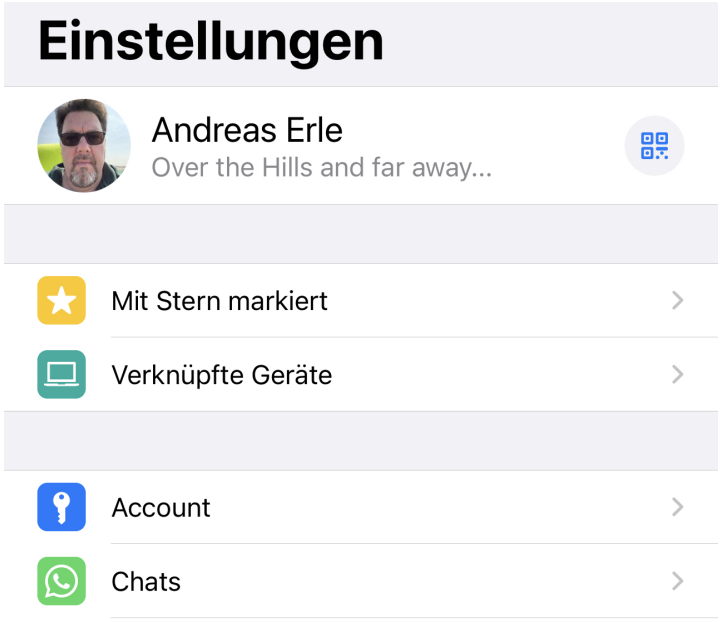
Schieb Report

Ausgabe 2022.22

Vorsicht bei WhatsApps mit Anrufaufforderungen

Jedes Kommunikationsmittel bietet Angreifern Möglichkeiten, es zu missbrauchen. Wenn Ihr eine WhatsApp mit einer Telefonnummer mit *-Codes vorne bekommt, ignoriert diese unbedingt!

Das WhatsApp-Konto ist für viele Anwender der Kern ihrer Kommunikation. Der schnell Chat nebenbei, aber auch die Absprache von Verabredungen oder sogar der Abschluss von Geschäften finden über den Messenger statt. Kommt Euer Konto in falsche Hände, dann kann Euch rechenbarer Schaden entstehen! Gerade geht eine Welle von vermeintlichen Aufforderungen zu einem Rückruf durch die WhatsApp-Welt. Seid vorsichtig, bevor ihr der Aufforderung Folge leistet!



Die Rufnummern, die Ihr Anrufen sollt, fangen mit ****21*** an. Was wie der Teil der Rufnummer aussehen soll, ist in Wirklichkeit ein so genannter GSM-Code, ein Steuerbefehl für Funktionen des Mobilfunknetzes. In diesem Fall wird damit die Rumleitung von Eurer Rufnummer auf die Rufnummer, die sich hinter dem GSM-Code befindet, eingerichtet.

Alle Anrufe an Eure Nummer gehen dann an die Nummer des Angreifers. Der startet dann eine Registrierung von WhatsApp mit Eurer Nummer mit der Übermittlung des Codes per Anruf. Da der Anruf ja an seine Rufnummer umgeleitet wird, kann er das Konto verifizieren und damit Euer WhatsApp-Konto übernehmen.

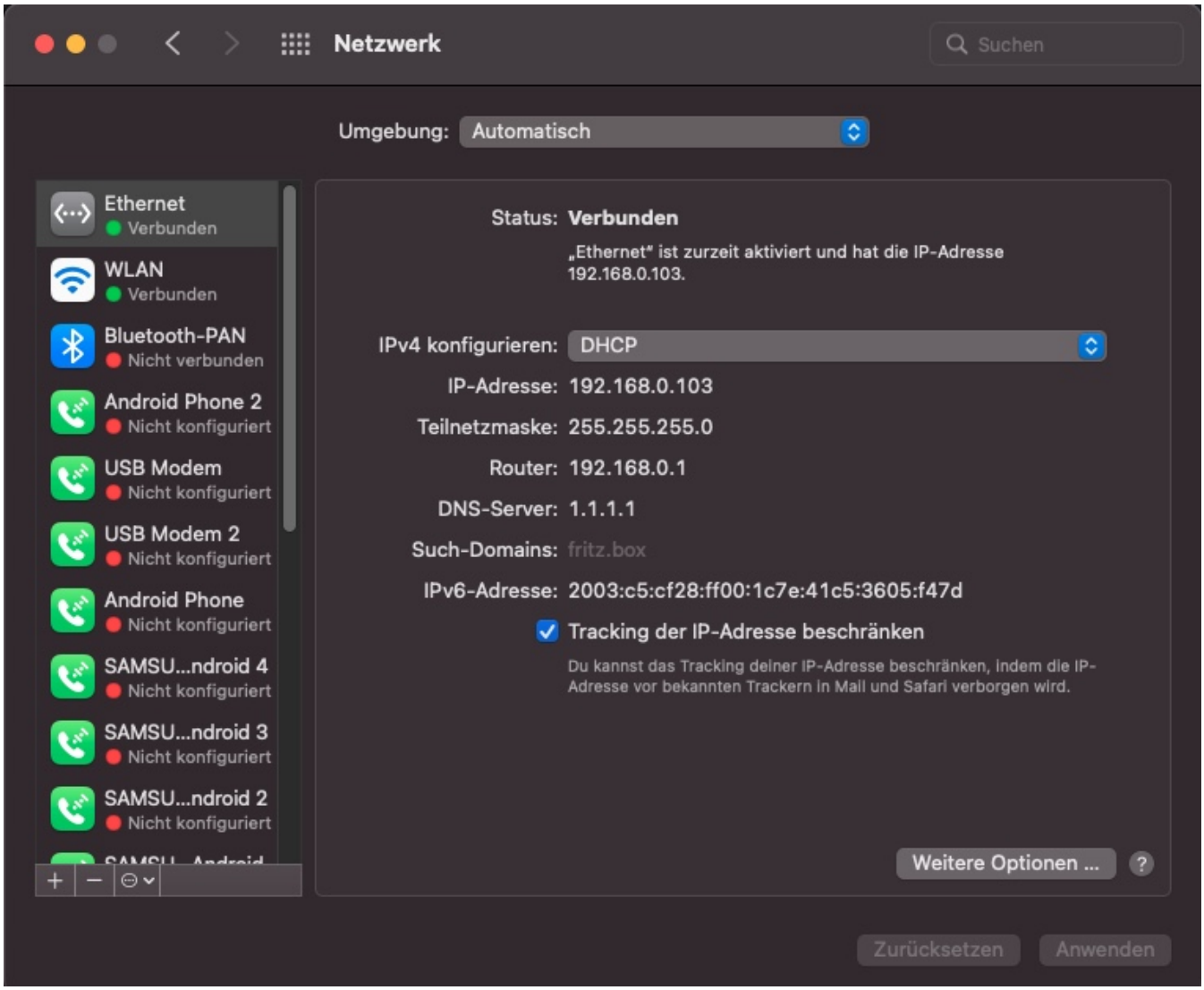
Die Lösung: Ignoriert die Nachricht und blockiert den Absender!

Verändern der Netzwerkeinstellungen beim Mac

Das Netzwerk: Buch mit sieben Siegeln und zentrale Stelle für alle Verbindungen zu Ressourcen wie dem Internet, Servern oder Druckern. MacOS bietet Euch viele Einstellungen und Hacks!

Eine Netzwerkverbindung kann über verschiedene Wege kommen: Klassisch über das LAN-Kabel vom Router oder kabellos über eine WLAN-Verbindung. Auch USB-Modems oder gekoppelte Smartphones bieten eine Netzwerkverbindung, und das meist automatisch.

Die Übersicht der Netzwerkverbindungen auf einem Mac seht Ihr, wenn Ihr in den **Einstellungen** auf **Netzwerk** klickt. Auf der linken Seite zeig macOS Euch alle konfigurierten Verbindungen an. Ein grüner Punkt bedeutet, dass die Verbindung besteht. ein roter, dass sie getrennt ist. Das hilft beispielsweise, wenn Ihr kleine Daten über das Netzwerk bekommt: Ist die Verbindung getrennt, dann ist entweder das Kabel nicht verbunden, die WLAN-Verbindung gestört oder die Gegenstelle - meist der Router - nicht online.



Nicht mehr benötigte Verbindungen könnt Ihr markieren und nach einem Klick auf das **Minus-Zeichen** und Eingabe Eures Anmeldekennwortes löschen. Das macht vor allem bei Smartphones Sinn, die Ihr nicht mehr benutzt oder im Besitz habt. Versteckt und leider nicht genug bekannt: Hier könnt Ihr auch festlegen, dass das Tracking Eurer IP-Adresse beschränkt werden soll. Ist die Option aktiviert, dann versuchen Mail und Safari, Eure IP-Adresse vor bekannten Trackern zu verbergen und Euch damit weniger verfolgbar zu machen.

Ein Klick auf **Weitere Optionen** öffnet die Detaileinstellungen:

- Unter **TCP/IP** könnt Ihr festlegen, dass die IP-Adresse des Gerätes nicht - wie im Standard - automatisch vom Router bezogen wird, sondern von Euch manuell vergeben wird.
- Unter **DNS** könnt Ihr den für die Namensauflösung wichtigen DNS-Server einstellen. Dieser ist im Standard vorgefüllt mit den Informationen, die der

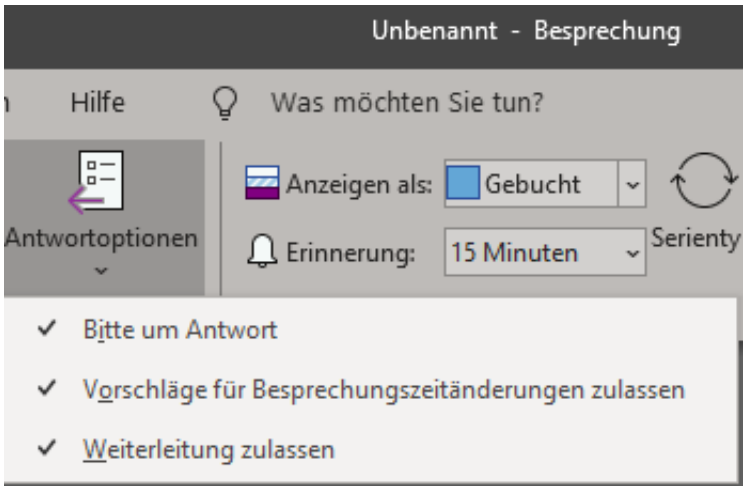
Router liefert, kann aber auch manuell geändert werden. Beispielsweise auf 1.1.1.1. den schnelle Cloudflare-DNS.

- **WINS** legt die Identifikation des Gerätes in einem Windows-Netzwerk fest, im Speziellen den Namen der Arbeitsgruppe und dem Namen, unter dem das Gerät angezeigt wird.
- Wenn Ihr zentral über einen Proxy-Server ins Internet geht, dann könnt Ihr diesen unter **Proxies** festlegen.

Weiterleitung von Terminen einschränken

Ihr organisiert eine Besprechung, und plötzlich tauchen alle möglichen anderen Teilnehmer auf, die Ihr nicht eingeladen habt. Das könnt Ihr unterbinden!

Termininhalte sind manchmal vertraulich. Ihr organisiert den Termin mit genau den Teilnehmern, mit denen Ihr sprechen wollt, und vertraut darauf, dass Ihr niemand anderen eingeladen habt. Dummerweise können die Eingeladenen aber selber Eure Einladung weiterleiten. Mit Glück - und richtig konfiguriertem Exchange-Server - bekommt Ihr darüber eine automatische Information. In den weitaus meisten Fällen sitzt ihr indem Termin, und plötzlich sind noch andere Teilnehmer dabei. Aus dieser Situation rauszukommen, ohne jemanden vor den Kopf zu stoßen, ist kaum möglich. Darum: regelt das im Vorfeld schon im Termin!



Wichtig: Legt eine neue **Besprechung** an, nicht einen neuen **Termin**, indem Ihr auf das entsprechende Symbol in der Outlook-Symbolleiste klickt. Termine sind - auch wenn sie die Einladung von anderen Teilnehmern erlauben, eher für Eure eigenen Themen, während Besprechungen für übergreifende Dinge mit mehreren Teilnehmern gedacht sind.

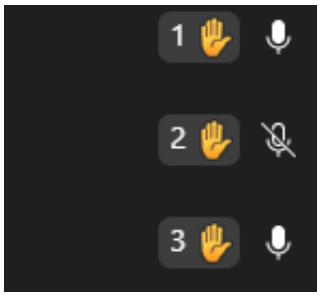
Im Termin klickt auf **Antwortoptionen** in der Symbolleiste, dann entfernt den Haken bei **Weiterleitung zulassen**. Der ist im Standard aktiviert. Wenn Ihr die Berechtigung ausgeschaltet habt, dann kann der Termin nicht mehr weitergeleitet werden und die Teilnehmer müssen Euch bitten, das zu machen.

Wer ist jetzt dran? Reihenfolge von Wortmeldungen in Teams

Wenn ein Meeting nicht komplett im Chaos versinken soll, müssen Wortmeldungen per Handzeichen erfolgen und in der Reihenfolge der Meldung abgearbeitet werden. Microsoft Teams scheint da nicht strukturiert, ist es aber!

Ihr kennt die Situation sicherlich: Jeder will seine Meinung kundtun, alle reden durcheinander und am Ende gehen fast alle Infos im entstehenden Chaos unter. In klassischen (Vor-Ort) Meetings gibt es dann einen Moderator, der eine Liste der Wortmeldungen führt und das Wort in der richtigen Reihenfolge erteilt.

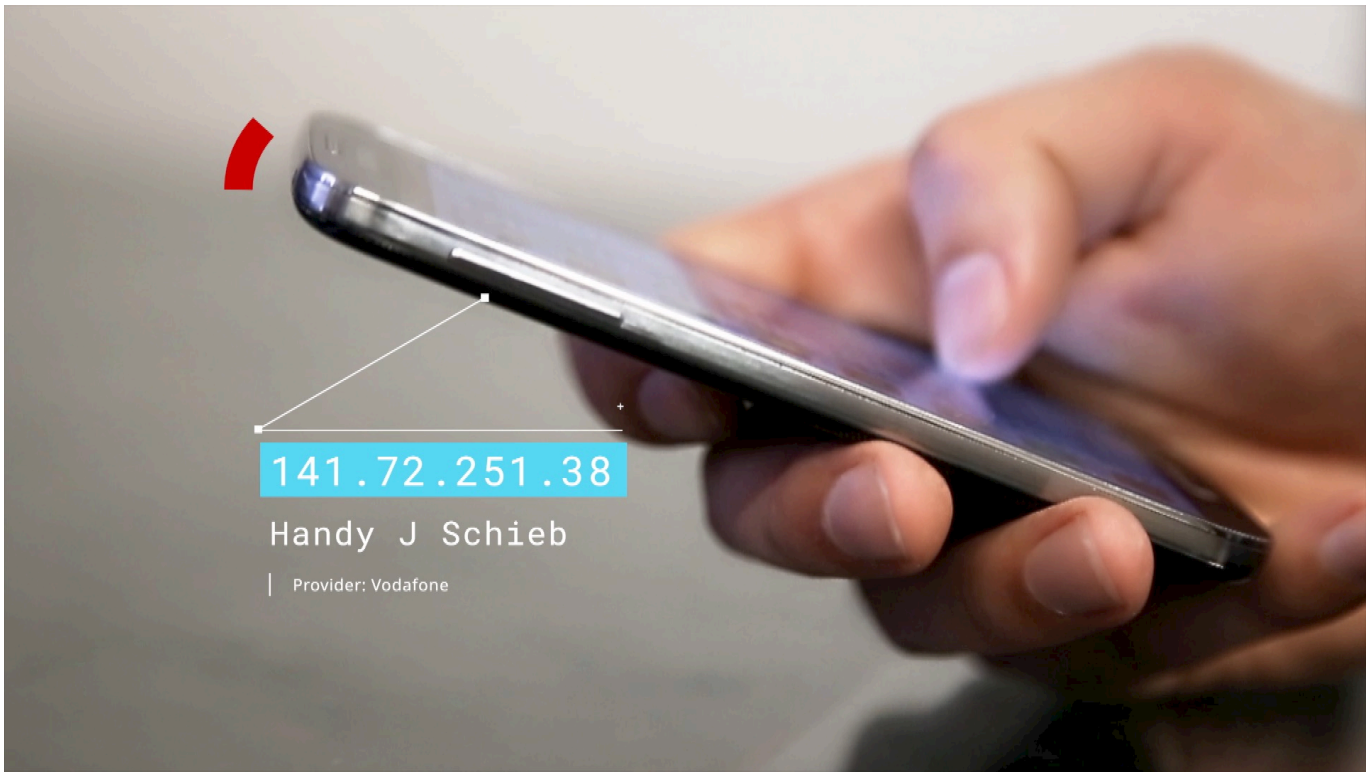
In Teams könnt Ihr das im Tools machen: Klickt oben in der Symbolleiste auf **Reaktionen** und dann auf das **Symbol mit der Hand**. Neben dem Bild des Teilnehmers erscheint dann auch eine virtuelle Hand für die Wortmeldung. Bleibt nur das Problem: Wer ist wann dran?



Die ganze Ordnung der Wortmeldungen ist schnell erledigt, wenn sich die Teilnehmer darum streiten, dass ihr Wortmeldung vor der der anderen dran war. Teams hilft hier, zeigt die Reihenfolge allerdings ein wenig versteckt an: Klickt auf die Teilnehmer des Termins in der Symbolleiste.

Neben den Namen seht Ihr die Handzeichen, und neben den virtuellen Händen eine kleine Zahl. Die gibt die Position in der Liste der Wortmeldungen an und wird automatisch aktualisiert, wenn ein Teilnehmer seine Hand wieder senkt. Damit gibt es keine Diskussion mehr, wer als Nächstes reden darf!

Datenschutz vs. Kinderschutz: Was ist eigentlich eine IP-Adresse?



Es wird aktuell viel über Täter-, Opfer- und Datenschutz gesprochen. Nach meiner Beobachtung verstehen viele aber nicht genau, was eine IP-Adresse eigentlich ist - und wieso die Polizei hier häufig nicht weiter kommt. Ein Versuch der Erklärung.

Der aktuelle Fall rund um die Missbrauchsfälle in Wermelskirchen schockiert alle: die Öffentlichkeit, die ermittelnden Polizeibeamten – und die Politik. Natürlich will man das verhindern, den Tätern auf die Schliche kommen. Doch die Polizei sagt – ein ums andere Mal: Wir kommen in vielen Fällen nicht weiter.

NRW-Innenminister Reul sagt das. Auch Holger Münch, der Chef des BKA, der mitteilt, dass allein im vergangenen Jahr 2100 ermittelte Fälle nicht zu Ende gebracht werden konnten, weil die nötigen Daten fehlen. Täterschutz statt Opferschutz, sagen viele – und dieser Eindruck drängt sich ja tatsächlich auf. Was verhindert der Datenschutz eigentlich?

Polizei kommt mit Ermittlungen oft nicht weiter

Sowohl NRW-Innenminister Reuel als auch Polizeibeamte beklagen, dass sie oft mit ihren Ermittlungen nicht weiterkommen, obwohl ihnen konkrete Beweise vorliegen. Woran liegt das?

Das hat mit der Art und Weise zu tun, wie wir im Netz kommunizieren. Hier gilt prinzipiell ein hohes Maß an Anonymität. Wir müssen uns ja nicht ausweisen, keinen echten Namen nennen, nicht mal eine Handynummer oder Postadresse hinterlassen.

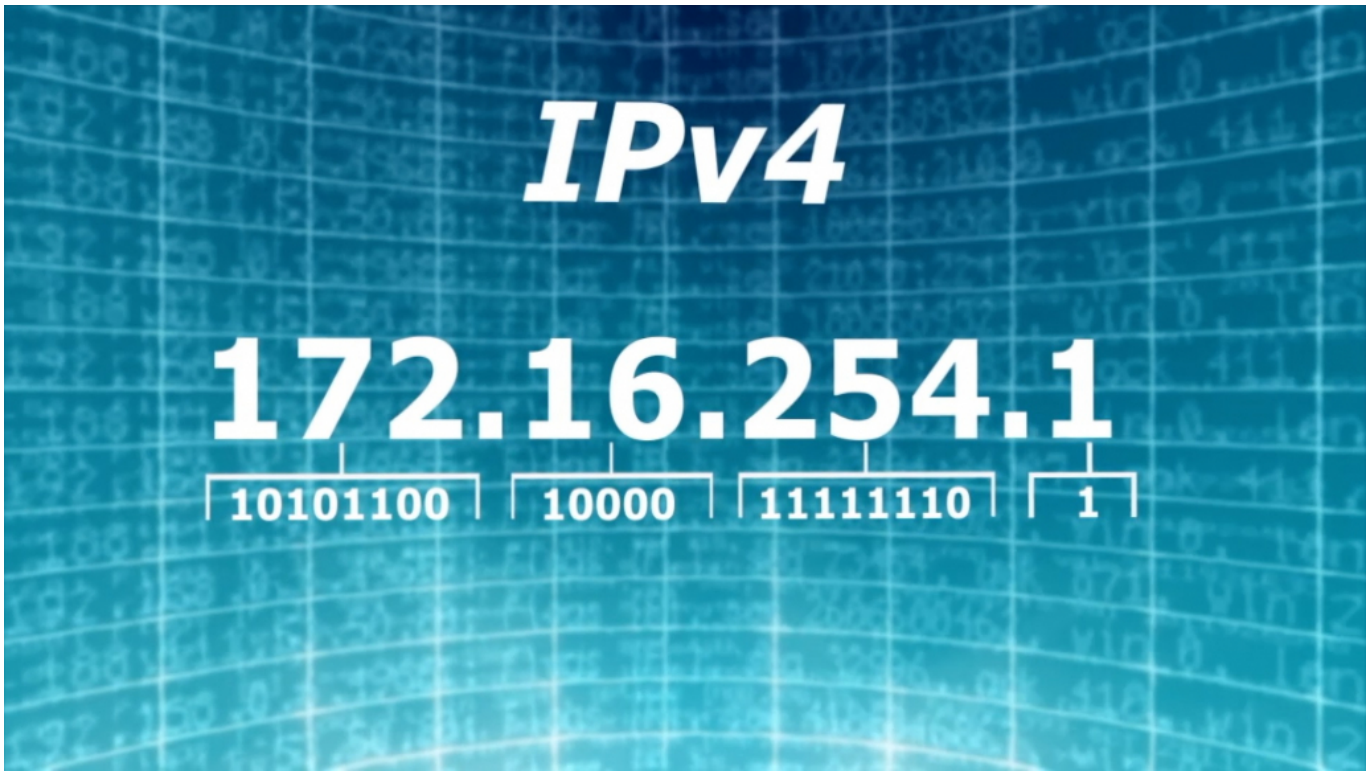
Wir sind prinzipiell anonym im Netz unterwegs. Das ist auch gut so und sogar ein verbrieftes Grundrecht. Wenn Polizeibeamte einem Verdacht nachgehen und in Protokollen Hinweisen auf den Austausch von Missbrauchsbildern finden, haben sie in der Regel nur eine einzige Spur: die IP-Adressen der Menschen, die dort in der Vergangenheit Bilder geladen, abgeliefert oder ausgetauscht haben. Diese IP-Adressen werden in der Regel gespeichert und protokolliert, auf den Servern, die Inhalte anbieten oder einen Datenaustausch oder Chat ermöglichen.

Das ist die IP-Adresse

Den Begriff „IP-Adresse“ hören wir oft – was ist das eigentlich?

Fangen wir mit dem Begriff an: „IP“ steht für „Internet Protokoll“. Das ist quasi die Methode, wie im Internet Daten ausgetauscht werden. Hier braucht jedes Gerät, das mit dem Internet verbunden ist, eine eigene IP-Adresse. Egal, ob Smartphone, Tablet, Desktop-PC, Rauchmelder, Klingelanlage, per App fernsteuerbare Lichtleiste – oder Server von Unternehmen: Alle haben so eine eindeutige, unverwechselbare IP-Adresse. Die Datenpakete, die wir unentwegt unbemerkt hin und her senden, haben als Absender eine IP-Adresse und als Empfänger eine IP-Adresse.

Das Internet sorgt nur dafür, dass diese Pakete zugestellt werden. Blitzschnell. So eine IP-Adresse besteht aus vier Zahlen zwischen 0 und 255, etwa 191.168.0.1. Weil sich damit aber nur rund 4,3 Milliarden Geräte abbilden lassen, früher genug, heute längst nicht mehr, wird seit einigen Jahren auch eine erweiterte IP-Adresse (IPv6 genannt) verwendet. Die ist viel länger – und wird zunehmend benutzt. Aber von all dem merken wir als Benutzer nichts. Das machen die Apps, Programme, Computer, Smartphones, Server und Rechenzentren alles unbemerkt unter sich aus.



Wer steckt hinter einer IP-Adresse?

Aber dann müsste es doch ziemlich einfach sein, eine Täterin, einen Täter zu ermitteln: Nachschauen, wem die IP-Adresse gehört – und die Handschellen klicken.

Das wäre so, wenn Du und ich, wenn Dein Handy und mein Handy jeweils eine eigene, individuelle, unveränderliche IP-Adresse hätten – und auch irgendwo registriert wäre, wem sie gehört. Wie bei einer Telefonnummer zum Beispiel. Aber so ist es nicht. Wir als Konsumenten erhalten ständig neue IP-Adressen zugewiesen von unseren Mobilfunk-Providern oder DSL-Anbietern. Wir haben keine eigene, feste. Schalten wir das Handy ein, gibt’s eine IP-Adresse aus dem Fundus des Mobilfunkanbieters.

Unser DSL-Anbieter gibt uns eine andere IP-Adresse für zu Hause – und ändert die meist, spätestens alle 24h. Der Grund: Es gab lange Zeit zu wenige IP-Adressen, da mussten die Provider wirtschaften. Mittlerweile werden längere IP-Adressen verwendet, da gibt es keine Knappheit. Theoretisch könnte man jedem Gerät eine eigene, feste, unveränderliche Adresse geben. Aber das will niemand, weil das die Anonymität aufheben würde.

Bedeutet: Wenn die Polizei eine IP-Adresse findet, die in der Vergangenheit

verwendet wurde, weiß sie bestenfalls, welchem Provider sie gehört. Die Polizei muss dann anfragen: Wer hat am 25. November 2021 um 13:32 Uhr und 12 Sekunden die IP-Adresse sowieso benutzt? Da Provider dieser Daten in der Regel nur wenige Tage bis Wochen vorhalten, danach werden sie aus Datenschutzgründen gelöscht, können sie die Frage meist nicht beantworten. Ende der Ermittlungen.

Vorratsdatenspeicherung

Und genau hier kommt die umstrittene Vorratsdatenspeicherung ins Spiel. Provider sollen solche Nutzungsdaten länger speichern, etwa für solche Ermittlungen.

Die Vorratsdatenspeicherung ist in der EU eigentlich vorgeschrieben, wir hatten sie in Deutschland auch schon – doch sie ist seit 2017 ausgesetzt. Weil Bundesverfassungsgericht und EUGH die Gesetze gekippt haben. Mit dem Argument: unverhältnismäßig. Denn es werden sehr viele Daten – auch Orts- und Kommunikationsdaten – anlasslos von uns allen gespeichert. Eine Art

Generalverdacht – mit hohem Risiko, dass die Daten Begehrlichkeiten wecken und missbräuchlich verwendet werden.

Da machen Datenschützer und Netzaktivisten einen Punkt. Solche Daten müssten also absolut sicher erhoben und gespeichert werden – und nur für wirklich relevante Fälle genutzt werden dürfen: Terrorismus, Schwerstkriminalität, Missbrauchsfälle. Aber nicht für jeden Parkverstoß – oder sogar zu politischen Zwecken, was die Sorge vieler Kritiker ist.

Meiner Ansicht nach wäre das möglich. Dazu müssten aber zum einen die Gesetze wasserdicht formuliert sein, am besten europaweit, und penibel auf eine rechtsstaatliche Nutzung geachtet werden. Mit unabhängiger Kontrolle der Nutzung. Ich glaube, dann könnten die meisten Menschen mit so einer Regel leben (nicht alle), und die Polizei hätte mehr Daten, die so dringend braucht.

Digitale Kummunikation: Faszinierend und erschreckend zugleich

Wir informieren uns heute digital - und wir informieren auch andere digital. Das ist auf der einen Seite faszinierend, denn diese direkte Kommunikation bietet eine Menge Möglichkeiten. Aber es sind auch eine Menge Probleme damit verbunden, vor allem Desinformation, Hate Speech und Verschwörungstheorien.

Die Digitalisierung ist nicht aufzuhalten: Längst ist sie in praktisch jeden Bereich unseres Lebens vor- und eingedrungen. Und da wo noch nicht, ist es wohl nur eine Frage der Zeit. Egal ob privat, zu Hause, im Büro, an der Schule oder Hochschule, in der Medizin und vor allem im Bereich der Information – einfach überall.

Die Digitalisierung 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, die mir mitunter durchaus

Kopfzerbrechen bereitet.

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 Inforamtionen 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?

Und das ist zum Beispiel in Krisenzeiten durchaus riskant.

Kommunikation in Krisenzeiten

b Corona oder nun im Ukraine-Konflikt: Es kursieren die merkwürdigsten Falschmeldungen und Verschwörungstheorien durchs Netz. Zum Beispiel Bilder, in denen der ukrainische Präsident Selenskij ein T-Shirt mit Hakenkreuz in der Hand hält, angebliche Abschüsse oder Erfolge – Kriegspropaganda im großen Stil. Selbst dass die Ukraine sich wieder mit Atomwaffen bewaffne, wird behauptet.

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?

Im Netz muss man ständig auf der Hut sein. Selbst bei vermeintlich seriösen Quellen.

Twitter führt neue Regeln ein - erst mal

Der Kurznachrichtendienst Twitter hat jetzt angekündigt, sich in Krisenzeiten stärker um die Reglementierung von Desinformation zu kümmern. Tweets mit Falschinformationen soll man nicht mehr liken können, es sollen Warnhinweise auftauchen – und seriöse Quellen bevorzugt werden. Wie lange das Bestand hat, wenn Elon Musk wie geplant Twitter tatsächlich kaufen sollte, steht in den Sternen. Denn Elon Musik hat „Freiheit total“ angekündigt – und meint damit: Jeder soll alles twittern dürfen.

Dabei hat schon der Philosoph Marcus Cicero gesagt: "Es gibt keine Freiheit ohne Regeln". Doch mit Regeln tun sich immer mehr Menschen schwer, insbesondere online. „Zensur!“, heißt es dann gleich empört. Wer nach Regeln verlangt, dem droht ein Hate Storm.

"Es gibt keine Freiheit ohne Regeln"
Marcus Cicero

Wie viel Meinungsfreiheit wollen wir uns leisten?

Vor allem 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.

Weg von Facebook: Auf Tauchstation

Immer mehr Anwendern geht die eigene Dauersichtbarkeit bei Facebook auf die Nerven. Trennt Euch doch einfach davon!

So gerne Ihr Facebook vielleicht auch nutzt (oder genutzt habt): Manchmal gibt es Situationen, da wollt Ihr einfach nicht sichtbar sein. Sei es ein Ort oder eine Veranstaltung, bei der Ihr nicht bei Facebook gesehen werden sollt, Ihr habt es nur teilweise in der Hand. Natürlich könnt Ihr darauf verzichten, dort einzuchecken. Wenn einer Eurer Freunde Euch aber markiert, dann seid Ihr erst einmal doch ungewollt sichtbar. Das lässt sich leicht verhindern!

Die erste Möglichkeit dazu ist das Einschalten der Chronikprüfung. Damit müsst Ihr jedes Mal, wenn jemand in Eure Chronik schreibt, die Freigabe dazu erteilen. Markierungen werden automatisch an die Chronik angeheftet. Dazu klickt in Facebook auf den Pfeil nach unten ganz rechts, dann auf **Einstellungen** > **Chronik und Markierungen**. Hier könnt Ihr unter **Überprüfung** die Freigabe einschalten.

Diese Vorabprüfung schützt zwar die Chronik, in dem Beitrag, in dem Ihr markiert wurdet, seid Ihr aber immer noch sichtbar. Wenn Ihr dies ausschließen wollt, dann hilft nur die Deaktivierung Ihres Facebook-Kontos. Diese funktioniert auch temporär!

Unter **Einstellungen** > **Allgemein** > **Konto verwalten** könnt Ihr die Deaktivierung vornehmen. Dadurch wird das Profil gesperrt. Der Name und das Foto werden von meisten Beiträgen und Seiten, die Ihr auf Facebook geteilt habt, entfernt. Manche Informationen können weiterhin für andere sichtbar sein. Beispielsweise der Name in deren Freundeslisten und Nachrichten, die Ihr gesendet habt.

Während der Deaktivierung sed Ihr als Benutzer auf Facebook gar nicht verfügbar. Derjenige, der Euch markieren will, bekommt Euch nicht angezeigt. Nach dem Aufheben der Deaktivierung wird das Profil wieder vollkommen hergestellt. So zumindest das Versprechen von Facebook.

Zero-Day-Lücke „Follina“ in MS Office – Hintergründe und Tipps

Ein neuer Zero-Day-Bug bei der Remote-Code-Ausführung in Microsoft Office sorgt zurzeit für Wirbel. Genauer gesagt handelt es sich wahrscheinlich um eine Sicherheitslücke bei der Codeausführung, die über Office-Dateien ausgenutzt werden kann.

Die IT-Sicherheitsexperten von Sophos beschreiben Lücke und Hintergründe und verweist auf Lösungsmöglichkeiten. Zudem wurde inzwischen von Microsoft eine offizielle Problemumgehung veröffentlicht.

Nach allem, was bislang bekannt ist, gibt es eventuell aber auch andere Möglichkeiten, diese Schwachstelle auszulösen oder zu missbrauchen. Der Sicherheitsforscher Kevin Beaumont hat der Lücke den Namen „Follina“ gegeben, der sich als nützlicher Suchbegriff zu dem Thema erweist, bis eine offizielle CVE-Nummer vergeben ist. Sophos-Experte Paul Ducklin gibt in seinem Blogbeitrag einen Einblick in Hintergründe und Lösungsansätze.

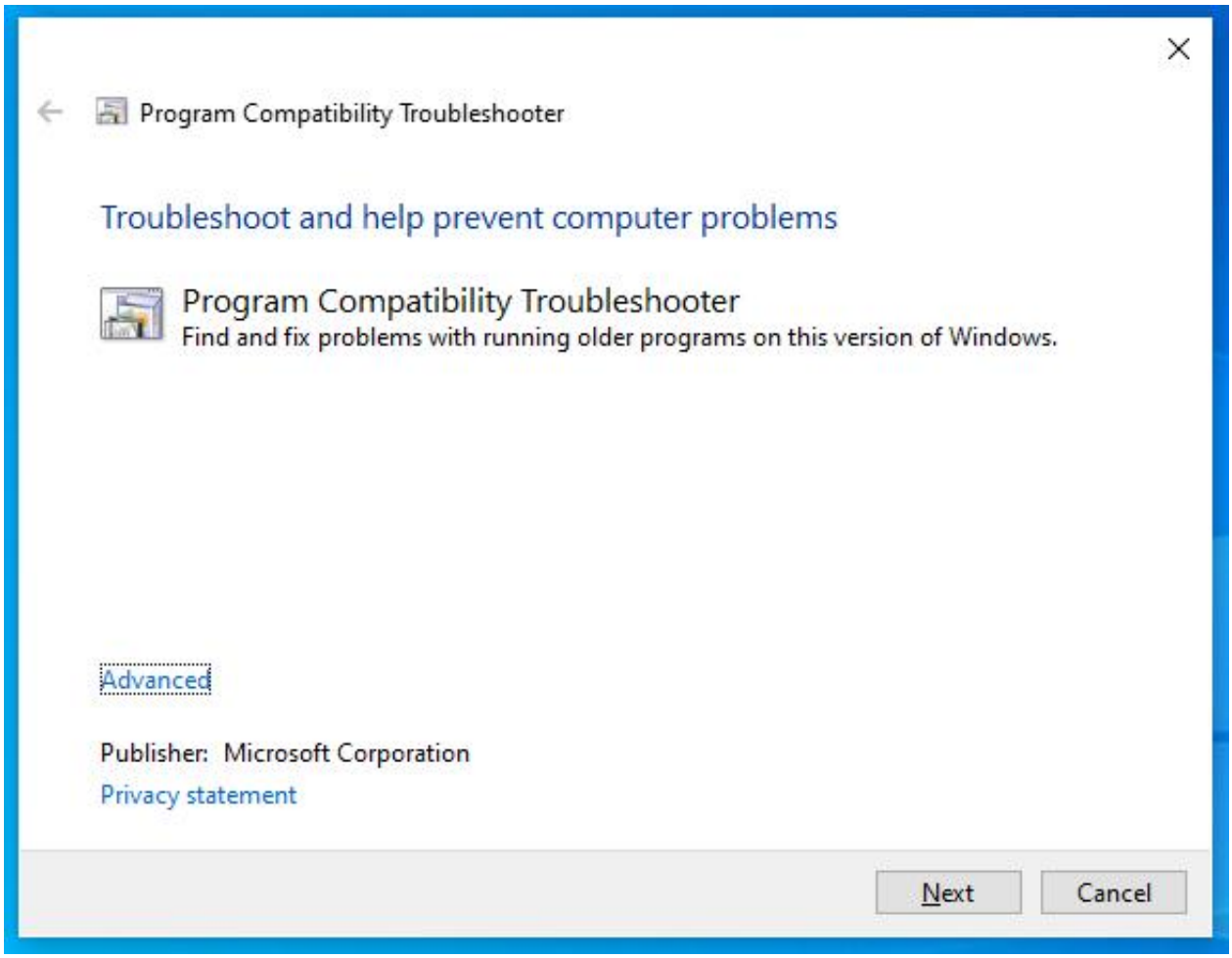
Wie funktioniert die aktuelle Lücke?

- Anwender öffnen eine mit versteckter Malware versehene DOC-Datei, die sie z.B. per E-Mail erhalten haben.
- Das Dokument verweist auf eine normal aussehende https:-URL, die heruntergeladen wird.
- Diese https:-URL verweist auf eine HTML-Datei, die einen JavaScript-Code enthält.
- Das JavaScript wiederum verweist auf eine URL mit der ungewöhnlichen Kennung ms-msdt: anstelle von https:. Unter Windows ist ms-msdt: ein proprietärer URL-Typ, der das MSDT-Software-Toolkit startet. MSDT ist die Abkürzung für Microsoft Support Diagnostic Tool.
- Die zum MSDT via URL übermittelte Befehlszeile führt dazu, dass nicht vertrauenswürdiger Code ausgeführt wird.

Wenn der bösartige ms-msdt:-Link aufgerufen wird, löst er einen MSDT-Befehl mit Befehlszeilenargumenten wie dem folgenden aus:

msdt /id pcwdiagnostic ....

Wenn es von Hand ausgeführt wird, ohne andere Parameter, lädt dieser Befehl automatisch MSDT und ruft die Programmkompatibilitäts-Fehlerbehebung auf, die harmlos aussieht:



Von hier aus können Nutzer eine App zur Fehlerbehebung auswählen, die verschiedene, support-bezogene Fragen beantwortet, automatisierte Tests in der App durchführt oder das Problem Microsoft meldet und gleichzeitig verschiedene Daten zur Fehlerbehebung hochlädt. Obwohl Nutzer:innen wahrscheinlich nicht erwarten, nur durch das Öffnen eines Word-Dokuments in dieses Diagnoseprogramm zu kommen, ist die Wahrscheinlichkeit doch erhöht, dass diese Reihe von Popup-Dialogfeldern „akzeptiert“ wird.

Automatische Remote-Skriptausführung

Im „Follina“-Fall sieht es allerdings so aus, als ob die Angreifer auf einige ungewöhnliche, aber auch sehr tückische Optionen gekommen sind, um sich in die Befehlszeile einzuschleichen. In der Folge erledigt die MSDT-Fehlerbehebung ihre Arbeit ferngesteuert. Anstatt gefragt zu werden, wie der Anwendende fortfahren möchte, haben die Cyberkriminellen eine Reihe von Parametern konstruiert, die nicht nur dazu führen, dass die Operation automatisch fortgesetzt wird (zum Beispiel die Optionen /skip und /force), sondern nebenbei auch ein

PowerShell-Skript aufrufen.

Zu allem Übel muss dieses PowerShell-Skript sich noch nicht einmal in einer Datei auf der Festplatte befinden – es kann in verschlüsselter Quellcodeform direkt aus der Befehlszeile selbst bereitgestellt werden, zusammen mit allen anderen verwendeten Optionen. Im „Follina“-Fall wird die PowerShell laut Hammond dazu verwendet, um eine ausführbare Malware-Datei zu extrahieren und zu starten, die in komprimierter Form bereitgestellt wurde.

Keine Makros erforderlich

Wichtig ist der Fakt, dass dieser Angriff von Word ausgelöst wird, das auf die betrügerische ms-msdt: URL verweist, auf die von einer URL verwiesen wird, die in der DOC-Datei selbst enthalten ist. Aufgrund dieses Vorgehens sind keine VBA-Office-Makros (Visual Basic for Applications) notwendig, sodass dieser Trick auch dann funktioniert, wenn Office-Makros deaktiviert sind.

Deshalb sieht das Ganze wie ein praktisches Office-URL-„Feature“ aus, kombiniert mit einem hilfreichen MSDT-Diagnose-„Feature. In der Tat wird allerdings eine Sicherheitslücke erzeugt, die per Klick einen Remote-Code-Execution-Exploit verursachen kann. Auf diese Weise kann schon das Öffnen eines derart präparierten Word-Dokuments Malware übertragen, ohne dass Nutzer:innen es bemerken.

Tatsächlich schreibt Hammond, dass dieser Trick in einen noch direkteren Angriff umgewandelt werden kann, indem der betrügerische Inhalt in eine RTF-Datei anstatt in eine DOC-Datei verpackt wird. In diesem Fall reiche es aus, nur eine Vorschau des Dokuments im Windows Explorer anzuzeigen, um den Exploit auszulösen, ohne auch nur darauf zu klicken, um es zu öffnen. Allein das Rendern des Thumbnail-Vorschaufensters brächte Windows und Office bereits zum Stolpern.

Was ist zu tun?

Microsoft hat bereits eine offizielle Problemumgehung veröffentlicht und wird hoffentlich zügig einen dauerhaften Patch vorlegen. So praktisch die proprietären ms-xxxx-URLs von Microsoft auch sein mögen, die Tatsache, dass sie darauf ausgelegt sind, Prozesse automatisch zu starten, wenn bestimmte Dateitypen

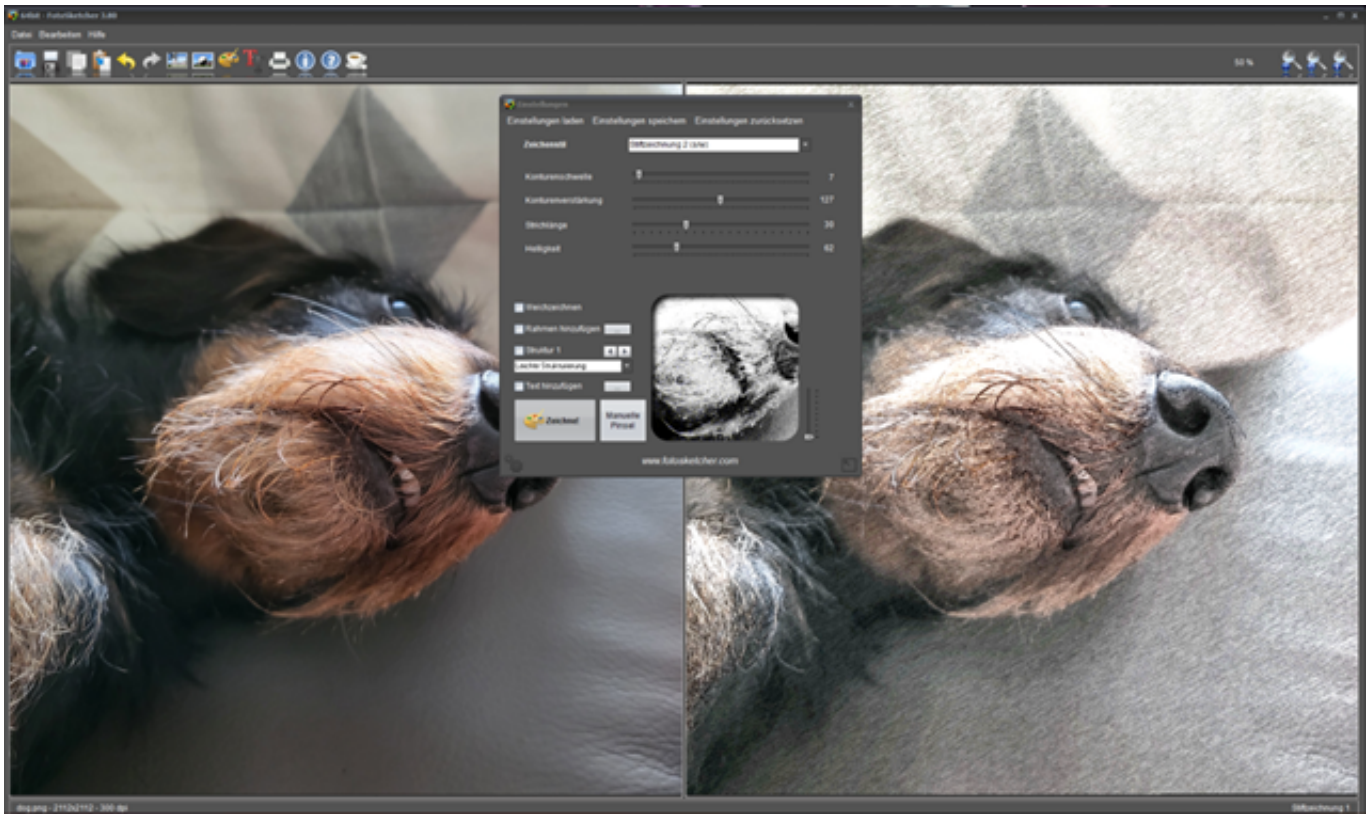
geöffnet oder auch nur in der Vorschau angezeigt werden, ist eindeutig ein Sicherheitsrisiko.

Zudem besteht eine in der Community allgemein anerkannte Problembehandlung darin, einfach die Beziehung zwischen ms-msdt: URLs und dem Dienstprogramm MSDT.EXE zu unterbrechen. Eine detaillierte Beschreibung hierzu gibt Sophos-Experte Paul Ducklin in seinem Blogbeitrag.

Vom Foto zum künstlerischen Bild: FotoSketcher

Fotos sind auf der einen Seite eine Abbildung der Realität. Manchmal sollen sie aber auch einen künstlerischen Anspruch haben und beispielsweise wie ein Gemälde aussehen. Wir zeigen Euch, wir Ihr das schnell erreichen könnt!

Die professionelle Bearbeitung der Bilder ist das eine. Manchmal aber soll es gar nicht so perfekt sein, sondern ein Bild soll eher einer Zeichnung, einem Cartoon oder einem Gemälde entsprechen. Statt hier manuell irgendwelche Filter anzuwenden, nutzt doch einfach die kostenlose App FotoSketcher.



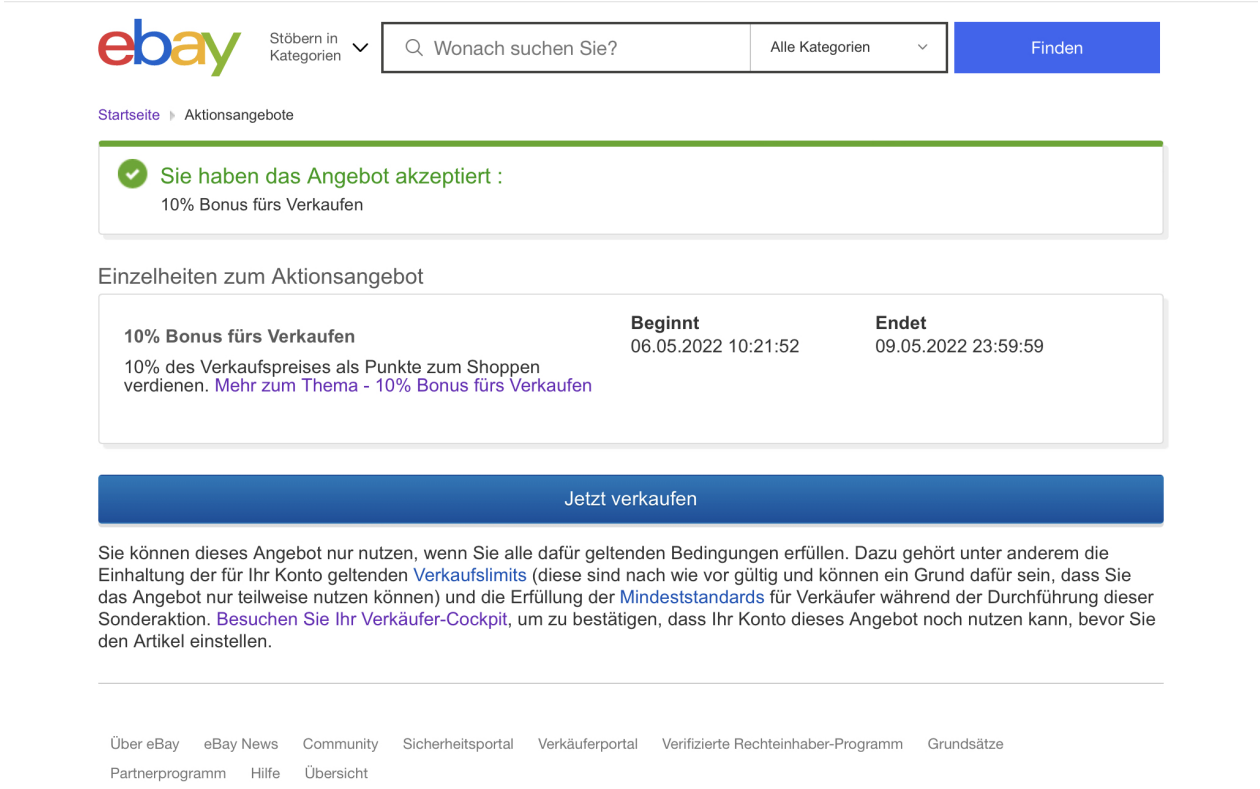
1. Klickt auf das Dateisymbol oben links in der App und such Euch das Bild heraus, das Ihr umwandeln wollt.
2. FotoSketcher bietet eine Vielzahl von Filtern, die Ihr auf die Bilder anwenden könnt. Klickt auf **Zeichenstil** und wählt den aus, den Ihr für passend haltet.
3. Die App zeigt im Vorschaufenster die Änderungen am Bild in einer Voransicht an. Mit dem Regler rechts davon könnt Ihr hinein- und herauszoomen.
4. Mit den Reglern unter dem Zeichenstil könnt Ihr diesen noch weiter anpassen. Hier müsst Ihr einfach so lange probieren, bis Euch das Ergebnis gefällt.
5. Mit einem Klick auf **Zeichne!** wendet Ihr die Einstellungen auf das Bild an. Die Berechnung des Zielbildes kann – abhängig vom Rechner, dessen CPU und Speicher – einen Moment dauern.
6. Klickt auf die **Diskette**, um das Bild zu speichern und dann weiterzuverwenden.

Bonuspunkte bei eBay auch ohne Banner aktivieren

Verkaufen bei eBay kostet Gebühren. Die werden dann und wann durch Bonuspunkte vermindert. Wir zeigen Euch, wie Ihr das Maximum herausholt.

Wie so oft gilt: Nichts ist umsonst im Leben. Das gilt auch für die Verkäufe bei eBay. So schon der Verkaufsbetrag aussieht, es gehen immer noch knapp 10 Prozent davon in die Taschen von eBay. Ärgerlich auf der einen Seite, verargumentierbar auf der anderen: eBay bietet die Plattform mit Soft- und Hardware, Kundenservice und mehr. Das muss bezahlt werden.

Zurückgehende Umsätze und Abwanderung von Kunden zum kostenlosen eBay-Kleinanzeigen haben eBay aber zum Umdenken gezwungen: Die Kunden werden durch Bonusaktionen gelockt. Eine davon sind die Bonus-Punkte: Pro verkauften Euro gibt es 5% als Gutschein zurück. Dieser Gutschein kann beim Einkauf bei eBay eingesetzt werden und verringert den Zahlbetrag entsprechend. Manchmal sind es auch 10%, was ja einen deutlichen Unterschied macht!



Diese Sonderaktion lässt sich aktivieren, wenn sie als Banner angezeigt wird, wenn Ihr eBay aufruft. Statt aber jetzt dauernd zu aktualisieren, könnt Ihr Euch mit diesem Hack Zeit sparen: Der direkte Link zu diesen Aktionen ist der hier. Wenn Ihr für die 10%-Aktion berechtigt seid, dann könnt Ihr sie direkt unter dem Link aktivieren.

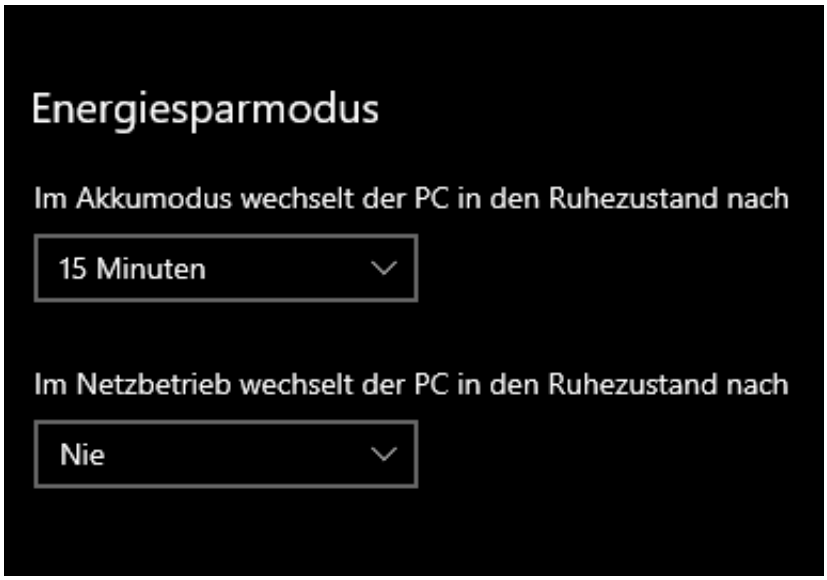
Der funktioniert nicht? eBay hat nach eigenen Angaben in der Testphase eine Aufteilung vorgenommen: Manche Kunden bekommen Bonuspunkte, andere reduzierte Gebühren. Diese Zuweisung soll sich frühestens Ende Juni 2022 ändern lassen!

Wenn ein Gerät nicht ins Standby geht

Wird ein Gerät mit einem Akku betrieben, dann sollte es bei Nichtverwendung in den Standby-Modus gehen. Klappt das nicht, dann ist der Akku schnell leer. Das kann verschiedene Ursachen haben!

Energiespareinstellungen kontrollieren

Zuallererst solltet Ihr die Energiespareinstellungen des Geräts kontrollieren. Unter Windows findet Ihr die in den **Einstellungen** unter **System** > **Netzbetrieb & Energiesparen**. Wichtig ist hier neben den Einstellungen für das Ausschalten des Bildschirms (die massiv Strom sparen) das Einschalten des Energiesparmodus.



Bei Smartphones wird der Standbymodus automatisch verwendet. Je nach Betriebssystem könnt Ihr hier nur wenig manuell einstellen. Sucht nach **Energie** im Menü des Geräts, um die entsprechenden Einstellungen zu finden. Da das automatische Standby bei diesen Geräten aber nicht generell ausgeschaltet werden kann, wird hier die Ursache für das Nicht-Abschalten der Geräte nicht liegen!

Verbindungen trennen

Wenn die Standbyeinstellungen stimmen, das Gerät aber trotzdem nicht in Standby geht, dann liegt das in den meisten Fällen an Verbindungen, die das Gerät aktiv aufgebaut hat. Kontrolliert das Folgende:

- Ist eine App geöffnet, die das Gerät auf Grund ihrer Aufgabe aktiv hält? Beendet alle Apps, um das herauszufinden.
- Ist eine Hardware verbunden, die den Standby verhindert? Bei Digitalkameras sorgt beispielsweise die Verbindung zu einer externen Fernbedienung regelmäßig dafür, dass die Kamera nicht zur Ruhe kommt, weil sie sonst nicht über die Fernbedienung auslösen könnte. So etwas kommt auch bei Tablets und PCs vor. Hier müsst Ihr Euer Gerät auf Herz und Nieren überprüfen, wenn das Ausschalten und Entfernen des Akkus nicht hilft.