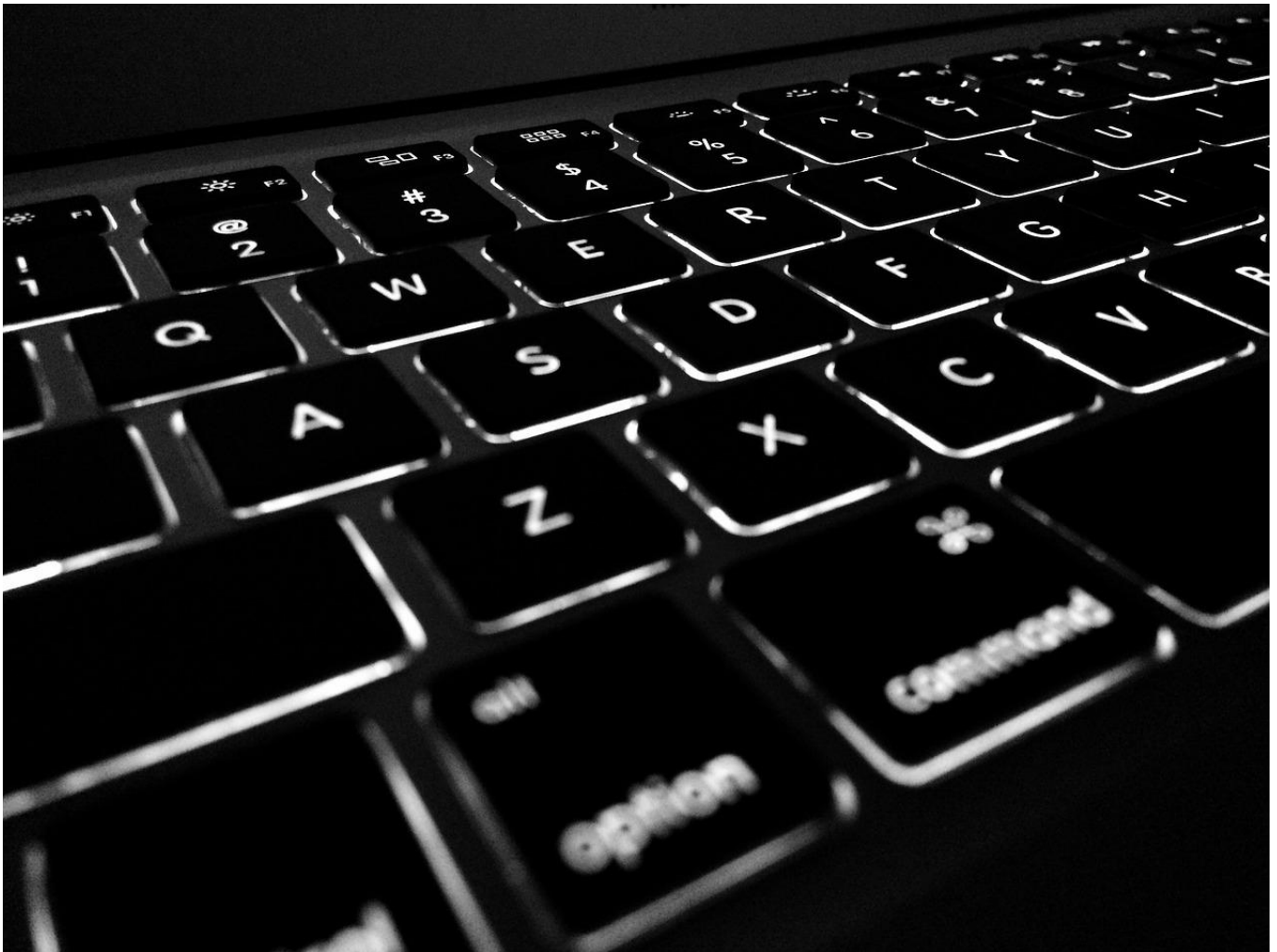


A portrait of a man with short brown hair and a slight smile, wearing a teal button-down shirt. He is positioned on the left side of the frame, with his arms crossed. The background is dark. The text 'Schieb Report' is overlaid on the right side in a large, white, sans-serif font.

Schieb Report

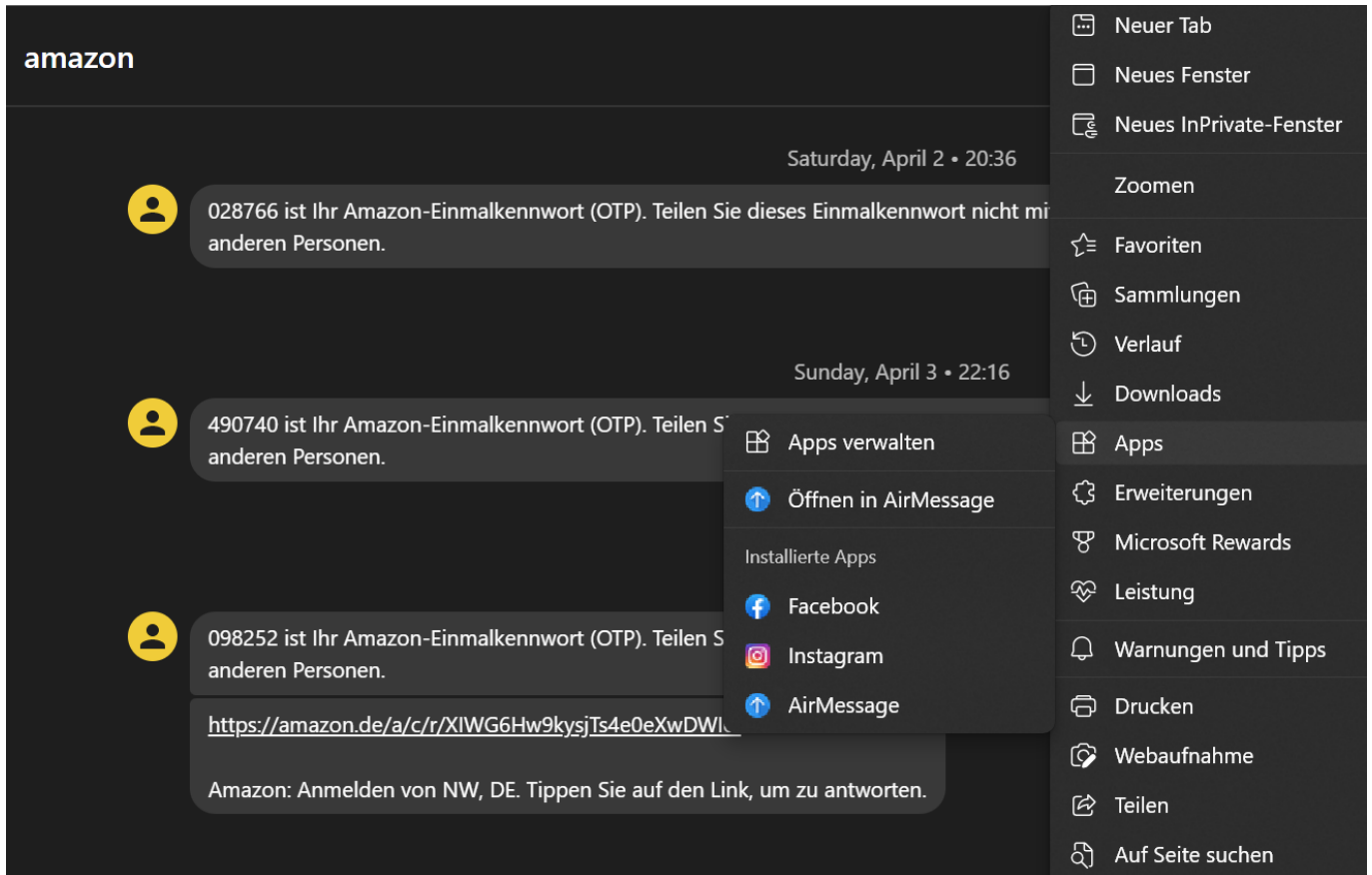
Ausgabe 2022.19

iMessage unter Windows: Geht!



Ihr habt ein iPhone und einen PC, aber keine Lust, dauernd Euer iPhone in die Hand zu nehmen, um Nachrichten zu lesen? Und das Internet sagt, unter Windows geht das nicht? Wenn Ihr auch noch einen Mac habt, dann geht das sogar sehr einfach!

Grundsätzlich ist die Herausforderung, dass Apple keinen Zugriff von anderen als den eigenen Betriebssystemen auf iMessage (und andere Dienste) zulässt. Aus dem Grund ist auch der Mac nötig, denn der kann das. Mit der Software AirMessage, die wir [hier](#) vorgestellt haben, können die iMessages in ein Google-Konto übertragen werden. Das ist eigentlich für Android-Smartphones gedacht, lässt sich aber auch mit einem beliebigen Gerät mit einem Webbrowser nutzen. [Hier](#) findet Ihr den Webclient.



Das Schöne: Microsoft Edge erlaubt es, aus einer Webseite automatisch eine App zu bauen. Dazu ruft Ihr die [AirMessage-Seite](#) auf und klickt dann oben rechts in Edge auf die drei Punkte. Im Menü klickt auf **Apps > Diese Site als App hinzufügen**.

Die Seiten-App wird nun als Eintrag zu den Programmen hinzugefügt und lässt sich auch an die Taskleiste anheften. Wenn die Webseite Benachrichtigungen unterstützt, dann werden diese auch als Symbole am App-Symbol in der Taskleiste angezeigt.

App-Datenschutzbericht in iOS aktivieren



Apps laufen auf Eurem iPhone so vor sich hin, in Vordergrund, im Hintergrund, Ihr seht nur, was sie auf dem Bildschirm tun. Der App-Datenschutzbericht gibt Euch mehr Informationen!

Am Ende bleibt bei jede rApp immer eine Unsicherheit übrig: Selbst wenn Ihr genau nachschaut, [welche Berechtigungen sie verwendet](#), dann ist diese Information nur grob: Eine App mag berechtigt auf die Datenverbindung zugreifen und Daten abrufen oder senden. Tut sie das mit dem Server des Anbieters, ist das okay. Gehen die Daten aber an eine andere Adresse, dann nicht. iOS hat mit dem App-Datenschutzbericht eine versteckte, aber unheimlich mächtige Kontrolle an Bord.




App-Datenschutzbericht

Der App-Datenschutzbericht zeigt, wie oft Apps die von dir erteilte Berechtigung zum Zugriff auf deine Daten, z. B. auf deinen Standort oder dein Mikrofon, nutzen. Zudem ist eine Übersicht der Netzwerkaktivitäten jeder App, der Netzwerkaktivitäten von Websites und der am häufigsten kontaktierten Domains enthalten. [Weitere Infos ...](#)

[App-Datenschutzbericht aktivieren](#)


Den müsst Ihr einmalig unter **Einstellungen > Datenschutz > App-Datenschutzbericht** aktivieren. Danach findet Ihr im selben Menü den kontinuierlich aktivierten Datenschutzbericht für alle Apps.


ZUGRIFF AUF DATEN UND SENSOREN


 **Nest** >
vor 3 Sek. · Standort


Diese Apps haben in den letzten 7 Tagen auf deine Daten und Sensoren zugegriffen.

APP-NETZWERKAKTIVITÄT

 **Nest** >
22

 **Fotos** >
2

 **Safari** >
1

 **WhatsApp** >
1

Diese Apps haben in den letzten 7 Tagen Domains kontaktiert.

Unter Zugriff auf Daten und Sensoren findet Ihr eine Historie der letzten 7 Tage über die Zugriffe von Apps auf Daten und Sensoren. Tippt eine App an, dann seht Ihr detailliert, was die App in der Zeit gemacht hat. Jeder Zugriff (ab Aktivierung des Protokolls) wird aufgezeichnet.

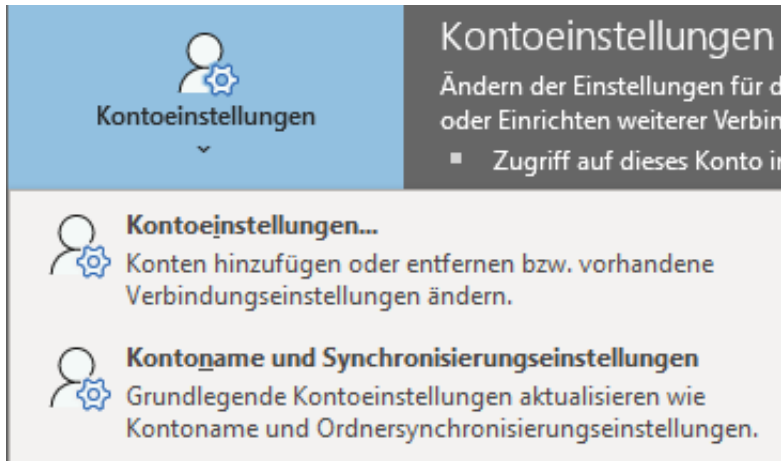
Unter App-Netzwerkaktivität seht Ihr sortiert nach Apps alle Aufrufe im Netzwerk und Internet, sowohl wann als auch mit welcher Adresse bzw. URL die Kommunikation stattgefunden hat. Die Adressen mögen auf den ersten Blick nicht direkt sprechend sein, oft hilft aber da eine Suche im Internet!

Einbinden eines freigegebenen Postfachs in Outlook



Arbeiten im Team bedeutet immer, dass auch zugriff auf E-Mails und Termine anderer Postfächer nötig ist. Die Aussage "Habe ich Dir freigegeben!" ist hier nur der erste Schritt. Wir zeigen, wie Ihr die freigegebenen Postfächer einbinden könnt.

Das Postfach eines Benutzers ist im ersten Schritt eine lokale Angelegenheit: Es wird angelegt im Outlook auf dem PC des Benutzers, ist aber - zumindest bei einem Microsoft 365- oder Exchange-Postfach - natürlich nur eine Kopie des Serverpostfaches. Hat der Besitzer eine Freigabe erteilt, dann meldet Ihr Euch nicht mit diesem Konto an, sondern bindet es nur ein. Das hat den Vorteil, dass der Eigentümer kein Passwort weitergeben muss, sondern für jeden Zugreifenden die Berechtigungen selbst festlegen kann.



Um nun eine solche Freigabe einzubinden, geht wir folgt vor:

- Klickt in Outlook auf **Datei > Informationen > Kontoeinstellungen > Kontoeinstellungen.**
- Klickt in der Übersicht der Konten auf Euer aktuelles Outlook-Konto, dann auf **Ändern.**
- Um an die zusätzlichen Postfächer zu kommen, müsst Ihr als nächstes auf **Weitere Einstellungen** klicken.
- In der Registerkarte **Erweitert** könnt Ihr dann das freigegebene Postfach **Hinzufügen.**

Das so eingebundene Postfach erscheint in der Ordnerübersicht Eurer Outlook. Was Ihr mit den Elementen machen könnt, hängt von den Rechten ab. Sollt Ihr beispielsweise Mails aus diesem Postfach versenden und bekommt eine Fehlermeldung, dann kontaktiert den Eigentümer des Postfaches. Der kann die Berechtigungen prüfen und gegebenenfalls anpassen.

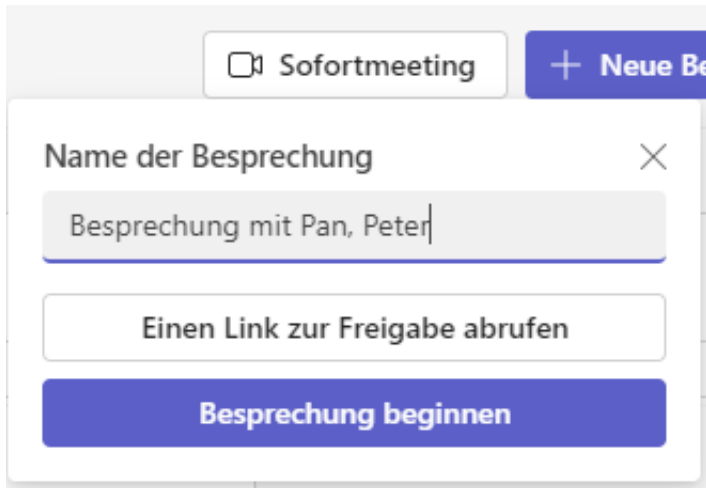
Sofortmeetings mit Teams starten



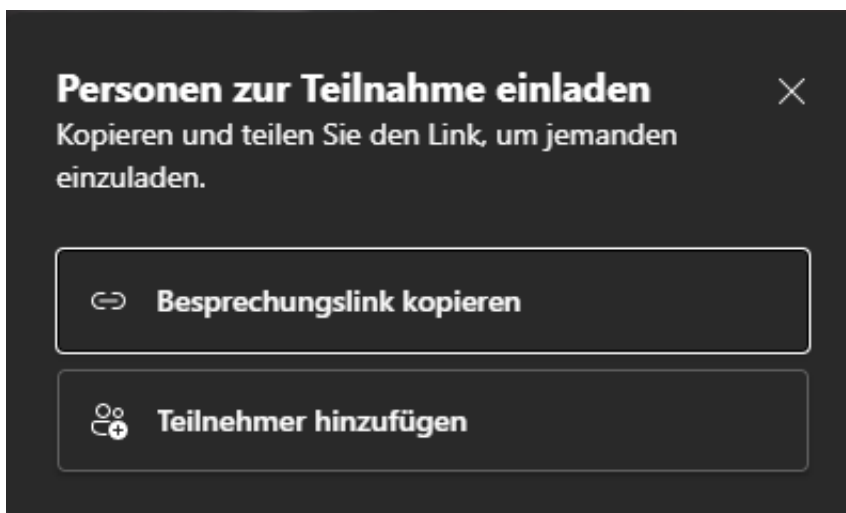
Manchmal muss eine Besprechung spontan stattfinden und kann nicht lang geplant werden. Wir zeigen Euch, wie das mit [Teams](#) geht!

[Microsoft Teams](#) ist das Drehkreuz der Kommunikation im Unternehmen und zunehmend auch privat. Neben der Zusammenarbeit erlaubt die Microsoft-Software auch die Durchführung von Videokonferenzen. Das ist komfortabel, wenn ein geplanter Termin ansteht. Dann könnt Ihr In Outlook (oder im Teams-Kalender) den Termin einstellen, die Teilnehmer einladen und direkt einen Links zur Besprechung einfügen.

Wenn Ihr aber spontan Redebedarf habt, dann braucht Ihr ja eigentlich keinen Termin mit einem Zeitpunkt in der Zukunft, sondern wollt sofort, ohne Umwege sprechen. Teams bietet dazu die Sofortmeetings.



Wechseln in Teams in den Kalender und klickt dann am oberen Bildschirmrand auf **Sofortmeeting**. Gebt den **Namen der Besprechung** ein und klickt dann auf **Besprechung beginnen**. Teams startet im Hintergrund eine Besprechung, in der Ihr nur selbst seit.



Klickt auf **Teilnehmer hinzufügen**, um andere Teilnehmer hinzuzufügen, die in den Kontakten sind. Alternativ könnt Ihr den **Besprechungslink kopieren** und dann per Chat, WhatsApp oder E-Mail an Teilnehmer weiterleiten. Dies können dann durch einen Klick auf den Link an der spontanen Besprechung teilnehmen.

Einen zusätzlichen Vorteil hat die Sofortbesprechung übrigens: Egal, ob weitere Teilnehmer darin sind oder nicht: Euer Status springt sofort automatisch auf "In einer Besprechung" und Teams hält den PC davon ab, automatisch in den Standbymodus zu gehen, auch wenn Ihr nicht daran sitzt.

Chat-Scans gegen Verbreitung von Missbrauchsbildern



Die Pläne der EU-Kommission im absolut berechtigten und notwendigen Kampf gegen Kindesmissbrauch und der Verbreitung von Missbrauchsbildern stehen in der Kritik. Und das völlig zu Recht: Die Pläne sind maßlos, dilettantisch durchdacht und miserabel konzipiert.

Die EU-Kommission hat am Mittwoch ein geplantes Regelwerk vorgestellt, das ganz explizit Kinder schützen soll. Die Kommission will die Verbreitung von Bildern mit Missbrauchshandlungen strenger verfolgen, ebenso das Cyber-Grooming: So wird das genannt, wenn sich Erwachsene unter Vortäuschung falscher Tatsachen an Kinder ranmachen, zum Beispiel in Chats. Die Kommission hat ein umfangreiches Paket mit weitreichenden Kompetenzen für eine neue Behörde und vor allem Pflichten für Onlinedienste und Plattformen vorgestellt. Und dagegen regt sich Protest: In der Community – aber auch unter Experten. Denn einige fürchten nicht weniger als ein Ende der Privatsphäre.



EU-Kommission will neue Behörden einrichten

Die beiden EU-Kommissare Dubravka Šuica (Demografie) und Ylva Johansson (Inneres) haben Mittwoch öffentlich beklagt: Jedes fünfte Kind werde Opfer von sexuellem Missbrauch.

Sie konzentrieren sich bei ihren Aktivitäten auf das Internet. Denn dort, im Internet, seien allein im vergangenen Jahr 85 Millionen Bilder zu finden gewesen, die sexuelle Gewalt gegen Kinder zeigten. In 90 Prozent der Fälle lagere das Material auf Servern in der EU. Aus diesem Grund sei Brüssel besonders gefordert.

Man wolle einen „einen Weltstandard gegen die illegalen Aufnahmen“ entwickeln. Die Tatsache, dass so viele der Aufnahmen auf EU-Servern liegen ist in der Tat ein Warnsignal, das muss ich sagen. Doch die beiden Kommissarinnen haben nicht etwa verstärkte Polizeiarbeit, vermehrte Löschanstrengungen der Bilder oder anderweitige Maßnahmen angekündigt, sondern ausgerechnet dort angesetzt, wo Protest quasi programmiert ist. Sie wollen ein EU-Zentrum gegen

Kindesmissbrauch gründen, das Onlinedienste zwingen kann, die gesamte(!) Kommunikation aller(!) Nutzer nach verbotenen Inhalten zu scannen.

E-Mails, Chats und Inhalte

Was genau könnte denn da durchsucht werden – ist das genau definiert?

Im Grunde ist alles gemeint, was denkbar ist. E-Mails selbstverständlich, aber auch Chats mit WhatsApp, Threema oder Signal. Selbst Chats, die nur beiläufig angeboten werden, etwa in Games, sollen auf Anordnung überwacht und durchsucht werden. Finden die Unternehmen bei diesen Untersuchungen Missbrauchsmaterial – so der Plan –, müssen sie die zuständige Behörde sowie ein neu einzurichtendes EU-Zentrum informieren, da eigens gegründet und in Den Haag angesiedelt sein soll.

Möglichst nahe an Europol. Und mehr als das: Dieses EU-Zentrum soll sogar passende Werkzeuge, also Software entwickeln und anbieten, für kleinere Dienste, die es sonst nicht hinbekommen, alles zu durchforsten. Daran lässt sich erkennen, dass eben nicht nur Meta, Google und Apple gemeint sind, sondern wirklich alle. Das kann man entschlossen nennen – Kritiker sprechen von einem „Big Brother Moment“, weil allmächtige Behörden geschaffen werden.



Verschlüsselung kompromittiert

Die Kritik ist unüberhörbar und konzentriert sich vor allem auf die Chats.

Und das aus zwei Gründen. Einmal, weil die Untersuchungen flächendeckend angeordnet werden und nicht etwa für einzelne Personen. Vor allem aber, weil sie die Betreiber zwingt, die heute übliche Verschlüsselung zu umgehen. Dazu muss man wissen: Messenger kommunizieren heute alle mit einer sicheren Ende-zu-Ende-Verschlüsselung, egal ob WhatsApp, Signal, Threema oder Telegram. Hier kann niemand mitlesen.

Auch die Betreiber nicht. Wenn es nun eine gesetzliche Vorgabe gibt, im Bedarfsfall mitlesen zu können, dann ginge das nur, wenn die Verschlüsselung geschwächt wird – und zwar erheblich. Entweder, die Betreiber haben eine Hintertür, haben auch den Schlüssel oder sie müssen auf den Endgeräten – also zum Beispiel auf unseren Smartphones – die Nachforschungen anstellen, das wird dann „Client Side Scan“ genannt. |

In jedem Fall ist die Kommunikation aber nicht mehr sicher. Denn solche „Hintertüren“ könnten nicht nur missbraucht werden – etwa von Staaten wie Ungarn –, sondern würden auch missbraucht werden. Hacker und Betrüger würden schon einen Weg finden. Das Vertrauen wäre komplett verschwunden. Es gibt keine sichere Kommunikation mit Backdoors. Punkt.

Jede Kritik berechtigt

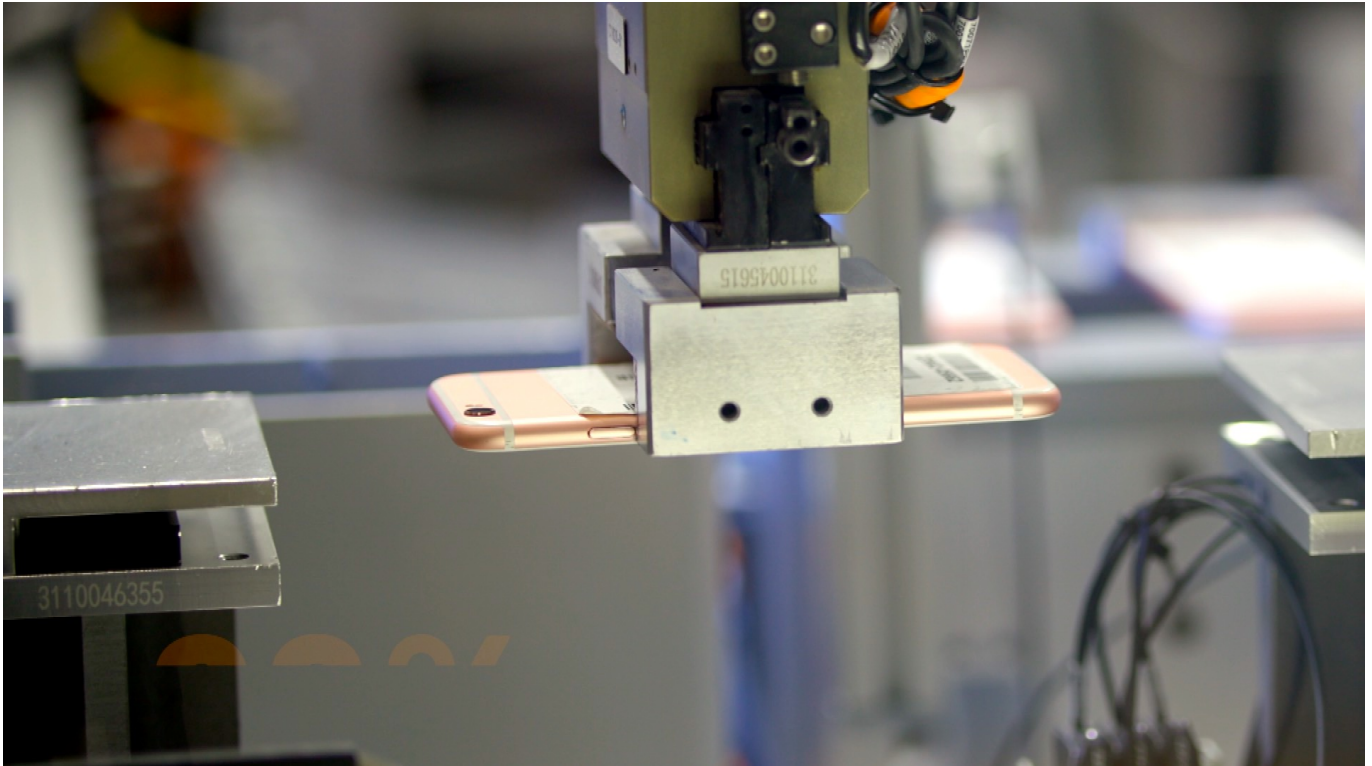
Bürgerrechtler und Netzaktivisten gehen auf die Barrikaden.

Die Ziele sind absolut unterstützenswert, daran gibt es ja gar keine Frage. Da muss man auch als normaler Bürger mal Einschränkungen oder Unbequemlichkeiten, logisch. Aber was hier vorgelegt wird, ist ein Datenschutz-Albtraum. Es scheint mir dilettantisch geplant, politisch inkompetent und miserabel durchdacht. Denn so wie das vorgestellt wurde, kann das nur Widerstand bedeuten. Die Zerstörung der Vertraulichkeit verschlüsselter Kommunikation in toto ist schon ein viel zu hoher Preis.

Aber dann kommen noch die Risiken des Missbrauchs dazu: Wenn solche Mechanismen erst einmal etabliert sind, würden sie garantiert auch missbraucht. Oder die Menschen würden es zumindest ständig annehmen, was auch nicht besser ist. Selbst Ermittler sagen: Wir brauchen nicht mehr Hinweise, sondern die Richtigen. Ganz abgesehen davon, dass Polizei und vor allem Justiz besser ausgestattet werden müssten, um die Arbeit zu machen. Gut gemeint ist nicht gut gemacht und der Zweck heiligt nicht die Mittel. Leider sind die Werkzeuge, die die

EU-Kommission da ausgewählt hat, fast alle aus dem Giftschränk. Viel besser wäre es, zum Beispiel die Anstrengungen beim Löschen solcher Inhalte entschieden voranzutreiben.

Recycling-Roboter „Daisy“: 20 Sekunden pro Altgerät



Wer Klimaschutz will, muss auch an das Thema Recycling von Smartphones ran. Hersteller Apple will bis 2030 komplett klimaneutral sein. Der Recycling-Roboter „Daisy“ kann alte iPhones innerhalb von 20 Sekunden komplett zerlegen.

Auf einem gut abgeschirmten Firmengelände im niederländischen Breda steht in einer entlegenen Arbeitshalle die Roboteranlage „Daisy“: Mehrere Greifarme, die in ruckartigen Bewegungen völlig ermüdungsfrei immer wieder dieselben Aufgaben erledigen. Daisy zerlegt blitzschnell ein altes iPhone in alle Einzelteile. Eine Art Anti-Montage, die präzise, schnell und effizient erfolgt – und das Recycling verbessert.

Nur zwei „Daisys“ gibt es auf der Welt: Ein Modell steht in Austin, Texas – das andere in Breda in den Niederlanden.

Daisy kennt 20 verschiedene Modelle

Alte, von Kunden eingesandte oder zurückgegebene iPhone-Modelle werden vorab mit einem Barcode gekennzeichnet. Damit Daisy „weiß“, um welches Modell es sich handelt. Daisy kann 20 Modelle zerlegen – und kennt alle dazu nötigen Handgriffe. Das kann man wirklich so sagen, denn auch die Roboterarme von Daisy haben Greifarme. Zuerst wird das Altgerät geöffnet, dann das Display entfernt. Es folgen die Schrauben.

In einem zweiten Schritt wird das alte Handy quasi schockgefrostet – damit der Kleber bricht. Bei diesem Arbeitsschritt klopft Daisy den eigentlich verklebten Akku heraus, damit der keinen Schaden nimmt. Im dritten Arbeitsschritt schließlich demontiert Daisy alle Klein- und Einzelteile, etwa die „Taptic Unit“, die für das Vibrieren zuständig ist und wertvolle Magneten enthält. Aber auch Kameralinse, Lautsprecher, Platine, Speicher und was sich sonst so alles in einem Smartphone befindet werden fein säuberlich herausmontiert.

Rund 1,2 Million Geräte pro Jahr

Die Anlage sammelt alle Bauteile und trennt die Werkstoffe. Einige davon, etwa die „Taptic Unit“, werden später von einem zweiten Roboter bearbeitet („Dave“), der die Magneten aus den kleinen Modulen popelt. „Taz“ übernimmt andere Aufgaben, und gewinnt aus dem Recycling-Material seltene Erden zurück.

Nur etwa 20 Sekunden dauert das pro Gerät. Daisy kann 200 Altgeräte pro Stunde zerlegen. 1,2 Millionen Geräte im Jahr. Der Aufwand lohnt sich, denn die auf diese Weise sorgfältig getrennten Werkstoffe lassen sich mühelos wiederverwenden. In neuen Geräten. Und das macht Apple auch: Im neuen iPhone zum Beispiel kommen Magneten, Gold, Lötzinn und Plastik bereits nahezu zu 100% aus recyceltem Material.

Klimaneutralität: Enormer Spareffekt

„Wir wollen bis 2030 vollkommen klimaneutral sein und einen vollständigen Werkstoffkreislauf erreichen“, erklärt Sarah Chandler. Sie ist im Apple-Konzern für Nachhaltigkeit zuständig – und will mit Daisy zeigen, dass vollständiges Recycling möglich ist. Schon bald sollen auch iPads, Notebooks, iMacs oder Watches vollständig recycelt werden – anderenfalls lassen sich die ambitionierten Klimaziele nicht erreichen.

Wie sinnvoll ein lückenloses Recycling ist, beweisen die nackten Zahlen: Eine Tonne von Daisy recyceltes Material ersetzen 2.000 Erze aus einem Bergwerk. Der Einspareffekt ist riesig, insbesondere in punkto Energie, Wasser und CO2-Ausstoß.

Apple bietet sein Know-how und seine Technologie kostenlos an: Wollen anderen Hersteller oder Werkstoffverwerter ähnliche Anlagen bauen, erhalten sie von Apple lizenzfrei die Technologie. „Wir würden uns freuen, wenn möglichst viele aus der Industrie mitmachen“, erklärt Sarah Chandler.

Ein Problem verrät Sarah Chandler allerdings noch: Die Menschen geben ihre Geräte noch viel zu selten zurück. Studien schätzen, dass allein in Deutschland 200 Millionen Altgeräte in den Schubladen liegen. Wertvolle Ressourcen. Deshalb hat Apple ein „Trade-In“-Programm: Wer sein Altgerät zurück gibt, erhält dafür Geld. Wie viel das ist, hängt vom jeweiligen Gerät ab.

Wir brauchen mehr Cyber-Resilienz



In Düsseldorf treffen sich die Digitalminister der G7-Staaten. Neben vielen anderen Aspekten steht angesichts des Angriffskriegs Russlands auf die Ukraine auch das Thema „Cyber-Resilienz“ im Fokus. Ein Begriff, den wir viel zu selten hören - aber sehr wichtig ist.

Die Digitalminister der G7-Staaten wollen über viele Aspekte der Digitalisierung sprechen: Neben der Frage, wie die Digitalisierung einen zukunftsweisenden Beitrag zu Klimaschutz und Nachhaltigkeit beitragen kann und wie sich die Digitalisierung so gestalten lässt, dass sie den gemeinsamen Werten und Bedürfnissen offener und demokratischer Gesellschaften entspricht, steht auch und vor allem das Thema Cyber-Sicherheit auf dem Programm.



Hybrider Krieg: Militär und Cyberangriffe

Hintergrund ist der Angriffskrieg Russlands auf die Ukraine. Ein hybrider Krieg: Die offenkundigen militärischen Operationen werden durch Propaganda (auch und vor allem im Netz) sowie gezielten Cyberangriffen begleitet. Russischen Hackergruppen werden zahlreiche Hackaktionen zugeordnet, etwa den auf das Satellitennetzwerk Viasat, der kurz nach dem Angriff auf die Ukraine erfolgt ist und die Infrastruktur von Windrädern zur Folge hatte.

Es gibt diverse [russische Hackerverbände](#), die gezielt die IT-Infrastruktur von Regierungen, aber vor allem von Energieerzeugern angreifen – auch im Westen. Bundesinnenministerin Faeser hat aufgrund der aktuellen Bedrohungslage vor einer Woche öffentlich die Bevölkerung dazu aufgerufen, Notvorräte anzulegen – weil eine Beeinträchtigung der europäischen Stromnetzwerke nicht ausgeschlossen werden kann. Hackern könnte es gelingen, das fragile System anzugreifen und zu stören. Tagelange Stromausfälle hätten bei uns fatale Folgen.

Vorbauen durch Cyber-Resilienz

Experten wie Manuel Atug vom Chaos Computer Club (CCC) warnen eindringlich davor, und besser zu schützen und empfehlen deshalb dringend mehr **Cyber-Resilienz** – nicht nur in der Energie-Versorgung, sondern allgemein.

Gemeint ist damit, dass IT-Infrastruktur nicht nur ganz generell besser vor Cyberangriffen geschützt werden muss (Abwehr), sondern dass selbst bei einem erfolgreichen Angriff alles weitgehend normal und stabil weiterläuft. Das gilt natürlich ganz besonders für sogenannte „kritische Infrastruktur“.

Das ist bislang eher nicht der Fall. Die Liste erfolgreicher Cyber-Angriffe mit komplett ausgefallenen Systemen oder zumindest erheblichen Einschränkungen ist lang. Vor zwei Jahren hat an der Universitätsklinik Düsseldorf die Ransomware „DoppelPaymer“ gewütet – und tagelang Notaufnahme und Operationen behindert. Der Angriff hat sogar Menschenleben gekostet.

Städtische Verwaltung tagelang lahmgelegt

Auch die Rechnersysteme der Verwaltung gleich mehrerer Städte und Gemeinde wurden in den letzten Jahren teilweise komplett lahmgelegt: Selbst simpelste Behördenvorgänge konnten dann tagelang nicht mehr durchgeführt werden, weil die IT-Systeme der Stadt durch Ransomware lahmgelegt wurde.

All das sind Beispiele für mangelnde Cyber-Resilienz: Selbst vergleichsweise einfache Ransomware-Angriffe sorgen für komplettes Chaos. Oft sind nicht nur einzelne Server betroffen, sondern gleich mehrere – oder sogar alle. Es fehlt an Konzepten, wie in solchen Situationen vorgegangen werden soll. Es braucht Rückfallsysteme, die in solchen Situationen zum Einsatz kommen – und solide Backups wichtiger Daten, die nicht ebenfalls verseucht oder verschlüsselt sein dürfen.

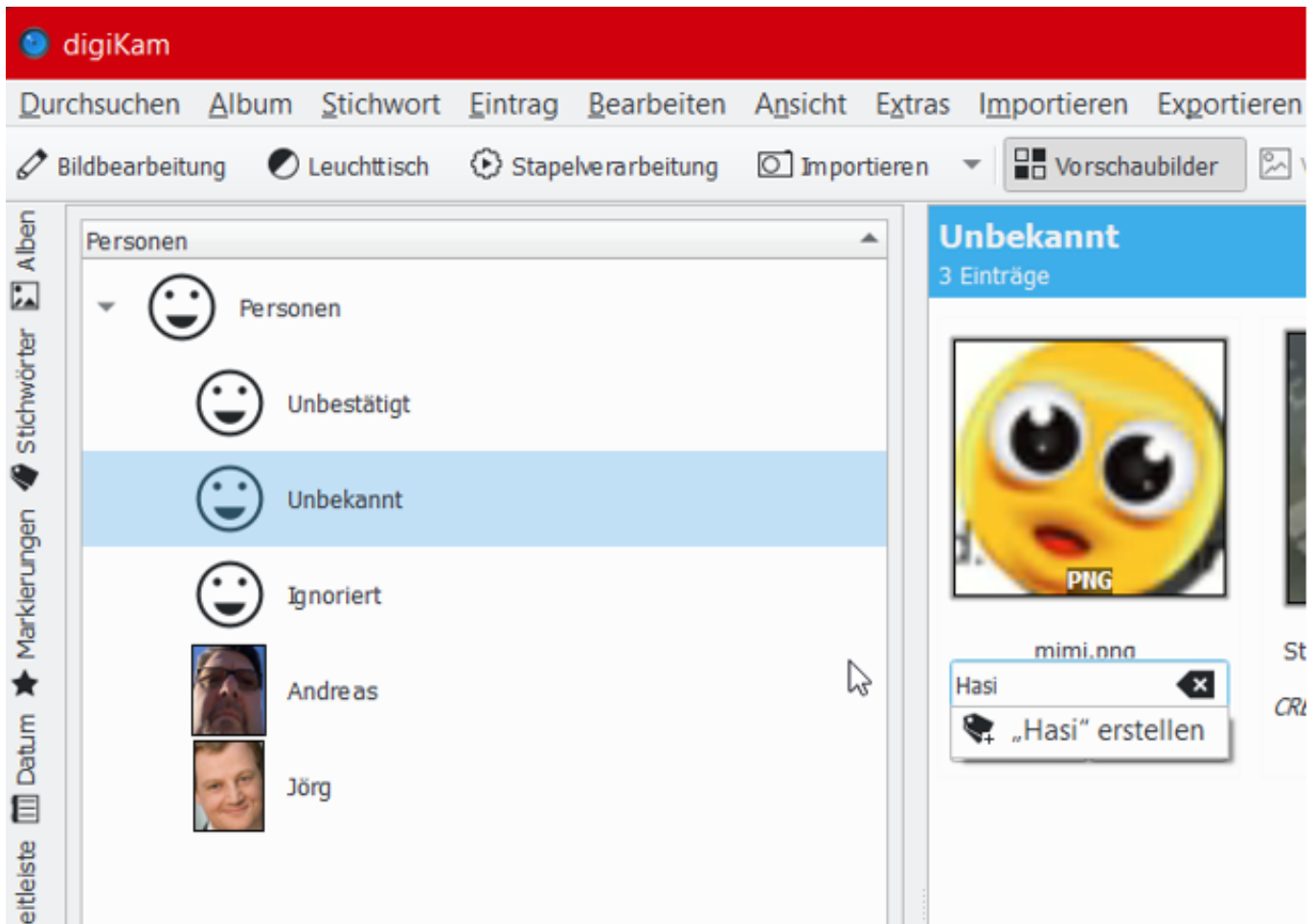
Alle, die mit IT-Sicherheit betraut sind, müssen umdenken. Es braucht aber auch möglicherweise entsprechende Vorschriften, um Behörden, Unternehmen und Institutionen zu zwingen, entsprechende Vorbereitungen zu treffen.

DigiKam: Tagger-App für Fotos



Fotos haben noch einige andere Eigenschaften als normale Dateien. Beispielsweise sind der Ort und die Personen darauf wichtig, was bei einer Excel-Tabelle eher nicht der Fall ist. Die kostenlose App [digiKam](#) ist da eine tolle Unterstützung!

Nach der Installation folgt der erste Einrichtungsvorgang, und hier solltet Ihr auf eine Einstellung achten: Die App speichert die Tags in einer eigenen Datenbank. Das ist schön, nutzt Euch aber eben nur in der App selbst etwas. Darum aktiviert im Dialog **Informationen zu Dateien hinzufügen**. Dann schreibt die App Eure Infos in die EXIF-Daten der Bilder, sodass sie auch in anderen Apps nutzbar sind!



1. Die App verwendet im Standard den Bilder-Ordner aus den Bibliotheken. Das könnt Ihr ändern, indem Ihr unter **Einstellungen > digiKam einrichten** weitere Ordner hinzufügt.
2. Es dauert einen Moment, bis alle Bilder in der Voransicht angezeigt werden, weil die App erst einmal die Ordner durchsuchen und die Miniansichten der Bilder laden muss.
3. Als Erstes markiert alle Bilder und klickt dann mit der rechten Maustaste hinein. Klickt dann auf **Nach Gesichtern suchen**. Die App analysiert jetzt die Bilder und weist Ihnen Gesichter zu, sortiert dabei gleiche Gesichter zueinander. Klickt ein Bild an, dann könnt Ihr ihm eine Person zuweisen.
4. Bei neuen Bildern wird die Person automatisch zugeordnet, wenn sie dem ersten Bild nur halbwegs ähnlich sieht.
5. Ebenfalls über die rechte Maustaste könnt Ihr einem Bild eine **Stichwörter zuweisen**. Stichwörter sind nichts anderes als Tags.
6. Auch Markierungen wie Bewertungen und Kategorien könnt ihr hier vergeben.

Das Programm hat eine unglaubliche Vielzahl von Funktionen. Wenn Ihr viele

Bilder verarbeitet, dann nehmt Euch ein wenig Zeit, um es kennenzulernen.

Elon Musk will Donald Trump zu Twitter zurückholen



Der reichste Mensch der Welt, Elon Musk, will Twitter kaufen. Und umgestalten. Aber wie genau? Vielen macht es Sorge, dass ein einzelner Mensch eine so wichtige Plattform besitzt – und Kontrolle über die Meinungsfreiheit bekommt. Jetzt hat Musk sogar angekündigt, den von Twitter verbannten Ex-Präsidenten Donald Trump wieder ins Netzwerk zu lassen.

Die Chefetage von [Twitter hat dem Verkauf zugestimmt](#). Elon Musk zahlt 44 Mrd. Dollar für [Twitter](#). Kein Bargeld, sondern mit Aktienanteilen und Krediten. Und auch nicht alleine, Elon Musk hat über sieben Milliarden von Investoren eingesammelt, die sich an dem Deal beteiligen wollen. Eins scheint aber klar: Elon Musk, der ja auch Tesla gegründet hat und leitet, wird Chef des Ganzen und will das Unternehmen von der Börse nehmen, damit er Twitter alleine leiten kann.

Ob das so kommt, ist sehr wahrscheinlich, aber nicht 100% sicher. Es gibt einige Stolpersteine: Bekommt er das Geld zusammen? Machen die Twitter-Aktionäre am Ende einen Rückzug? Gibt es möglicherweise Behörden, die Schwierigkeiten machen? Es sieht nicht danach aus, aber alles ist möglich. Es sind aber definitiv mehrere große Investoren dabei, der ehemalige Chef der Softwarefirma Oracle etwa oder saudische Prinzen.

Es ist also nicht ganz so, dass ein Mann alleine eine Plattform kauft. Die Großinvestoren werden sicher auch mitreden wollen.



Kritik an Elon Musk wird lauter

Nun gibt es eine Menge Kritik daran, dass ein Mann alleine das Unternehmen führen will. Dabei kündigt er doch an, sich für mehr Meinungsfreiheit einzusetzen.

Das Problem, das viele sehen: Wollen wir auf einer [Plattform](#) unterwegs sein, auf der ein Mann mehr oder weniger alleine bestimmt, was im Rahmen der Meinungsfreiheit geht? Werden wirklich alle alles sagen dürfen, wie Elon Musk ankündigt, der von einer „maximalen Meinungsfreiheit“ spricht – auch Verschwörungswurpler, Nazis, Islamisten und Linke? Es gibt keine Freiheit ohne Regeln.

Und es gibt keine Freiheit ohne gegenseitiges Verständnis, sagt Albert Camus. Eine solche Ankündigung wie die von Musk kann einem also Sorgen bereiten. Abgesehen davon gibt es selbstverständlich Regeln, in Deutschland das [NetzDG](#),

in Europa künftig der „Digital Services Act“, der Playern wie Twitter klare Auflagen machen. Natürlich darf eine öffentliche Plattform wie Twitter nicht machen was sie will. Wenn Mitglieder dort gegen Regeln verstoßen, muss das Netzwerk einschreiten – auch wenn Elon Musk das nicht will. Aber ansonsten drohen hohe, empfindliche Strafen. Es kostet Geld. Das ist dann eine Sprache, die auch Elon Musk versteht. Deshalb sollte man die Ankündigungen vielleicht auch nicht zu ernst nehmen.

Kommt Donald Trump zurück zu Twitter?

Jetzt hat Elon Musk angekündigt, den wegen zahlreicher Fehltritte aus Twitter verbannten Ex-Präsidenten Donald Trump wieder reinzulassen.

Die Entscheidung, Trump von Twitter zu verbannen, sei "moralisch falsch und einfach nur dumm" gewesen, kritisierte Musk bei einer Veranstaltung der "Financial Times". Es gibt viele, die seine Meinung teilen. Ich denke auch: Nicht eine Plattform sollte entscheiden, wer gebannt werden darf und wer nicht. In diesem Punkt hat Elon Musk Recht.

Aber die Tatsache, dass er wie selbstverständlich selbst entscheiden möchte, macht das eigentliche Problem deutlich: Elon Musk will auf Twitter regelrecht regieren. Er ist die Instanz. Er entscheidet. So ist das auch bei Tesla. Da wirft er schon mal gerne Journalisten raus, etwa vom ZDF, die unangenehme Fragen stellen. Elon Musk ist also unberechenbar – und entscheidet willkürlich. Keine guten Nachrichten für eine öffentliche Plattform wie Twitter.



Donald Trump könnte 2024 wieder kandidieren

Doch würde Trump überhaupt zurück wollen – er hat doch ein eigenes Netzwerk am Start?

Noch sagt Donald, der 80 Millionen Follower auf Twitter hatte und zweifellos zu einem dem wichtigsten User des Netzwerks gehörte, er wolle gar nicht zurück. Aber sein eigenes Netzwerk, das sich „Truth Social“ nennt, ist ein Flop: Kaum einer will in dieses Netzwerk, das zudem mit vielen technischen Problemen zu kämpfen hat. Da viele davon ausgehen, dass Trump erneut 2024 für die Präsidentschaft kandidieren dürfte, könnte es anders kommen: Trump wird jede Möglichkeit nutzen, Aufmerksamkeit zu bekommen. Wenn das auf Twitter am besten funktioniert, wird er wieder zu Twitter gehen. Keine Frage.


Duplikate entfernen in Excel



Excel-Tabellen können riesig werden. Da lassen sich Doppelerfassungen von Daten manuell schwer ausschließen. Die gute Nachricht: Excel kann dabei helfen!


Bevor die Daten in Excel verarbeitet werden, steht der mühsame Schritt an: Die Erfassung der Daten. Oft stammen diese aus irgendwelchen Quellen, die nicht im Einfluß des Benutzers stehen. Ebenso häufig sind die Quelldateien ellenlang und kaum manuell zu kontrollieren. Schnell schleichen sich Dopplungen ein, Datensätze, die irgendwo versehentlich zweimal erfasst wurden. Die lassen sich automatisiert von Excel entfernen.

Daten
Überprüfen
Ansicht
💡
Sie wünschen




Geografie


A ↓
Z ↓




Sortieren




Filtern



Löschen



Neu anwenden

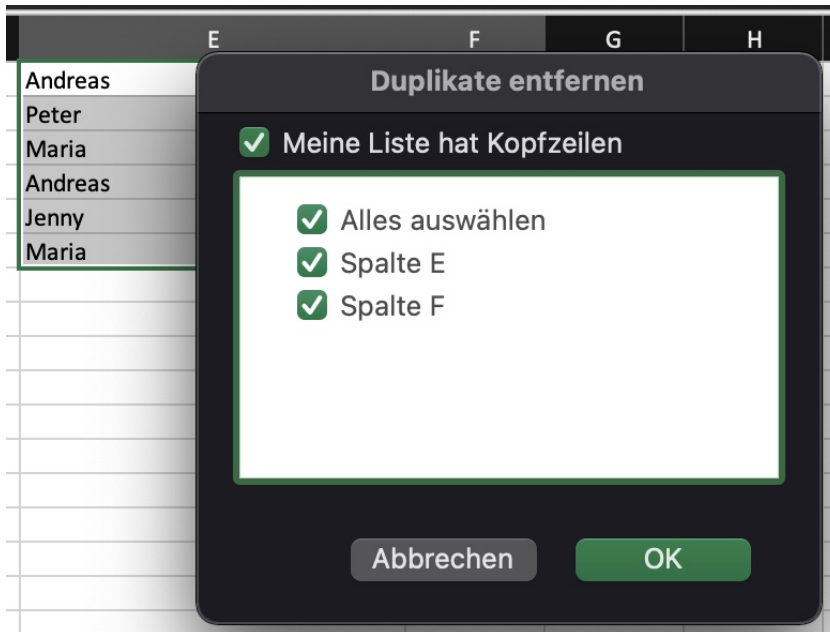


Erweitert

	E	F	G	H
	Andreas	12		
	Peter	23		
	Maria	55		
	Andreas	15		
	Jenny	36		
	Maria	55		

Markiert dazu in der Tabelle die Zellen, die untersucht werden sollen. Wichtig dabei: Wenn Eure Daten mehrere Spalten enthalten, dann müsst Ihr eine Entscheidung treffen: Wenn es Euch um den kompletten Datensatz geht, der überprüft werden soll, dann markiert alle Datenzeilen und gleichzeitig alle Spalten darin.

Im Beispiel kommen sowohl "Andreas" als auch "Maria" doppelt vor. Würdet Ihr nur die Spalte mit den Namen markieren, dann würden beide als Dopplungen entfernt werden. Wird die Spalte mit der Punktzahl hinzugenommen, dann hat nur Maria einen doppelten Eintrag!



Klickt in Excel in der Registerkarte **Daten** auf **Duplikate entfernen**. Solltet Ihr den Eintrag nicht finden, dann vergrößert das Fenster: Ist es zu schmal, dann werden einzelne Optionen nur als kleine Symbole angezeigt!

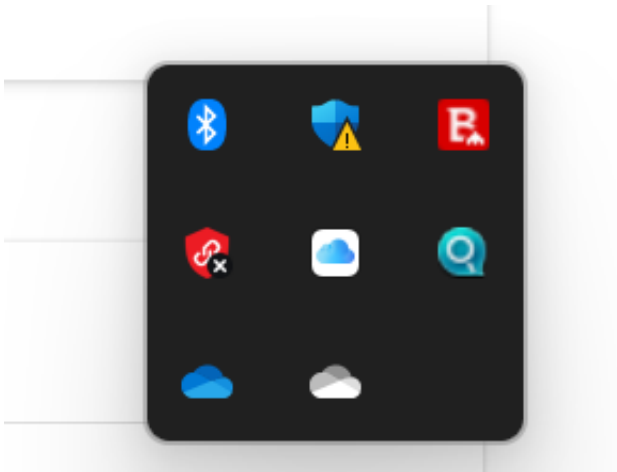
Wenn Eure Daten keine Überschriften enthalten, dann entfernt den Haken neben **Meine Liste hat Kopfzeilen**. Ein Klick auf OK startet das Entfernen von Dopplungen. Am Ende zeigt Excel Euch eine Zusammenfassung an, wie viele Dopplungen entfernt wurden.

Warnung im Windows Defender auflösen



Windows hat mit dem [Defender](#) einen Basisschutz gegen Bedrohungen vorinstalliert. Normalerweise merkt Ihr den nicht, dann zeigt das Symbol plötzlich ein gelbes Ausrufezeichen an und damit ein Problem. Löst es mit wenig Aufwand!

Die Meinungen gehen auseinander, ob der Windows Defender eine zusätzliche Antiviren-Software ersetzen kann. Eines aber ist unstrittig: Er schützt recht gut vor Bedrohungen wie Viren, Firewall-Angriffe und andere Bedrohungen werden in den meisten Fällen von ihm abgefangen. Es macht also absolut Sinn, auf eine Warnung zu reagieren.



Klickt doppelt auf das Schild mit dem Ausrufezeichen im Benachrichtigungsbereich der Taskleiste oder klicken in den Einstellungen von Windows auf **Datenschutz und Sicherheit > Windows Sicherheit**.



Windows zeigt Euch die einzelnen **Schutzbereiche** an. Das Warnsymbol aus dem [Benachrichtigungsbereich](#) findet Ihr dann an einer oder mehreren

Kategorien. Klickt die Kategorie an.

Windows zeigt jetzt die Detailinformationen der Schutzkategorie an und darin auch die Änderung die Ihr vornehmen müsst, um die Warnung wegzubekommen. Das können ganz unterschiedliche Dinge sein: Aktualisieren des Virenschutzes, Verifikation der Kontoinformationen Eures Microsoft-Kontos, eines haben diese Fehler aber gemeinsam:

Windows führt Euch detailliert durch die Behebung des Fehlers. Nach einem Neustart Eures PCs sollte dann alles wieder in Ordnung sein und die Warnung nicht mehr auftreten.

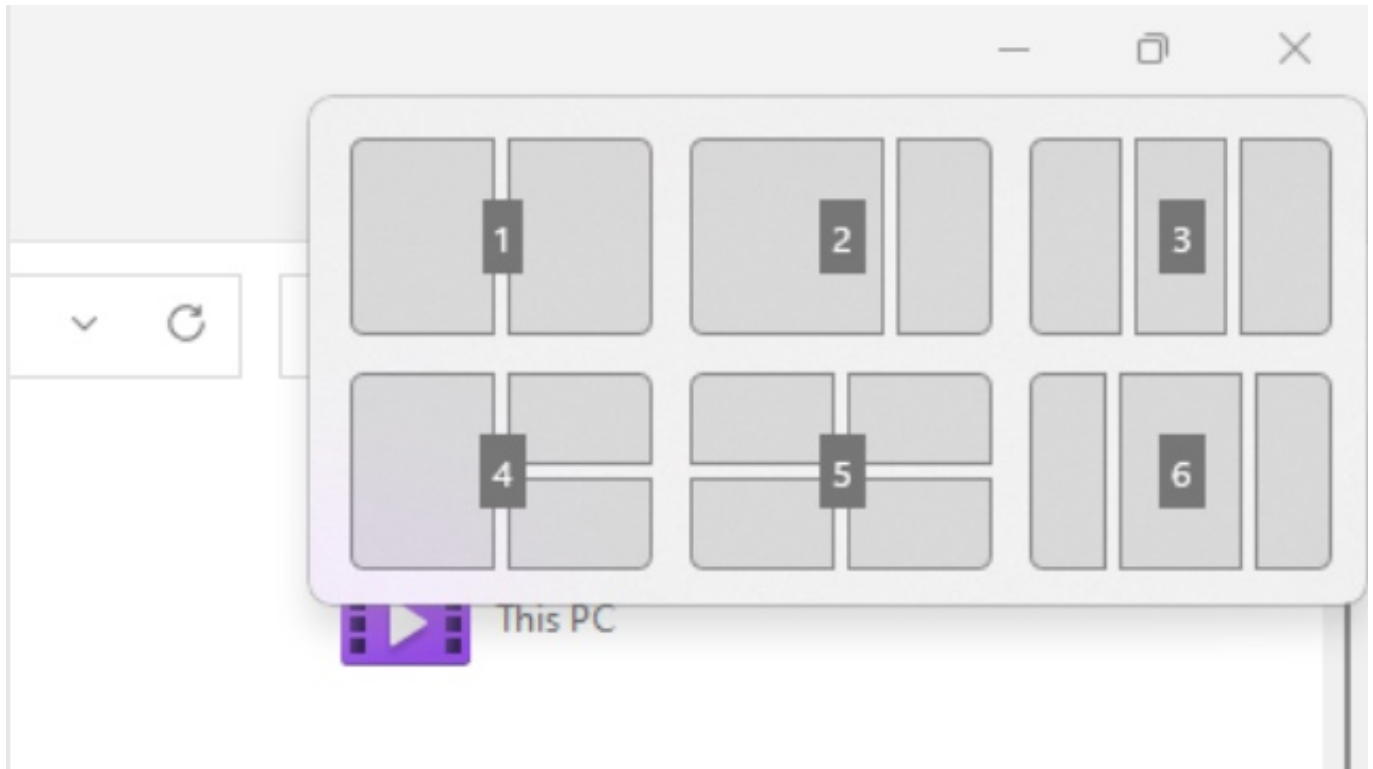
Neue Snap-Layouts für Windows 11



Je mehr Programme offen sind, desto mehr Fenster wollen verwaltet werden. Die Snap-Layouts von Windows 11 helfen dabei. Jetzt ist die Funktionalität nochmal erweitert worden.

Auf dem stationären PC habt Ihr meistens mehr als einen Monitor, aber auch der reicht nicht, um alle Fenster sichtbar zu haben

Diese müsst Ihr einmal aktivieren, indem Ihr unter Einstellungen auf **System** > **Multitasking** > **Fenster andocken** die beiden Optionen mit **Snap-Layouts** im Text aktiviert.



Um ein Fenster in ein solches Layout einzuordnen, bewegt den Mauszeiger im betroffenen Fenster auf die **Maximieren-Schaltfläche**. Windows 11 zeigt jetzt verschiedene Schablonen an, in die die Fenster eingeordnet werden können. Für jedes Element der Schablone zeigt das System eine Übersicht der offenen Fenster an. Klicken Sie darin jeweils das Fenster an, das an diese Position und Größe geschoben werden soll.

Das wird sich jetzt noch einmal verbessern: Wer über das [Windows Insider-Programm](#) Vorabversionen bekommt, der kann jetzt schon die - im Standard etwas hakelige - Funktion der Snap-Layouts per Tastenkombination nutzen. Drückt dazu einfach **Windows + Z**, dann könnt Ihr über die Zifferntasten das gewünschte Layout aussuchen. Das geht schneller als der Weg über die Maximieren-Schaltfläche, wenn Ihr die Maus nicht gerade sowieso in der Hand habt.

Für die normalen Windows-Anwender wird die Funktionalität mit dem nächsten Update ausgerollt.