Schieb Report

Ausgabe 2022.13

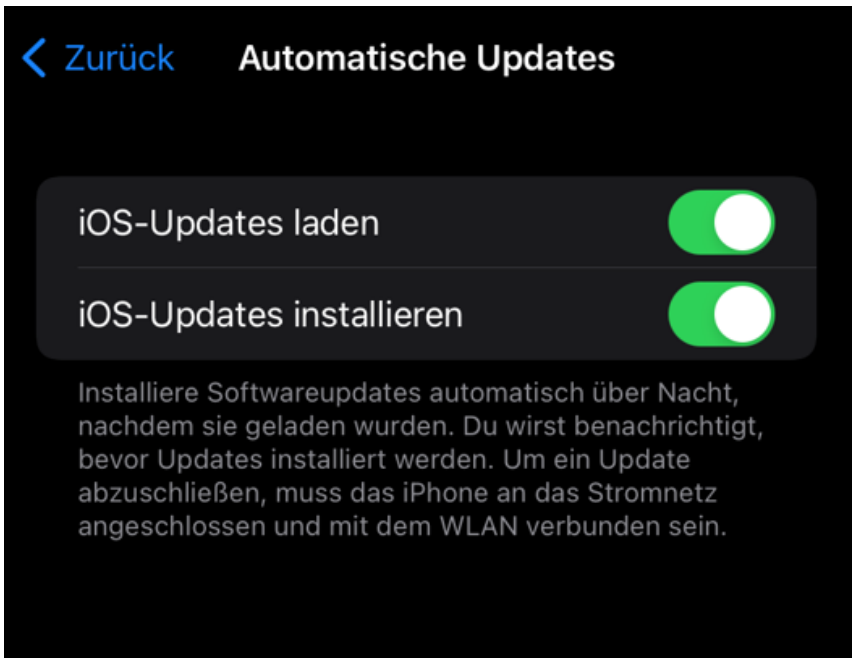
Updates auf Smartphones installieren

Das Betriebssystem ist der erste und wichtigste Punkt für Angriffe auf Eure Daten. Ein immer aktuell gehaltenes Betriebssystem ist schon einmal ein guter Basisschutz. Das gilt auch für Smartphones!

Auch Smartphones haben ein Betriebssystem. Ob Android oder iOS, Sicherheitslücken gibt es bei beiden Systemen. Wenn Ihr überlegt, wie viele persönliche und schützenswerte Daten Ihr auf Eurem Smartphone dabei habt, dann sind auch hier die potenziellen Schäden groß, wenn Daten verloren gehen. Also: Automatische Updates sind auch auf einem Smartphone Pflicht!

Unter iOS tippt auf **Einstellungen** > **Allgemein** > **Softwareupdate** > **Automatische Updates** > **Ein**, um die automatischen Updates zu installieren. iOS unterscheidet nach der Größe des Updates, ob es dieses auch bei einer Mobilfunkverbindung herunterlädt oder auf eine WLAN-Verbindung wartet. Lasst also WLAN eingeschaltet, sonst kommen große Updates nur manuell auf das

Gerät.



Bei Android tippt auf **Einstellungen** > **Geräteinformationen**" und aktiviert unter **Automatische Aktualisierung** die automatischen Updates.

Das Smartphone weist nach dem Herunterladen darauf hin, dass ein Update installiert werden soll und erlaubt es den Anwender, das zu verschieben. Durch den Neustart, der bei Smartphone-Updates Standard ist, würden Telefonate unterbrochen und Ihr wärt eine Zeit nicht erreichbar. Das könnt Ihr selbst durch verschieben der Installation beeinflussen.

Bitcoin und Blockchains sollen grüner werden

"Change the Code, not the climate" fordern Umweltschützer (unter anderem Greenpeace) in einer aufwändigen Kampagne von #Bitcoin Entwicklern. Es sollten unbedingt effizientere Methoden zum Einsatz kommen, so wie bei #Ethereum.

Energie sparen: Das ist aktuell ein besonders wichtiges Thema. Nicht nur wegen Klimawandel und Nachhaltigkeit, sondern auch wegen der möglichen Energieengpässe, ie entstehen können, wenn kein russisches Gas mehr ankommt. Wir haben uns so daran gewöhnt, dass alles im Überfluss vorhanden ist – auch Strom und Energie –, dass wir uns kaum bis gar keine Gedanken darüber machen.

Doch jetzt ist Umdenken angesagt. Zum Beispiel auch bei Bitcoin und Blockchains ganz allgemein. Der Bitcoin gilt als Klimasünder, weil er unheimlich viel Energie verbraucht. Doch jetzt gibt es einen Ansatz, wie sich dieser Energieverbrauch erheblich reduzieren lässt. Aber wie?

Kampagne von Umweltschützern

Eine aktuelle Kampagne der Umweltorganisationen Greenpeace (USA) und der "Environmental Working Group", die unter Cleanup Bitcoin auch im Netz zu finden ist, fordert möglichst schnell Änderungen am Prinzip (dem Code) der Kryptowährung Bitcoin. Das Ziel: den stromhungrigen Mining-Prozess überflüssig zu machen. Angesichts des Verbrauchs und der schlechten Umweltbilanz sollten die Entwickler lieber zum "Proof of Stake" (PoS) genannten Verfahren wechseln, auf das auch die Kryptowährungsplattform Ethereum umsteigen will.

Wie das Wall Street Journal berichtet, unterstützt Chris Larsen die Kampagne mit 5 Millionen US-Dollar. Der Gründer der Kryptowährung (und damit Bitcoin-Alternative) Ripple. Larsen besteht darauf, er handele hier als Privatmann und nicht als Repräsentant seiner Kryptogeld-Company.

Bitcoin und sein Energieverbrauch

Der Bitcoin ist eine Krypto-Währung – die erste Kryptowährung und zweifellos auch die bekannteste, aber ja keineswegs die einzige. Es gibt auch viele andere wie Ripple, Ethereum und viele andere. Aber bleiben wir beim Bitcoin. Es gibt gleich zwei Gründe, wieso der Bitcoin eine Menge Energie benötigt. Einmal bei der Erzeugung, dann auch bei der Verwaltung. Viele wissen es nicht, aber Bitcoin werden quasi „erzeugt“. So wie Banknoten gedruckt werden. Allerdings ist die Anzahl der Bitcoin technisch begrenzt: Es wird nie mehr als 21 Millionen Bitcoin geben. Es sind bereits weit mehr als 19 Mio. im Umlauf. Jeden Tag kommen etwa 1.800 neue dazu. Bis Schluss ist. Diese Bitcoin müssen „errechnet“ werden.

Vereinfacht gesprochen: durch Knacken besonders schwieriger Rechenaufgaben. Das machen Privatleute, keine Bank. Wer einen neuen Bitcoin errechnet, das wird auch „Mining“ (Schürfen) genannt, darf ihn behalten. Es wird aber immer schwieriger, neue Bitcoins zu erschürfen, je mehr Bitcoins es gibt. Und deshalb ist der Rechenaufwand enorm – entsprechend hoch ist auch der Energiebedarf. Laut der University of Cambridge verbraucht der Bitcoin schon jetzt mehr Energie als Schweden – und laut den Forschern entwickelt sich das rasant.

Kritik am Klimakiller-Vorwurf

Das ist auch ein Argument der Bitcoin-Befürworter – und es stimmt natürlich auch. Aber die Forscher unterstellen einen gewissen Strom-Mix. Und auch die Verwaltung der Bitcoin in der berühmten Blockchain – eine Art dezentrale Verwaltung und Buchhaltung des Bitcoin – verbraucht Energie. Je mehr Bitcoin es gibt, je mehr Transaktionen, desto höher der Aufwand und der Energiebedarf.

Im Journal „Nature“ ist nachzulesen, dass laut einer Studie der Bitcoin alleine auf Dauer für bis zu 2 Grad Klimaerwärmung verantwortlich sein könnte, wenn die Kryptowährung großflächig eingesetzt würde. Was derzeit aber nicht der Fall ist. Diese Kalkulation ist quasi eine GAU-Studie.

Legt aber den Finger in die Wunde: Bitcoin verbraucht wahnsinnig viel Energie. Und selbst wenn alle Miner grüne Energie verwenden würden, so steht diese grüne Energie nicht für andere wichtige Aufgaben zur Verfügung – und wird dann dort durch fossile Energie substituiert.

„Unfun fact“: Organisierte Miner von Bitcoin haben sogar Kohleminen in den USA gekauft und setzen auch Fracking-Gas ein, um auch die letzten nicht mal mehr zwei Millionen Bitcoin „erschürfen“ zu können. Denn das ist ja ein Geschäft: Ein Bitcoin ist 42.000 EUR wert – da kann man also investieren. Doch die meisten Miner achten eben nicht auf Nachhaltigkeit.

Bitcoin "den Stecker ziehen"?

Kann man ihnen nicht einfach den Stecker ziehen?

Ja und Nein. China zum Beispiel hat im September 2021 das Mining und den Handel mit Bitcoin und anderen Kryptowährungen untersagt. Offiziell wegen des hohen Energiebedarfs. Denn es gab so viele Bitcoin-Miner in China, dass sogar die generelle Energieversorgung des Landes gefährdet war. In Wahrheit wird China aber auch andere Gründe gehabt haben, den Bitcoin zu verbieten.

China hat ja gerne die Kontrolle über alles. In der EU hatte ein Verbot des Bitcoin erwogen, aber sich dagegen entschieden. Bitcoin-Miner sind sehr agil: Sie gehen schnell dort hin, wo der Strom günstig ist. Also würde nur ein weltweites Embargo/Verbot dazu führen können, das Schürfen neuer Bitcoins zu unterbinden. Faktisch ist es unmöglich.

Greenpeace stellt Forderungen

Nun gibt es aber Forderungen von Greenpeace – und vielen anderen –, etwas zu ändern. Es sei nämlich möglich, den Energiebedarf deutlich zu reduzieren.

Es gibt eine Kampagne „Change the code, not the climate“ – also „ändere den Code, nicht das Klima“ – hinter dem vor allem Greenpeace steckt, macht aktuell auf das drängende Problem aufmerksam. Mit einer eigenen Webseite unter anderem. In der Tat gibt es heute sehr viel bessere Methoden, Kryptowährungen zu managen als das bei Bitcoin der Fall ist.

Bei Bitcoin kommt „Proof of Work“ zum Einsatz, da wird sozusagen Rechenarbeit belohnt. Sehr viel effektiver ist das „Proof of Stake“-Verfahren. Die Kryptowährung Ethereum setzt jetzt auf dieses Verfahren, hat also umgestellt. Ein anderes Modell, das quasi mit Bürgschaften arbeitet.

Und was lässt sich damit sparen? Laut Wissenschaftlern unglaubliche 99%. Das bedeutet, dass 99% des Energieaufwands und damit auch des CO2-Ausstoßes eingespart werden könnten.

Wieso also warten: Ab die Post – und Bitcoin auch umstellen, oder?

Wenn das mal so einfach wäre. Denn dann müsste praktisch die gesamte Bitcoin-Infrastruktur umgestellt werden. Alles müsste neu programmiert und ersetzt werden. Die alten Bitcoin gegen neue getauscht. Ein riesiger Aufwand. Grundsätzlich denkbar wäre das. Aber die, die viele Bitcoin haben und/oder die Infrastruktur bestreiten, etwa den Tausch Bitcoin/echtes Geld wie EUR, haben viel in ihre Systeme investiert und werden das nicht freiwillig machen. Genau deshalb die öffentliche Kampagne: Sie will Entscheider und auch Politik erreichen, damit ein Umdenken stattfindet und Druck erzeugt wird. Im Interesse des Klimas wäre das auf alle Fälle.

Aber wäre der Vorteil nicht irgendwann aufgebraucht – weil dann, wenn

Kryptowährungen und Blockchains generell einen grünen Anstrich haben, sie dann plötzlich 100x mehr eingesetzt werden – und der Vorteil dann kompensiert wird?

Nun, diese Bereiche explodieren sowieso. Es wäre also zweifellos sinnvoll dafür zu sorgen, dass die Techniken deutlich energieeffektiver werden. Blockchains kommen in vielen sinnvollen Projekten zum Einsatz. Ein Metaverse ohne Blockchain wäre auch nicht vorstellbar. Man muss also alles gleichzeitig machen: Bei Blockchains konsequent auf „Proof of Stake“ umstellen und dafür sorgen, dass Rechenzentren weltweit generell grüne Energie einsetzen. Denn Bitcoin und Blockchain sind wahrlich nicht die einzigen Klimasünder, wenn es um Digitalisierung geht.

Phishing-Schutz im Browser aktivieren

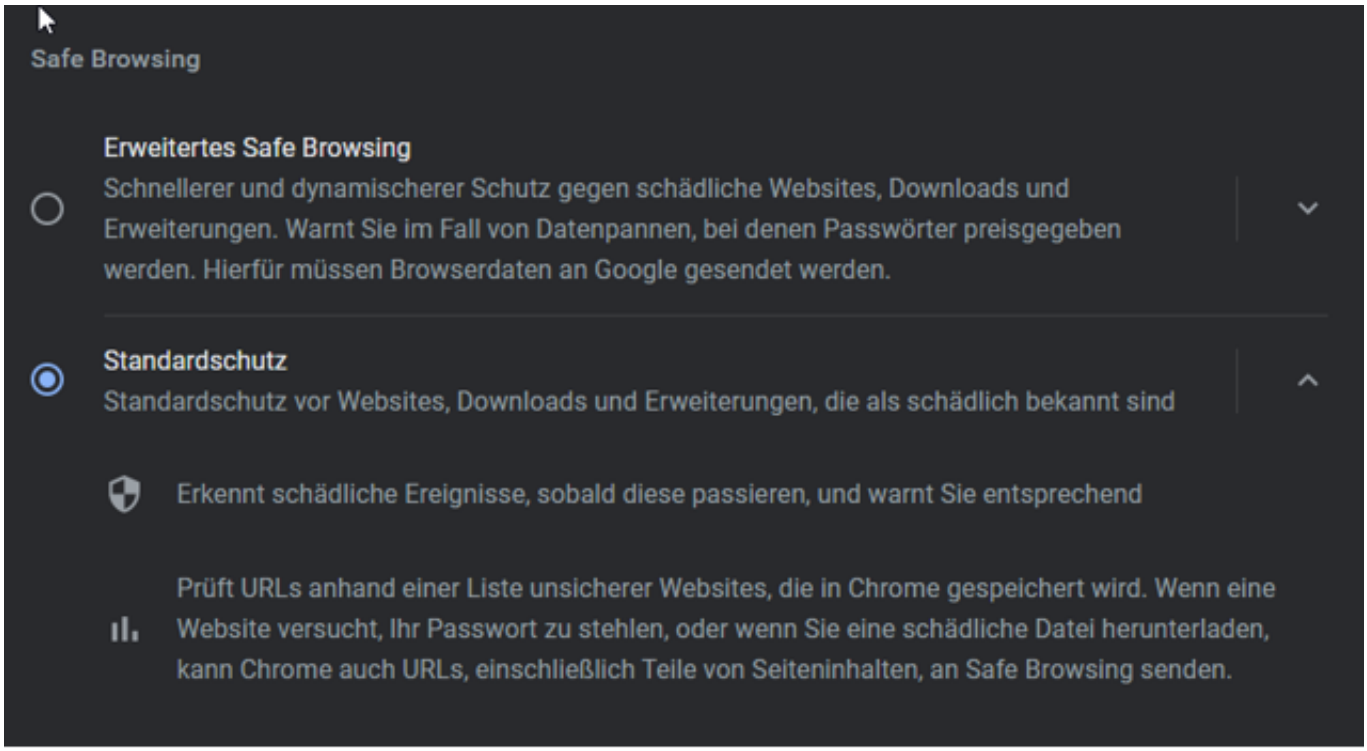
Hinter allen Browsern stehen große Hersteller, für die das Thema Sicherheit extrem wichtig ist. Darum haben sie Mechanismen an Bord, die Euch vor betrügerischen Webseiten und Phishingversuchen schützen sollen. Ihr müsst sie nur aktivieren und nutzen!

Microsoft Edge

Einmal mehr hat Microsoft es einfacher als andere Hersteller: Man nutzt einfach die Mechanismen, die sich auch für Windows als Betriebssystem bewährt haben.

- In Edge klickt auf die **drei Punkte** oben rechts > **Einstellungen** > **Datenschutz, Suche und Dienste**.
- Rollt ganz nach unten in den Bereich Sicherheit, dort finden sich zwei wichtige Optionen.
- **Microsoft Defender Smartscreen** nutzt den Cloud-Service von Microsoft, in dem Informationen von Benutzern aus der ganzen Welt zusammen

laufen und aktuelle Phishing-Attacken sammeln, analysieren und die Browser der Benutzer dagegen wappnen.
- **Potenziell unerwünschte Apps blockieren** verhindert den versehentlichen oder absichtlichen Download von Apps, die Schaden verursachen oder das System instabil machen können.
- Aktiviert beide Optionen, um Euch zu schützen!



Mozilla Firefox

Auch Firefox bietet entsprechende Schutzfunktionen:

- Klickt auf das **Hamburgermenü** oben rechts > **Einstellungen** > **Datenschutz & Sicherheit**.
- Rollt ganz nach unten in den Bereich Sicherheit, dort befindet sich die Option **Gefährliche und betrügerische Inhalte blockieren**. Aktiviert darunter beide Punkte.
- Zusätzlich Aktiviert den **Zertifikatscheck**. Der sorgt dafür, dass die Zertifikate, die die Vertrauenswürdigkeit von Webseiten sicherstellen, noch einmal unabhängig bestätigt werden.

Google Chrome

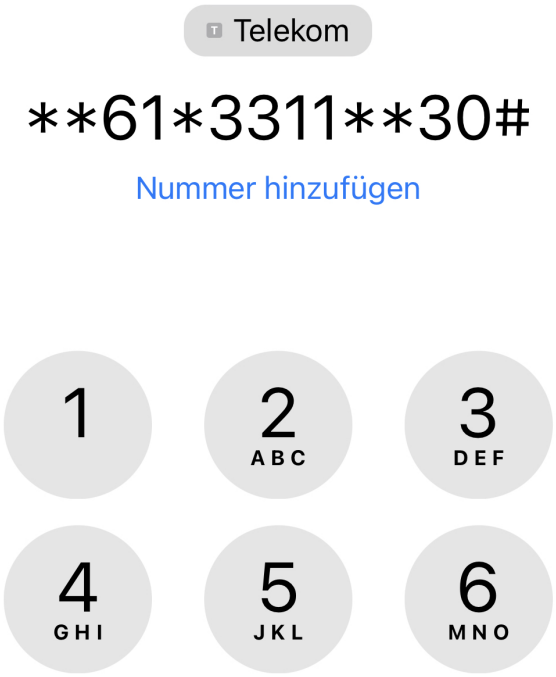
Google Chrome nutzt wie Microsoft Edge die Chromium Engine als Basis, trotzdem sind die Anti-Phishing-Optionen ein wenig anders:

- Klickt auf die **drei Punkte** oben rechts > **Einstellungen** > **Datenschutz & Sicherheit**.
- Rollt nach unten zu **Safe Browsing**.
- Neben dem **Standardschutz** bietet Chrome auch noch das **Erweiterte Safe Browsing**, das ein Cloud-Lösung ähnlich dem SmartScreen von Microsoft, verwendet. Dazu müsst Ihr allerdings zustimmen, dass detailliertere Informationen an Google geschickt werden.

Verlängern der Klingeldauer bei Smartphones

Das Telefon klingelt. Bevor Ihr den Anruf annehmen konntet, ist schon die Mailbox drangegangen. Das muss nicht sein, meinen wir. Und zeigen Euch einen Hack, der hilft!

Vorab: Die Dauer des Klingelns ist keine Einstellung des Smartphones! Sucht also nicht in den Menüs, da werdet Ihr keine Einstellungen dazu finden. Im Gegensatz zu Anrufbeantwortern, Faxgeräten und anderen Geräten ist hier der Netzbetreiber Eurer SIM-Karte der Verantwortliche. Die Mailbox beziehungsweise die Ansage, dass Ihr nicht erreichbar seid, kommt über das Netz.



Nun könnt Ihr nicht einfach so Netzeinstellungen ändern, zumindest nicht global. Für die Anpassung individueller Netzfunktionen bieten die Netzbetreiber allerdings die so genannten Netzbetreibercodes an. Die werden über die Tastatur eingegeben und dann mit dem grünen Hörer abgeschickt, als würdet Ihr eine Rufnummer anrufen. Stattdessen führt das Netz den Befehl aus und meldet den Erfolg zurück.

Für die Verlängerung des Klingelns ist der Code

61*#

Der Netzcode ist für die Telekom 3311, für Vodafone 5500 und für O2 333 (kein Tippfehler, er ist wirklich nur dreistellig!). Für die Sekunden könnt Ih 5-30 eingeben, in 5 Sekunden-Schritten. Im Beispiel oben wird also eine Telekom-SIM-Karte (3311) auf 30 Sekunden Klingeldauer eingestellt. Nach erfolgreichem Abschluss des Vorgangs zeigt Euer Smartphone Euch eine Erfolgsmeldung an:

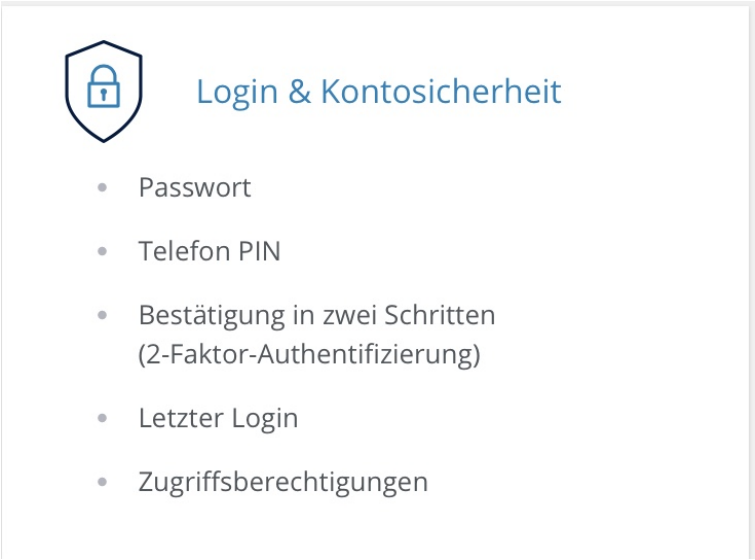

Einstellung erfolglos: Registrierung
Rufweiterleitung: Synchrone Datenübertragung
Wenn unbeantwortet
Einstellung erfolglos: Registrierung
Rufweiterleitung: Asynchrone Datenübertragung
Wenn unbeantwortet
Schließen

Zwei-Faktor-Authentifizierung (2FA) bei IONOS/1und1 einrichten

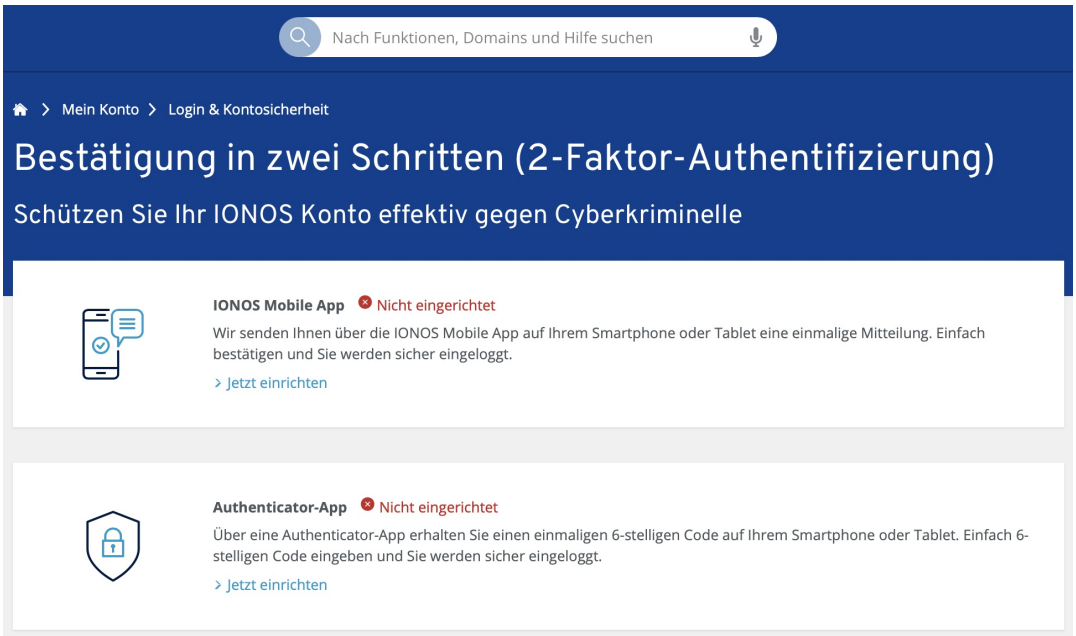
Ein Passwort ist nicht mehr Schutz genug. Zu einfach kann es gehackt werden. Die Lösung: Die Zwei-Faktor-Authentifizierung. Die lässt sich auch bei Webseiten von IONOS/1&1 einfach einrichten!

Passwort-Leaks, Phishing-Attacken, Social Engineering, die Möglichkeiten, das Passwort an Übeltäter zu verlieren, sind unzählbar. Das ist bei E-Mail- und Dienstkonten schon eine Katastrophe, bei einer Webseite sind die Auswirkungen noch einmal andere. Das Defacing, das Ersetzen der Inhalte der Seite durch Nachrichten der "Eroberer", hat eine direkte Außenwirkung. Diese Fall kann eintreten, wenn ein Angreifer die Zugangsdaten erbeutet. Das Anmelden am Hosting-Konto und das Ändern der FTP-oder Wordpress-Zugangsdaten ist dann ein Klacks. IONOS/1&1 als einer der verbreitetsten Hoster bietet als Schutz dagegen die Zwei-Faktor-Authentifizierung bei der Anmeldung an die

Administrationskonten an.



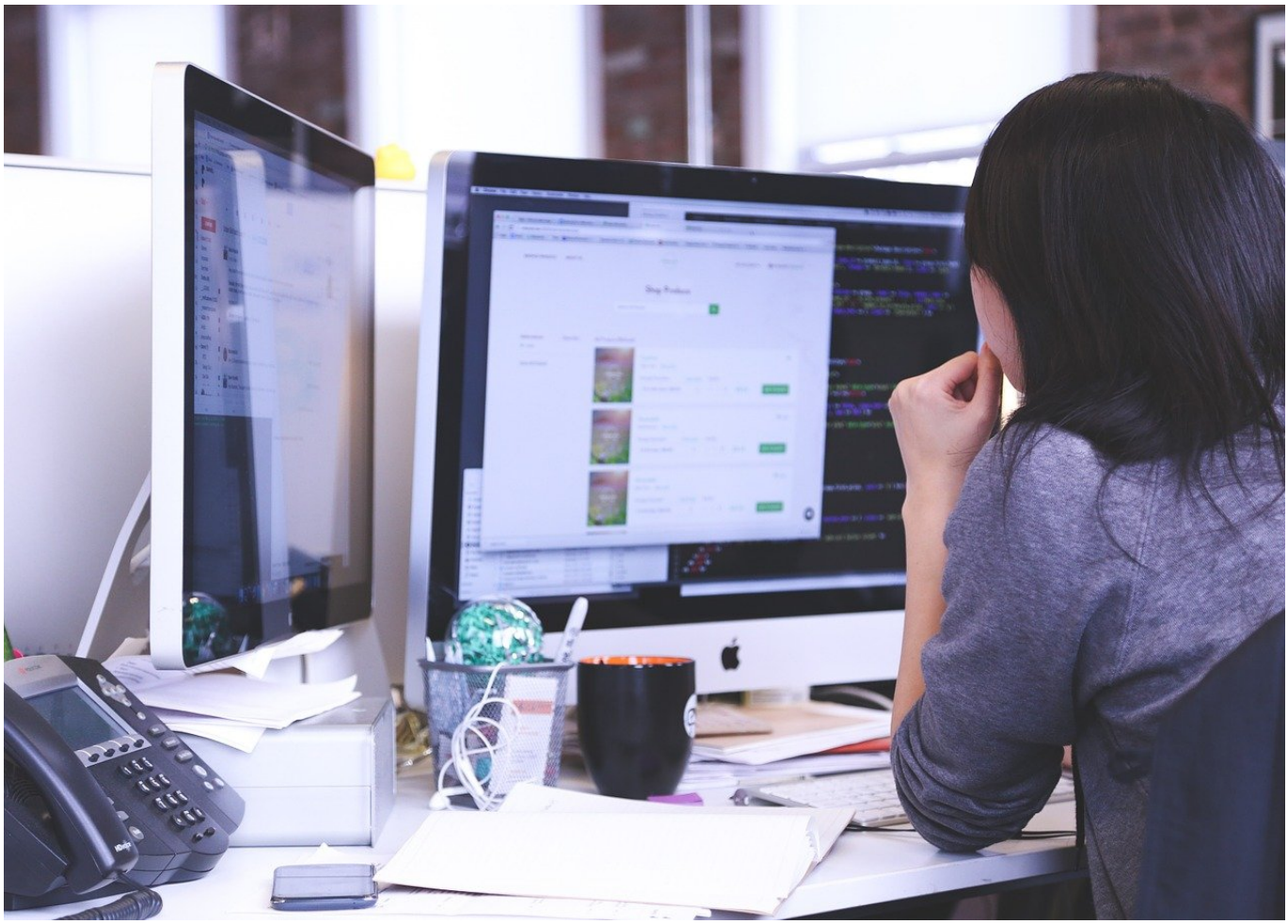
Um die einzurichten, meldet Euch (noch nur mit dem Passwort) an der Admin-Oberfläche an und klickt dann auf **Euren Namen** > **Mein IONOS** > **Login & Kontosicherheit** > **Bestätigung in zwei Schritten**.



IONOS bietet zwei verschiedene Möglichkeiten für den zweiten Faktor an: Zum einen die IONOS Mobile App, die unter anderem auch Einstellungen zum Hostingkonto erlaubT. Die zweite Möglichkeit ist die Verwendung einer normalen Authenticator-App, die dann auch für andere Konten verwendet werden kann. Egal welche der beiden Lösungen gewählt wird: Nach Eingabe des Passwortes fordert die Admin-Konsole von IONOS/1&1 dann die Ziffernfolge ab, die die

installierte App gerade anzeigt. Wer Euer Smartphone nicht in seinem Besitz hat, der bleibt außen vor!

Schutz von PowerPoint-Präsentationen

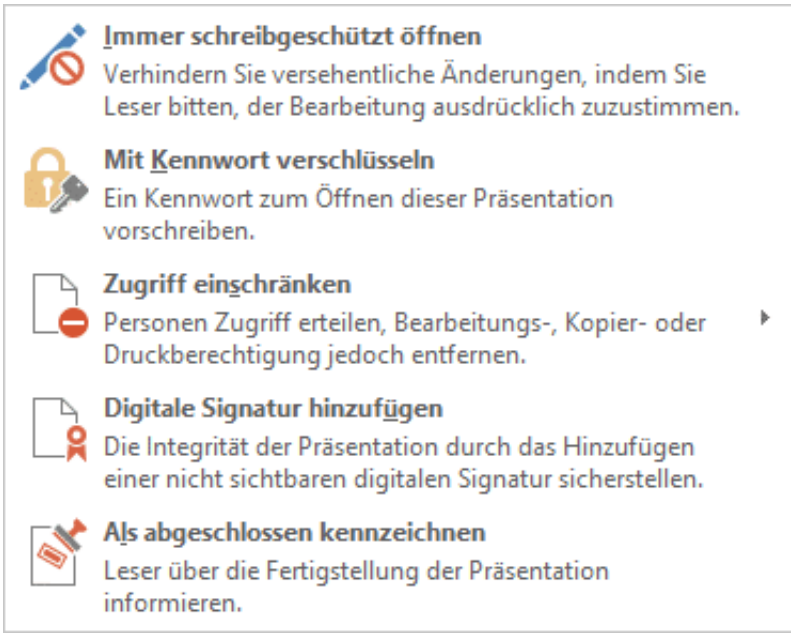


PowerPoint-Präsentationen sind aufwändig in der Erstellung, wenn sie schön sein sollen. Da sollen möglichst wenig Leute ungehindert dran basteln dürfen. Das unterstützt PowerPoint mit Rechten.

Office-Dokumente werden nicht nur am eigenen PC, sondern auch in der Zusammenarbeit mit anderen Anwendern genutzt. Wenn Ihr gemeinsam arbeiten wollt und die Empfänger das Dokument auch bearbeiten dürfen, müsst Ihr nichts weiter machen. Was aber, wenn der Empfänger nur bestimmte Rechte haben soll?

Die Schutzfunktionen für Präsentationen finden sich in PowerPoint unter **Datei** > **Informationen** > **Präsentation schützen**. Hier gibt es die Möglichkeit, unterschiedliche Schutzstufen für eine Präsentation festzulegen.

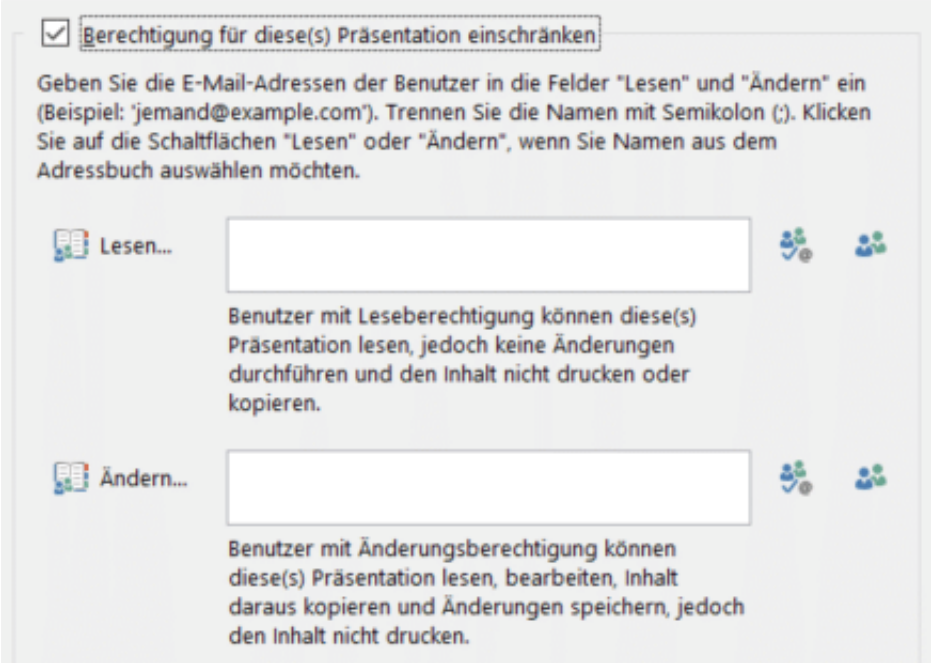
Die einfachste soll versehentliche Änderungen ausschließen: Oft öffnet man eine Datei neben vielen anderen offenen Dokumenten. Schnell passieren dann ungewollte Änderungen. Ein vermeintliches Tippen in einer E-Mail, der Cursor steht aber in der Präsentation. Wird die gespeichert, dann ist die Präsentation unbemerkt verändert. Mit **Immer schreibgeschützt öffnen** muss der Empfänger bestätigen, dass er Änderungen vornehmen will.



Eine gute Idee ist es, die Präsentation **Mit Kennwort zu verschlüsseln**, damit zieht Ihr eine zusätzliche Schutzschicht ein: Der Anwender benötigt das Kennwort, um die Datei öffnen zu können.

Die stärkste Schutzstufe ist **Zugriff einschränken**. Herfür braucht Ihr eine technische Infrastruktur wie Office 365 mit seinem Rechtesystem im Hintergrund.

Über das darin vorhandene Benutzerverzeichnis könnt Ihr genau festlegen, welche Benutzer die Datei nur (aber immerhin) lesen können und welche sie schreiben können.



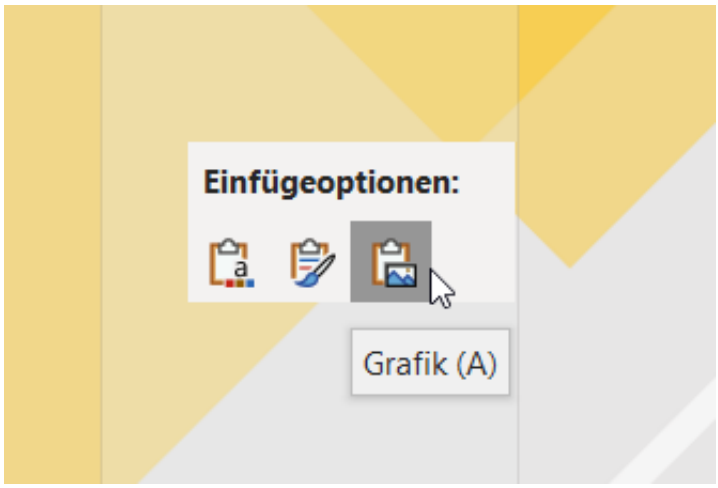
Einfügen von Objekten aus PowerPoint/Office in eine E-Mail

Manchmal geht es schneller, Informationen aus PowerPoint in eine E-Mail zu bringen. Das ist recht einfach, aber bedarf eines Tricks, um die Elemente auch lesbar und sauber angeordnet zu halten.

Der einfachste Weg, eine PowerPoint-Präsentation weiterzugeben, ist der Versand per E-Mail als Anhang. Das ist aber nicht immer gewünscht: Der zusätzliche Doppelklick hält den ein oder anderen Empfänger ab, diese zu öffnen. Vor allem, wenn er den Inhalt sowieso nur widerwillig liest. Da macht es Sinn, die Inhalte direkt in die E-Mail einzubetten.

Outlook als Microsoft E-Mail-Programm kann mit allen Office-Formaten umgehen, so auch mit PowerPoint. Das bringt mit sich, dass es alle Elemente dynamisch so anordnet, wie es gerade in die E-Mail passt. Macht der Anwender die E-Mail

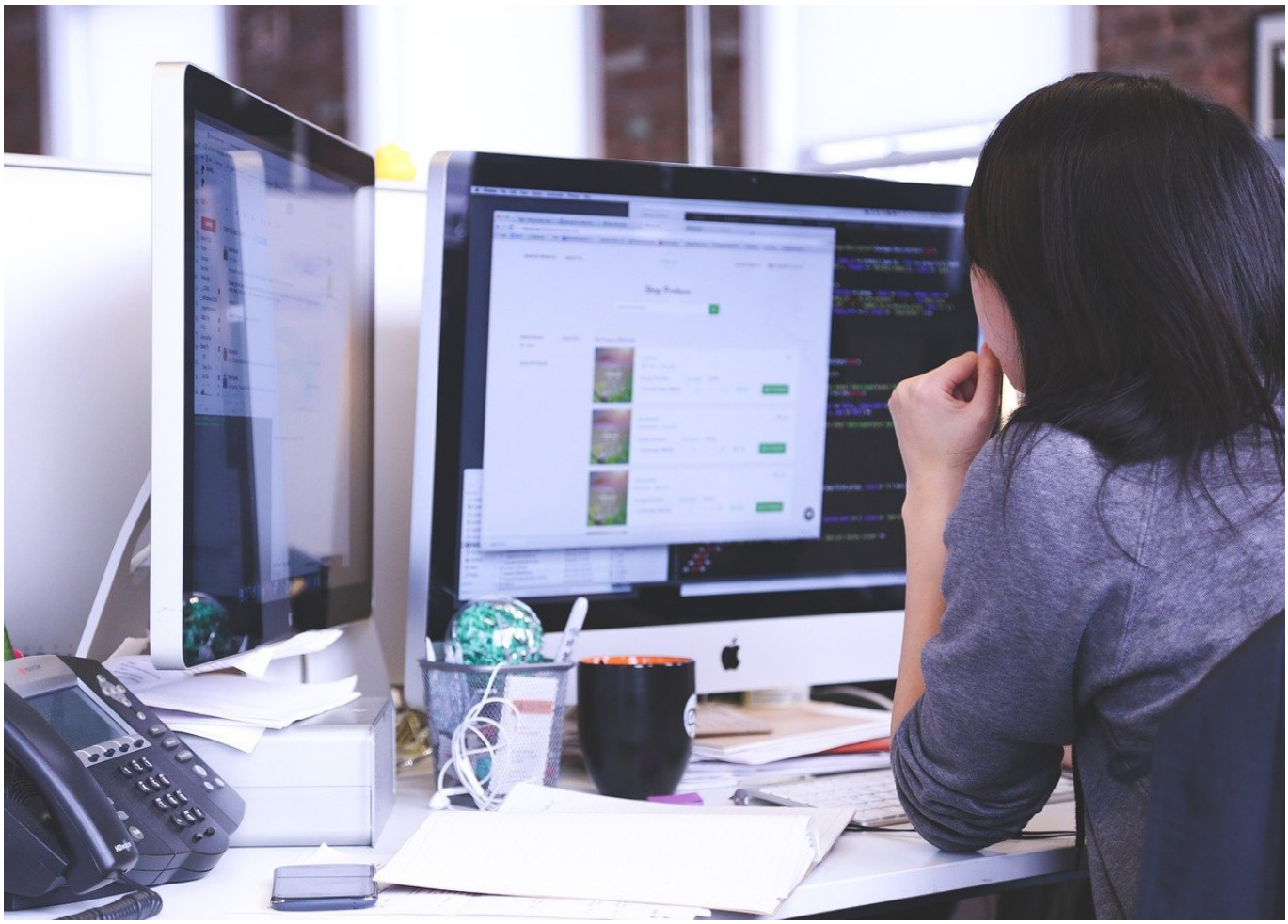
breiter, dann verschieben sich Elemente und die Anordnung geht kaputt. Dagegen hilft folgender Trick:



- Markiert mit **Strg** + **A** alle Elemente der Folie und kopiert sie mit **Strg** + **C** in die Zwischenablage.
- Legt eine neue E-Mail in Outlook an.
- Klickt mit der rechten Maustaste in die Mail, dann unter **Einfügeoptionen** auf den dritten Eintrag (Grafik).

Windows fügt die Elemente der PowerPoint nun als eine Gesamtgrafik ein. Damit sind alle Elemente so angeordnet, wie sie in PowerPoint waren. Auch das Vergrößern/Verkleinern der E-Mail ändert daran nichts mehr!

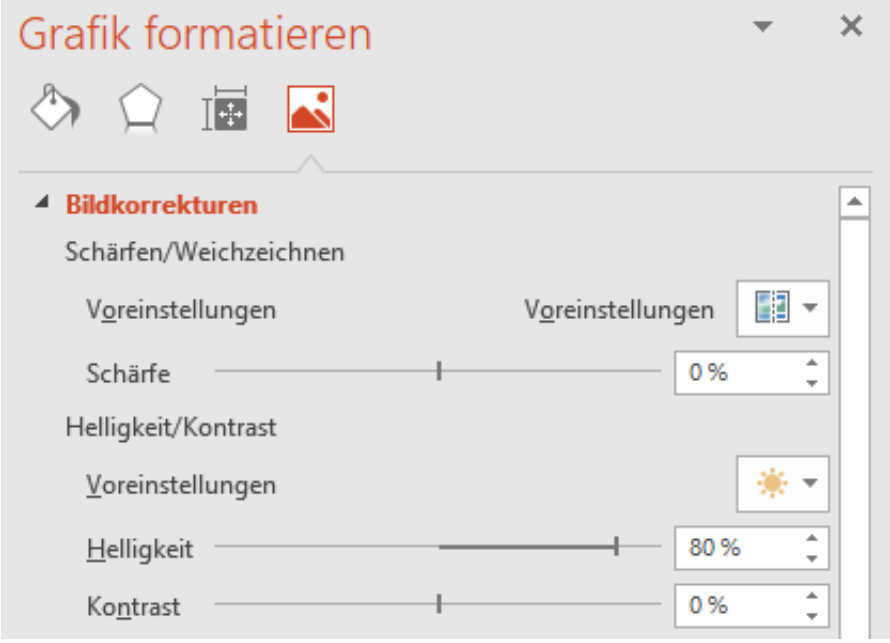
Grafiken in Powerpoint neu einfärben



PowerPoint lebt von Bildern. Manchmal sind die aber nicht so, wie Ihr sie haben wollt. Kein Grund für ein Grafikprogramm, dass geht schnell in PowerPoint selbst!

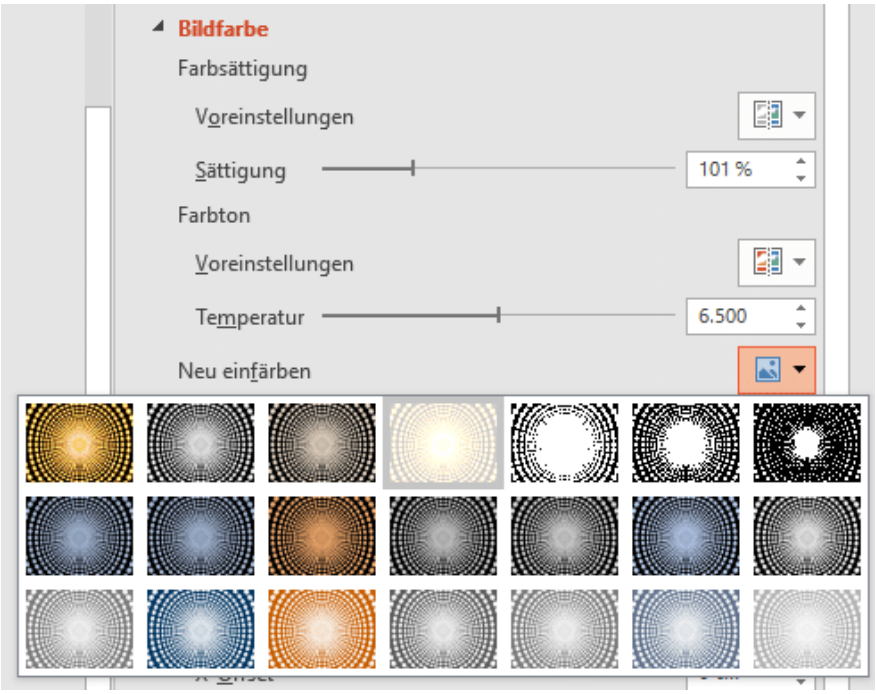
Microsoft PowerPoint ist für viele nicht einfach nur ein Präsentationswerkzeug, sondern auch das Standard-Programm, mit dem sie eben mal schnell etwas dokumentieren oder eine kleine Vorlage erstellen: Ein Türschild, einen Gutschein, eine Tischkarte - die Möglichkeiten sind endlos. Wer sich in Powerpoint gut auskennt, hat relativ schnell schicke Vorlagen erstellt. Die von Powerpoint genutzten Grafiken sind oft schick - doch Einfluss haben Anwender eher wenig darauf. Doch Powerpoint bietet die Möglichkeit, die Grafiken abzuändern.

Klickt dazu mit der rechten Maustaste auf das Bild, dann auf **Grafik formatieren**. PowerPoint öffnet nun ein zusätzliches Einstellungsmenü am rechten Bildschirmrand.



Über **Bildkorrekturen** könnt Ihr die Schärfe, die Helligkeit und den Kontrast des Bildes ändern. Damit bekommen Ihr zu dunkle oder zu helle Bilder in den Griff. Unter Voreinstellungen finden sich für viele der Einstellungen Voransichten, wie das Bild aussehen könnte. Klickt auf ein Minibild, um die zugrundeliegenden Einstellungen anzuwenden.

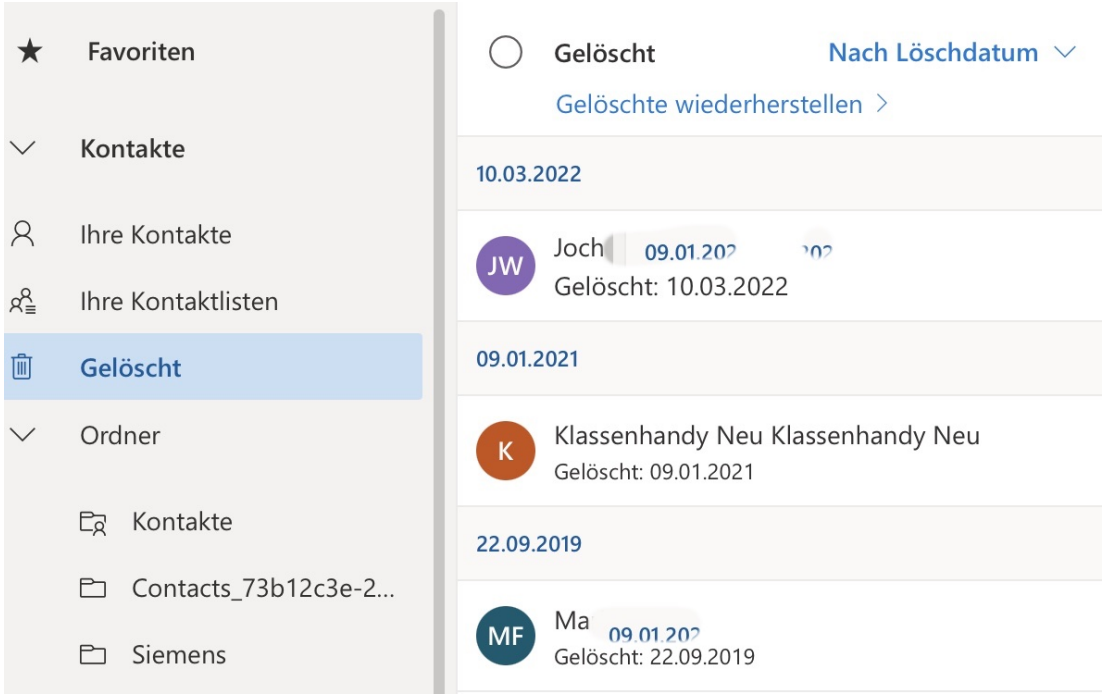
Unter **Bildfarbe** könnt Ihr das Bild **Neu einfärben**. Diese Funktion ist besonders bei Diagrammen und schematischen Bildern hilfreich, denn dort können die Farben angepasst werden, ohne dass das Bild komisch wirkt. Bei einem Foto macht das nur Sinn, wenn tatsächlich eine Verfremdung erreicht werden soll.


Bildfarbe
Farbsättigung
Voreinstellungen
Sättigung
101 %
Farbton
Voreinstellungen
Temperatur
6.500
Neu einfärben

Wiederherstellung von Kontakten in Outlook/Microsoft 365

Wenn plötzlich in WhatsApp nur noch Nummern statt Namen auftauchen, liegt das oft an gelöschten Kontakten in Ihrem Outlook. Wolltet Ihr die nicht löschen? Dann gibt es noch Hoffnung!

Kontakte sind weit mehr als Adressen und Telefonnummern: In den Notizen befinden sich alle möglichen Freitextinformationen wie Kundennummern, diverse Angaben zum Kontakt und Links zu Wegbeschreibungen und anderen Informationen. Diese lassen sich nicht so einfach zurückholen, wenn der Kontakt erst einmal gelöscht ist. Schließlich habt Ihr sie teils über viele Jahre manuell zusammengesucht!



In Microsoft 365 (ehemals Office 365) werden Kontakte erst einmal nicht physisch gelöscht, sondern bleiben in einem separaten Ordner liegen. Aus diesem Ordner - vergleichbar mit dem Papierkorb in Windows - lassen sie sich wiederherstellen.

Dazu öffnet die Microsoft 365-Kontakte unter https://outlook.office.com/people/. Klickt dann in der Seitenleiste auf **Gelöscht**, Outlook zeigt alle Kontakte an, die gelöscht wurden und sortiert diese nach dem Löschdatum. Damit lässt sich leicht zuordnen, welche Kontakte von einem versehentlichen Löschen betroffen waren. Finden sich die Kontakte dort nicht, dann sind sie vielleicht von einem PC- oder Smartphone-Outlook gelöscht worden. Klickt auf **Gelöschte wiederherstellen**, dann zeigt Outlook die Kontakte an, die gelöscht und dann synchronisiert worden sind.

Um Kontakte wiederherzustellen, klickt auf den Kreis neben einem Kontakt und markiert ihn damit. Nach Markierung aller gewünschten Kontakte klickt im Detailbereich des Fensters auf **Wiederherstellen**. Nach der nächsten Synchronisation sind die Kontakte dann auch wieder auf allen Geräten verfügbar.

Trend Micro warnt vor Kryptomining-Angriffen auf Cloud-Infrastrukturen

Trend Micro, einer der weltweit führenden Anbieter von Cybersicherheitslösungen, veröffentlicht einen neuen Forschungsbericht zum Thema Kryptowährungs-Mining. Der Report legt dar, wie Cyberkriminelle die Cloud-Infrastrukturen von Unternehmen kompromittieren und für ihre Zwecke missbrauchen. Immer wieder kämpfen dabei sogar verschiedene Gruppen um die Kontrolle über betroffene Systeme.

Der Bericht zeigt, dass Bedrohungsakteure zunehmend nach angreifbaren Instanzen suchen und diese ausnutzen. Unter anderem setzen sie auf Brute-Forcing von SecureShell (SSH)-Anmeldeinformationen, um Cloud-Ressourcen für das Kryptowährungs-Mining zu kompromittieren. Die Opfer weisen häufig veraltete Cloud-Software in der Cloud-Umgebung, mangelnde Cloud-Sicherheitshygiene oder unzureichende Kenntnisse über den Schutz von Cloud-Diensten auf. Dadurch erleichtern sie es den Angreifern, Zugang zu den Systemen zu erhalten.

Während der Pandemie sind die Investitionen in Cloud Computing rasant gestiegen. Dabei führt die einfache Bereitstellung der neuen Systeme dazu, dass viele Cloud-Anwendungen länger als nötig online sind – häufig ungepatcht und fehlkonfiguriert.

Das bösartige Kryptomining hat verschiedene negative Folgen für betroffene Unternehmen: Zum einen droht der zusätzliche Computing-Workload wichtige Cloud-Dienste zu verlangsamen. Zum anderen steigen die Betriebskosten für jedes infizierte System um bis zu 600 Prozent. Darüber hinaus kann Kryptomining ein Vorbote für eine noch gravierendere Kompromittierung sein. Viele professionelle Bedrohungsakteure setzen Mining-Software ein, um zusätzliche Einnahmen zu generieren, bevor Online-Käufer den Zugang zu Ransomware, gestohlenen Daten und mehr von ihnen erwerben.

„Schon wenige Minuten der Kompromittierung können den Angreifern Gewinne einbringen. Deshalb beobachten wir einen kontinuierlichen Kampf um Cloud-CPU-Ressourcen. Es ist wie ein reales ‚Capture-the-Flag'-Spiel, wobei die Cloud-Infrastruktur des betroffenen Unternehmens das Spielfeld ist", erklärt Richard Werner, Business Consultant bei Trend Micro.

„Solche Bedrohungen erfordern eine einheitliche, plattformbasierte Sicherheit, um zu gewährleisten, dass sich die Angreifer nicht verstecken können. Die richtige Plattform unterstützt IT-Teams dabei, ihre Angriffsfläche zu überblicken, das Risiko einzuschätzen und den richtigen Schutz zu wählen, ohne dabei einen hohen Mehraufwand zu generieren."

Bedrohung von Krypto-Mining

Die Forscher von Trend Micro legen die Aktivitäten mehrerer Kryptomining-Bedrohungsgruppen detailliert offen – darunter folgende Gruppen und ihre Vorgehensweisen:

- Outlaw kompromittiert Internet-of-Things (IoT)-Geräte und Linux-Cloud-Server, indem sie bekannte Schwachstellen ausnutzt oder Brute-Force-Angriffe auf SSH durchführt.
- TeamTNT (1) nutzt verwundbare Software, um Hosts zu kompromittieren. Anschließend stiehlt die Gruppe Anmeldeinformationen für weitere Dienste, um so auf neue Hosts zuzugreifen und deren fehlkonfigurierte

Services zu missbrauchen.
- Kinsing installiert ein XMRig-Kit für das Mining von Monero und entfernt dabei alle weiteren Miner von dem betroffenen System.
- 8220 kämpft mit Kinsing um dieselben Systeme. Häufig vertreiben sie sich gegenseitig von einem Host und installieren anschließend ihre eigenen Kryptowährungs-Miner.
- Kek Security wird mit IoT-Malware und der Ausführung von Botnet-Diensten assoziiert.

Um die Bedrohung durch Kryptowährungs-Mining-Angriffe in der Cloud einzudämmen, empfiehlt Trend Micro folgende Sicherheitsmaßnahmen für Unternehmen:

- Stellen Sie sicher, dass die Systeme auf dem neuesten Stand sind und nur die erforderlichen Dienste ausgeführt werden.
- Setzen Sie Firewalls, Intrusion-Detection-Systeme (IDS)/ Intrusion-Prevention-Systeme (IPS) und Cloud Endpoint Security zur Begrenzung und Filterung des Netzwerkverkehrs für bekannte schädliche Hosts ein.
- Vermeiden Sie Konfigurationsfehler mit Hilfe von Cloud-Security-Posture-Management-Tools.
- Überwachen Sie den Datenverkehr zu und von Cloud-Instanzen und filtern Sie Domänen heraus, die mit bekannten Mining-Pools verbunden sind.
- Führen Sie kostenorientierte Regeln zur Überwachung offener Ports, Änderungen am Domain-Name-System (DNS)-Routing und der Auslastung der CPU-Ressourcen ein.

Weitere Informationen

Den vollständigen Bericht *A Floating Battleground Navigating the Landscape of Cloud-Based Cryptocurrency Mining* finden Sie in englischer Sprache hier: https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/probing-the-activities-of-cloud-based-cryptocurrency-mining-groups

Surftipp: Infos über Filme und Serien

Die Medienlandschaft hat sich enorm verändert. Die Menschen schauen immer noch gerne Filme und Serien - aber verstärkt beim Streamingdienst. Aber welche Serien und Filme taugen was? Gute Empfehlungen und Besprechungen gibt es bei Kinofans.

Die jüngsten Oscars waren eine ordentliche Überraschung. Gleich zwei große Produktionen von Streamingdiensten haben gleich mehrere Oscars erhalten.

Die Tragikomödie "**Coda**" (Abkürzung für "Child of Deaf Adults", also "Kind gehörloser Erwachsener") hat die Trophäe für den besten Film erhalten. Eine Produktion von Apple TV+. Damit wurde erstmals nicht ein Kinofilm, sondern eine Streamingproduktion als "bester Film" geehrt.

Für die beste Regie wurde die Neuseeländerin Jane Campion ausgezeichnet, und zwar für den großen Coda-Konkurrenten "The Power of the Dog". Das wiederum ist eine Produktion von Netflix - und dort auch schon zu sehen.

Top-Produktionen der großen Streamingdienste

Die wahnsinnigen Budgets, die die großen Streamingportale im Kampf um die Zuschauergunst zu verteilen haben, lassen also mitunter richtig gute Filme entstehen. Für viele junge Menschen ist es egal, ob sie einen Film im Kino oder zu Hause sehen. Viele schauen sogar lieber zu Hause. Und in Zeiten der Pandemie war es - bei geschlossenen Kinos - ja auch gar nicht anders möglich.

Aber welche Filme und Serien taugen was? Was passiert, wer spielt mit, was sagen Kritiker? Wer so etwas wissen will, sollte bei Kinofans.com vorbeischauen. Die Experten besprechen hier ausführlich aktuelle Netflix Filme und Serien im Stream.

Hier erfahrt Ihr nicht nur, was gerade im Kino läuft - was ja auch ein guter Benefit ist! -, sondern eben auch und vor allem, welche Filme und Serien bei den Streamingdiensten angesagt sind. Mit aktuellen Empfehlungen, Tipps für Serien und News aus dem Bereich Streaming. Denn viele Binge-Watcher wüssten gerne, wie es mit ihren Lieblingsserien weitergeht: Kommt eine neue weitere Staffel - und wenn ja: Wann?

Praktische Suchfunktion

Das Layout von Kinofans.com ist zweifellos noch etwas altbacken und könnte mal ein Update/eine Aktualisierung vertragen. Aber der Inhalt überzeugt. So ist es selbstverständlich auch möglich, das Portal nach Titeln, Schauspielern oder Regisseuren zu durchsuchen. Einfach ins bescheidene Suchfeld oben rechts eingeben - schon erscheinen die entsprechenden Fundstellen.

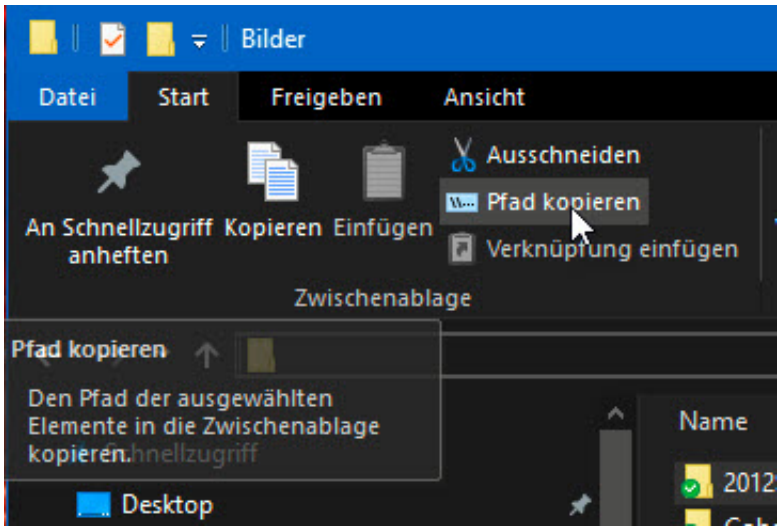
Kinofans beschreibt, was im Film passiert - und darunter erscheint eine Übersicht, bei welchen Streamingportalen der Film oder die Serie zu sehen ist - und was es ggf. kostet, sofern der Film oder die Serie nicht Bestandteil eines Abos ist. Diese Informationen kommen dann von JustWatch - und sind für mich immer besonders hilfreich und nützlich. Ich sehe dann, wo ich etwas ggf. "kostenlos" schauen kann. Oder besser: ohne zusätzliche Kosten.

Dateipfade in Windows 11 identifizieren

Dateinamen sind wichtig, um eine Datei zu finden braucht Ihr aber auch deren Speicherort. Mit unserem Hack lässt sich dieser schnell herausfinden!

Wenn Ihr im Netzwerk arbeitet, dann bewegt Ihr Euch nicht nur auf Datenträgern und lokalen Laufwerken, sondern auch auf Netzlaufwerken. Deren Bezeichnungen sind meist lang und unleserlich. Auch bei einer lokalen Ordnerstruktur kann der Dateiname inkl. seines Speicherorts so lang sein, dass ein Abtippen wenig Spaß macht.

Der Windows Explorer ist das Standardprogramm für den Weg durch die Ordnerstrukturen. Wenn ein Netzwerklaufwerk angesprochen werden soll, dann klickt auf **Netzwerk** und sucht den Server und das Laufwerk hinaus. Alternativ gebt den Namen des Servers mit "" am Anfang ein. Um den Pfadnamen weiterzugeben, gibt es jetzt zwei Möglichkeiten:



1. Klickt mit der rechten Maustaste auf die Datei oder den Ordner und dann auf Eigenschaften. Unter **Ort** findet sich der aktuelle Pfad, der sich markieren und kopieren lässt.
2. Markiert Datei oder Ordner, dann klickt im Reiter **Start** auf **Pfad kopieren**. Der Pfad (nur der Ordner bei einem Verzeichnis, Ordner und Dateiname, wenn eine Datei angewählt ist) befindet sich direkt in der Zwischenablage.