderung werden. Speichern Sie sie doch einfach!

Wenn Sie eine Nachricht speichern wollen, dann klicken Sie in der Nachrichtenblase auf die drei Punkte neben der Nachricht. Klicken Sie dann auf **Nachricht speichern**. Die Nachricht wird markiert und bei den gespeicherten Nachrichten abgelegt. Die Zahl der gespeicherten Nachrichten ist deutlich geringer als die Gesamtzahl, das hilft Ihnen beim Überblick.



Um nun wieder auf eine gespeicherte Nachricht zugreifen zu können, klicken Sie in der Teams-App oder der Teams-Webseite auf Ihr Kontobild und dann auf **Gespeichert**.

Alternativ geben Sie in der Befehlszeile ***/gespeichert*** ein. Diese Befehl ruft eine Übersicht der gespeicherten Nachrichten auf. Um die Markierung einer Nachricht aufzuheben klicken Sie wieder auf die drei Punkte neben der Nachricht und dann auf **Speicherung dieser Nachricht aufheben**.

Buchungen speichern mit TripIt

Je komplexer Ihre Reise wird, desto komplizierter auch der Reiseplan. Füge, Hotelbuchungen, Mietwagen, all das kommt in separaten E-Mails. Natürlich zwischen der ganzen Flut anderer Emails. Da kann die Suche nach der Flugnummer oder dem CheckIn-Code fürs Hotel schonmal dauern. Einfacher geht es mit der TripIt-App und dem dahinterliegenden Service.

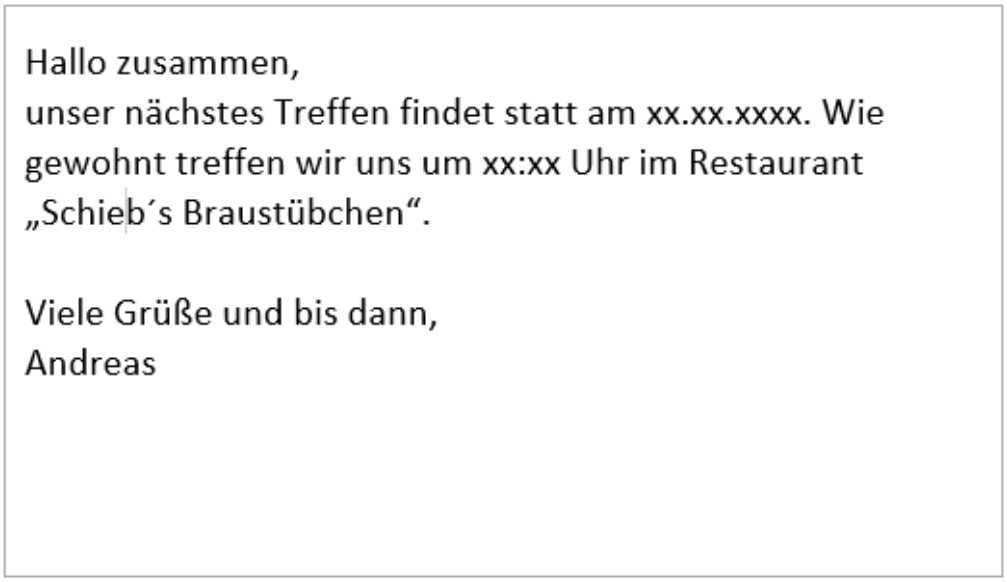
Registrieren Sie sich mit Ihrer eigenen Emailadresse, die dann als zentrale Identifikation dient. Wenn Sie ein E-Mail-Konto von Yahoo, Google Mail oder Outlook.com haben, dann importiert TripIT Ihre Reisedaten ganz von allein aus Ihrem Posteingang. Bei anderen Anbietern müssen Sie die entsprechenden E-Mails einfach an die E-Mail-Adresse plans@tripit.com weiterleiten.

Der Dienst stellt Ihnen dann aus allen vorliegenden E-Mails einen Reiseplan mit allen relevanten Informationen zusammen. Den können Sie sich in der App ansehen, verändern und erweitern. Damit aber nicht genug: TripIT verknüpft die vorliegenden Daten mit weiteren Informationen, die Sie unterwegs brauchen können: Wie kommen Sie vom Flughafen zum Hotel? Wo ist Ihr Gate auf dem Flughafen? Und was ist in der Nähe Ihrer Aufenthaltsorte, was interessant sein könnte?

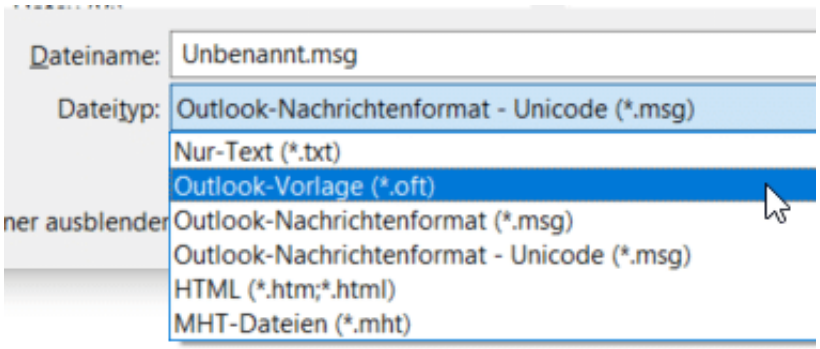
Die TripIt-App gibt es kostenlos für iOS und Android.

Erstellen eines E-Mail-Templates

Neben standardisierten Antworten auf E-Mails werden Sie immer mal wieder neue E-Mails verschicken, die ähnlich sind. Beispielsweise die Einladung zu einem Termin, die bis auf Datum, Uhrzeit und vielleicht Ort genau gleich ist. Da ist es unnötiger Aufwand, diese immer wieder neu zu schreiben. Outlook kennt dafür die so genannten Templates, die Sie mit wenigen Schritten einrichten können. Dazu legen Sie eine neue Email in Outlook an. Schreiben Sie den Inhalt einmal herunter, also alle Informationen, die in der E-Mail fest sind und bei jeder Verwendung wieder verwendet werden sollen. Dabei lassen Sie Platzhalter für die veränderlichen Angaben, z.B. indem Sie sie durch X ersetzen.



Statt die E-Mail dann abzuschicken, klicken Sie auf **Datei** > **Speichern unter**. Wählen Sie unter **Dateityp** statt des normalen Nachrichtenformats **Outlook-Vorlage** aus. Nachdem Sie der Vorlage nun einen sprechenden Namen gegeben haben, speichern Sie sie. Je mehr Vorlagen Sie speichern, desto genauer sollten Sie auf den Namen achten: Es gibt keine weitere Möglichkeit zur Unterteilung.

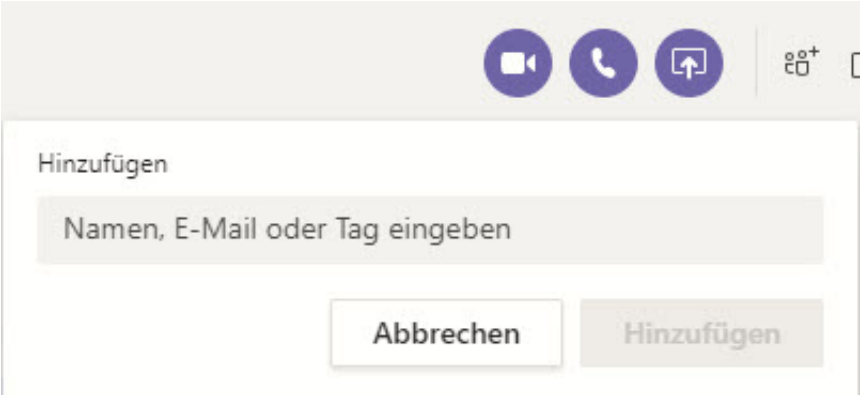


Um nun diese Vorlage zu verwenden, klicken Sie in Outlook auf **Datei** > **Neue Elemente** > **Weitere Elemente** > **Formular auswählen**. Wählen Sie unter **Suchen in**: ganz oben in der Formularauswahl **Vorlagen im Dateisystem**. In der sich nun öffnenden Liste finden Sie alle Ihre Vorlagen und können die gewünschte auswählen.

Vorsicht bei Teams-Sitzungen und temporären Teilnehmern!

Microsoft Teams ist neben Zoom eine der am meisten verwendeten Applikationen zur Durchführung von Videokonferenzen. Durch die Einschränkungen durch Corona gehen immer mehr Unternehmen dazu über, auch größere Sitzungen mit vielen Teilnehmern virtuell durchzuführen. Wie aber stellen Sie sicher, dass nur die Teilnehmer in der Sitzung sind, die auch darin sein dürfen?

Eigentlich ist das Durchführen einer Videokonferenz recht einfach: Sie laden die Teilnehmer über einen Termin ein, diese klicken auf den Link in dem Termin und können daran teilnehmen. In der Praxis zeigt sich aber, dass während einer Besprechung Rückfragen nötig sind. Die damit angesprochenen Teilnehmer müssen separat eingeladen werden. Das machen Sie, indem Sie auf das Symbol mit den beiden **Figuren** und dem **Plus-Zeichen** oben rechts im Teams-Fenster klicken und dann den Namen, die E-Mail-Adresse oder die Telefonnummer des Teilnehmers eingeben.



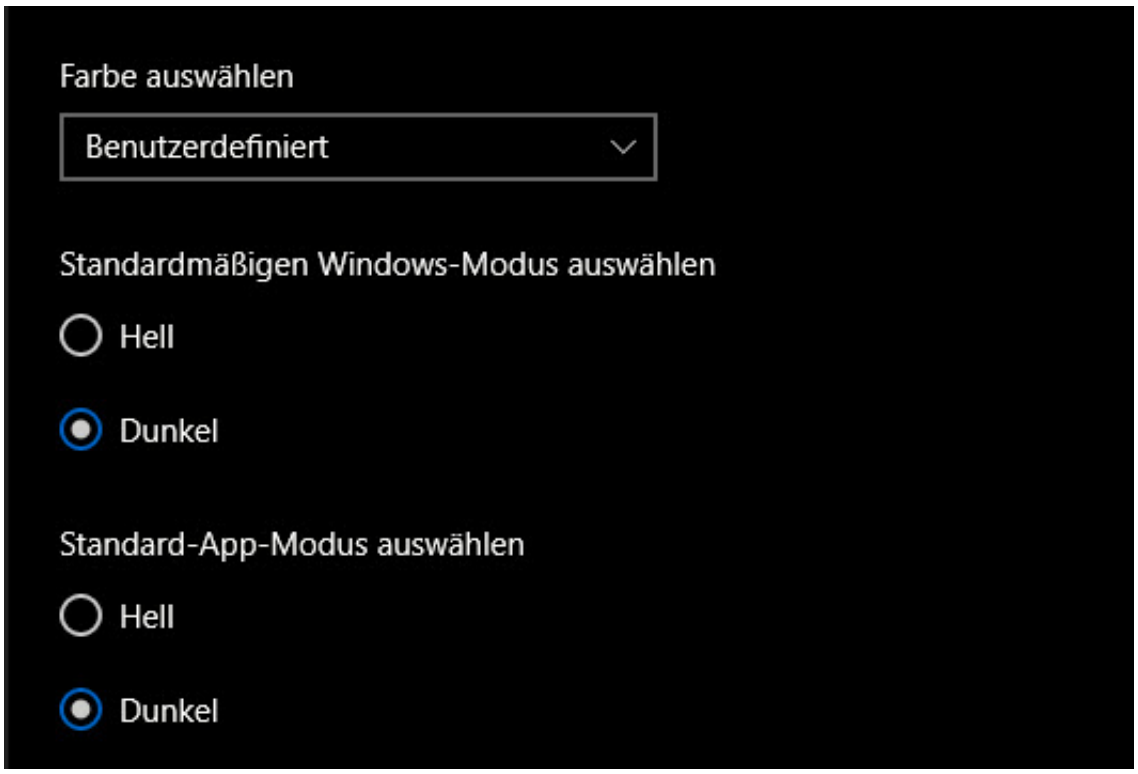
Verlässt der Teilnehmer die Sitzung, dann kann er nicht mehr mithören oder die geteilten Bildschirminhalte sehen. Was aber oft vergessen wird: Er ist immer noch Teilnehmer des Besprechungs-Chats. Dieser wird oft genutzt, um neben dem Hauptgespräch Informationen oder Links auszutauschen. Dies sollte ein gelöschter Teilnehmer nicht mehr sehen können.

Die Lösung: Klicken Sie in der Symbolleiste auf **Chat**, dann oben rechts auf das Symbol mit den Personen und der Zahl. Darin finden Sie alle Teilnehmer, die in der Sitzung sind und waren. Klicken Sie auf das Kreuz neben dem Namen, um einen Teilnehmer auch aus dem Chat zu löschen.

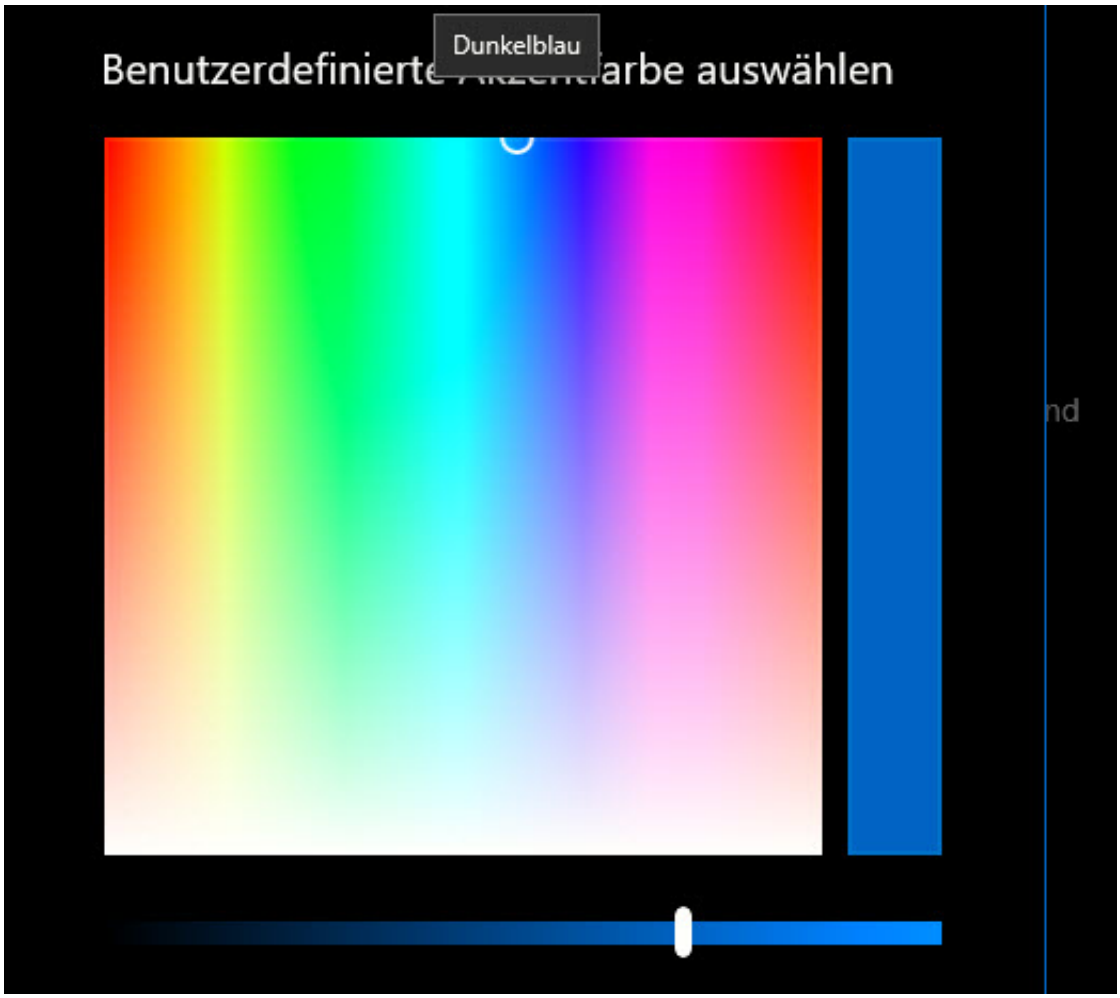
Wenn die benutzerdefinierten Farben nicht verfügbar sind

Windows hat einen langen Weg genommen seit den ersten Versionen. Vorbei sind die Zeiten, in denen kaltes Grau vorherrschte. Mittlerweile können Sie fast jedes Element der Oberfläche anpassen und auf Ihren Geschmack färben. Dumm nur, wenn die benutzerdefinierten Optionen verschwunden oder nicht aktivierbar sind. Wir zeigen Ihnen, wo Sie schauen müssen!

Die Farbeinstellungen finden Sie unter **Einstellungen** > **Personalisierung** > **Farben**. Die erste Auswahl ist die des Farbschemas: Seit 2019 können Sie sowohl ein dunkles als auch ein helles Thema einstellen. Das hat Microsoft sich ein wenig von Android abgeschaut, wo das dunkle Thema schon seit einigen Versionen sehrt beliebt ist.



Stellen Sie unter **Farbe auswählen** die Einstellung auf **Benutzerdefiniert**, um selbst feinere Anpassungen vornehmen zu können. Hier können sie nun unterschiedliche Farbvorgaben von Windows einstellen. Alternativ stimmen Sie das Farbschema passend zu Ihrem Hintergrundbild ein, indem Sie **Automatisch eine Akzentfarbe aus meinem Hintergrund auswählen** aktivieren.



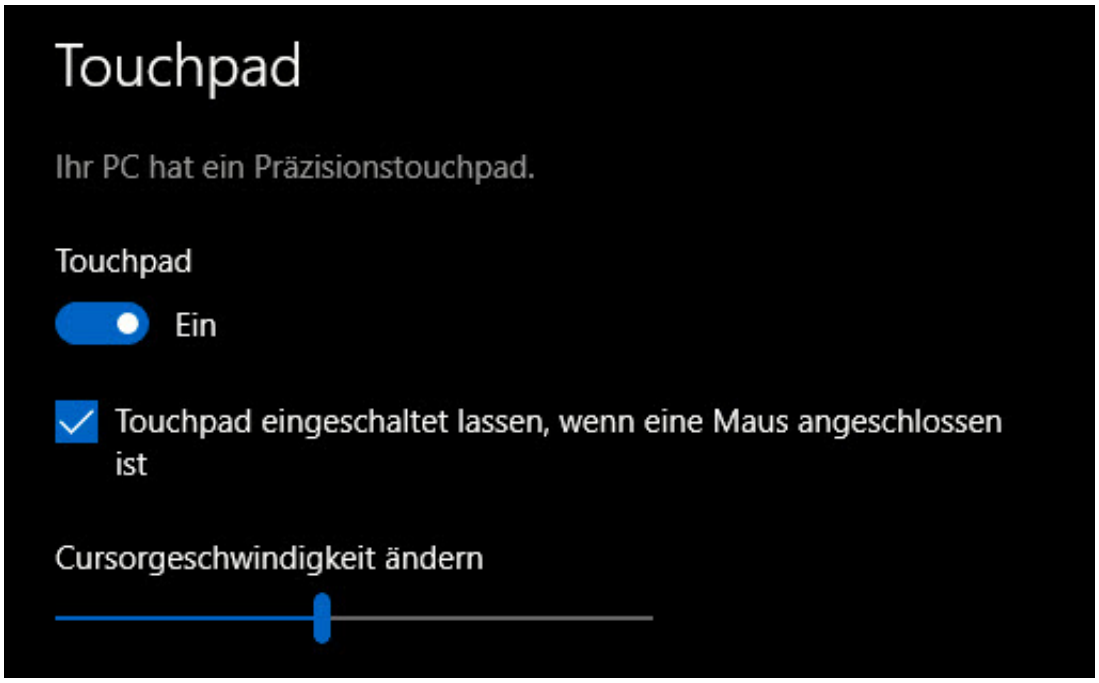
Noch feiner können Sie Einfluss nehmen, wenn Sie **Benutzerdefinierte Farbe** anklicken. Dann zeigt Windows Ihnen einen Farbverlauf, aus dem Sie die Farbe Ihrer Wahl festlegen können.

Zu guter Letzt können Sie festlegen, auf welchen Flächen diese Farbe angezeigt werden soll: **Start, Taskleiste und Info-Center** und **Titelleisten und Fensterrahmen** können Sie frei nach Gusto aktivieren und deaktivieren.

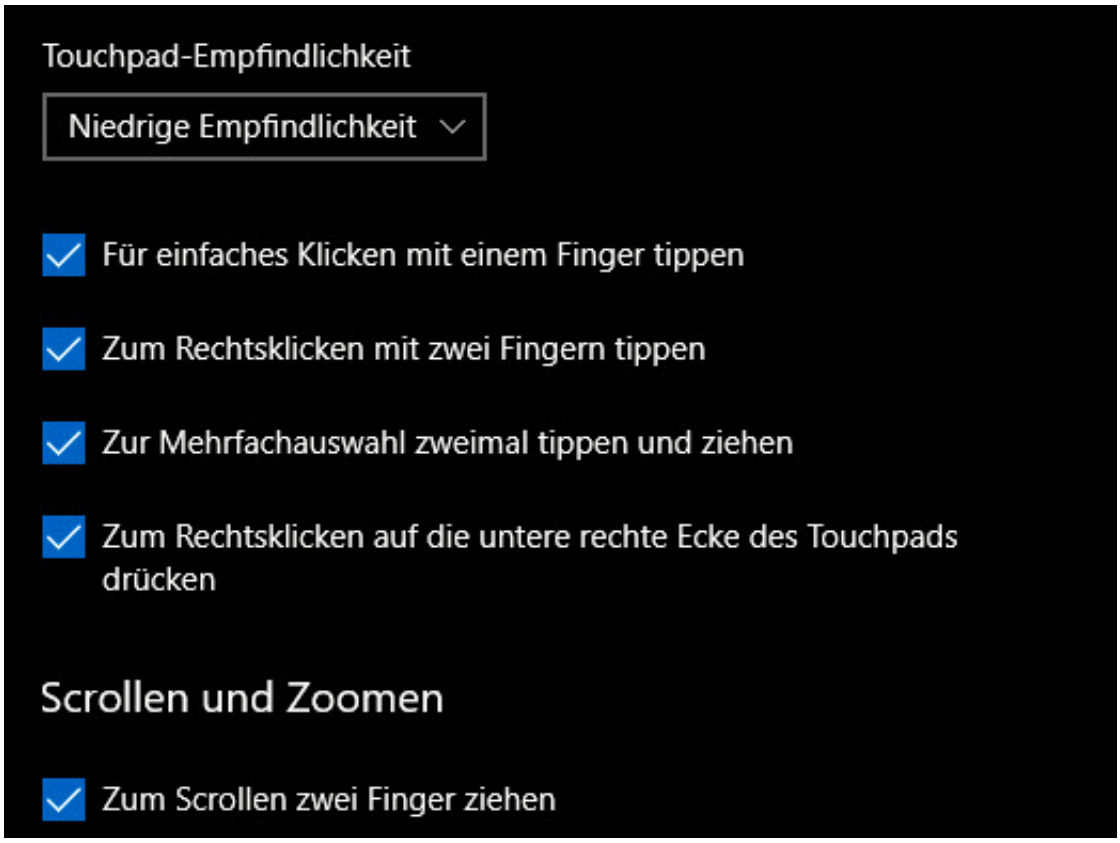
Wenn das Touchpad nicht mehr funktioniert

Manche Anwender bevorzugen immer die Maus für Eingaben am PC. Andere haben sich so an das Touchpad gewöhnt, dass sie es der Maus vorziehen. Dumm nur, wenn das Touchpad plötzlich bestimmte Funktionen nicht mehr ausführt oder ganz ausfällt. Als erstes schließen Sie eine Maus an, dann probieren Sie unsere Tipps!

Wenn Sie keine Maus zur Verfügung haben, starten Sie den Rechner einmal neu. Das geht auch über die Tastatur: Drücken Sie gleichzeitig **Alt** + **Strg** + **Entf**, da so oft die **Tab-Taste**, bis Sie auf dem Symbol mit dem Kreis und dem Strich in der Mitte angekommen sind. Drücken Sie die Leertaste und gehen Sie mit den Pfeiltasten auf **Neu Starten**. Ein Drücken der Leertaste startet dann den Rechner neu. Viele Probleme sind damit schon gelöst.



Wenn das Touchpad gar nicht funktioniert, dann kontrollieren Sie erst einmal, ob es überhaupt eingeschaltet ist. Dazu tippen Sie "Touchpad" in der Suchleiste ein und klicken Sie auf eines der Suchergebnisse. Touchpad sollte auf **Ein** stehen. Ebenfalls sollte **Touchpad eingeschaltet lassen, wenn eine Maus angeschlossen ist** eingeschaltet bleiben.



Wenn nur bestimmte Funktionen nicht vorhanden sind, dann schauen Sie sich die Optionen im unteren Teil des Einrichtungsbildschirms an. Hier fehlen oft Häkchen, die zu Problemen führen.