Schieb Report

Ausgabe 2019.41

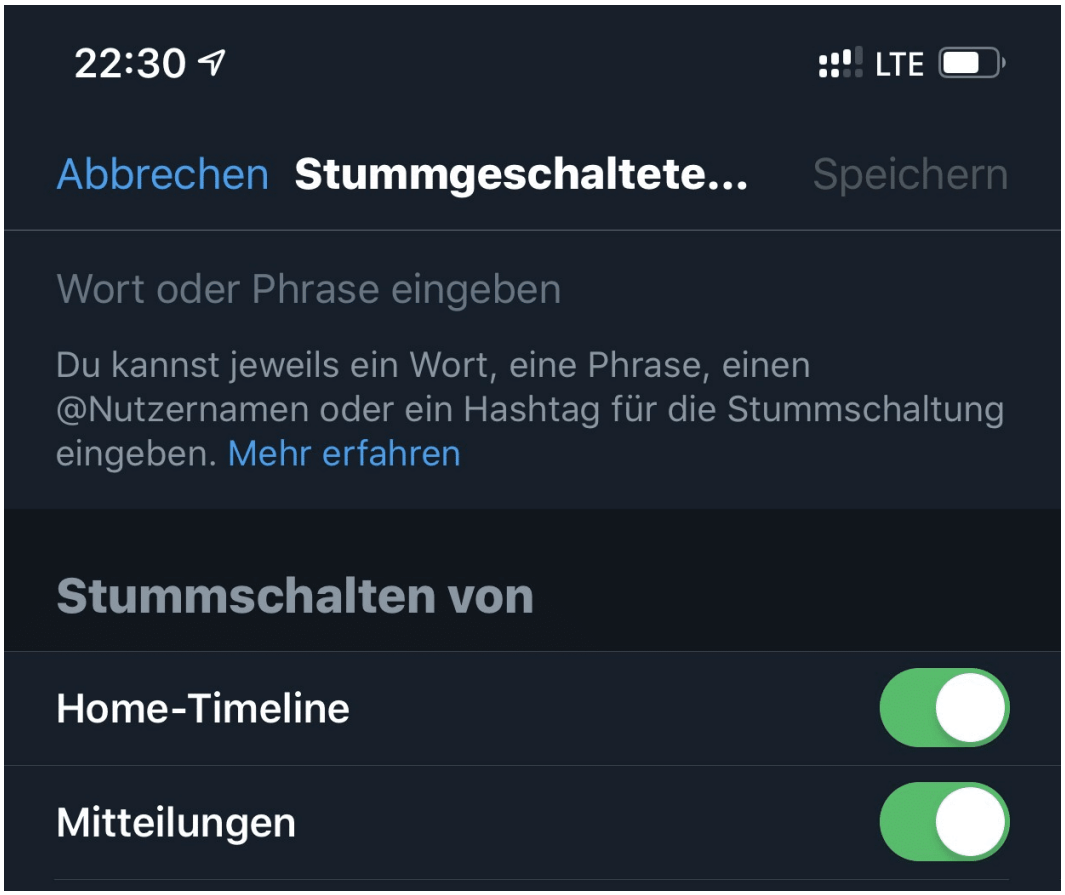
Bestimmte Begriffe in Twitter stummschalten

Das Internet hat viele Schattierungen, und neben den vielen schönen natürlich auch unschöne. Dazu gehört die schier unendliche Vielzahl an Themen und der Umgang damit, der nicht immer jedem Benutzer gefällt. Gerade unmoderierte Dienste wie Twitter, in denen quasi jeder schreiben kann, was er möchte, sind hier für den ein oder anderen Anwender ein Problem. Das muss nicht sein: Sie können beliebige Themen und Wörter ausblenden und in der Timeline ausgeblendet werden. Wir zeigen Ihnen, wie das geht.

Gehen Sie in Ihre Twitter-App auf dem Smartphone, tippen Sie auf Ihr Kontobild und dann auf **Einstellungen und Datenschutz**. Twitter selbst fragt in regelmäßigen Abständen nach, ob Sie eine solche Stummschaltung ausführen wollen, dann können Sie natürlich auch direkt auf dieses Banner klicken.

Aktivieren Sie den **Qualitätsfilter**, um Twitter eine Vorauswahl von unangemessenen Posts machen zu lassen. Diese werden dann automatisch ausgeblendet. Das Risiko hierbei: Sie haben wenig Kontroller, ob nicht vielleicht doch ein Post dabei ist, der vielleicht interessant wäre. Besser ist hier die manuelle Nutzung von Filtern:

Tippen Sie auf **Stummgeschaltet** > **Stummgeschaltete Wörter**. Sie können nun unter **Hinzufügen** neue Wörter hinzufügen, die zu einer Ausblendung führen sollen. Wählen sie durch die Schalter aus, ob der Filter auf die **Home-Timeline** und/oder die **Mitteilungen** wirken soll.



Aber der Aktivierung verwendet Twitter die eingegebenen Begriffe automatisch, um Beiträge auszublenden und Sie nicht mehr zu belästigen.

Eine eigene Internetseite mit Instagram-Bildern anlegen

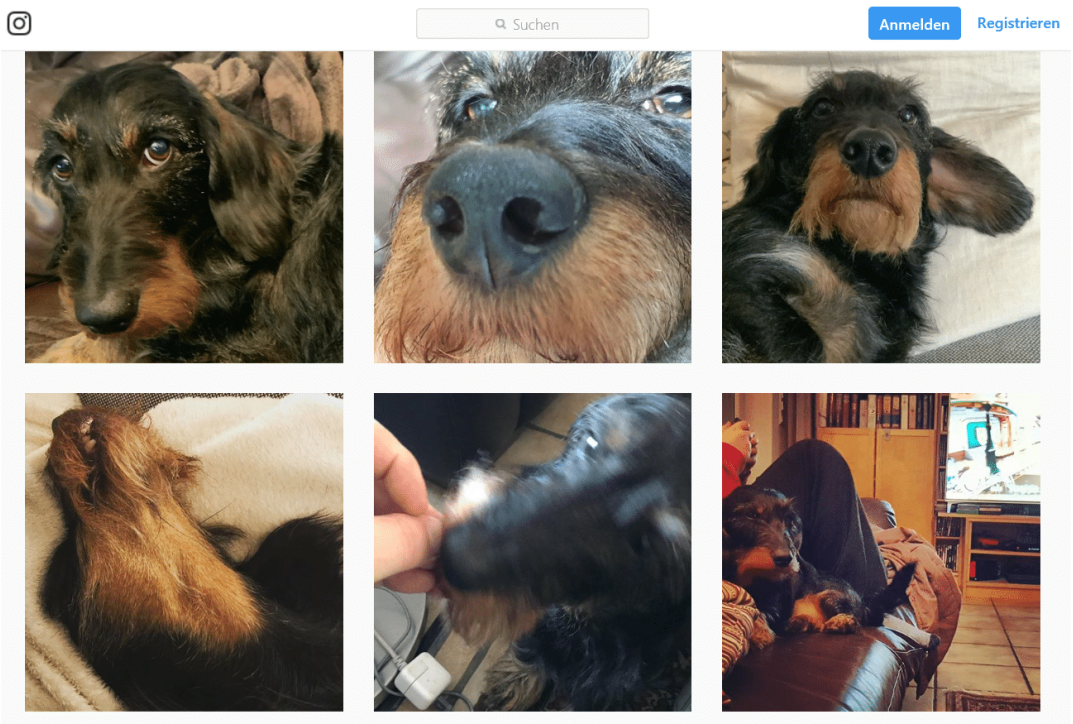
Eine eigene Internetseite ist für viele Privatanwender irgendetwas zwischen Luxus und unnötig. Sie nutzen soziale Netzwerke, laden dort Kommentare und Bilder hoch. Weitere Inhalte für eine Webseite haben Sie aber nicht. Die Kombination der beiden Themen kann aber reizvoll sein: Wenn Sie Bilder auf Instagram beispielsweise per Hastags kategorisieren, dann können Sie im Handumdrehen eine Webseite daraus machen.

Überlegen Sie sich einen passenden Hashtag, der noch nicht existiert und den Sie jedem der Fotos, das Sie zum Thema auf Instagram hochladen, geben. Alle Beiträge zu einem Hashtag bekommen Sie unter der Adresse

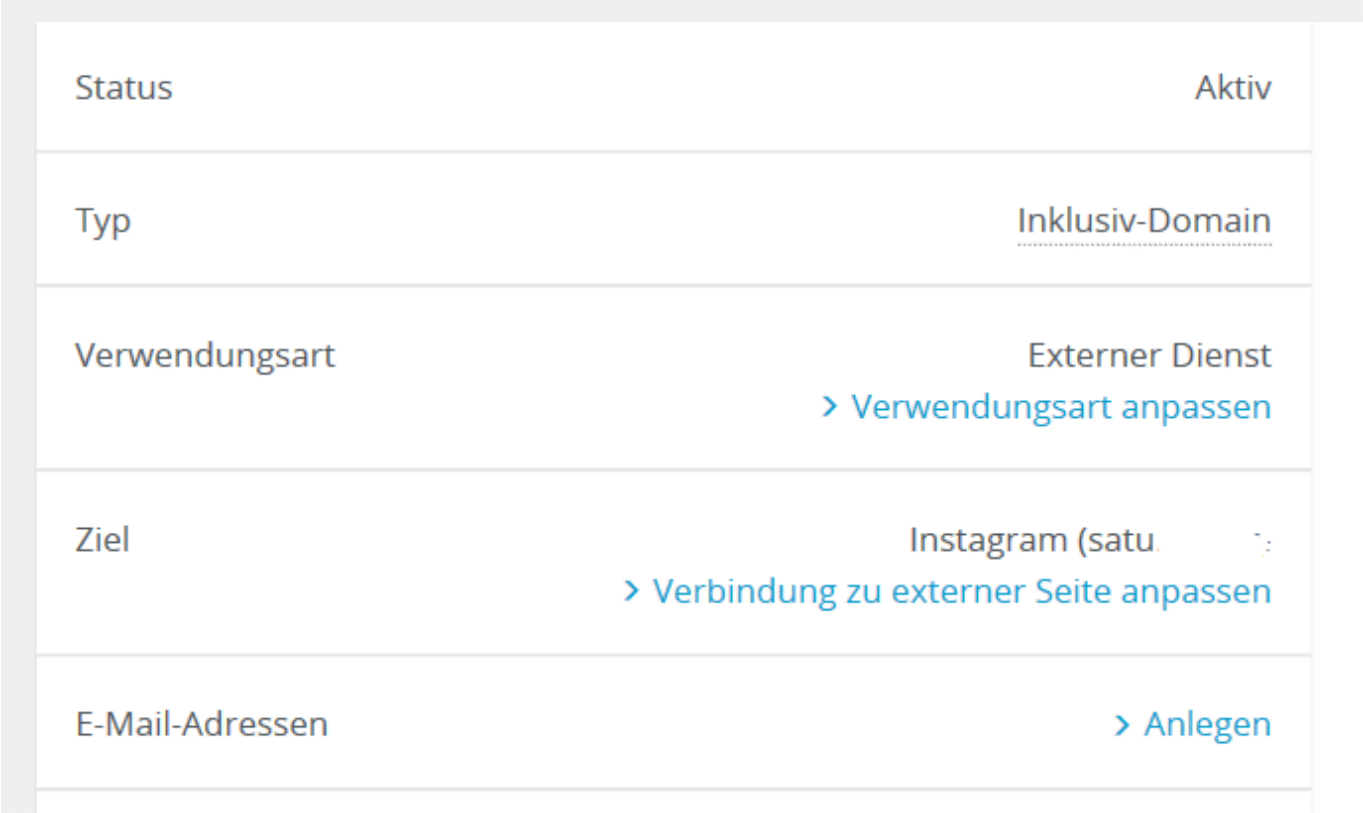
http://www.instagram.com/explore/tags/

wobei sie den letzten Teil natürlich mit dem echten Hashtag ersetzen müssen.

Wenn Sie sich nun eine Internetadresse besorgen, wie es 1und1, GMX, Strato und andere anbieten, dann können Sie hinter der Adresse die Instagram-URL mit Ihrem Hashtag hinterlegen.



Dazu gehen Sie in die Konfigurationsoberfläche Ihrer Webseite. In den Einstellungen zur Domain können Sie entweder **Externer Dienst** oder **Weiterleitung** einstellen. Damit verweist die Internetadresse nicht auf einen eigenen Webspace, sondern leitet bei Aufruf an die Instagram-Seite weiter. Geben Sie als Ziel dann die URL mit Ihrem Hashtag ein. Schon sind Ihre Bilder in ansprechender Form unter der angegebenen Adresse erreichbar. HTML-Kenntnisse oder einen eigenen Webspace brauchen dafür nicht.


Status
Aktiv
Typ
Inklusiv-Domain
Verwendungsart
Externer Dienst
Verwendungsart anpassen
Ziel
Instagram (satu
Verbindung zu externer Seite anpassen
E-Mail-Adressen
Anlegen

Textkorrekturen unter iOS 13

Das Schreiben auf einem Smartphone ist auch mit zierlichen Fingern eine Herausforderung: Die Tasten auf der Bildschirmtastatur liegen eng beieinander. So kann es schnell passieren, dass Sie sich vertippen und die Autokorrektur nicht automatisch eingreift. In iOS 13 hat Apple hier einige Veränderungen in der Bedienung der Tastatur vorgenommen. Wir zeigen Ihnen wie Sie trotzdem schnell Fehler korrigieren können.

Die iOS-Tastatur hat keine Cursortasten. Damit ist es auf den ersten Blick schwierig, den Cursor an die Stelle im Text zu schieben, an der der Fehler steht. In älteren iOS-Versionen zeigte das iPhone eine Lupe an, wenn Sie den Finger länger auf eine Textpassage gehalten haben. Unter iOS 13 ist das nicht mehr der Fall. Allerdings ist das Verfahren identisch: Halten Sie den Finger auf den Text, dann ziehen Sie den Finger leicht nach unten. Sie sehen nun den Cursor und können ihn mit dem Finger an die richtige Stelle bewegen.

Wenn Ihr iPhone kein Force-Touch mehr hat (was ja auch die neue iPhone 11-Serie trifft), dann fällt vermeintlich die Möglichkeit der Nutzung der Tastatur als Touchpad weg. "Vermeintlich" deshalb, weil die Funktion auch unter iOS 13 noch vorhanden ist: Halten Sie den Finger länger auf der Leertaste (statt, wie bisher, auf einem beliebigen Bereich der Tastatur), dann können Sie durch Bewegen des Fingers wie auf einem Touchpad den Cursor frei im Text bewegen.


Ich
Ja
Die

Löschen/Anpassen der Eigenschaften von Dokumenten

Sie haben viel Aufwand in die Entwicklung eines Dokumentes gesteckt. Die Excel-Tabelle, die mit einer Menge an Formeln und Logik Zauberdinge vollbringt. Oder die Word-Vorlage, die mit Makros und Formatierungen den Geschäftsbericht mit wenig zusätzlichem Aufwand zu neuem Glanz verhilft. Solche Dateien wollen Sie sicherlich gerne auch bei anderen Gelegenheiten verwenden. Allerdings soll nicht sichtbar sein, wo diese vorher schon eingesetzt wurden. Darum stellen Sie sicher, dass die Dateien von allen Metainformationen bereinigt werden!

Die Idee ist gut, die Auswirkungen, wenn Sie den Hintergrund nicht kennen, können aber katastrophal sein: Die Office-Programme speichern neben dem Namen des Dokumentes, der ja offen sichtbar ist, noch eine Vielzahl weiterer Informationen. Beispielsweise den Namen und das Unternehmen des Autors, Datum und Uhrzeit von Erstellung und Veränderung, welche Vorlage der Ersteller verwendet hat etc. All diese Informationen ziehen sich oft über Generationen hinweg: Der erste Anwender erstellt die Datei. Damit füllt Office initial die Meta-Informationen. Der gibt sie weiter, es werden Veränderungen vorgenommen, und so weiter. Die Metainformationen bleiben aber in der Datei.

Irgendwann sind diese komplett falsch, ja sogar gefährlich. Steht in den Metainformationen ein Unternehmen, das nicht das eigene ist, dann kann man Ihnen sogar Diebstahl intellektuellen Eigentums unterstellen. Die Lösung: Löschen Sie die Eigenschaften einfach, oder passen Sie sie an. Klicken Sie dazu die Datei mit der rechten Maustaste im Explorer an, dann wählen Sie die Registerkarte **Details**. Windows 10 zeigt Ihnen nun eine Vielzahl von Informationen an. Ändern Sie diese, indem Sie hineinklicken und den neuen Wert über die Tastatur eingeben. Wenn Sie alle löschen wollen, dann klicken Sie auf **Eigenschaften und persönliche Informationen entfernen** ganz unten.

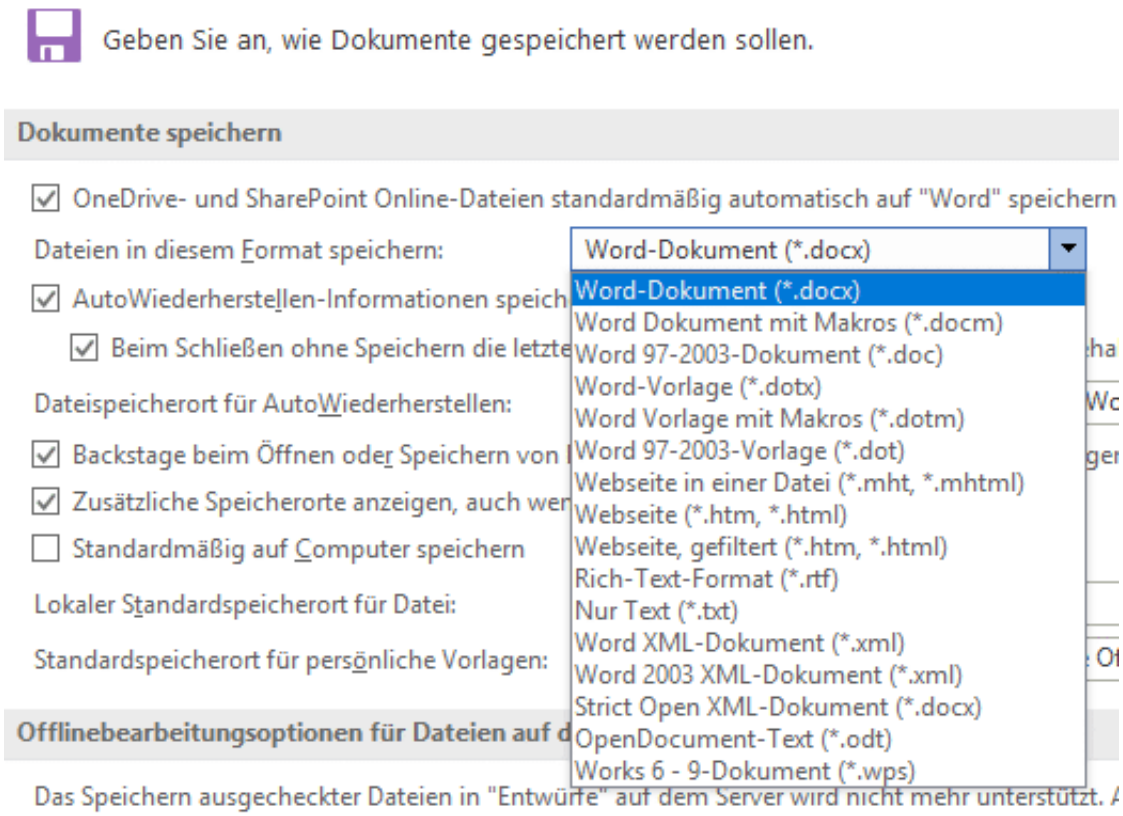
Maximale Kompatibilität bei Word-Dokumenten sicherstellen

Word ist immer noch das verbreitetste Programm zur Textverarbeitung. Die meisten anderen Programme orientieren sich an seinen Funktionen und versuchen, möglichst Dokumente zwischen den Programmen austauschbar zu halten. Wenn Sie eine Datei nur als Information versenden, der Empfänger aber keine Bearbeitung durchführen muss, dann können Sie stattdessen das PDF-Format verwenden. Wenn Sie ein Word-Dokument versenden wollen, dann sollten Sie die folgenden Tipps beachten.

Word ist nicht gleich Word, und eine Word-kompatible Textverarbeitung auch nicht. Das merken Sie vor allem dann, wenn ein Dokument bestimmte Inhalte (wie Formatierungen, Schriftarten etc. mitbringt). Es kann schnell passieren, dass ein Dokument dann komplett unformatiert erscheint. Nur, weil eine Formatierung zwischen den Versionen der Textverarbeitung nicht übereinstimmt.

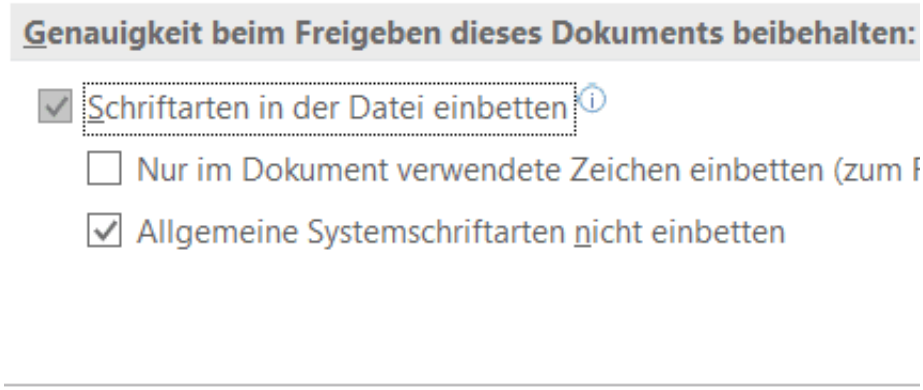
XML-Format vs. altes Format

Microsoft hat irgendwann eine Umstellung des Dokument-Formats der Office-Programme vorgenommen, zu erkennen an dem "x" in der Erweiterung. Aus .DOC wurde beispielsweise .DOCX. Auch wenn die Formate kompatibel zueinander sind: Je komplexer die Datei, desto eher gibt es Probleme in der Darstellung in einer alten Word-Version. Wenn Sie häufiger mit Benutzern Dateien austauschen, die eine alte Word-Version nutzen, dann stellen Sie das Format gleich auf das ursprüngliche Format um. Dazu klicken Sie in Word auf **Datei** > **Optionen** > **Speichern** und wählen Sie als Format **Word 97-2003-Dokument** aus.



Besondere Schriftarten

Eine Textverarbeitung lebt vom Text, und der wiederum von der Schriftart, in der Sie ihn darstellen. Normalerweise sind die Schriftarten Teil von Windows. Sie können aber zusätzliche Schriftarten installieren. Diese sind dann nur auf Ihrem Rechner vorhanden. Der Rechner des Empfängers kann sie im Standard nicht darstellen. Word behilft sich dann damit, die nicht vorhandene Schriftwart durch eine allgemeine zu ersetzen. Das sieht oft nicht schön aus. Dieses Problem können Sie leicht vermeiden: Aktivieren Sie unter **Datei > Optionen > Speichern** unter **Genauigkeit beim Freigeben dieses Dokuments beibehalten** die Option **Schriftarten in Datei einbetten**. Damit wird die Datei zwar leicht größer, der Empfänger kann sie aber auch korrekt anzeigen lassen, wenn er die Schriftart nicht selber installiert hat.

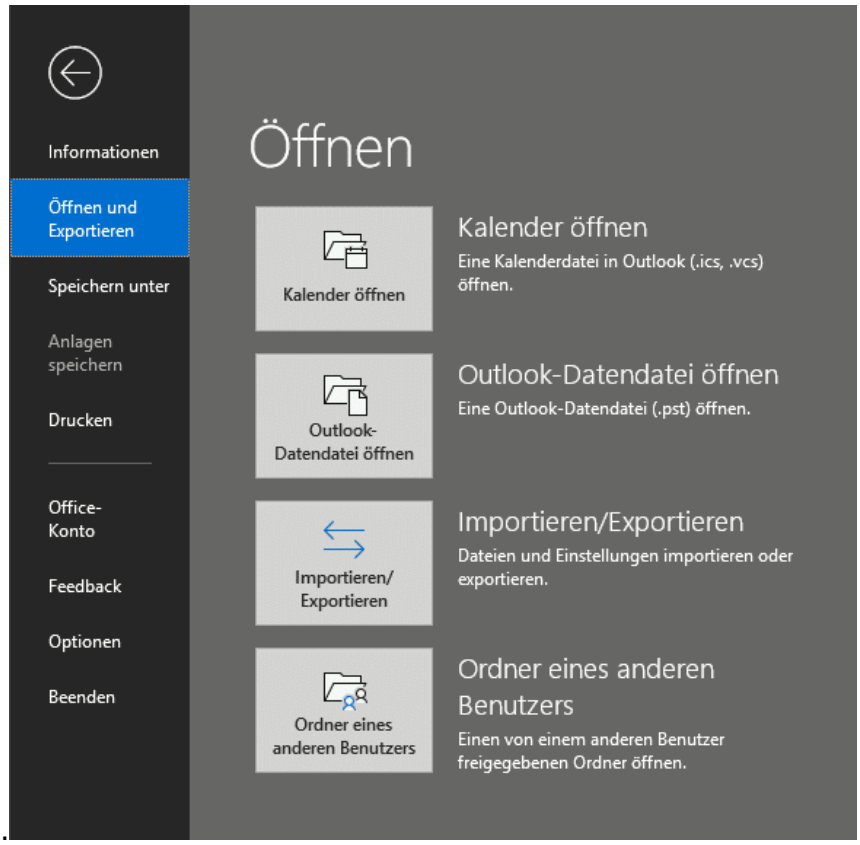


Der Backup der E-Mail-Daten aus Outlook

Ihre E-Mails sind schnell ein nicht mehr wegzudenkender Bestandteil Ihrer Arbeit. Wenn Sie noch ein lokal verwaltetes E-Mail-Konto haben, dann sollten Sie dringend daran denken, dieses regelmäßig zu sichern. Auch für den Umstieg auf ein Online-Postfach wie Office 365 benötigen Sie eine solche Sicherung. Über Microsoft Outlook ist diese schnell durchgeführt.

Der erste Schritt zum Transfer der Daten ist der Export aus Outlook in eine PST-Datei. Outlook verwendet dieses Format, um komplette Postfächer konsolidiert in einer einzigen Datei zu sichern und damit portabel zu machen. Allerdings haben die Produktverantwortlichen es konsequent in allen Versionen von Outlook geschafft, die Exportfunktion zu verstecken:

In Outlook müssen Sie unter **Datei** auf **Öffnen** > **Importieren** klicken



In dem sich nun öffnenden Dialog (der eigentlich dem Import dient) befindet sich eine Option "In Datei exportieren". Diese klicken Sie nun an und wählen **Outlook Datendatei (PST-Datei)** als Ziel.

Wichtig ist nun, die oberste Ebene des Postfaches auszuwählen, damit Sie nicht nur die E-Mails, sondern auch die Kontakte und Termine (so diese in dem zu exportierenden Konto vorhanden sind) miterfassen. Ebenso sollten Sie zwingend der Haken bei **Unterordner**

einbeziehen setzen, damit nicht nur der Posteingang, sondern auch die Ordner, die der Anwender darin angelegt hat, erfasst und mit kopiert werden.

Zum Abschluss müssen Sie den Namen und den Speicherort der Datei angeben. Beide sollten sinnvoll gewählt werden, um die Datei für den Import wiederzufinden. Je nach Größe des Postfaches dauert der Exportvorgang von einigen Sekunden bis zu einigen Stunden.

Problemfall Live-Videos: Können Einschränkungen helfen?

Der Attentäter von Halle hat seine Mordserie auf einer Video-Plattform live gestreamt - danach hat sie sich rasant verbreitet. Ein bekanntes Muster, das sich wiederholt - immer wieder. Das wirft die Frage auf, ob es hilfreich ist, dass jeder jederzeit alles streamen kann. Anonym. Ohne irgend eine wirksame Kontrolle.

Wer ein öffentliches Radio- oder Fernsehprogramm ausstrahlen möchte, braucht dafür eine Lizenz. Nicht nur, weil damit bestimmte Frequenzen belegt werden - das auch, zumindest war das früher relevant -, sondern vor allem, weil auf diese Weise sehr viele Menschen erreicht werden. Unmittelbar. Live. Damit ist eine enorme Verantwortung verbunden. Es gibt also nun wirklich sehr gute Gründe, wieso nicht jeder einen Radio- oder Fernsehsender starten und betreiben darf. Und wenn, dann gehen damit eine Menge Verpflichtungen einher.

Unhaltbar: Jeder kann jederzeit alles streamen

Heute ist das anders. Heute kann jeder einen Live-Stream auf Facebook, Youtube, Instagram, Twitter oder Twitch starten - und nicht nur jeden Unsinn daherreden, sondern auch hetzen oder terroristische Taten live übertragen. Das war bei den Anschlägen in Christchurch so. Und das war auch in Halle so. Auch aus Deutschland werden also mittlerweile Live-Streams in die Welt gejagt, die Gewalt und Terror zeigen.

Das wirft doch die Frage auf, ob es richtig sein kann, dass einfach jeder - völlig unkontrolliert - einen solchen Live-Stream starten darf. Jeder. Egal wie verrückt, egal wie kompetent, egal wie erfahren - und auch egal, mit welchem Ziel.

Terroristen und Täter wie in Halle sind dankbar für diese Möglichkeiten. Sie können so ihre Untaten bekannt machen. Das Öffentlichmachen ihrer Tat - sogar live! - ist ein erhebliches Tatmotiv. Sie werden "berühmt". Für immer mit der Tat verbunden. Das Netz vergisst nichts. Die Tätervideos sind nie wieder komplett aus dem Netz zu entfernen - bei aller Anstrengung, die unternommen werden mag.

Verhinderungsmechanismen können nicht wirksam greifen

Zwar hat es nach Christchurch geheißen, Facebook, Youtube und Co. wollten das Verbreiten von Kopien solcher Terrorvideos unterbinden. Schneller und effektiver. Es gab sogar einen "Christchurch Gipfel". Danach wurde das Global Internet Forum to Counter eingerichtet, das die rasante Verbreitung solcher Gewaltvideos bei Facebook, Twitch und Co. ausbremsen soll. Aber ob das wirklich gelungen ist, darf bezweifelt werden.

Auch stellt sich die Frage, ob es besser ist, ob - wie in Halle geschehen - das Video eines Augenzeugen etwas in den Sozialen Medien verloren hat. Ich finde: Nein. Niemals sollten Amateure entscheiden dürfen, was öffentlich zu sehen ist.

Leider sind First-Person-Shooter und Actionspiele heute von realen Bildern nicht mehr zu unterscheiden. Selbst KI ist nicht in der Lage, haben uns Experten bei Facebook im Cosmotech-Podcast erklärt, bei einem Live-Stream zu unterscheiden zwischen Fiktion (Game) und Realität (Christchurch, Halle). Wenn dem so ist, sollte es eben gar nicht erlaubt sein, live zu streamen. Denn wie unverantwortlich ist es, dass jeder jederzeit alles streamen kann?

Es darf auch nicht jeder hinters Steuer und Auto fahren. Warum darf jeder streamen? Es darf nicht jeder unterrichten. Wieso darf jeder streamen? Wir sollten darüber diskutieren, ob die vermeintliche "Freiheit", dass im Netz jeder jederzeit alles darf - zudem in der Regel anonym -, nicht doch ein erhebliches Problem ist.

Wenn ich Twitch wäre – ich würde mich schämen, dass über meinen Kanal solche Bilder verteilt werden. Und das nicht zum ersten Mal. Aber wer heute zu Twitch geht, findet keinerlei Hinweise, was eben erst Ungeheuerliches hier geschehen ist.

Anlässe wie die in Halle sind Grund genug, darüber zu diskutieren, welche Regeln es geben sollte. Im Augenblick haben wir keine. Das ist nicht gut.

https://soundcloud.com/user-999041145

Wenn Onlinedienste den Stecker ziehen

Ein Abschalten mit Ankündigung: Bis zum 29. Oktober haben Nutzer in Venezuela Zeit, ihre Daten aus der Cloud zu holen und lokal auf Festplatte zu speichern. Fotos. Videos. Skizzen. Grafiken. Danach ist Schluss. Der Softwareriese Adobe – bekannt zum Beispiel für seine Foto-Software Photoshop – sperrt ab dem 29. Oktober für Bürger aus Venezuela den Zugang zu ihren in der Cloud gespeicherten Daten – und sogar den zu den Apps. Weil die US-Regierung das anordnet. Aus politischen Gründen. Und das ist kein Einzelfall.

Fangen wir mit dem Fall Adobe an. Adobe sperrt User aus Venezuela aus der Cloud aus.

Es gibt schon lange einen erbitterten politischen Streit zwischen den USA und Venezuela. Jetzt hat die US-Regierunter unter Präsident Donald Trump durch die Exekutivanweisung 1883 alle Geschäfte mit Venezuela strikt untersagt. Personen, Unternehmen, Organisationen aus den USA dürfen keine Transaktionen mehr durchführen.

Deshalb hat Adobe allen Kunden in Venezuela die Zusammenarbeit aufgekündigt: Ab dem 29. Oktober gibt es keinen Zugriff mehr auf die „Creative Cloud“, wo Künstler, Redakteure, Fotografen ihre Arbeiten, Skizzen, Foos etc. ablegen, wenn sie mit Programmen wie Photoshop, Illustrator, Lightroom, InDesign oder Adobe arbeiten. Bestehende Abos dürfen nicht verlängert werden, bereits gezahlte Gebühren nicht erstattet. Früher oder später werden dann auch die Apps nicht mehr funktionieren, weil die Abos nicht mehr verlängert werden können. Einfach ausgeknipst – von heute auf morgen.

Kein Einzelfall: Es weitere Beispiele

Die US-Regierung hat auch untersagt, mit dem chinesischen Hersteller Huawei zu kooperieren. 5G baut Mobilfunktechnik, etwa für 5G, ist aber auch ein riesiger Smartphone-Hersteller. Deshalb hat Google die Partnerschaft mit Huawei aufgekündigt. Es gibt kein Android und keine Google-Apps mehr für Huawei-Smartphones. Das hat sogar Folgen für bestehende Kunden, die ihre Apps nicht mehr aktualsieren können. Einfach, weil es der US-Präsident anordnet. Von heute auf morgen.

Eine ganz schöne Abhängigkeit. Wenn man das weiterdenkt, könnten wir doch praktisch überall betroffen sein – wir speichern doch immer mehr in der Cloud.

Allerdings: Microsoft Office zum Beispiel läuft heute auch als Abo-Modell, in der Cloud. Also Word, Excel, Powerpoint. Viele speichern ihre Dokumente in der Microsoft-Cloud, OneDrive. Sollte Trump auf die Idee kommen, auf Europa böse zu sein, hätte das katastrophale Folgen: Die Büroprogramme ließen sich vom einen auf den anderen Moment nicht mehr benutzen. Der Zugriff auf die Daten wäre blockiert, zumindest bei Daten, die auf US-Servern gespeichert sind. Ein Desaster. Oder wenn Google seine Dienste verweigert, die Apps sperrt, die Kalender blockiert – auch das hätte schlimme Folgen. Ja: Wir sind abhängig.

Umdenken - und weniger abhängig machen

Wenn man sieht, wie einfach die US-Regierung mal eben Apps ausknipst oder Zugänge sperrt, sollten wir unbedingt umdenken.

Es wäre sehr wichtig, dass wir uns unabhängig – oder wenigstens weniger abhängig – machen von US-Unternehmen. Gar nicht so einfach, da diese überall präsent sind. Wir merken es nicht mal: Behörden speichern Daten auf Servern von Google, Amazon oder Microsoft. Fatal!

Es müssten europäische Cloud-Lösungen her. Diese müssten in bestimmten Bereichen bevorzugt oder ausschließlich genutzt werden. Es müsste auch transparent sein für alle User,

wo genau Daten und Apps gespeichert sind. Das Ausfallrisiko müsste deutlich gemacht werden. Die kritische Infrastruktur – Banken, Verkehr, Geld, Sicherheit – müsste frei sein von solchen Abhängigkeiten.

Ein schönes Beispiel ist Linux. Das Server-Betriebssystem ist auf den aller meisten Servern weltweit im Einsatz – in der ein oder anderen Form. Das gehört keinem Konzern. Es werden keine Lizenzen gezahlt. Da kann niemand einen Stecker ziehen. Das funktioniert sehr gut.

Auch der Erfinder des Web, Tim Berners-Lee, hat einige Ideen, wie man das Netz wieder dezentraler organisieren könnte – und damit unabhängiger machen könnte. Jeder einzelne User hätte dann auch mehr Kontrolle über seine eigenen Daten, ein angenehmer Nebeneffekt. Aber es bräuchte den politischen Willen, derartige Strukturen zu bevorzugen oder sogar vorzuschreiben – davon sind wir derzeit meilenweit entfernt. Leider. Die Politik sieht das Problem nicht und handelt auch nicht. Obwohl Trump jederzeit den Stecker ziehen könnte – im wahrsten Sinne des Wortes.

Ein Gundrecht auf Verschlüsselung?

Nachrichten zu verschlüsseln ist eine gute Idee: Auf diese Weise können Fremde, Kriminelle oder Geheimdienste nicht "mithören". Zum Glückl ist das Verschlüsseln von Nachrichten heute sehr einfach, zumindest beim Messenger. Doch einige Regierungen wollen Hintertüren vorschreiben.

Früher war es eine positive Eigenheit von Threema, Signal, Telegram und Co., dass hier alle ausgetauschten Nachrichten konsequent Ende-zu-Ende-verschlüsselt wurden. Heute ist das auch bei WhatsApp Standard.

Facebook hat angekündigt, die Verschlüsselung sogar weiter auszubauen - und auch im Facebook Messenger und bei Instagram zu installieren. Eine gute Nachricht für alle, die sich beim Nachrichtenaustausch nicht gerne über die Schulter schauen lassen. Denn Ende-zu-Ende-Verschlüsselung bedeutet: Hier können selbst die Anbieter nicht schnüffeln. Auch Facebook nicht.

Staaten fordern Zugriff auf Kommunikation

Die USA, Großbritannien und Australien fordern aber nun erneut eine Hintertür in der Verschlüsselung. Ganz offiziell. Mit dem Argument, Behörden wie Polizei und Geheimdienste müssten in bestimmten Fällen Zugang zur Kommunikation haben. Etwa, um Kinder vor Gewalt

und sexuellem Missbrauch zu schützen. Auch deutsche Innenminister fordern das immer wieder.

Ein perfider Trick, denn wer wollte da "Nein!" sagen, wenn es darum geht, Kinder vor Gewalt zu schützen. Oder Kinderporno-Ringe aufzudecken.

Natürlich ist es ein enormes Problem für Polizei und Behörden, wenn Kommunikation kinderleicht und von jedem sicher verschlüsselt werden kann. Selbst Terroristen müssen sich heute nicht mehr die Mühe machen, seltene Software zu installieren, um sicher verschlüsselt zu kommunizieren. Jeder kann es. Selbstredend ist das eine enorme Belastung für die Behörden. Das ist gar keine Frage.

Allerdings: Warum sollte Verschlüsselung und damit das Abwehren von Spionage - etwa durch fremde Staaten, dem eigenen Staat oder Kriminelle - nur einigen Wenigen vorbehalten sein?

Jede Hintertür wird auch missbraucht

Eine Hintertür nur für die Guten gibt es nicht. Wenn es eine Hintertür gibt, dann wird sie auch missbraucht. Etwa von Konzernen wie Facebook, die dann - wenn es rauskommt - von einem Versehen sprechen. Von Kriminellen. Von Staaten. Die Tatsache, dass sogar die USA nach so einer Hintertür schreien, darf wohl als Beleg dafür gewertet werden, dass selbst die NSA Schwierigkeiten hat, in der verschlüsselte Kommunikation vorzudringen.

Apropos NSA: Es ist eben diese Behörde, die einen erheblichen Grund für das Sicherheitsbedürfnis darstellt. Schließlich haben die NSA und damit die USA praktisch jeden, anhaltslos und illegal bespitzelt. Da dürfen sich die Schnüffelstaaten nicht wundern, wenn die Menschen nach geeigneten Mitteln suchen, um sich zu wehren.

Es gibt zwar kein internationales Grundrecht auf verschlüsselte Kommunikation. Aber vielleicht sollte das mal diskutiert werden. Unbescholtene Bürger sollten nicht bespitzelt werden dürfen - und ein Recht auf unbeobachtete Kommunikation haben. Das ist natürlich in Unrechtsstaaten besonders wichtig.

https://vimeo.com/269831761

Amazon kann auch Gesichtserkennung

Die Leute stellen sich immer mehr Alexa-Geräte zu Hause hin. Klar, denn vieles davon ist praktisch - aber ist es auch sicher? Eher nicht. Vor allem, wenn man weiß, dass Amazon auch Gesichtserkennung kann. Manche Alexa-Geräte sind mit Kameras ausgestattet. Die Regeln für Gesichtserkennung formuliert der Onlineriese gerade sogar selbst.

Amazon nur ein Onlineshop? Von wegen. Jeff Bezos' Konzern streckt seine Tentakeln in alle Richtungen aus. Dass Amazon über eine eigene KI-Software zur Gesichtserkennung verfügt, weiß kaum jemand: AWS Recognition heißt der Dienst.

Jeder kann den Service bei Amazon buchen. Als Cloud-Lösung - für wenige Euro im Monat. Wer das System mit Fotos füttert, kann von der KI-Software im Blitztempo Gesichter in Fotoaufnahmen oder sogar Videos erkennen (lassen). Recognition funktioniert tadellos: Ich habe es ausprobiert. Sie erkennt Gesichter, schätzt das Alter, verrät ob die Person auf dem Foto lächelt oder glücklich ist - und vieles mehr. Die KI-Software für die eigenen Zwecke zu nutzen, ist vergleichsweise einfach.

Auch Amazon kann nach Gesichtern suchen

Das Beispiel zeigt, wie einfach es heute ist, nach Gesichtern zu suchen. Die entsprechenden

Funktionen liegen in der Cloud bereit - für vergleichsweise kleines Geld. Einige Polizeibehörden in den USA nutzen diesen Service bereits, etwa in Florida oder Oregon. Das System leistet gute Hilfe bei der Fahndungsarbeit. Die Behörden laden also Fotos bei Amazon hoch, um andere Fotos oder möglicherweise sogar Live-Video-Streams auf bekannte Gesichter zu durchforsten.

Nicht ganz ohne Beigeschmack, finde ich, wenn einer der größten Datensammler der Erde - der gerade erst diverse neue Alexa-Geräte vorgestellt hat, um an noch mehr Daten zu kommen -, von Behörden frei Haus mit Gesichtsdaten versorgt wird.

Zwar will niemand unterstellen (ich auch nicht), dass sich Amazon als Konzern bei seinen Cloud-Diensten bedient. Aber: Wer weiß... Wir haben in der Branche schon so manches erlebt. Außerdem gibt es immer wieder Sicherheitslecks. Misstrauen schadet also nicht.

Was es braucht, sind klare Regeln - vor allem bei einem so sensiblen Thema wie der Gesichtserkennung. Das sieht sogar Amazon-Chef Jeff Bezos so.

> "Gesichtserkennung ist ein perfektes Beispiel für etwas, das wirklich positive Auswirkungen hat, so dass man es nicht bremsen will', fügte Bezos hinzu. 'Aber gleichzeitig gibt es auch Potenzial für einen Missbrauch der Technologie, so dass man Vorschriften will."
> Jeff Bezos

Amazon arbeitet selbst an den Regulierungen

Aber was macht Amazon? Formuliert nun selbst Regeln und sogar potenzielle Gesetze zur Regulierung. Allen Ernstes: Amazon schreibt gemeinsam mit Microsoft auf, wie die Regeln aus ihrer Sicht aussehen sollten. Das ist so, als würde ich dem Finanzminister aufschreiben, wie ich mir eine gerechte Steuerpolitik vorstelle (Journalisten sind von der Steuerpflicht befreit!), oder wenn ich meiner Stadt die Parkregeln diktieren könnte. Schön wäre das schon. Aber würde man mich lassen? Wohl eher nicht...

Große Konzerne aber haben mehr Erfolg darin, Politiker zu "überzeugen". Wie genau die Regeln aussehen sollen, die Amazon da ausarbeitet, ist nicht bekannt. Für Amazon typisch wäre aber: Es ist alles erlaubt, was technologisch geht und dem Unternehmen Profit bringt. Nur bei extremem Widerstand oder strengen Regulierungen ändert sich was.

Was sagt nun Amazon dazu? Ich wollte es natürlich wissen. Doch - wie leider immer bei Amazon - gab es nichts, auch kein Gespräch, nur ein Link auf einen Blogeintrag. Das muss dann aber auch wirklich reichen.

https://vimeo.com/364783887

Wer ist noch echt? KI erzeugt Gesichter und Porträtaufnahmen

Wenn wir Werbeanzeigen sehen – egal ob in der Zeitung, im Internet oder im Fernsehen –, dann ist uns klar: Da wird uns was vorgemacht. Wir sehen Models, die begeistert sind, sich freuen, schick und fröhlich aussehen. Aber: Es sind immerhin Menschen. Oder? Na, da kann man sich nicht mehr so sicher sein. Denn immer häufiger sind nicht mal die Menschen echt. Sie kommen heute oft aus der Retorte. Besser: Aus der KI.

Dass KI Gesichter erkennen kann, darüber haben wir hier ja bereits gesprochen. Aber nun kann KI auch Gesichter erzeugen

Künstliche Intelligenz wird tatsächlich verstärkt dazu eingesetzt, um Porträtaufnahmen von Menschen zu erzeugen. Man könnte auch sagen: zu faken. Denn die KI erstellt Porträtaufnahmen von Menschen, die wirklich täuschend echt aussehen. Es gibt praktisch keinen Hinweis darauf, dass die auf dem Foto gezeigte Person nicht existieren könnte. Wer sich davon selbst überzeugen möchte, geht mal auf die Webseite thispersondoesnotexist.com. Hier wird jedes Mal – in genau dem Moment! – ein neues Porträtfoto erzeugt und gezeigt. Die Person gibt es garantiert nicht!

Aber wie ist das möglich? Wie kann KI solche wirklich verblüffend echt aussehenden Fotoaufnahmen generieren?

Täuschend echt aussehende Porträts

Das ist die Stärke von KI: Man füttert die Software mit Hunderten, Tausenden von Fotos – davon gibt es im Internet ja reichlich. Die KI analysiert die Aufnahmen und erstellt Regeln, wie menschliche Gesichter aussehen: Wie sehen Augen aus, wo sitzt die Nase, wo der Mund – und das alles in verschiedenen Blickrichtungen und bei unterschiedlichen Kamerapositionen.

Wenn genügend Datenmaterial verfügbar ist, kann die KI-Software aus diesen Vorlagen blitzschnell neue Fotos zusammensetzen: Die Augen von Person A, mit der Augenfarbe von Person B, mit dem Silberblick von Person C, mit der Brille von Person D, mit der Nase von Person E, dem Lächeln von Person F und der Frisur von G – und so weiter. Dann werden noch Aspekte mit Licht, Schatten etc. perfekt berechnet – fertig ist das Porträtfoto einer Person, die es gar nicht gibt.

Wissenschaftler haben den Täuschungseffekt untersucht

Und das lässt sich wirklich nur schwer erkennen - auch wenn das schwer vorstellbar ist.

Das haben zwei Wissenschaftler von der University Washington untersucht. Sie wollten wissen: Können die User mühelos echte von falschen Aufnahmen unterscheiden? Unter www.whichfaceisreal.com kann jeder den Test selbst machen: Zwei Fotos sind zu sehen – eins ist echt, eins aus der KI. Der Besucher muss sich nur entscheiden, welche der beiden Aufnahmen er für echt hält. Danach erfährt man auch gleich, ob man richtig gelegen hat... So viel kann ich schon sagen: Es ist fast unmöglich. Statustisch gesehen denkt mindestens die Hälfte der Menschen, dass die unechten Fotos echt sind.

Einsatz in der Werbung

Aber was macht man mit solchen Fake-Gesichtern? In der Werbung einsetzen?

Zum Beispiel. KI-Porträts sind ideal geeignet für Werbung im Netz. Werber bekommen so unverbrauchte Gesichter, die garantiert noch nirgendwo sonst zu sehen waren – und täuschend echt aussehen. Außerdem kosten sie nichts, es gibt keinen Ärger, weil man die Aufnahmen für bestimmte Zwecke einsetzt – nur Vorteile also. Unter generated.photos kann sich jeder eine Datenbank mit 100.000 KI-Gesichtern kostenlos herunterladen und die Aufnahmen nutzen. Das ist nur ein Anfang.

Da liegt der Verdacht nahe, dass es auch Missbrauch gibt. Die Aufnahmen werden natürlich immer besser. Sie werden eingesetzt, um Fake-Profile bei Facebook und Co. echt aussehen zu

lassen. Der nächste Schritt sind dann von KI erzeugte Gesichter in Videos. Das ist natürlich deutlich schwieriger. Aber es ist nur eine Frage der Zeit, bis auch das geschafft ist. Bedeutet für uns: Wir können nichts mehr glauben. Alles ist Fake. Unecht. Virtuell.

Datenkrake Amazon

Amazon – kennen wir alle. Da gibt es einfach alles zu kaufen: Ob Schuhe, Bücher, Spülmaschinen-Tabs, Möbel, Lebensmittel... Doch Amazon ist längst viel mehr als nur der größte Onlineshop der Welt. Der Konzern ist eine Macht im Bereich der Medien.

Jeff Bezos ist der Mann, der Amazon erfunden hat – und jetzt sogar zum Mond will. Bezos ist es gelungen, Amazon zum mit Abstand größten Onlineshop der Welt zu machen. Mehr als das: Für die meisten von uns ist Amazon so eine Art Suchmaschine für Kaufprodukte. Wer etwas kaufen will, schaut erst mal hier nach, ob es das gibt – und was es kostet. Und: Kauft oft auch gleich hier.

Kein Monopol - aber fast: Alle anderen haben es schwer

Amazon hat kein Monopol – aber doch fast.

Alle anderen Anbieter haben es jedenfalls richtig schwer, gegen diese Übermacht anzukommen. Das liegt unter anderem daran, dass Amazon seine Kunden besser kennt als jeder andere Onlineshop – und sie deshalb optimal ansprechen kann.

Um es klar zu sagen: **Amazon ist einer der eifrigsten Datensammler der Welt**. Amazon sammelt ständig Daten. Nicht nur, wenn man etwas kauft. Es reicht schon, wenn man etwas sucht. Oder sich etwas anschaut.

Eine, die sich mit diesem Thema besonders gut auskennt, ist die Datenschützerin Katharina Nocun. Sie hat intensiv recherchiert, wie Amazon funktioniert – und welche Daten beim Einkaufen und Stöbern auf Amazon anfallen. Es sind jede Menge sensibler Daten.

Katharina sagt: „Ich kann das in einem Satz zusammenfassen. Und zwar: Amazon speichert jeden Klick, den Nutzer machen. Also alles, was ich jemals auf dieser Plattform gemacht habe, hat Amazon gespeichert. Da sieht man alles.

Welche Suchanfragen ich gemacht habe, welche Bücher ich mir nur angeschaut habe, wann ich auf Bewertungen geklickt habe, wann ich mir Bewertungen genauer angesehen habe. Es ist wirklich eine Rundumprotokollierung von allem, was ich auf der Plattform mache. Und daraus lassen sich natürlich viele Sachen ablesen. Es ist eine Sache, was ich kaufe – aber es ist eine andere Sache, was ich recherchiere.“

> "Amazon speichert jeden Klick, den Nutzer machen."

Alexa und Echo sind ständig aktive Spione

Allerdings. Doch Amazon speichert einfach alles. Und mit Alexa hat Amazon einen weiteren Datenlieferanten. Wer mit Alexa spricht, versorgt Amazon mit Infos: Welche Fragen habe ich? Welche Interessen habe ich? Sogar wie es mir geht, erfährt Amazon. Denn Amazon hat ein Patent darauf, anhand der Stimme die aktuelle Stimmungslage zu erkennen. Oder Krankheiten zu erkennen. Ob diese Technik bereits zum Einsatz kommt, ist unbekannt.

„Ich möchte nicht, dass nebenbei ein psychologisches Profiling von mir gemacht wird. Und genau das ist aber mit solchen Daten möglich. Allein die Tatsache, wann ich wach bin, wann ich schlafe, wann ich besonders viel vergleiche, wann ich überlege, das kann eben auch zu anderen Zwecken benutzt werden. Und solche Klick-Streams zeigen eben auch, dass die Grenze zwischen Werbung und psychologischen Profiling immer weiter verschwimmt.“

Welche Daten hat Amazon denn nun genau?

Wer nachschauen will, welche Daten Amazon konkret so hat und speichert, hat es nicht leicht (demnächst veröffentliche ich eine genaue Bescbhreibung).

Doch Amazon baut die Palette an Alexa-Assistenten gerade aus. Demnächst sollen mit Echo Frame, Echo Loop und Echo Buds weitere Geräte auf den Markt kommen, die einen ständig mit Amazon verbinden – und dort Daten abliefern. Zum Beispiel diese Kopfhörer. Echo Buds.

Aber, die Kopfhörer sind eben auch ständig mit Amazon verbunden. So weiß Amazon auch noch, wo wir uns aufhalten. Was wir tun. Mit wem wir uns treffen...

Eine Idee: Wer mit den neuen Kopfhörern im Ohr durch den Supermarkt geht, kann fragen: Alexa: Wo sind die Tomaten?

Datan abgreifen im Alltag

Und Alexa sagt einem dann: Gehe nach vorne bis zum Obstregel, dann links abbiegen – vorne liegen die Bio-Tomaten, daneben die Cherry-Tomaten.

Das ist wirklich geplant. Erst mal in den Amazon-Lebensmitteln, die es schon gibt. Später aber möglicherweise auch in anderen Geschäften. Das bedeutet: Amazon erweitert seinen Aktionsradius bis in die physische Welt. hinein. Selbst dort, wo wir noch in echten Geschäften einkaufen, ist Amazon dann präsent.

Das Problem: Wer die neuen Echo-Produkte benutzt, der liefert nicht nur jede Menge Daten bei Amazon ab – oft, ohne es zu merken. Sondern macht Amazon noch mächtiger, als der Konzern ohnehin schon ist.

Ich habe Amazon übrigens um Stellungnahme gebeten. Amazon war zu keinem Gespräch bereit.

An Amazon als Onlineshop vorbeizukommen ist schwierig genug. Aber man muss sich ja nicht auch noch mit Technik versorgen, die Amazon noch mächtiger macht.

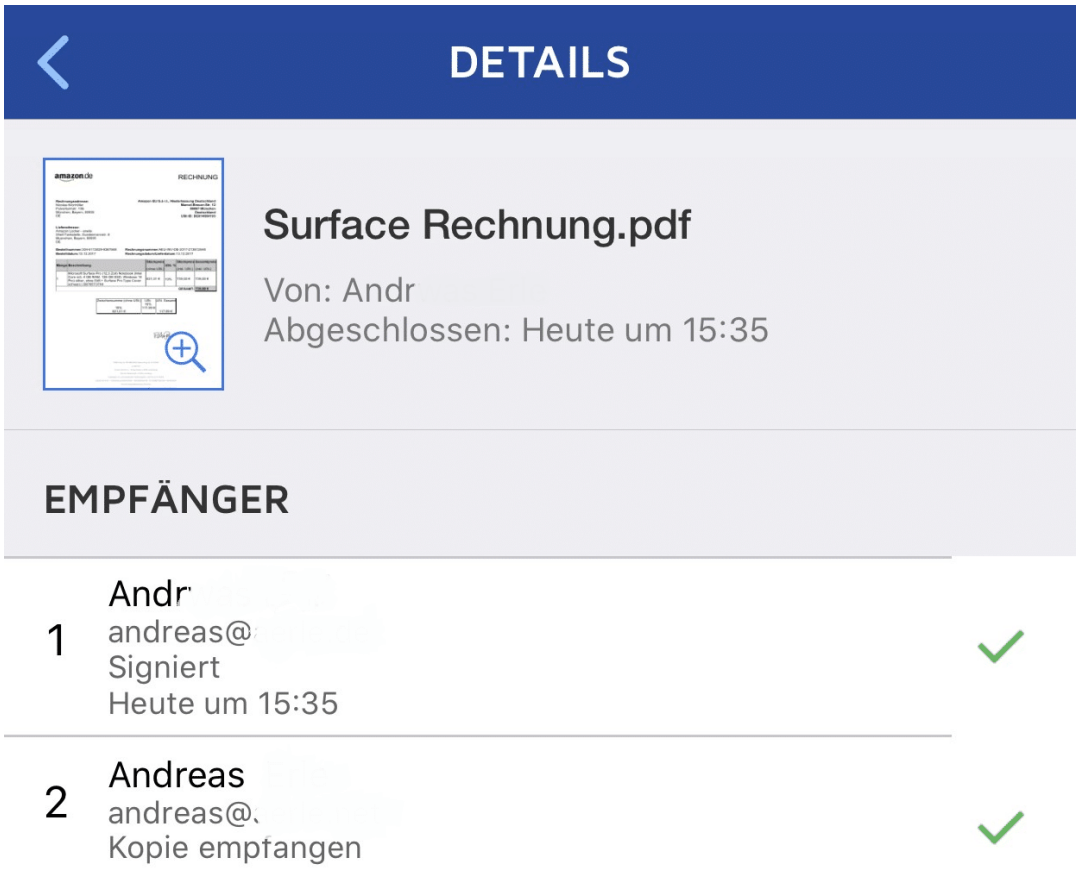
https://www.youtube.com/watch?v=L9RL3hU0s08&t=665s

Dokumente signieren mit DocuSign

Der Austausch von Unterlagen ist schon lange kein physisches Versenden mehr. Verträge und andere Dokumente werden schnell per E-Mail ausgetauscht, Änderungen kommuniziert und umgesetzt. Dabei ist es egal, ob Sie das am PC, am Tablet oder am Smartphone machen. Das Problem nur: Wie bekommen Sie dann eine Unterschrift auf ein Dokument? Die einfache Lösung: Durch DocuSign.

Natürlich können Sie mit einem PDF-Bearbeitungsprogramm und einem Stift eine Unterschrift auf ein Dokument zaubern. Das aber ist aufwändig und hat - weil der Weg nicht nachvollziehbar ist - keine Rechtswirkung. Vor allem geht es oft gar nicht mal mehr um das physische Dokument, sondern um den Nachweis, wann die Unterschrift erfolgt ist. DocuSign bietet hier verschiedene Pläne an: Wenn Sie selbst Dokumente unterschreiben und dann an einen Empfänger schicken wollen, dann kostet das gar nichts. Wenn Sie aber selber ein Dokument zur Unterschrift an einen Partner schicken wollen, dann ist ein kostenpflichtiges Abo nötig. Das liegt zwischen EUR 9,99 bis EUR 38,- im Monat. Der Preis ist abhängig von der Zahl der Dokumente, die Sie maximal im Monat signieren wollen.

Die Handhabung ist kinderleicht: Installieren Sie die App, fügen Sie das Dokument aus dem Speicher, einem Clouddienst oder als Scan über die Kamera Ihres Smartphones hinzu. Dann wählen Sie aus, ob Sie selber unterschreiben oder das Dokument an einen Dritten zur Unterschrift schicken wollen.

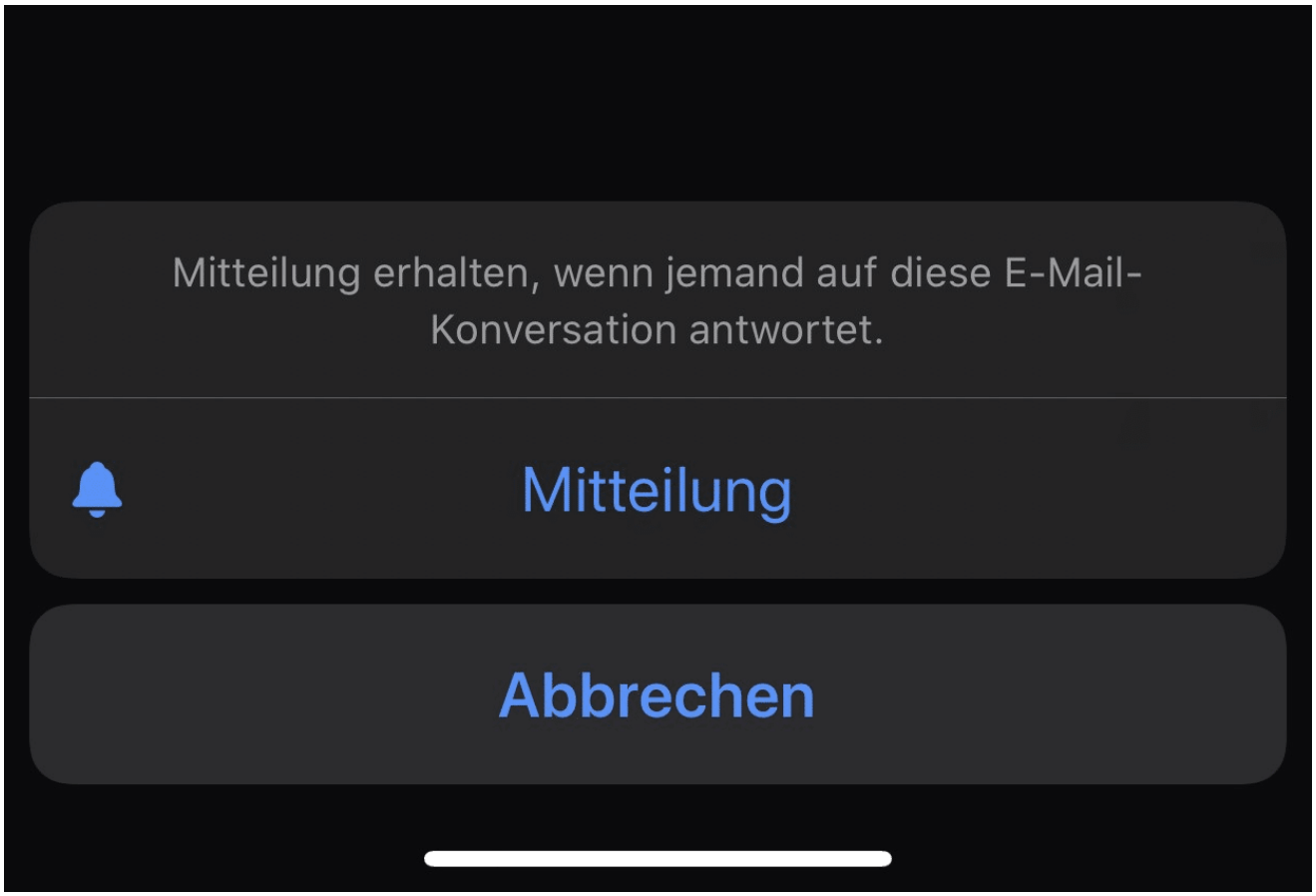


Für jedes Dokument können Sie genau nachvollziehen, wann wer es unterschieben hat und die Unterschrift auf dem Dokument ansehen. DocuSign selber garantiert über deren System, dass die Unterschrift echt ist - zumindest der Kommunikationsweg nachvollziehbar ist.

Besondere Benachrichtigung für neue Antworten unter iOS 13

Die Zahl der Kommunikationskanäle ist unerschöpflich. Mail, WhatsApp, Messenger, Telegram, SMS, immer mehr Apps signalisieren Ihnen eine neue Nachricht. Je nach Auslastung passiert es schnell, dass Ihnen da eine Nachricht durchgeht, weil Sie sie übersehen. Das ist beim fröhlichen Meinungsaustausch mit Kollegen kein Beinbruch, bei einer wichtigen E-Mail aber schon. Apple hat in iOS 13 noch eine zusätzliche Benachrichtigungsebene eingeführt, um das zu verhindern. Wir zeigen Ihnen, wo sich die versteckt.

Die Benachrichtigungseinstellungen von iOS sind recht fein aufgegliedert. Für jede App können Sie separat festlegen, wo und wie eine Benachrichtigung bei einer neuen Nachricht erfolgt. Allerdings ist es reizvoll, einfach alle Apps mit Benachrichtigungen zu versehen, so verpassen Sie nichts. Apple hat allerdings erkannt, dass Mail als Medium immer noch den professionelleren Themen dient. Sie finden Nun beim Schreiben einer neuen (oder Beantworten eines eingegangenen) E-Mail eine kleine **Glocke** neben dem Betreff. Klicken Sie darauf, dann können Sie eine Mitteilung aktivieren.



Diese versendet iOS, wenn zu dem Thema (festgelegt durch den Betreff der E-Mail) eine neue Nachricht eingeht. Die Benachrichtigung wird automatisch als wichtig angenommen und ignoriert den Nicht-Stören Modus. Sie sehen Sie also, auch wenn eigentlich alle Benachrichtigungen stumm sind.

Wenn Sie das nicht mehr wollen, nehmen Sie eine beliebige E-Mail aus der Kommunikation und schalten Sie die Benachrichtigung wieder durch ein Tippen auf die Glocke aus.

PSD2: Online Banking wird sicherer

Schon einmal von der neuen europäischen Zahlungsrichtlinie PSD2 gehört? Hinter der neuen Richtlinie mit dem sperrigen Begriff **Payment Services Directive 2** verbergen sich zahlreiche Veränderungen und Verbesserungen, die den Zahlungsverkehr und das Online Banking innerhalb der Europäischen Union sicherer machen sollen.

Alle Kunden einer Bank mit bestehendem Online Banking haben im Spätsommer 2019 Post im Briefkasten oder E-Mailfach von ihrer Hausbank erhalten. Darin wurden die neuen Verfahren zum sicheren Zahlungsverkehr im Internet erklärt.

Mit welchen Veränderungen müssen sich Bankkunden in Deutschland beim Online Banking in Zukunft anfreunden? Dieser Ratgeber klärt über die neuen Verfahren für Bankgeschäfte im Internet auf.

Online-Banking ist beliebt

Die Zeiten der gelben Überweisungsträger in Deutschland dürften bald schon Geschichte sein. Immer mehr Menschen tätigen Ihre Bankgeschäfte im Internet. Das Online Banking in Deutschland erfreut sich seit Jahren einer steigenden Beliebtheit. Inzwischen erledigt mehr als die Hälfte der Bevölkerung ihre Bankgeschäfte online.

Junge Menschen unter 40 Jahren nutzen bereits heute überwiegend das Internet für Ihre Bankgeschäfte. Die zunehmende Beliebtheit geht auf die Altersgruppe der 40- bis 50-jährigen zurück, die vermehrt auf Online Banking zugreifen. Nur jeder vierte Mensch im Rentenalter nutzt hingegen das komfortable Online Banking.

Von größerer Bedeutung in Zukunft wird das Mobile Banking sein. Zwar führen die meisten Kunden ihre Bankgeschäfte aktuell noch von einem stationären PC aus, der Anteil der Nutzer mit einem Smartphone oder Tablet steigt jedoch rasant. Ein beliebtes Endgerät für Onlinebanking ist das iPhone von Apple. Das iPhone gehört zu den leistungsstärksten Smartphones auf dem Markt. Es ist mit einem hochauflösenden Display, einer starken Kamera und einem großen Speicher ausgestattet. In Verbindung mit einem Vertrag mit einer Allnet Flatrate ist das Apple iPhone ein treuer Begleiter und ideal für das Online-Banking.

Für mehr Sicherheit

Mit der neuen Zahlungsrichtlinie der Europäischen Union soll primär die Sicherheit von Bankkunden gestärkt werden. Im Kern fordert die neue Richtlinie stärkere und sicherere Maßnahmen für die Kundenauthentifizierung sowie für den Zugriff auf Konten durch Drittanbieter.

Mit der PSD2 gibt es nun erstmals einheitliche rechtliche und technische Vorgaben, die Banken beim Online-Banking erfüllen müssen. Die wesentlichste Veränderung für Bankkunden ist die sogenannte Zwei-Faktor-Authentifizierung. Um Zugang zum Bankkonto zu erhalten oder Zahlungen zu autorisieren, müssen Bankkunden fortan ihre Identität auf zwei verschiedenen Wegen nachweisen

Die neue Kundenauthentifizierung

Bankkunden müssen sich ab sofort daran gewöhnen, ihre Identität sicher nachzuweisen. Die PSD2 fordert eine "starke" Kundenauthentifizierung. Stark bedeutet, die Identität nicht länger nur mit einem Passwort oder einen Fingerabdruck nachzuweisen. Zwei "Faktoren" müssen mindestens genutzt werden. In der Praxis haben sich drei "Faktoren" durchgesetzt, die für die Authentifizierung möglich sind:

- Faktor **Wissen**. Der Nachweis der Identität erfolgt über die Eingabe eines Passworts, einem Pin oder eines Musters
- Faktor **Habitus**. Der Nachweis der Identität erfolgt über ein zuvor registriertes Endgerät wie einem Tablet von Samsung oder einem Smartphone

- Faktor **Sein**. Der Nachweis der Identität erfolgt über einen biometrischen Nachweis, in der Regel handelt es sich dabei um einen Fingerabdruck

Der Nachweis der Identität ist bei allen Zahlungsaufträgen erforderlich. Überweisungen oder Transaktionen mit einer Kreditkarte zählen dazu. Zudem greift die Zwei-Faktor-Authentifizierung auch für den Log-in in das Online-Banking. Die meisten Banken informieren über die neuen Standards. Mit einem Erklärvideo zur Zwei-Faktor-Authentifizierung der DKB wird das neue Verfahren leicht verständlich dargestellt - und natürlich gibt es auch bei schieb.de entsprechende Erklärungen.

Weitere Änderungen für Bankkunden

Das Online-Banking soll nicht nur sicherer, sondern auch komfortabler werden. Die starke Kundenauthentifizierung muss bei einigen Banken nicht bei allen Log-ins in das Online-Banking nachgewiesen werden. Sie haben die Möglichkeit, Art. 10 der neuen Richtlinie anzuwenden. Danach ist es ausreichend, wenn Kunden alle 90 Tage ihre Identität auf zwei Wegen sicher nachweisen. Innerhalb dieser Frist von 90 Tagen reicht der Nachweis eines Faktors zur Authentifizierung.

Von diesem komfortablen Log-in in das Online Banking sind Zahlungsaufträge im Internet ausgenommen. Für sie gilt die Regel, die Identität mit mindestens zwei Faktoren nachzuweisen.

Tipps für sicheres Online-Banking

Unabhängig von der neuen Richtlinie für einen sicheren Zahlungsverkehr im Internet können Bankkunden selbst Maßnahmen ergreifen. So sollten alle Bankgeschäfte online nur von einem eigenen Endgerät ausgeführt werden. Die Nutzung fremder Computer, Laptops oder Smartphones birgt die Gefahr, dass die Daten in die falschen Hände geraten. Gleiches gilt für die Nutzung des W-LAN-Signals. Es ist möglich, das öffentliche oder fremde Netze nicht ausreichend geschützt sind und Unbefugte darauf zugreifen.

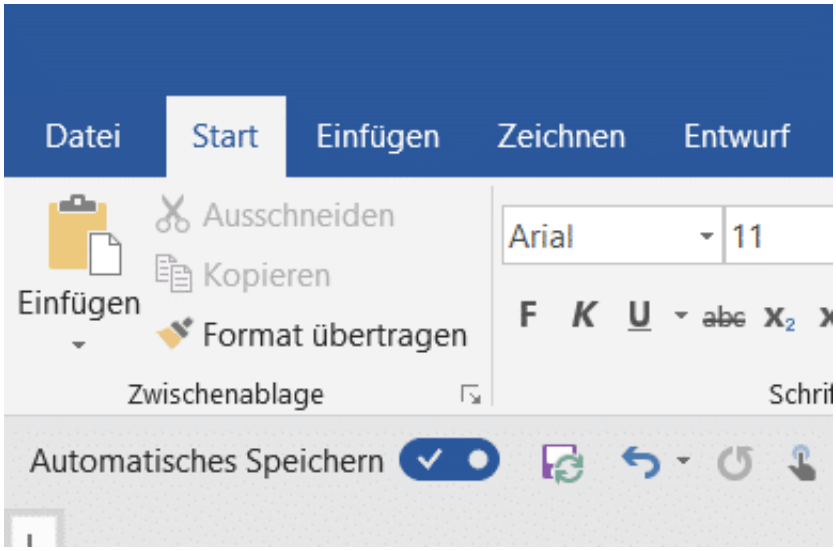
Weitere Tipps für sicheres Online-Banking:

- Das bestehende Antivirenprogramm stets mit den neusten Updates versorgen
- Den genutzten Browser ebenfalls stets updaten
- Keinen Zugang auf das Online-Banking von Links in E-Mails oder fremder Webseiten tätigen
- Stets das Sicherheitszertifikat der Bank beim Online-Banking überprüfen

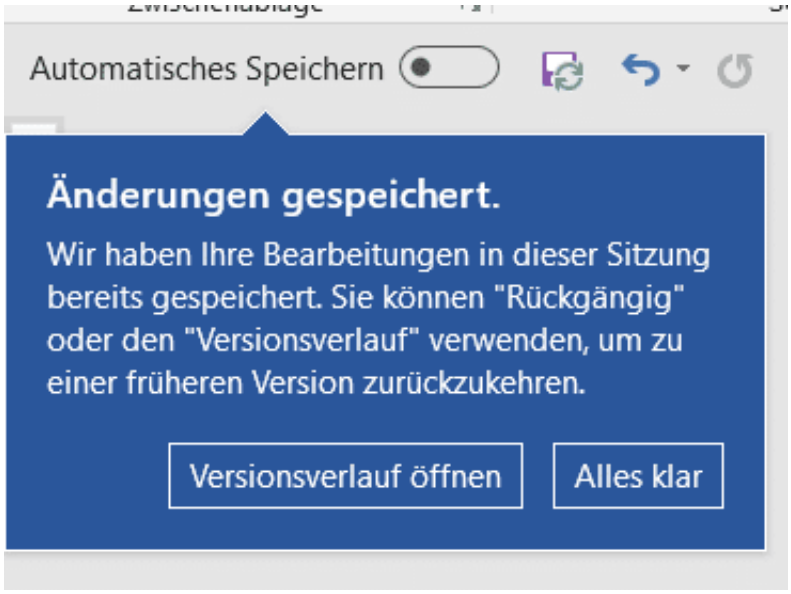
Automatisches Speichern in der Cloud in Office

Die Verwendung der Cloud als Speicher hat viele Vorteile. Dokumente können direkt anderen Anwendern zur Verfügung gestellt werden, ohne eine gleiche Festplatte nutzen zu müssen. Die Dateien sind zentral auf dem Cloudspeicher (ob nun OneDrive oder Sharepoint) abgelegt. Allerdings kann hier das Problem auftreten, dass Sie eine Datei zu speichern vergessen oder einen falschen Stand gespeichert haben. Die Mechanismen bei einer lokalen Kopie auf dem PC greifen hier nicht. Mit wenigen Schritten können Sie aber auch in der Cloud auf Sicherungsstände zugreifen.

Im Standard ist in den Office-Programmen die automatische Speicherung eingeschaltet, wenn Sie eine Cloud-Datei bearbeiten. Das erkennen Sie an dem aktivierten Schalter **Automatisches Speichern** unter der Symbolleiste von Word, Excel und PowerPoint. Dadurch wird in automatischen Abständen der aktuelle Strand gesichert. Ohne, dass Sie manuell etwas tun müssen. Im Gegensatz zu der manuellen Speicherung birgt das das Risiko, dass Änderungen gespeichert sind, die Sie eigentlich gar nicht wollten.



Wenn Sie mit einem Dokument herumexperimentieren, um den richtigen Inhalt und die beste Form zu finden, dann können Sie die automatische Speicherung natürlich auch über den Schalter ausschalten. Was aber, wenn es schön zu spät ist? Wenn Sie das automatische Speichern ausschalten, dann bekommen Sie einen Hinweistext von Word angezeigt. Klicken Sie auf **Versionsverlauf öffnen**, dann zeigt Word Ihnen eine Liste der Speicherpunkte an.

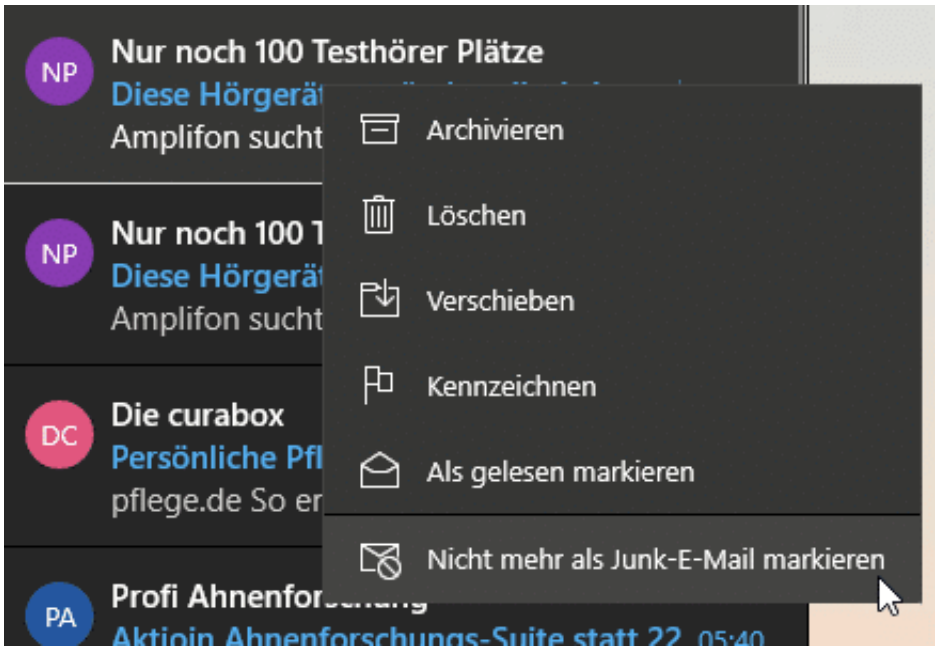


Wenn Sie auf das kleine Uhrsymbol oben rechts in der Symbolleiste der Office-Programme klicken, dann kommen Sie ebenfalls direkt in den Versionsverlauf. Wählen Sie einen Speicherpunkt aus, indem Sie auf **Version öffnen** klicken. Das Dokument ist danach wieder in dem Stand, zu dem es zum Speicherzeitpunkt war. Sie können sich damit möglichst nah an den Stand heranbewegen, zu dem das Dokument noch in Ordnung war.

Korrigieren von SPAM-Ordner und Junk-Email

Jeder Mail-Anbieter hat mittlerweile einen eigenen Filter für SPAM-E-Mails. Auf Grund verschiedener Regeln werden E-Mails, die als unerwünschte Werbung erkannt werden, dort eingeordnet. Nun ist nicht jede Regel perfekt und fehlerfrei, insofern kann es durchaus passieren, dass „echte“ E-Mails dort landen. Wir zeigen Ihnen, wie Sie selbst das Heft in die Hand nehmen und die Erkennung verbessern können.

Suchen Sie sie sich in Ihrem Mail-Programm den SPAM-Ordner heraus. Der kann Werbung, Junk-E-Mail, SPAM etc. heißen. Durch einen Klick mit der rechten Maustaste auf den Ordner können Sie ihn zu den Favoriten hinzufügen. Damit ist er immer im oberen Teil der Ordner sichtbar und schnell im Zugriff. Schauen Sie regelmäßig hinein!



Sie können die Erkennung von Werbung verbessern, wenn Sie selbst falsch klassifizierte E-Mails markieren. Klicken Sie mit der rechten Maustaste auf eine E-Mail, uns wählen Sie entweder **Als Junk-E-Mail markieren** oder **Nicht mehr als Junk-E-Mail markieren**. Bei der nächsten E-Mail behandelt die Mail-App sie anders, bei Outlook funktioniert das genauso.

Wenn Sie den Clutter-Ordner von Office 365 nutzen, dann können Sie die Korrektur der SPAM-Erkennung noch einfacher durchführen: Greifen Sie eine der als SPAM markierten E-Mails und ziehen Sie sie mit der Maus aus dem SPAM-Ordner in den Posteingang. Es kann sein, dass Sie dies mehr als einmal machen müssen: Clutter lernt aus Ihrem Verhalten, und das kann dauern.