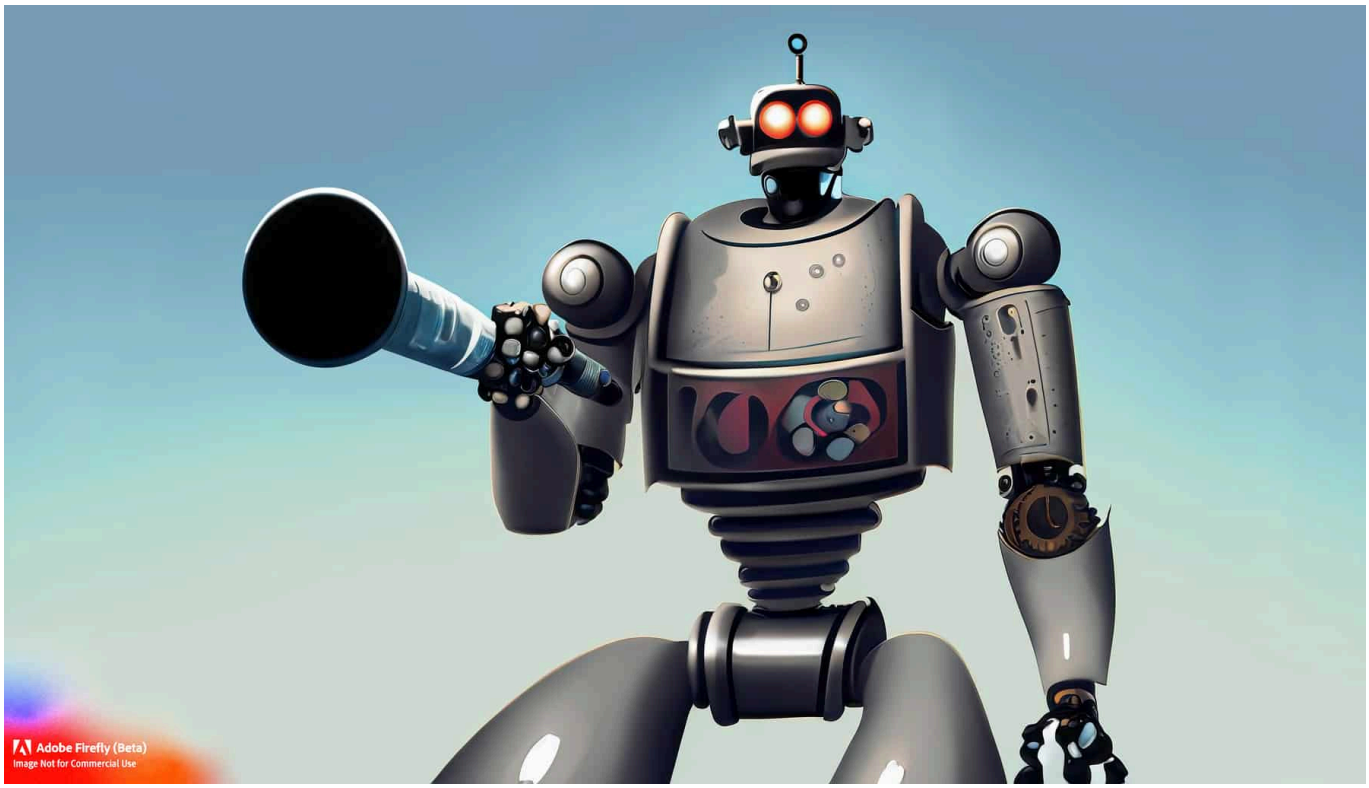
# Schieb Report

Ausgabe 2023.20

# Werden wir belauscht? Wenn Apps Gespräche mithören...




**Elon Musk hat jüngst behauptet, die Messenger-App WhatsApp würde seine User belauschen - und ausspionieren. Das wurde wiederlegt. Doch viele Leute glauben, dass Apps mithören und passende Werbung platzieren.**

Das Smartphone ist immer mit dabei. In unserer Hosentasche. Oder es liegt auf dem Tisch vor uns, während wir uns unterhalten. Ein stummer Zeuge, der alles mitbekommt. Viele Fragen sich: Hört da eigentlich jemand zu? Ich bekomme ja nicht mit, wenn das Mikro auf ist... Und immer wieder gehen Geschichten viral, dass man sich gerade über etwas unterhalten hat – und zwei Stunden später erscheint die passende Werbung dazu. In einem aktuellen Fall verdächtige ein Mitarbeiter von Twitter den Messenger-Dienst WhatsApp, Gespräche abzuhören – und Twitter-Chef Elon Musk hat das groß getwittert. Was ist dran an diesen Geschichten?

## Elon Musk erhebt schwere Vorwürfe gegen Whatsapp

Niemand Geringerer als Elon Musk behauptet auf Twitter, dass der Messenger-Dienst WhatsApp von Meta gelegentlich das Mikrofon aktiviert, um möglicherweise Gespräche zu belauschen. Was ist da dran?

Elon Musk twittert sogar einen Screenshot, indem man genau sieht, dass das mobile Betriebssystem Android den Zugriff auf das Mikrofon protokolliert – in einer Zeit, in der der Mitarbeiter WhatsApp garantiert nicht benutzt hat. Das ist in der Tat eine ungewöhnliche Beobachtung – aber eben noch längst kein Beweis, dass eine gezielte Spionage stattfindet.

https://twitter.com/elonmusk/status/1655967673107337216

Mittlerweile hat sich herausgestellt: Es gibt einen Fehler im mobilen Betriebssystem Android, der zu solchen Protokolleinträgen führen kann, unter bestimmten Umständen und das auf dem Google-eigenen Handy Pixel und auf einigen Samsung-Geräten. Aber es sind fehlerhafte Einträge. Den Zugriff auf das Mikrofon hat es nicht wirklich gegeben. Ein Neustart des Handys beseitigt den Fehler und damit das Problem.

## Aufmerksamkeits-Bias: Wir sehen, was wir sehen wollen

Aber man hört häufig Geschichten, auch im Kollegenkreis: Stellt Euch vor, wir haben über das neue Kleid von Dior gesprochen – und eine Stunde später habe

ich eine Werbe-Anzeige im Display dazu gesehen! Das kann doch kein Zufall sein... Wir werden belauscht, heißt es dann. Was ist da dran?

Solche Geschichten höre ich auch immer wieder, sie halten sich hartnäckig. Aber es gibt bislang keine Belege, dass sie den Tatsachen entsprechen. Klar, technisch wäre es denkbar, dass Facebook Gespräche abhört und dann passende Werbung zeigt – oder Google. Was allerdings dagegen spricht: Es würde auffallen. Denn zum einen müsste es unentwegt Zugriff auf das Mikro geben, was protokolliert wird. Z

um anderen würden ständig Daten abfließen, was zumindest Experten auffallen würde. Außerdem ist das praktisch überall streng verboten. Wenn das rauskäme, wären die Unternehmen geliefert. Das kann sich kein börsennotiertes Unternehmen leisten. In Wahrheit tritt ein anderes Phänomen ein: Wir reden über ein Produkt, von mir aus eine Bohrmaschine. Und eine Stunde später erscheint genau die in der Werbung.

Doch wenn wir darüber reden, haben wir uns auch damit beschäftigt. Vielleicht ein Tag vorher eine Webseite gesehen, auf der es um Handwerk geht – und/oder diese Bohrmaschine. Wir haben gegoogelt. Oder andere aus dem Haushalt haben gegoogelt oder einen Artikel gelesen... All das kann dazu führen, dass eine solche Anzeige erscheint. Aber diese Erklärung sehen wir nicht, stattdessen sehen wir eine Bestätigung für einen Verdacht. Hätten wir nicht über die Bohrmaschine gesprochen, wäre uns die Anzeige gar nicht aufgefallen. Das nennt sich Aufmerksamkeits-Bias. Das ist menschlich – aber unzutreffend.

## Mythos: Lauschende Apps

Der Mythos, dass Apps Menschen über das Mikrofon ihrer Smartphones belauschen und dann passende Werbung zu den Themen anzeigen, über die sie zuvor gesprochen haben, ist weit verbreitet. Dieser Mythos hat zu vielen Spekulationen und Besorgnis unter den Nutzern geführt. Hier sind einige wichtige Punkte, die dabei helfen können, den Mythos zu verstehen:

1. Technische Machbarkeit: In technischer Hinsicht wäre es möglich, dass eine App das Mikrofon eines Smartphones aktiviert und Gespräche aufzeichnet. Allerdings wäre dies rechtlich äußerst bedenklich und würde wahrscheinlich gegen die Datenschutzbestimmungen und Gesetze vieler Länder verstoßen.

2. Mangel an Beweisen: Trotz vieler Behauptungen und Anschuldigungen gibt es bisher keine stichhaltigen Beweise dafür, dass Apps heimlich Gespräche aufzeichnen, um personalisierte Werbung anzuzeigen. Viele dieser Behauptungen basieren auf reinen Spekulationen und Einzelfällen, die nicht ausreichend belegt sind.
3. Alternative Erklärungen: Es gibt alternative Erklärungen dafür, warum personalisierte Werbung angezeigt wird. Unternehmen sammeln umfangreiche Daten über das Verhalten der Nutzer im Internet, einschließlich Suchanfragen, besuchter Websites und getätigter Käufe. Mit Hilfe von Algorithmen und maschinellem Lernen können sie Profile erstellen und Anzeigen basierend auf diesen Informationen gezielt ausliefern, ohne dass eine tatsächliche Überwachung durchgeführt wird.
4. Zufall und Aufmerksamkeits-Bias: Oftmals entsteht der Eindruck, dass Apps tatsächlich Gespräche belauschen, weil Menschen dazu neigen, auf Dinge zu achten, die ihre Erwartungen bestätigen. Wenn jemand über ein bestimmtes Thema spricht und kurz darauf eine Werbeanzeige dazu sieht, wird dies als Bestätigung des Mythos interpretiert, während ähnliche Ereignisse, bei denen keine passende Werbung erscheint, einfach ignoriert werden.
5. Datenschutz und rechtliche Aspekte: Unternehmen sind daran interessiert, das Vertrauen der Nutzer zu wahren und rechtliche Konsequenzen zu vermeiden. Eine illegale Überwachung von Gesprächen über das Mikrofon würde nicht nur erheblichen rechtlichen und finanziellen Risiken ausgesetzt sein, sondern auch zu einem massiven Vertrauensverlust führen, der das Geschäftsergebnis langfristig schädigen könnte.

Bitte nicht missverstehen: Es ist zweifellos wichtig, grundsätzlich vorsichtig zu sein und die Berechtigungen von Apps zu überprüfen, um den Datenschutz zu gewährleisten. Wenn jedoch keine stichhaltigen Beweise vorliegen und alternative Erklärungen plausibel sind, sollte der Mythos um das Abhören über das Smartphone-Mikrofon mit einer gesunden Skepsis betrachtet werden.

## Siri, Alexa und Cortana hören mit

Allerdings ist es schon so, dass das Mikrofon immer mithören kann – ich kann doch „Hey Siri“ sagen, und man Handy spricht sofort mit mir...

Je nachdem, welches System wir benutzen – Siri, Alexa, Cortana – und wie wir die Geräte eingestellt haben (ob sie durchgängig lauschen sollen oder nicht) sind

die Mikros immer offen. Sie verstehen aber nicht jedes Wort. Dafür sind die Geräte zu „dumm“. Sie hören nur den jeweiligen Schlüsselbegriff: „Siri“, „Alexa“, „Cortana“. Fällt das Schlüsselwort, wird eine Aufzeichnung gemacht – und das Gesprochene geht an einen Server in der Cloud.

Dort wird die Sprachanalyse durchgeführt – und die Antwort zurückgeliefert! Das geht blitzschnell, deswegen merken wir es nicht. Aber die Sprachanalyse findet nicht im PC oder Smartphone statt. Dieser Mechanismus wird heutzutage in den modernen Betriebssystemen protokolliert. Wir müssen den Zugriff auf das Mikrofon explizit freigeben – und können das Protokoll einsehen.

Wir können auch bei Siri, Alexa oder Cortona in die Protokolle gehen, online, und uns anhören, was das aufgezeichnet wurde. Das können auch schon mal Gesprächsfetzen sein, etwa wenn wir eine „Alexa“ zu Hause haben und ein „Alex“ zu Besuch ist... Dann springt das System gelegentlich an. Aber auch hier: Ständiges Abhören, das wäre illegal und fällt auf.

*Der HomePod ist vollgepackt mit Innovationen von Apple, der Intelligenz von Siri und Smart Home Funktionen und sorgt für ein unglaubliches Hörerlebnis*

## Sicherheitseinstellungen überprüfen

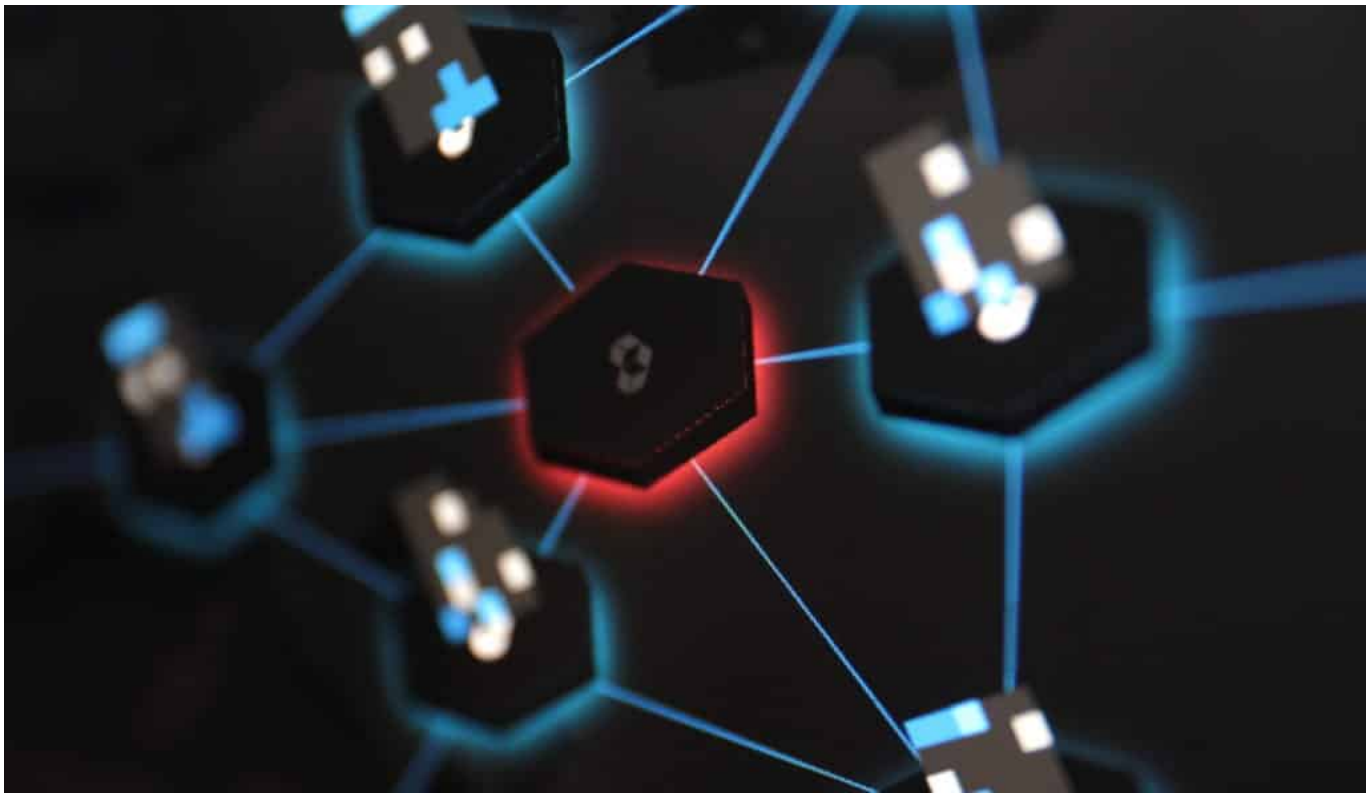
Bedeutet das: Ich muss mir gar keine Gedanken und Sorgen machen, abgehört zu werden?

So würde ich das nicht formulieren. Es ist gut, wachsam zu sein. Ein massenweises Abhören durch Google, Meta und Co. schließe ich aus. Gezielte

Spionage aber nicht. Wir wissen von israelischen Unternehmen, die gegen Bezahlung Menschen ausspionieren. Sie jubeln den Opfern Apps unter oder schalten Funktionen frei, die Mikro oder Kamera aktivieren. Dann ist ein Belauschen durchaus möglich.

Aber das wird eher nur in wenigen Einzelfällen geschehen, da aufwändig. Ich empfehle, ab und zu mal in die Sicherheitseinstellungen zu gehen und dort den Zugriff auf das Mikro zu überprüfen: In welchen Apps ist der Zugriff gewährt worden – und braucht es den wirklich? Wann wurde zuletzt auf das Mikro zugegriffen? Kann man alles sehen. Und im Zweifel lässt sich hier auch der Zugriff auf das Mikro wieder deaktivieren, was man auch machen sollte, wenn es keinen guten Grund für die Nutzung des Mikros gibt.

# Downloads löschen: Wenn der Speicher am iPad/iPhone voll wird



**Ihr habt Eure Daten unter Kontrolle, und deinstalliert auch Apps, die Ihr nicht mehr braucht, direkt wieder? Trotzdem wird Euer Speicher immer voller? Dann lest weiter!**

## Bilder: Schnell gemacht und speicherhungrig

Eigentlich ist es nicht wirklich logisch: Auf einem Windows- oder macOS-Gerät läuft ein umfangreiches Betriebssystem, große Programme und Eure Daten sind auch noch mit dabei. Viele Anwender kommen locker mit einem 128 GB-Modell aus, ohne in Speicherprobleme zu laufen. Bei einem iPhone hat Apple mittlerweile auf 128 GB in der Basisvariante umgestellt, die meistverkaufte Ausstattung hat 256 GB. Und trotzdem wird der Speicher immer mal wieder eng. Woran liegt das?

Zwei Datenkategorien sind auf einem Smartphone fast immer, auf einem Notebook oder Tablet nur in geringerem Maße vorhanden: Musik und Fotos.


Wenn Ihr mit MP3-Dateien arbeitet, statt zu streamen, dann kommen immer wieder neue Musikstücke hinzu, die Ihr synchronisiert. Das lässt die Musikbibliothek schnell anwachsen. Hier macht es Sinn, Playlisten zu verwenden, die von der Größe her zu begrenzen und nur diese mit dem Smartphone zu synchronisieren.

Bei den Fotos ist es ähnlich: Das Smartphone dient als Immer-dabei-Kamera, der große Speicher macht es fast unnötig, Bilder zu selektieren und die nicht so schönen zu löschen. Da kommen über die Jahre schon mal zwei- oder gar dreistellige Gigabyte an Daten zustande. Das könnt Ihr bei iOS charmant lösen:

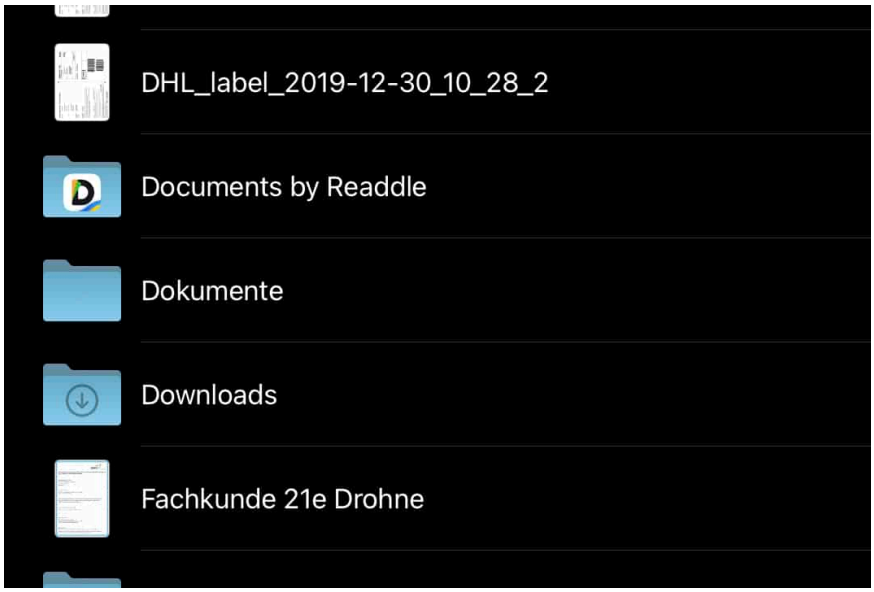
- Klickt auf **Einstellungen** > Fotos.
- Aktiviert **iPhone-Speicher optimieren**.

iOS lagert die Fotos in der Originalauflösung in iCloud aus und lässt nur ein Minibild mit verringerter Auflösung (und damit Größe) auf dem Gerät. Sobald Ihr das öffnet und vergrößern wollt, wird das Original geladen. Ihr verliert also keine Informationen, spart aber eine Menge Speicher!

## Vernachlässigte Gefahr: Downloads und Screenshots

Zwei Kategorien von Daten, die Ihr selten auf dem Schirm habt, sind die Downloads. Wann immer Ihr auf einer Webseite eine Datei herunterladet, wird diese zwischengespeichert. Aber eben nicht gelöscht. Diese Dateien nehmen mit

der Zeit eine Menge an Platz weg. Statt Euch jetzt durch Browsereinstellungen zu quälen, geht wie folgt vor:




- Startet die Dateien-App.
- Tippt in der linken Leiste auf **Downloads**.
- Tippt dann auf **Auswählen** > **Alles auswählen**.
- Tippt unten am Bildschirm auf **Löschen**.
- Alle Downloads werden gelöscht und der Speicher freigegeben.

Zum Löschen der Screenshots geht so vor:

- Öffnet die Fotos-App, dann tippt darin oben links auf das Symbol mit der Ordneransicht.
- Tippt auf **Alben**, dann auf **Bildschirmfotos**.
- Tippt dann auf **Auswählen** > **Alle**.
- Tippt unten am Bildschirm auf den Papierkorb.
- Alle Screenshots werden gelöscht und der Speicher freigegeben

# MacOS-Malware: Schützt Euch vor AMOS

**macOS war lange Zeit nahezu Malware-frei. Zu gering war der Marktanteil, dass es sich gelohnt hätte, Malware zu entwickeln. Mittlerweile hat sich das aber geändert. Aktuell sucht AMOS die Mac-Benutzer heim und versucht, Daten zu entwenden. Schützt Euch!**

## AMOS - Telegram als Malware-Shop

Viren sind am Ende nichts anderes als Programme. "Schadsoftware" eben. In den letzten Jahren haben sich die Kanäle dafür vervielfacht. Was früher nur im Darknet zu finden war, ist jetzt beispielsweise auch auf Telegram verfügbar. Da gibt es für jede Bösartigkeit eine eigene Gruppe, und da kommt auch AMOS her. Die lässt sich dort für den Schnäppchenpreis von USD 1000 pro Monat kaufen und erlaubt dem Käufer, ganz gezielt Angriffe zu planen. Über eine Weboberfläche lassen sie die Ziele konfigurieren.

Die Malware versteckt sich hinter eine DMG, also einem Installationspaket für macOS. Wie so oft muss der Anwender bei der Installation sein System-Passwort eingeben. Das wird dann durch AMOS dazu genutzt, das System zu durchsuchen

und auf vertrauliche Informationen zuzugreifen. Wenn diese durch das Kennwort geschützt sind, dann nutzt AMOS das abgegriffene Passwort, um sie freizuschalten. Die Informationen werden dann an einen Remote-Server geschickt und dort weiterverwertet.

## Schutz vor Malware auf dem Mac

Absoluter Schutz vor Viren, Ransomware und anderer Schadsoftware ist eine Illusion. Dafür gibt es zu viele Möglichkeiten, wie Ihr Euch die einfangen könnt. Wann immer Ihr online seid und Dateien herunterladet oder Webseiten besucht, lauft Ihr Gefahr, Euch eine solche Schadsoftware einzufangen. In den meisten Fällen aber hilft wirklich gesunder Menschenverstand:

- Wenn Ihr eine App im App Store bekommt, dann ladet sie von dort. Apple kontrolliert Apps hier sehr detailliert auf Schadensfunktionen. Das ist keine 100%-Sicherheit, aber schaltet schon ein großes Einfallstor für Schadsoftware aus.
- Wenn Ihr Software von einer Webseite herunterladet und diese nicht im App Store verfügbar ist, dann seid Euch sicher, dass der Anbieter auch vertrauenswürdig ist. Das ist oft bei kleineren Entwicklern der Fall, die den Prozess im App Store umgehen wollen.
- Seid Euch absolut sicher: Wer eine teure Software für einen Bruchteil des Preises anbietet, der hat nicht Euren Vorteil im Sinn. Beispielsweise dient für AMOS eine vermeintliche Vollversion von Adobe Premiere als trojanisches Pferd.

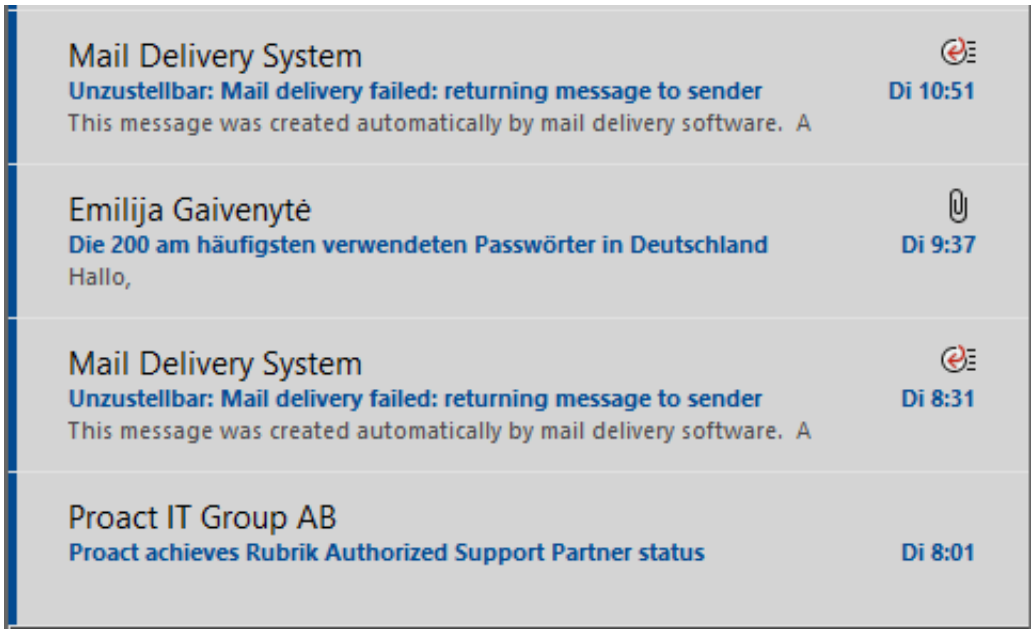
# Outlook: Junk-E-Mail richtig konfigurieren


**SPAM nervt. Der Junk E-Mail-Filter von Outlook hilft dagegen. Es ist aber nicht weniger störend, wenn bestimmte E-Mails fälschlicherweise als SPAM klassifiziert werden und Ihr sie zu spät seht. Tut etwas dagegen!**

## Junk-E-Mail: Wofür?

SPAM-E-Mails stören Euren Arbeitsablauf. Neben der Tatsache, dass sich darin auch durchaus Schadsoftware oder Phishing-Links verbergen können, kosten Sie Euch Zeit und Speicherplatz. Microsoft Outlook versucht das so weit es geht in den Griff zu bekommen, indem es eingehende E-Mails schon vor der Zustellung klassifiziert. Sind darin bestimmte Merkmale vorhanden, dann wird die E-Mail aussortiert. Zu diesen Faktoren gehören:

- Viele Empfänger im An-Feld
- Schlüsselwörter und Sonderzeichen im Betreff oder Inhaltsbereich der E-Mail
- Viele Links, Anhänge, Bilder oder aktive Inhalte

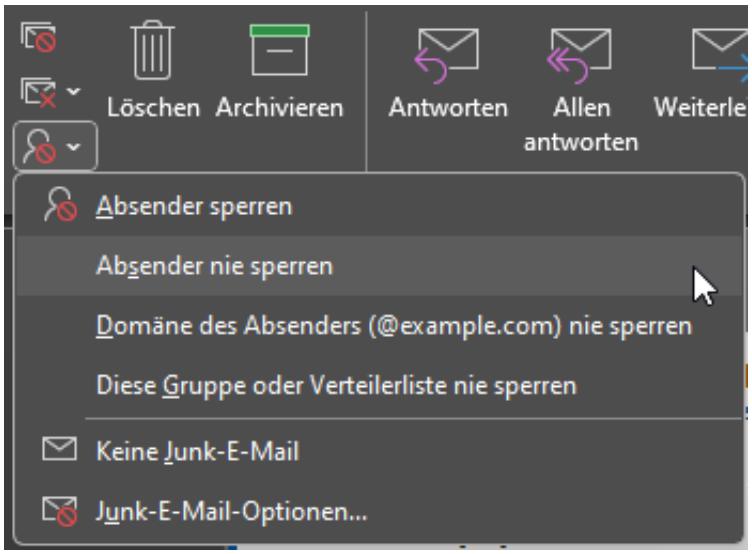



So gut automatisierte Erkennung ist, so sehr kann sie auch fehlerhaft sein. Ein Newsletter, der in der Regel einige diese Elemente enthält, eine weitergeleitete E-Mail, die von einem Eurer Kontakte stammt, es gibt viele Beispiele. Diese sollten möglichst nicht als SPAM klassifiziert werden. Das müsst Ihr Outlook im Einzelfall mitteilen, alleine unterscheiden kann es die Vertrauenswürdigkeit der besonderen E-Mails ja nicht.

## Anpassen des Outlook Junk-Filters

Meist fällt Euch die fälschliche Klassifizierung einer E-Mail erst dadurch auf, dass Ihr sie im Junk-Ordner statt im Posteingang findet. Daher müsst Ihr Eure Gegenmaßnahmen auch genau von dort einleiten:

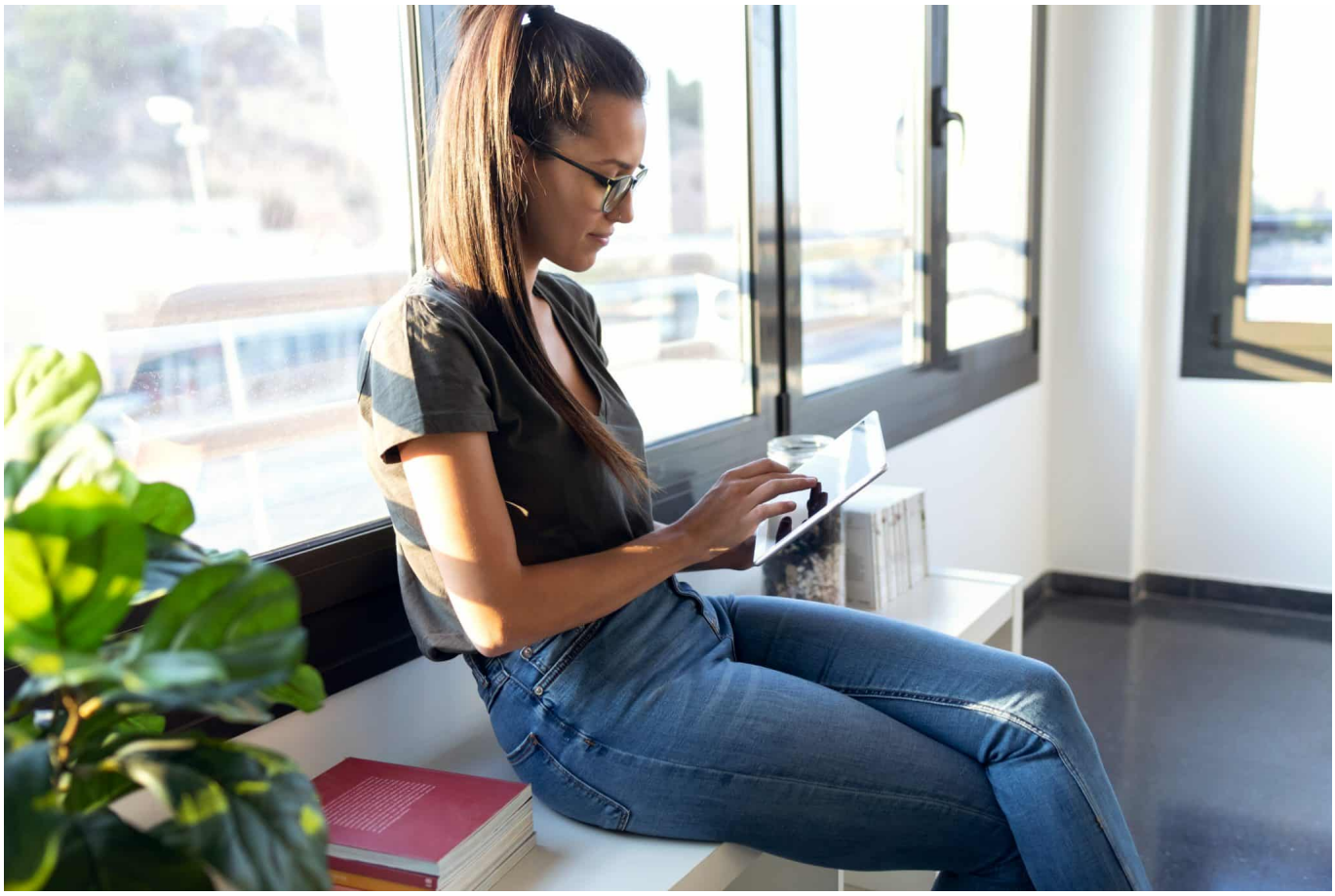
- Klickt in den Ordner **Junk E-Mail** in Outlook.
- Sucht die E-Mail heraus, die eigentlich hätte zugestellt werden sollen. Dabei kontrolliert genau, dass es tatsächlich eine echte E-Mail und keine ähnlich aussehende Phishing E-Mail ist!
- Klickt mit der rechten Maustaste auf die E-Mail in der Übersicht.




Ihr habt nun verschiedene Möglichkeiten, die E-Mail einzuordnen. Outlook wird Eure Einstellungen nach der Auswahl automatisch übernehmen:

- **Absender nie sperren** schiebt diesen Absender auf eine sogenannte Whitelist, eine Liste immer zugelassener Absender. Tatsächlich bedeutet das auch, dass auch echte SPAM-E-Mails des Absenders damit zugestellt werden.
- **Domäne des Absenders nie sperren** geht einen Schritt weiter: Wenn die E-Mail von *andreas@schieb.de* kam, dann wird nicht nur diese E-Mail-Adresse in die Whitelist aufgenommen, sondern alle E-Mail-Adressen, die von der Domäne *schieb.de* kommen.
- **Diese Gruppe oder Verteilerliste nie sperren** wirkt nicht auf den Absender, sondern den Empfänger: Newsletter werden oft an einen bestimmten Verteiler geschickt, hinter dem sich viele E-Mail-Adressen verbergen. Mit dieser Einstellung werden alle E-Mails an den Verteiler zugestellt - unabhängig von der Absenderadresse.

# Mehr digitale Teilhabe



Wir leben in einer Welt der Widersprüche. Die einen beklagen, dass in Sachen Digitalisierung in Deutschland nicht genug vorangeht – vor allem in Behörden und Verwaltung. Wenn Digitalisierung da ist, befürchten viele aber Datenschutzprobleme.

Trotzdem geht immer mehr online – und oft ist es ja auch bequem. Das führt dazu, so das Ergebnis einer aktuellen Studie, die diese Woche vom Branchenverband Bitkom vorgestellt wurde, dass selbst jene, die mit Digitalisierung bislang nicht so viel am Hut hatten privat, nachrüsten wollen.

## Studie: Mehrheit will mehr digitale Teilhabe

Es hat sich offensichtlich herumgesprochen, dass man online eine Menge machen und erledigen kann: Online mit anderen kommunizieren, Ticket für die Abendveranstaltung per App buchen, mal mit ChatGPT chatten – das geht nur mit Smartphone und/oder online am Computer. Drei von fünf Deutschen (60 Prozent) wollen mehr und intensiver am digitalen Leben teilhaben, hat die Studie herausgefunden.

Bei den Ältere über 75 Jahren ist der Wunsch besonders groß: Hier wünschen es sich sogar 69 Prozent, mehr online zu machen – hier ist aber auch der Nachholbedarf am größten. Doch wer nun denkt, bei den Jungen ginge nicht mehr online, der täuscht sich:

In der Altersklasse 16 bis 29 Jahren wünscht sich über die Hälfte mehr digitale Teilhabe (55 Prozent) – das hat mich ein wenig überrascht. Aber das ist zumindest das Ergebnis einer repräsentativen Umfrage im Auftrag der Initiative „Digital für alle“ des Branchenverband Bitkom unter mehr als 1.000 Personen in

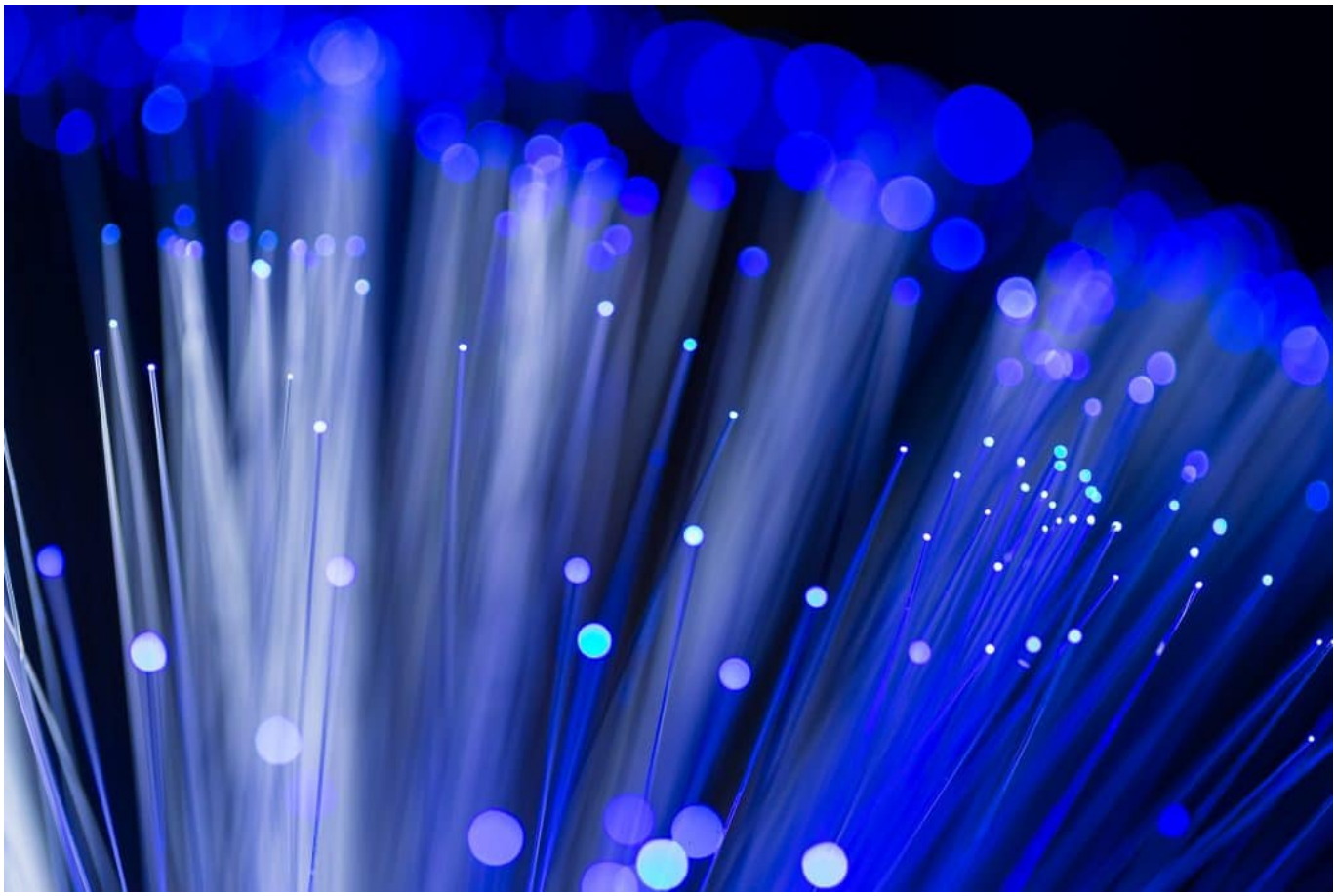
Deutschland ab 16 Jahren. Es gibt also noch Nachholbedarf.

*DSL und Mobilfunk sind in Deutschland häufig lagsam und teuer*

## Die Gründe für Zurückhaltung

Laut Umfrage gibt es drei Hauptgründe, die Menschen abschrecken: Zu unsicher, zu kompliziert, zu teuer. Weit oben auf der Liste steht – wenig überraschend – die Sorge um die Sicherheit der eigenen Daten, das sagen 64 Prozent. Kein Wunder, schließlich vergeht kaum m ein Tag ohne Hiobsbotschaften. Knapp vier von zehn Menschen (38 Prozent) ist die Nutzung zu kompliziert und drei von zehn (29 Prozent) fehlt das technische Wissen, um sich im Netz zu orientieren.

Ein Fünftel der Menschen hat Angst, etwas falsch zu machen (20 Prozent), oder weiß nicht, wo man bei Fragen oder Problemen Unterstützung bekommen kann (22 Prozent). Verständlich, denn wo gibt es heute noch Support? Aber es werden auch Kostengründe genannt. Jeder Achte (12 Prozent) kann sich die Nutzung der Geräte und Anwendungen nach eigenen Angaben nicht leisten.



*Glasfaser: Schnell und klimafreundlich - aber nicht ausreichend vorhanden*

## Das muss passieren

Wir machen alle gerne Witze über das berühmte Fax im Amt und Funklöcher... Wie sind wir aufgestellt in Deutschland in Sachen Digitalisierung?

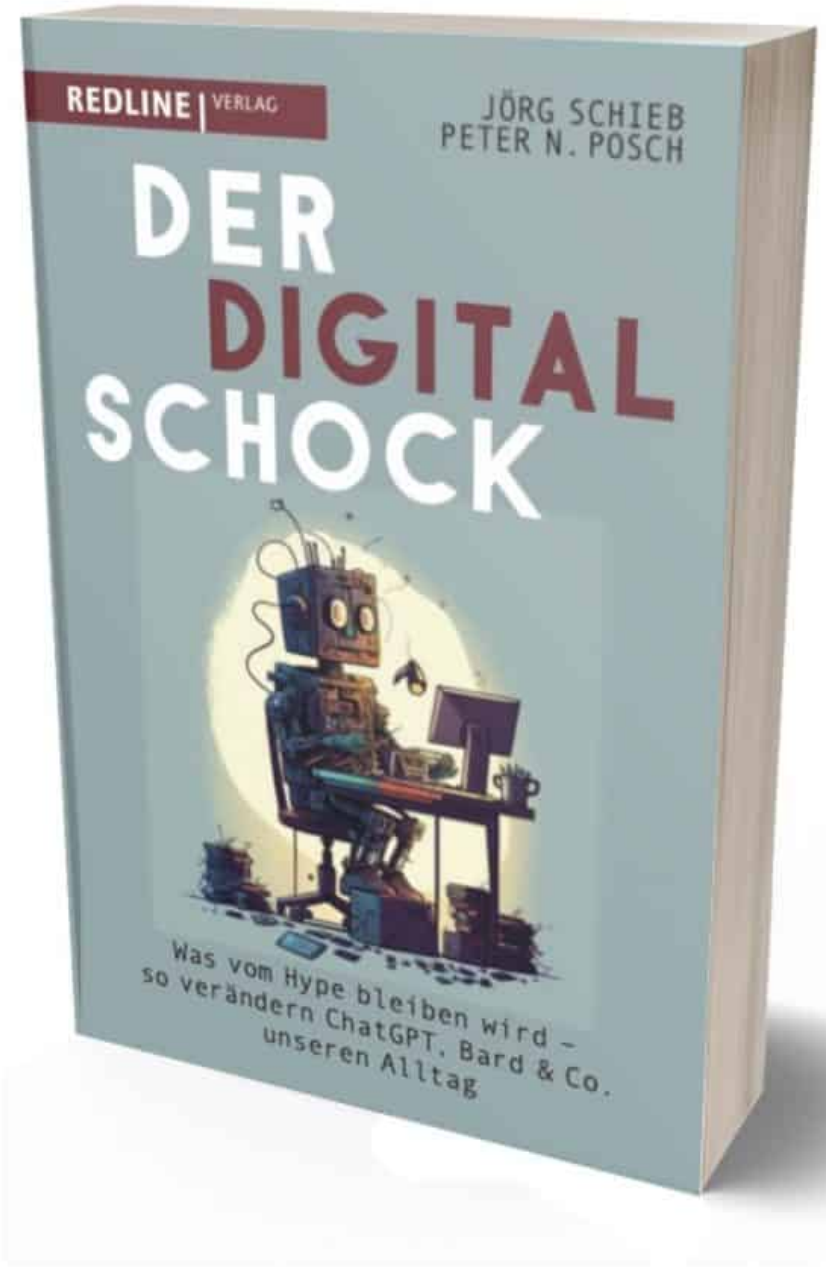
Es ist ja kein Geheimnis, dass die Herausforderungen der Digitalisierung in Deutschland alles andere als gut bewältigt werden. Das fängt bei der immer noch vergleichsweise schlechten Versorgung mit Breitband – ob per Glasfaser oder Mobilfunk an – und hört bei der Ausbildung nicht auf.

DSL und Glasfaser sind bei uns in Deutschland deutlich teurer als in anderen EU-Ländern. Dasselbe gilt für den Mobilfunk. Kein Wunder also, dass viele Menschen meinen, sie könnten sich Onlinegehen nicht leisten.

Und es ist nicht immer ein Problem der Regierung. Vodafone zum Beispiel hat allein im letzten Jahr 122.000 Breitband-Kunden verloren – wegen schlechter Qualität und häufig miserablem Service. Ich habe diese Erfahrungen selbst

gemacht.

Es braucht mehr Auswahl, mehr Wettbewerb, mehr Druck. Schulen und Hochschulen müssen ans Netz. Da sind wir dann doch wieder bei der Bundesregierung: Es ist ihre Aufgabe, für Infrastruktur zu sorgen.



Mein Buch der Digitalschock: Alles, was Ihr über ChatGPT wissen müsst

## Aktionstag Digitaltag

Ein Argument, nicht online zu gehen, was ja auch: Sorge um die eigenen Daten und Unkenntnis.

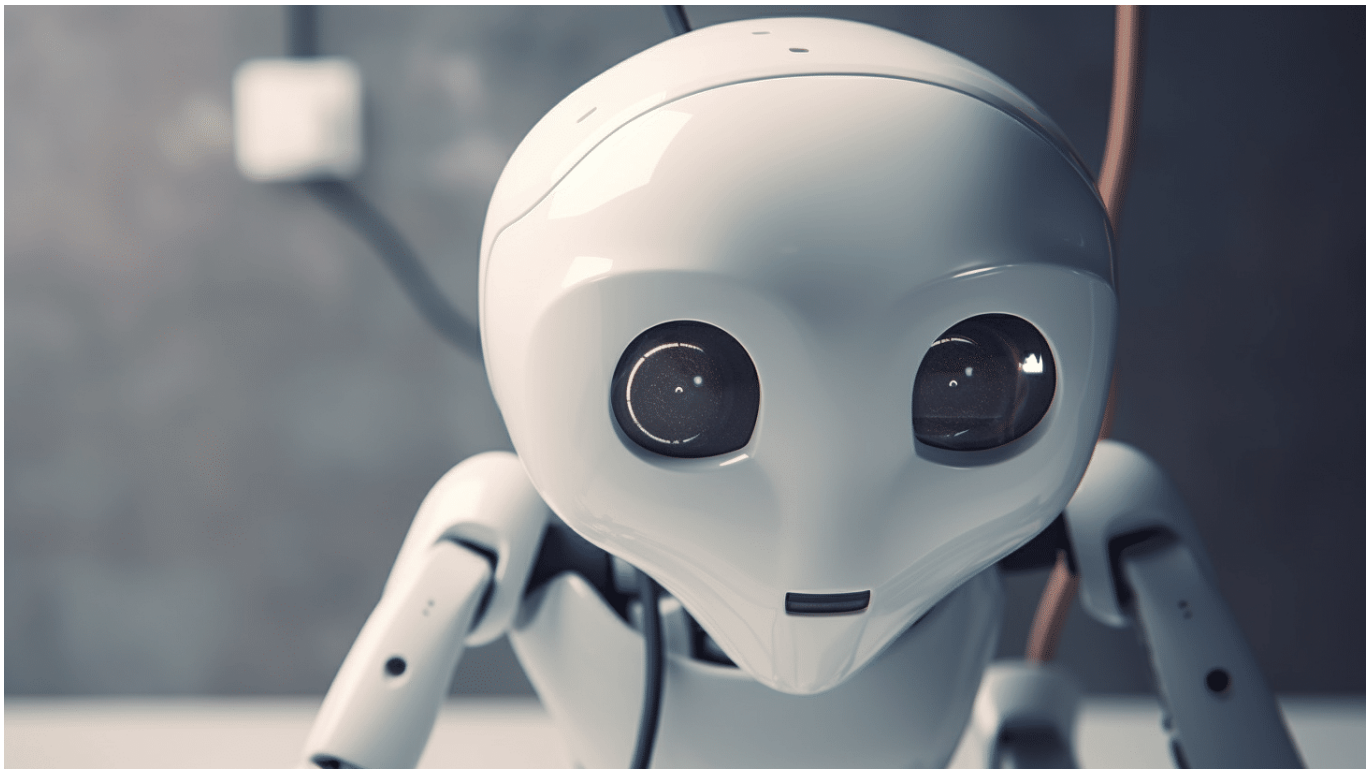
Was wäre da aus Sicht des Netzdenkers erforderlich?

Erstmal: Am 16. Juni gibt es einen Aktionstag Digitaltag mit Hunderten Aktionen in Volkshochschulen, Museen, öffentlichen Einrichtungen, mit jeder Menge Vorträge und Schulungen. Unter digitaltag.eu gibt es eine prima Übersicht, wo, wann, was stattfindet. Aber das ist nur eine einmalige Aktion.

Digitalisierung gehört endlich an die Schulen und Hochschulen, nicht als Informatik, sondern um Digitalkompetenz zu vermitteln: IT-Sicherheit, Datenschutz, Medienkompetenz. Das muss alles vermittelt werden. Nicht nur, damit Bürger kompetent sind, sondern auch, damit mehr Menschen Lust bekommen, kompetent in diesem Bereich zu arbeiten.

Es braucht ja Fachkräfte, die Apps entwickeln, Support machen, für IT-Sicherheit sorgen oder KI-Systeme aufsetzen. Es gibt viel zu tun!

# Was ist Künstliche Intelligenz? (KI)



**Es wird aktuell viel über KI geschrieben und gesprochen. Aber was ist KI eigentlich - also wann und wie verwendet man den Begriff?**

Künstliche Intelligenz (KI) bezieht sich auf die Fähigkeit von Maschinen, menschenähnliches Verhalten zu imitieren oder Aufgaben auszuführen, die normalerweise menschliche Intelligenz erfordern. Es handelt sich um ein multidisziplinäres Gebiet, das verschiedene Aspekte der Informatik, Mathematik, Statistik, Psychologie und Neurowissenschaften umfasst.

KI-Systeme basieren auf Algorithmen und Modellen, die es ihnen ermöglichen, Muster zu erkennen, Daten zu analysieren, Schlussfolgerungen zu ziehen und Entscheidungen zu treffen. Es gibt verschiedene Arten von KI, darunter:

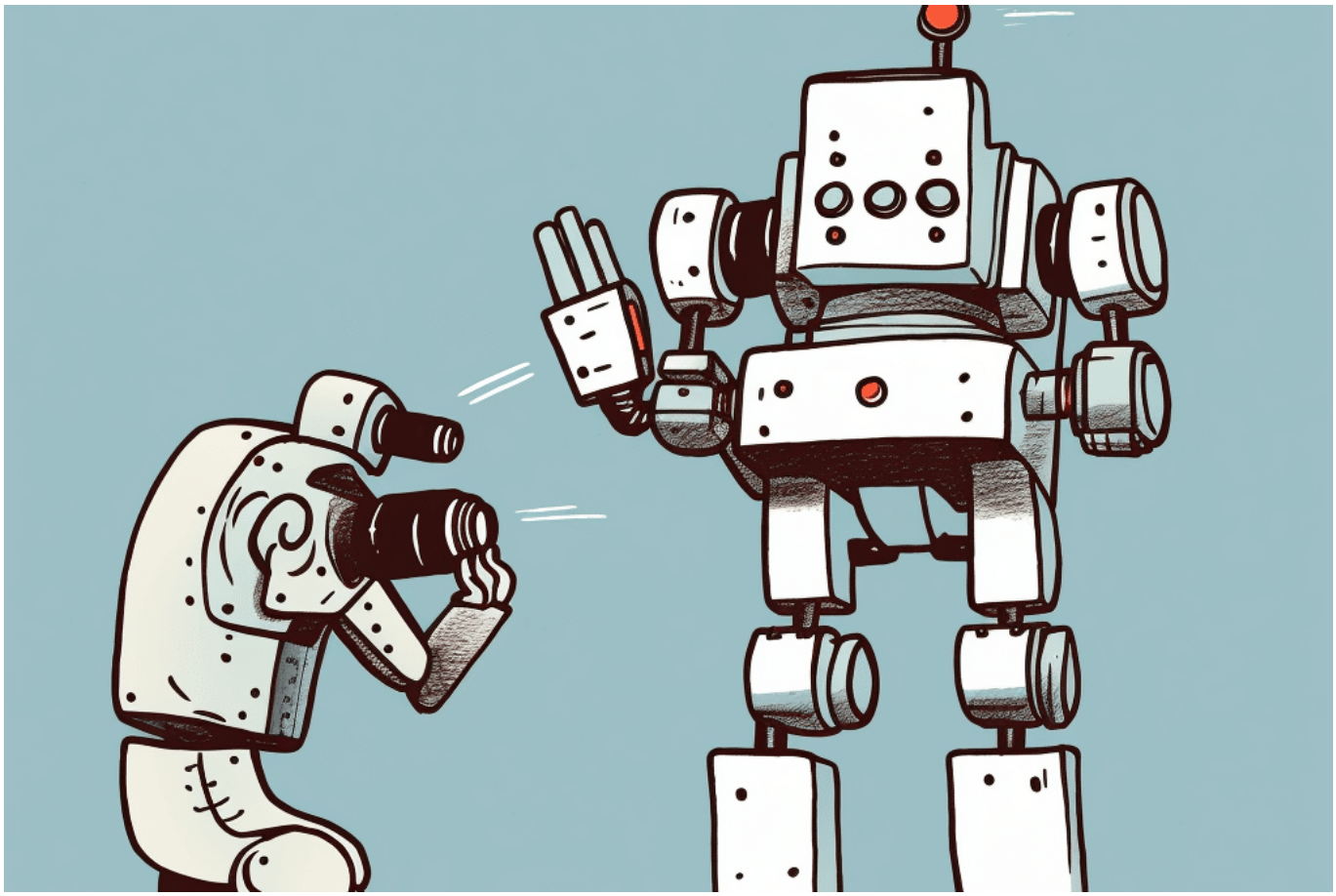
1. Schwache KI: Hierbei handelt es sich um KI-Systeme, die auf bestimmte spezifische Aufgaben oder Probleme beschränkt sind. Diese Systeme können zum Beispiel Bilderkennung, Spracherkennung oder Übersetzungen durchführen.
2. Starke KI: Dies bezieht sich auf KI-Systeme, die in der Lage sind, eine

breite Palette von kognitiven Aufgaben zu bewältigen, die normalerweise menschliche Intelligenz erfordern. Starke KI-Systeme sind in der Lage, Probleme zu verstehen, zu lernen, zu adaptieren und sogar Bewusstsein zu entwickeln.

3. Maschinelles Lernen: Dies ist ein Teilgebiet der KI, das sich mit der Entwicklung von Algorithmen befasst, die es Computern ermöglichen, aus Daten zu lernen und Vorhersagen oder Entscheidungen zu treffen, ohne explizit programmiert zu sein. Dabei werden Techniken wie neuronale Netze, Entscheidungsbäume und Support-Vektor-Maschinen eingesetzt.
4. Neuronale Netze: Diese basieren auf dem Modell des menschlichen Gehirns und sind eine spezielle Art von Algorithmen, die in der Lage sind, Mustererkennung und -analyse durchzuführen. Tiefe neuronale Netze, auch als Deep Learning bezeichnet, sind derzeit eine der leistungsfähigsten Techniken im Bereich der KI.

KI wird in vielen Bereichen eingesetzt, darunter Medizin, Finanzen, Verkehr, Unterhaltung, Sicherheit und Robotik. Beispiele für KI-Anwendungen sind virtuelle persönliche Assistenten wie Siri und Alexa, selbstfahrende Autos, Gesichtserkennungssysteme, Spam-Filter und medizinische Diagnosesysteme.

Es ist wichtig zu beachten, dass KI auch Herausforderungen und ethische Fragen mit sich bringt, wie beispielsweise Datenschutz, Arbeitsplatzautomatisierung, Voreingenommenheit in den Algorithmen und die potenzielle Kontrolle von KI-Systemen. Daher ist es von großer Bedeutung, KI verantwortungsbewusst und ethisch einzusetzen.



Ein Roboter fotografiert einen anderen Roboter

## Der Begriff Künstliche Intelligenz

Der Begriff "Künstliche Intelligenz" ist seit seiner Einführung in den 1950er Jahren weit verbreitet und hat sich als gebräuchliche Bezeichnung für das Feld etabliert. Es ist jedoch möglich, dass der Begriff einige Missverständnisse hervorruft oder unrealistische Erwartungen weckt.

Der Ausdruck "Künstliche Intelligenz" kann den Eindruck erwecken, dass es sich um eine Form von Intelligenz handelt, die mit menschlicher Intelligenz gleichwertig ist oder diese sogar übertrifft. In der Realität sind die meisten KI-Systeme jedoch auf spezifische Aufgaben oder Probleme beschränkt und können nicht in allen Aspekten mit menschlicher Intelligenz konkurrieren. Die meisten KI-Systeme sind auf bestimmte Daten oder Kontexte angewiesen und können Schwierigkeiten haben, außerhalb ihres spezifischen Anwendungsbereichs zu funktionieren.

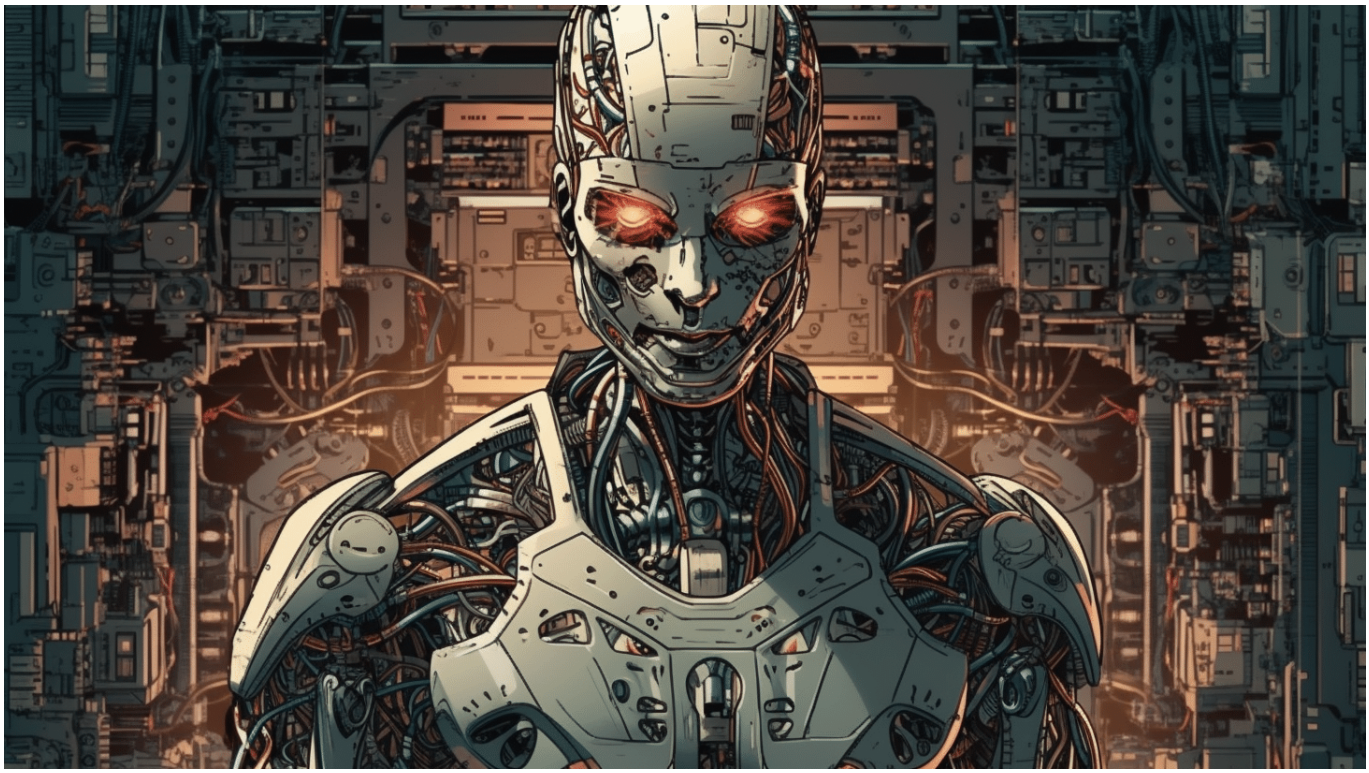
Ein weiterer Punkt ist, dass der Begriff "Intelligenz" selbst eine komplexe und vielschichtige Eigenschaft ist, die schwer zu definieren und zu quantifizieren ist.

Es gibt unterschiedliche Auffassungen darüber, was Intelligenz ausmacht und wie sie gemessen werden kann. Künstliche Intelligenz kann sich daher von menschlicher Intelligenz in Bezug auf ihre Funktionsweise und ihre Grenzen unterscheiden.

Einige Experten haben vorgeschlagen, den Begriff "Künstliche Intelligenz" durch präzisere Bezeichnungen zu ersetzen, um Missverständnisse zu vermeiden. Zum Beispiel wird der Begriff "Erweiterte Intelligenz" manchmal verwendet, um die Idee zu betonen, dass KI-Systeme dazu dienen können, menschliche Fähigkeiten zu erweitern und zu unterstützen, anstatt sie zu ersetzen.

Insgesamt ist es wichtig, bei der Betrachtung von Künstlicher Intelligenz und den damit verbundenen Begriffen wie "Intelligenz" und "KI" eine gewisse Vorsicht walten zu lassen und sich bewusst zu machen, dass es sich um ein sich entwickelndes Feld handelt, das seine Grenzen und Einschränkungen hat.

# KI: Eine Einschätzung der Möglichkeiten und Grenzen von Künstlicher Intelligenz

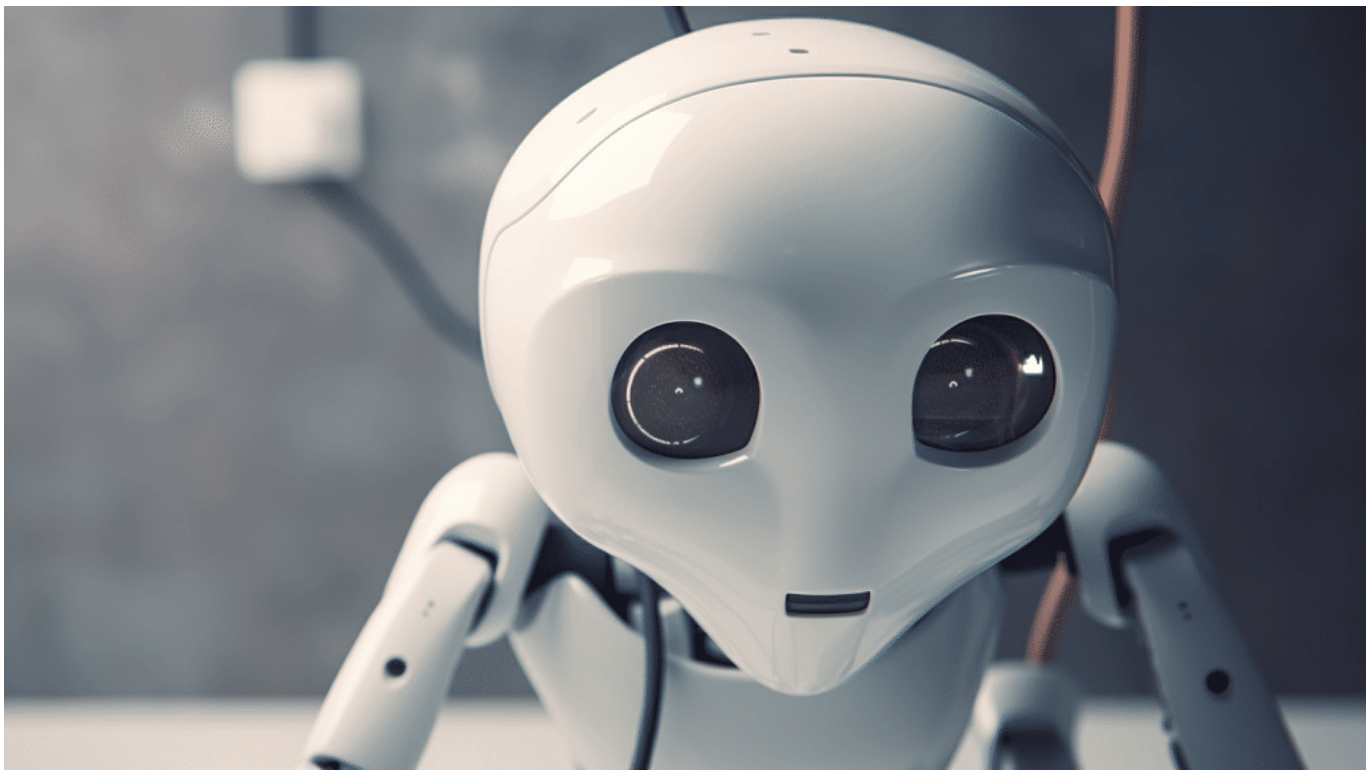


**Eine Einschätzung der Möglichkeiten und Grenzen von Künstlicher Intelligenz (KI).**

Wer hat in den letzten Wochen nicht mehrfach in Konferenzen oder auf Partys über die Chancen und Risiken von Künstlicher Intelligenz im Allgemeinen und über ChatGPT im Besonderen gesprochen? Bitte Hand heben... Ich bin überzeugt: Keiner hebt die Hand.

Kein Wunder, denn Künstliche Intelligenz (KI) ist derzeit eines der heißesten Themen in der Geschäftswelt. Es gibt viele Ansichten darüber, was KI alles kann und was nicht. In diesem Artikel möchte ich diese Frage beantworten und eine ehrliche Einschätzung darüber geben, welche Möglichkeiten KI derzeit tatsächlich

bietet.



*KI braucht eine Menge Energie*

## Was Künstliche Intelligenz kann

Zunächst einmal müssen wir verstehen, was KI wirklich ist. KI bezieht sich auf die Fähigkeit von Maschinen, menschenähnliche Intelligenz auf einer bestimmten Ebene zu entwickeln – daher auch der Name. Man kann vortrefflich darüber streiten, ob das „Intelligenz“ ist und wo sie eigentlich anfängt. Aber der Begriff ist geprägt – und wir müssen damit arbeiten. Bezeichnungen wie „maschinelles Lernen“ sind jedenfalls sehr viel besser. Denn das kann KI wirklich gut: Lernen!

KI verwendet Algorithmen, um Daten zu analysieren, Muster zu erkennen und Entscheidungen zu treffen. Es gibt verschiedene Arten von KI, einschließlich der regelbasierten KI, die auf der Grundlage von vordefinierten Regeln Entscheidungen trifft, der lernenden KI, die durch den Einsatz von Trainingsdaten ihre Entscheidungsfähigkeit verbessert und der tiefen KI, die neuronale Netze nutzt, um komplexe Entscheidungen zu treffen. Es gibt also verschiedene Disziplinen – und man sollte sie nicht immer alle im selben Atemzug nennen.

KI ist derzeit in der Lage, eine Vielzahl von Aufgaben zu erledigen, die

menschliche Intelligenz erfordern. Hier sind einige Beispiele:

1. **Bild- und Spracherkennung:** KI kann Bilder und Sprache erkennen und interpretieren. Dies hat Anwendungen in der Automatisierung von Geschäftsprozessen, der Analyse von Kundendaten und der Verbesserung von Kundenerlebnissen.
2. **Vorhersageanalysen:** KI kann Daten analysieren, um Vorhersagen zu treffen. Dies wird in vielen Branchen eingesetzt, einschließlich der Finanzdienstleistungen, der Gesundheitsbranche und des Einzelhandels.
3. **Entscheidungsfindung:** KI kann Entscheidungen treffen, indem sie Muster und Zusammenhänge in großen Datenmengen erkennt. Dies wird in vielen Unternehmen eingesetzt, um Prozesse zu optimieren und Kosten zu reduzieren.
4. **Chatbots und virtuelle Assistenten:** Darüber wird danke ChatGPT derzeit am meisten gesprochen. KI kann verwendet werden, um Chatbots und virtuelle Assistenten zu erstellen, die Kundenanfragen beantworten und den Kundensupport verbessern können.

*Was passiert, wenn jemand die Ballons loslässt?*

## Was Künstliche Intelligenz nicht kann

Allerdings gibt es auch einige Dinge, die KI (bislang) definitiv nicht kann. So kann KI definitiv nicht kreativ sein – auch wenn manche begeistert Beifall klatschen, wenn KI-Systeme wie Midjourney auf Anweisung (Sprache zu Bild) Bilder erzeugen, die mal traumähnlich aussehen, mal fast echte Fotografien – und damit den Medienbetrieb in eine Krise stürzt. Aber echte Kreativität im Sinne von: Hier wird etwas völlig Neues gedacht, entwickelt oder erschaffen, das ist nicht möglich. Per Definition, denn KI berechnet am Ende lediglich Wahrscheinlichkeiten, was am ehesten zur Anfrage passt. Wer rechnet, kann nicht kreativ sein. Wer denkt und fühlt schon. Aber Maschinen denken und fühlen nicht.

Auch emotionale Intelligenz und Empathie sind nicht die Sache von KI. Bestenfalls Simulationen davon. Dasselbe gilt für ein Urteilsvermögen: KI kann keine moralischen oder ethischen Entscheidungen treffen. Es kann keine subjektiven Entscheidungen treffen, die auf persönlichen Erfahrungen oder Überzeugungen beruhen. Allerdings kann KI „verstehen“: Wer ChatGPT ein Bild präsentiert, das ein Kind mit 30 gas-befüllten Luftballons in der Hand zeigt, und die KI fragt: „Was passiert, wenn das Kind die Kordel loslässt“, erfährt von ChatGPT-4: „Die Ballons fliegen weg“.

Das ist schon ein Durchbruch, weil eine Form von „Verstehen“.

Gleichwohl kann KI keine derzeit keine menschlichen Interaktionen vollständig ersetzen. Obwohl Chatbots und virtuelle Assistenten helfen können, Kundenanfragen zu bearbeiten, können sie keine menschliche Interaktion ersetzen, wenn es um komplexe Anfragen oder Probleme geht.


Mein Buch der Digitalschock: Alles, was Ihr über ChatGPT wissen müsst

# KI im Unternehmen: Verantwortungsvoller Umgang gefragt!

Als Unternehmer stellt man sich natürlich die Frage: Wie kann ich KI denn sinnvoll einsetzen, wo bietet sich das jetzt schon an? Die Antwort lautet: Wo nicht?

KI bietet derzeit viele Möglichkeiten für Unternehmen, um Prozesse zu automatisieren, die Effizienz zu verbessern und bessere Entscheidungen zu treffen. KI ist jedoch nicht die Lösung für alle Probleme und es gibt Bereiche, in denen menschliche Intelligenz nach wie vor unersetzlich ist. Es ist wichtig, dass Unternehmen die Grenzen von KI verstehen und sicherstellen, dass sie KI-Systeme verantwortungsvoll und ethisch einsetzen.

# Neue Funktion in WhatsApp: Chats lassen sich mit Passwort absichern


**Das haben sich bestimmt viele gewünscht: Bald lassen sich in WhatsApp einzelne Unterhaltungen in einem besonderen Ordner ablegen, der durch ein separates Passwort geschützt ist.**

WhatsApp, eine der beliebtesten Messenger weltweit, hat kürzlich eine neue Funktion eingeführt, die es den Benutzern ermöglicht, ihre Chats mit einem Passwort zu schützen. Diese innovative Sicherheitsmaßnahme wurde entwickelt, um sensible Informationen vor unautorisiertem Zugriff zu schützen und die Privatsphäre der Benutzer weiter zu stärken. Laut WhatsApp Blog wird die Funktion zeitnah freigeschaltet.

## Mehr Sicherheit für diskrete Chats

Die neue Chatsperre-Funktion in WhatsApp wurde eingeführt, um die Sicherheit der Chats zu erhöhen und Benutzern die Möglichkeit zu geben, ihre persönlichen

Gespräche vor neugierigen Blicken zu schützen. Indem sie ein Passwort festlegen, können Benutzer sicherstellen, dass nur autorisierte Personen Zugriff auf ihre Chatverläufe haben.

Um die Funktion zu nutzen, müssen Benutzer zunächst die neueste Version von WhatsApp auf ihrem Gerät installieren. Anschließend können sie in den Einstellungen den Abschnitt "Chatsperre" aufrufen und ein individuelles Passwort festlegen. Das Passwort kann entweder eine PIN oder ein Fingerabdruck-Scan sein, je nach den unterstützten Funktionen des Geräts.

Sobald die Chatsperre aktiviert ist, wird WhatsApp bei jedem Versuch, die Anwendung zu öffnen, nach dem Passwort fragen. Dadurch ist sichergestellt, dass nur autorisierte Personen Zugriff haben, die das Passwort kennen. Diese zusätzliche Sicherheitsmaßnahme schützt insbesondere sensible und private Informationen vor unbefugtem Zugriff, selbst wenn das Gerät in die falschen Hände gerät.


*WhatsApp Chat Lock: Passwort für Chats*

## Privatsphäre schützen - auch in der Gruppe

Diese Funktion ist besonders hilfreich für Benutzer, die ihre Privatsphäre schützen

möchten, insbesondere wenn sie ihr Gerät mit anderen teilen oder vor neugierigen Blicken bewahren möchten. Zusätzlich zur Chatsperre-Funktion können Benutzer auch auswählen, ob sie Benachrichtigungen im Sperrbildschirm anzeigen möchten oder nicht. Dies ermöglicht eine noch höhere Sicherheit und schützt vor versehentlichem Anzeigen vertraulicher Informationen.

Die Chatsperre-Funktion ist nicht nur für Einzelpersonen von Vorteil, sondern auch für Gruppenchats. Benutzer haben die Möglichkeit, die Chatsperre für bestimmte Gruppen einzurichten, um sicherzustellen, dass nur diejenigen, die das Passwort kennen, auf die Inhalte zugreifen können. Dies ist besonders nützlich, wenn sensible Informationen innerhalb der Gruppe geteilt werden und die Vertraulichkeit gewährleistet werden muss.

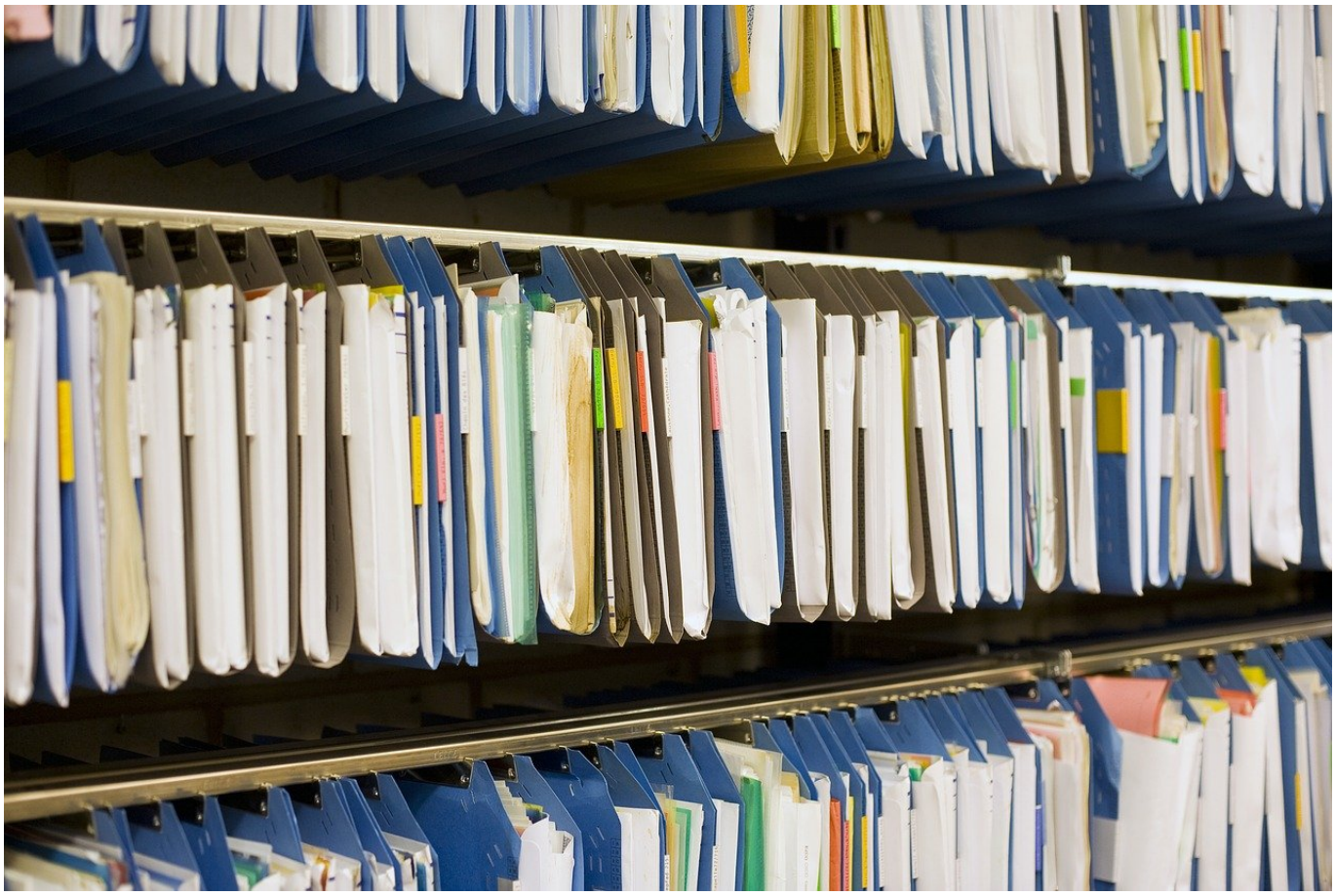
Es ist erwähnenswert, dass WhatsApp bereits eine Ende-zu-Ende-Verschlüsselung für alle Chats anbietet, um sicherzustellen, dass nur die beteiligten Benutzer die Nachrichten lesen können. Die neue Chatsperre-Funktion ergänzt diese Verschlüsselung und bietet eine zusätzliche Sicherheitsebene für die Nutzer.

Insgesamt ist die Einführung der Chatsperre-Funktion in WhatsApp ein Schritt in die richtige Richtung, um die Privatsphäre der Benutzer zu schützen und unautorisierten Zugriff auf ihre Chats zu verhindern.

Darüber hinaus hat WhatsApp darauf geachtet, die Chatsperre-Funktion benutzerfreundlich zu gestalten. Benutzer können das Passwort jederzeit ändern oder deaktivieren, wenn sie dies wünschen. Dies ermöglicht Flexibilität und erleichtert die Verwaltung der Chatsicherheit nach den individuellen Bedürfnissen und Vorlieben der Benutzer.

Es ist jedoch wichtig zu beachten, dass die Chatsperre-Funktion zwar eine wertvolle Sicherheitsmaßnahme ist, aber nicht als Ersatz für allgemeine Sicherheitspraktiken dienen sollte. Benutzer sollten weiterhin starke Passwörter verwenden, regelmäßig ihre Gerätesicherheit überprüfen und verdächtige Aktivitäten melden, um ihre digitale Sicherheit zu gewährleisten.

# Windows 11: Netzlaufwerke verbinden

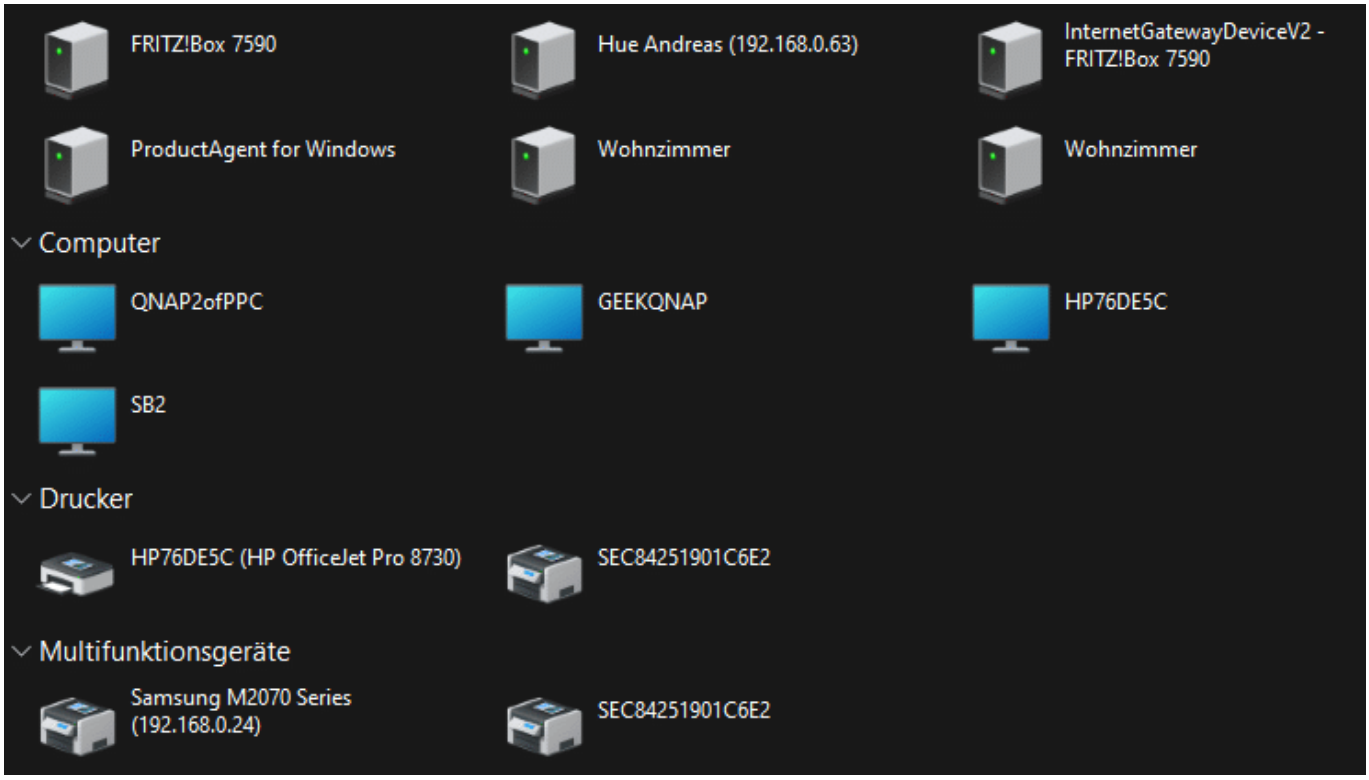


**Immer mehr Geräte bieten ihren Speicher im Netzwerk zum Zugriff an: Router, Netzwerkfestplatten, Freigaben an einem PC. Diese könnt Ihr in den meisten Fällen komfortabel als Laufwerke in den Explorer einbinden!**

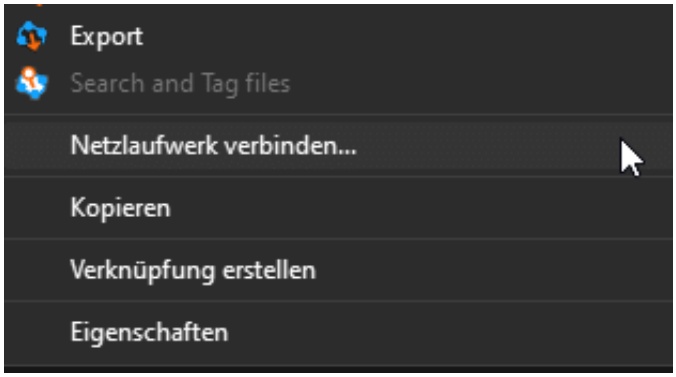
## Netzwerkspeicher: Was ist das?

Es ist schon lange nicht mehr so, dass Ihr nur auf einem Gerät arbeitet. Desktop und Tablet, diverse Netzwerkgeräte wie ein NAS (Network Attached Storage, also eine Netzwerkfestplatte), Euer Router, der einen USB- oder sogar SD-Karten-Slot hat und andere Geräte speichern Daten. Statt nun zwischen diesen Gerten hin- und herzulaufen und Daten zu übertragen, wird die Netzwerkverbindung dazu verwendet. Wenn Ihr der Meinung sei, dass das bei Euch ja nicht der Fall ist, dann

- Startet den Windows Explorer.
- Klickt im Verzeichnisbaum auf der linken Seite auf **Netzwerk**.
- In der Liste seht Ihr alle Geräte, die Ihr über das Netzwerk ansprechen könnt.




Zu den Geräten gehören natürlich auch Drucker, Netzwerklautsprecher und vieles andere, Die Kategorie Computer aber zeigt Euch alle klassischen Geräte mit Speichern.

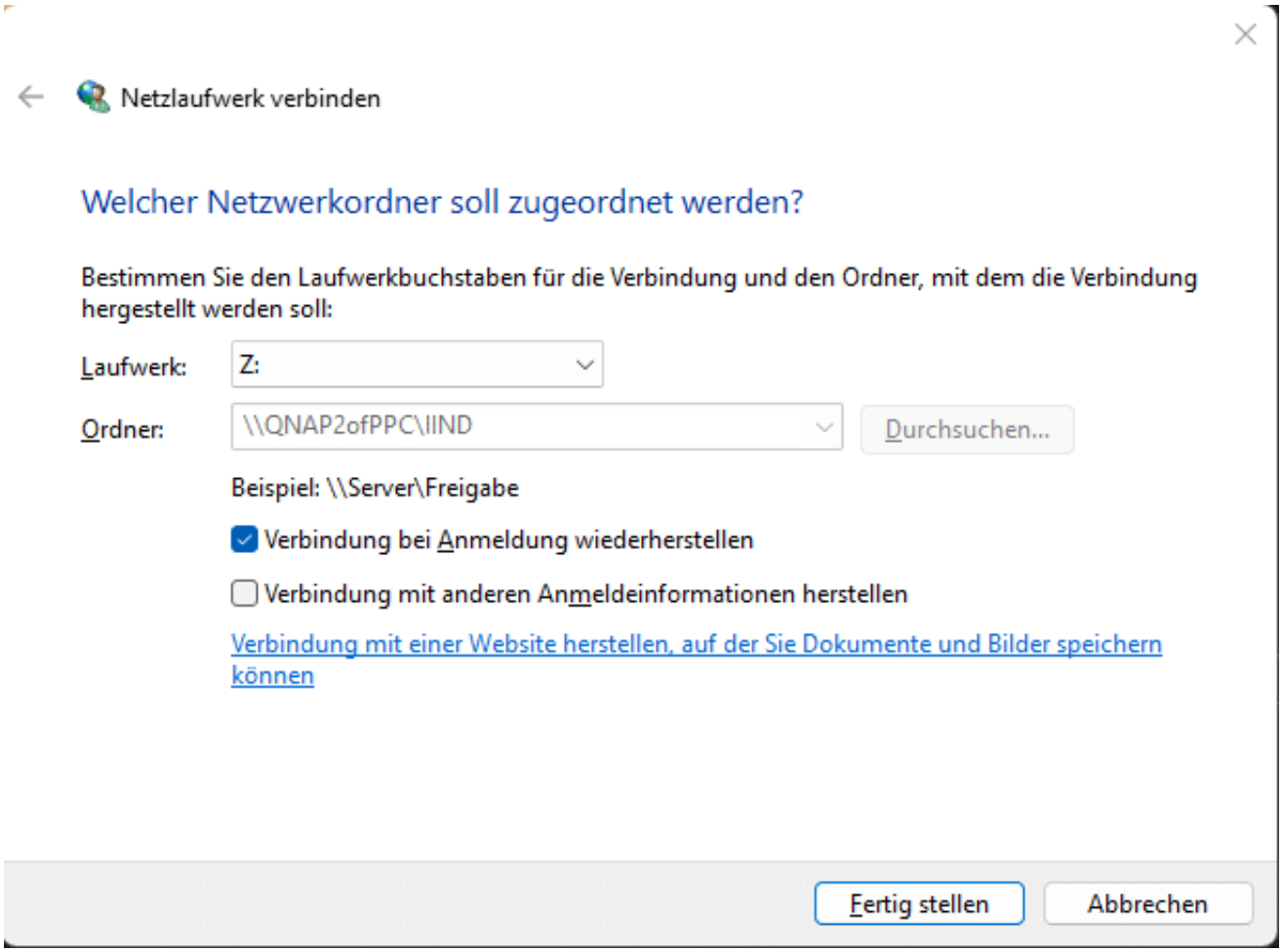



## Hinzufügen eines Netzwerklaufwerks

Grundsätzlich könnt Ihr durch einen Doppelklick auf ein Gerät in dieser Übersicht dessen freigegebenen Laufwerke öffnen und dann darauf zugreifen, einfacher und

komfortabler ist es aber, wenn Ihr die direkt als eigenes Laufwerk im Explorer zur Verfügung habt. Das ist mit wenig Aufwand machbar:

- Öffnet das Netzlaufwerk aus der Netzwerkumgebung, wie oben beschrieben,
- Klickt mit der rechten Maustaste hinein, dann unten im sich öffnenden Menü auf **Netzlaufwerk verbinden**.
- Im sich öffnenden Fenster müsst Ihr nun einige Rahmendaten festlegen.
- Unter **Laufwerk** wählt Ihr den Laufwerksbuchstaben, unter dem das Netzlaufwerk in Windows verfügbar sein soll. Windows zeigt Euch nur freie Buchstaben an (dazu gehört zum Beispiel nicht C:, der ja schon für die Systemfestplatte belegt ist).
- Der **Ordner** ist die Netzwerkadresse, die Windows erkennt. Die setzt sich immer zusammen aus dem Gerät, in dem die Netzwerkfestplatte eingebaut ist und dem Namen der Freigabe. Sie ist in der Form  \\\. Hier müsst Ihr nichts ändern.
- Wenn die Anmeldung ohne Benutzername und Passwort oder mit Euren Windows-Anmeldedaten stattfindet, dann müsst Ihr nichts machen. Wenn Ihr separate Anmeldedaten habt, dann klickt auf **Verbindung mit anderen Anmeldeinformationen herstellen**. Windows fragt diese Informationen ab, und Ihr könnt entscheiden, ob diese gespeichert werden sollen oder nicht.
- Wenn Ihr das neue Laufwerk immer verfügbar haben wollt, wenn Windows startet, dann setzt einen Haken bei **Verbindung bei der Anmeldung wiederherstellen**.


Netzlaufwerk verbinden
Welcher Netzwerkordner soll zugeordnet werden?
Bestimmen Sie den Laufwerkbuchstaben für die Verbindung und den Ordner, mit dem die Verbindung hergestellt werden soll:
Laufwerk:
Z:
Ordner:
\\QNAP2ofPPC\IIND
Durchsuchen...
Beispiel: \\Server\Freigabe
Verbindung bei Anmeldung wiederherstellen
Verbindung mit anderen Anmeldeinformationen herstellen
Verbindung mit einer Website herstellen, auf der Sie Dokumente und Bilder speichern können
Fertig stellen
Abbrechen