

A portrait of a man with short brown hair and a slight smile, wearing a teal button-down shirt. He is positioned on the left side of the frame, with his arms crossed. The background is dark. The text 'Schieb Report' is overlaid on the right side in a large, white, sans-serif font.

# Schieb Report

**Ausgabe 2023.14**

## Motorola: Vor 50 Jahren das erste Telefongespräch per Mobilfunk



Heute scheint es überall auf der Welt eine Selbstverständlichkeit, dass man auch ohne Kabel telefonieren kann - mobil und überall. Der Startschuss ist vor genau 50 Jahren gefallen: das erste Mobiltelefonat.

Vor 50 Jahren, am 3. April 1973, gab es das erste Mobilfunktelefonat der Welt. Geführt hat es Ingenieur Martin Cooper, der zu dieser Zeit bei Motorola arbeitete. Ein Konzern, der später für seine Prozessoren bekannt wurde, damals aber die ersten Mobiltelefone gebaut hat.

Cooper nutzte das damals revolutionäre **DynaTAC-Handy**, das er gemeinsam mit seinem Team bei Motorola entwickelt hatte. Das DynaTAC war das erste kommerziell verfügbare Mobiltelefon und gilt heute als Meilenstein in der Geschichte der Telekommunikation.

Das erste mobile Telefongespräch, das eine wahre weltweite Revolution auslösen sollte (wenn auch nicht in dem Tempo, in dem so etwas heute geschieht), war an sich eher schnöde. "Hi, Joel", murmelte Motorola-Ingenieur Martin Cooper ins

Telefon und damit zu seinem Kollegen. "Ich rufe dich von einem Mobiltelefon aus an. Ein richtiges Mobiltelefon. Ein persönliches, tragbares Mobiltelefon", erinnert Cooper sich an den ersten Anruf von einem Mobilfunkgerät jemals.



## Wow: Telefonieren ohne Kabel!

Zu dieser Zeit war das Telefonieren ohne Kabel noch völlig ungewohnt und unvorstellbar. Bis dahin war es üblich, mit einem kabelgebundenen Telefon zu telefonieren. Das DynaTAC war eine völlig neue Technologie und ein gewaltiger Durchbruch in der Geschichte der Telekommunikation. Das Handy war allerdings alles andere als handlich: Es war fast 30 cm lang, wog über 1 kg und hatte nur eine Sprechzeit von 30 Minuten. Zudem kostete es rund 3.995 US-Dollar, was umgerechnet heute etwa 22.000 Euro entspricht.

Heute ist das DynaTAC ein Relikt vergangener Zeiten. Das moderne Smartphone hat das Mobiltelefon revolutioniert und ist zu einem unverzichtbaren Begleiter in unserem Alltag geworden. Die Entwicklungen in der Telekommunikation haben in den letzten 50 Jahren einen gewaltigen Sprung gemacht. Heute können wir nicht

nur telefonieren, sondern auch im Internet surfen, E-Mails schreiben, Videos streamen, Spiele spielen und vieles mehr.

## **DynaTAC - kennt heute keiner mehr**

Die Geschichte des Mobilfunks begann jedoch lange vor dem DynaTAC. Bereits in den 1920er Jahren wurden die ersten drahtlosen Telefongespräche geführt, allerdings waren diese noch sehr begrenzt und störungsanfällig. In den 1940er Jahren wurden die ersten Mobilfunknetze für militärische Zwecke entwickelt. Es dauerte jedoch noch bis in die 1970er Jahre, bis die Technologie für den zivilen Gebrauch verfügbar war.

Das DynaTAC war ein Durchbruch in der Geschichte der Telekommunikation und hat den Weg für weitere Entwicklungen geebnet. In den 1980er Jahren wurden die ersten Mobilfunknetze für den öffentlichen Gebrauch eingeführt und in den 1990er Jahren kamen die ersten GSM-Netze auf den Markt. Mit der Einführung von UMTS, LTE und 5G haben sich die Möglichkeiten und die Geschwindigkeit des Mobilfunks noch weiter verbessert.

## **Gesellschaftliche Entwicklung des Mobilfunks**

Die Entwicklung von Mobiltelefonen ist jedoch nicht nur eine technologische, sondern auch eine gesellschaftliche Entwicklung. Handys haben die Art und Weise verändert, wie wir kommunizieren und wie wir unsere Freizeit verbringen. Die ständige Verfügbarkeit von Telefonen hat auch Auswirkungen auf unsere Arbeits- und Lebensgewohnheiten. Viele Menschen fühlen sich ständig unter Druck, erreichbar zu sein, was zu einer Zunahme von Stress und Burnout führen kann.

In den letzten Jahren haben sich auch Bedenken hinsichtlich der gesundheitlichen Auswirkungen von Mobiltelefonen auf den menschlichen Körper und insbesondere das Gehirn ergeben. Es gibt Hinweise darauf, dass die Strahlung von Mobiltelefonen schädlich sein kann und mit der Entstehung von Hirntumoren und anderen Gesundheitsproblemen in Verbindung gebracht werden kann. Die Forschung auf diesem Gebiet ist jedoch umstritten und es besteht weiterhin Bedarf an weiteren Studien, um die langfristigen Auswirkungen von Mobiltelefonen auf die Gesundheit zu verstehen.



## *Heute nutzen die Menschen ihre mobilen Geräte weniger zum Telefonieren*

Ein weiteres Problem im Zusammenhang mit Mobiltelefonen ist die zunehmende Abhängigkeit von Technologie und die damit verbundene Einschränkung der menschlichen Fähigkeit, soziale Interaktionen und zwischenmenschliche Beziehungen aufzubauen und aufrechtzuerhalten. Viele Menschen verbringen heute einen Großteil ihrer Zeit damit, auf ihre Smartphones zu starren, anstatt echte soziale Kontakte zu pflegen.

Insgesamt ist die Entwicklung von Mobiltelefonen eine beeindruckende Erfolgsgeschichte, die die Art und Weise, wie wir kommunizieren und leben, grundlegend verändert hat. Die Technologie hat uns viele Vorteile gebracht, aber es gibt auch Herausforderungen und Probleme, die mit der zunehmenden Nutzung von Mobiltelefonen verbunden sind. Es ist wichtig, dass wir uns dieser Probleme bewusst sind und uns bemühen, Technologie auf eine Weise zu nutzen, die sowohl uns als auch der Gesellschaft als Ganzes zugutekommt.

## Was ist besser für die Augen: Schwarz auf Weiß oder Weiß auf Schwarz?



**Wir alle sitzen viel am Bildschirm, bearbeiten Texte oder scrollen durch Webseiten. Da stellt sich früher oder später die Frage: Was ist eigentlich besser: Schwarze Schrift auf weißem Grund - oder umgekehrt? Kann man schließlich einstellen, aber worüber freuen sich die Augen?**

Eine Frage, die sich viele Menschen stellen, ist, welche Farbkombination bei Texten am "augenfreundlichsten" ist: Schwarz auf Weiß oder Weiß auf Schwarz? Es gibt viele Meinungen und Vorlieben zu diesem Thema, aber was sagen wissenschaftliche Erkenntnisse dazu?

Zunächst einmal ist es wichtig zu verstehen, wie das Auge funktioniert. Das Auge passt sich an unterschiedliche Lichtbedingungen an, um eine klare Sicht zu ermöglichen. In einer gut beleuchteten Umgebung ist es am besten, Text in dunkler Farbe auf hellem Hintergrund zu lesen, da dies weniger Anstrengung für die Augen bedeutet. Wenn jedoch die Umgebung dunkel ist, kann es angenehmer sein, Text in heller Farbe auf dunklem Hintergrund zu lesen, da dies weniger Licht in die Augen lässt und somit weniger Augenbelastung bedeutet.



*Schwarz auf Weiß oder Weiß auf Schwarz?*

## **Wissenschaftliche Studien belegen: Schwarz auf Weiß ist besser**

Es gibt auch wissenschaftliche Studien, die sich mit diesem Thema beschäftigen. Eine Studie aus dem Jahr 2007, die in der Zeitschrift "Ophthalmic and Physiological Optics" veröffentlicht wurde, hat gezeigt, dass das Lesen von Text in schwarzer Schrift auf weißem Hintergrund am besten für die Augen ist. Die Forscher fanden heraus, dass die Lesegeschwindigkeit und das Leseverständnis am höchsten waren, wenn der Text in schwarzer Schrift auf weißem Hintergrund angezeigt wurde.

Eine weitere Studie aus dem Jahr 2014, die in der Zeitschrift "Journal of Applied Psychology" veröffentlicht wurde, hat gezeigt, dass das Lesen von Text in weißer Schrift auf schwarzem Hintergrund weniger effektiv war als das Lesen von Text in schwarzer Schrift auf weißem Hintergrund. Die Forscher fanden heraus, dass die Lesegeschwindigkeit und das Leseverständnis beim Lesen von Text in weißer Schrift auf schwarzem Hintergrund im Vergleich zum Lesen von Text in schwarzer Schrift auf weißem Hintergrund um etwa 32 Prozent reduziert waren.

Es gibt jedoch auch einige Faktoren, die berücksichtigt werden sollten, wenn es um die Wahl der Farbkombination für Texte geht. Zum Beispiel kann das Alter der Person eine Rolle spielen. Ältere Menschen haben oft Schwierigkeiten, kleinere Schriftgrößen oder Texte mit niedrigem Kontrast zu lesen. In diesem Fall kann es für ältere Menschen möglicherweise einfacher sein, Text in heller Farbe auf dunklem Hintergrund zu lesen.

## **Auch Weiß auf Schwarz hat seine Vorteile**

Ein weiterer wichtiger Faktor ist die Art der Tätigkeit, die ausgeführt wird. Wenn Sie zum Beispiel längere Zeit am Computer arbeiten, kann das Lesen von Text in heller Farbe auf dunklem Hintergrund weniger anstrengend für die Augen sein, da dies weniger Licht in die Augen lässt.

Zusammenfassend lässt sich sagen, dass schwarze Schrift auf weißem Hintergrund die augenfreundlichste Farbkombination für das Lesen von Texten ist. Wissenschaftliche Studien haben gezeigt, dass das Lesen von Text in schwarzer Schrift auf weißem Hintergrund die höchste Lesegeschwindigkeit und das höchste Leseverständnis bietet. Es gibt jedoch auch Faktoren wie das Alter und die Art der Tätigkeit, die berücksichtigt werden sollten, wenn es um

die Wahl der Farbkombination für Texte geht. Wenn Sie längere Zeit am Computer arbeiten, kann das Lesen von Text in heller Farbe auf dunklem Hintergrund weniger anstrengend für die Augen sein. Eine Studie aus dem Jahr 2016, die in der Zeitschrift "Applied Ergonomics" veröffentlicht wurde, hat gezeigt, dass das Lesen von Text in weißer Schrift auf schwarzem Hintergrund bei geringerer Helligkeit am Computerbildschirm weniger müde macht.





*Displays sind generell nicht gerade optimal für unsere Augen*

## **Augen entlasten: So geht's**

Eine andere Studie aus dem Jahr 2017, die in der Zeitschrift "Displays" veröffentlicht wurde, hat gezeigt, dass das Lesen von Text in weißer Schrift auf schwarzem Hintergrund bei niedrigeren Helligkeitsstufen auf dem Bildschirm auch die Augenbelastung reduzieren kann. Die Forscher fanden heraus, dass der Kontrast zwischen Text und Hintergrund bei niedrigeren Helligkeitsstufen größer ist, was zu weniger Belastung für die Augen führt.

Es ist auch wichtig zu berücksichtigen, dass jeder Mensch anders ist und unterschiedliche Vorlieben hat, wenn es um die Farbkombination von Texten geht. Einige Menschen finden es angenehmer, Text in heller Schrift auf dunklem Hintergrund zu lesen, während andere es vorziehen, Text in dunkler Schrift auf hellem Hintergrund zu lesen. Es hängt auch davon ab, welche Art von Text gelesen wird. Zum Beispiel kann es für das Lesen von längeren Texten wie Büchern und Artikeln angenehmer sein, Text in dunkler Schrift auf hellem Hintergrund zu lesen, während es für das Lesen von kürzeren Texten wie

Nachrichten und Tweets angenehmer sein kann, Text in heller Schrift auf dunklem Hintergrund zu lesen.

Es ist auch wichtig zu beachten, dass der Bildschirm selbst eine Rolle spielt. Einige Bildschirme sind besser für das Lesen von Text in heller Schrift auf dunklem Hintergrund geeignet, während andere besser für das Lesen von Text in dunkler Schrift auf hellem Hintergrund geeignet sind. Es ist wichtig, die Helligkeit des Bildschirms an die Umgebung anzupassen, in der Sie arbeiten, um die Augenbelastung zu reduzieren.

## **Es kommt drauf an**

Insgesamt gibt es keine eindeutige Antwort darauf, welche Farbkombination am augenfreundlichsten ist. Es hängt von verschiedenen Faktoren wie dem Alter, der Art der Tätigkeit und den persönlichen Vorlieben ab. Wissenschaftliche Studien haben jedoch gezeigt, dass das Lesen von Text in schwarzer Schrift auf weißem Hintergrund die höchste Lesegeschwindigkeit und das höchste Leseverständnis bietet.

Wenn Sie längere Zeit am Computer arbeiten, kann es jedoch angenehmer sein, Text in heller Schrift auf dunklem Hintergrund zu lesen, insbesondere bei geringerer Helligkeit am Bildschirm. Es ist wichtig, die Helligkeit des Bildschirms anzupassen und die persönlichen Vorlieben zu berücksichtigen, um die Augenbelastung zu reduzieren.

## Genesis Market: Seid Ihr auch betroffen?



**Die Polizei hat die kriminelle Online-Plattform „Genesis Market“ stillgelegt: Hier haben Cyberkriminelle sensible persönliche Daten für illegale Geschäfte gesammelt und verkauft. Nicht nur Passwörter und Zugangsdaten, sondern auch Session Cookies. Ihr solltet überprüfen, ob Ihr betroffen seid.**

Durch eine enge Zusammenarbeit internationaler Cybercrime-Behörden bei FBI, BKA, der niederländischen „National High Tech Crime Unit“ (NHTCU), dem Europäischen Polizeiamt (Europol) und weiteren Stellen ist es gelungen, die Verkaufsplattform „Genesis Market“ stillzulegen und 119 Täterinnen und Täter festzunehmen. Sei 2018 haben Cyberkriminelle hier von arglosen Opfern gestohlene Zugangsdaten zu E-Commerce-Plattformen und Online-Zahlungsdiensten gesammelt und verkauft. Ein enormes Sicherheitsrisiko für alle Betroffenen.

**Nicht nur Passwörter erbeutet, auch „Session Cookies“**

Ungewöhnlich an der Vorgehensweise bei „Genesis Market“ ist, dass die Bande nicht nur Passwörter gesammelt und verkauft, sondern auch sogenannte „Session Cookies“ erbeutet hat. Das sind während eines Onlinevorgangs auf dem eigenen Rechner oder Smartphone hinterlegte Dateien (Cookies), die nach einem erfolgreichen Login-Vorgang automatisch angelegt werden. Wer darüber verfügt, kann sich für eine gewisse Zeit auch ohne Passwort oder Zwei-Faktor-Authentifizierung direkt bei Onlinediensten anmelden – was für die Betroffenen ein hohes Sicherheitsrisiko darstellen.

Session Cookies sind kleine Textdateien, die von einer Webseite auf dem Computer des Benutzers während einer Sitzung gespeichert werden. Eine Sitzung bezieht sich auf den Zeitraum, in dem der Benutzer die Webseite besucht und aktiv damit interagiert. Die Session Cookies werden automatisch gelöscht, sobald der Benutzer die Sitzung beendet und den Webbrowser schließt.



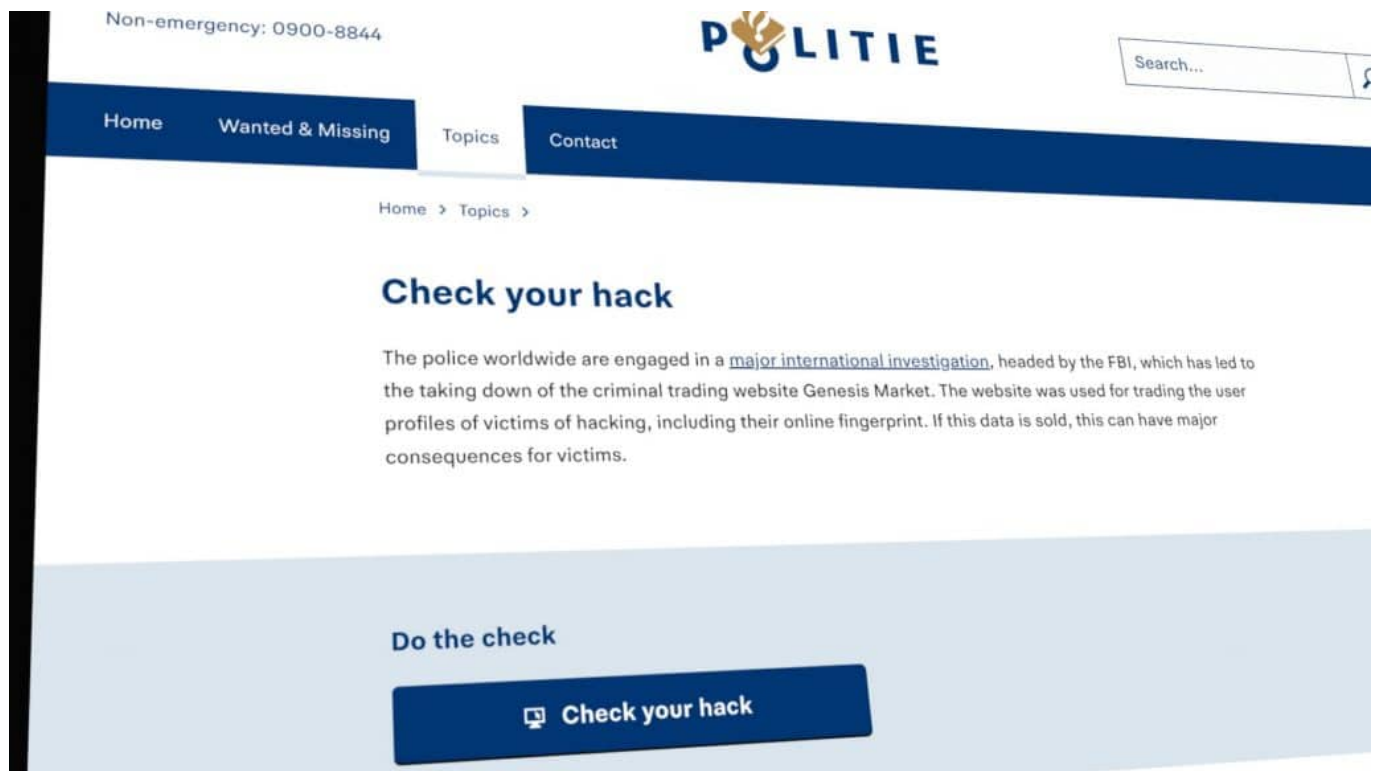
## *Hacker nutzen erbeutete Daten für kriminelle Aktivitäten*

Session Cookies werden verwendet, um Informationen über die Sitzung des Benutzers zu speichern, wie z.B. den Inhalt des Warenkorbs in einem Online-Shop oder die Anmeldedaten des Benutzers während der Sitzung. Dadurch müssen Benutzer nicht bei jeder Interaktion auf der Webseite erneut ihre Anmeldedaten eingeben oder den Inhalt ihres Warenkorbs erneut hinzufügen. Die Verwendung von Session Cookies erleichtert die Benutzererfahrung und reduziert die Notwendigkeit, wiederholte Eingaben zu tätigen.

Da Session Cookies nur temporär gespeichert und automatisch gelöscht werden, sobald der Benutzer die Sitzung beendet, sind sie in der Regel sicherer als persistente Cookies, die auf dem Computer des Benutzers gespeichert bleiben und möglicherweise längerfristig Informationen sammeln können.

Doch genau diese Session Cookies wurden durch eingeschleuste Malware abgegriffen und gesammelt. Cyberkriminelle können so auf Kosten der Opfer einkaufen, Geld abheben oder Identitätsdiebstahl betreiben. Die [niederländische Polizei hat eine Onlinesite](#) eingerichtet, auf der jeder nachschauen kann, ob er

sie ganz persönlich betroffen ist und in den Datenbanken von „Genesis Market“ auftaucht. Es reicht, dort die eigene Mail-Adresse einzugeben. Auf der Webseite erscheinen keinerlei Informationen, um den Datenschutz zu gewährleisten. Wer tatsächlich betroffen ist, erhält nach der Anfrage eine E-Mail der Behörde mit entsprechenden Informationen.



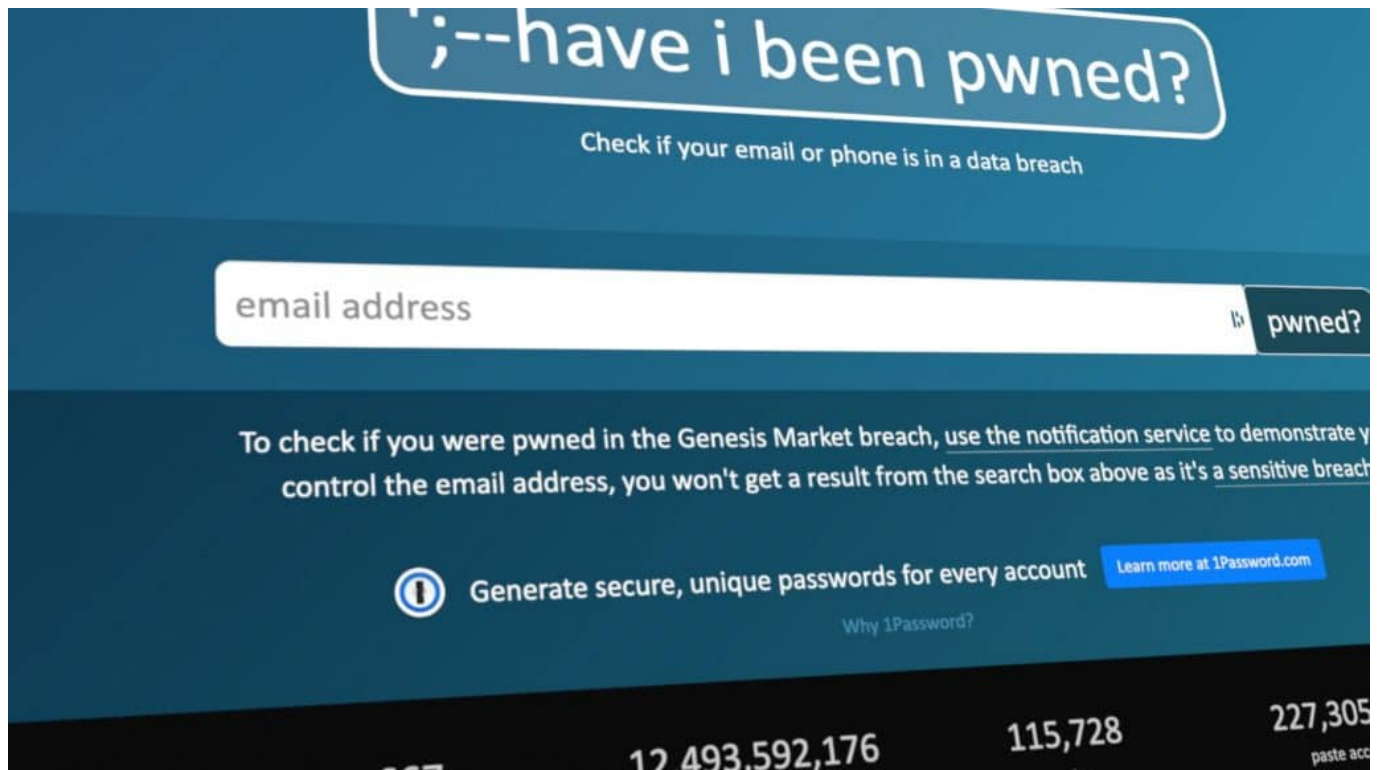
*Niederländische Polizei bietet einen Service an: Bin ich betroffen?*

## Überprüfen: Schon mal gehackt worden?

BKA und Europol empfehlen zudem, auch Online-Angebote wie „Have I been pwned“ zu verwenden. Wer hier seine E-Mail-Adresse eingibt, erfährt sofort, ob persönliche Daten wie Name, Adresse, E-Mail-Adresse, Geburtsdatum, Telefonnummer oder Passwörter in bereits in kriminellen Darknet-Foren aufgetaucht sind. Die Webseite sammelt durch „Breaches“ (unbefugter Zugriff auf sensible Daten) erbeutete Daten.

[haveibeenpwned.com](https://haveibeenpwned.com) kann bedenkenlos genutzt werden: Das weltweit angesehene Angebot wird von einem IT-Sicherheitsexperten betrieben. Die Daten werden auch von vielen Spezialprogrammen genutzt wie Passwort-Manager oder Browsern.

Sollten die eigenen Zugangsdaten bei haveibeenpwned.com auftauchen, empfiehlt es sich, die eigenen Zugangsdaten genau zu prüfen. Ggf. ist es zu empfehlen, in den betroffenen Onlinediensten (das Angebot sagt einem, welche es sind) das Passwort zu ändern – ebenso überall dort, wo dasselbe Passwort verwendet wurde/wird. Das sollte zwar niemand machen, aber die Praxis zeigt, dass viele Menschen aus Bequemlichkeit dennoch dasselbe Passwort an mehreren Stellen einsetzen.



*Have I been Pwned: Die beste Webseite, um herauszufinden, ob eigene Daten im Darknet kursieren*

## Phishing-Schutz im Browser aktivieren

Sollte die eigene Mobilfunknummer in einem Breach auftauchen, ist erhöhte Vorsicht angebracht: Cyberkriminelle kennen dann den Namen und die Mobilfunknummer und können gezielt SMS-Nachrichten oder Whatsapp-Nachrichten verschicken, in denen sie einen sogar mit Namen ansprechen. Das wirkt authentisch und birgt die Gefahr, auf eine manipulierte Webseite (Phishing) geleitet zu werden. Dort wiederum könnten dann erneut sensible Zugangsdaten abgegriffen werden.

Last not least sei empfohlen, einen modernen Browser zu verwenden (unbedingt

durch Updates aktuell halten) und dort den Phishing-Schutz zu aktivieren. Dazu muss ggf. in den Einstellungen unter „Datensicherheit“ das „sichere Browsen“ aktiviert werden (oder ähnlich genannte Funktion). Vorteil: Landet man mit dem Browser auf einer Fake-Webseite, die bereits für Phishing-Angriffe bekannt ist, erhält man eine gut sichtbare Warnung – und kann so nicht mehr verleitet werden, sensible Daten einzugeben.

?



## BKA warnt erneut vor Enkeltrick: Schaden enorm



**Das Bundeskriminalamt legt Zahlen vor: Der Enkeltrick - meist per WhatsApp und Co. angewandt -, funktioniert erstaunlich gut. WhatsApp-Nutzer sollten grundsätzlich vorsichtig sein.**

Als Autor eines unterhaltsamen Techblogs möchte ich heute über eine ernsthafte Angelegenheit sprechen, die viele Menschen betrifft: den Enkeltrickbetrug. Das Bundeskriminalamt warnt vor einer neuen Variante dieses Betrugs, die über Messenger-Apps wie WhatsApp und Co. durchgeführt wird.

Beim Enkeltrick geben sich Betrüger als Verwandte oder Bekannte aus und bitten um Geld. Sie behaupten, in einer Notlage zu sein und dringend finanzielle Hilfe zu benötigen. In der neuen Variante des Enkeltricks nutzen die Betrüger Messenger-Apps, um ihre Opfer zu kontaktieren. Sie geben sich dabei als vertraute Kontakte aus und nutzen das Vertrauen ihrer Opfer, um sie dazu zu bringen, Geld zu überweisen.



## Betrüger nutzen oft gestohlene Profile

Die Betrüger nutzen dabei oft gestohlene Profile und greifen auf persönliche Informationen zurück, die sie über soziale Netzwerke und andere Online-Quellen gesammelt haben. Sie verwenden oft auch eine ähnliche Sprache und Ausdrucksweise wie die vertrauten Kontakte, um ihre Opfer zu täuschen.

Um sich vor dem Enkeltrick zu schützen, gibt es einige wichtige Schritte, die man beachten sollte. Man sollte immer misstrauisch sein, wenn jemand unerwartet um Geld bittet. Es ist wichtig, die Identität des vermeintlichen Verwandten oder Bekannten zu überprüfen, indem man sie zum Beispiel telefonisch kontaktiert. Es ist auch ratsam, keine persönlichen Informationen preiszugeben und keine Links oder Anhänge von unbekanntem Absendern zu öffnen.

Im Zweifelsfall sollte man sich an die Polizei wenden und den Verdacht auf Betrug melden. Nur so können wir gemeinsam dafür sorgen, dass sich die Betrüger nicht durchsetzen und unschuldige Menschen nicht um ihr Geld gebracht werden.



## Betrüger passen Betrugsmaschen an

Es ist auch wichtig, dass man sich bewusst macht, dass Betrüger ständig neue Methoden entwickeln, um ihre Opfer zu täuschen. Man sollte deshalb immer vorsichtig sein und seine persönlichen Daten und Konten schützen.

Eine weitere Möglichkeit, sich vor Betrug zu schützen, ist die Nutzung von Zwei-Faktor-Authentifizierung. Diese Methode erfordert bei der Anmeldung in ein Konto oder bei der Durchführung einer Transaktion eine zusätzliche Bestätigung, wie zum Beispiel einen Code, der per SMS auf das Mobiltelefon gesendet wird. Dies erschwert es Betrügern erheblich, auf fremde Konten zuzugreifen.

## Updates einspielen!

Auch das Aktualisieren der Software und die Installation von Sicherheitsupdates auf mobilen Geräten und Computern können helfen, Betrug und andere Online-Gefahren zu minimieren.

Insgesamt ist es wichtig, dass man sich bewusst macht, dass der Einzeltrick und andere Betrugsmethoden nicht einfach verschwinden werden. Es ist jedoch möglich, sich durch ein paar einfache Schritte und bewusstes Handeln zu

schützen. Wir alle können dazu beitragen, dass Betrüger nicht erfolgreich sind und Opfer vermieden werden können.

## Elon Musk tauscht Twitter-Logo gegen das der Kryptowährung Dogecoin aus



**Das typische Logo mit weißem Vogel auf blauem Grund ist bei Twitter verschwunden. Stattdessen prangt ein Hundegesicht an der Stelle. Das Logo der Kryptowährung Dogecoin.**

In der Welt der Kryptowährungen gibt es immer wieder Überraschungen. Diesmal ist es Elon Musk, der für Aufsehen sorgt. Der Tech-Milliardär hat sein Twitter-Profilbild gegen das Logo der Kryptowährung Dogecoin ausgetauscht. Dies hat bei vielen Fans der Währung für Begeisterung gesorgt und den Preis der Währung in die Höhe getrieben.

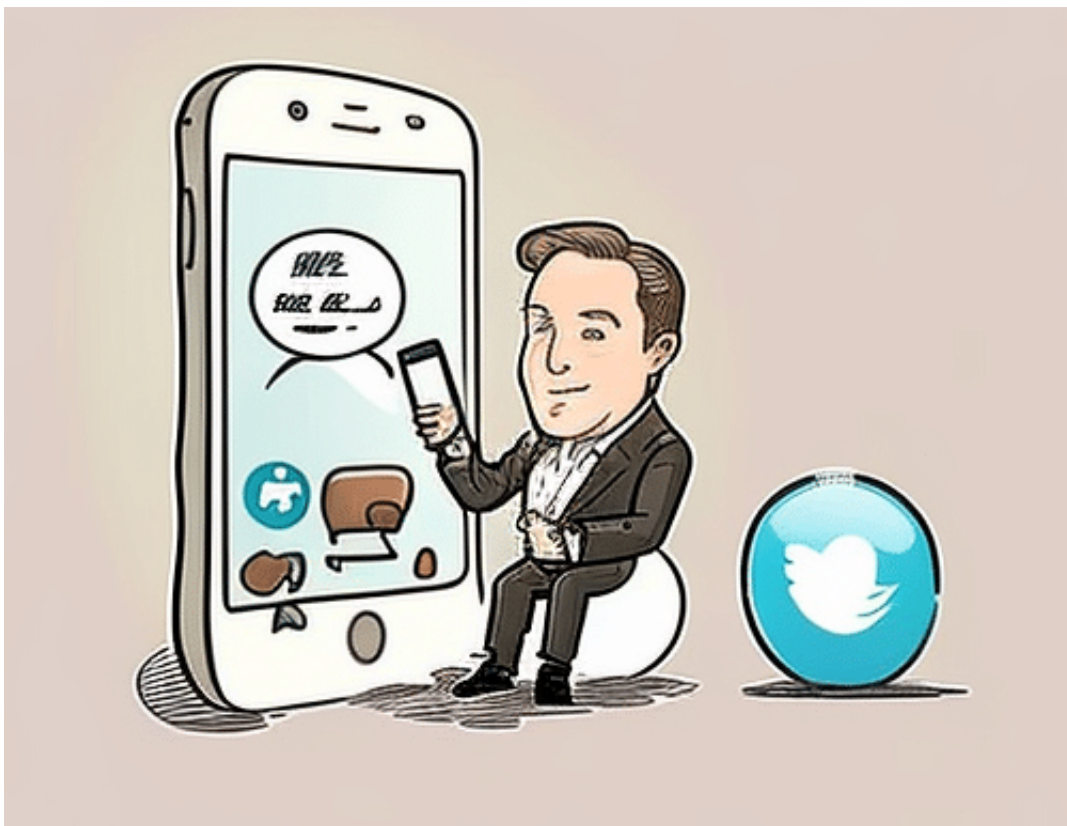
### **Was steckt hinter der Aktion?**

Doch was steckt hinter dieser Aktion? Elon Musk hat in der Vergangenheit bereits mehrfach sein Interesse an Kryptowährungen publik gemacht, sowohl an Bitcoin wie an das sehr viel unbekanntere Dogecoin, dabei aber öfter Dogecoin in den Fokus gerückt. Mit diesem Schritt setzt er ein weiteres Signal und stärkt das

Vertrauen in die Digitalwährung.

Die Reaktionen auf Musks Profilbild-Wechsel waren unterschiedlich. Während einige begeistert waren und in der Aktion eine Bestätigung ihrer eigenen Investitionsentscheidung sahen, gab es auch kritische Stimmen. Denn Musk hat in der Vergangenheit bereits mehrfach durch seine Tweets den Preis von Kryptowährungen beeinflusst und somit auch Spekulationen angeheizt.

In jedem Fall zeigt der Schritt von Elon Musk erneut, dass Kryptowährungen auch von Prominenten als Investmentmöglichkeit ernst genommen werden und in der breiten Öffentlichkeit zunehmend an Bedeutung gewinnen. Es bleibt abzuwarten, welche Auswirkungen die Aktion langfristig haben wird und ob sich Dogecoin als eine ernstzunehmende Kryptowährung etablieren kann.



Elon Musk und

Twitter

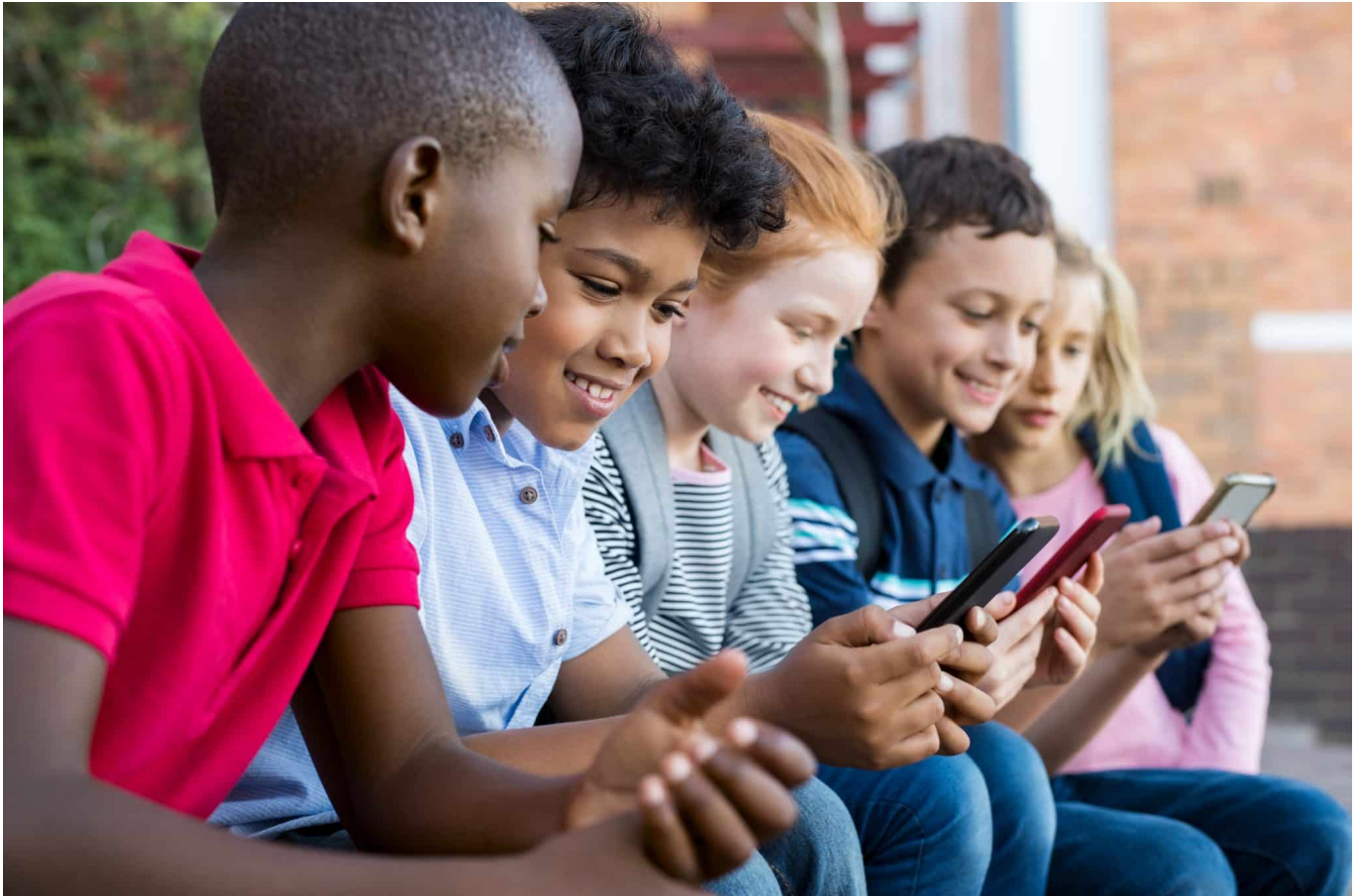
## Was ist Dogecoin

Dodgecoin (DOGE) ist eine Kryptowährung, die ursprünglich als Scherz in Anlehnung an den Internet-Meme "Doge" ins Leben gerufen wurde. Sie basiert auf dem Open-Source-Protokoll von Litecoin und wurde im Jahr 2013 von Billy Markus und Jackson Palmer entwickelt. Anders als Bitcoin, dessen maximale Menge auf 21 Millionen begrenzt ist, gibt es bei Dodgecoin keine Begrenzung der Gesamtmenge.

Dodgecoin ist bekannt für seine schnellen Transaktionszeiten und niedrigen Transaktionsgebühren. Die Währung wird von einer aktiven Community unterstützt, die sich für die Verbreitung und Akzeptanz von Dodgecoin einsetzt. In der Vergangenheit hat die Währung immer wieder durch die Unterstützung von Prominenten wie Elon Musk Aufmerksamkeit erregt und an Wert gewonnen.

Obwohl Dodgecoin als Scherz gestartet wurde, hat es sich im Laufe der Jahre zu einer ernstzunehmenden Kryptowährung entwickelt und wird von vielen Investoren als attraktives Investment betrachtet. Allerdings gibt es auch Bedenken hinsichtlich der Stabilität und Sicherheit von Dodgecoin sowie der Möglichkeit von Marktmanipulationen aufgrund des fehlenden Limits der Gesamtmenge.

## Was sollten Eltern tun - auch die Chats der Kinder lesen?



**Das Smartphone ist heute für die meisten Kinder und Jugendlichen der treueste Begleiter - Tor zur Welt und Schnittstelle zu Freunden. Da sind Eltern versucht, auch mal einen Blick ins Smartphone des Nachwuchs zu werfen. Eine gute Idee?**

Die Mehrheit der Kinder und Jugendlichen nutzt heutzutage eine Vielzahl von Messaging-Apps wie WhatsApp, TikTok, Snapchat und Instagram, um mit Freunden und Familie in Kontakt zu bleiben. Oder auch, um sich zu informieren oder unterhalten. Nicht wenige Eltern sind besorgt, was ihre Kinder wohl online machen - und ob sie sich in einer sicheren Umgebung bewegen. Eine Frage, die sich viele Eltern stellen, ist in diesem Zusammenhang, ob es wohl in Ordnung ist, die Chats ihrer Kinder heimlich zu lesen.

**Auch Kinder haben ein Recht auf Privatsphäre**



Zunächst einmal ist es wichtig zu betonen, dass die Privatsphäre und der Datenschutz von Kindern und Jugendlichen geschützt werden müssen. Auch wenn Eltern besorgt über das Verhalten ihrer Kinder sind, sollten sie sich bewusst sein, dass das heimliche Lesen von Chats eine Verletzung der Privatsphäre ihrer Kinder darstellt. Das Vertrauen zwischen Eltern und Kindern kann dadurch erheblich beeinträchtigt werden (spätestens wenn das rauskommt, dürfte das als sicher gelten).

Darüber hinaus sollten sich Eltern darüber bewusst sein: Auch Kinder und Jugendliche haben ein Recht auf Privatsphäre. Es kann den Minderjährigen durchaus helfen, ein gesundes Verhältnis zu ihren Eltern aufzubauen, wenn sie das Gefühl haben, dass sie ihre eigenen Entscheidungen treffen und ihre eigenen Erfahrungen sammeln können, ohne dabei von den Eltern ständig "überwacht" zu werden. Wenn Eltern nun die Chats des Nachwuchses lesen, kann dazu führen, dass Kinder und Jugendliche das Gefühl haben, dass sie keine Kontrolle über ihre Privatsphäre haben und dass ihre Eltern ihnen nicht vertrauen (was im Prinzip dann auch zutrifft).

Gleichzeitig gibt es ernsthafte Gefahren, über die sich die meisten Kinder nicht bewusst sind. Eine Zwickmühle für Eltern.



## Eltern haben auch eine Aufsichtspflicht

Es ist von entscheidender Bedeutung, dass Eltern sich bewusst sind, dass es sehr wohl Situationen geben kann, in denen es notwendig ist, die Chats ihrer Kinder zu lesen. Zum Beispiel dann, wenn es einen konkreten und begründeten Verdacht auf Mobbing, Cybergrooming oder Cybertroulling gibt. Oder wenn das Kind sich in einer unsicheren Situation befindet und möglicherweise Hilfe benötigt.

In solchen Fällen sollten Eltern jedoch zuerst mit ihren Kindern sprechen und versuchen, die Situation gemeinsam zu lösen.

Eine Möglichkeit, die Privatsphäre von Kindern und Jugendlichen zu schützen, aber gleichzeitig dafür zu sorgen, dass sie sicher online sind, ist die Verwendung von Überwachungs-Software wie die [Schutz.Software von Kaspersky](#). Solche Software kann helfen, die Aktivitäten von Kindern und Jugendlichen im Internet zu überwachen, ohne dabei ihre Privatsphäre zu verletzen. Eltern können auf diese Weise sicherstellen, dass ihre Kinder sicher im Internet surfen und dass sie nicht Opfer von Mobbing oder anderen Online-Gefahren werden.

Eine weitere Möglichkeit und noch viel bessere Möglichkeit, das Vertrauen zwischen Eltern und Kindern zu stärken und eine offene Kommunikation zu fördern, ist die Etablierung klarer Regeln und Richtlinien für die Nutzung von Messaging-Apps und anderen Online-Tools. Eltern können mit ihren Kindern gemeinsam Regeln aufstellen, die sicherstellen, dass sie verantwortungsbewusst und sicher im Internet unterwegs sind.

## Am wichtigsten: offene Kommunikation

Insgesamt ist es wichtig, dass Eltern und Kinder offen miteinander kommunizieren und gemeinsam Regeln aufstellen, um sicherzustellen, dass Kinder und Jugendliche in einer sicheren Umgebung im Internet unterwegs sind. Eltern sollten sich bewusst sein, dass das heimliche Lesen von Chats eine Verletzung der Privatsphäre ihrer Kinder darstellt und dass sie sich auf Überwachungs-Software und klare Regeln verlassen sollten, um sicherzustellen, dass ihre Kinder sicher online sind.

Darüber hinaus sollten Eltern ihre Kinder über die Risiken und Gefahren aufklären, die mit der Nutzung von Messaging-Apps verbunden sind. Dazu gehört beispielsweise das Risiko von Cyber-Mobbing, das Risiko von Kontakt mit

Fremden oder das Risiko, dass private Informationen oder Bilder ungewollt geteilt werden. Wenn Kinder und Jugendliche sich dieser Risiken bewusst sind, können sie besser darauf vorbereitet sein und verantwortungsvoll handeln.

Es ist auch wichtig, dass Eltern respektvoll mit den Online-Aktivitäten ihrer Kinder umgehen. Es ist wichtig, dass Kinder und Jugendliche das Gefühl haben, dass ihre Eltern ihnen vertrauen und sie unterstützen. Wenn Eltern das Vertrauen ihrer Kinder gewinnen können, werden diese wahrscheinlich offener darüber sprechen, was sie im Internet tun und welche Probleme oder Bedenken sie haben.



## **Am besten gemeinsam besprechen**

Schließlich ist es wichtig, dass Eltern die Privatsphäre ihrer Kinder respektieren und ihnen das Gefühl geben, dass sie unabhängig sind. Das bedeutet, dass Eltern die Chats ihrer Kinder nur dann lesen sollten, wenn es wirklich notwendig ist und dass sie ihre Kinder darüber informieren sollten, wenn sie dies tun. Wenn Kinder das Gefühl haben, dass ihre Privatsphäre respektiert wird, werden sie eher offen über ihre Online-Aktivitäten sprechen und sich sicherer fühlen.

Insgesamt ist es wichtig, dass Eltern und Kinder offen und ehrlich miteinander kommunizieren und ein gesundes Vertrauensverhältnis aufbauen. Eltern sollten sich bewusst sein, dass das Lesen von Chats eine Verletzung der Privatsphäre ihrer Kinder darstellt, aber dass es Situationen geben kann, in denen dies notwendig ist, um die Sicherheit ihrer Kinder zu gewährleisten. Durch klare Regeln, Überwachungssoftware und eine offene Kommunikation können Eltern sicherstellen, dass ihre Kinder sicher im Internet unterwegs sind und sich gleichzeitig unabhängig und respektiert fühlen.

## Handel mit Rohstoffen: Welche Auswirkungen hat das Spekulieren auf unser Leben?



**Heute kann auf alles spekuliert werden, nicht nur auf steigende oder fallende Aktienkurse oder Devisen, sondern auch auf Rohstoffpreise. Doch welche Auswirkungen hat diese Spekulation auf unser Leben?**

Der Handel mit Rohstoffen ist ein wichtiger Bestandteil unserer Wirtschaft und kann große Auswirkungen auf unser Leben haben. Spekulationen auf dem Rohstoffmarkt können Preise in die Höhe treiben und somit die Preise für alltägliche Dinge beeinflussen.

### **Was sind Rohstoffe?**

Rohstoffe sind die Grundlage für viele Produkte, die wir täglich nutzen. Sie sind natürliche Ressourcen, die aus der Erde gewonnen werden, wie zum Beispiel Öl, Gas, Holz, Metalle und Mineralien. Rohstoffe sind unverzichtbar für die Wirtschaft

und den Handel, da sie als Ausgangsmaterial für die Produktion von Waren dienen.

Rohstoffe sind von großer Bedeutung für die Wirtschaft und den Alltag. Ohne sie könnten wir nicht leben, denn sie dienen als Grundlage für die Produktion von Gütern und Dienstleistungen. Sie sind also ein wichtiger Faktor für die Wertschöpfungskette.

Einige Rohstoffe wie Erdöl, Kohle oder Gas werden als [fossile Brennstoffe](#) genutzt, um Energie zu erzeugen. Andere Rohstoffe wie Metalle oder Mineralien werden in der Industrie zur Herstellung von Maschinen, Elektronikgeräten oder Baustoffen verwendet.

Die Verfügbarkeit und der Preis von Rohstoffen haben großen Einfluss auf die Wirtschaft. Wenn es Engpässe bei der Versorgung mit bestimmten Rohstoffen gibt, kann dies zu Produktionsausfällen führen und somit auch die Preise für Endprodukte beeinflussen.

Doch nicht nur wirtschaftliche Aspekte spielen eine Rolle: Auch Umwelt- und Sozialstandards bei der Gewinnung von Rohstoffen sind wichtig. Eine nachhaltige Nutzung von Ressourcen ist notwendig, um zukünftigen Generationen eine intakte Umwelt zu hinterlassen.

Insgesamt lässt sich sagen, dass Rohstoffe unverzichtbar für unsere Gesellschaft sind. Es ist daher wichtig, einen verantwortungsvollen Umgang mit ihnen zu pflegen und Alternativen zu entwickeln, um ihre Nutzung nachhaltiger zu gestalten.



*Rohstoffe müssen meist mit enormen Aufwand gefördert werden*

## **Wie funktioniert der Handel mit Rohstoffen?**

Wenn man über Rohstoffe spricht, denkt man oft an Gold, Silber oder Öl. Aber es gibt noch viele andere Rohstoffe, die gehandelt werden können, wie zum Beispiel Kupfer, Zink oder Baumwolle. Der Handel mit Rohstoffen kann auf verschiedene Arten erfolgen, aber der bekannteste Weg ist der Handel an der Börse. Hier werden Rohstoffe in Form von Futures oder Optionen gehandelt.

Dabei geht es nicht um den physischen Handel mit den Rohstoffen, sondern um den Handel mit Verträgen, die den Kauf oder Verkauf des Rohstoffs zu einem bestimmten Preis zu einem bestimmten Zeitpunkt ermöglichen. Spekulanten können auf diese Weise auf steigende oder fallende Preise setzen und so Gewinne erzielen. Allerdings kann das Spekulieren auch negative Auswirkungen haben, wie zum Beispiel Preisschwankungen, die sich auf die Verbraucherpreise auswirken können. Es ist wichtig, dass der Handel mit Rohstoffen transparent und reguliert ist, um solche Auswirkungen zu minimieren.

Der Handel mit Rohstoffen hat sich in den letzten Jahren sehr verändert, da es durch die vielen digitalen Neuheiten immer wieder neue Möglichkeiten gibt den Handel zu verändern und in vielen Fällen sogar zu vereinfachen: Durch automatisierte Handelsroboter wie "Oil Profit", zu finden bei <https://www.business2community.com/de/kryptowaehrung/oel-profit-erfahrungen>, kann das Handeln ganz oder teilweise automatisiert werden und so mit einigen Handgriffen vielversprechende Erfolge zeigen.

Man muss sich allerdings auch bei solchen Produkten im Klaren sein, dass es immer Risiken geben kann. Man sollte Spekulationen nicht mit sicheren Anlagemöglichkeiten vertauschen.

## Welche Faktoren beeinflussen den Preis von Rohstoffen?

Die Preise von Rohstoffen werden in erster Linie durch das Verhältnis von Angebot und Nachfrage bestimmt. Wenn die Nachfrage nach einem bestimmten Rohstoff hoch ist, steigt der Preis, da das Angebot begrenzt ist. Umgekehrt sinkt der Preis, wenn die Nachfrage geringer ist als das Angebot.

Ein Beispiel dafür ist der Ölmarkt. Die weltweite Nachfrage nach Öl ist sehr hoch, da es eine wichtige Energiequelle für viele Branchen und Länder ist. Gleichzeitig gibt es jedoch nur begrenzte Vorkommen an Öl auf der Erde. Wenn also das Angebot knapp wird, steigt der Preis für Öl.

Auch politische Ereignisse können die Nachfrage nach Rohstoffen beeinflussen und somit den Preis verändern. Zum Beispiel kann ein Konflikt in einem wichtigen Förderland zu einer Verknappung des Angebots führen und somit den Preis erhöhen.

Zusätzlich können auch Wetterbedingungen oder Naturkatastrophen die Verfügbarkeit von Rohstoffen beeinträchtigen und somit den Preis beeinflussen. Wenn beispielsweise eine Dürreperiode die Ernte von Getreide einschränkt, kann dies zu einer Verknappung des Angebots führen und den Preis erhöhen.

Insgesamt sind Angebot und Nachfrage also entscheidende Faktoren für den Preis von Rohstoffen. Es lohnt sich daher, diese Faktoren im Auge zu behalten,



um mögliche Entwicklungen auf dem Markt frühzeitig erkennen zu können.

## **Regulationen der Rohstoff-Spekulationen**

Die Finanzaufsicht wird jeweils selber von den jeweiligen Ländern geregelt, ebenso gibt es verschiedene Finanzaufsichten auf europäischer Ebene. Es gibt keinen weltweit verbindlichen Rahmen, allerdings gibt es viele Organisationen und Verbindungen, die versuchen, Einigkeit auf internationalen Märkten herzustellen.

Bei dem Handeln mit Rohstoffen ist hierbei auf internationaler Ebene unter anderem die Internationale Organisation der Wertpapieraufsichtsbehörden, kurz IOSCO, zuständig.

## Teams: Bessere Sichtbarkeit sicherstellen



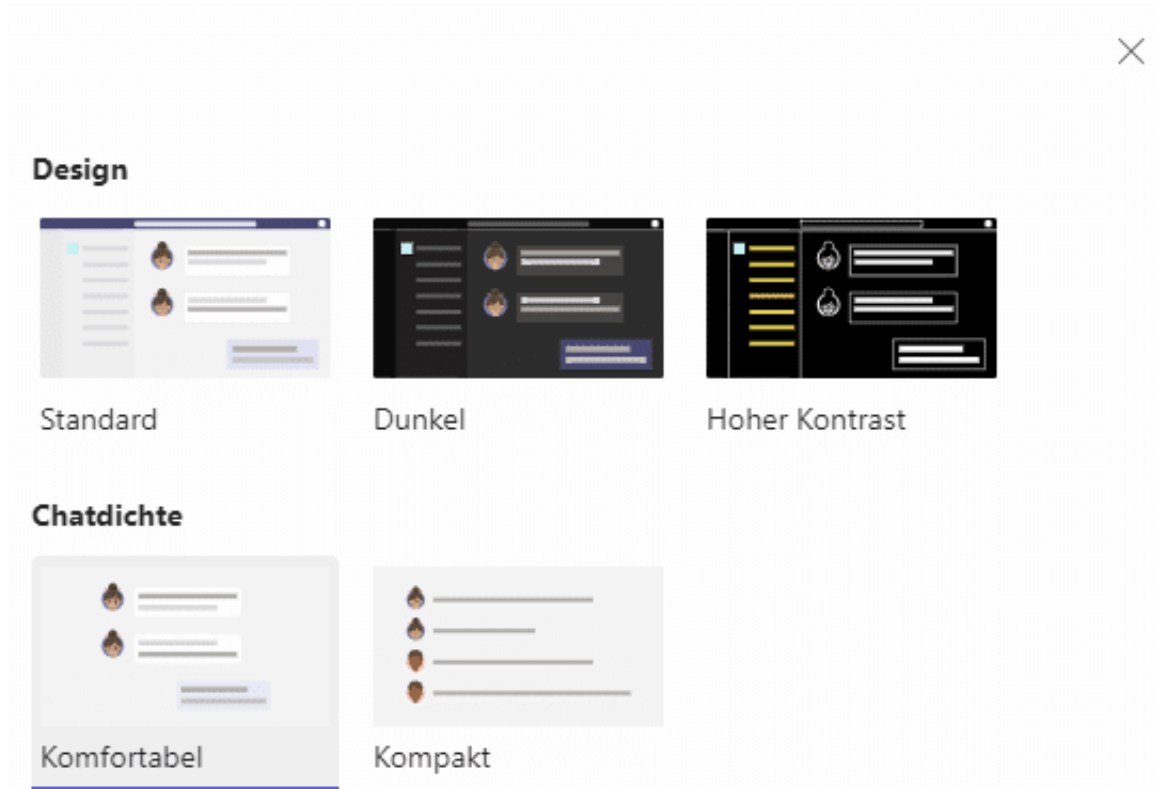
Wenn Ihr Teams verwendet, dann müsst Ihr Euch auf das verlassen, was Ihr seht. Wenn Ihr aber ein eingeschränktes Sehvermögen habt, dann kann das zur Herausforderung werden. Nutzt dafür die in Teams versteckten Mittel!

### Design des Chats anpassen

Neben dem Video ist der Haupt-Kommunikationskanal in Teams der Chat. Wie bei einem Messenger könnt Ihr mit anderen Anwendern, in einem Termin oder in direktem Gespräch Nachrichten austauschen, Dokumente anhängen etc. Das sollte aber dann auch so dargestellt werden, dass Ihr die Nachrichten optimal sehen könnt. Hier erlaubt Teams einige Einstellungen, die Euch da helfen können:

- Klickt in Teams auf die **drei Punkte** neben eurem Kontobild.
- Klickt im Menü auf **Einstellungen**.
- Unter **Allgemein** findet Ihr diverse Einstellungen, die die Darstellung des Chats beeinflussen.
- Unter **Design** stellt Ihr den Kontrast des Chats ein: **Hell** und **Dunkel** entsprechen dem hellen und dem dunklen Thema von Windows. Wenn Ihr Probleme habt, die Texte gut erkennen zu können, dann schaltet stattdessen **Hoher Kontrast** ein. Dadurch geben sich die Texte besser vom Hintergrund ab und sind somit leichter zu erkennen.

- Unter **Chatdichte** könnt Ihr den Abstand zwischen einzelnen Nachrichten erhöhen. Der Vorteil ist, dass Eure Augen sich weniger anstrengen müssen, um den Text lesen zu können.




## Untertitel und Gebärdensprache

Bei immer mehr Videokonferenzen werden auch Gebärdendolmetscher eingesetzt. Normalerweise ordnet Teams die Bilder der Sprechenden nach eigenen Algorithmen an, abhängig von den Gesprächsbeiträgen und anderen Faktoren. Da macht es Sinn, wenn diese Personen auch sichtbar sind. Das könnt Ihr in Teams automatisiert machen lassen:

- Klickt in Teams auf die **drei Punkte** neben eurem Kontobild.
- Klickt im Menü auf **Einstellungen**.
- Klickt links auf **Zugänglichkeit**.
- Aktiviert **In Besprechungen auf meinem Bildschirms Signer\*innen priorisieren**.
- Die Schaltfläche **Signer\*innen verwalten** wird erst dann aktiv. Klickt darauf, dann wählt Personen aus, die diese Rolle innehaben, indem Ihr deren Namen eingibt und sie aus der Ergebnisliste auswählt.

- Nimmt eine dieser Personen an einer Besprechung teil, dann wird sie auf Eurem Bildschirm priorisiert dargestellt.



### Gebärdensprache

In Besprechungen auf meinem Bildschirm Signer\*innen priorisieren

[Signer\\*innen verwalten](#)

### Untertitel

In meinen Besprechungen immer Untertitel anzeigen

### Anzeige

Animationen deaktivieren (erfordert Neustart von Teams)

- Zusätzlich könnt Ihr **In meinen Besprechungen immer Untertitel anzeigen** eine Transkription aktivieren, die den gesprochenen Text verschriftlicht.
- Wenn Euch die Animationen in Teams irritieren, dann schaltet **Animationen deaktivieren** ein. Danach müsst Ihr dann Teams einmal neu starten.

## Word: Zeit sparen durch Wortersetzungen



**Textverarbeitung ist eine Aufgabe, die meist wenig Spaß macht. Je mehr Ihr Euch helfen lassen könnt, desto schneller seid Ihr fertig. Wir zeigen Euch einige Hilfsmittel, die Word direkt mitbringt.**

### **Text unterteilen durch automatische Linien**

Text wird oft im Rahmen der normalen Formatierungs- und Strukturierungsoptionen von Word unterteilt: Ihr ordnet ihn in Kapitel und Unterkapitel ein, verwendet Aufzählungen und [Tabellen](#). Eine viel einfachere Unterteilung von Textpassagen nutzt Ihr eher selten: Die waagerechten Striche. Das liegt vor allem daran, dass diese nicht ganz so einfach zu erzeugen sind. Niemand möchte gerne so oft hintereinander die Minus- oder Unterstrich-Taste drücken, bis der daraus entstehende Strich über die komplette Breite des Bildschirms geht. Müsst Ihr aber auch nicht:

- An einer beliebigen Stelle des Word-Dokumentes - sinnvollerweise am Anfang einer Zeile - gebt dreimal hintereinander das Zeichen für die Linienart ein, dann drückt die Eingabetaste.
- [Word](#) wandelt die drei eingegebenen Zeichen dann in eine die Seitenbreite ausfüllende Linie um. Als Zeichen verwendet:
  - -, um eine dünne, durchgezogene Linie
  - \_, um eine fette durchgezogene Linie
  - \*, um eine gepunktete Linie oder
  - #, um eine dreifache, fette Linie einzufügen.

---

==

\*\*\*

###



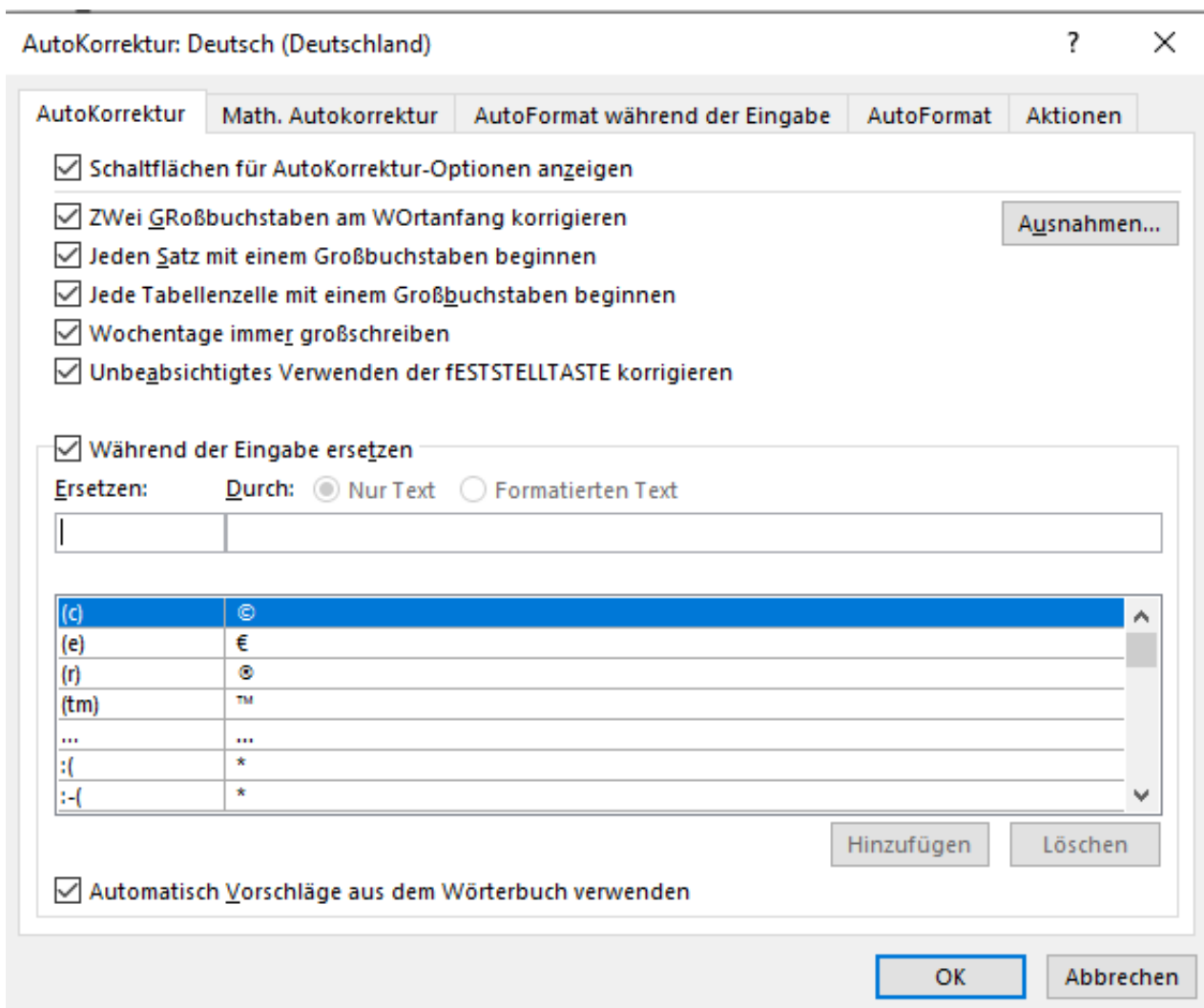
## Abkürzungen durch Autokorrektur

Was bei Strichen möglich ist, das könnt Ihr mit Begriffen und Abkürzungen genauso machen: Gebt einen Kurztext ein, Word ersetzt diesen auf Wunsch dann durch den vollständigen Text. Beispielsweise kann so aus "mfg" automatisch "Mit freundlichen Grüßen" werden. Das Tolle dabei: Die Ersetzungen könnt Ihr frei selbst festlegen!

- Klickt in einem [Word](#)-Dokument auf **Datei > Optionen**.
- Klickt dann in der Leiste links auf **Dokumentprüfung**.
- Klickt dann auf die Schaltfläche **Autokorrektur-Optionen**.
- Stellt sicher, dass der Haken bei **Während der Eingabe ersetzen** gesetzt ist.
- In der Tabelle im unteren Teil des Bildschirms seht Ihr die Ersetzungen,

die Word bereits automatisch vornimmt.

- Gebt jetzt über der Tabelle in das linke Feld die Abkürzung ein, in das rechte Feld den Text, den Word dann stattdessen in das Dokument einfügen soll.
- Durch einen Klick auf Hinzufügen wird die Abkürzung aufgenommen und ist ab sofort aktiv.
- Wenn Ihr die Ersetzung weder deaktivieren wollt, dann sucht sie in der Tabelle heraus, klickt sie an und klickt dann auf **Löschen**.



die so festgelegten automatischen Ersetzungen werden von Word während des Tippens automatisch vorgenommen, Ihr müsst nichts mehr tun: Gebt am Beispiel "mfg" ein, sobald Ihr die Leertaste oder ein Satzzeichen tippt, wird daraus automatisch "Mit freundlichen Grüßen".

## Easter Eggs: Versteckte Funktionen und Überraschungen in Games, Software und online



**Osteier suchen hat Tradition. Aber auch Easter Eggs haben Tradition: Versteckte Funktionen oder Überraschungen in Software, Games, Onlinediensten oder sogar in Filmen.**

Easter Eggs in Games und Software beziehen sich auf versteckte Nachrichten, Funktionen, Witze oder Referenzen, die von Entwicklern als Überraschung für die Nutzer eingebaut wurden. Der Begriff "Easter Egg" leitet sich von der Tradition ab, zu Ostern bunt bemalte Eier zu verstecken, die Kinder dann suchen und finden sollen. In diesem Zusammenhang bedeutet es, dass die Entwickler etwas Verborgenes in ihrer Software oder ihrem Spiel "versteckt" haben, das die Nutzer entdecken können.

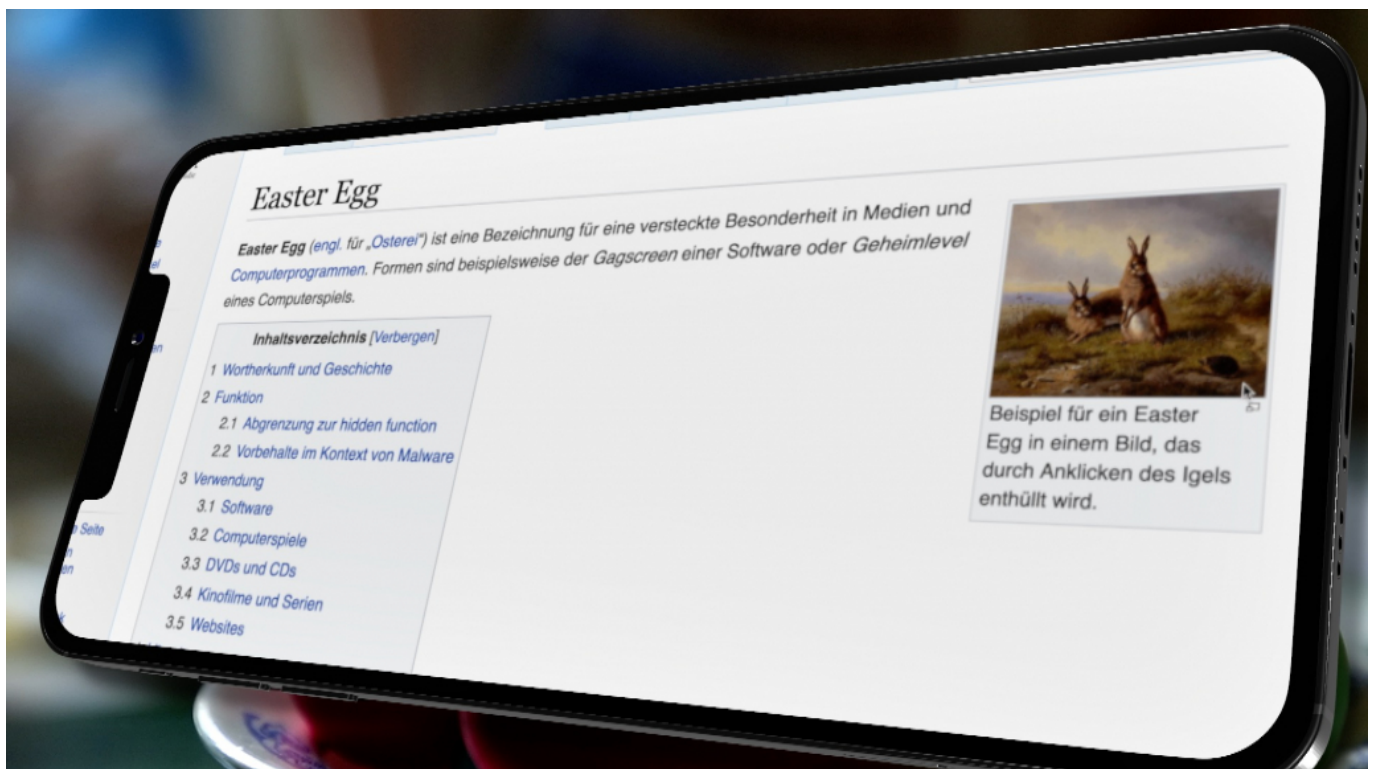
### **Die ersten Easter Eggs bereits in den 1970er Jahren in Games**

Die Tradition der Easter Eggs begann in den 1970er Jahren, als der Videospiel-



Entwickler Warren Robinett ein verstecktes Easter Egg in seinem Spiel "Adventure" für die Atari 2600-Spielkonsole einbaute. Zu dieser Zeit erhielten Entwickler keine Anerkennung für ihre Arbeit an Spielen, und Robinett wollte sicherstellen, dass sein Name irgendwie mit seinem Spiel in Verbindung gebracht wurde. Daher schuf er einen geheimen Raum im Spiel, der nur durch eine bestimmte Abfolge von Aktionen zugänglich war. In diesem Raum war die Nachricht "Created by Warren Robinett" zu sehen.

Seitdem haben zahlreiche Entwickler Easter Eggs in ihren Spielen und Softwareanwendungen eingebaut, oft als humorvolle oder kulturelle Referenzen. Einige Easter Eggs dienen lediglich als Gag oder Scherz, während andere nützliche Funktionen oder versteckte Spielmodi freischalten. Oftmals sind Easter Eggs eine Art, die Kreativität der Entwickler zum Ausdruck zu bringen und die Spieler oder Nutzer zu belohnen, die Zeit und Mühe darauf verwenden, das Spiel oder die Software gründlich zu erkunden.



*Easter Egg im Wikipedia Eintrag*

## Der Reiz des Unbekannten

Der Reiz von Easter Eggs liegt in der Entdeckung des Unerwarteten und dem Gefühl der Belohnung, das damit einhergeht. Sie tragen auch zur Community-

Bildung bei, da Spieler und Nutzer ihre Entdeckungen teilen und diskutieren, um weitere Easter Eggs aufzudecken. In vielen Fällen sind Easter Eggs eine Hommage an die Entwickler, die ihre persönlichen Interessen oder Vorlieben in ihre Arbeit einfließen lassen.

Im Laufe der Jahre haben Easter Eggs auch in der Film- und Fernsehindustrie an Popularität gewonnen. Regisseure und Drehbuchautoren verstecken oft Anspielungen oder Referenzen zu anderen Werken, realen Ereignissen oder kulturellen Phänomenen, um aufmerksame Zuschauer zu überraschen und zu erfreuen.

Die Popularität von Easter Eggs zeigt, dass diese Tradition einen wichtigen kulturellen Aspekt in der Unterhaltungsindustrie darstellt. Sie bieten den Schöpfern die Möglichkeit, ihre Persönlichkeit und Kreativität in ihrer Arbeit auszudrücken, während sie gleichzeitig eine enge Bindung zu ihrem Publikum schaffen.

## **Easter Eggs als Marketinginstrument**

Manchmal werden Easter Eggs auch als Marketinginstrument eingesetzt, um das Interesse der Nutzer an einem Produkt oder einer Marke zu wecken. Indem Easter Eggs in einem Spiel oder einer Software versteckt werden, können Unternehmen das Interesse der Nutzer länger aufrechterhalten und das Engagement steigern. Dies kann dazu führen, dass die Spieler das Spiel länger spielen oder die Software häufiger nutzen, was letztendlich zum Erfolg des Produkts beiträgt.

In einigen Fällen können Easter Eggs jedoch auch kontrovers sein, insbesondere wenn sie unangemessene Inhalte enthalten oder als unlauterer Wettbewerb angesehen werden. Daher ist es wichtig, dass Entwickler bei der Verwendung von Easter Eggs die potenziellen Auswirkungen auf ihre Zielgruppe und das Gesamterlebnis der Nutzer berücksichtigen.

Insgesamt sind Easter Eggs ein interessantes und unterhaltsames Phänomen, das zeigt, wie Kreativität und Entdeckungsfreude in verschiedenen Bereichen der Unterhaltungsindustrie zum Ausdruck kommen können. Sie bieten sowohl den Schöpfern als auch den Konsumenten eine einzigartige Möglichkeit, ihre Leidenschaft und Hingabe an ihre Arbeit oder ihr Hobby zu teilen und gleichzeitig die Magie des Entdeckens und Erkundens zu erleben.



*Namen der Entwickler in einem modernen Video Game*

## **Easter Eggs haben sich weiter entwickelt**

Easter Eggs haben sich im Laufe der Jahre weiterentwickelt und sind in verschiedenen Formen in unterschiedlichen Medien aufgetaucht. In der heutigen Zeit sind Easter Eggs nicht nur auf Spiele und Software beschränkt, sondern finden sich auch in Websites, Apps und sogar Hardware-Geräten. Sie haben sich zu einem wichtigen Bestandteil der Popkultur entwickelt und spiegeln oft Trends, Humor und Interessen einer bestimmten Zeit wider.

Mit der Weiterentwicklung von Technologien und der zunehmenden Vernetzung der digitalen Welt werden Easter Eggs immer raffinierter und vielfältiger. Sie reichen von komplexen Rätseln, die in virtuellen Welten versteckt sind und nur durch Zusammenarbeit gelöst werden können, bis hin zu subtilen visuellen oder akustischen Hinweisen, die auf andere kulturelle Ereignisse oder Phänomene verweisen.

Ein gutes Beispiel für die Evolution von Easter Eggs ist die Entstehung von Alternate Reality Games (ARGs), bei denen Rätsel und versteckte Hinweise in verschiedenen Medien und Plattformen eingebettet sind. Die Spieler müssen diese Hinweise finden und miteinander verknüpfen, um das gesamte Rätsel zu

lösen und eine zugrunde liegende Geschichte oder Belohnung freizuschalten.

## Easter Eggs bilden Communities

Easter Eggs können auch zur Bildung von Online-Communities beitragen, da sie Menschen dazu ermutigen, zusammenzuarbeiten, Informationen auszutauschen und gemeinsam an der Entdeckung und Lösung von Rätseln zu arbeiten. Durch das Teilen von Easter Eggs und die Diskussion über deren Bedeutung und Herkunft können Nutzer und Fans tiefer in die Welt der Spiele, Filme und anderen Medien eintauchen und ihre Begeisterung und Leidenschaft miteinander teilen.

In einer zunehmend digitalisierten Welt, in der das Tempo der Innovationen und Veränderungen immer schneller wird, bieten Easter Eggs einen Hauch von Menschlichkeit, Kreativität und persönlicher Verbindung. Sie erinnern uns daran, dass hinter den Bildschirmen und Codes echte Menschen mit eigenen Ideen, Interessen und Leidenschaften stehen. Easter Eggs sind ein kleines, aber bedeutungsvolles Zeichen dafür, dass trotz der Technologie die Fähigkeit, sich zu amüsieren, zu überraschen und miteinander in Verbindung zu treten, weiterhin im Mittelpunkt unserer Erfahrungen steht.

## 20 Beispiele für Easter Eggs

Hier sind 20 Easter Eggs aus verschiedenen Medien wie Games, Software, Onlinediensten und Filmen:

**Game: The Witcher 3: Wild Hunt Easter Egg:** Der Weeping Angels Doctor Who-Bezug  
Anleitung: In der Nebenquest "Scenes from a Marriage" im Hearts of Stone DLC, findet man Statuen, die den Weeping Angels aus der Doctor Who-Serie ähneln. Beobachte sie genau, und sie verändern ihre Position, wenn du nicht hinsiehst.

**Game: Grand Theft Auto V Easter Egg:** Geheimnis um den Mount Chiliad  
Anleitung: Auf der Spitze des Mount Chiliad in San Andreas gibt es eine Seilbahnstation mit einer geheimen Karte, die auf eine mögliche Alien-Verschwörung oder einen versteckten Jetpack hinweist. Die Suche nach der Lösung dieses Rätsels beschäftigt die Spieler bis heute.

**Game: Red Dead Redemption 2 Easter Egg:** Die Geisterbahn von Lemoyne  
Anleitung: In der Nähe des Bahnhofs in Lemoyne

gibt es ein verlassenes Haus, das scheinbar von Geistern heimgesucht wird. Besuche das Haus bei Nacht, um seltsame Geräusche und unheimliche Schatten zu hören und zu sehen.

**Software: Google Maps Easter Egg:** Pac-Man im Google Maps-Straßenmodus Anleitung: Suche in Google Maps einen Ort, klicke auf das Pac-Man-Symbol in der unteren linken Ecke und spiele Pac-Man auf den Straßen deiner Stadt.

**Onlinedienst: YouTube Easter Egg:** Snake-Spiel Anleitung: Pausiere ein YouTube-Video, drücke die Pfeiltaste nach links und gleichzeitig die Pfeiltaste nach oben. Das klassische Snake-Spiel startet, und du kannst es direkt im Videoplayer spielen.

**Game: Fortnite Easter Egg:** Der Kevin-Teleporter Anleitung: In der Nähe von Greasy Grove gibt es einen Teleporter, der an den mysteriösen Würfel namens Kevin erinnert. Wenn man hineingeht, wird man an einen zufälligen Ort auf der Karte teleportiert.

**Film: The Mandalorian (Disney+ Serie) Easter Egg:** Die Eiskönigin-Referenz Anleitung: In Staffel 2, Episode 2, trägt der Frosch-Passagier eine Tasche mit Eiern, die der Eiskönigin Elsa ähnelt. Dies ist eine subtile Anspielung auf die Eiskönigin von Disney.

**Game: God of War (2018) Easter Egg:** Infinity Gauntlet Anleitung: Sammle alle sechs Verzauberungen, die den Infinity-Steinen aus dem Marvel-Universum entsprechen, und kombiniere sie mit der Shattered Gauntlet of Ages. Du erhältst dann eine Waffe, die dem Infinity Gauntlet aus den Avengers-Filmen ähnelt.

**Film: Deadpool 2 Easter Egg:** Brad Pitt Cameo Anleitung: Während der Szene, in der X-Force-Mitglied Vanisher in Stromleitungen stürzt, zeigt sich Brad Pitts Gesicht für einen kurzen Moment als Vanisher.

**Game: The Legend of Zelda: Breath of the Wild Easter Egg:** Schrein der Göttin im Tempel der Zeit

**Game: The Legend of Zelda: Breath of the Wild Easter Egg:** Schrein der Göttin im Tempel der Zeit Anleitung: Im zerstörten Tempel der Zeit findet man einen Schrein der Göttin. Dies ist eine Anspielung auf frühere Zelda-Spiele, bei denen der Tempel der Zeit eine wichtige Rolle spielte.

**Software: Microsoft Excel Easter Egg:** Excel 97 Flugsimulator Anleitung: In Excel 97, öffne ein neues Arbeitsblatt, drücke F5, gebe "X97:L97" ein und drücke Enter. Drücke nun Strg+Shift und

klicke auf das Chart Wizard-Symbol. Ein versteckter Flugsimulator wird gestartet.

**Onlinedienst: Google Search Easter Egg: "Do a Barrel Roll"**

Anleitung: Gib "Do a Barrel Roll" in die Google-Suchleiste ein und die gesamte Suchergebnisseite dreht sich 360 Grad.

**Film: Guardians of the Galaxy Easter Egg: Stan Lee Cameo**

Anleitung: In einer Szene kommuniziert Stan Lee, der Schöpfer vieler Marvel-Charaktere, mit den Watchers, einer Gruppe von Wesen, die das Marvel-Universum beobachten.

**Game: Assassin's Creed Valhalla Easter Egg: Harry Potter-Referenz**

Anleitung: Im Lunden-Gebiet findest du einen verlassenen Turm, der stark an den Turm erinnert, in dem Harry Potter in den Büchern und Filmen lebte. Du kannst sogar eine Eule finden, die Hedwig ähnelt.

**Software: Adobe Photoshop Easter Egg: Versteckte Toast-UI**

Anleitung: In Photoshop CC, drücke Strg+K, um die Voreinstellungen zu öffnen. Halte die Alt-Taste gedrückt und klicke auf das "Pfützen"-Icon. Eine geheime "Toast" Benutzeroberfläche wird enthüllt.

**Onlinedienst: Google Earth Easter Egg: Flight Simulator**

Anleitung: Öffne Google Earth Pro, klicke auf "Tools" in der Menüleiste und wähle "Flight Simulator". Du kannst dann zwischen verschiedenen Flugzeugen wählen und in der realen Welt fliegen.

**Film: Toy Story 4 Easter Egg: A113**

**Anleitung:** In einer Szene sieht man eine Nummernschild, das "A113" liest. Dies ist eine Referenz auf den Klassenzimmer-Code für das California Institute of the Arts, an dem viele Pixar-Mitarbeiter studiert haben.

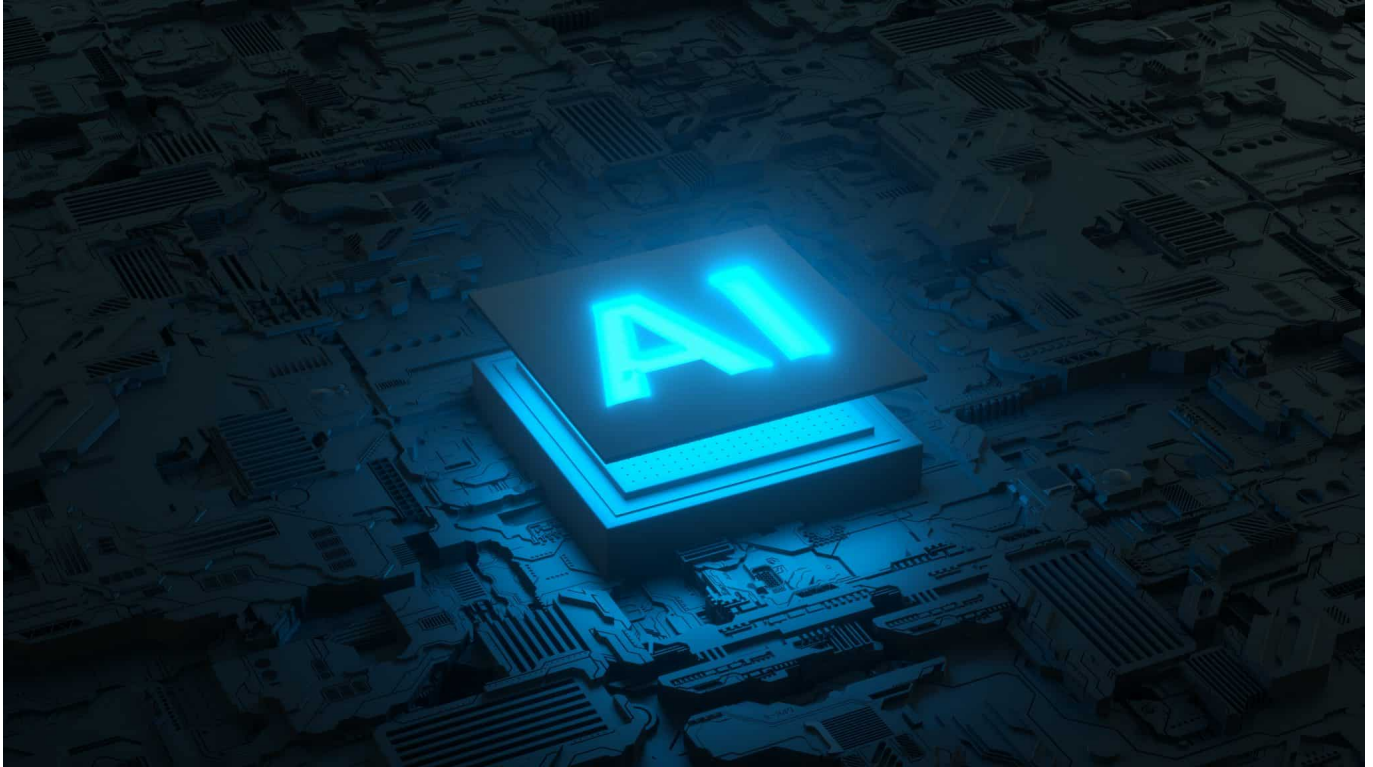
**Game: Marvel's Spider-Man (2018) Easter Egg: Avengers Tower**

Anleitung: Beim Erkunden von New York City in Marvel's Spider-Man kannst du den Avengers Tower finden. Dies ist eine Anspielung auf das Marvel Cinematic Universe und die Avengers-Filme.

**Film: Die Eiskönigin 2 Easter Egg: Verstecktes Mickey Mouse-Symbol**

Anleitung: In einer Szene, in der Anna und Olaf durch den Wald gehen, sind die Silhouetten von drei Steinen in der Form von Mickey Mouse arrangiert. Dies ist ein häufiges Easter Egg in Disney-Filmen

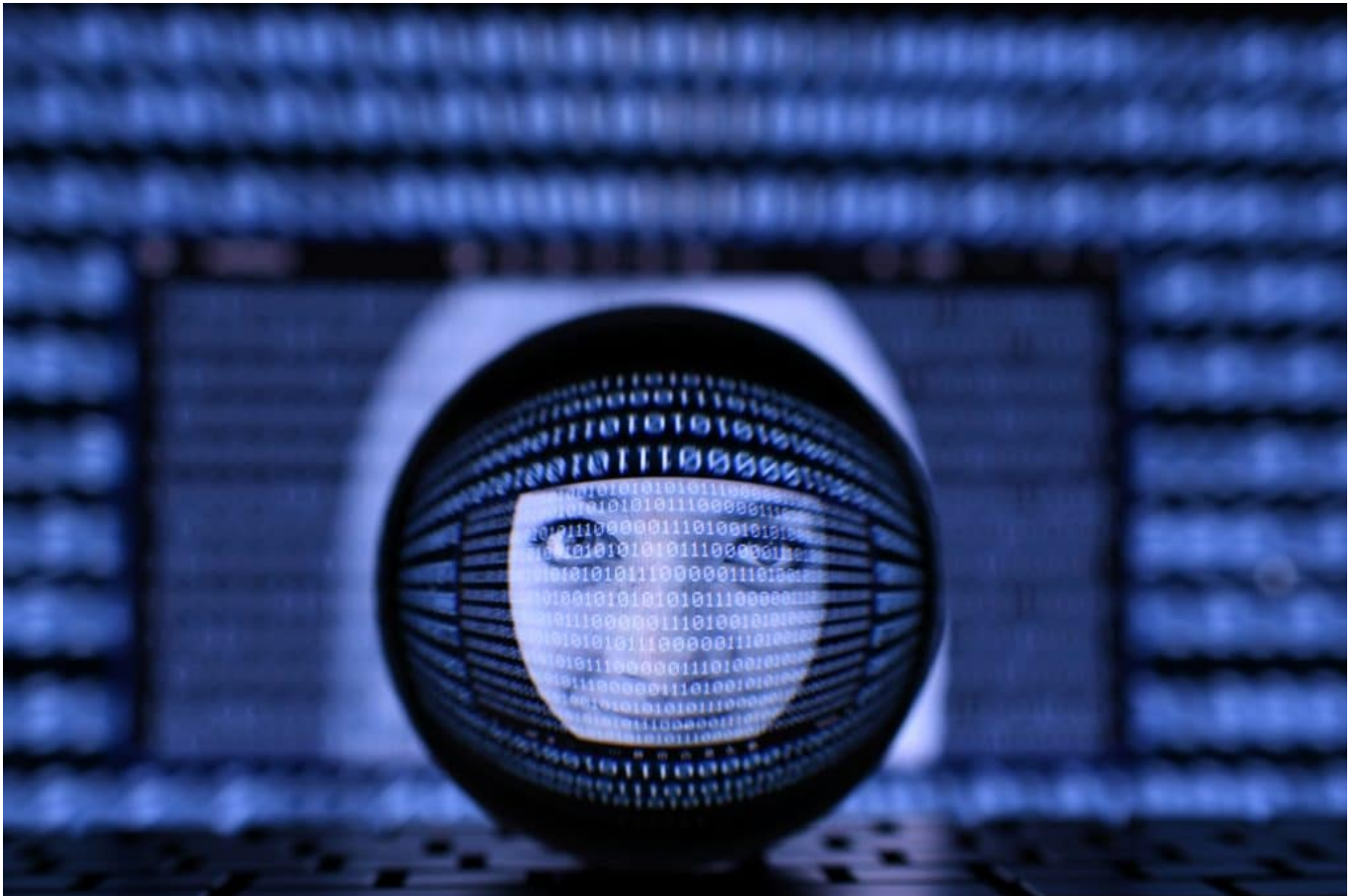
## Künstliche Intelligenz: Eine faszinierende Technologie und die Frage der Kontrolle



**Ein offener Brief, unterschrieben von vielen Vordenkern der Tech-Branche: Die Weiterentwicklung von KI soll pausieren - damit alle mal durchatmen und Regeln aufgestellt werden können. Eine gute Idee?**

Künstliche Intelligenz (KI) ist längst kein bloßes Science-Fiction-Konzept mehr, sondern in unserem Alltag präsent und beeinflusst viele Aspekte unseres Lebens. KI-Systeme steuern Autos, optimieren Energienetze und helfen uns, den perfekten Film auf Netflix zu finden.

Doch wie entwickelt sich diese Technologie, und wie können wir sie kontrollieren? In diesem Artikel werfen wir einen unterhaltsamen und verständlichen Blick auf die Entwicklung der Künstlichen Intelligenz und die Herausforderungen, die sie mit sich bringt.



*Sechs Monate Entwicklungspause für KI: Experten fordern ein innehalten*

## **KI - Eine rasante Entwicklung**

Wer glaubt, KI sei etwas vergleichsweise Neues, der täuscht sich. Denn die Grundlagen der Künstlichen Intelligenz reichen bis in die 1950er Jahre zurück. Damals waren Computer noch gigantische Maschinen, die ganze Räume füllten (und den Raum ordentlich aufheizten) und vor allem für militärische und wissenschaftliche Zwecke genutzt wurden.

In den folgenden Jahrzehnten entwickelten sich Computer und KI-Systeme rasant weiter. In den 1990er Jahren gelang es KI-Systemen, Schachweltmeister zu schlagen und einfache Spracherkennungsaufgaben zu meistern.

Mit der Einführung des Internets und der Vernetzung von Computern wurde die Entwicklung von Künstlicher Intelligenz weiter beschleunigt. Heute nutzen wir KI-Systeme, die auf maschinellem Lernen basieren, um komplexe Aufgaben zu lösen, von der Gesichtserkennung bis zur Übersetzung von Texten in Echtzeit (wie zum Beispiel das in Deutschland entwickelte, wirklich empfehlenswerte



DeepL).

## Die Kontrolle von Künstlicher Intelligenz

Doch auch das Thema Verantwortung muss diskutiert werden.. Denn mit der rasanten Entwicklung der KI-Technologie stellt sich jedoch die Frage, wie wir diese kontrollieren und sicherstellen können, dass sie im Einklang mit unseren ethischen Grundsätzen und gesellschaftlichen Werten steht.

Ein Aspekt, der bei der Kontrolle von Künstlicher Intelligenz eine Rolle spielt, ist die Transparenz. Viele KI-Systeme, insbesondere solche, die auf neuronalen Netzwerken basieren, sind sogenannte "Black Boxes". Das bedeutet, dass wir zwar sehen können, welche Ergebnisse sie liefern, aber nicht genau verstehen, wie sie zu diesen Ergebnissen gelangen.



*Microsoft führt KI zur Unterstützung bei Microsoft Office ein*

Um KI-Systeme besser kontrollieren zu können, ist es wichtig, ihre Funktionsweise und Entscheidungsprozesse nachvollziehbar zu gestalten. Forscher arbeiten daher an Methoden, um KI-Systeme transparenter und erklärbarer zu machen. So könnten wir sicherstellen, dass Künstliche Intelligenz ethischen Richtlinien folgt und nicht diskriminierend oder manipulativ agiert.

Ein weiterer Aspekt der Kontrolle von Künstlicher Intelligenz ist die Regulierung. Wie bei jeder neuen Technologie gibt es auch bei KI ethische und rechtliche Fragestellungen, die geklärt werden müssen. Zum Beispiel stellt sich die Frage, wer haftet, wenn ein autonomes Fahrzeug einen Unfall verursacht: der Hersteller, der Besitzer oder das KI-System selbst?

Um diese und andere Fragen zu beantworten, sind Regierungen und internationale Organisationen gefordert, Gesetze und Regelungen zu erarbeiten,

die den Umgang mit Künstlicher Intelligenz regeln. Diese Regelungen sollten sowohl den Schutz der Privatsphäre und Grundrechte der Nutzer gewährleisten als auch die Verantwortung der Hersteller und Entwickler von KI-Systemen klar definieren.

## **Die Rolle von Unternehmen und Forschung**

Neben Gesetzgebern und Regulierungsbehörden spielen auch Unternehmen und Forschungseinrichtungen eine wichtige Rolle bei der Kontrolle von Künstlicher Intelligenz. Durch die Einhaltung von ethischen Richtlinien und die Entwicklung von verantwortungsbewussten KI-Systemen können sie dazu beitragen, die Technologie sicher und vertrauenswürdig zu gestalten.

Ein Beispiel für verantwortungsvolle KI-Forschung ist die Zusammenarbeit von Wissenschaftlern aus verschiedenen Ländern und Disziplinen, die gemeinsam an der Entwicklung von KI-Systemen arbeiten, die menschenähnliche Fähigkeiten besitzen und gleichzeitig ethischen Grundsätzen folgen.



*Snapchat führt einen KI-Chatbot ein: "My AI" soll zum neuen Freund der User werden*

## **Die Zukunft der Künstlichen Intelligenz**

Die Zukunft der Künstlichen Intelligenz ist spannend und ungewiss zugleich. Einerseits eröffnen sich durch die Weiterentwicklung von KI-Systemen zahlreiche Möglichkeiten, um unser Leben zu verbessern und gesellschaftliche Herausforderungen wie den Klimawandel oder die medizinische Versorgung zu bewältigen.

Andererseits birgt die rasante Entwicklung von Künstlicher Intelligenz auch Risiken, wie den Missbrauch von KI für Überwachung oder Desinformation. Um diese Risiken zu minimieren, ist es entscheidend, dass wir die Kontrolle über KI-Systeme behalten und ihre Entwicklung auf eine Weise gestalten, die im Einklang mit unseren Werten und ethischen Grundsätzen steht.

## **Wichtigstes Ziel: Im Dienste der Menschheit**

Die Entwicklung der Künstlichen Intelligenz ist zweifellos faszinierend und bietet

immense Chancen, unser Leben und unsere Gesellschaft positiv zu beeinflussen. Gleichzeitig stellt die Frage der Kontrolle eine zentrale Herausforderung dar, der wir uns stellen müssen. Durch Transparenz, Regulierung, verantwortungsbewusste Forschung und Zusammenarbeit können wir die KI-Technologie so gestalten, dass sie im Dienste des Menschen steht und das Potenzial hat, unsere Zukunft nachhaltig zu verbessern.

Die Künstliche Intelligenz ist ein weites und spannendes Feld, das uns alle betrifft. Indem wir uns aktiv mit dieser Technologie auseinandersetzen und uns über ihre Möglichkeiten und Herausforderungen informieren, können wir als Gesellschaft darauf hinarbeiten, eine Zukunft zu gestalten, in der Künstliche Intelligenz zum Wohle aller eingesetzt wird. Dabei ist es wichtig, stets einen kritischen und informierten Blick auf die Technologie und ihre Anwendungen zu bewahren, um sicherzustellen, dass sie unseren ethischen und gesellschaftlichen Werten entspricht.

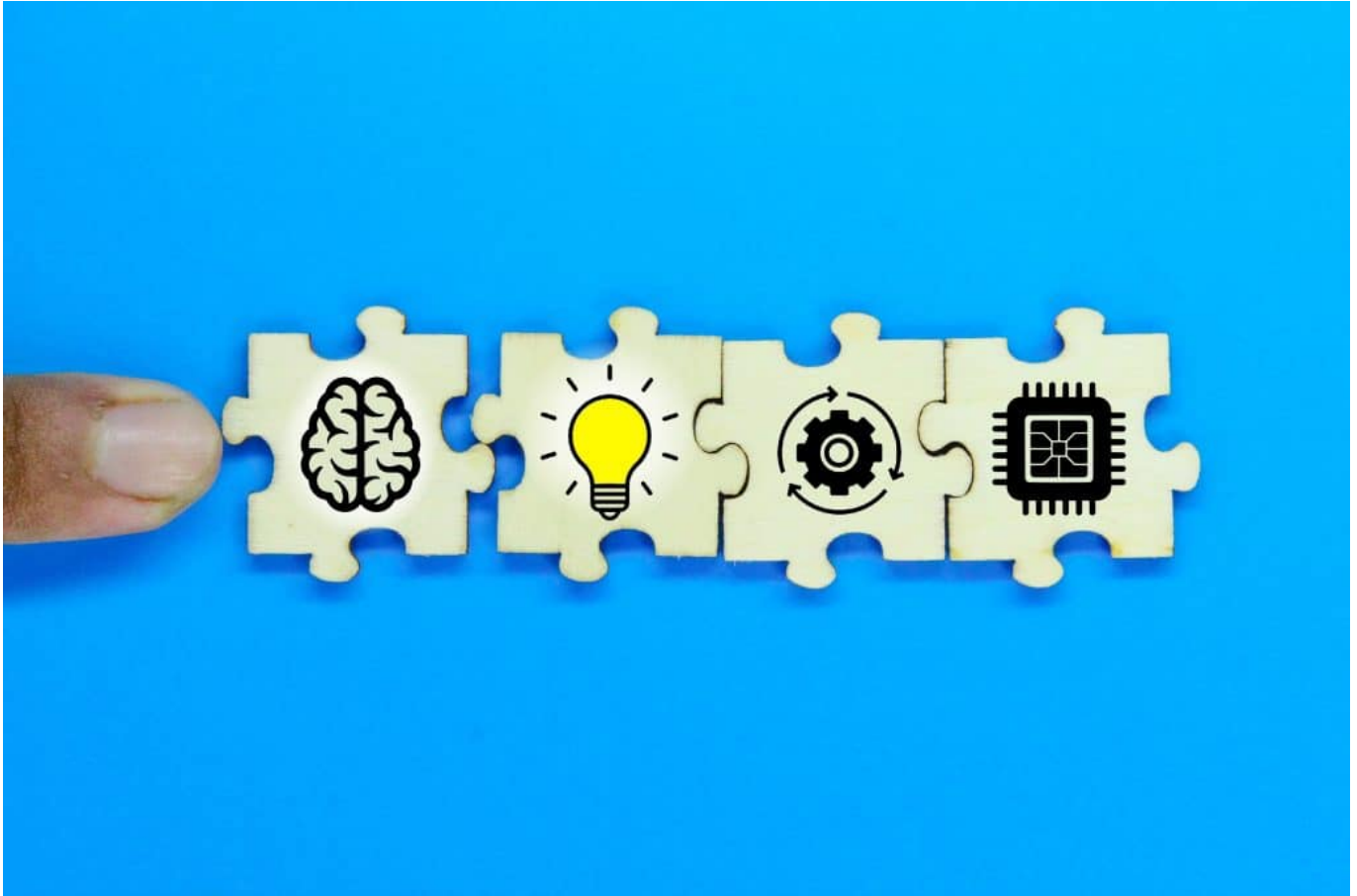
## Warum man sich vom Begriff KI nicht blenden lassen sollte



**Nicht überall, wo KI drauf steht, steckt auch KI drin: Der Hypebegriff wird häufig zum Marketing missbraucht.**

KI. Diese beiden Buchstaben hört man aktuell gefühlt irgendwie ständig. Künstliche Intelligenz scheint in alle Bereiche unseres Lebens einzudringen. Spätestens seit dem Hype um ChatGPT wird das deutlich. Aber wie das mit Hypes so ist: Die einen sind begeistert, die anderen sind genervt – und wieder andere versuchen, daraus Profit zu schlagen. Plötzlich steckt angeblich überall „KI“ drin, nur weil ein paar Entscheidungen gefällt oder Prozesse optimiert werden.

KI als Schlagwort, das verkauft sich gut. Und plötzlich sind auch die Beauty-Filter in der Smartphone-App KI. Aber stimmt das überhaupt? Steckt wirklich überall KI drin, wo KI draufsteht?



## Unterschied von KI und Algorithmen

Klären wir aber erst mal, was KI eigentlich ist - und wo die Unterschiede zu "normalen" Computerprogrammen liegen.

Es ist im Grunde ganz einfach: Als Künstliche Intelligenz (KI) bezeichnen wir die (angestrebte) Fähigkeit von Maschinen, Aufgaben auszuführen, die normalerweise menschliche Intelligenz erfordern. KI simuliert menschliches Verhalten und menschliche Fähigkeiten, wie z.B. Spracherkennung, Bilderkennung (das ist eine Katze, das ist ein Hund, und das ist eine Katze auf dem Dach, die auf den Hund schaut) oder Entscheidungsfindung. Algorithmen hingegen, also die klassischen Computerprogramme, sind eine Abfolge von mathematischen und logischen Anweisungen, die ein Computer strikt der Reihe nach ausführt, um eine bestimmte Aufgabe auszuführen oder ein Problem zu lösen. Berechne erst dies, dann nimm das Ergebnis und tue das.

Algorithmen werden programmiert, KI wird trainiert. Sie lernt – und wendet das gelernte Wissen an. KI-Systeme basieren zwar auch auf Programmen, aber nur,

um das Lernen zu ermöglichen, nicht um die Handlungen vorwegzunehmen. Der Unterschied besteht also darin, dass KI ein übergeordnetes Konzept ist, um menschenähnliche Intelligenz nachzubilden.



*Algorithmen geben dem Computer genau vor, was er zu tun hat*

## Der Begriff "Künstliche Intelligenz"

Wir müssen aber auch über den Begriff KI selbst sprechen. Weckt der nicht unerfüllbare Erwartungen, weil der Begriff „Intelligenz“ enthalten ist – das verbinden wir doch automatisch mit uns Menschen...

Stimmt. Manche Experten sagen, es wäre besser, wir würden von „Entscheidungssystemen“ oder von „autonomen Systemen“ sprechen statt von KI. Dann wäre der Aspekt „Intelligenz“ raus. Denn darüber lässt sich streiten, wo Intelligenz anfängt und wo sie aufhört.

In der Wissenschaft wird aber dennoch durchaus von einer „Superintelligenz“ gesprochen: So wird es bezeichnet, sollte es tatsächlich gelingen, ein KI-System

zu schaffen, dass eigenständig denkt und die Denkfähigkeiten des Menschen zu übertreffen. Ein Zustand, der zu Recht viele Menschen ängstigt. Denn, so die Sorge, ab dem Moment könnte der Mensch die Superintelligenz nicht mehr verstehen und eingreifen.

## **KI kann schon sinnvoll genutzt werden**

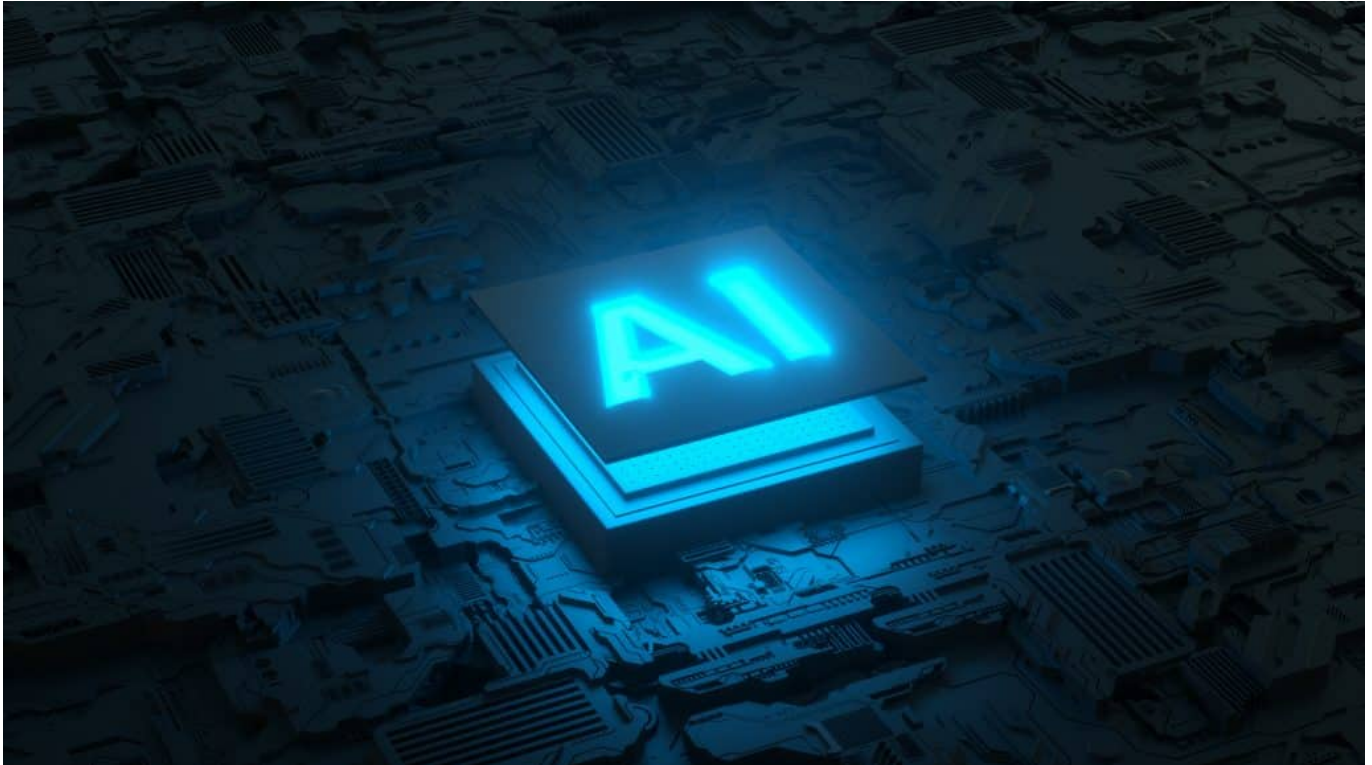
Aber in welchen Bereichen kann KI heute schon sinnvoll eingesetzt werden – und wird auch eingesetzt?

Ein wichtiger Bereich ist die Medizin. Mithilfe von KI lassen sich schneller und zuverlässiger Krankheiten erkennen und diagnostizieren. Beispiele sind die Analyse von bildgebender Diagnostik, das berühmte Röntgenbilder, das CT, das MRT. In solchen Bildern können KI-Systeme und zuverlässig Auffälligkeiten erkennen und auf mögliche krankhafte Veränderungen hinweisen. Selbst Diagnosen sind möglich.

Eine große Stärke liegt auch bei individuellen Therapien: Besonders bei Patienten mit multiplen Erkrankungen und Medikation kann eine KI schnell Therapiepläne entwickeln, die auf die Bedürfnisse und Besonderheiten eines Patienten zugeschnitten sind. Auch bei der Entwicklung neuer Medikamente kommt KI zum Einsatz. Aber auch bei der Verarbeitung großer Datenmengen, Stichwort: Big Data.

In selbstfahrenden Autos. Zu Betrugsprävention in Banken. Zur Produktionsoptimierung in Fabriken. Im Militär. Oder auch in der Ausbildung: KI-Systeme können viel besser auf individuelle Stärken und Schwächen eingehen als ein Buch oder ein „normales“ Lernprogramm. Es gibt schon eine lange und beeindruckende Liste.





## **Nicht überall, wo KI draufsteht, ist auch KI drin**

Ich habe es scho angedeutet: Nicht überall, wo „KI“ drauf steht, ist auch KI drin. Gibt es ein paar Beispiele, wo mit KI geworben wird, obwohl gar keine KI im Einsatz ist?

Vor allem im „Smart Home“ ist das der Fall: Da werden Staubsauger-Roboter auf den Boden gestellt, der sich durch die Wohnung schieb, irgendwann den Grundriss kennt und nicht mehr die Treppe runterfällt, die Couch geschickt umfährt und vieles mehr. Wird gerne als Wunder der KI verkauft – sind aber ganz normale Algorithmen. Sie legen einen Plan der Wohnung an und beachten und optimieren die Fahrtwege.

Das können normale Programme, dafür braucht es keine KI. Dasselbe gilt für „smarte“ Thermostate oder Heizungen, die angeblich lernfähig sind: In Wahrheit optimieren ganz normale Algorithmen die Wärmezufuhr. Keine Hexerei nötig, nicht mal KI. Auch ist oft zu hören, dass KI über die Vergabe von Krediten entscheidet – in der Regel sind es aber keine KI-Systeme, sondern ganz normale algorithmische Programme, die nach strengen Regeln und Datenauswertung die Entscheidungen treffen.

Allerdings wird in diesem Segment auch mit KI experimentiert, das muss man der

Ehrlichkeit halber erwähnen. Auch so mancher Filter, der in Social Media unser Gesicht verfremdet, ist keine KI im strengen Sinne, sondern ein Algorithmus. Man muss wirklich genau hinschauen, ob wirklich KI nötig und sinnvoll ist.

## Offener Brief fordert sofortigen Stopp

Vor einigen Tagen wurde [ein offener Brief veröffentlicht](#), der ausdrücklich zu einem sofortigen Stillstand bei der Weiterentwicklung von KI aufruft. Wer und was steckt dahinter?

Es haben wirklich viele Prominente aus dem Silicon Valley mitformuliert und unterschrieben, darunter der Apple-Mitbegründer Steve Wozniak, aber auch Elon Musk. Hunderte Namen dieser Größenordnung haben unterschrieben und unterstützen die Forderung, die Entwicklung fortschrittlicher KI-Systeme einzustellen. Das betrifft auch ChatGPT5, der geplante Nachfolger vom aktuellen ChatGPT4.

Der Grund, einen Entwicklungsstopp bei KI zu fordern: KI berge tiefgreifende Risiken für die Gesellschaft und Menschheit. Was zweifelsohne zutrifft, ohne Wenn und Aber. Die Unterzeichner des offenen Briefs verlangen ein Moratorium, sollten die Unternehmen der Aufforderung nicht nachkommen.

Das allerdings würde ja voraussetzen, dass sich so schnell viele Regierungen darauf verständigen könnten, was eher unrealistisch erscheint. Die Kritiker sehen viele Probleme: Durch KI erzeugte Propaganda, automatisierte Jobs und Job-Verlust allerorten, eine Intelligenz, die uns alle früher oder später überflüssig machen und sogar übertreffen könnte. Eine „Superintelligenz“, wie das auch genannt wird.

## Realistisch oder nicht?

Zunächst einmal: Die Bedenken und Argumente sind ausnahmslos begründet und nachvollziehbar – und auch zutreffend. Und in der Tat wäre es wünschenswert, würden sich Regierungen in aller Welt dieser Sache sofort und ernsthaft annehmen. Denn in der Tat kann und wird KI einen tiefgreifenden Wandel bedeuten. Das Problem ist aber: Regierungen sind träge. Es gibt viele andere Themen. Ohne Druck wird da nicht viel passieren.

Der offene Brief ist da nicht Druck genug. Gleichzeitig haben wir aktuell einen

brutalen Wettbewerb: Alle großen Digitalkonzerne wollen vorne mitspielen, jetzt keine Marktanteile einbüßen. Die Karten werden völlig neu gemischt. Es geht darum, möglichst der größte Player im Bereich der KI zu werden, denn hier liegt die Zukunft. Das sagen alle Experten voraus. Im Vergleich zur KI ist das Internet eine kleine Erfindung gewesen. Ich bin skeptisch, dass es zu einem Einhalten oder Abwarten bei den verantwortlichen Unternehmen kommt – in China würde man das sicher nutzen, um sich einen Vorteil zu erarbeiten.

## DeepFakes: Die (fast) perfekte Illusion



**Mit der sich rasant verbreitenden KI-Technologie wird das Erstellen von DeepFakes immer einfacher: Fake-Aufnahmen, die echt aussehen - aber es nicht sind. Nicht immer unterhaltsam, sondern durchaus auch brisant und gefährlich.**

In einer Welt, in der Technologie und Künstliche Intelligenz immer rasanter voranschreiten, eröffnen sich uns ungeahnte Möglichkeiten - und ebenso große Herausforderungen. Eine dieser Herausforderungen sind DeepFakes.

Der Begriff "DeepFake" setzt sich aus "Deep Learning" und "Fake" zusammen und beschreibt eine Technologie, die das Potenzial hat, die Wahrnehmung von Realität auf den Kopf zu stellen.

In diesem Artikel möchte ich einen detaillierten Einblick geben, was DeepFakes sind, wie sie entstehen, wieso es heute so einfach ist, sie herzustellen, und wie man sie erkennen kann. Zum Schluss werfen wir einen Blick in die Zukunft und zeigen auf, wie wir mit DeepFakes umgehen sollten.



Wenn Jörg mal ins Weiße Haus einzieht...

## Was sind DeepFakes?

DeepFakes sind manipulierte Medieninhalte, die darauf abzielen, das Aussehen oder die Stimme einer Person so überzeugend zu verändern oder zu imitieren, dass es schwerfällt, sie von realen Inhalten zu unterscheiden.

In den meisten Fällen handelt es sich dabei um Videos, in denen das Gesicht einer Person durch das Gesicht einer anderen Person ersetzt wird. Aber auch Audioaufnahmen, in denen Stimmen nachgeahmt werden, können als DeepFakes bezeichnet werden.

## Wie entstehen DeepFakes?

DeepFakes entstehen durch den Einsatz von künstlicher Intelligenz und maschinellem Lernen. Der Prozess beginnt mit der Sammlung einer großen Menge an Bildern oder Videos der zu manipulierenden Personen. Diese Daten werden dann verwendet, um ein neuronales Netzwerk darauf zu trainieren, die Gesichtsmerkmale der Personen zu erkennen und zu reproduzieren.

Der nächste Schritt ist das Generieren von "Fake"-Inhalten. Dazu wird ein zweites

neuronales Netzwerk trainiert, das in der Lage ist, die Gesichtszüge einer Person auf die einer anderen Person zu übertragen. Hierbei kommen sogenannte "Generative Adversarial Networks" (GANs) zum Einsatz.

GANs bestehen aus zwei Teilen: einem Generator und einem Diskriminator. Der Generator erzeugt die DeepFakes, während der Diskriminator versucht, sie von echten Inhalten zu unterscheiden. Beide Netzwerke werden so lange gegeneinander trainiert, bis der Generator Fälschungen erzeugen kann, die der Diskriminator nicht mehr von realen Inhalten unterscheiden kann.



## Wieso ist es heute so einfach, DeepFakes herzustellen?

Die Entwicklung von DeepFakes wurde durch mehrere Faktoren begünstigt:

- **Zugänglichkeit von Daten:** Heutzutage sind Unmengen an Bildern und Videos von Personen online verfügbar. Diese Daten dienen als Trainingsmaterial für neuronale Netzwerke, die DeepFakes erzeugen.
- **Fortschritte in der KI-Forschung:** Die Entwicklung von Techniken wie GANs hat es ermöglicht, täuschend echte DeepFakes zu erzeugen. GANs sind in den letzten Jahren immer leistungsfähiger geworden und können nun auch mit weniger Trainingsdaten arbeiten.

- **Benutzerfreundliche Tools:** Es gibt mittlerweile zahlreiche Apps und Online-Plattfformen, die es auch technisch weniger versierten Nutzern ermöglichen, DeepFakes zu erstellen. Diese Tools haben die Schwelle für das Erstellen von DeepFakes erheblich gesenkt.
- **Leistungsstarke Hardware:** Moderne Grafikprozessoren (GPUs) und spezialisierte KI-Chips ermöglichen das schnelle Trainieren von neuronalen Netzwerken. Dies hat die Zeit, die für das Erstellen von DeepFakes benötigt wird, erheblich verkürzt.

## Wie lassen sich DeepFakes erkennen?

Trotz ihrer raffinierten Technik gibt es Anzeichen, die darauf hindeuten können, dass ein Video oder eine Audiodatei manipuliert wurde:

**Inkonsistenzen in der Beleuchtung:** DeepFakes können Schwierigkeiten haben, die Lichtverhältnisse im Originalvideo korrekt nachzubilden. Achten Sie auf ungewöhnliche Schatten oder Lichtreflexe.

**Unnatürliche Bewegungen:** Insbesondere bei älteren DeepFakes können Gesichtsbewegungen oder Lippenbewegungen ungewöhnlich wirken. Auch wenn neuere Techniken dies verbessert haben, können immer noch Anomalien auftreten.

**Artefakte:** Manchmal hinterlassen DeepFakes Bildartefakte, die auf eine Manipulation hinweisen können. Dazu gehören Unschärfen, Rauschen oder unscharfe Kanten.

**Kontext und Quelle:** Prüfen Sie, ob das Video oder die Audiodatei von einer vertrauenswürdigen Quelle stammt, und stellen Sie den Kontext der Aufnahme fest. Wenn etwas zu sensationell oder unglaubwürdig erscheint, ist es möglicherweise ein DeepFake.

Es gibt auch KI-basierte Tools, die entwickelt wurden, um DeepFakes automatisch zu erkennen. Diese Tools nutzen maschinelles Lernen, um Anomalien in Videos oder Audiodateien zu identifizieren, die für das menschliche Auge oder Ohr möglicherweise nicht wahrnehmbar sind.

## Zukunftsperspektiven: Wie sollen wir mit DeepFakes umgehen?

Der Umgang mit DeepFakes wird in den kommenden Jahren zweifellos eine immer größere Herausforderung werden. Um die negativen Auswirkungen von DeepFakes zu minimieren und eine gesunde Informationslandschaft zu erhalten, sollten wir auf verschiedenen Ebenen handeln:

- **Aufklärung und Bildung:** Es ist wichtig, das Bewusstsein für DeepFakes zu schärfen und Menschen beizubringen, wie sie manipulierte Inhalte erkennen können. Dies sollte Teil der allgemeinen Medienkompetenz sein, die in Schulen und anderen Bildungseinrichtungen vermittelt wird.
- **Technologieentwicklung:** Wir sollten in die Erforschung und Entwicklung von KI-basierten Tools investieren, die DeepFakes erkennen und bekämpfen können. Gleichzeitig sollten wir uns bewusst sein, dass dies ein "Wettlauf der KIs" sein wird, bei dem DeepFake-Erzeuger ständig versuchen werden, die Erkennungsmethoden zu umgehen.
- **Regulierung und Gesetzgebung:** Gesetzgeber sollten klare Regeln und Sanktionen für den Missbrauch von DeepFakes schaffen, um kriminelle Aktivitäten, Rufschädigung und Desinformation einzudämmen. Dabei gilt es, den richtigen Balanceakt zwischen Meinungsfreiheit und dem Schutz vor Schaden zu finden.
- **Verantwortung der Plattformen:** Soziale Medien und Online-Plattformen sollten eine aktivere Rolle bei der Bekämpfung von DeepFakes übernehmen. Dazu gehört das Implementieren von Erkennungssystemen, die schnelle Entfernung von schädlichen Inhalten und das Aufzeigen von Manipulationen, um Nutzer zu informieren.
- **Kollaboration:** Die Zusammenarbeit zwischen Regierungen, Unternehmen, Forschungseinrichtungen und Zivilgesellschaft ist entscheidend, um den Herausforderungen von DeepFakes wirksam zu begegnen. Gemeinsame Anstrengungen und Informationsaustausch können dazu beitragen, effektive Lösungen zu entwickeln und die Öffentlichkeit zu schützen.





Hinweise für DeepFakes sind Störungen und Unzulänglichkeiten

## Was bringt die Zukunft?

DeepFakes stellen eine bedeutende Herausforderung für unsere digitale Gesellschaft dar. Sie haben das Potenzial, die Wahrnehmung von Realität zu verzerren, Desinformation zu fördern und das Vertrauen in Medieninhalte zu untergraben.

Um diesen Herausforderungen zu begegnen, müssen wir auf verschiedenen Ebenen handeln, von der Bildung und Aufklärung über technologische Innovationen bis hin zu regulatorischen Maßnahmen.

Indem wir uns bewusst werden, wie DeepFakes entstehen und wie man sie erkennen kann, können wir besser darauf vorbereitet sein, sie zu bekämpfen und ihre negativen Auswirkungen zu minimieren. Letztendlich liegt es an uns allen, eine kritische und informierte Haltung gegenüber den Inhalten einzunehmen, die wir konsumieren und teilen, und gemeinsam für eine verantwortungsbewusste Nutzung von Technologie einzutreten

## DeepFakes: Wie umgehen mit Fake-Fotos und wie sie erkennen?



**DeepFakes werden immer besser, lassen sich immer schwerer erkennen - und sind gleichzeitig immer einfacher herzustellen. Eine unheilvolle Kombination.**

Im Netz kursieren nicht nur merkwürdige Behauptungen und FakeNews, sondern immer öfter auch merkwürdige Fotos – und Fake-Fotos. Gerade erst zum Beispiel Fotos, die den Papst in stylischer Daunenjacke zeigen. Kaum zu glauben, oder?

Aber es handelt sich dabei um ein Fake-Foto. Erzeugt mit Hilfe von Künstlicher Intelligenz (KI). Die Aufnahmen, die solche KI-Systeme ausspucken, werden immer überzeugender. Gleichzeitig wird es immer einfach, solche Bilder zu erstellen.



*Fotos, die Donald Trump in einer solchen Situation zeigen, sind brisant*

## DeepFakes vom Papst in weißer Luxusjacke

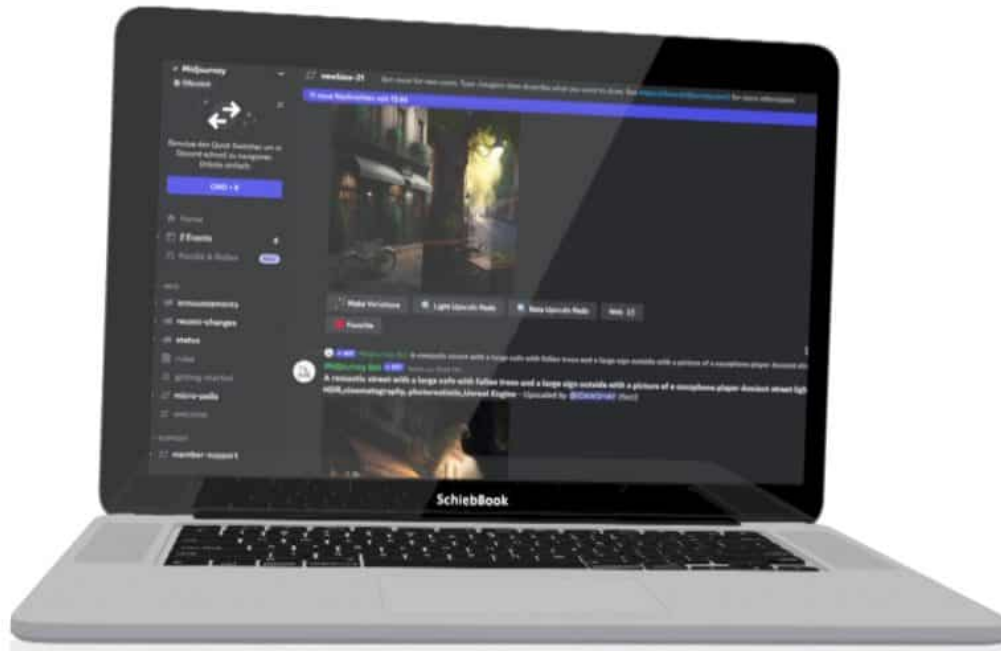
Papst Franziskus in hipper Daunenjacke. Ein wenig ungewöhnlich zwar – aber warum nicht? Vielleicht ist es gerade kalt in Rom. Sieht jedenfalls echt aus... Ist aber Fake. Eine Fälschung.

Dasselbe gilt für diese Aufnahmen. Sie zeigen Donald Trump, wie er sich energisch einer Verhaftung widersetzt. Macht Sinn: In New York droht ihm aktuell tatsächlich eine Haftstrafe. Aber: Ebenfalls Fake. Ebenso diese Aufnahme, die Wladimir Putin knieend vor dem chinesischen Regierungschef Xi Jinping zeigt.

Alles Fake-Bilder. Entstanden mit Hilfe von KI, Künstlicher Intelligenz.

Mit KI lassen sich eben nicht nur Texte erstellen, Stichwort ChatGPT, sondern auch Bilder. Auch Fotos. Aufnahmen, die zumindest auf den ersten Blick täuschend echt aussehen. Und das immer einfacher – und nahezu kostenlos.

Solche Aufnahmen werden **Deepfakes** genannt. **Deep**, weil Deep Learning dahintersteckt. Eine besondere Art von KI-Technologie. Und **Fake** – na ja, weil es eben Fakes sind. Fälschungen.



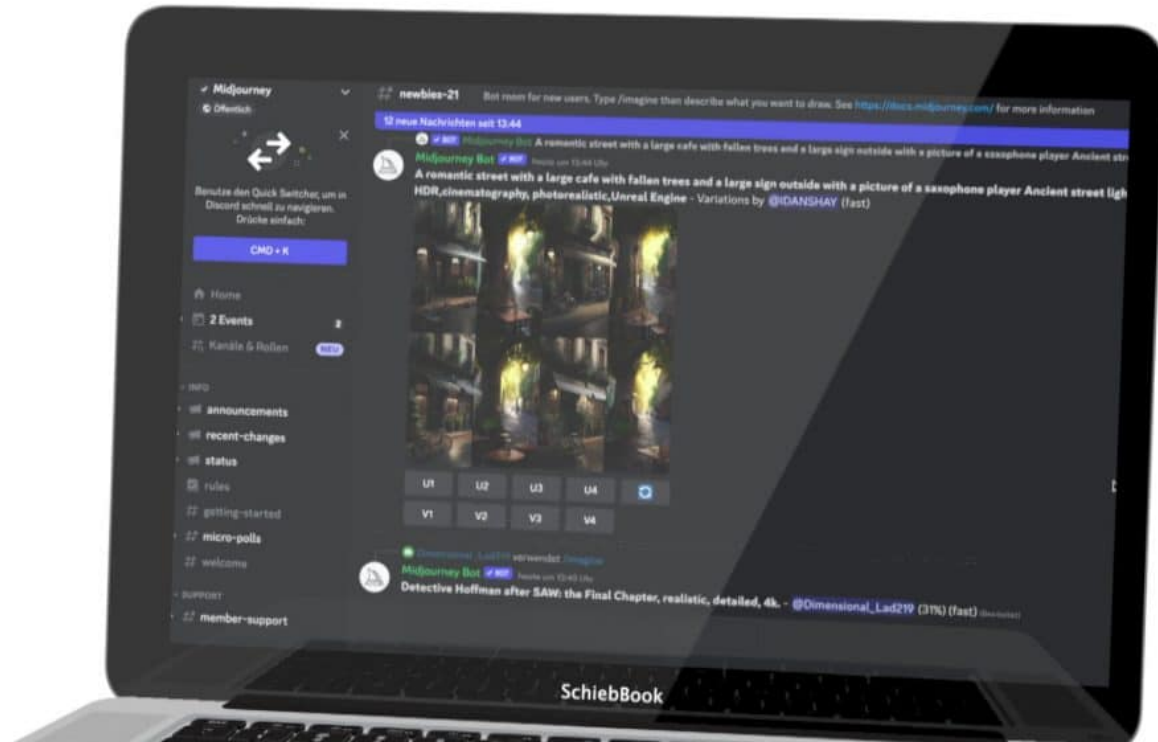
*Es gibt diverse KI-Systeme, mit denen sich hochwertige Deepfakes herstellen lassen*

## **Midjourney erstellt fotorealistische Bilder**

Eine solche KI ist Midjourney. Die erzeugt im Augenblick technisch gesehen die besten Bilder. Es reicht, dass ich sage: Ich brauche ein Bild von Donald Trump in Moskau – und voilà. Haben wir Fotos von Donald Trump im Moskau.

Wer sich noch ein bisschen mehr Mühe gibt bei der Beschreibung, dem sogenannten Prompt, der bekommt schnell noch viel bessere Aufnahmen. Das alles dauert nicht lange und kostet auch nicht viel. Gerade erst ist die neue Version 5 von Midjourney an den Start gegangen: Spezialisiert auf fotorealistische Aufnahmen – aus der KI.

Es gibt derzeit ein halbes Dutzend solcher KI-Systeme – und unzählige Apps, die darauf aufsetzen. Auch auf dem Smartphone – aber da dienen sie eher dem Spaß, mit deutlich schlechteren Ergebnissen. Die Profisysteme hingegen werden immer besser, liefern immer bessere Ergebnisse.



*Midjourney produziert erstaunliche Fotos und Aufnahmen*

## DeepFakes immer einfacher herzustellen

Ein kompromittierendes Foto von einem angeblich „heimlichen“ Treffen einer jungen Frau und Donald Trump – das lässt sich mit Werkzeugen wie Midjourney wirklich schnell und einfach herstellen. Wer ein paar Fotos der betreffenden Frau hochlädt, kann sie von der KI nachbilden lassen.

Und das macht die Brisanz deutlich: Wer Menschen mittels Deepfakes in bestimmten Situationen präsentiert, kann schnell ihren Ruf ruinieren und auch massive Folgen haben. Und wenn es um Politiker geht, kann ganz leicht ein gesellschaftlicher Schaden entstehen. Auch politischer Tumult. Oder Tumulte an den Börsen.

Keine Frage: Die Technologie, die es erlaubt und ermöglicht, Deepfakes herzustellen, ist hoch explosiv. Denn niemand kann wissen, wer, was damit anstellt. Wir müssen also genauer hinschauen, wenn wir Fotos präsentiert bekommen...“



*Wenn Jörg mal ins Weiße Haus einzieht...*

## **Kleine Hinweise für den Fake**

Noch enthalten die meisten Deepfake-Fotos kleine Unstimmigkeiten. Vor allem an Armen und Händen – wie hier bei Susanne. Die sehen unstimmig aus, manchmal fehlen Finger.

Auch gibt es oft sogenannte Artefakte. Kleine Störungen im Bild. Das sieht man aber erst, wenn man ganz genau hinschaut.

Es gibt schon Werkzeuge, die einem sagen, wie hoch die Wahrscheinlichkeit ist, dass ein Foto von KI erstellt wurde – oder eben doch von einem Menschen.

Wir müssen als Gesellschaft auf der Hut sein. Wir werden künftig aller Voraussicht nach überschüttet mit Deepfakes. Nicht nur Fotos. Auch Videos. Denn schon werden KI-Systeme öffentlich zugänglich, etwa **Dreamix**, die mehr oder weniger dasselbe auch für Videos ermöglichen. Es wird also noch wichtiger, alles zu hinterfragen, was man im Netz findet. Nicht nur Texte, auch Fotos und Videos.



*Hinweise für DeepFakes sind Störungen und Unzulänglichkeiten*

## Wie hoch ist eigentlich der Energieaufwand bei KI-Systemen?



**Wir alle reden aktuell viel von und über KI-Systeme wie ChatGPT oder Midjourney. Wir sind beeindruckt von der Leistungsfähigkeit - aber wie hoch ist eigentlich der damit verbundene Energieaufwand?**

Der Energieverbrauch von Künstlicher Intelligenz (KI) ist in den letzten Jahren aufgrund des exponentiellen Wachstums der KI-Modelle und der steigenden Anforderungen an Rechenleistung und Energie immer mehr in den Fokus gerückt. In diesem Beitrag werden wir ausführlich auf den Energieverbrauch von KI-Systemen eingehen, die Faktoren, die dazu beitragen, und die Auswirkungen auf die Umwelt und die Kosten.

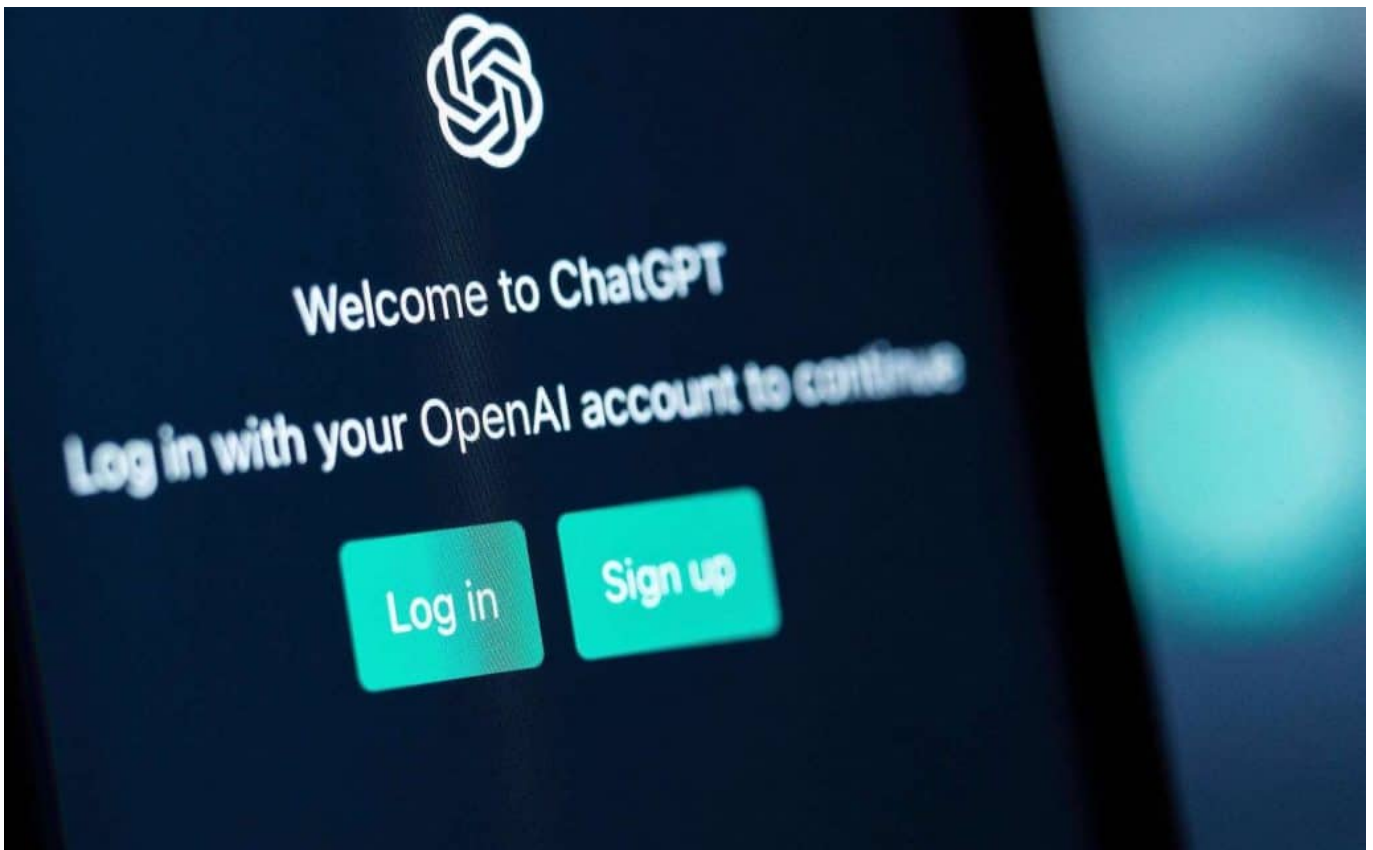
### **Größe und Komplexität der Modelle**

Eine der Hauptursachen für den hohen Energieverbrauch von KI-Systemen ist die Größe und Komplexität der Modelle. In den letzten Jahren haben KI-Forscher zunehmend größere und komplexere neuronale Netze entwickelt, um



anspruchsvollere Aufgaben zu bewältigen. Beispielsweise hatte GPT-3, das im Jahr 2020 veröffentlicht wurde, 175 Milliarden Neuronen, während sein Vorgänger GPT-2 nur 1,5 Milliarden Neuronen hatte.

Größere Modelle erfordern mehr Rechenleistung und Energie, um sowohl während des Trainings als auch bei der Anwendung effizient zu funktionieren. Das Training eines KI-Modells kann Tage, Wochen oder sogar Monate dauern, abhängig von der Größe des Modells und der verwendeten Hardware. Während dieser Zeit verbraucht das KI-System kontinuierlich Energie.



ChatGPT: Mit 100 Mio. Anwendern nach drei Monaten die am schnellsten wachsende App aller Zeiten

## Hardware und Infrastruktur

Der Energieverbrauch von KI-Systemen hängt auch von der verwendeten Hardware und Infrastruktur ab. KI-Modelle werden in der Regel auf leistungsfähigen Grafikprozessoren (GPUs) oder spezialisierten KI-Chips wie Tensor Processing Units (TPUs) trainiert. Diese Hardwarekomponenten sind speziell für parallele Rechenoperationen optimiert und bieten im Vergleich zu herkömmlichen CPUs eine höhere Energieeffizienz. Trotzdem verbrauchen sie

immer noch erhebliche Mengen an Energie, insbesondere wenn sie in großen Rechenzentren betrieben werden.

Rechenzentren, die für das Training und die Anwendung von KI-Systemen eingesetzt werden, verbrauchen ebenfalls erhebliche Mengen an Energie für Kühlung und Infrastruktur. Da KI-Systeme oft eine hohe thermische Last erzeugen, müssen Rechenzentren effektive Kühlungssysteme verwenden, um die Hardware vor Überhitzung zu schützen. Diese Systeme verbrauchen zusätzliche Energie, die zum Gesamtenergieverbrauch der KI-Systeme beiträgt.

## Energieverbrauch und Kosten

Es ist schwierig, präzise Zahlen zum Energieverbrauch und den Kosten von KI-Systemen zu nennen, da sie stark von der Größe des Modells, der verwendeten Hardware und der Dauer des Trainings abhängen. Allerdings können wir einige Schätzungen und Beispiele geben, um einen Eindruck von den Größenordnungen zu vermitteln.

Ein Beispiel ist das bereits erwähnte GPT-3 Modell von OpenAI. Schätzungen zufolge beliefen sich die Kosten für das Training von GPT-3 auf etwa 4,6 Millionen US-Dollar, wobei der Großteil dieser Kosten auf den enormen Energieverbrauch während des Trainings zurückzuführen ist. Um das Modell zu trainieren, wurden etwa 3.000 GPUs von Nvidia (V100) verwendet, die über mehrere Wochen laufen mussten.

Ein anderes Beispiel ist das Training von BERT, einem weit verbreiteten Modell für die Verarbeitung natürlicher Sprache. Forscher schätzten, dass das Training von BERT etwa 1.470 MWh an Energie verbrauchte, was dem durchschnittlichen Energieverbrauch von 126 US-amerikanischen Haushalten in einem Jahr entspricht.

Diese Beispiele zeigen, dass der Energieverbrauch von KI-Systemen erheblich sein kann, und sie veranschaulichen auch die steigenden Kosten, die mit der Entwicklung immer größerer und komplexerer Modelle verbunden sind.



*Snapchat führt einen KI-Chatbot ein: "My AI" soll zum neuen Freund der User werden*

## **Umweltauswirkungen und Reduzierung des Energieverbrauchs**

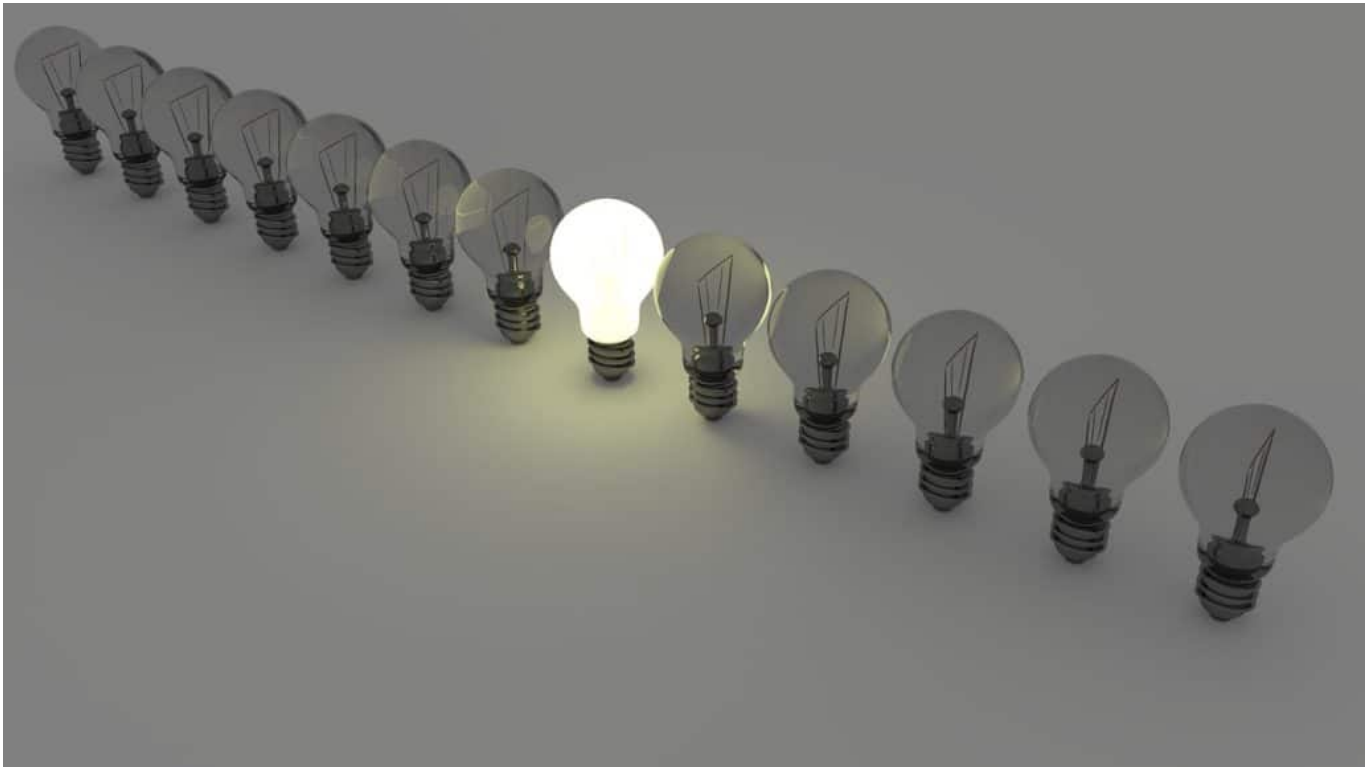
Der hohe Energieverbrauch von KI-Systemen wirft auch Fragen bezüglich der Umweltauswirkungen auf, insbesondere im Zusammenhang mit dem CO<sub>2</sub>-Ausstoß und dem Klimawandel. KI-Forschung und -Entwicklung sind in der Regel auf große Rechenzentren angewiesen, die einen bedeutenden Anteil an den weltweiten CO<sub>2</sub>-Emissionen haben.

Angesichts der wachsenden Bedenken um die Umwelt arbeiten Forscher und Unternehmen kontinuierlich daran, den Energieverbrauch von KI-Systemen zu reduzieren. Einige Ansätze zur Reduzierung des Energieverbrauchs sind:

1. **Effizientere Algorithmen und Architekturen:** Forscher entwickeln ständig neue Algorithmen und Modellarchitekturen, die weniger Energie verbrauchen, ohne die Leistung zu beeinträchtigen. Beispielsweise können Techniken wie Pruning oder Quantisierung dazu beitragen, die

Größe von neuronalen Netzen zu reduzieren und ihren Energieverbrauch zu verringern.

2. **Energieeffizientere Hardware:** Unternehmen wie Nvidia, Intel und Google entwickeln energieeffizientere GPUs, TPUs und andere spezialisierte KI-Chips, die weniger Energie verbrauchen als herkömmliche CPUs. Diese Chips können den Energieverbrauch von KI-Systemen weiter reduzieren, ohne ihre Leistung zu beeinträchtigen.
3. **Verteiltes Rechnen und Edge Computing:** Anstatt KI-Modelle in zentralisierten Rechenzentren zu trainieren, kann das Training auf mehrere Standorte oder Geräte verteilt werden, um den Energieverbrauch zu reduzieren. Edge Computing ermöglicht es, KI-Modelle näher an den Datenquellen auszuführen, wodurch der Energieverbrauch für Datenübertragung und -verarbeitung verringert werden kann.
4. **Nutzung erneuerbarer Energien:** Um den CO<sub>2</sub>-Fußabdruck von KI-Systemen zu reduzieren, können Rechenzentren erneuerbare Energien wie Solarenergie, Windkraft oder Wasserkraft nutzen. Viele große Unternehmen wie Google, Facebook und Amazon haben bereits angekündigt, ihre Rechenzentren auf erneuerbare Energien umzustellen, um ihre Umweltauswirkungen zu reduzieren.
5. **Energieeffiziente Kühlungssysteme:** Da Rechenzentren erhebliche Mengen an Energie für die Kühlung verbrauchen, ist die Entwicklung und Implementierung energieeffizienterer Kühlungssysteme ein weiterer Ansatz zur Reduzierung des Energieverbrauchs. Beispiele für innovative Kühltechnologien sind Flüssigkühlung, Freikühlung und die Verwendung von Wärmetauschern, um Abwärme effizient abzuleiten.
6. **Neuartige Trainingsmethoden:** Forscher untersuchen auch alternative Trainingsansätze wie "One-shot Learning" oder "Few-shot Learning", bei denen KI-Modelle mit weniger Daten und somit geringerem Rechenaufwand trainiert werden können. Diese Ansätze könnten dazu beitragen, den Energieverbrauch während des Trainings von KI-Systemen zu reduzieren.



## Fazit

Der Energieverbrauch von KI-Systemen ist ein wichtiges Thema, das sowohl aufgrund der steigenden Kosten als auch der Umweltauswirkungen Beachtung findet. Die Größe und Komplexität der Modelle, die verwendete Hardware und die Infrastruktur sind entscheidende Faktoren für den Energieverbrauch von KI-Systemen.

Während es schwierig ist, präzise Angaben zum Energieverbrauch und den Kosten zu machen, zeigen Beispiele wie GPT-3 und BERT, dass der Energieverbrauch von KI-Systemen erheblich sein kann. Um die Umweltauswirkungen und die Kosten zu reduzieren, arbeiten Forscher und Unternehmen kontinuierlich an der Entwicklung effizienterer Algorithmen, Hardware und Infrastrukturen sowie der Nutzung erneuerbarer Energien und innovativer Kühlungstechnologien.

In den kommenden Jahren werden wahrscheinlich weitere Fortschritte in der KI-Forschung und -Entwicklung erzielt, um den Energieverbrauch weiter zu reduzieren und die Nachhaltigkeit von KI-Systemen zu verbessern.

## 50 interessante Statistiken über ChatGPT



**Wir haben mal 50 wichtige und interessante Fakten über den derzeit meist diskutierten Chatbot ChatGPT zusammengetragen.**

ChatGPT ist ein fortschrittlicher Chatbot, der auf künstlicher Intelligenz und maschinellem Lernen basiert. Er wurde von OpenAI entwickelt und ist bekannt für seine Fähigkeit, menschenähnliche Antworten auf Fragen zu geben. Hier sind 50 interessante Statistiken über ChatGPT:

1. ChatGPT verwendet die GPT-3-Technologie, die aus 175 Milliarden Parametern besteht und derzeit als das größte NLP-Modell (Natural Language Processing) auf dem Markt gilt.
2. ChatGPT hat Zugang zu einer enormen Datenmenge, einschließlich Millionen von Artikeln und Texten, auf die er zugreifen kann, um Antworten auf Fragen zu generieren.
3. ChatGPT hat eine Erfolgsrate von 80%, wenn es darum geht,

- menschenähnliche Antworten auf Fragen zu geben.
4. Die durchschnittliche Länge der Antworten von ChatGPT beträgt etwa 50 Wörter.
  5. ChatGPT ist in der Lage, auf eine Vielzahl von Themen zu antworten, darunter Unterhaltung, Nachrichten, Wissenschaft, Geschichte, Politik und mehr.
  6. ChatGPT kann auch Bilder und Links einfügen, um Benutzern zusätzliche Informationen und Ressourcen zur Verfügung zu stellen.
  7. ChatGPT kann auch zur Generierung von Texten verwendet werden, z. B. für das Schreiben von Artikeln oder das Erstellen von Inhalten für soziale Medien.
  8. ChatGPT kann auch in anderen Sprachen als Englisch antworten, darunter Spanisch, Deutsch, Französisch und Chinesisch.
  9. ChatGPT wird kontinuierlich verbessert und weiterentwickelt, um noch präzisere und nützlichere Antworten auf Fragen zu geben.
  10. ChatGPT hat das Potenzial, den Kundenservice in verschiedenen Branchen zu verbessern und Prozesse zu automatisieren.
  11. ChatGPT kann als persönlicher Assistent für Benutzer dienen, indem er Termine vereinbart, Erinnerungen setzt und Aufgaben organisiert.
  12. ChatGPT kann in der Bildung eingesetzt werden, um Schülern Lerninhalte bereitzustellen und Fragen zu beantworten.
  13. ChatGPT kann im Gesundheitswesen eingesetzt werden, um Patientenfragen zu beantworten und Gesundheitsdaten zu sammeln, um die Diagnose und Behandlung von Krankheiten zu verbessern.
  14. ChatGPT kann im Finanzdienstleistungsbereich eingesetzt werden, um Kunden bei der Überweisung von Geldern zu unterstützen und Finanzdienstleistungen bereitzustellen.
  15. ChatGPT kann in der Logistik und im Verkehrswesen eingesetzt werden, um den Transport von Waren und Personen zu automatisieren.
  16. Die Anzahl der täglichen Interaktionen mit ChatGPT beträgt derzeit mehrere tausend.
  17. ChatGPT hat bereits über 100 Millionen Antworten auf Fragen generiert.
  18. Die beliebtesten Themen, auf die ChatGPT antwortet, sind Unterhaltung, Nachrichten, Wissenschaft und Technologie.
  19. ChatGPT hat in einer Testphase eine Genauigkeit von 98% bei der Beantwortung von Fragen gezeigt.
  20. ChatGPT hat eine durchschnittliche Reaktionszeit von unter einer Sekunde.
  21. ChatGPT kann auch Ironie und Sarkasmus erkennen und entsprechend

- darauf reagieren.
22. ChatGPT kann auch verschiedene Stimmlagen erkennen und die Antworten entsprechend anpassen.
  23. ChatGPT kann auch Emotionen erkennen und darauf reagieren, um eine menschenähnlichere Interaktion zu ermöglichen.
  24. Die meisten Benutzer von ChatGPT sind zwischen 18 und 34 Jahre alt.
  25. Die meisten Benutzer von ChatGPT sind männlich.
  26. ChatGPT hat das Potenzial, Arbeitsplätze in verschiedenen Bereichen zu automatisieren, einschließlich Kundenservice und Support.
  27. ChatGPT kann auch dazu beitragen, den Zeitaufwand und die Kosten für die Schulung von Kundenservice-Mitarbeitern zu reduzieren.
  28. ChatGPT kann auch dazu beitragen, die Kundenzufriedenheit zu verbessern, indem er schnelle und genaue Antworten auf Fragen gibt.
  29. ChatGPT kann auch dazu beitragen, die Effizienz von Prozessen zu verbessern, indem er automatisch auf Fragen und Anfragen reagiert.
  30. ChatGPT kann auch dazu beitragen, menschliche Fehler bei der Bearbeitung von Anfragen und Fragen zu reduzieren.
  31. ChatGPT kann auch dazu beitragen, die Markenbekanntheit zu verbessern, indem er Kunden schnell und effektiv unterstützt.
  32. ChatGPT kann auch dazu beitragen, die Datenqualität und -konsistenz zu verbessern, indem er automatisch auf Fragen und Anfragen reagiert.
  33. ChatGPT kann auch dazu beitragen, die Skalierbarkeit von Unternehmen und Organisationen zu verbessern, indem er automatisch auf Fragen und Anfragen reagiert.
  34. ChatGPT kann auch dazu beitragen, die Arbeitsbelastung von Kundenservice-Mitarbeitern zu reduzieren, indem er einfache Fragen und Anfragen automatisch beantwortet.
  35. ChatGPT kann auch dazu beitragen, die Betriebskosten von Unternehmen und Organisationen zu reduzieren, indem er die Notwendigkeit von menschlichen Kundenservice-Mitarbeitern reduziert.
  36. ChatGPT kann auch dazu beitragen, die Reaktionszeit auf Kundenanfragen und -fragen zu verbessern, indem er automatisch auf Fragen und Anfragen reagiert.
  37. ChatGPT kann auch dazu beitragen, die Effektivität von Marketing- und Vertriebsstrategien zu verbessern, indem er Kunden schnell und effektiv unterstützt.
  38. ChatGPT kann auch dazu beitragen, die Kundenbindung zu verbessern, indem er schnelle und genaue Antworten auf Fragen gibt.
  39. ChatGPT kann auch dazu beitragen, das Kundenerlebnis zu verbessern,



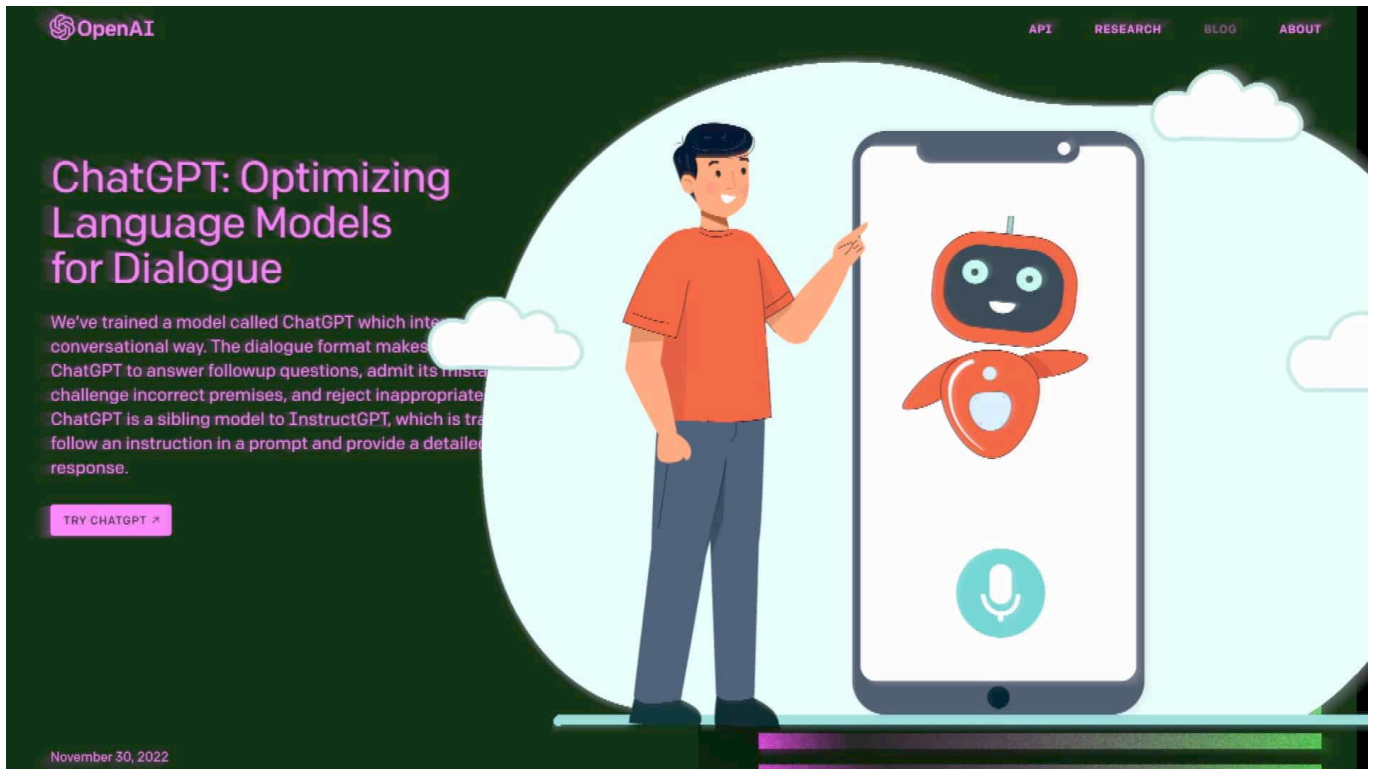
- indem er menschenähnliche Antworten auf Fragen gibt.
40. ChatGPT kann auch dazu beitragen, die Umsätze von Unternehmen und Organisationen zu steigern, indem er schnelle und effektive Kundenunterstützung bietet.
  41. ChatGPT kann auch dazu beitragen, die Produktivität von Mitarbeitern zu steigern, indem er einfache Fragen und Anfragen automatisch beantwortet.
  42. ChatGPT kann auch dazu beitragen, die Betriebszeit von Unternehmen und Organisationen zu erhöhen, indem er automatisch auf Fragen und Anfragen reagiert und somit eine kontinuierliche Kundenunterstützung ermöglicht.
  43. ChatGPT kann auch dazu beitragen, die Erfassung und Analyse von Kundendaten zu verbessern, indem er automatisch auf Fragen und Anfragen reagiert und somit wertvolle Informationen sammelt.
  44. ChatGPT kann auch dazu beitragen, die Qualität von Produkten und Dienstleistungen zu verbessern, indem er Kundenfeedback schnell und effektiv sammelt.
  45. ChatGPT kann auch dazu beitragen, die Benutzerfreundlichkeit von Produkten und Dienstleistungen zu verbessern, indem er schnelle und genaue Antworten auf Fragen gibt.
  46. ChatGPT kann auch dazu beitragen, die Effektivität von Schulungen und Schulungsprogrammen zu verbessern, indem er automatisch auf Fragen und Anfragen reagiert und somit eine schnellere und effektivere Schulung ermöglicht.
  47. ChatGPT kann auch dazu beitragen, die Barrierefreiheit von Produkten und Dienstleistungen zu verbessern, indem er Antworten auf Fragen in verschiedenen Sprachen und Stimmen bereitstellt.
  48. ChatGPT kann auch dazu beitragen, die Sicherheit von Produkten und Dienstleistungen zu verbessern, indem er Kundenfragen schnell und effektiv beantwortet und somit potenzielle Sicherheitsprobleme identifiziert und löst.
  49. ChatGPT kann auch dazu beitragen, die Geschwindigkeit von Geschäftsprozessen zu erhöhen, indem er automatisch auf Fragen und Anfragen reagiert und somit eine schnellere und effektivere Kommunikation ermöglicht.
  50. ChatGPT kann auch dazu beitragen, die Effektivität von Entscheidungsprozessen zu verbessern, indem er wertvolle Informationen sammelt und somit eine bessere Entscheidungsgrundlage bereitstellt.

Wow, was für eine Aufstellung - einige Fakten, die zusammengekommen sind bei der Recherche für mein neues Buch über ChatGPT.



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

## Warum gibt ChatGPT mitunter falsche Antworten?



**Der gefeierte Chatbot ChatGPT liefert meist erstaunlich gute Antworten oder sogar eloquente Erklärungen und Texte ab. Doch manchmal sind die Antworten schlicht falsch - warum?**

Der Chatbot ChatGPT kann aus verschiedenen Gründen manchmal falsche Antworten geben. Ich habe selbst einige Erklärungen dafür; wollte aber von ChatGPT selbst wissen, welche Gründe für falsche Antworten existieren. Das ist die Replik. :)

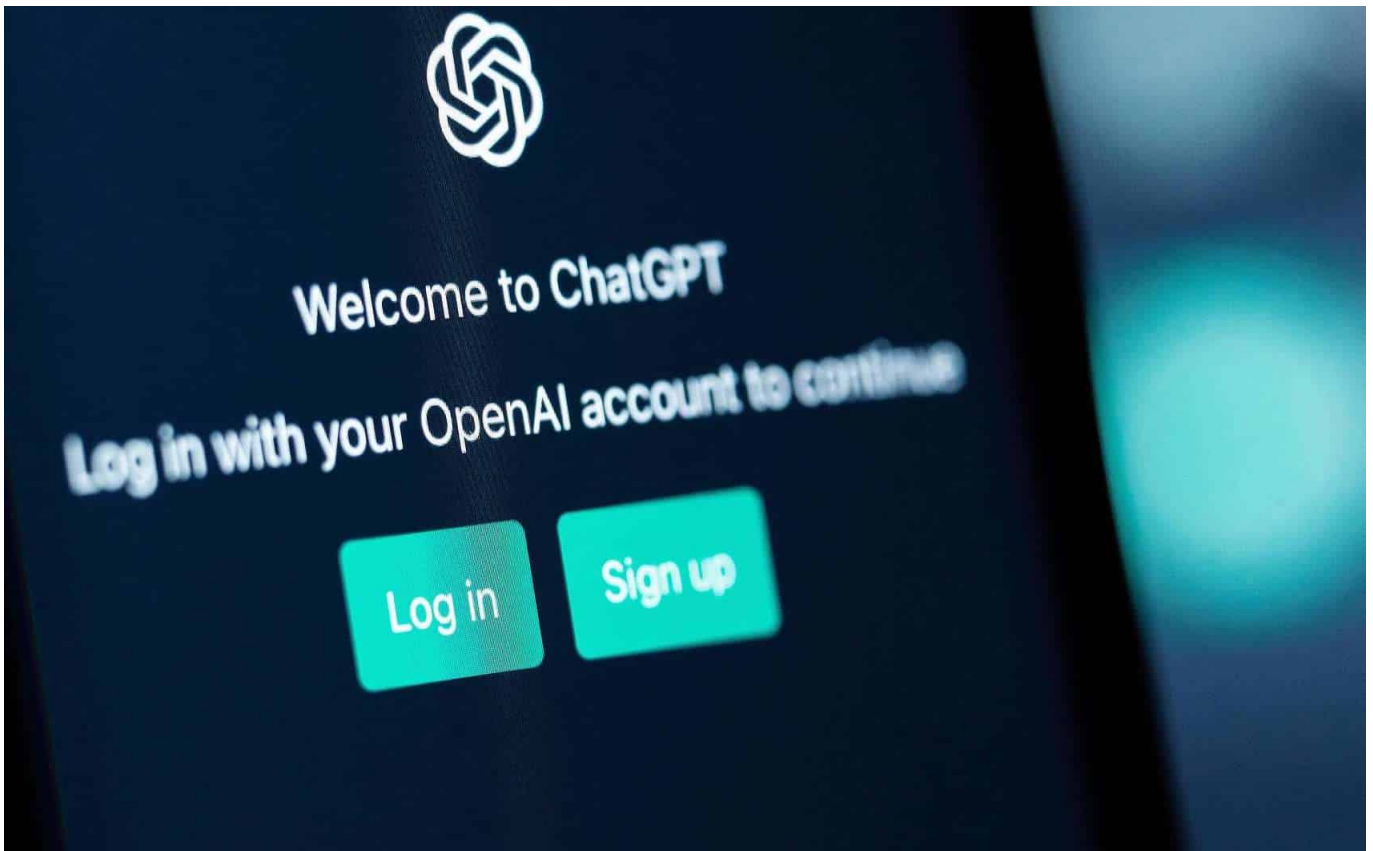
1. Trainingsdaten: ChatGPT wurde auf einer großen Menge von Textdaten aus dem Internet trainiert. Da diese Daten sowohl korrekte als auch falsche Informationen enthalten können, kann das Modell unbeabsichtigt inkorrekte Informationen erlernen und wiedergeben.
2. Ambiguität: Bei mehrdeutigen oder unklaren Fragen kann ChatGPT Schwierigkeiten haben, die genaue Absicht des Benutzers zu verstehen und eine angemessene Antwort zu liefern.
3. Wissenslücken: Da ChatGPT auf dem Stand von 2021 trainiert wurde, ist es möglich, dass das Modell keine aktuellen Informationen über bestimmte

Themen hat oder Veränderungen in bestimmten Bereichen nicht kennt.

4. Spekulation: Manchmal versucht ChatGPT, eine Antwort zu geben, auch wenn es keine ausreichenden Informationen hat. In solchen Fällen kann die KI spekulieren und eine ungenaue Antwort liefern.
5. Bestätigungsverzerrung: Während des Trainings kann ChatGPT Bestätigungsverzerrungen aus den Trainingsdaten lernen. Das bedeutet, dass es möglicherweise eher dazu neigt, eine bestimmte Art von Antwort zu geben, basierend auf den Mustern, die es in den Trainingsdaten beobachtet hat.

Die Forscher und Entwickler von OpenAI arbeiten kontinuierlich daran, die Genauigkeit und Qualität von ChatGPT zu verbessern, um solche Probleme zu minimieren und Benutzern verlässlichere und hilfreichere Antworten zu bieten.

## Chatbot ChatGPT in Italien gesperrt - Datenschutz im Fokus



**Italienische Behörden haben den Zugang zum populären Chatbot ChatGPT gesperrt. Begründung: Sorgen um den Datenschutz - und den Jugendschutz.**

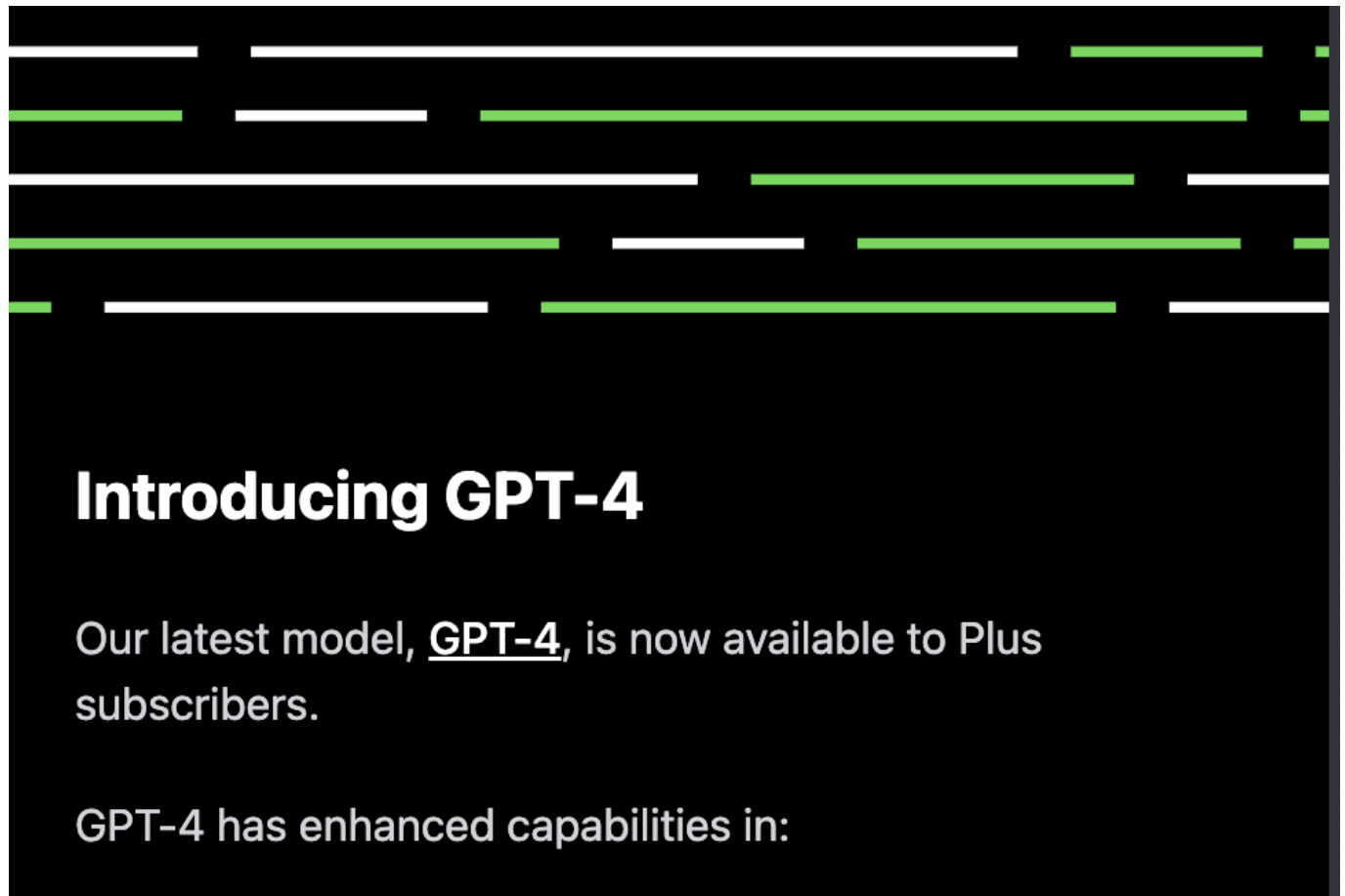
In Italien wurde jetzt der Zugang zum Chatbot ChatGPT gesperrt. "Mit sofortiger Wirkung", so die Behörde. Die Datenschutzbehörde des Landes kritisiert das Sammeln personenbezogener Daten sowie fehlenden Jugendschutz.

In einer Welt und einem Internet, wo Pornoseiten frei für alle zugänglich sind, erscheint mir zumindest das Jugendschutzargument wenig überzeugend.

Allerdings wirft der Fall durchaus ein Schlaglicht auf die zunehmende Bedeutung von Datenschutzfragen im Zusammenhang mit KI-Systemen und Chatbots.

Die italienische Behörde kritisiert vor allem, dass Betreiber OpenAI keine

Rechtsgrundlage für das massenhafte Sammeln und Speichern personenbezogener Daten habe - also keine Datenschutzbestimmungen und Nutzungsbedingungen. Darüber hinaus fehle es an Maßnahmen zu einem geeigneten Jugendschutz, so gebe es keine Alterskontrolle für Minderjährige (was auf so ziemlich alle Social Media Dienste ebenso zutrifft).



*Bei ChatGPT4 erfolgt keine Altersabfrage*

## Es drohen hohe Strafzahlungen

Das US-Unternehmen wurde aufgefordert, "innerhalb von 20 Tagen über ergriffene Maßnahmen zu informieren". Andernfalls drohe "eine Strafe von bis zu 20 Millionen Euro oder bis zu vier Prozent des Jahresumsatzes" nach geltendem EU-Recht.

Chatbots wie ChatGPT basieren auf künstlicher Intelligenz und werden immer häufiger eingesetzt, um Kundenanfragen und Supportanfragen zu bearbeiten. Dabei können sie in der Lage sein, aufgrund ihres Lernens und ihrer

Trainingsdaten menschenähnliche Antworten zu geben. Das macht sie zu einem effizienten und kostengünstigen Instrument für Unternehmen, um den Kundenservice zu verbessern.

Allerdings sind Chatbots auch mit Datenschutzproblemen verbunden. Da sie in der Regel auf große Datenmengen zugreifen und Informationen von Benutzern sammeln, besteht das Risiko, dass persönliche Daten in die falschen Hände geraten. In Italien hat die Datenschutzbehörde daher entschieden, ChatGPT zu sperren, weil sie Bedenken hinsichtlich der Sicherheit der von ihm gesammelten Daten hatte.



*ChatGPT wurde in Italien von Behörden gestoppt*

## **Datenschutz: Das nächste große Thema bei KI**

Diese Entscheidung zeigt, dass die Behörden zunehmend auf Datenschutzfragen achten und die Verwendung von KI-Systemen und Chatbots genauer überwachen. In Zukunft wird es wahrscheinlich noch mehr Regulierungen geben, um sicherzustellen, dass die Privatsphäre der Benutzer geschützt wird.



Unternehmen, die Chatbots einsetzen, müssen daher sicherstellen, dass ihre Systeme mit den geltenden Datenschutzvorschriften konform sind. Sie müssen sicherstellen, dass die Daten, die von ihren Chatbots gesammelt werden, sicher und geschützt sind und dass die Benutzer über die Verwendung ihrer Daten informiert werden.

Um dies zu erreichen, müssen Unternehmen auch sicherstellen, dass ihre Chatbots mit geeigneten Sicherheitsfunktionen ausgestattet sind. Dazu gehören Verschlüsselungstechnologien, um sicherzustellen, dass die Daten während der Übertragung sicher sind, sowie Funktionen zur Überwachung und zum Schutz von Datenbanken, die die gesammelten Daten speichern.

Letztendlich ist es wichtig, dass Unternehmen und Behörden gemeinsam daran arbeiten, die Sicherheit und den Datenschutz im Zusammenhang mit KI-Systemen und Chatbots zu verbessern. Nur so kann sichergestellt werden, dass diese Technologien ihr volles Potenzial entfalten können, ohne dass dabei die Privatsphäre der Benutzer gefährdet wird.

Es ist auch wichtig zu bedenken, dass Chatbots nicht nur im Bereich des Kundensupports eingesetzt werden können, sondern auch in anderen Bereichen wie Bildung, Gesundheitswesen und Finanzdienstleistungen. In diesen Bereichen können sie dazu beitragen, Prozesse zu automatisieren, den Informationsaustausch zu erleichtern und die Effizienz zu verbessern.

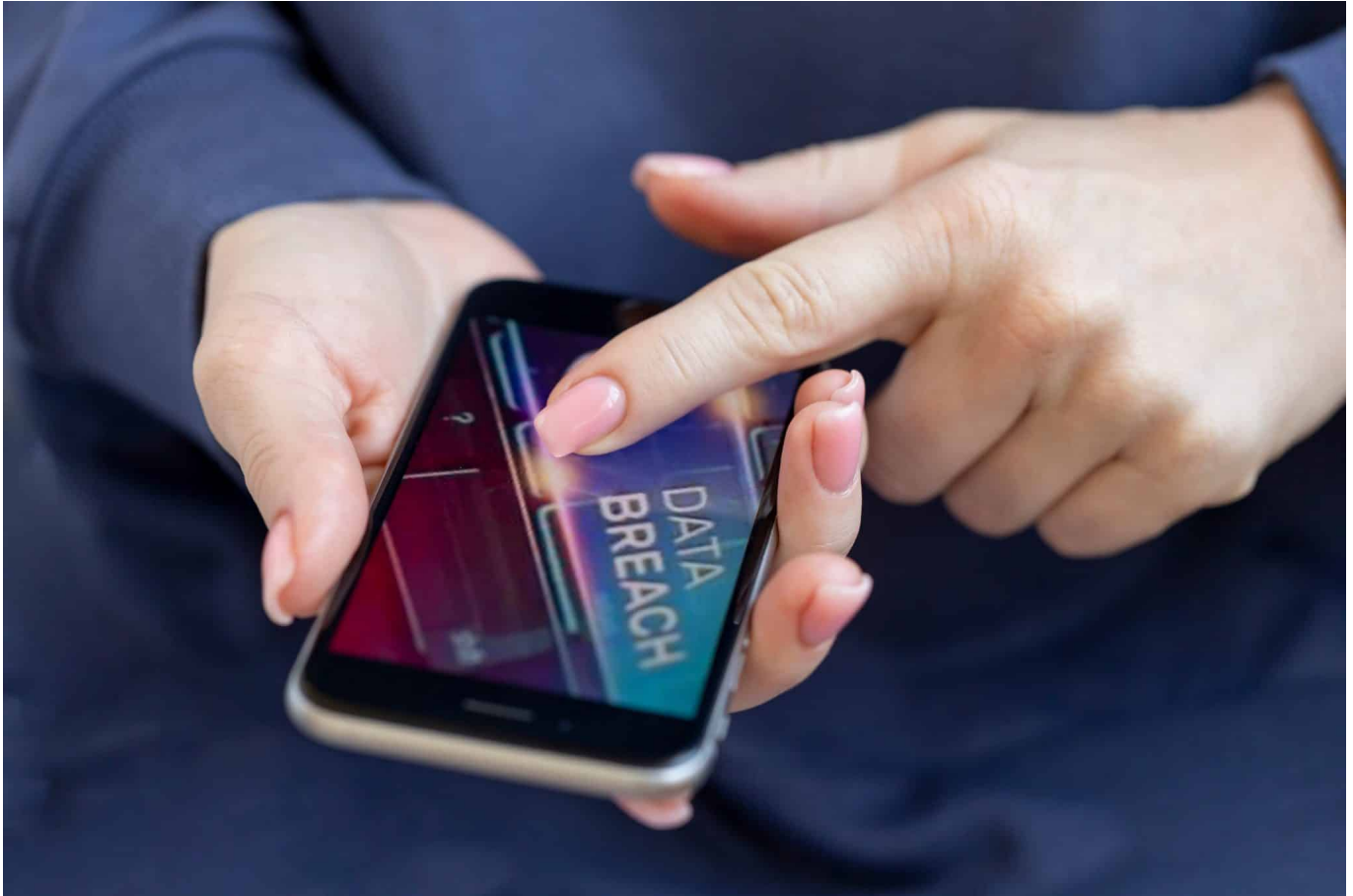
Im Bereich der Bildung können Chatbots beispielsweise verwendet werden, um Lerninhalte bereitzustellen und Schüler bei der Bearbeitung von Hausaufgaben zu unterstützen. Im Gesundheitswesen können sie dazu beitragen, Patientenfragen zu beantworten und Gesundheitsdaten zu sammeln, um die Diagnose und Behandlung von Krankheiten zu verbessern. Im Finanzdienstleistungsbereich können sie Kunden bei der Überweisung von Geldern unterstützen und Finanzdienstleistungen bereitstellen.

Um jedoch das volle Potenzial von Chatbots und KI-Systemen ausschöpfen zu können, müssen Unternehmen und Behörden sicherstellen, dass sie mit den geltenden Datenschutz- und Sicherheitsvorschriften konform sind. Die Benutzer müssen auch über die Verwendung ihrer Daten informiert werden und die Möglichkeit haben, ihre Einwilligung zur Verwendung ihrer Daten zu geben oder zu widerrufen.

Es gibt bereits Best Practices, die von Unternehmen und Organisationen befolgt werden können, um sicherzustellen, dass ihre Chatbots und KI-Systeme sicher und geschützt sind. Dazu gehört die Verwendung von sicherer Datenübertragung, die Implementierung von Zugangskontrollen und Sicherheitsüberwachungen, die Anonymisierung von Benutzerdaten, die Bereitstellung von Datenschutzrichtlinien und die Einrichtung von Datenschutzbeauftragten.

Insgesamt ist die Entwicklung von Chatbots und KI-Systemen ein wichtiger Schritt in Richtung Automatisierung und Effizienzsteigerung in verschiedenen Bereichen. Allerdings ist es auch wichtig, dass Unternehmen und Behörden den Datenschutz und die Sicherheit der Benutzer im Auge behalten und sicherstellen, dass diese Technologien in Einklang mit den geltenden Vorschriften und Best Practices eingesetzt werden. Nur so können wir das volle Potenzial von Chatbots und KI-Systemen ausschöpfen und gleichzeitig die Privatsphäre und den Schutz der Benutzer gewährleisten.

## Was ist eigentlich ein "Breach"?



**Wenn Cyberkriminelle Zugangsdaten, Passwörter oder sensible persönliche Daten entwenden, wird das gerne als "Breach" bezeichnet. Aber verbirgt sich genau hinter dem Begriff?**

Kaum ein Tag vergeht, an dem nicht von mittleren oder großen Raubzügen berichtet wird: Hacker und/oder Cyberkriminelle greifen unentwegt sensible Daten an, um sie kriminell zu missbrauchen. Ein Problem, denn Daten sind heutzutage die wertvollste Ressource für viele Unternehmen. Daher ist es von entscheidender Bedeutung, dass diese Daten sicher und geschützt sind.

### **Der Begriff "Breach"**

Ein "Breach" (engl. für "Durchbruch" oder "Bruch") bezieht sich auf den unbefugten Zugriff auf sensible oder vertrauliche Informationen. Ein Breach kann durch verschiedene Arten von Angriffen verursacht werden, wie zum Beispiel

durch Hacking, Phishing oder Malware-Infektionen.

Wenn ein Breach auftritt, können die Auswirkungen schwerwiegend sein, insbesondere wenn es um persönliche oder finanzielle Informationen geht. Betroffene können zum Beispiel Opfer von Identitätsdiebstahl werden oder finanzielle Verluste erleiden. Organisationen, die von einem Breach betroffen sind, können auch rechtliche und finanzielle Konsequenzen erfahren, wie z.B. Geldstrafen und einen Verlust des Vertrauens der Kunden und Partner.



*Oft stecken auch Hacker hinter einem Breach; Sie versuchen sich Zugang zu sensiblen Daten zu verschaffen*

## **Nicht immer stecken Hacker dahinter**

Es ist wichtig zu beachten, dass ein Breach nicht zwingend und auf eine feindliche Handlung (etwa gezielte Hackangriffe oder Einsatz von Malware) zurückzuführen ist. Manchmal kann ein Breach durch menschliches Versagen verursacht werden, wie z.B. durch den Verlust oder Diebstahl von Geräten, die vertrauliche Informationen enthalten. Ein weiterer Faktor, der Breaches

verursachen kann, ist mangelnde Sicherheitsmaßnahmen, wie z.B. das Fehlen von Verschlüsselungstechnologien oder unzureichende Passwortsicherheit.

Um einen Breach zu vermeiden, ist es wichtig, angemessene Sicherheitsmaßnahmen zu ergreifen, wie z.B. den Einsatz von Verschlüsselungstechnologien, starke Passwörter, regelmäßige Sicherheitsüberprüfungen und Schulungen für Mitarbeiter zum Thema Datensicherheit. Es ist auch wichtig, im Falle eines Breach schnell zu handeln, um den Schaden zu minimieren und die betroffenen Personen zu informieren.

## **Gefährlich: Zugangsdaten futsch**

Eine der häufigsten Arten von Breaches ist der Verlust von Zugangsdaten, wie z.B. Benutzernamen und Passwörtern. Oft werden diese Daten gestohlen, indem Hacker Schwachstellen in Systemen oder Anwendungen ausnutzen oder Phishing-E-Mails verwenden, um Benutzer zur Preisgabe ihrer Anmeldedaten zu verleiten. Sobald ein Angreifer Zugriff auf diese Daten hat, kann er sie verwenden, um auf geschützte Ressourcen zuzugreifen und weitere Angriffe auszuführen.

Ein weiterer häufiger Typ von Breach ist der sogenannte "Malware-Breach". Hierbei handelt es sich um eine Infektion von Computern oder Netzwerken durch Malware-Software, die es einem Angreifer ermöglicht, unbefugten Zugriff auf vertrauliche Daten zu erhalten. Malware kann über verschiedene Kanäle verbreitet werden, wie z.B. E-Mail-Anhänge, infizierte Websites oder USB-Sticks. Sobald die Malware installiert ist, kann sie verschiedene Aktionen durchführen, wie z.B. die Übertragung von vertraulichen Informationen an den Angreifer oder die Kontrolle des betroffenen Systems.

Ein weiterer Typ von Breach ist der sogenannte "Physical-Breach". Hierbei handelt es sich um den physischen Zugang zu einem System oder einem Raum, der vertrauliche Informationen enthält. Ein Physical-Breach kann durch den Diebstahl oder Verlust von Geräten wie Laptops oder Smartphones verursacht werden, die vertrauliche Informationen enthalten. Es kann auch durch den Einbruch in ein Büro oder ein Lager verursacht werden, in dem sensible Daten aufbewahrt werden.



*Wenn man einen Breach bemerkt, ist es meistens schon zu spät*

## Sicherheitsvorkehrungen

Um Breaches zu verhindern, ist es wichtig, dass Organisationen eine umfassende Sicherheitsstrategie umsetzen. Dazu gehören Maßnahmen wie:

1. Zugangsbeschränkungen: Nur autorisierte Benutzer sollten Zugriff auf geschützte Ressourcen haben. Es ist wichtig, sicherzustellen, dass Passwörter regelmäßig geändert werden und dass die Zugangsdaten sicher aufbewahrt werden.
2. Verschlüsselung: Durch die Verschlüsselung von Daten können sie vor

unbefugtem Zugriff geschützt werden. Es ist wichtig, dass Organisationen eine starke Verschlüsselungstechnologie verwenden, um sicherzustellen, dass Daten auch im Falle eines Breaches geschützt bleiben.

3. Schulung von Mitarbeitern: Mitarbeiter sollten regelmäßig in Bezug auf Datensicherheit geschult werden, um sicherzustellen, dass sie sich bewusst sind, wie sie vertrauliche Informationen schützen können.
4. Sicherheitsüberprüfungen: Organisationen sollten regelmäßig Sicherheitsüberprüfungen durchführen, um Schwachstellen in ihren Systemen zu identifizieren und zu beheben, bevor sie ausgenutzt werden können.
5. Incident Response Plan: Organisationen sollten einen Incident Response Plan haben, um schnell und effektiv auf einen Breach reagieren zu können. Der Plan sollte detaillierte Schritte enthalten, die bei einem Breach unternommen werden müssen, um den Schaden zu minimieren und die betroffenen Personen zu informieren.

Insgesamt ist ein Breach eine ernsthafte Bedrohung für die Datensicherheit und kann schwerwiegende Folgen haben. Es ist wichtig, dass Organisationen angemessene Sicherheitsmaßnahmen ergreifen, um Breaches zu verhindern, und einen Incident Response Plan haben, um schnell und effektiv auf einen Breach zu reagieren, falls dieser auftritt.

[embedyt] <https://www.youtube.com/watch?v=mEsDEVAgUKg>[/embedyt]

## Outlook: Termineinladungen richtig nutzen



**Termine an riesige Teilnehmerkreise: Da explodiert schnell Eure Inbox, wenn alle Zu- oder Absagen. Das könnt Ihr verhindern. Und trotzdem noch nachvollziehen, wie welcher Teilnehmer reagiert hat.**

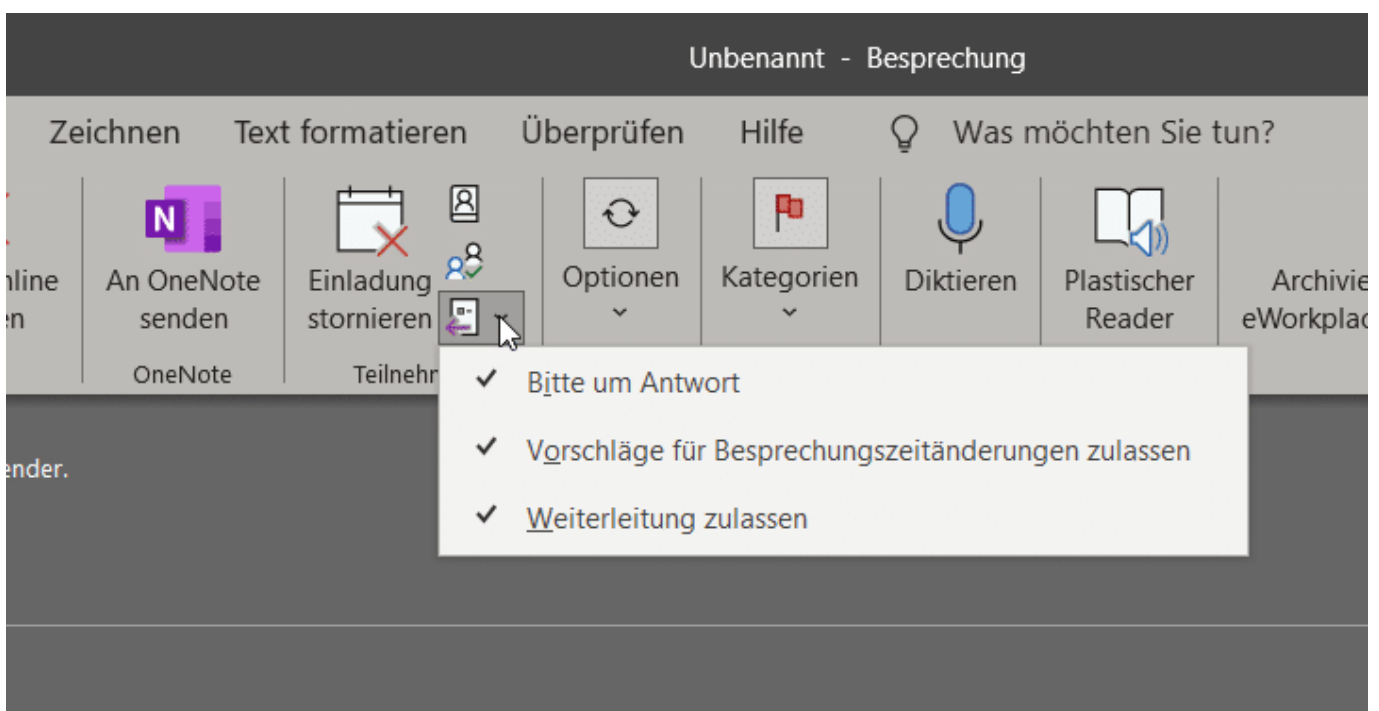
### Versand von Terminen ohne Rückmeldung

Der Papierkalender ist tot: Es lebe die elektronische Terminverwaltung! Jeder Online-Dienst (wie [Google](#), [Outlook](#) etc.) hat neben dem E-Mail-Posteingang auch einen [Kalender](#), den Ihr im Zuge der Synchronisation auf Smartphone, Tablet und PC bringen könnt. Damit seid Ihr immer synchron und verpasst keinen Termin mehr. Allerdings ist der effektive Umgang mit Terminen abhängig von einigen Voraussetzungen. Frei nach dem Motto "Wie man in den Wald hineinruft".

- Wenn Ihr einen neuen Termin versendet, dann fordert Ihr im Standard vom Empfänger eine Rückmeldung ein.



- Viele Programme zeigen diese auch als RVSP (aus dem Französischen stammende Schriftformel für *répondez s'il vous plaît, bitte antworten Sie*) an.
- Das macht bei Terminen mit kleiner Teilnehmerrunde Sinn, wenn Ihr aber viele Teilnehmer einladet, dann platzt irgendwann Eure Mailbox vor Zu- und Absagen. In einem solchen Fall macht es Sinn, die Terminbestätigung einfach nicht anzufordern.
- Das geht ganz einfach: Klickt im Termin im Symbolleistenbereich **Teilnehmer** auf das kleine Symbol **Antwortoptionen** > **Bitte um Antwort** und entfernt den Haken.
- Damit könnt Ihr immer noch die Antworten der Eingeladenen sehen und habt einen Überblick über den Termin, die Antwortmails bleiben aber aus.
- Eine weitere Alternative ist, den [Versand der Termineinladung zu verzögern](#), dass sie erst dann rausgeht, wenn die Antworten Euch nicht mehr stören.



## Wer hat wie geantwortet?

Die E-Mail, die die Rückmeldung zu einem Termin enthält, ist am Ende nichts anderes als ein Zusatzbonus. Wenn Ihr die zum Wohle Eures [Posteingangs](#) ausgeschaltet habt, dann macht das nicht: Tatsächlich ist sie direkt im Termin gespeichert. Ihr könnt jederzeit darauf zugreifen.

- Öffnet den Termin in Outlook durch einen Doppelklick, dann klickt auf **Anzeigen > Status**.
- Outlook öffnet nun die Übersicht der Teilnehmer, ihre Rolle (erforderlicher oder optionaler Teilnehmer) und die Rückmeldung, die jeder Teilnehmer gegeben hat.

- Ist die Rückmeldung **Keine**, dann macht es gegebenenfalls Sinn, noch einmal nachzufragen. In diesem Fall hat der Teilnehmer gar nicht reagiert. Da liegt es nahe, dass die Termineinladung an ihm vorbeigegangen ist.

Auf die Besprechungsanfrage erhaltene Antworten:

<input type="checkbox"/>	Name	Anwesenheit	Antwort
<input checked="" type="checkbox"/>	<a href="#">Eric, Andreas</a>	Besprechungsorganisator	Keine
<input type="checkbox"/>	<a href="#">andreas@aerl...</a>	Erforderlicher Teilnehmer	Zugesagt
<input checked="" type="checkbox"/>	<a href="#">support@worldof...</a>	Erforderlicher Teilnehmer	Keine
<input type="text" value="Hier einen Namen hinzufügen"/>			

## Twitter legt Teile des Quellcode offen



**Nun ist es also so weit: Twitter hatte angekündigt, Teile seines Quellcodes offenzulegen. Jetzt kann jeder sehen, nach welchen Kriterien der Algorithmus einzelne Postings pusht oder unterdrückt. Twitter ruft sogar zur Mitarbeit auf!**

Twitter hat kürzlich angekündigt, dass es einige Teile seines Quellcodes öffentlich zugänglich gemacht hat. Aber was bedeutet das eigentlich?

Der Quellcode ist der Programmiercode, der die Grundlage für eine Software bildet. Wenn man den Quellcode einer Software hat, kann man verstehen, wie sie funktioniert und gegebenenfalls Änderungen vornehmen (oder auch Sicherheitslücken ausnutzen).

Es gibt prinzipiell zwei Arten, mit seinem Quellcode umzugehen. Entweder, man hält ihn gut unter Verschluss (Closed Source), dann können nur Mitarbeiter reinsehen. Oder man stellt den Programmcode der Öffentlichkeit zur Verfügung, damit jeder sich einen Eindruck davon machen, ob es versteckte Funktionen gibt und/oder ob mit den Daten sorgfältig umgegangen wird. Beide Prinzipien haben Vor- und Nachteile.

Twitter hat jetzt einige Teile seines Quellcodes für die Öffentlichkeit zugänglich gemacht. Vor allem jenen Teil, der für die Entscheidungen verantwortlich ist, was auf der Timeline erscheint. Was bedeutet, dass jeder, der daran interessiert ist, den Code lesen und verstehen kann.

## Mehr Transparenz

Warum hat Twitter das getan und den Quellcode [hier bei Github für alle öffentlich zugänglich gemacht](#)? Einer der Gründe ist, dass Twitter sich für mehr Transparenz und Zusammenarbeit einsetzt. Wenn der Quellcode öffentlich zugänglich ist, kann jeder Entwickler Vorschläge für Änderungen einreichen oder sogar selbst Änderungen vornehmen. Das könnte dazu beitragen, dass Twitter-Features verbessert und die Software insgesamt stabiler und sicherer wird.

Außerdem könnte das Öffnen des Quellcodes für mehr Innovation sorgen. Entwickler können Ideen für neue Funktionen oder Anwendungen basierend auf dem Twitter-Quellcode entwickeln und diese der Twitter-Community zur Verfügung stellen.



*Elon Musk und Twitter: Eine Posse, die politische Schwäche zum Vorschein bringt*

## Auch ein Sicherheitsrisiko?

Natürlich gibt es auch Risiken bei der Offenlegung von Quellcode. Wenn jemand eine Sicherheitslücke im Code entdeckt, könnte er diese ausnutzen und dadurch Schaden anrichten. Aber Twitter hat angekündigt, dass es sorgfältig überwachen wird, wer auf den Code zugreift und Änderungen vornimmt, um sicherzustellen, dass die Sicherheit der Software gewährleistet bleibt.

Insgesamt könnte das Öffnen von Teilen des Quellcodes für Twitter eine positive Veränderung bedeuten. Mehr Transparenz und Zusammenarbeit könnten dazu beitragen, dass die Software verbessert wird und mehr Innovation entsteht