Schieb Report

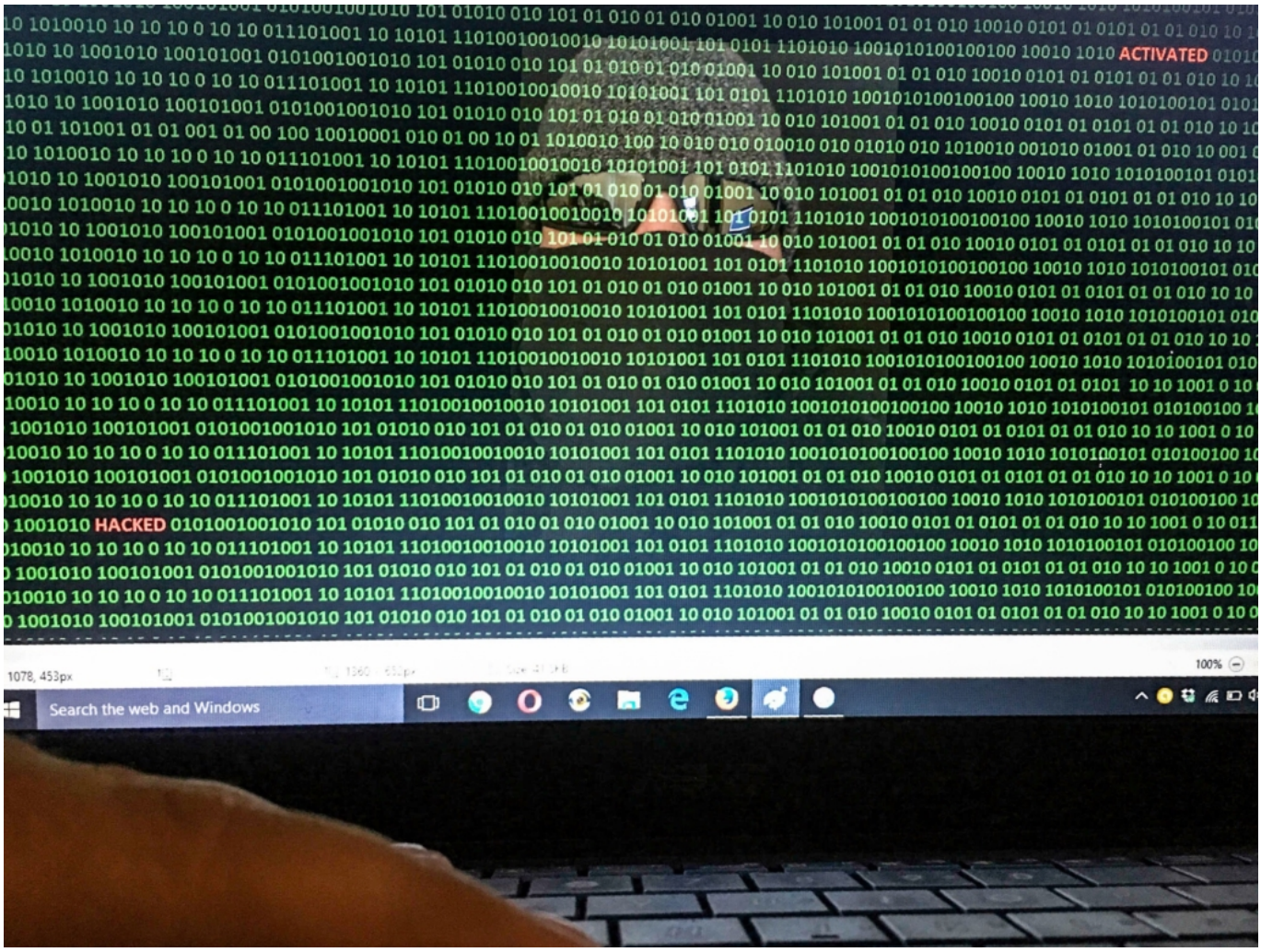
Ausgabe 2020.11

Neue Sicherheitslücke in Prozessoren entdeckt

Verschiedene Forscherteams haben eine weitere gravierende Schwachstelle in aktuellen Prozessoren identifiziert und in Whitepapers beschrieben, die heute veröffentlicht worden sind: Mittels einer neuen Angriffsmethode namens „Load Value Injection in the Line Fill Buffers“ (LVI-LFB) können versierte Hacker gezielt Daten in Rechenzentren stehlen, ohne Spuren zu hinterlassen.

Möglich wird die LVI-LFB-Attacke – wie auch die 2018 und 2019 entdeckten Seitenkanalattacken Meltdown, Spectre und MDS (Microarchitectural Data Sampling) – durch die Manipulation leistungssteigernder Hardware-Funktionen der Prozessoren. Im Gegensatz zu den genannten Sicherheitslücken erlaubt LVI-LFB jedoch erstmals einen gezielten Zugang zu Daten.

Die neu entdeckte Angriffsmethode betrifft alle modernen Intel-Prozessoren in Servern, Desktops und Laptops, die zwischen 2012 und 2020 produziert wurden - also einschließlich jener, die nach Bekanntwerden von Meltdown, Spectre und MDS hergestellt wurden. Die Attacke kann sich besonders verheerend in Rechenzentren sowie öffentlichen und privaten Clouds auswirken. Denn in solchen Umgebungen, in denen Abteilungen und Organisationen Hardware gemeinsam nutzen, kann ein Angreifer, der nur über geringste Privilegien verfügt, sensible Informationen eines anderen Nutzers oder einer anderen virtuellen Umgebung ausspionieren.



Nach Aussage von Bogdan Botezatu, leitender Bedrohungsanalyst bei Bitdefender, reichen vorhandene Abwehrmaßnahmen für bereits bekannte Seitenkanalattacken nicht aus, um die Sicherheitslücke zu schließen: „Vollständig schließen lässt sich die Sicherheitslücke nur durch

Austausch der Hardware oder durch Deaktivierung von Funktionen wie Hyperthreading und damit einhergehenden erheblichen Leistungseinbußen.“

Bitdefender hat die Sicherheitslücke am 10. Februar 2020 an Intel berichtet. Der Prozessor-Hersteller war jedoch zuvor schon im April 2019 von den folgenden Forschern auf den Angriffsweg aufmerksam gemacht worden: Jo Van Bulck, Daniel Moghimi, Michael Schwarz, Moritz Lipp, Marina Minkin, Daniel Genkin, Yuval Yarom, Berk Sunar, Daniel Gruss und Frank Piessens. In einer koordinierten Offenlegung ist die Sicherheitslücke heute unter der Kennung Code CVE-2020-0551 veröffentlicht worden. Bob Botezatu: „Dass verschiedene Teams unabhängig voneinander diesen Angriffsweg entdeckt haben, spricht Bände über die Gefahr, dass er jetzt und in Zukunft für Cyberspionage zum Einsatz kommt.“

Whitepaper beschreibt vier Szenarien
Das ausführliche Whitepaper von Bitdefender zu LVI-LFB mit dem Titel „Load Value Injection in the Line Fill Buffers: How to Hijack Control Flow without Spectre“ enthält vier Bedrohungsszenarien, die sich aus der Schwachstelle ergeben und ist kostenlos verfügbar unter dem Link https://businessresources.bitdefender.com/hubfs/Bitdefender_Whitepaper_LVI-LFB_EN.pdf

Umgang mit Alarmen bei Nest Protect

Smarthome ist seit einiger Zeit ein Thema, das immer mehr Bedeutung erlangt. Immer mehr Geräte sind mit dem Internet verbunden und sammeln Daten, die dann an einen Dienst übertragen und ausgewertet werden. Im einfachsten Fall bieten sie dem Anwender eine Bedienmöglichkeit, Geräte wie die NEST Protect Rauchmelder sind von der Bedienung nicht App-gestützt. Bei einem Alarm wird das schnell zur Herausforderung.

Ein Rauchmelder ist kein klassische bedienbares Gerät: Er misst das Vorliegen von Rauch und Kohlenmonoxid und alarmiert dann akustisch (durch eine Ansage und einen lauten Ton) und visuell (durch den grell aufleuchtenden Lichtring). Der Erfahrung nach sind viele der Alarme Fehlalarme, beispielsweise weil Essen in der Pfanne anbrennt und Rauch an einen der Melder kommt.

NEST Protect warnt im ersten Moment am konkret betroffenen Melder. Erst wenn der Rauch nicht abzieht, dann wird ein echter Alarm ausgelöst. Alle Geräte, auf denen die App installiert ist, bekommen nun eine Pop-Up-Meldung. Die enthält die Position des Melders und den Auslöser. Der Alarm allerdings ertönt auf allen Meldern, die sich am Standort befinden.

Eine Deaktivierung des Alarms ist in der App nicht möglich. Hierzu müssen Sie einen beliebigen Melder finden und einmal auf den großen Knopf in der Mitte des Melders drücken. Der Alarm geht aus und die Deaktivierung wird an die anderen Melder übertragen. Endlich ist Ruhe!

Sicherungen schonen bei Mehrfachsteckdosen

Kennen Sie das Problem, dass Ihr Arbeitszimmer nicht genug Steckdosen für all Ihre Geräte hat? Zwei Monitore, Notebook, PC, Drucker, Netzteile für mehrere mobile Geräte, alle wollen stromversorgt werden. Die Lösung ist oft eine Mehrfachsteckdose, mit der drei bis fünf Geräte an eine physische Steckdose angeschlossen werden. Je nach Last, die daran hängt, kann Ihnen das aber schnell die Sicherung kosten. Dafür gibt es aber eine Lösung!

Vor allem Schaltsteckdosen sind davon betroffen: Wenn Sie diese einschalten, dann bekommen alle daran angeschlossenen Geräte gleichzeitig Strom. Das verursacht eine Stromspitze, die die normale Last um ein Vielfaches überschreitet. Die Sicherung interpretiert daraus ein Problem und löst aus. Meist hängen an dieser Sicherung aber noch weitere Geräte, die dann natürlich auch alle aus sind. Ungünstig, wenn es sich dabei um einen PC oder eine Netzwerkfestplatte handelt, die ordentlich heruntergefahren werden sollten!

Lösungen für diese Problem suchen Sie nahezu vergeblich: Eine Mehrfachsteckdose schaltet alle Anschlüsse gleichzeitig ein, nicht nacheinander. Das würde die Lastspitzen, die sich ja für jeden Anschluss summieren, verringern. Diese Lösung gibt es bei einem kleinen Ingenieurbüro als "Steckdosenleiste mit sequentieller Einschaltverzögerung", die PowerSeq_501. Wird diese eingeschaltet, dann geht nur die erste Steckdose an, die anderen werden nacheinander mit jeweils einer Sekunde Versatz eingeschaltet.

Sicherheitsexperte stellt Microsoft-Betrüger bloß

Da ist einem britischen Sicherheitsexperten ein Coup gelungen: Er hat sich in die Überwachungssysteme von Betrügern gehackt - und sie live beim Betrügen beobachtet. Großartig.

Ich kann gar nicht zählen, wie oft ich das schon gefragt wurde - und das seit Jahren: "Bei mir haben Microsoft-Mitarbeiter angerufen. Sie haben auf meinem Rechner angeblich einen Virus entdeckt und wollen den entfernen." Manchmal rufen die angeblichen Supporter von Microsoft an. Manchmal schaffen sie es, Alarm-Hinweise auf den Bildschirm zu zaubern.

Aber immer mit der Absicht, arglose Opfer in aller Welt zu betrügen. Mal, indem Gebühren für diesen "Service" (Virus entfernt) berechnet werden - öfter, indem sie sensible Passwörter und Zugangsdaten entwenden.

Experte hat Überwachungskameras der Betrüger gehackt

Es passiert tausendfach pro Woche, dass gutgläubige Menschen nachgeben und den Betrügern Zugriff auf ihre Rechner gewähren. Der Trick ist uralt - funktioniert aber immer noch. Obwohl die Verbraucherzentrale ausführlich davor warnt und die Vorgehensweise beschreibt. Im schlimmsten Fall blockieren die Betrüger den Rechner und erpressen später Geld, um ihn

wieder freizugeben. Oder sie verlangen Geld, um das angebliche, aber gar nicht vorhandene Problem zu beseitigen. Oder beides.

Nun ist einem britischen Sicherheitsexperte, der sich Jim Browning nennt (aber sicher anders heißt), etwas Großartiges gelungen: Es hat sich seinerseits in das Call-Center einer solchen Betrügerbande in New Delhi eingehackt. Er hat sogar die Kontrolle über Dutzende Überwachungskameras im Gebäude übernommen - und so 70.000 Anrufmitschnitte angefertigt. Also den Betrügern bei der Arbeit zugesehen und ihr betrügerisches Verhalten dokumentiert.

Einblicke in die Welt organisierter Kriminalität

Aber nicht nur das: Er dokumentiert auch, wie gehässig sich diese Kriminellen über ihre Opfer auslassen. Die Krönung ist aber, dass es ihm sogar gelungen ist, mit diesen Betrügern als vermeintliches Opfer zu sprechen (es erscheinen Rufnummern auf den PCs der Opfer, die sie anrufen sollen!). Er hat dieses Gespräch aufgezeichnet und präsentiert es in einem Video.

Respekt! Es stellt sich beim Betrachter eine Mischung aus Schadenfreude und Verwunderung ein. Schadenfreude darüber, dass diese Betrüger so gekonnt und elegant vorgeführt werden. Und Verwunderung, mit welcher Selbstverständlichkeit die Leute ihren "Job" machen, als wären sie in einem echten Call-Center, in dem Leuten geholfen wird. Dabei betrügen sie Menschen am laufenden Band. Sie lügen, betrügen und richten Schaden an.

https://www.youtube.com/watch?v=le71yVPh4uk&feature=emb_title

Da diese "Call-Center" nahezu immer in Indien sitzen - und nun ein unanfechtbarer Beleg für Existenz und Vorgehen dieser Betrügerbanden vorgehen: Wann geht die indische Regierung endlich rigoros dagegen vor?

Eine WordPress-Webseite erstellen: So geht's

Mit einer eigenen Webseite, einem eigenen Blog oder sogar mit einem eigenen Onlineshop im Wev vertreten sein: Das ist heute nicht mehr besonsders schwierig. Eine besonders einfache Methode, die in den meisten Fällen ganz gut funktioniert, ist das Einrichten einer WordPress-Präsenz. Das erfordert zwar ein bisschen Übung, ist aber vergleichsweise einfach.

Wer noch keine Erfahrung mit dem Aufbauen einer eigenen Webpräsenz mit WordPress hat, erhält in diesem Text die nötige Hilfestellung. Das Erstellen einer Seite mit WordPress- Schritt für Schritt erklärt: So klappt es auch für Einsteiger. Auch ohne Vorkenntnisse in Programmierung oder Webdesign.

Schritt 1: Das Hosting

Um eine WordPress-Seite zu installieren, braucht man im Grunde genommen nur zwei Dinge:

- Das Webhosting
- Eine Webadresse (Domain)

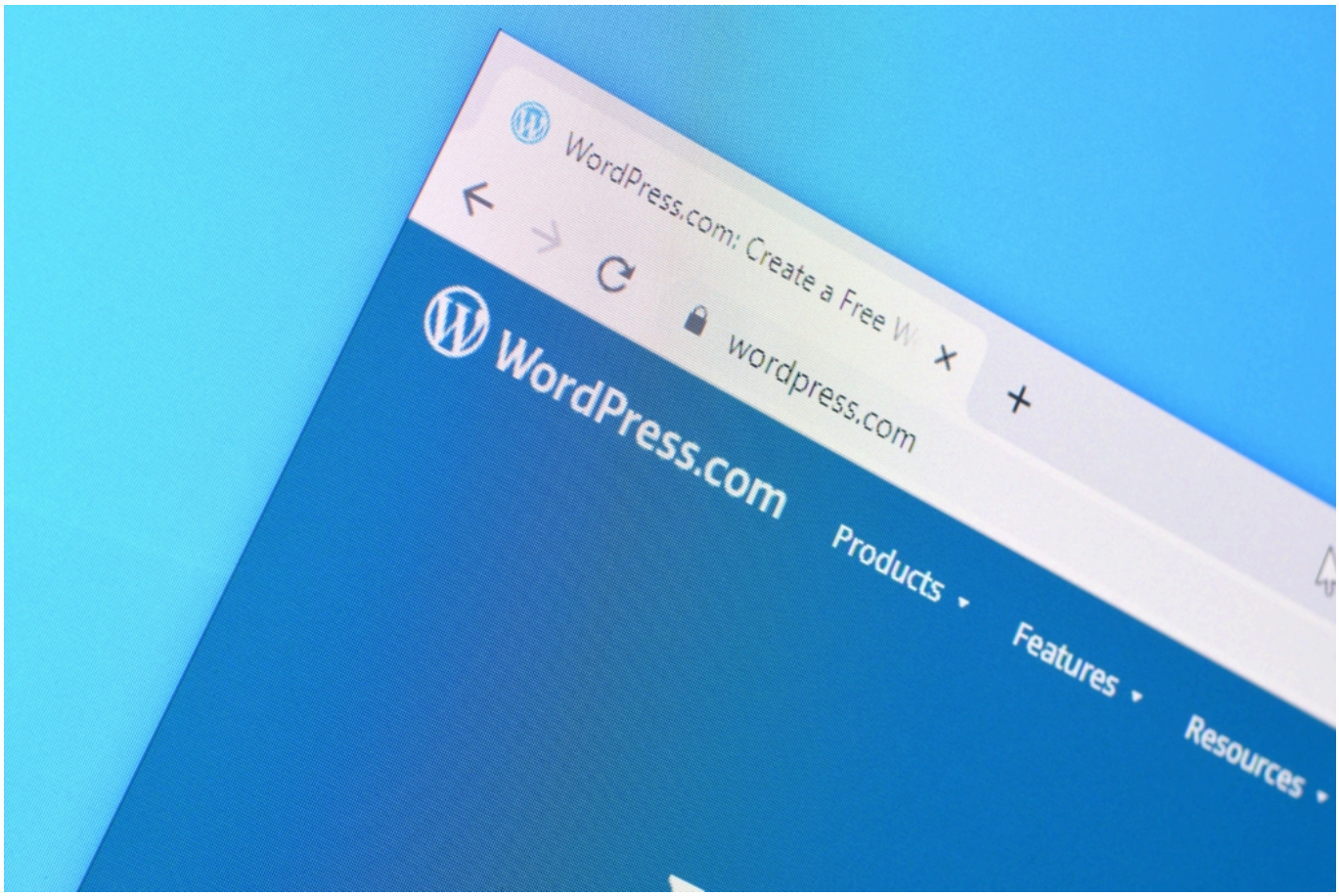
WordPress an sich ist kostenlos. Eine Domain kostet dagegen schon mal 5-10 Euro im Monat. Wenn man sich für einen der etwas besseren Webhoster entscheidet, braucht die Seite dann anschließend auch nicht so lange um zu laden, dies wirkt sich wiederum gut auf das Google Ranking aus.

Anbieter von Webhosting gibt es im Internet unzählige. Was die günstigeren Anbieter angeht, so haben die meistens mindestens einen Haken: Manchmal stimmt einfach der Service nicht, oder es sind gewisse Extrakosten versteckt. Auf jeden Fall sollten Sie bei der Auswahl von Anbietern immer gut abwägen und Vorsicht walten lassen.

Schritt 2: Die Domain

Es gab einmal eine Zeit, in der Google Domains mit spezifischen Schlüsselwörtern höher eingestuft hat. Ein Schlüsseldienst unter schluessel-dienst.de hatte ein höheres Anrsehen. Doch das bringt heutzutage keinen Vorteil mehr. Google hat diese Regel abgeschafft, da sie des Öfteren ausgenutzt wurde. Den exakten Suchbegriff zu verwenden, mit dem man bei Suchmaschinen gefunden werden will, gilt es heutzutage tunlichst zu vermeiden.

Im Internet findet man etliche Domainendungen, wie .blog, . Shop, .training usw.. Was diese Endungen angeht, so sind die Expertenmeinungen geteilt. Manche sagen, dass man Domains mit diesen Endungen auf jeden Fall meiden sollte. Andere wiederum sagen, diese Domains sind die Zukunft. Momentan sind diese Endungen allerdings noch eher unbekannt. Es gilt nach wie vor auf bekannte Endungen wie .net, .de, .com, .ch oder .at zu setzen.



Schritt 3: Das Installieren von WordPress

Wenn Sie an diesem Punkt angekommen sind, sollten Sie sich bereits um das Hosting und die Domain gekümmert haben. Für gewöhnlich findet man in der Email, die einem der Hosting Betreiber schickt, die jeweiligen Zugangsdaten um WordPress zu installieren.

Sobald man sich im Menü der Hostinplattform befindet, sollte dort irgendwo ein Link zur Software Installation auf dem Webspace sein. Dort findet man eine Liste mit unterschiedlichen Software Tools vor, die man mit wenigen Klicks installieren kann. Wählen Sie hier bitte WordPress aus. Als nächstes erstellt das Programm eine sogenannte Datenbank. Nach Abschluss der Installation muss man lediglich noch seinen Benutzernamen und das Passwort im Browser auswählen. Das war's dann eigentlich schon, Sie haben WordPress erfolgreich installiert.

Schritt 4: Passen Sie die Inhalte Ihrer neuen Webseite an

Gratulation! Sie haben WordPress also erfolgreich installiert. Jetzt fängt der Spaß sozusagen erst richtig an. Im Folgenden erklären wir Ihnen einige der Funktionen bei WordPress. Auf Ihrer Domain sollten Sie bereits etwas wie eine einstweilige Webseite vorfinden. Was Sie dort sehen nennt man übrigens Frotend. Allerdings gibt es bei WordPress noch das dem gegenüberstehende Backend. Dies ist der Adminbreich indem man diverse Bilder, Videos und vor allem Texte einfügen kann.

Das Dashboard

Ein WordPress Dashboard gibt einem einen übersichtlichen Überblick über seine WordPress Seite. Links sieht man den gesamten Adminbereich, der als eine Art Navigationsleiste angezeigt wird. Das Dashboard ist jener Bereich, indem man Inhalte auf seiner Webseite einfügen kann. Auch die Navigation und das Design können hier geändert werden. Dazu gehört das Implementieren eines Logos under die Einstelungen der Farben. Sie können sich gerne ein eigenes Logo erstellen und es anschließend im Dashboard einfügen.

Die grundlegende Planung des Aufbaus einer Webseite

Am Anfang sollte man sich durchaus etwas Zeit dafür nehmen, den grundlegenden Aufbau einer Webseite zu planen. Dafür sollten Sie in der Lage sein, zumindest folgende Fragen zu beantworten:

- Was ist Ihre Zielgruppe?
- Was wollen Sie mit Ihrer Webseite eigentlich erreichen?
- Was für eine Art von Inhalten wollen Sie veröffentlichen?
- Wie soll die Navigation aufgebaut sein?

Das Auswählen einer Designvorlage

WordPress bietet allerlei Vorlagen von Design für Webseiten an, für gewöhnlich lassen diese sich recht einfach einbinden. Selbst komplett ohne Programmier- und Designvorkenntnisse sollten Sie mit deren Hilfe in der Lage sein, außergewöhnlich schöne Webseiten zu erstellen.

So passen Sie Ihre Vorlage an

Bei WordPress gibt es ein äußerst nützliches Tool, nämlich der sogenannte Design Customizer. Mit seiner Hilfe kann man bequem Layout, Schriften und Farben in den jeweiligen Themes anpassen. Hierfür muss man einfach auf Design und anschließend auf Customizer klicken. Danach sollte sich eigentlich auf der linken Seite von WordPress eine Spalte öffnen. In dieser hat man alle zur Verfügungen stehend Einstellungsmöglichkeiten. Welche dieser Einstellungen Sie verwenden möchten, hängt wiederum vom geplanten Aufbau Ihrer Webseite ab.

Sollten Sie sich bis zum Schluss an unsere Anleitung und Ratschläge gehalten haben, sind sie jetzt der stolze Besitzer einer voll umfassenden WordPress Webseite.

Sicheres Online Shopping

Ein Trend, den es schon lange gibt - und der sich auch nicht mehr umkehrt: Online einzukaufen ist ebenso beliebt wie bequem. Wer keinen großen Beratungsbedarf hat (hier sind echte Ladenlokale durchs nichts zu ersetzen), genießt dabei auch einige Vorzüge: Wer online einkauft, spart nicht nur Zeit, sondern nicht selten auch Geld (allerdings keineswegs automatisch(. Vom stressigen Rummel in vollen Kaufhäusern und genervten Verkäufern an überfüllten Kassen mal ganz abgesehen.

Aber der Online-Handel ist keine Welt der Glückseligen. Auch hier kommt es immer wieder zu Schwierigkeiten: Zu viel Geld abgebucht, Ware beschädigt und nicht pünktlich geliefert, Schwierigkeiten mit der Rückgabe und vieles andere mehr. Das ist ärgerlich und kann manchmal auch ziemlich teuer werden. Solche Erfahrungen erschrecken die Verbraucher. Es lässt den Online Einkauf unseriös oder sogar gefährlich erscheinen.

Das ist natürlich nicht generell der Fall. Wer online einkauft, sollte allerdings tatsächlich ein paar grundlegende beachten.

Regeln beim Online Shopping

Bei den wichtigsten Regeln für das Online-Shopping geht es nicht nur um den sicheren Erhalt der Ware, sondern natürlich auch um den Datenschutz. Wenn Sie folgende Dinge beachten, sind Sie auf der sicheren Seite und gehen bei der gemütlichen Schnäppchenjagd keine Risiken ein.

In den meisten Onlineshops werden Ihnen verschiedene Zahlmethoden angeboten. Das Zahlen mit Kreditkarte scheint am einfachsten, ist aber nicht wirklich die sicherste Variante. Hat Ihr Browser eine Sicherheitslücke, könnten die Daten abgefangen werden. Kommt selten vor, kann aber passieren. Nicht alle Shops verfügen über eine verschlüsselte (SSL-Verschlüsselung) Datenübertragung. Daher sollten die Daten der eigenen Kreditkarte und Bankverbindung nicht so bedenkenlos preis gegeben werden.

Bei einigen Onlineshops ist der Kauf per Nachnahme möglich. Hier bezahlt der Kunde tatsächlich erst, wenn der Postbote mit der Ware vor der Tür steht. Dennoch gibt es auch hier ein Risiko. Da Sie das Paket erst nach Zahlung ausgehändigt bekommen, kann sich das hinterher immer noch als unangenehme Überraschung erweisen, wenn zum Beispiel das Paket oder die Ware beschädigt sind oder die Lieferung nicht der Beschreibung des Onlineshops entspricht. Sicher können Sie dann die Ware immer noch zurück senden. Der Ärger, die Arbeit, eventuelle Rücksendekosten und der Zeitaufwand sowie erst einmal keine Ware in den Händen – das bleibt alles an Ihnen hängen.

Die beste Alternative

Die sicherste Alternative ist unweigerlich der **Rechnungskauf**. Bei den Deutschen besonders beliebt. Hier sind Kunden vor bösen Überraschungen gefeit und zahlen erst, wenn sie die Ware sicher erhalten haben und diese der Beschreibung des Händlers entspricht. Ein Betrug durch den Händler ist bei einer Bestellung auf Rechnung nahezu unmöglich. Mittlerweile wird die Zahlart „Kauf auf Rechnung“ von den meisten seriösen Onlineshops wie selbstverständlich angeboten. Bei bekannten großen Onlinehändlern können Sie Ihre Rechnungen sogar erst am Ende des Monats mit einer Banküberweisung in einem Schritt ausgleichen.

Zusätzliche Sicherheiten

Wenn sie beim Online-Shopping auf Sicherheit setzen möchten, können Sie auf einige Gütesiegel achten. Seriöse Online-Shops können diese Siegel beantragen und werden dann strengen Kontrollen unterzogen. Sie erhalten nur dann eine Zertifizierung, wenn diese Anforderungen erfüllt sind.

Solche Siegel zeigen dem Verbraucher an, dass sowohl der Onlinehändler als auch die unterschiedlichen Bestellprozesse des Shops geprüft wurden. Dabei gibt es für die einzelnen

Siegel unterschiedliche Überprüfungsmethoden sowie Qualitätsanforderungen. Daher sollte man ungefähr eine Ahnung haben, wofür die einzelnen Siegel stehen. Denn nicht jedes Qualitätssiegel bietet tatsächlich Sicherheit.

Als sicher empfohlen werden folgende Siegel:

Shops mit diesem Siegel erfüllen umfangreiche Qualitätskriterien. Sie gehen verantwortungsvoll mit Ihren Kundendaten um und nehmen Ihnen mit dem Käuferschutz finanzielle Risiken ab.

Dieses Siegel umfasst mehrere Prüfverfahren und verspricht Ihnen Datensicherheit und Systemsicherheit.

In Shops mit diesem Siegel kann der Verbraucher sicher einkaufen. Bei Problemen mit dem Händler unterstützt das EHI Retail Institut den Verbraucher bei der Durchsetzung seiner Rechte.

Es handelt sich hier um ein anspruchsvolles Siegel, das zu wesentlichen Verbesserungen des Datenschutzes und der Datensicherheit für den Verbraucher beiträgt.

Allerdings muss auch hier gewarnt werden. Zum einen ist es durchaus möglich, Gütesiegel in den Shop zu integrieren, obwohl keine Prüfung des Shops stattgefunden hat (klarer Fall von Missbrauch, kommt aber vor). Und zum anderen prüfen die Siegel zwar die Shops und Bestellprozesse, können Sie als Verbraucher jedoch nicht vor Pishing schützen. Damit wären wir wieder beim Kauf auf Rechnung, da hier keine Bankdaten übertragen werden müssen und

somit auch nicht ausspioniert werden kann.

Festplatten auf Macs verschlüsseln

Je sensibler unsere Daten werden, desto mehr ist der Wunsch nach adäquatem Schutz da. Neben den richtigen Passwörtern und biometrischen Zugangsdaten ist eine Möglichkeit, die Daten auf einem Datenträger zu verschlüsseln. Bei Windows 10 geht das über Bitlocker. Mac-Benutzer schauen ein wenig neidisch auf die andere Seite. Vollkommen ohne Grund!

Auch macOS hat seine Variante von Bitlocker, nur heisst die anders: FileVault ist in den neueren Versionen von macOS fest integriert. Die Idee dahinter: Wird eine Festplatte im Mac verschlüsselt, dann ist sie nur auf dem Rechner nutzbar, auf dem die Verschlüsselung durchgeführt wurde. Stiehlt jemand die Festplatte, dann kann er diese zwar formatieren und neu bespielen, an Ihre Daten aber kommt er nicht.

Sie können FileVault aktivieren, indem Sie auf den **Apfel** oben links, dann auf **Systemeinstellungen** und auf **Sicherheit** klicken. Um die Aktivierung durchführen zu können, klicken Sie auf das Schloss unten links in dem Fenster und geben Sie dann das Passwort Ihres Mac ein.

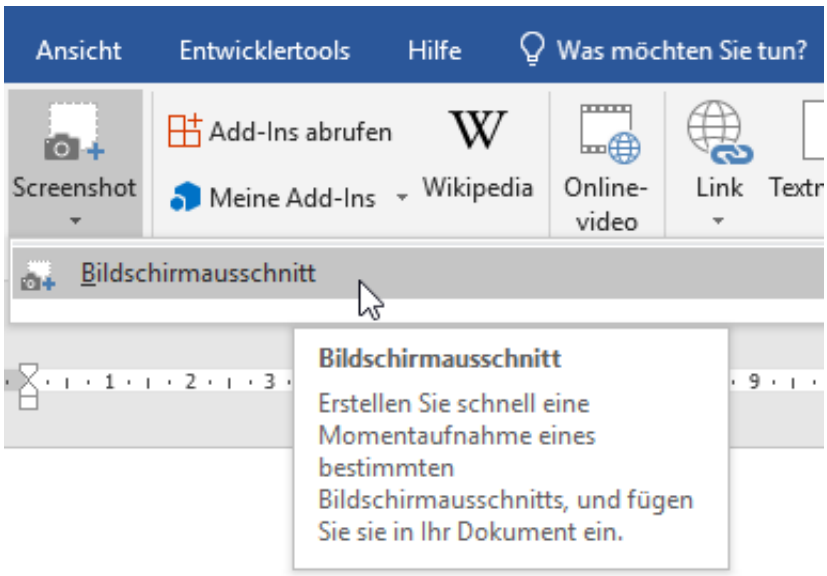
Nachdem Sie auf **FileVault aktivieren...** geklickt haben, erzeugt macOS den Schüssel aus den Hardwaredaten Ihres Mac. Um später die Festplatte doch noch verwenden zu können, wenn sich beispielsweise durch eine Reparatur eine der Hardwarekomponenten und damit der Schlüssel geändert haben, können Sie einen Wiederherstellungsschlüssel erzeugen. Entweder direkt über die Entsperrung über Ihr iCloud-Konto, oder indem Sie den Schlüssel manuell woanders speichern.


Sicherheit
Suchen
Dein iCloud-Account „sa[redacted]“ kann verwendet werden, um den Schutz deiner Festplatte aufzuheben und dein Passwort zurückzusetzen, falls du dein Passwort vergessen solltest.
Soll dein Passwort nicht mithilfe deines iCloud-Account zurückgesetzt werden, kannst du einen Wiederherstellungsschlüssel erstellen und diesen an einem sicheren Ort aufbewahren, um gegebenenfalls das Passwort deiner Festplatte zurücksetzen zu können.
Mein iCloud-Account darf meine Festplatte entsperren
Wiederherstellungsschlüssel erstellen und meinen iCloud-Account nicht verwenden
Abbrechen
Zurück
Fortfahren
Zum Schützen auf das Schloss klicken.
Weitere Optionen ...

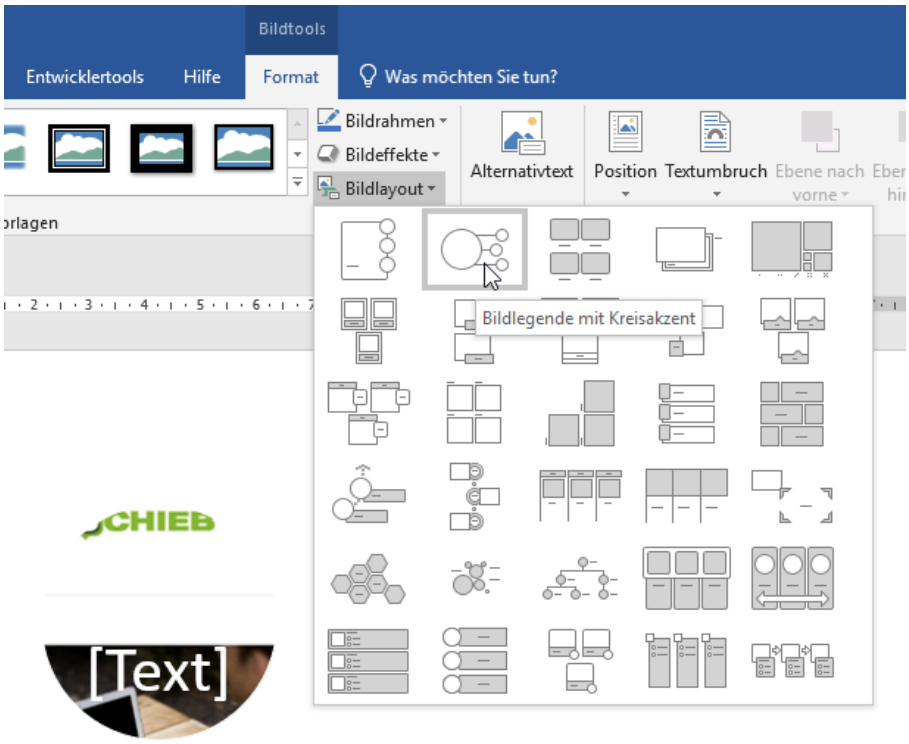
Optimal mit Screenshots arbeiten in Word

Bilder sagen immer mehr als tausend Worte. Und oft ist es so, dass Sie die Bilder nicht auf der Festplatte haben, sondern von einer Webseite holen, in einem Programm vorliegen haben oder aus einer anderen Quelle besorgen. Der einfachste und zeitsparendste Weg: Machen Sie Screenshots, und setzen Sie dazu kein eigenes Programm ein, sondern machen diese direkt in Word.

Relativ unbekannt ist, dass Word eine sehr komfortable Funktion zum erstellen und formatieren von Screenshots integriert hat. Statt externe Programme wie beispielsweise das kostenlose Greenshot zu verwenden, klicken Sie in Word einfach auf **Einfügen** > **Screenshot**.



Word erkennt nun offenen Fenster, auf Wunsch können Sie also direkt ein ganzes Fenster auswählen, ohne manuell etwas auszuwählen. Wenn Sie nur einen bestimmten Bereich brauchen, dann klicken sie auf **Bildschirmausschnitt**.



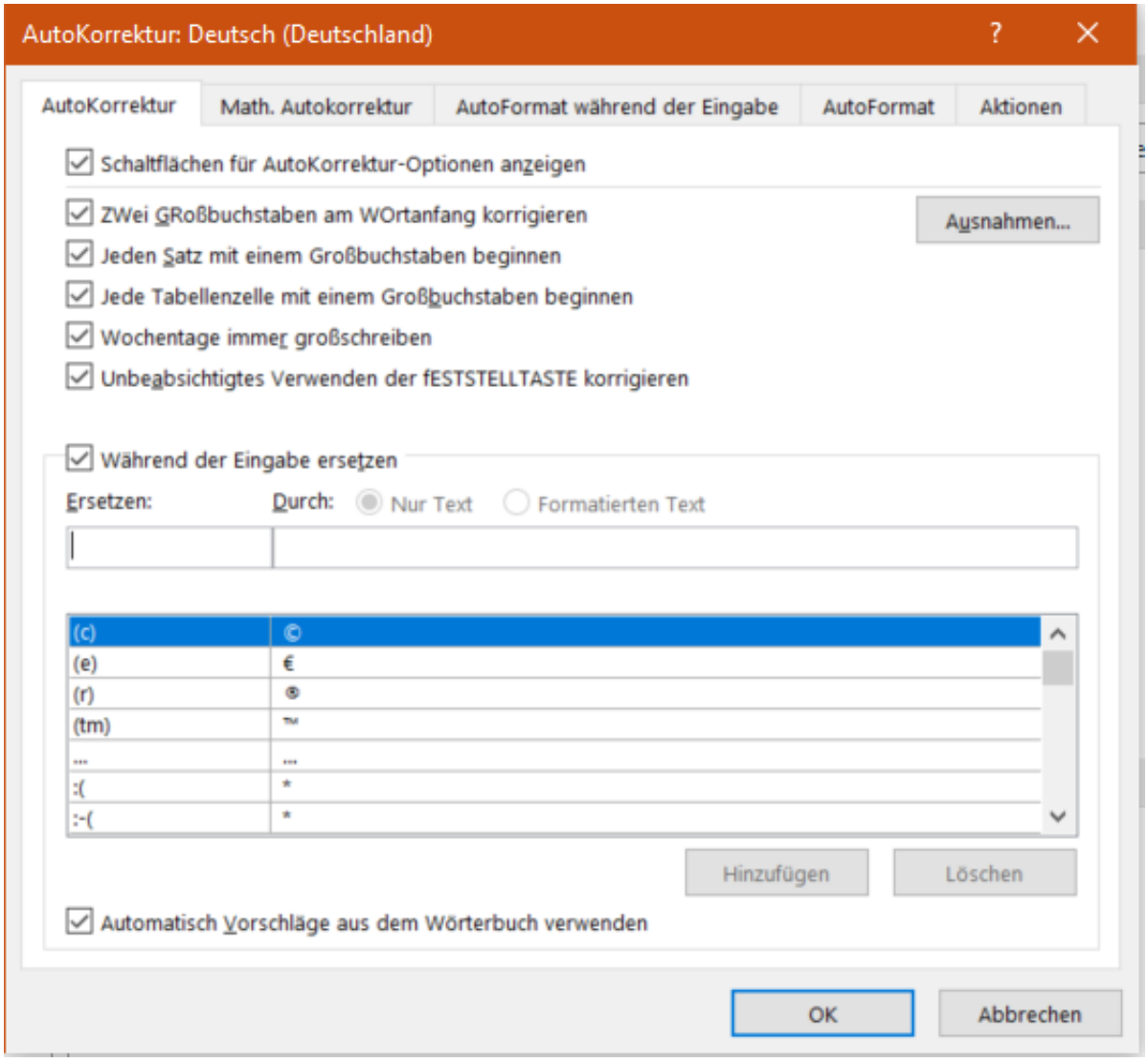
Der Bildschirm wird nach einem Moment heller und Word zeigt Ihnen einen Mauszeiger an, mit dem Sie einen Bildschirmbereich auswählen können. Rahmen Sie den Bereich des Bildschirms ein, wenn Sie die Maustaste loslassen, dann wird die Grafik eingefügt.

Wenn Sie jetzt auf **Bildlayout** klicken, dann können Sie die Form der Grafik anpassen und beispielsweise noch Texte als Unterschrift mit aufnehmen und eingeben. Die Position und den Textfluss können Sie dann wie bei jeder anderen Grafik festlegen.

Automatisches Ersetzen von Text in Word

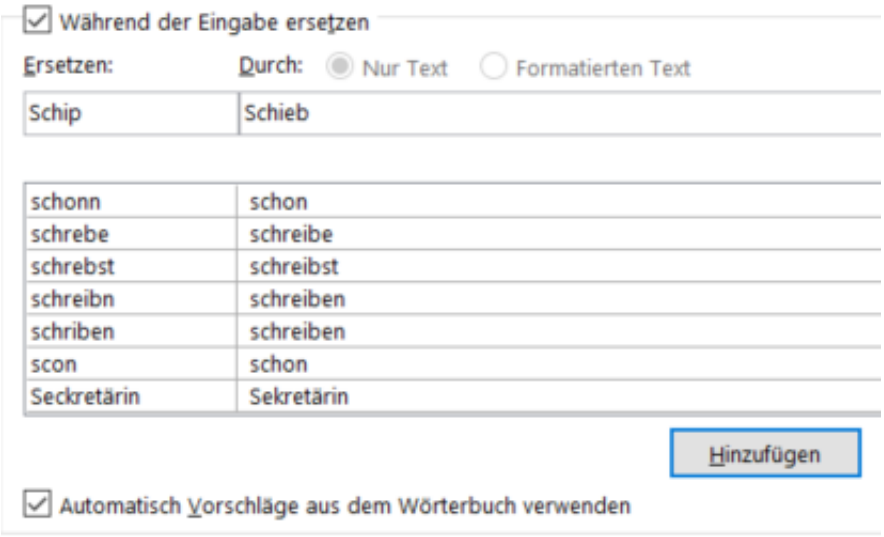
Sie haben keine Zeit. Alles muss immer schneller gehen. Das wirkt sich auch darauf aus, wie Sie tippen. Zum einen ist die Schnelligkeit ein Thema: Je schneller Sie drucken, desto eher machen Sie Tippfehler, und oft sind es die gleichen. Zum anderen gibt es bestimmte Phrasen, die immer wieder kommen. Statt "Mit freundlichen Grüßen" nur "mfG" zu tippen, würde massiv Zeit sparen. Word unterstützt Sie hier!

Sie können unterschiedliche Korrekturen und Ersetzungen konfigurieren, die Word dann automatisch im Dokument durchführen würde. Diese können Sie in Word unter **Datei** > **Optionen** > **Dokumentprüfung** > **Autokorrektur** erreichen. Hier sehen Sie einige allgemeine Einstellungen, die klassische Eingabefehler korrigieren. Zum Beispiel **ZWei GRoßbuchstaben am WOrtanfang korrigieren** (die Tippfehler sind keine, sondern deuten die Funktion an). Dieser Fehler kommt beim schnellen Tippen immer wieder vor.



Die richtigen Zeitsparer sind aber Ihre individuellen Vertipper und die automatische Ersetzung

von Abkürzungen. Dazu klicken Sie unter **Während der Eingabe ersetzen** auf das freie Feld und geben sie dann die Abkürzung bzw. den immer wieder falsch geschriebenen Begriff links und die richtige/ausgeschriebene Schreibweise rechts ein.

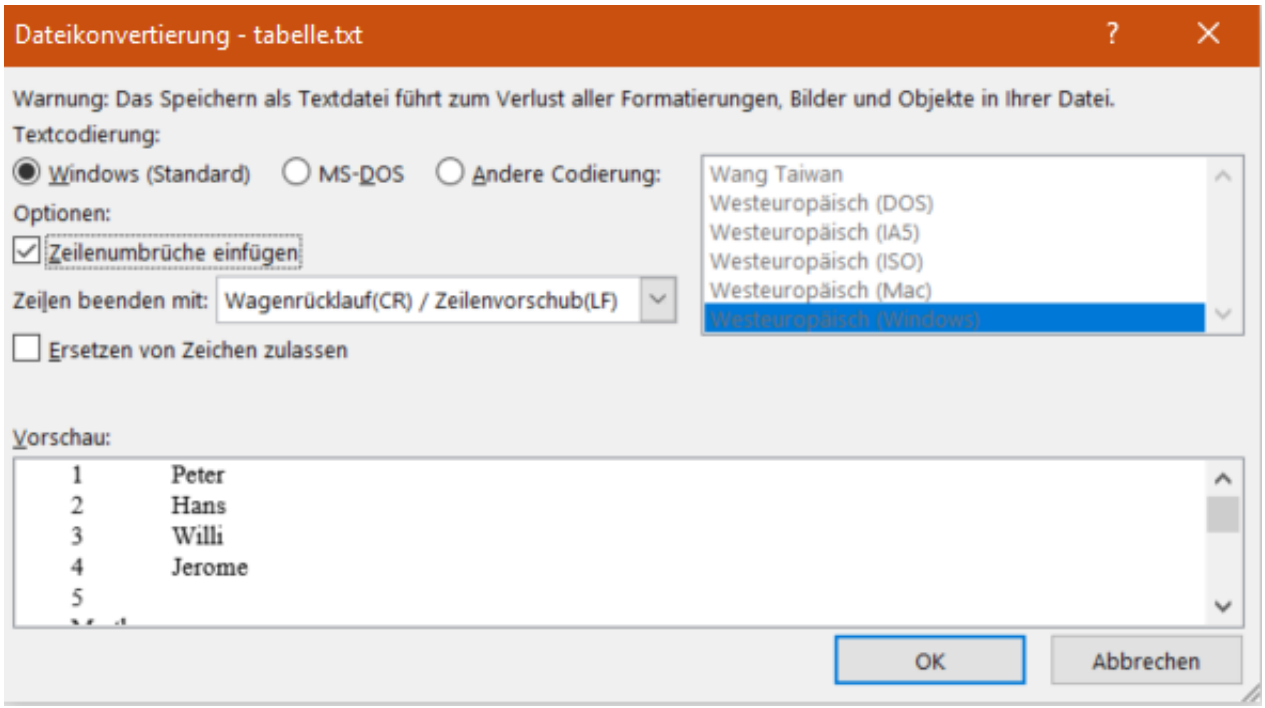


Durch einen Klick auf **Hinzufügen** können die Ersetzung dann hinzufügen. Diese wird sofort aktiv und lässt Sie Zeit und Frust beim schnellen Tippen sparen.

Textdateien in Excel einfügen

Wenn Sie Daten direkt in Form einer Excel-Tabelle bekommen, dann ist das Leben einfach. Öffnen Sie sie, Excel hat die Daten richtig formatiert in den Zellen und die Bearbeitung ist einfach. Oft bekommen Sie aber nur Text-Dateien, weil die Quelle ein Gerät wie ein Datalogger ist oder ein Programm, das nicht direkt im Excel-Format abspeichern kann. Wie zeigen Ihnen, wie Sie eine Textdatei in Excel importieren können.

Um die Daten aus der Textdatei in separate Spalten zu bekommen, ist folgendes wichtig: Es muss ein Trennzeichen vorhanden sein. Wenn Sie den Export aus dem Quellprogramm beeinflussen können, dann empfiehlt sich das CSV-Format. Die Abkürzung steht für Comma Separated Values, das Komma wird also zwischen den einzelnen Zellen automatisch hinzugefügt. Der Vorteil: Die Zellen können Leerzeichen enthalten.



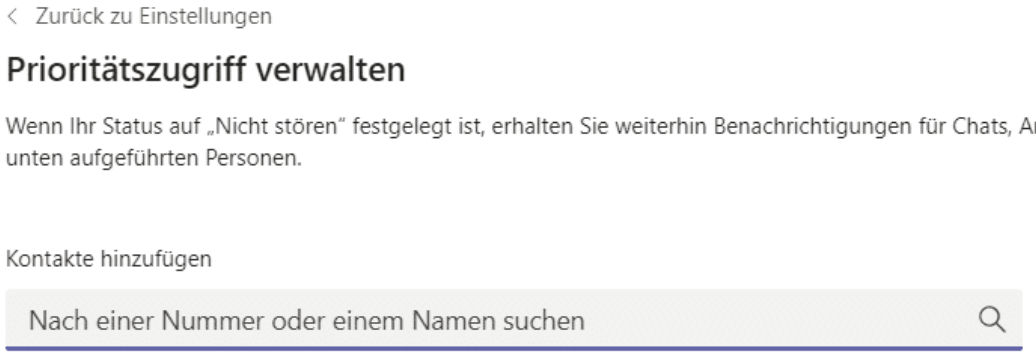
In Excel klicken Sie auf **Datei** > **Öffnen** > **Durchsuchen**, dann wählen Sie rechts vom Dateinamen Textdateien (*.prn. *.txt, *.csv) aus und öffnen dann die Textdatei von der Festplatte. Excel startet nun den Textkonvertierungs-Assistenten. Wählen Sie **Getrennt** als Dateityp, dann wählen Sie das Trennzeichen aus. Excel zeigt Ihnen in der Datenvorschau aus, die der Text aus der Datei auf die einzelnen Zellen verteilt werden würde. Experimentieren Sie nun so lange mit den Einstellungen herum, bis das Ergebnis in der Voransicht passt. Dann bekommen Sie eine wunderbar formatierte und bearbeitbare Tabelle.

Benachrichtigungen in Teams konfigurieren

Microsoft Teams ist die angedachte Lösung vieler Probleme: Telefonie, Chat, gemeinsames Arbeiten in einem virtuellen Team, das nicht notwendigerweise an einem Ort sitzen muss. Das führt dazu, dass Sie andauernd von Benachrichtigungen unterbrochen werden. Diese zeigen Ihnen neue Nachrichten, Benachrichtigungen zu Erwähnungen, Aufgaben und vieles mehr. Wir zeigen Ihnen, wie Sie die Benachrichtigungen auf Ihre Bedürfnisse anpassen.

Unter **Einstellungen** > **Benachrichtigungen** können Sie für jede einzelne Benachrichtigung festlegen, wie sie erfolgen soll. Sie können Sie **stumm** schalten, als **Banner**, **Banner und E-Mail** oder nur im Neuigkeiten-**Feed**. Diese Einstellungen aber sind generell gültig, es wird immer Gelegenheiten geben, in denen Sie weniger gestört werden wollen. In einem solchen Fall können Sie den Status **Nicht stören** wählen.

Der hat aber einen Nachteil: Dann bekommen Sie gar keine Nachrichten mehr. Nun können Sie sich auf den Standpunkt stellen "Dann muss man sich halt entscheiden!". Müssen Sie aber nicht: Klicken Sie in den Einstellungen auf **Datenschutz** > **Prioritätenzugriff verwalten**. Hier können Sie alle Teilnehmer eingeben, die in Ihrer Prioritätenliste sind. Von diesen Kontakten erhalten Sie dann auch während der "Nicht stören"-Zeiten Benachrichtigungen.


Zurück zu Einstellungen
Prioritätszugriff verwalten
Wenn Ihr Status auf „Nicht stören“ festgelegt ist, erhalten Sie weiterhin Benachrichtigungen für Chats, Anrufe
unten aufgeführten Personen.
Kontakte hinzufügen
Nach einer Nummer oder einem Namen suchen

Digitalisierung: Wem vertrauen im Netz?

Die Digitalisierung scheint nicht mehr aufzuhalten. Sie dringt in praktisch alle Bereiche unseres Lebens vor und ein. Und sie verändert auch die Art und Weise, wie wir uns informieren. Wie wir an Nachrichten kommen. Aber eben auch, wie wir uns eine Meinung bilden. Früher war das ein Monopol von Sendern, Verlagen, Medienhäusern. Heute kann jeder mit der Öffentlichkeit in Kontakt treten – und die Sozialen Netzwerke sind die Verteilstationen. Eine Folge der Digitalisierung.

Noch nie war es so einfach, sich zu informieren. Rechner anschalten oder Handy schnappen. Suchmaschine aufrufen. Suchbegriff eingeben. Voilà: Zig Fundstellen, kaum ein Thema mit dem sich nicht Dutzende oder hunderte Privatmenschen, Blogs, Youtuber und Foren beschäftigen.

Wenn es unbedingt Artikel sein müssen, hilft noch ein Klick auf "News" weiter, damit wirklich nur Nachrichten und Blogposts angezeigt werden. Andere recherchieren auf Twitter, bemühen einen News-Feed oder schauen bei Facebook nach.

Infos in Massen, nie war es leichter und schneller möglichen Fragen zu stellen und Antworten zu finden. Nur: Welche Antworten sind richtig? Welche Informationen gehören ins Köpfchen und welche in den digitalen Mülleimer? Wer kann schon immer so genau beurteilen, ob die Quelle der Nachrichten seriös ist, ob die Informationen stimmen?

Praktisch unbegrenzte Verteilung von Verschwörungstheorien

Das ist zum Beispiel in Zeiten von Corona durchaus riskant. Es geistern Verschwörungstheorien durchs Netz, die behaupten, frisch aufgestellte 5G-Masten seien für Corona verantwortlich. Die Regierungen wollten die Bevölkerung dezimieren. Andere geben Tipps, dass der Konsum von Knoblauch vor Corona schütze. Auf dem Videoportal TikTok sind Straßen mit lauter angeblichen Corona-Toten zu sehen.

Extrem schädlich, panikmachende, irre Beiträge, die nur Verwirrung stiften und Menschen gefährden können. Und die stehen gleichwertig wirkend neben mühsam recherchierten journalistisch aufgearbeiteten Beiträgen. Unsinn und Falschmeldungen werden leider nicht durch die Nutzer abgestraft, sondern mitunter sogar besonders viel geklickt. Gewinnt in der digitalen Welt die Meinungsmache vor den Fakten?

https://soundcloud.com/user-999041145/vertrauen

Was ist seriös, was verlässlich?

Im Netz muss man ständig auf der Hut sein. Selbst bei vermeintlich seriösen Quellen. So hat der US-Präsident gerade ein Video geteilt, das Präsidentschaftskandidat Joe Biden zeigt, der angeblich sagt: "Wir müssen Donald Trump wiederwählen".

Eine widerwärtige Manipulation, weil eine Rede entsprechend geschnitten und gestutzt und dann vom US-Präsidenten selbst verteilt wurde. Millionen Nutzer sehen sie innerhalb von Minuten. Die Technologie, die so etwas ermöglicht, erfordert einen disziplinierten Umgang, starke moralische Werte und viel Verantwortungsgefühl. Oder man missbraucht sie eben mit ein paar Klicks und einer Wischgeste für die eigenen Zwecke.

Meinungsfreiheit wird häufig missverstanden

Die sogenannten "Sozialen Medien", die alles andere als sozial sind und deshalb besser Online-Plattformen genannt werden sollen, entziehen sich jeder Verantwortung. Sie geben vor, die Meinungsfreiheit schützen zu wollen.

Meinungsfreiheit: Darunter verstehen viele auch Hass, Hetze, Lügen, Manipulation, Desinformation, Aggression... Hat es immer gegeben. Natürlich. Aber in der Vergangenheit hat man damit nicht immer gleich die ganze Welt erreicht.

Natürlich: Die Möglichkeiten von Internet und Online-Plattformen sind bemerkenswert. Das Wissen der Welt in der Hosentasche und ein Sprachrohr, das mich mit jedem verbindet oder eben der Spion, der mich aushorcht, mit Lügen füttert und manipuliert. Die Digitalisierung sie

löst große Probleme, schafft aber auch ganz neue.

#Corona: Arbeiten im Homeoffice - so wird es sicher

Viele Firmen bieten ihren Mitarbeitern an, von Zuhause zu arbeiten, sei es partiell oder sogar dauerhaft, weil Fachkräfte in der globalisierten Welt nun einmal nicht immer vor Ort sind -oder weil, wie im aktuellen Fall, das Corona-Virus besondere Maßnahmen erfordert. Das kann gut gelingen, wenn alle ein paar Sicherheitsmaßnahmen beachten.

Geübte Homeworker kennen sich bereits mit Heimarbeit aus und verfügen über die entsprechenden Zugänge und das Equipment wie Laptop und Smartphone. Aktuell aber gehen viele Unternehmen angesichts des explorativen Ausbruchs von SARS-CoV-2 auf Nummer sicher und bieten ihren Mitarbeitern die Möglichkeit, von Zuhause zu arbeiten.

Aber, damit die physische Sicherheit der Belegschaft nicht zugleich zur Bedrohung für die Cybersicherheit wird, müssen wichtige Maßnahmen beachtet werden.

Vorweg: Bleibt ein Kollege aus Präventionsgründen mit sofortiger Wirkung zuhause, bleibt keine Gelegenheit mehr, sich über den üblichen Weg – eingerichtetes Laptop und Telefon abholen und Vor-Ort-Schulung zum sicheren Teleworker – vorzubereiten. Das wahrscheinlichere Szenario sieht eher so aus: aus der Ferne und von Null an müssen die Geräte für die Verbindung mit dem Unternehmensnetzwerk aufgesetzt werden. Das ist mühsam und fehleranfällig.

Deshalb hier fünf Tipps, wie der Start in die Heimarbeit sicherer und einfacher gelingt:

1. Einfache Startbedingungen schaffen

Es gibt Produkte, die ein SSP anbieten, ein Self-Service-Portal. Ein Service, mit dem sich der Nutzer aus der Ferne verbinden kann, womöglich sogar mit einem Laptop ab Werk, und das sicher und einfach eingerichtet werden kann, ohne Vorort-Setup durch die betriebliche IT-Abteilung.

Viele SSPs erlauben es den Nutzern, zwischen verschiedenen Zugangslevels zu wählen, so dass sie entweder ein persönliches Gerät (wenn auch mit geringerem Zugang zu wenigeren Unternehmenssystemen als mit einem dezidierten Gerät) oder eines, das ausschließlich der Firmennutzung dient, verwenden können.

Die drei Schlüsselelemente, die man schnell und genau installieren sollte, heißen:

Verschlüsselung – Schutz – und Patching.

- Verschlüsselung bedeutet hier, dass die gesamte Geräteverschlüsselung aktiviert ist. Das schützt bei Diebstahl sämtliche Daten auf dem Gerät.
- Schutz heißt, zunächst einmal auf bewährte Sicherheitssoftware (wie Anti-Virus) zu setzen, Konfigurierung nach Bedarf.
- Patching inkludiert die Einstellung für den User, so viele Sicherheitsupdates wie möglich automatisch zu erhalten.

Notsituation Datendiebstahl: Hier gilt es zu klären, ob ein meldepflichtiger Datendiebstahl vorliegt. Um darzulegen, dass man als Unternehmen alle notwendigen Vorsichtsmaßnahmen erledigt hat, sollte man im Betrieb die Maßnahmen (als Beweis) dokumentieren.

2. Arbeitsfähigkeit ermöglichen

Wenn der Mitarbeiter seine Arbeit nur mit Zugang zu Server XY erledigen kann, dann muss dieser auch im Homeoffice gewährleistet sein. Im Idealfall hat man dieses VOR dem Ernstfall bereits wirksam getestet.

Nicht alle Arbeitsprozesse im Betrieb funktionieren auch im Homeoffice, sei es aus Sicherheitsgründen, juristischen Hürden oder auch einfach Unternehmensregeln. Das sollte klar und rechtzeitig kommuniziert werden, um Frust und fehlende Arbeitsschritte zu vermeiden. Als Mitarbeiter im Homeoffice sollte man sich auf der anderen Seite aber auch darüber im Klaren sein und nicht versuchen, diese Grenzen kreativ zu umgehen.

3. Sicherheitsüberblick über Heimgeräte bewahren

Der Heimschaffende sollte nicht mit der Funktionalität seiner Geräte allein gelassen werden. Verfügt der Nutzer wie empfohlen über ein automatisches Update, muss es Funktionen für das Unternehmen geben, die automatische Umsetzung auch zu überprüfen. IT-Mitarbeiter im Betrieb sollten bei akut auftretenden Problemen remote zur Seite stehen, um die Arbeitsprozesse nicht langwierig zu verzögern. Auch diese Zeit sollte der Betrieb in den Abteilungen einkalkulieren.

4. Ein Briefkasten für Sicherheitsprobleme

Hilfreich ist das Aufsetzen einer betrieblichen E-Mail-Adresse, an die die Mitarbeiter Sicherheitsprobleme schnell und unbürokratisch schicken können.

Vor dem Hintergrund, dass viele Cyberattacken erfolgreich sind, weil die Betrüger es immer wieder und genau so lange versuchen, bis es zu einem gedankenlosen Klick kommt, dient ein Sicherheits-E-Mail-Briefkasten auch der Prävention: Auffälligkeiten lassen sich schnell registrieren und Warnungen können folgen.

Alle Hinweise der Nutzer, selbst überflüssige, sollten unbedingt gewürdigt werden. Die Infos zum Security-Service wiederum landen am besten nicht im E-Mail-Account als Link, sondern, um es Betrügern auch in diesem Bereich schwer zu machen, offline via Brief, Infokarte oder Ähnlichem Zuhause.

5. Shadow-IT-Lösungen im Auge behalten

Shadow-IT heißt, dass Nicht-IT-Mitarbeiter mit ihren eigenen Möglichkeiten technische Probleme lösen, sei es aus Bequemlich- oder zeitlicher Dringlichkeit. Dieser Entwicklung muss nicht zwangsläufig Einhalt geboten werden, wie das folgende Beispiel deutlich macht. Allerdings sollte klar sein, dass „Shadow IT“ nicht nur für Probleme sorgen kann, wenn sie schief geht, sondern auch im Erfolgsfall – so z.B. bei Haftungsfragen.

Fallbeispiel

Arbeitet ein Kreis von Kollegen im Büro eng zusammen, ist jetzt aber durch das Homeoffice räumlich getrennt, werden sie vielleicht eine eigene Idee liefern, wie sie sich zukünftig austauschen wollen, auch mit Tools, die sie vorher nie verwendet haben. Diese Dynamik aus den Teams sollten Firmen nicht gleich ausbremsen, sondern unterstützen, sofern sie mit den Betriebssicherheitsregeln konform gehen. Eine temporäre Lösung kann auch neue und erfolgreiche Optionen für ein Unternehmen liefern. Als Organisation sollte man die Sicherheitsvorgaben klargemacht und Zugangsdaten zu den Teamlösungen haben, falls Passworte vergessen werden.

Fazit: Wo es im Realen jetzt Abstand halten heißt, gilt es virtuell zusammenzurücken

Wenn Unternehmen und Mitarbeiter also plötzlich in die Telearbeit einsteigen müssen, sollten sie eng und vertrauensvoll zusammenarbeiten. Wenn beispielsweise das IT-Team plötzlich darauf besteht, dass ein Kennwortmanager und 2-Faktor-Authentifizierung (2FA) verwendet wird, dann sollten Mitarbeiter der Aufforderung uneingeschränkt Folge leisten.

Auf der anderen Seite gilt es für die Systemadministratoren im Unternehmen, die heimarbeitenden Mitarbeiter und deren Fragen unbedingt ernst zu nehmen – egal wie oft sie sie stellen. Denn es kann sein, dass sie es beim ersten Mal nicht klar verstanden haben oder die Funktion, die sie benötigen, wirklich wichtig ist, um ihre Arbeit richtig zu machen.

Wir leben in schwierigen Zeiten. Für alle bedeutet dies, nicht zuzulassen, dass Angelegenheiten der öffentlichen Gesundheit die Art von Reibung verursachen, die der ordnungsgemäßen Durchführung der Cybersicherheit im Wege steht!

Im Trend: Deutsch lernen mit Apps und Online-Lernplattformen

Deutsche Sprache, schwere Sprache. Selbst Muttersprachler stolpern mitunter über bestimmte grammatikalische Regeln und Aussprachen. Wie schwierig muss es da für jemanden sein, der Deutsch nicht von Kindesbeinen an gelernt hat? Immer mehr Menschen aber müssen Deutsch lernen, weil sie hier leben - oder wollen Deutsch lernen, um sich besser mit Deutschen unterhalten zu können. Deshalb habe ich mal geschaut: Welche Lern- und Trainingsmöglichkeiten existieren denn da?

Eine fremde Sprache lernen: Zweifellos eine Herausforderung - aber eine, die durchaus Spaß machen kann.

Das Lernen selbst mag mühsam sein, doch der Weg zum Ziel bereitet auch Freude. Denn mit der Zeit versteht ein Sprachschüler immer mehr in der für ihn oder sie fremdem Sprache, kann sich besser ausdrücken - und wird am Ende mit einer Fähigkeit belohnt, die Freude machen kann: Sich mit anderen Menschen in einer eigentlich fremden Sprache unterhalten und sich im Land orientieren zu können.

Was Sie über Online-Nachhilfe wissen müssen

Sprachschulen sind natürlich immer eine gute Idee, wenn man eine fremde Sprache erlernen möchte. Aber mittlerweile lernen viele Menschen auch online und mit Apps. Doch wie effektiv ist

diese Art des Lernens wirklich und was sollte man beachten, wenn man schnell besser Deutsch sprechen will?

1. **Wo man den passenden Deutsch-Konversationskurs findet**

Man muss mittlerweile nicht mehr in der eigenen Umgebung nach Deutschlehrern suchen. Denn es gibt eine Vielzahl gut gemachter und nützlicher Apps und Webseiten, die einem dabei helfen, schnell und effektiv Deutsch sprechen zu lernen. Es ist aber für viele zu Beginn nicht einfach, in der Fülle des Online-Angebots den richtigen Kurs zu finden.

Eine der wohl bekanntesten und beliebtesten Online-Lernplattformen ist Preply – mit über 25’000 Lehrern und 100’000 Schülern, die Tag für Tag an Ihren Sprachkenntnissen arbeiten. Die Plattform macht es Einsteigern dabei sehr einfach, einen Deutsch Konversationskurs online zu absolvieren und im Nu besser Deutsch zu sprechen.

Dank digitalen Kommunikationsmitteln und einer ausgefeilten Videokonferenz-Software können Sprachschülerinnen und Sprachschüler sich auf Lernplattformen wie Preply effektiv und ortsunabhängig in der Konversation in Deutsch üben.

Die meisten Plattformen bieten zudem eigene Apps an, sodass Sprachschüler auch von unterwegs aus auf mobilen Geräten Deutsch lernen und Konversations-Übungen machen können – solange sie niemanden um sich herum stören...

2. **Die Vorzüge von Online Deutsch Nachhilfe**

Wer schon einmal in einem klassischen Nachhilfeinstitut nach Unterricht gesucht hat, der kennt auch die Nachteile: Man muss sich nach den meist starren Kurszeiten einer Schule richten, die Preise sind meist recht hoch und zusätzlich muss man noch Zeit für die An- und Abreise aufwenden. Kurz: Traditioneller Sprachunterricht kann ganz schön umständlich sein.

Wer hingegen Deutsch sprechen online üben will, der profitiert von den folgenden Vorzügen:

- **Maximale Flexibilität**: Auf Online-Lernplattformen stehen rund um die Uhr qualifizierte Nachhilfelehrer bereit. Man kann so den Unterricht ganz nach dem eigenen Rhythmus gestalten und die Lektionen in den Alltag integrieren.
- **Ortsunabhängigkeit**: Sie müssen sich weder zu einem Sprachinstitut noch zu ihrem Nachhilfelehrer bewegen, denn der Unterricht findet dort statt, wo es Ihnen passt – egal ob zu Hause, in einem Café oder im Hotel im Urlaub.
- **Volle Preiskontrolle:** Online Lernplattformen funktionieren wie Marktplätze, das heißt: je größer das Angebot, desto tiefer die Preise. Da sich auf Lernplattformen wie Preply tausende von Nachhilfelehrern tummeln, werden Sie keine Probleme dabei haben, Deutschunterricht in Ihrer Preisklasse zu finden.
- **Hohe Unterrichtsqualität**: Die meisten Lernplattformen stellen hohe Anforderungen an ihre Lehrer. Diese müssen sich und ihre Referenzen verifizieren lassen, sodass nur qualifizierte Nachhilfelehrer auf den Plattformen vertreten sind.
- **Effektives Lernen**: Sie haben dank Filter und Suchoptionen auf Online Lernplattformen

die Möglichkeit, ausschließlich mit deutschen Muttersprachlern Deutsch sprechen zu lernen. So erzielen Sie schnellere Fortschritte und üben mit Deutsch Trainern, die genau wissen, worauf sie achten müssen.

- **Kultureller Austausch:** Sie können übrigens mit Suchfiltern auch auswählen, von wo Ihr Nachhilfelehrer stammen soll. So bietet sich Ihnen die Möglichkeit, neben dem Verbessern Ihrer Deutschkenntnisse auch viel über die lokale Kultur des Konversationspartners zu lernen.
- **Zufriedenheitsgarantie**: Viele wissen nicht, dass die meisten Lernplattformen Probelektionen anbieten und bei Unzufriedenheit das bezahlte Geld zurückerstatten. So kann man ganz ohne Risiko einen neuen Lehrer ausprobieren.

3. **Wie kann ich mit Apps und Webseiten Deutsch sprechen lernen?**

Wer beginnen will, online Deutsch sprechen zu üben, der sollte folgendermaßen vorgehen:

1. Sich eine geeignete Lernplattform suchen (z.B. Preply, Busuu, Babbel, etc.)
2. Sich auf der Plattform anmelden und ein Profil anlegen: Das dauert in der Regel nur wenige Minuten.
3. Nach passenden Nachhilfelehrern suchen: Die meisten Plattformen bieten geeignete Filter an, um spezifisch nach Deutsch Konversationskursen zu suchen.
4. Eine Probelektion mit einem Nachhilfelehrer vereinbaren
5. Wenn Ihnen der Lehrer passt, lohnt es sich, frühzeitig Lernziele und den geplanten Lernrhythmus miteinander zu besprechen, sodass man sich voll auf das Deutsch Lernen konzentrieren kann.


heißt dein Opa? – Er
heißt Niko.

Fazit: Online-Plattformen und Lern-Apps bieten einige Vorzüge

Apps und Online Lernplattformen sind also eine praktische und sehr flexible Art, um

Fremdsprachen - auch Deutsch! - zu lernen. Die Einstiegshürden dafür sind eher gering. Wer mag, kann mit nur wenigen Klicks beginnen, per Videochat Deutsch zu lernen.

Dank innovativer Kommunikationstechnologie können Sprachschüler heute in Echtzeit mit Nachhilfelehrern Deutsch reden und in “Face-to-Face” Gesprächen seine Deutschkenntnisse verbessern. Die ausgefeilten Algorithmen der modernen Lernplattformen sorgen dabei für individuelle und erfolgversprechende Deutsch Konversationskurse.

Cortana in Windows 10 deaktivieren

Cortana war als direkter Angriff auf Apples Siri gedacht. Sowohl integriert in Windows 10 als auch auf dem mobilen Betriebssystem Windows Mobile/Windows Phone sollte die Sprachbedienung geräteübergreifend synchronisiert werden. Von Version zu Version wurde Cortana immer tiefer ein Windows integriert, bis die Deaktivierung gar nicht mehr möglich war.

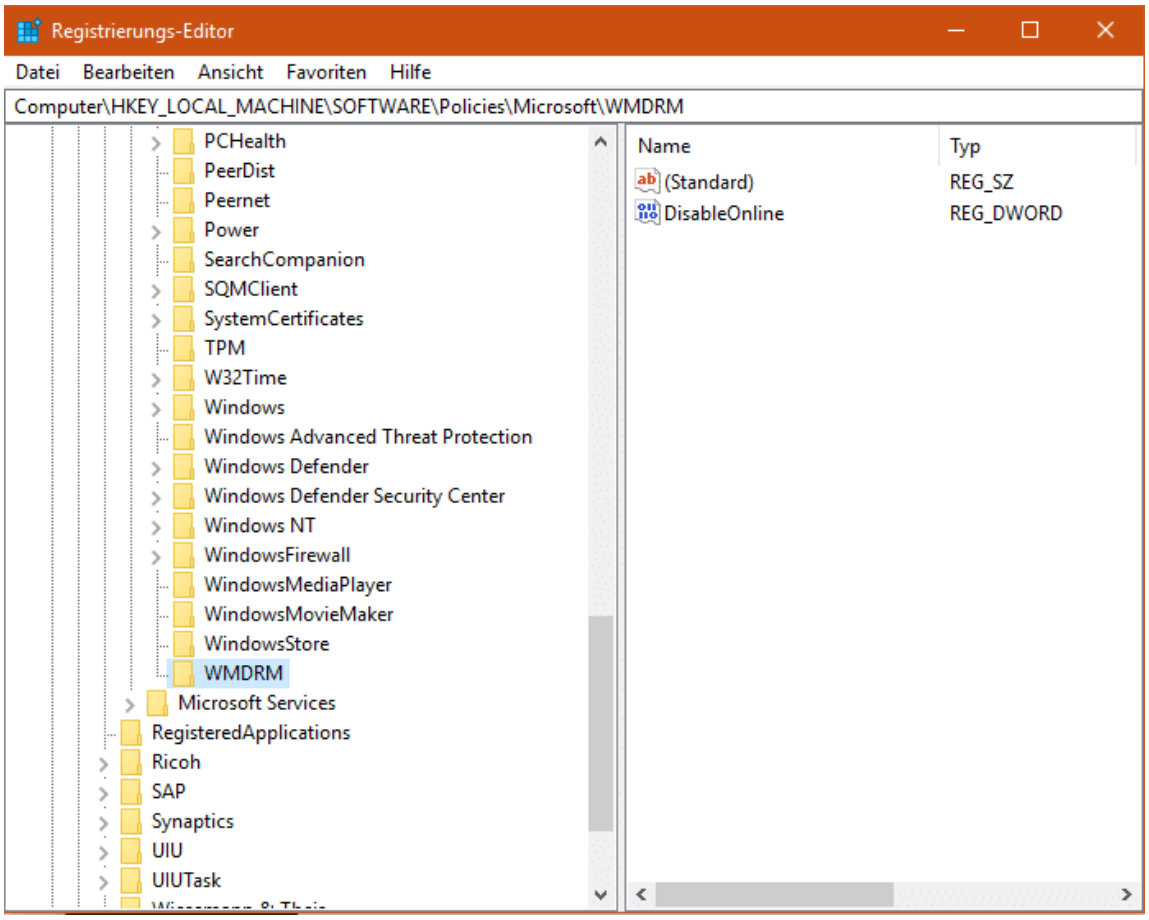
In den aktuellen Versionen lässt sich nur noch die Funktion "Hey Cortana", also die Aktivierung von Cortana per Sprachbefehl, deaktivieren. Diese Einstellung finden Sie unter **Einstellungen** > **Cortana**. Hier macht es auch Sinn, die Funktion von **Cortana im Sperrbildschirm** zu sperren.

Cortana nun aber komplett zu deaktivieren, ist seit dem Anniversary Update keine Option mehr. Microsoft hat viele interne Funktionen mit Cortana verknüpft, und will darum den Anwender davon abhalten, sie zu deinstallieren. Also müssen Sie auf die harte Tour ran: Deaktivieren Sie Cortana über die Registry.

Starten Sie den Registry Editor, indem Sie in der Suchleiste **regedit** eingeben und den **Registrierungs-Editor** starten.

Navigieren Sie dann zum Schlüssel

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search



Wenn **Windows Search** nicht existiert, dann klicken Sie mit der rechten Maustaste in den Windows-Eintrag und legen Sie ihn durch **Neu** > **Schlüssel** an.

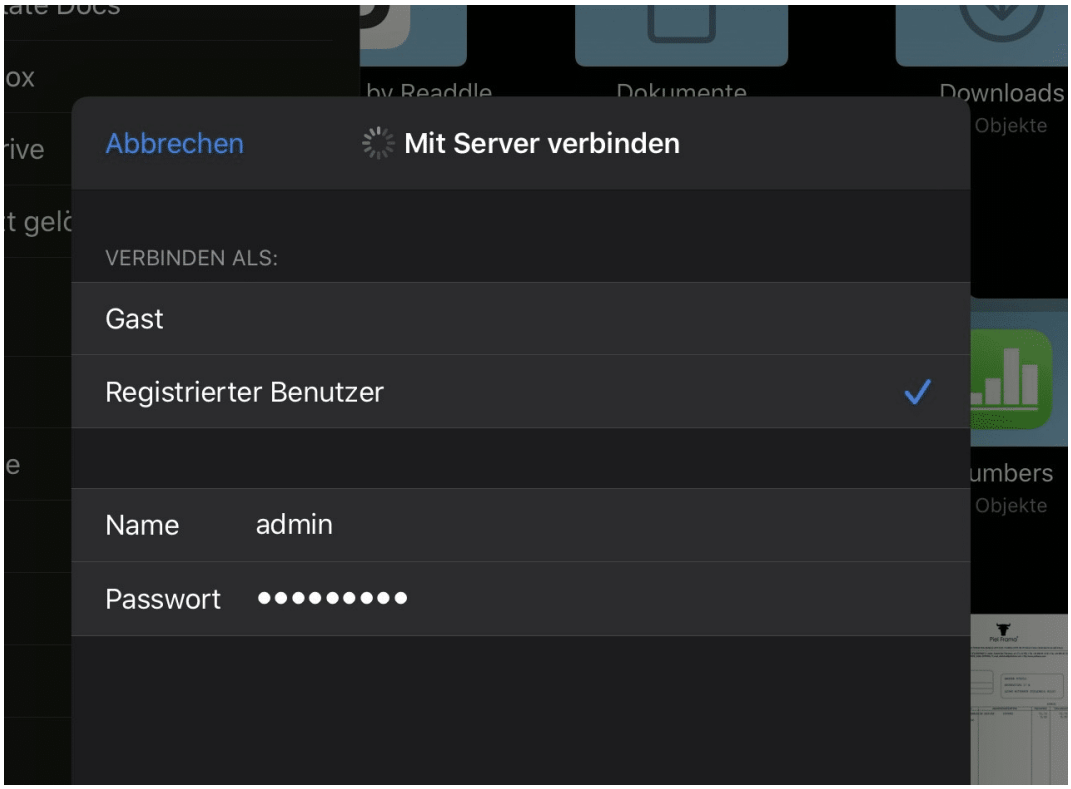
Legen Sie darin einen neuen **DWord-Wert (32-bit)** an, nennen Sie den **AllowCortana** und geben -sie ihm den Wert **0**. Nach einem Neustart ist Cortana deaktiviert und kann keine Daten mehr sammeln.

Direktzugriff auf Netzwerkfestplatten unter iPad OS 13

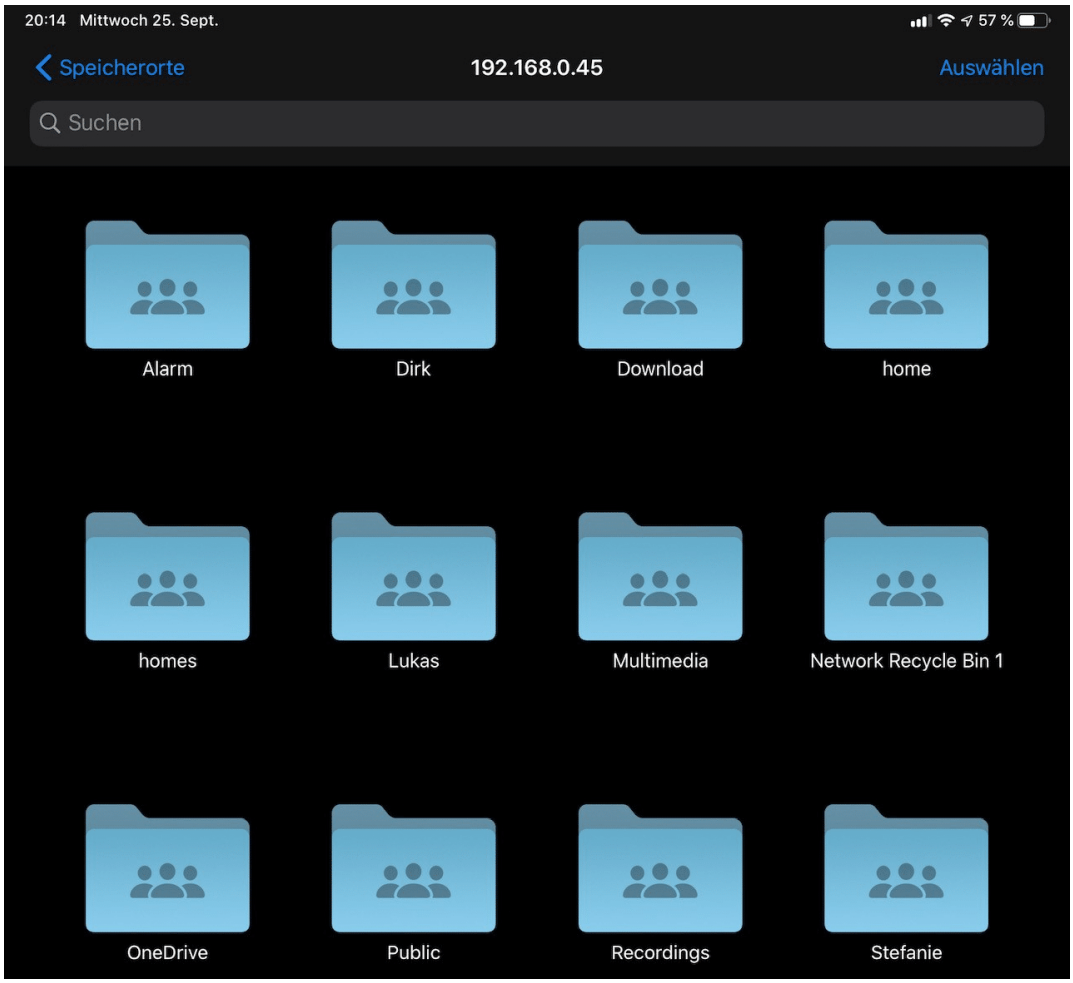
Lokaler Speicher ist out. Warum sollen Sie auf Ihren diversen Geräten Dateien doppelt führen? Speichern Sie sie auf einer Netzwerkfestplatte, dann können Sie in der Reichweite Ihres Netzwerks direkt von allen Geräten darauf zugreifen. Auf dem iPad war das lange nur mit Zusatzsoftware möglich. Mit der Einführung von iPadOS ist das jetzt - in Grenzen - auch nativ möglich. Sie müssen die Einstellungen nur finden.

Der Zugriff auf Netzwerkfestplatten hat eine Einschränkung: Er funktioniert direkt im System nur über das SMB ("Samba")-Protokoll. Das bedeutet, dass Sie bei Ihrer Netzwerkfestplatte dieses Protokoll auch aktiviert haben müssen. AFP und NFS reichen hier nicht aus. Das sollte aber kein Problem sein, die großen Hersteller wie QNAP und Synology haben SMB im Standard in den Systemen integriert. Nur eben nicht aktiviert. Schauen Sie dazu in der Anleitung Ihrer Netzwerkfestplatte nach, wie Sie SMB aktivieren können.

Starten Sie nun die **Dateien-App** von iPadOS. Tippen Sie auf die drei Punkte, dann auf **Mit Server verbinden**. Geben Sie nun die IP-Adresse des Servers in Ihrem Netzwerk ein, dazu Benutzername und Kennwort, mit dem Sie sich an die Netzwerkfestplatte anmelden.



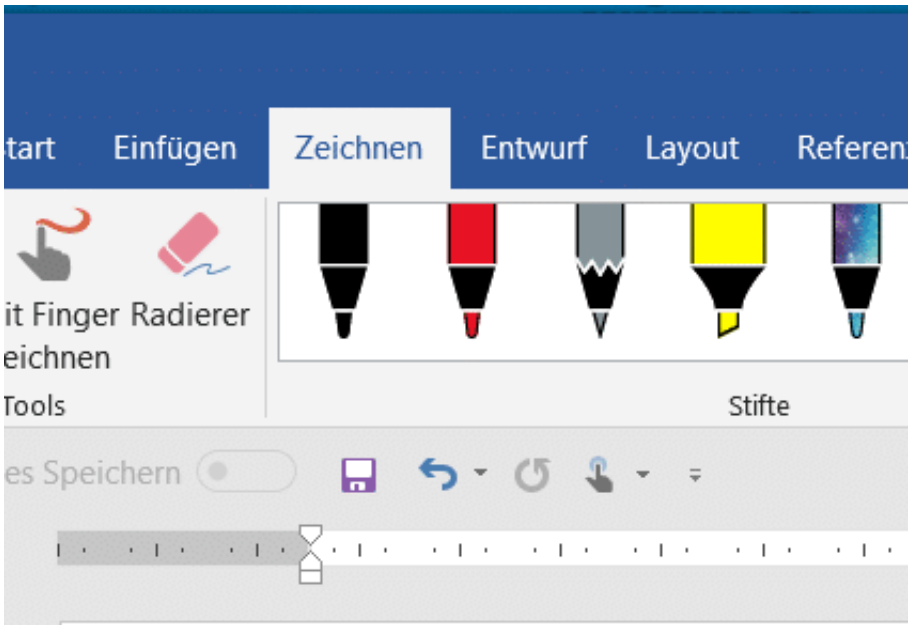
Nachdem die Verbindung erfolgreich hergestellt wurde, können Sie auf alle Freigaben der Netzwerkfestplatte zugreifen, Dateien Öffnen, auf andere Datenträger kopieren etc.


20:14 Mittwoch 25. Sept.
57 %
Speicherorte
192.168.0.45
Auswählen
Suchen
Alarm
Dirk
Download
home
homes
Lukas
Multimedia
Network Recycle Bin 1
OneDrive
Public
Recordings
Stefanie

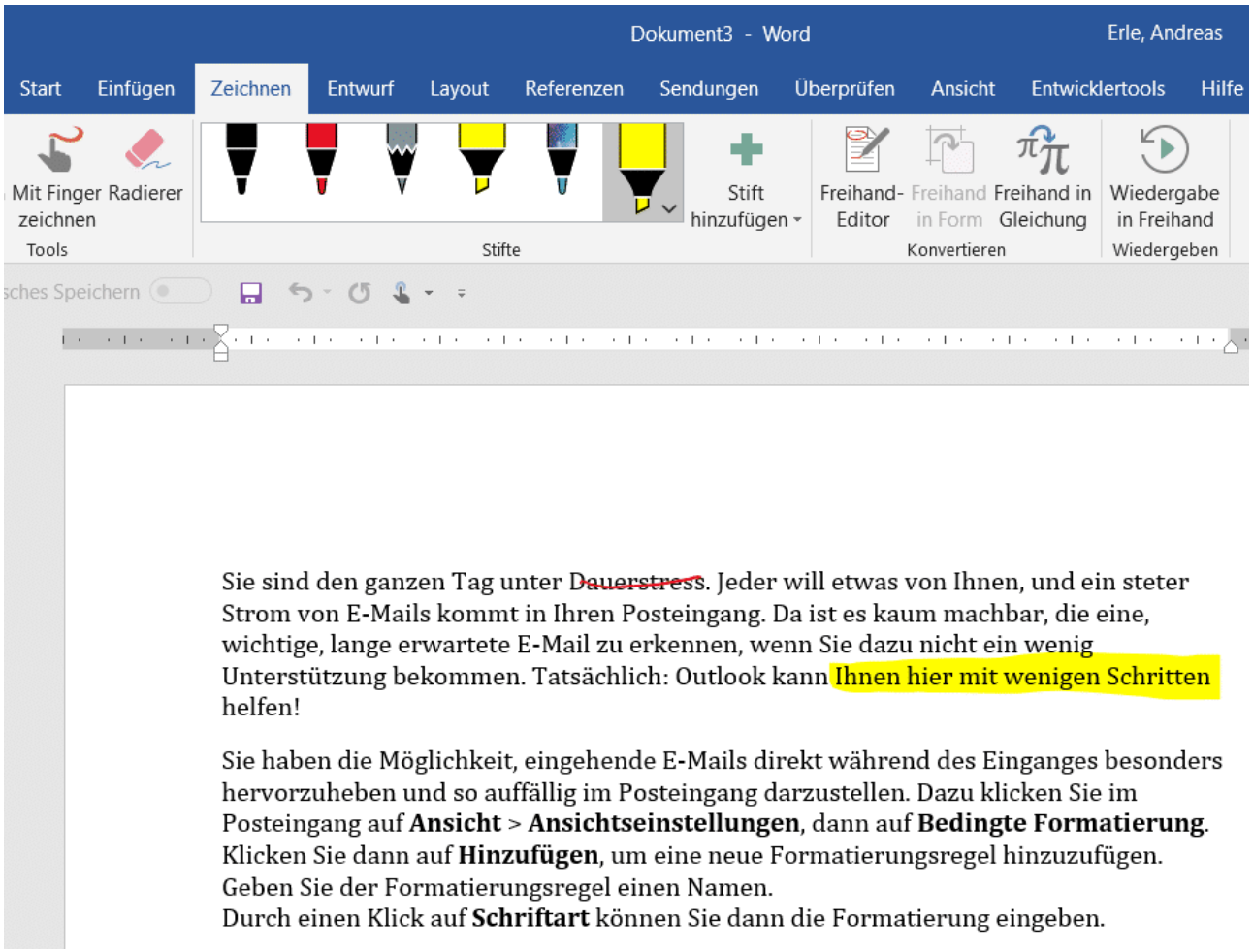
Kommentieren von Dokumenten in Office

Sie bekommen am Tag unzählige E-Mails mit Dokumenten, zu denen Sie etwas sagen sollen. Stellungnahme. Kommentar, Verbesserungsvorschlag, das ist leicht gesagt, aber manchmal schwer ausgeführt. Vor allem, wenn sie unterwegs sind. Das Speichern der Dokumente als PDF und dann die Bearbeitung in einem PDF-Viewer oder einer entsprechenden App ist keine wirkliche Alternative. Dabei können die Office-Programme das von Hause aus schon selbst!

Egal, ob Sie in Word, in Excel oder in PowerPoint sind, die neuen Versionen der Office-Programme haben einen Registerreiter **Zeichnen**. Klicken Sie darauf, dann öffnet sich eine Ansicht, in der Sie diverse Stifte sehen. Wenn Ihr Gerät einen Hardware-Stift hat, dann können Sie diesen direkt in die Hand nehmen und damit im Dokument Anmerkungen vornehmen.



Das Spannende: Die Datei wird im Ursprungsformat (DOCX, XLSX, PPTX) gespeichert inklusive der Anmerkungen, ist also entsprechend von jedem Empfänger mit den Office-Programmen zu öffnen und kann bearbeitet werden.



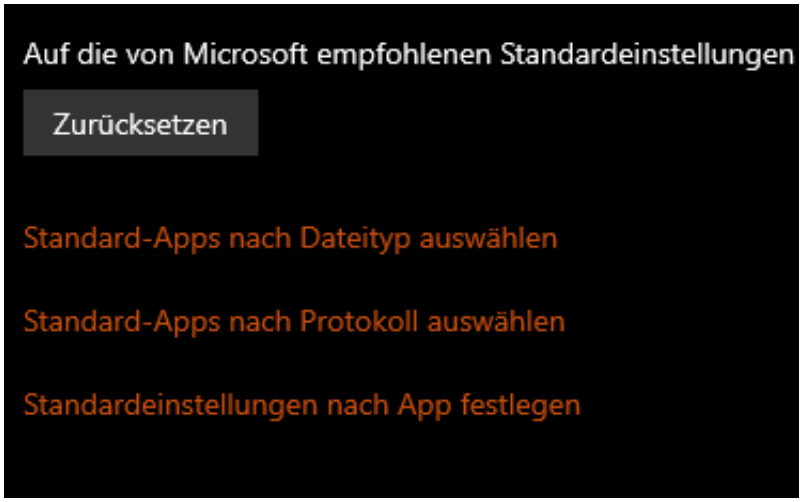
Haben Sie keinen Stift? Kein Problem: Klicken Sie auf die Schaltfläche **Mit Finger zeichnen**. Vorausgesetzt, dass Ihr Rechner einen Touchscreen hat können Sie einfach mit dem Finger auf dem Stift malen. Die Genauigkeit ist natürlich geringer, nichts desto Trotz haben Sie damit auch eine Vielzahl von zusätzlichen Möglichkeiten.

Edge als Standardprogramm für PDFs auswählen

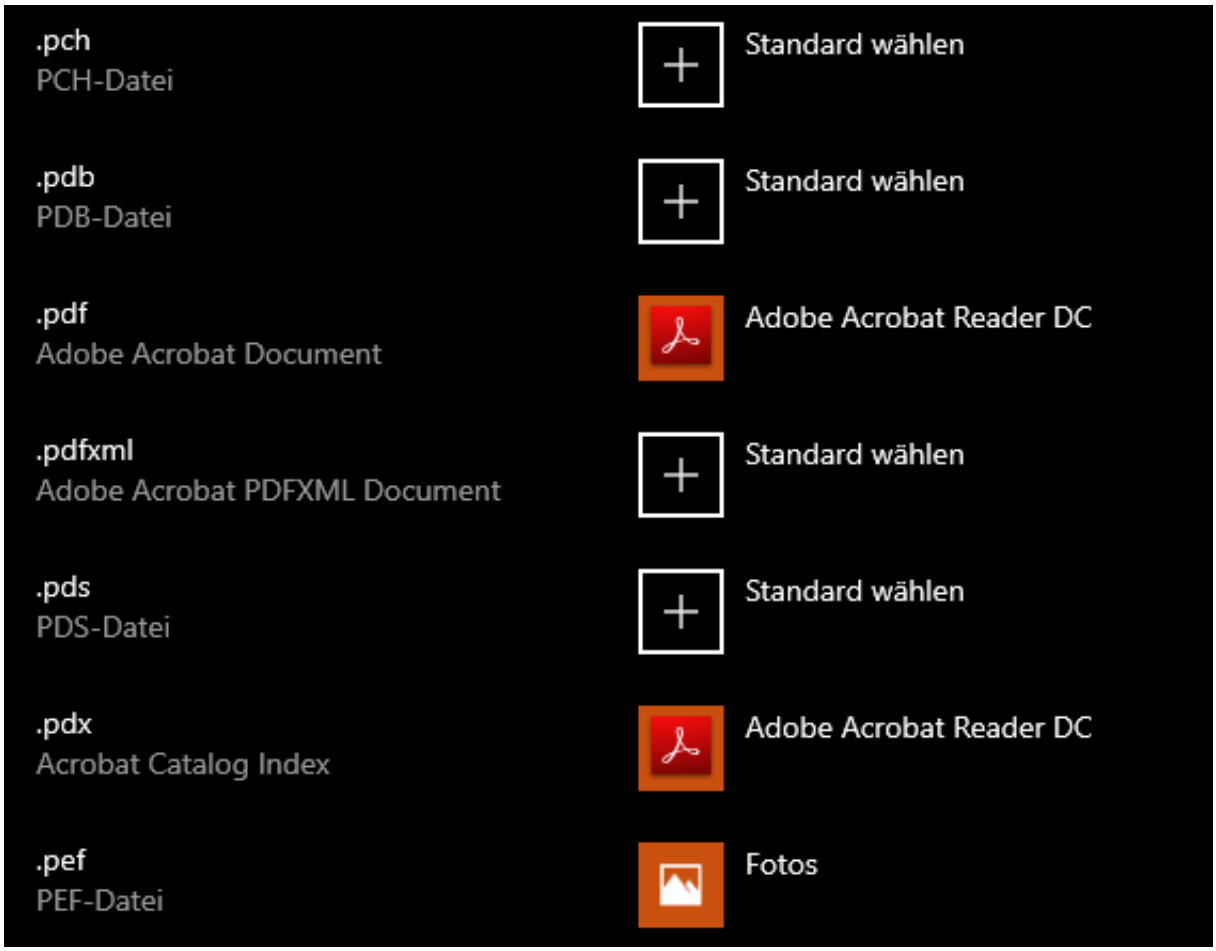
Der Acrobat Reader hat sich über die Jahre weiterentwickelt, ist aber in der kostenlosen Version immer noch nicht so leistungsfähig, wie man es sich wünschen würde. Parallel dazu hat sich Microsoft selbst immer mehr um das PDF-Format gekümmert. Edge - auch der neue Edge Chromium - sind leistungsfähige PDF-Bearbeitungsprogramme. Die können Sie sogar als Standard definieren.

Hier finden Sie einen Tipp, wie Sie direkt aus Windows heraus PDFs erzeugen können. Für die Bearbeitung einer selbst erzeugten (oder per E-Mail erhaltenen) PDF-Datei ist normalerweise der Acrobat DC nötig, auch wenn Word Ihnen hier auch helfen kann.

Eines der größten Mankos ist die mangelhafte Bearbeitungsmöglichkeit in Form von Kommentaren im Acrobat Reader. Das wiederum kann Edge hervorragend. Um diesen als Standard zum Öffnen von PDF-Dateiebn zu definieren, klicken Sie in den Windows 10-Einstellungen auf **Apps** > **Standard-Apps**.



Rollen Sie ein wenig nach unten und klicken Sie dann auf **Standard-Apps nach Dateityp** auswählen. Auf der linken Seite des Bildschirms sehen Sie dann eine Liste der Windows bekannten Datei-Erweiterungen. rollen Sie hinunter bis zu **.PDF**.



Klicken Sie auf den Eintrag rechts daneben. Normalerweise steht da **Adobe Acrobat Reader DC**. Klicken Sie auf den Eintrag, dann öffnet sich eine Liste von Apps. Wählen Sie darin Edge aus. Ab diesen Zeitpiunkt werden PDF-Dateien nach einem Doppelklick direkt in Edge geöffnet.