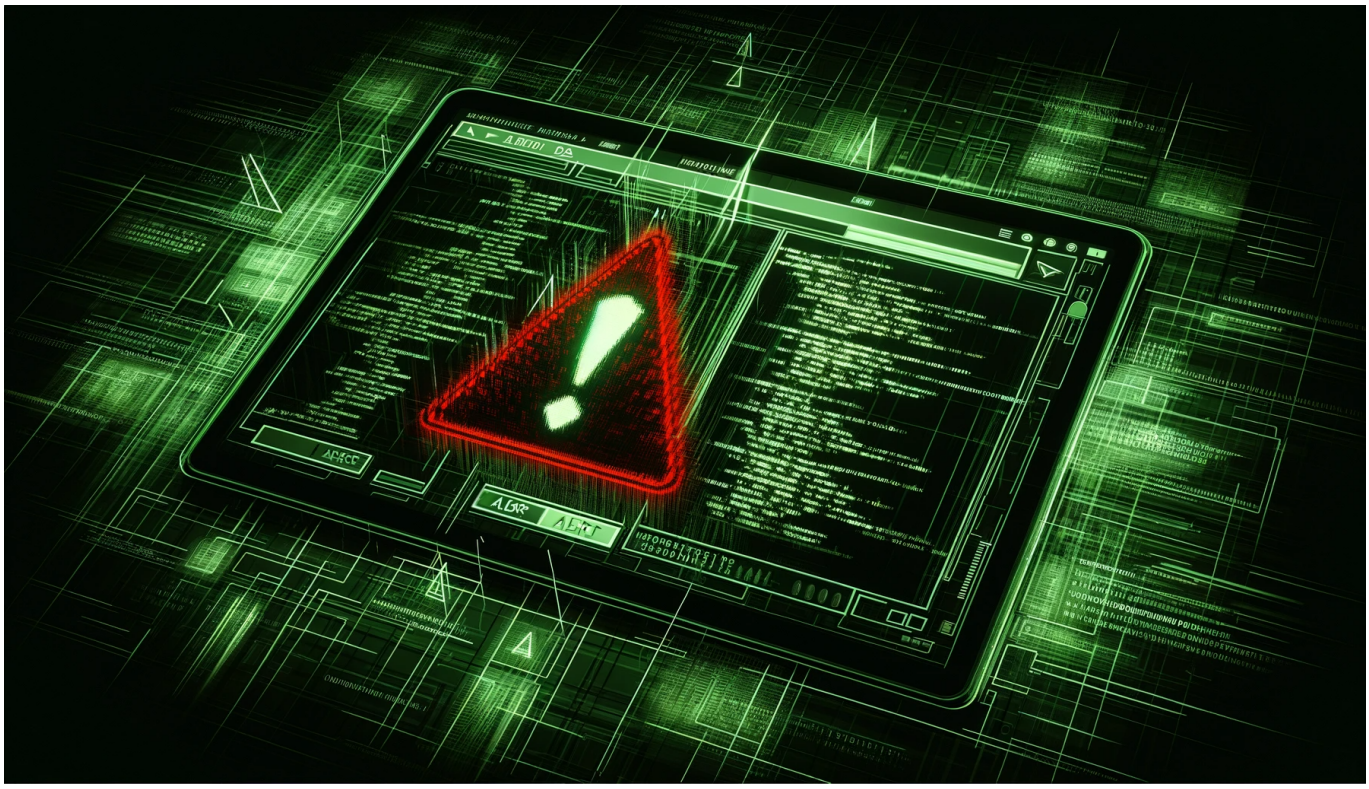
Schieb Report

Ausgabe 2024.04

Zero Day Exploits: Das unsichtbare Einfallstor für Cyberangriffe



Wir hören und lesen täglich von neuen Sicherheitslecks: Dann müssen wir Betriebssystem oder Software aktualisieren - und alles ist gut. Doch besonders gefährlich sind "Zero Day Exploits": Dafür gibt es (noch) keine Gegenmaßnahmen.

Sogenannte **Zero-Day Exploits** sind per Definition hochriskante Sicherheitslücken in Software, die von Angreifern ausgenutzt werden können, noch bevor der Hersteller davon Kenntnis hat.

Diese unsichtbaren Einfallstore ermöglichen es Hackern, unbemerkt in Systeme einzudringen und vertrauliche Daten zu stehlen oder Schaden anzurichten. Um Unternehmen vor solchen Angriffen zu schützen, ist ein umfassender Schutz und regelmäßiges Patchen von Schwachstellen von entscheidender Bedeutung.

Nur durch proaktive Sicherheitsmaßnahmen und eine ständige Überwachung können sich Unternehmen effektiv vor Zero-Day-Exploits und anderen Cyberbedrohungen schützen.

Hacker in aller Welt stürzen sich auf Zero Day Exploits

Was genau sind Zero Day Exploits?

Zero Day Exploits sind zweifellos ein ernstzunehmendes Thema in der Welt der Cyberkriminalität. Sie stellen eine unsichtbare Bedrohung dar und ermöglichen es Angreifern, unbemerkt in Systeme einzudringen und Schaden anzurichten.

Ein Zero Day Exploit bezieht sich auf eine Sicherheitslücke oder Schwachstelle in Software, die von den Herstellern noch nicht erkannt oder behoben wurde. Diese Schwachstellen werden von Cyberangreifern (unter anderem auch Regierungen) ausgenutzt, um unautorisierten Zugriff zu erlangen und schädlichen Code einzuschleusen.

Der Name "Zero Day" bedeutet, dass die Entdecker dieses Exploits null Tage Zeit haben, um sich vor dem Angriff zu schützen - es gibt praktisch keine Vorwarnung. Das macht Zero Day Exploits besonders gefährlich für Unternehmen und Privatpersonen, da sie oft ohne erkennbare Spuren hinterlassen werden können.

Die Bedeutung von Zero Day Exploits in der Cyberkriminalität

Durch Zero Day Exploits wird es den Hackern möglich, ihre Angriffe erfolgreich durchzuführen, ohne dass Unternehmen oder Privatpersonen im Voraus über die Bedrohungen informiert sind.

Die Auswirkungen solcher Angriffe können verheerend sein und großen Schaden anrichten. Unternehmen stehen vor der Herausforderung, ihre Systeme effektiv gegen derartige Zero-Day-Exploits zu schützen, da traditionelle Sicherheitsmaßnahmen oft nicht ausreichen, um diesen unsichtbaren Einfallstoren standzuhalten.

Es ist daher von großer Bedeutung für Hersteller und Security-Experten, kontinuierlich nach neuen sicherheitsrelevanten Schwachstellen zu suchen und entsprechende Updates bereitzustellen, um potentielle Zero-Day-Angriffe abzuwehren. Eine enge Zusammenarbeit zwischen Unternehmen und Sicherheitsexperten ist unerlässlich, um proaktiv gegen diese Bedrohung vorzugehen und einen effektiven Schutz zu gewährleisten.

Wie funktionieren Zero Day Exploits?

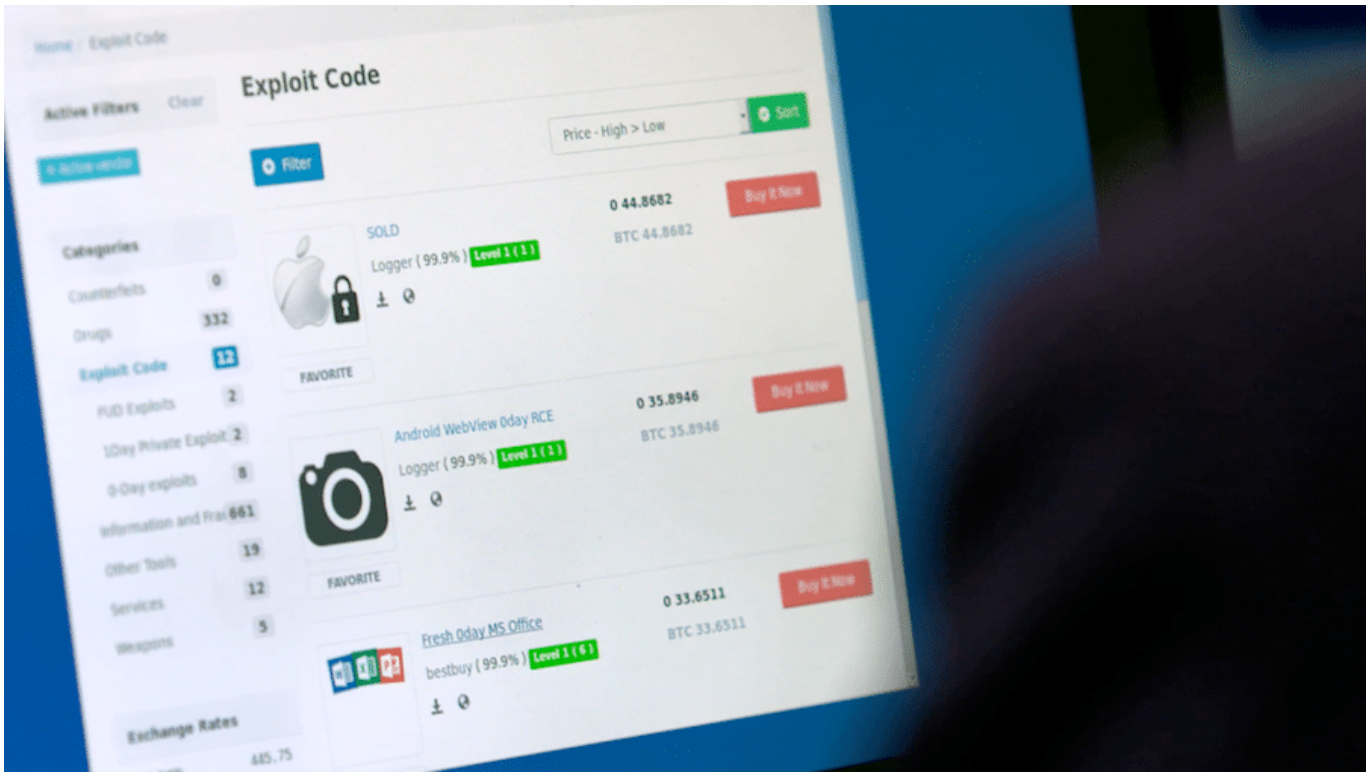
Die größte Herausforderung: Im Gegensatz zu anderen Schwachstellen sind Zero Day Exploits den Herstellern noch nicht bekannt, daher existiert (noch) kein Patch

oder Schutzmechanismus dagegen. Das erschwert den Schutz dagegen oder macht ihn sogar unmöglich.

Der Begriff "Zero Day" bezieht sich auf die Tatsache, dass zwischen der Entdeckung einer Sicherheitslücke und dem ersten erfolgreichen Angriff keine Zeit vergeht. Die Hacker nutzen diese kurze Zeitspanne aus, um unerkannt ihre Ziele anzugreifen. Um Zero Day Exploits erfolgreich durchzuführen, müssen die Angreifer tiefgreifende Kenntnisse über die Software haben und gezielt nach bisher unbekannten Schwachstellen suchen. Sobald sie eine solche Schwachstelle gefunden haben, entwickeln sie einen speziellen Code (**Exploit**), der es ihnen ermöglicht, Kontrolle über das angegriffene System zu erlangen.

Entscheidend ist auch, dass Hersteller von Software regelmäßig Updates bereitstellen, um bekannte Sicherheitslücken zu schließen und potenziellen Zero Day Exploits vorzubeugen. Zusätzlich sollten auch Nutzer ihre Systeme stets auf dem neuesten Stand halten und Vorsicht walten lassen beim Öffnen unbekannter E-Mails oder dem Besuch unsicherer Websites.

Ein umfassender Schutz gegen diese Art von Angriffen erfordert eine Kombination aus technischen Maßnahmen, wie z.B. Firewalls und Intrusion Detection Systemen, sowie einer regelmäßigen Sensibilisierung der Mitarbeiter für Sicherheitsthemen. Nur durch ein ganzheitliches Sicherheitskonzept können Unternehmen und Privatpersonen effektiv vor Zero Day Exploits geschützt werden.



Zero Day Exploits werden im Darknet zum Kauf angeboten

Bekannte Beispiele für erfolgreiche Zero Day Exploits

Im Laufe der Zeit gab es bereits einige bekannte Beispiele für (teilweise sehr) erfolgreiche Zero Day Exploits, die deutlich machen, wie gefährlich diese Angriffe sein können.

Ein solches Beispiel ist der Fall Stuxnet im Jahr 2010. Dieser Zero Day Exploit wurde gezielt gegen das iranische Atomprogramm eingesetzt und galt als besonders raffiniert. Die Angreifer nutzten mehrere bisher unbekannte Schwachstellen in der Industriesteuerungssoftware aus, um sich Zugang zu den Zentrifugen zur Urananreicherung zu verschaffen.

Dadurch konnten sie erheblichen Schaden anrichten und den Fortschritt des Atomprogramms empfindlich stören.

Ein weiteres bekanntes Beispiel ist der Zero Day Exploit mit dem Namen WannaCry im Jahr 2017. Dieser Angriff richtete sich vor allem gegen Unternehmen weltweit und verursachte einen immensen wirtschaftlichen Schaden. WannaCry nutzte eine Sicherheitslücke im Betriebssystem Windows aus, die zuvor vom Hersteller nicht gepatcht worden war.

Durch das Verschlüsseln von Daten erpressten die Angreifer Lösegeldzahlungen von den betroffenen Unternehmen. Diese Beispiele verdeutlichen die Gefahren von Zero Day Exploits und zeigen, dass sowohl große Organisationen als auch individuelle Nutzer gefährdet sind.

Zero Day Exploits sind eine ernstzunehmende Bedrohung in der digitalen Welt. Nur durch eine konsequente Zusammenarbeit zwischen Unternehmen, Herstellern und Nutzern kann effektiver Schutz gegen diese Angriffe gewährleistet werden.

Die Auswirkungen von Zero Day Exploits auf Unternehmen und Privatpersonen

Keine Frage: Für Unternehmen können die Auswirkungen von Zero Day Exploits verheerend sein. Hacker haben so die Möglichkeit, sensible Daten zu "stehlen" (also auszulesen) oder sogar ganze Netzwerke lahmzulegen. Besonders "beliebt" sind derzeit Ransomware-Angriffe,

Das kann nicht nur finanzielle Verluste zur Folge haben, sondern auch das Vertrauen der Kunden erschüttern und den Ruf eines Unternehmens nachhaltig

schädigen.

Aber auch Privatpersonen sind keineswegs vor Zero Day Exploits sicher. Durch gezielte Angriffe auf persönliche Geräte können Angreifer Zugang zu sensiblen Informationen wie Bankdaten oder Passwörtern erhalten, auch über das Smartphone. Identitätsdiebstahl und finanzielle Schäden sind möglich.

Um sich gegen diese Angriffe zu schützen, ist ein umfassender Sicherheitsansatz notwendig. Es ist wichtig, regelmäßige Updates und Patches für alle verwendeten Softwaresysteme durchzuführen sowie starke Passwörter zu verwenden und sie regelmäßig zu ändern. Auch Sicherheitslösungen wie Firewalls und Antivirenprogramme können helfen.

Die Bekämpfung von Zero Day Exploits erfordert ein Zusammenspiel von Herstellern, Sicherheitsfirmen und Anwendern. Durch eine kontinuierliche Überwachung und regelmäßige Aktualisierung der Software können potenzielle Schwachstellen schneller identifiziert und behoben werden.

Gleichzeitig müssen Unternehmen und Privatpersonen sich ihrer Verantwortung bewusst sein, ihre Systeme zu schützen und aktiv auf Sicherheitswarnungen zu reagieren. Insgesamt ist es unerlässlich, die Auswirkungen von Zero Day Exploits auf Unternehmen und Privatpersonen ernst zu nehmen.

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

Schutzmaßnahmen gegen Zero Day Exploits

Ein erster wichtiger Schritt besteht darin (und es ist wirklich elementar), die Software auf dem neuesten Stand zu halten. Hersteller veröffentlichen regelmäßig Updates und Patches, die Schwachstellen beheben können. Es ist daher ratsam, diese Aktualisierungen immer zeitnah zu installieren.

Unternehmen und Privatpersonen sollten ihre Netzwerke und Systeme mit einer robusten Sicherheitslösung ausstatten. Eine Firewall kann dabei helfen, verdächtigen Datenverkehr abzuwehren und unauthorisierte Zugriffe zu blockieren (eher in Unternehmen sinnvoll).

Ein weiterer sehr wichtiger Aspekt ist die Sensibilisierung der Mitarbeiter für potentielle Gefahren. Schulungen zum Thema IT-Sicherheit können dazu beitragen, dass Mitarbeiter Phishing-Angriffe erkennen und keine unsicheren Links oder Anhänge öffnen.

Zusätzlich zur Prävention ist es wichtig, ein effektives **Incident Response-Team** einzurichten. Das sollte im Falle eines Zero-Day-Exploits schnell handeln können, um den Angriff einzudämmen und möglichen Schaden zu begrenzen. Etwa, indem Backups angefertige und bei Bedarf wieder eingespielt werden.

Es gibt allerdings kein absolutes Maß an Sicherheit. Zero-Day-Exploits sind schwer vorhersehbar und können selbst bei optimaler Vorsorge auftreten.

Daher sollten Unternehmen auch über einen Notfallplan und Backup-Systeme verfügen, um im Ernstfall schnell reagieren zu können. Es ist wirklich unerlässlich, Schutzmaßnahmen gegen Zero-Day-Exploits zu ergreifen. Mit einer Kombination aus regelmäßigen Software-Updates, einer starken Sicherheitslösung, Mitarbeiter-Schulungen und einem gut organisierten Incident Response-Team können Unternehmen und Privatpersonen ihre Systeme bestmöglich schützen.

Russische Hacker greifen gezielt westliche Infrastruktur an

Aktuelle Entwicklungen in der Erforschung und Abwehr von Zero Day Exploits

Die rasante Weiterentwicklung von Technologien eröffnet auch Hackern immer wieder neue Möglichkeiten, Schwachstellen in Software aufzuspüren und für ihre Angriffe auszunutzen. Hersteller stehen vor der Herausforderung, ihre Produkte kontinuierlich zu verbessern, um solche Sicherheitslücken zu schließen.

Dabei arbeiten sie eng mit Sicherheitsexperten zusammen, um Zero Day Exploits frühzeitig zu erkennen und Gegenmaßnahmen zu entwickeln. Ein wichtiger Aspekt bei der Erforschung von Zero Day Exploits ist das Verständnis des Codes hinter den Angriffen. Nur durch eine genaue Analyse des Exploits können Sicherheitsexperten effektive Schutzmaßnahmen entwickeln.

Forscher suchen daher aktiv nach neuen Methoden zur Erkennung und Entschärfung solcher Angriffe. Aber auch Unternehmen spielen eine entscheidende Rolle bei der Abwehr von Zero Day Exploits. Sie müssen sicherstellen, dass ihre Software regelmäßig aktualisiert wird und alle verfügbaren Sicherheits-Patches installiert sind.

Zudem sollten sie auf bewährte Sicherheitspraktiken setzen, wie zum Beispiel die Implementierung eines guten Passwortmanagementsystems oder die Schulung der Mitarbeiter im Umgang mit potenziellen Bedrohungen.

Die Bekämpfung von Zero Day Exploits erfordert eine enge Zusammenarbeit zwischen Herstellern, Sicherheitsexperten und Unternehmen. Nur durch den Austausch von Informationen und das gemeinsame Arbeiten an Lösungen können wir uns effektiv gegen diese unsichtbaren Einfallstore schützen. In dieser ständigen Auseinandersetzung mit Zero Day Exploits liegt die Chance, unsere Systeme sicherer zu machen und Cyberangriffe erfolgreich abzuwehren.

Rechtliche Aspekte im Umgang mit Zero Day Exploits

Es gibt auch rechtliche Aspekte. Da es sich bei diesen Angriffen um bisher unbekannte Sicherheitslücken handelt, haben Unternehmen und Privatpersonen oft Schwierigkeiten, angemessen auf diese Bedrohungen zu reagieren. Die Verantwortung liegt sowohl bei den Herstellern von Software als auch bei den betroffenen Unternehmen, die ihre Systeme schützen müssen.

Ein wichtiger Punkt ist die Frage nach der Haftung für Schäden, die durch einen erfolgreichen Zero Day Angriff entstehen. Hierbei besteht eine gewisse Unsicherheit, da es sich um neu entdeckte Schwachstellen handelt und eventuell noch keine konkreten Schutzmaßnahmen existieren.

Es ist daher ratsam, dass Unternehmen eng mit ihren Rechtsabteilungen zusammenarbeiten, um mögliche Haftungsrisiken zu minimieren. Darüber hinaus gibt es in einigen Ländern gesetzliche Bestimmungen zur Offenlegung von Zero-Day-Schwachstellen. In solchen Fällen sind Hacker oder Sicherheitsforscher verpflichtet, gefundene Exploits an die Hersteller zu melden und ihnen eine angemessene Frist zur Behebung einzuräumen. Was ausgesprochen sinnvoll ist. Dies dient dem Schutz der Benutzer und unterstützt gleichzeitig die Weiterentwicklung sicherer Software.

Es ist auch wichtig zu beachten, dass nicht nur Angreifer Zero Day Exploits nutzen können - auch staatliche Behörden setzen sie gelegentlich ein, etwa um "Staatstrojaner" zu entwickeln und einzusetzen. In solchen Fällen kann es schwierig sein, den rechtlichen Rahmen eindeutig abzustecken und den richtigen Umgang mit solchen Schwachstellen zu bestimmen. An dieser Praxis gibt es darüber hinaus eine Menge Kritik.

Ein internationaler Austausch von Informationen und eine enge Zusammenarbeit zwischen Regierungen, Unternehmen und Sicherheitsexperten sind unerlässlich. Insgesamt ist es entscheidend, dass sowohl Unternehmen als auch Hersteller von Software die rechtlichen Aspekte im Umgang mit Zero Day Exploits ernst nehmen. Eine klare Vorgehensweise zur Meldung und Behebung von Schwachstellen sowie eine gute Zusammenarbeit zwischen allen Beteiligten sind essentiell, um die Auswirkungen solcher Angriffe zu minimieren und die Sicherheit der digitalen Welt kontinuierlich zu verbessern.

Verantwortlicher Umgang mit entdeckten oder ausgenutzten Zero-Day-Schwachstellen

Ein verantwortlicher Umgang mit entdeckten oder ausgenutzten Zero-Day-Schwachstellen ist von großer Bedeutung. Unternehmen sollten unverzüglich Maßnahmen ergreifen, um ihre Systeme zu schützen und weitere Angriffe zu verhindern.

Dazu gehört zum Beispiel das Patchen der Schwachstelle durch Updates oder das Implementieren von zusätzlichen Sicherheitsmaßnahmen. Es ist auch wichtig, dass Unternehmen eng mit Sicherheitsexperten zusammenarbeiten, um die Auswirkungen des Zero-Day-Exploits abzuschätzen und geeignete Gegenmaßnahmen zu treffen.

Das kann die Analyse des Codes beinhalten, um den Angriff besser zu verstehen und zukünftige Sicherheitslücken zu identifizieren. Darüber hinaus sollten Unternehmen transparent mit ihren Kunden kommunizieren und sie über den Vorfall informieren.

Dies zeigt nicht nur Verantwortungsbewusstsein gegenüber den betroffenen Personen, sondern ermöglicht es ihnen auch, entsprechende Schutzmaßnahmen zu ergreifen. Der verantwortliche Umgang mit Zero-Day-Schwachstellen erfordert eine kontinuierliche Überwachung und Aktualisierung der Sicherheitsmaßnahmen.

Unternehmen sollten ihre Systeme regelmäßig auf Schwachstellen überprüfen und sicherstellen, dass sie mit den neuesten Patches und Updates geschützt sind. Insgesamt ist es von größter Bedeutung, dass Unternehmen die Gefahren von Zero-Day-Exploits ernst nehmen und proaktiv handeln, um sich vor solchen Angriffen zu schützen.

Ein verantwortlicher Umgang mit entdeckten oder ausgenutzten Zero-Day-Schwachstellen kann dazu beitragen, die Sicherheit von Unternehmen und Privatpersonen zu gewährleisten und potenzielle Schäden zu minimieren.

Akkuschonen beim iPhone: 80 Prozent-Grenze einstellen

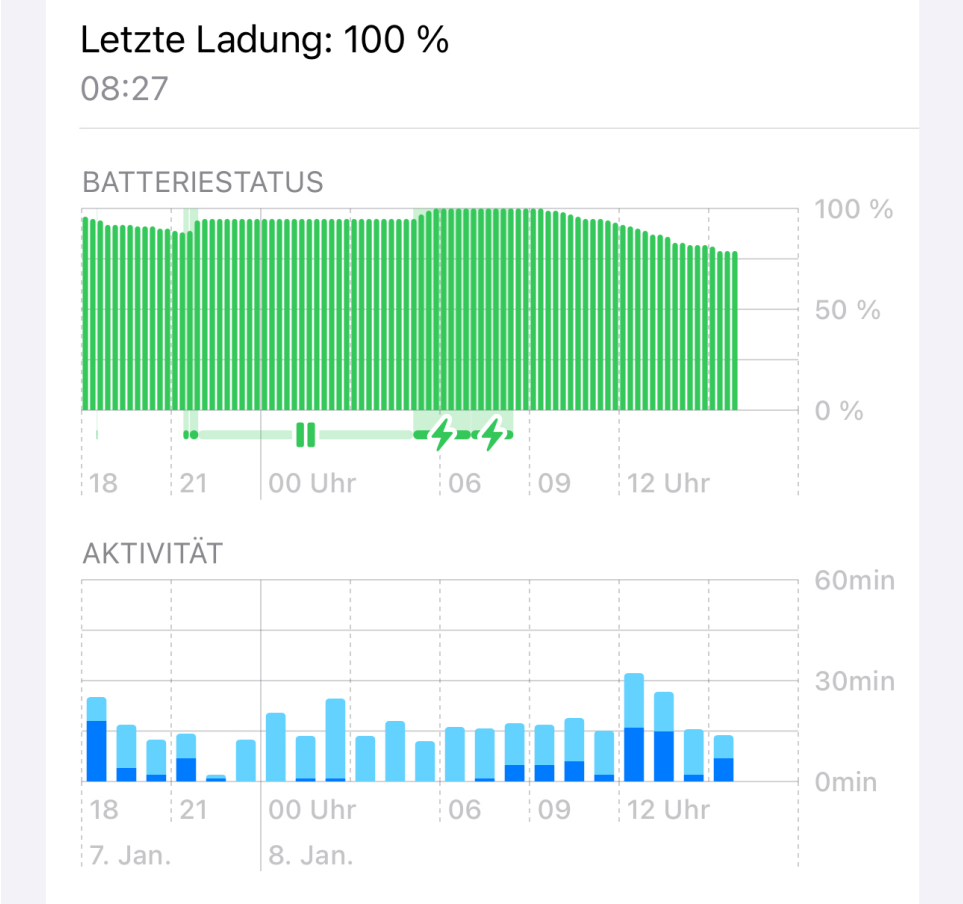
Der Akku: Seit jeher der Teil eines mobilen Geräts, der am kritischsten beäugt wird. Ist er leer, dann ist die Mobilität schnell am Ende. Die Hersteller arbeiten daran, die Laufzeit stetig zu optimieren, auch wenn das die Akkus ausreizt. Eine neue Einstellung in iOS 17 kann hier helfen!

Wann den Akku laden?

Gibt es den richtigen Termin zum Laden eines Akkus? Vermutlich so generell nicht. Auf der einen Seite wollt ihr das Telefon immer so vollgeladen wie möglich haben, andererseits tut es dem Akku auch nicht gut. Auch wenn es den Memory-Effekt, der früher so vielen Akkus den Garaus gemacht hat, nicht mehr in der Form gibt, regelmäßiges Laden und Entladen sind immer noch positiv für die Langlebigkeit eines jeden Akkus.

Das ist auch der Grund, warum Apple schon mit iOS 13 die Batterieoptimierung eingeführt hatte. Damit wird der Akku sporadisch nur auf 80 Prozent geladen. Die Zeitpunkte bestimmt das System selbst anhand eures Nutzungsverhaltens. Ihr

könnt natürlich auch manuell dafür sorgen, indem ihr das Telefon mit einem nur minimal entladenen Akku nicht aus die Ladeschale legt, sondern damit in den nächsten Tag startet!



Achtzig ist das neue 100%

Mit iOS 17 und aktuell nur für iPhone 15-Modelle ist Apple jetzt einen Schritt weitergegangen. Analysen haben gezeigt, dass Anwender eher dazu neigen, am Ende eines jeden Tages zu laden, auch wenn der Akku eigentlich noch für den zweiten Tag reichen würde. Die Ableitung, die Apple daraus gezogen hat: Dann reicht es auch aus, den Akku nur auf 80 Prozent zu laden. Diese Grenze ist nicht unüblich: Eine Ladung bis auf 80 Prozent geht schnell und ohne besondere Belastung des Akkus. Das Laden von 80 auf 100 Prozent dauert dann deutlich länger und erhitzt den Akku auch spürbar. Das sorgt in Summe dafür, dass dieser schneller verschleißt und an Kapazität verliert.

Um die Funktion einzuschalten, ruft die Einstellungen von iOS auf:

- Rollt nach unten bis zu den Einstellungen für die **Batterie**.

- In der Mitte des Bildschirms seht ihr die Entwicklung der Batterieladung über die letzten **24 Stunden** oder die letzten **10 Tage**. Dort könnt ihr auch erkennen, wann iOS aus eigenem Antrieb nur auf 80 Prozent geladen hat.
- Klickt auf **Batteriezustand & Ladevorgang** > **Ladeoptimierung**.
- Im Standard ist **optimiert** angewählt, was iOS die Entscheidung überlässt, wann es voll und wann nur bis 80 Prozent lädt.
- Aktiviert **80% Limit**, um euren Akku zu schonen und ihn immer nur auf 80 Prozent zu laden. iOS lädt dann bis 80 Prozent, beendet den Ladevorgang automatisch und beginnt erst wieder mit der Ladung, wenn der Ladezustand auf 75 Prozent gefallen ist.
- **Ohne** solltet ihr nur sehr bewusst aktivieren. Den Akku immer auf 100 Prozent zu laden gibt euch verlässlich die größtmögliche Akkukapazität. Allerdings werdet ihr feststellen, dass nach wenigen Monaten die maximale Akkukapazität nicht mehr bei 100 Prozent, sondern darunter liegt.

Social Media Posts mit passenden Hashtags per KI

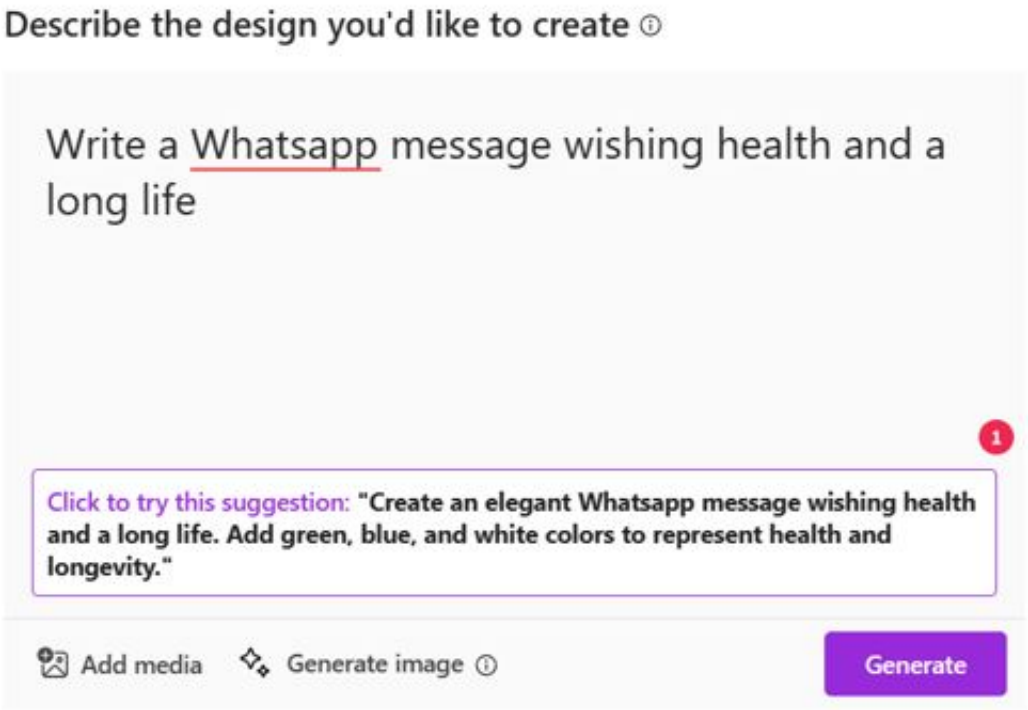
Ein Social Media Post auf Instagram, Facebook oder LinkedIn ist nicht nur der Text und das zugehörige Bild, sondern auch die passenden Hashtags für eure Zielgruppe. Der Microsoft Designer erlaubt es, das alles zusammen per KI erstellen zu lassen.

Erstellen von Designs

Oft ist ein Post auf Instagram oder Facebook mehr als nur der Text darin, erst Bilder, Schriftarten und andere Elemente machen ihn zu dem bunten, multimedialen Spaß, das heutzutage in den sozialen Medien erwartet wird. Der Designer fasst diese Kombination von Medien und Inhalten unter dem Begriff Design zusammen.

- Klickt im Designer auf **Generate** im **Design Creator**.

- Wenn ihr eigene Bilder für den Beitrag verwenden wollt, dann klickt auf **Add media** und fügt diese hinzu.
- Gebt in der Eingabezeile eine möglichst genaue Beschreibung dessen ein, was ihr als Endprodukt erwartet. Die KI geht hier zweigeteilt vor: Zuerst analysiert sie das, was ihr geschrieben habt und verbessert den Vorschlag.
- Entweder klickt ihr auf **Generate**, um euren Vorschlag zu verwenden, oder auf **Click to try this suggestion**, um den KI-Vorschlag zu verwenden.
- Wenn ihr nur ein Bild (und kein bewegtes Thema) bekommen möchtet, dann klickt auf **Generate image**.
- Der Microsoft Designer baut aus den von euch gelieferten Informationen jetzt ein Design und zeigt es an.
- Wenn ihr eigene Medien zur Verfügung gestellt habt, dann findet ihr die in dem Design. Wenn nicht, dann sucht sich der Designer eigene aus dem riesigen Fundus von Microsoft heraus. Das Design wird dann allerdings eher weniger persönlich, als wenn ihr es durch eigene Medien unterstützt.
- Klickt eines der generierten Designs an, um es im Detail zu sehen.
- Wenn ihr es verändern wollt, dann klickt auf **Customize Design**. Hier habt ihr die unterschiedlichsten Optionen: Ihr könnt eigene Medien nachträglich einfügen, Texte verändern. Weitere Seiten hinzufügen und gestalten und vieles mehr.
- Besonders hilfreich, um den Mangel der rein englischen Sprache auszugleichen: Klickt in ein Textfeld und dann unten rechts auf den Punkt. Dort klickt auf **Übersetzen** und dann auf **Deutsch**. Die Funktion habt ihr, wenn ihr eine aktuelle Version von Microsofts Edge-Browser einsetzt, sie hat mit dem Designer nichts zu tun. Trotzdem bekommt ihr damit die erzeugten Texte mit einem Klick auf Deutsch übersetzt!
- Klickt auf Download, um das Thema herunterzuladen. Wenn ihr es mit allen Animationen verwenden wollt, dann wählt als Typ MP4, sonst eines der angebotenen Bildformate.

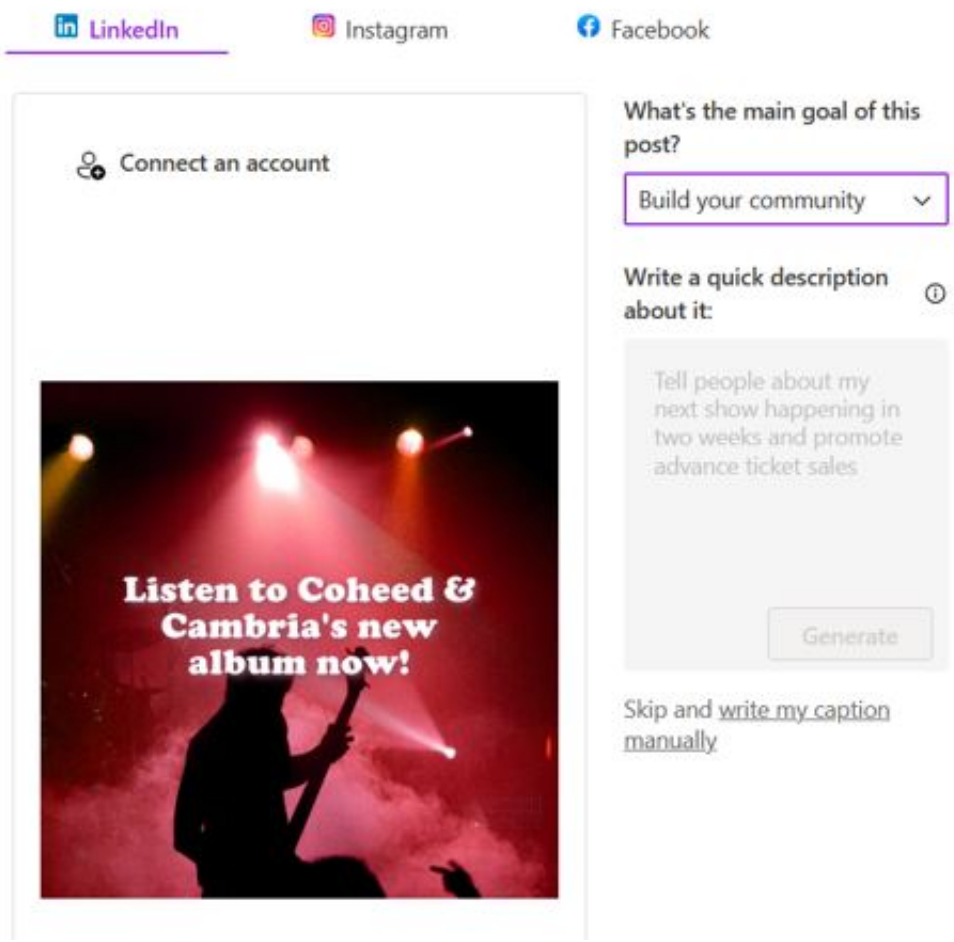


Automatisch die richtigen Tags finden

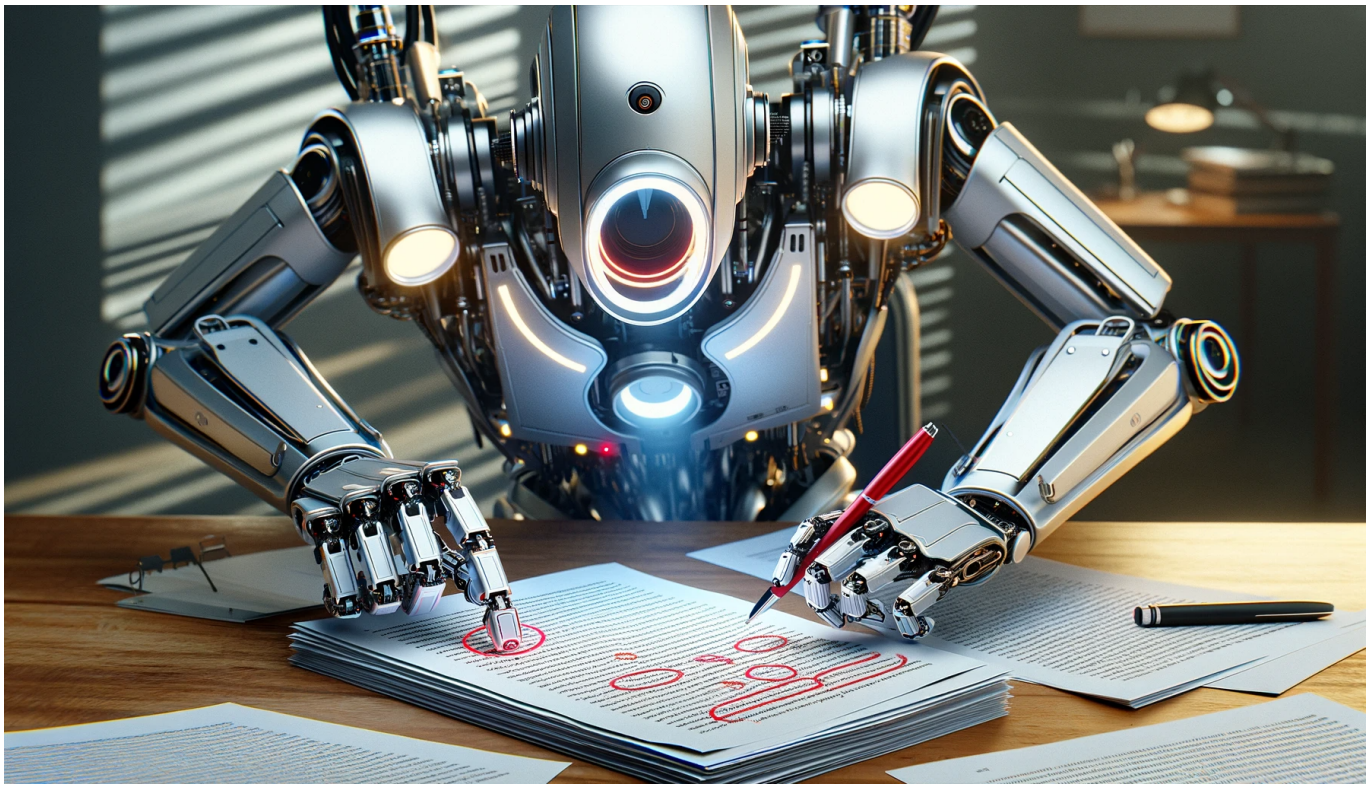
Wo wir gerade bei Social Media Posts sind: Medien sind schön, der Text aber manchmal eine Herausforderung. Und erst die richtigen Hashtags! Gerade letztere sind entscheiden dafür, dass eure gewünschte Zielgruppe die Beiträge auch liest. Auch hier kann der Designer unterstützen:

- Erzeugt erst einmal ein Design wie oben beschrieben, um die Basis für den Beitrag zu haben. Klickt dann auf **Download**.
- Statt das Design herunterzuladen, klickt unten bei den Symbolen für die sozialen Netzwerke auf **Try it**.
- Unter **What´s the main goal** wählt aus, was ihr mit dem Post erreichen wollt. Oft wird das **Build your Community** sein, also das Erreichen neuer Follower.
- Nun gebt ihr darunter eine kurze Beschreibung an, worum sich der Post dreht. Das ist etwa anderes als der Text in dem Design, dass der Designer erzeugt hat, denn es soll den Inhalt möglichst genau beschreiben, während der Text im Bild eher toll klingen soll.
- Klickt auf **Generate**, um aus Eurer Beschreibung einen Text zu erzeugen.
- Unter **Captions** findet ihr die von der KI generierten Texte, unter **Hashtags** dazu passende thematische Kurzbeschreibungen.

- Noch komfortabler: Wählt über der Voransicht den Dienst (aktuell LinkedIn, Instagram und Facebook) aus, dann klickt auf **Connect an account**. Nach der Anmeldung könnt ihr den Post mit all seinen Elementen direkt in den Dienst posten, ohne ihn manuell hochladen zu müssen!



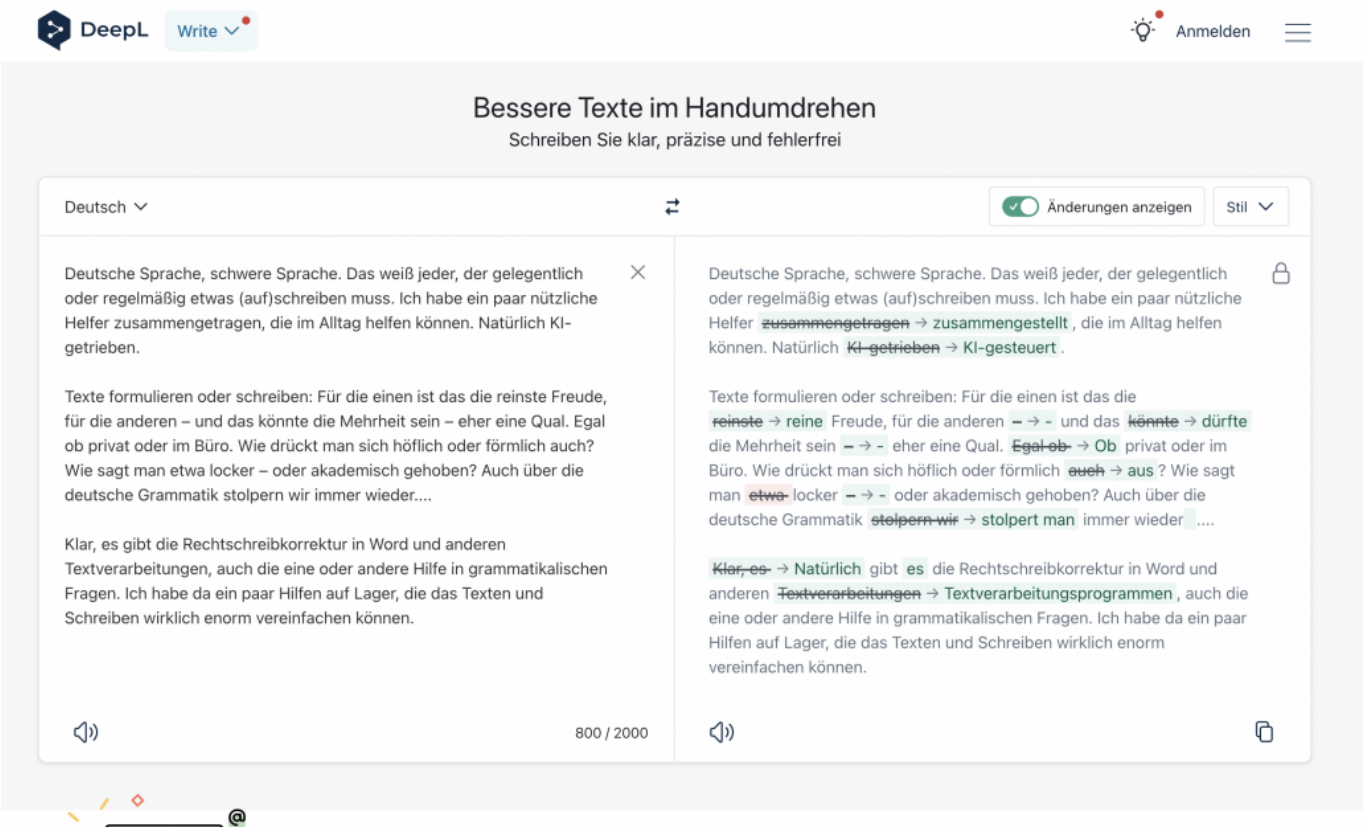
So könnt Ihr mit KI Eure Texte verbessern



Deutsche Sprache, schwere Sprache. Das weiß jeder, der gelegentlich oder regelmäßig etwas (auf)schreiben muss. Ich habe ein paar nützliche Helfer zusammengetragen, die im Alltag helfen können. Natürlich KI-getrieben.

Texte formulieren oder schreiben: Für die einen ist das die reinste Freude, für die anderen – und das könnte die Mehrheit sein – eher eine Qual. Egal ob privat oder im Büro. Wie drückt man sich höflich oder förmlich auch? Wie sagt man etwa locker – oder akademisch gehoben? Auch über die deutsche Grammatik stolpern wir immer wieder....

Klar, es gibt die Rechtschreibkorrektur in Word und anderen Textverarbeitungen, auch die eine oder andere Hilfe in grammatikalischen Fragen. Ich habe da ein paar Hilfen auf Lager, die das Texten und Schreiben wirklich enorm vereinfachen können.



Deepl Write korrigiert nicht nur Schreibfehler, sondern macht auch Verbesserungsvorschläge

Chatbots können korrigieren und umformulieren

Fangen wir doch ruhig mal mit den üblichen Verdächtigen an: ChatGPT. Der Chatbot kann nämlich nicht nur Texte genieren und in andere Sprachen übersetzen. Er kann auch helfen, bessere Formulierungen zu finden.

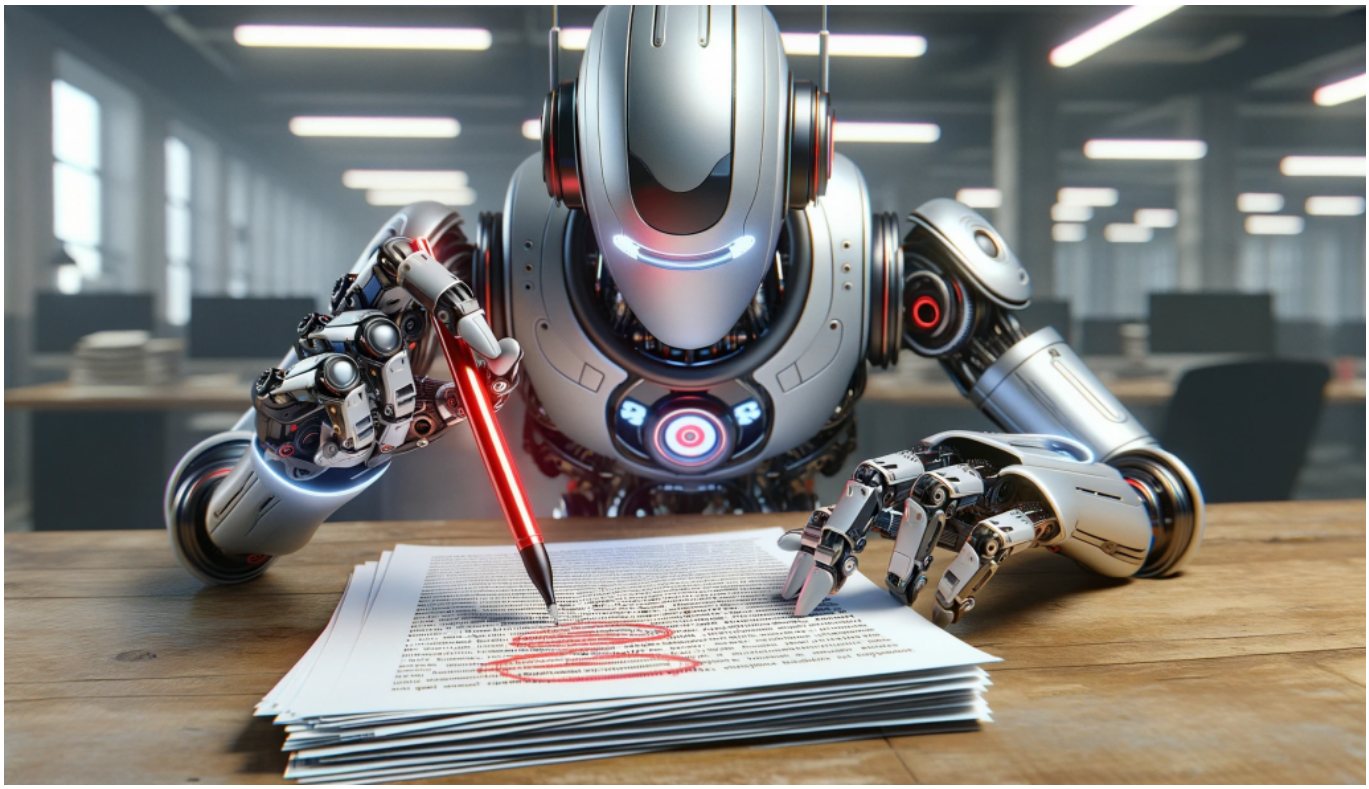
Wie formuliere ich eine Trauerkarte, wie einen Glückwunsch zum Jubiläum oder Geburtstag einer 17-Jährigen: Alles kein Problem, da macht der Chatbot durchaus gute Vorschläge. ChatGPT lässt sich auch als Thesaurus missbrauchen: Ich brauche ein anderes Wort für „Thesaurus“ – und ChatGPT schlägt „Synonymwörterbuch“ vor.

Doch jetzt mal für den Alltag: Wie sagt oder formuliert man Dinge locker, formell, geschäftlich oder akademisch? Das habe ich mal mit ChatGPT probiert – und folgende Ergebnisse bekommen:

Übersetze "**Ich habe nicht den geringsten Bock zu arbeiten**"
für mich bitte in akademische Sprache, damit es sich gehoben anhört.

"**Ich verspüre keinerlei Affinität, meine beruflichen Verpflichtungen zu erfüllen**."
Und sage das jetzt bitte noch in allerbestem Ruhrpott-Deutsch...
"**Ich hab echt null Bock auf Arbeit, ey.**"

Klappt doch. :)



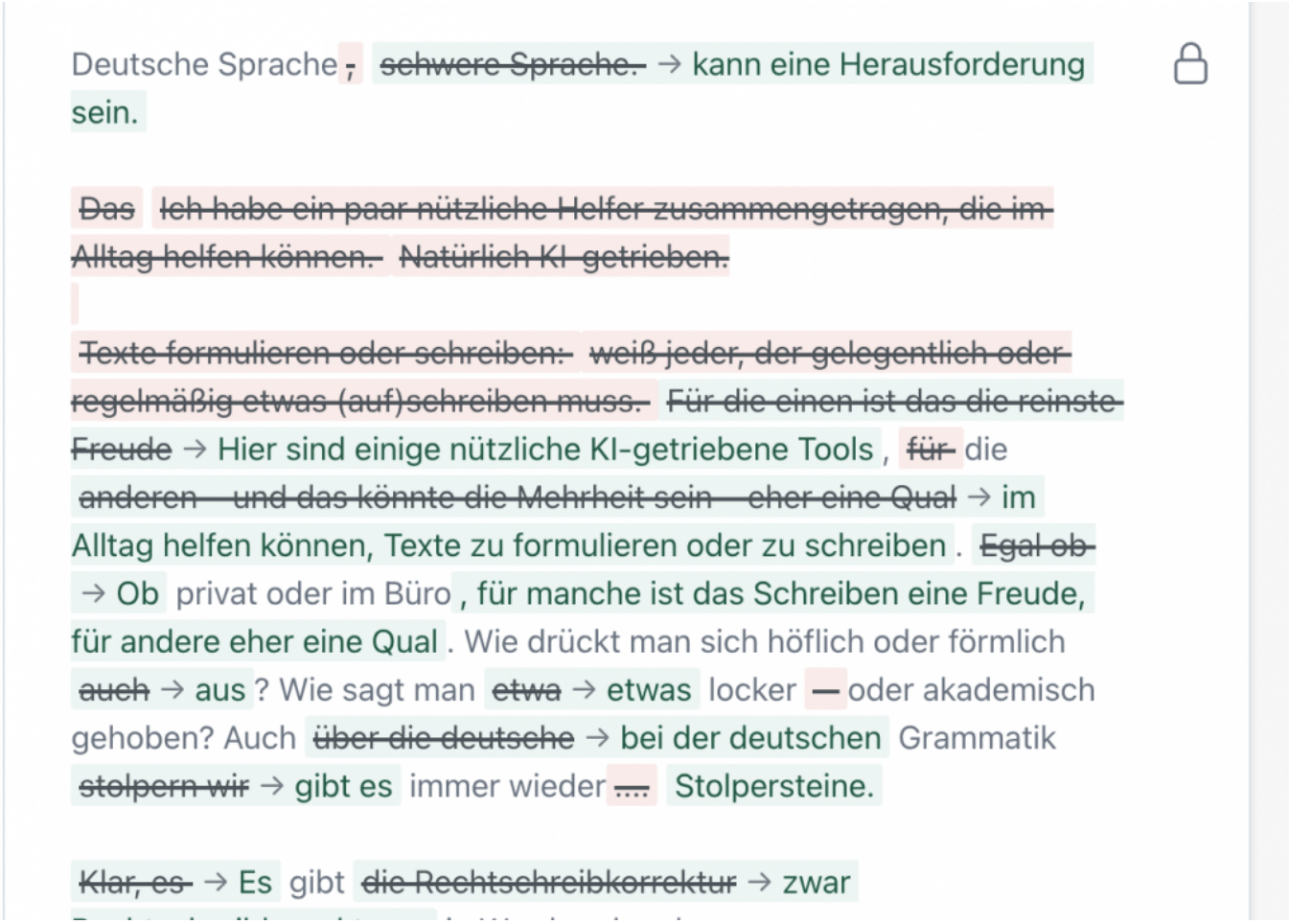
Deepl Write: Die Edelfeder als ständiger Helfer

Aber kann mir eine KI auch direkt beim Schreiben helfen: Grammatikfehler korrigieren, Füllwörter raus und sowas?

Absolut. Ich empfehle da Deepl Write. Deepl ist eine Firma aus Köln, die bekannt ist für Deepl Translate. Da steckt KI und Deep Learning dahinter, daher der Name. Die Übersetzungs-KI der Kölner gilt als absolut überlegen, besser als Google Translate und ähnliche Anbieter.

Deepl Write funktioniert nach ähnlichem Prinzip, konzentriert sich aber auf die deutsche Sprache. Ich kann einen Text nehmen, den ich in Word oder einem Browser schreibe, den bei Deepl Write einsetzen und korrigieren lassen. Sekundenbruchteile später sehe ich den korrigierten Text.

Ob Tippfehler, Rechtschreibfehler, Kommafehler, grammatikalische Fehler: Wird alles korrigiert. Die KI entfernt auch Füllwörter. Auf Wunsch werden die Korrekturen angezeigt, dann kann ich sehen und lernen, was die KI verbessert hat. Oder man übernimmt die korrigierte Fassung einfach und hat dann einen deutlich besseren Text.



Auf Wunsch kann Deepl Write sogar die Stilrichtung ändern

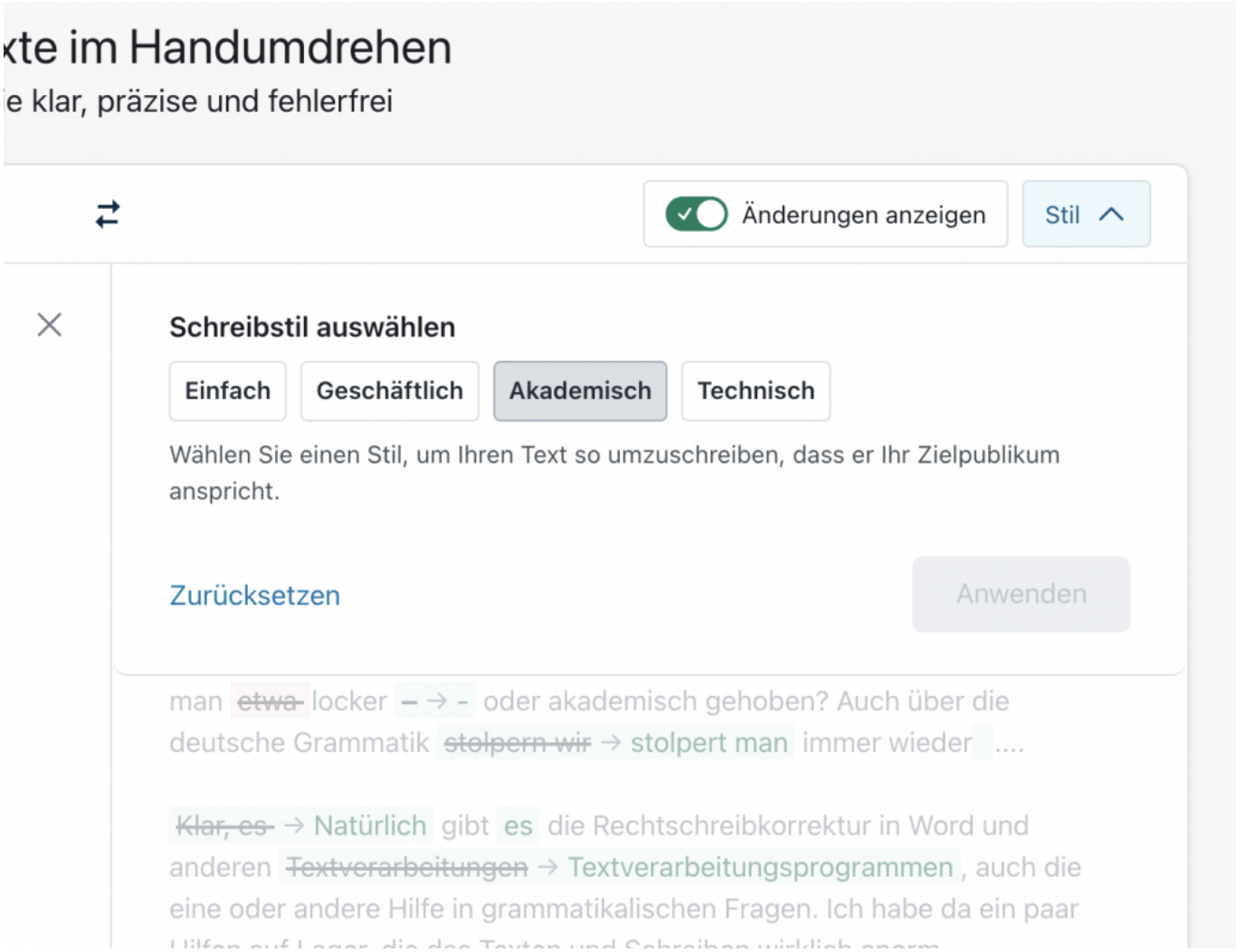
Deepl Write formuliert auf Wunsch um

Viele sind nicht so gut darin, sich förmlich auszudrücken – oder umgekehrt locker: Auch hier hilft die praktische Anwendung.

Das ist sogar eine Stärke von Deepl Write. Auf Wunsch formuliert die KI Texte geschmeidiger, so dass es besser verständlich wird. Und wer mag, kann sogar die Stilrichtung vorgeben: Einfach, geschäftlich, akademisch, technisch oder locker. Aus „Die Situation erscheint total absurd“ wird dann „Die Situation wirkt vollkommen absurd“.

Nur eine Kleinigkeit, klingt aber schon ganz anders. Das Werkzeug bietet wirklich eine Menge Möglichkeiten und hilft auch Menschen, die Deutsch lernen, wie sie sich anders oder besser ausdrücken können. Es gibt endlose Einsatzmöglichkeiten. Kurze Texte verbessert Deepl Write im Web.

Wer ganze Dokumente – etwa Word-Texte – verbessern lassen möchte, kann das auch. Selbst die Formatierungen bleiben da erhalten. In der kostenlosen Version ist das auf drei Dokumente im Monat beschränkt. Wer mehr will, bezahlt dafür – zu Recht, es ist wirklich ein leistungsfähiges System.



Der Wechsel von locker zu akademisch ist mit Deepl Write einfach

Language Tool: Korrekturen beim Schreiben

Noch praktischer wäre es natürlich, sage ich mal als Praktiker, ich bekomme die Korrekturen schon während ich schreibe, in Word oder im Browser.

Ich persönliche nutze „Language Tool“. Das ist eine Software, eine KI, die ganz ähnlich ist zu Deepl Write, an manchen Stellen aber weiter geht. Language Tool lässt sich als Erweiterung im Lieblings-Browser installieren oder sogar auch in Textprogramme wie Google Docs oder Word integrieren.

Meine Texte werden dann nicht nur auf Rechtschreibung und Grammatik überprüft, sondern auch Formulierungen, Satzbau und vieles mehr. In der kostenlosen Version kann man schon erstaunlich viel machen.

Nicht „Ich mache den Text kürzer“, meint die KI, sondern besser „Ich kürze den Text“... Wer mehr will, etwa Fremdwörter, Glossar, doppelte Formulierungen erkennen und dergleichen, der kann eine Premium-Version benutzen, die überschaubar kostet. Insgesamt: Für alle, die viel schreiben oder die deutsche Sprache nicht so beherrschen, sind solche Tools eine riesige Hilfe.

Beste Unterhaltung zu geringen Kosten: So lässt sich bei Musik, Filmen und Serien sparen!

Filme, Serien, Musik - kommt heute bei den meisten aus dem Internet. Streaming ist das Schlagwort. Was ungeheuer praktisch ist, das ist leider auch mit hohen Kosten verbunden. Zuletzt haben Streaminganbieter die Preise erhöht. Doch es lässt sich Geld sparen!

Streamingdienste sind die modernste Form der Unterhaltung und kommen nicht nur bei Serien und Filmen, sondern auch im Bereich Musik zum Einsatz. Je mehr solcher Dienste genutzt werden, desto höher sind die Ausgaben.

Da bei den meisten das Budget nicht unerschöpflich ist, macht es Sinn, die Ausgaben genau zu prüfen - und zu planen. Die gute Nachricht ist, dass es durchaus ein gewisses Sparpotenzial gibt. Deshalb nachfolgend die besten Tipps und Tricks, wie die Kosten für Unterhaltung nicht das Budget überschreiten.

Manchmal möglich: Gratis ausprobieren und ohne Kosten genießen

Nicht nur wenig, sondern gar nichts bezahlen? Das ist dank Plattformen wie www.mein-deal.com möglich, denn Konsumenten finden hier kostenlos zum Ausprobieren. Ob dabei auch ein Deal eines Streamingdienstes dabei ist, lässt sich zwar nicht immer vorhersagen. Aber die Chancen stehen grundsätzlich nicht schlecht.

Die Konkurrenz unter den Streamingdiensten hat in den letzten Jahren stark zugenommen. Was mit Netflix nahezu ganz allein begann, besteht heute aus Disney Plus, Wow-TV, Thalia Hörbüchern, Audible, Spotify und vielen anderen Anbietern mehr. Die Angebote der Dienste überschneiden sich oft, sodass ein kostenloser Probezeitraum bei einem neuen Anbieter die Vorlieben genauso gut befriedigt.

Wichtig: Soll die Probephase nicht nicht in ein reguläres Abo übergehen, ist eine rechtzeitige Kündigung wichtig. Je nach Anbieter schließt sich sonst ein kostenpflichtiger Vertrag an, für den der Kunde zahlen muss. Logisch eigentlich, die kostenlose Phase isrt schließlich zum Anwerben gedacht,

Wer ein Probeabo bucht, sollte es so gut es geht ausnutzen. Das nachfolgende Video ist perfekt für all jene geeignet, die gerade Netflix ausproboieren. Dort werden die 100 besten Filme des Jahres 2023 vorgestellt:

Der richtige Streamingtarif trägt zur Reduktion der Kosten bei

Die meisten Streamingdienste bieten ihre Filme und Serien in 4K Ultra HD an und richten sich damit an jene, die gute Grafik zu schätzen wissen. Das lohnt sich vor allem dann, wenn ein riesiger Fernseher vorhanden ist. Für all jene, die nur auf dem Smartphone oder dem Laptop schauen, sind diese Kosten obsolet.

Am Beispiel von Netflix zeigt sich, wie viel Sparpotenzial in der Wahl des richtigen Tarifs liegt:

- **Basis-Angebot:** Stand 2024 kostet dieses Abo 4,99 Euro und beinhaltet

das volle Paket von Netflix, mit kurzen Werbeeinblendungen vor Filmen und Serien.
- **Standard-Angebot:** Dieses Abo bietet für 12,99 Euro ein jederzeit kündbares Angebot in SD- und HD-Auflösung, allerdings ohne 4K.
- **Premium-Angebot:** Ausgewählte und verfügbare Serien und Filme lassen sich in Ultra-HD-Auflösung schauen, Netflix steht auf maximal vier Geräten zur Verfügung.

Zwischen dem Basis-Angebot und der Premium-Variante liegt eine Differenz von 13 Euro. Wer also ohnehin nur auf dem kleinen TV-Gerät oder dem Smartphone schaut, sollte einen Wechsel dringend in Betracht ziehen.

Tipp: Echte 4K-Liebhaber profitieren vom kostenlosen Upgrade bei Disney Plus, Amazon Prime und Apple TV +. Hier ist 4K in den Paketen enthalten, sodass die verfügbaren Serien und Filme in entsprechender Qualität angeboten werden. Ein Vergleich, ob es wirklich Netflix sein muss, lohnt sich daher für jeden Konsumenten.

Die Preiserhöhungen betrafen bei Disney+ erst mal nur Neukunden ab November

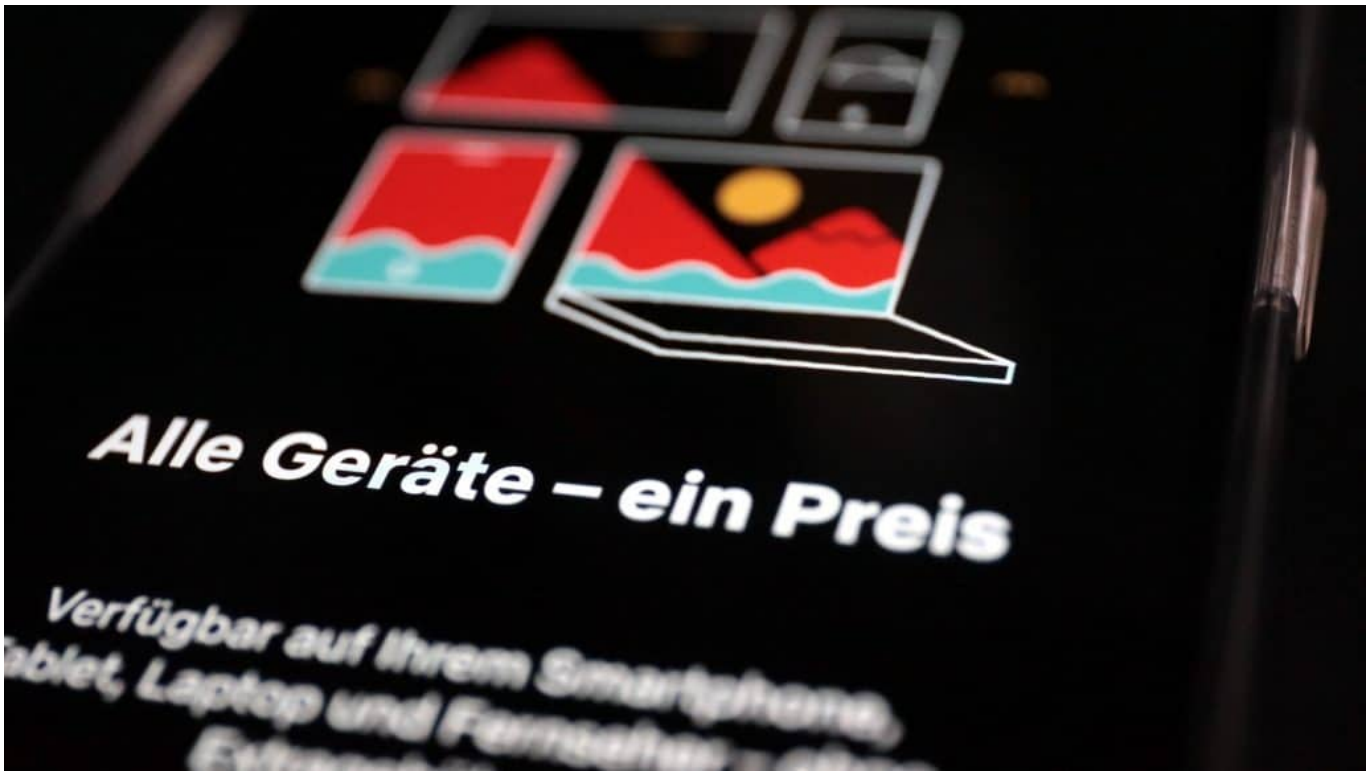
Mitgliedschaft mit Mitgliedern des gleichen Haushalts teilen

Es war ein Schock als Netflix verkündete, dass Account-Sharing künftig nicht mehr erlaubt ist. Vorher ließ sich ein Zugang gemeinsam mit bis zu drei weiteren Konsumenten nutzen, das reduzierte die Kosten deutlich.

Ganz verboten ist Account-Sharing aber auch heute nicht, zumindest wenn die Nutzer alle im gleichen Haushalt leben. Studenten-WGs oder auch Großfamilien profitieren davon, sich für einen Sharing-Tarif zu entscheiden. Den gibt es nicht nur bei Netflix, auch Amazon Prime lässt sich mit anderen teilen.

Wer gerne YouTube schaut und werbefrei nutzen möchte, profitiert von einer Premium-Mitgliedschaft. Sie ist nicht ortsgebunden und kann mit Freunden und Familienmitgliedern unabhängig vom Standort geteilt werden.

In Freundeskreisen lohnt es sich, wenn jeder einen anderen Dienst abonniert. Filme und Serien werden dann immer bei der Person geschaut, die den passenden Streamingdienst auf dem TV-Gerät hat.



Bundles von anderen Dienstleistern nutzen

Bei einem Bundle-Angebot werden mehrere Dienstleistungen zu einem (oft) günstigeren Gesamtpreis zusammengefasst. Mobilfunk- und Internetanbieter wie

Vodafone und die Telekom halten für ihre Kunden oft Komplettpakete bereit, bei denen Netflix, Amazon Prime und andere Streamingdienste bereits integriert sind. Es ist wichtig zu vergleichen, ob der Einzelpreis bei Bundle-Nutzung tatsächlich günstiger ist. Falls ja, kann sich ein solches Paket lohnen.

Achtung: Bei den meisten Streamingdiensten besteht die Möglichkeit, monatlich zu kündigen. Ein Bundle kann diese Option ausschließen, wenn der Internettarif beispielsweise über 24 Monate gebucht wurde.

Die lange Verbindung als Sparfaktor für Streamingdienste

Obwohl Flexibilität und ständige Kündbarkeit den meisten Konsumenten wichtig sind, gibt es auch eine Kehrseite der Medaille. Bei vielen Streaminganbietern zahlt sich Treue aus. Bei DAZN und Disney Plus gibt es beispielsweise die Möglichkeit ein Jahresabo abzuschließen und damit auf den Monat gerechnet Geld zu sparen.

Das macht jedoch nur dann Sinn, wenn der Streamingdienst regelmäßig genutzt wird. Wer beispielsweise weiß, dass jeden Monat neue Folgen der Lieblingsserie erscheinen und das Abo ohnehin schon seit mehreren Jahren läuft, kann auf diese Weise erheblich sparen.

Kostenlose Alternativen zur Unterhaltung nutzen

Umfragen zeigen, dass nicht mehr nur Streamingdienste eine Rolle bei der Unterhaltung spielen. Mediatheken von TV-Sendern erfreuen sich zunehmender Beliebtheit, denn sie haben einen Vorteil: ARD und ZDF beispielsweise bieten ihre Inhalte komplett kostenlos an und auch hier gibt es gelegentlich gute Filme und Serien zu sehen.

Wer bereit ist, auf Komfort und Werbefreiheit zu verzichten, profitiert außerdem von kostenlosen Streamingdiensten. Zwar ist das Angebot ohne Premium-Version etwas abgespeckt, genug zu schauen gibt es aber trotzdem.

Die bekanntesten Dienste sind:

- TV Now
- Netzkino
- Joyn

- Chrunchyroll
- Popcorntimes

Immer wieder kündigen lohnt sich fürs Bankkonto

Während in der kühlen Jahreszeit so mancher Filmeabend auf dem Programm steht, sehen die meisten Menschen im Sommer seltener fern. Die Abende führen in den Biergarten statt aufs Sofa und die Streamingabos kommen zu kurz. Wer vergisst zu kündigen, zahlt oft viele Monate für einen Dienst, ohne ihn zu nutzen. Es ist daher sinnvoll, einmal im Monat einen Abo-Check durchzuführen.

Die Zeit für eine Kündigung ist reif, wenn:

- ein Monat kein Zugriff erfolgt ist
- keine spannenden Serien oder Filme angekündigt sind
- in den nächsten Monaten mehr Outdoor-Beschäftigung ansteht

Tipp: Manchmal bieten Streamingdienste Schnäppchen und Rabatte an, um ihre Kunden wieder anzulocken. Die Kündigung kann somit gleich doppelte Vorteile mitbringen und lohnt sich bei Nichtnutzung in jedem Fall.

Angebote, Rabatte und Aktionen beachten

Streamingdienste werden immer moderner, mittlerweile schlagen Algorithmen bereits die geeignete Musik oder die neuesten Filme vor. Jeder möchte „der Beste“ sein, insbesondere im Zeitalter der wachsenden Konkurrenz. Das führt dazu, dass nicht nur die Funktionalität immer komfortabler wird, sondern dass auch Rabattaktionen und Angebote in Hülle und Fülle auftauchen.

Es lohnt sich, regelmäßig die Augen nach Deals offenzuhalten, um wahre Schnäppchen für die eigene Freizeitgestaltung zu nutzen. Während dieser Phasen macht es Sinn, die Konkurrenz kurzfristig zu kündigen. Bietet also Amazon Prime gerade ein Top-Angebot an, darf Netflix während dieser Phase pausieren und umgekehrt. Durch Streamingdienst-Hopping reduzieren sich die monatlichen Kosten, da immer nur ein Dienst aktiv genutzt wird.

YouTube statt Streaming – eine Alternative für Gelegenheitskonsumenten

Geht es um Musik, ist YouTube eine gute Alternative zu Spotify und Co. Die Videos zahlreicher Interpreten stehen kostenlos zur Verfügung, ohne Premium-Version mit vorheriger Werbung. Da die Videoplattform den Download von Inhalten ermöglicht, lässt sich die eigene Playlist auf diese Weise kostenlos zusammenstellen. Zwar ist der Komfort bei Spotify, Audible und anderen Streamingdiensten höher, dafür aber auch die Kosten.

Auch die Auswahl an Hörbüchern auf YouTube ist in den letzten Jahren deutlich gewachsen. Vom Kinderhörspiel bis hin zum Podcast für Lernende ist hier alles dabei, was Unterhaltung auf die Ohren bringt. Bevor ein Streaming-Abonnement abgeschlossen wird, lohnt es sich, zunächst die Verfügbarkeit auf YouTube zu checken.

Ein VPN kann jeden PC und jedes Mobilgerät effektiv schützen vor Hackern und Datendieben

Vielfalt mit VPNs erweitern und im Ausland schauen

Wer kennt es nicht? Irgendwann sind alle Top-Serien bei Netflix auserzählt und es gibt keine neuen Inhalte. An dieser Stelle kann ein Virtual Privat Network (VPN)

Abhilfe schaffen. Es ermöglicht die Umgehung von Geoblocking und schafft Zugang zu ausländischen Serien und Filmen.

Zwar sind diese nur mit Untertiteln verfügbar, erhöhen das Potenzial des Streaminganbieters aber deutlich. Bevor also ein Wechsel stattfindet, lohnt es sich, zunächst die Inhalte der Nachbarländer zu checken und das Abo voll auszunutzen.

Der gute alte Fernseher für Filme

Beim linearen TV nervt vor allem eines: Die Werbung. Oft scheint es, als ob zwischen den Werbeblöcken kurze Abschnitten des Films gezeigt werden und nicht umgekehrt. Wer ohnehin einen Kabelanschluss hat, kann vom TV-Programm trotzdem profitieren.

Smart-TVs machen es möglich, im TV gezeigte Inhalte direkt auf einer SSD-Festplatte zu speichern. Wenn also der Lieblingsfilm läuft, lässt er sich so mit wenig Speicherplatz sichern und jederzeit genießen. Die dazwischen gezeigte Werbung kann mit einem kostenlosen Videoprogramm einfach weggeschnitten oder beim Abspielen übersprungen werden.

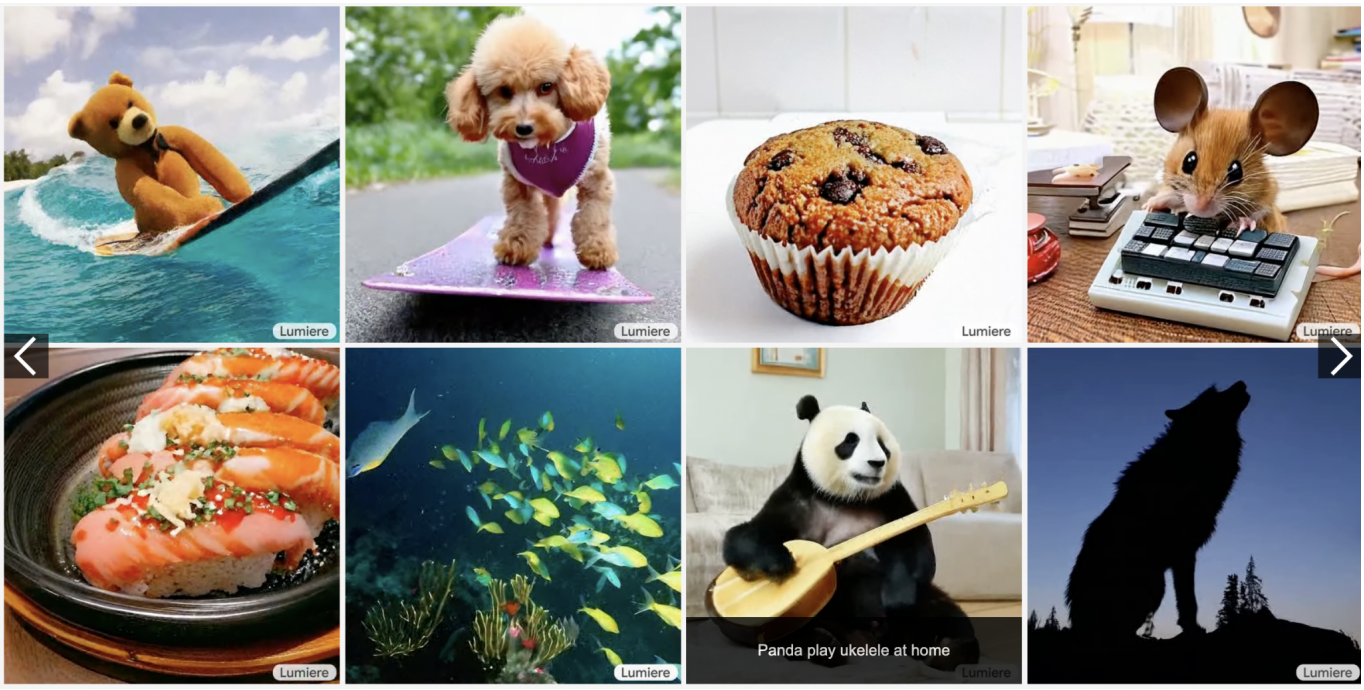
Fazit: Budget festlegen, Alternativen austesten und bei Streamingdiensten sparen sind die Schlüssel zur kostengünstigen Unterhaltung

Für alle, die sich um Geld keine Gedanken machen müssen, bietet die Welt der Streaminganbieter genug Abwechslung für ein ganzes Leben. Alle anderen profitieren davon, wenn sie sich im Vorfeld ein Budget festlegen. So wird verhindert, dass zu viel Geld in (ungenutzte) Dienste fließt.

Ein beliebtes Verfahren ist das „Monatsmodell“: Hierbei wird jeden Monat (oder auch einmal pro Quartal) der Streaminganbieter gewechselt. Im Januar Amazon Prime, im Februar Netflix, im März Disney Plus und so weiter.

Mit ein wenig Budgetplanung, der Suche nach kostenlosen Testphasen und der Nutzung von Alternativen lässt sich bares Geld sparen, das am Ende für etwas anderes verfügbar ist.

Google Lumiere: Durchbruch bei KI-Videos



Google ist es gelungen, eine bemerkenswert leistungsfähige KI zur Erzeugung von Videos an den Start zu bringen. Lumiere erzeugt aus dem Nichts bis zu fünf Sekunden lange Videos. Ein Anfang.

KI kann heute Texte erzeugen, Fotos und Bilder, auch Audios – und das in zunehmend guter Qualität. Nur an Bewegtbildern (Videos) hat sich die KI bislang die Zähne ausgebissen.

Denn Videos sind selbst für KI sehr anspruchsvoll. Doch das könnte sich bald ändern, denn Google hat ein KI-System entwickelt, das selbst diese Hürde meistert und mehrsekündige Videosequenzen herstellen kann.

Ein erster Anfang, wie vor einigen Monaten, als KI die ersten echt aussehenden Bilder erzeugt hat.

Google Lumiere kann auch bestehende Bilder animieren

Google Lumiere: Eine Verbeugung vor der gleichnamigen Brüdern

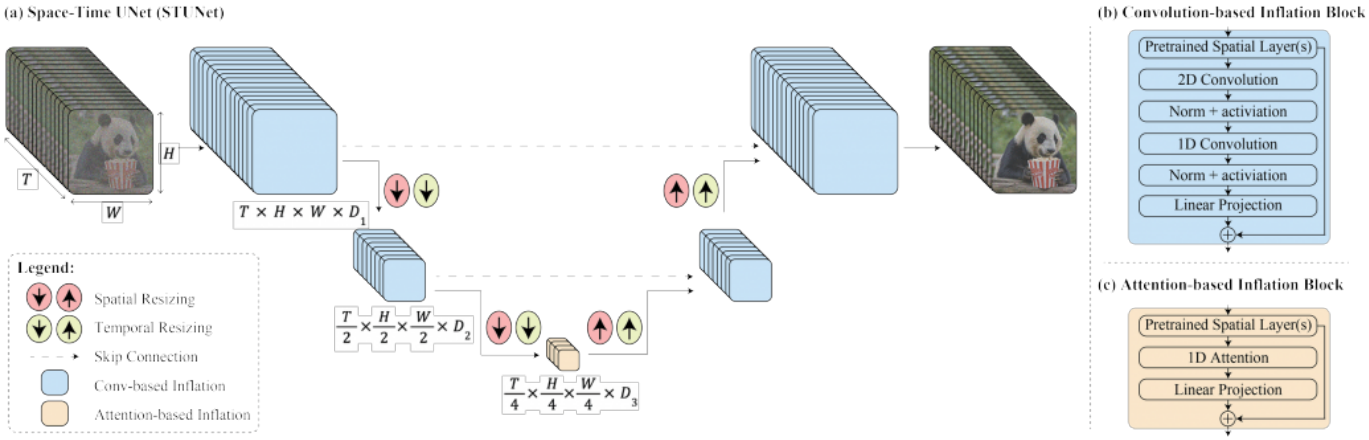
In Fachkreisen spricht man gerade über diese neue KI-Technologie, die Google da entwickelt hat.

Fangen wir doch mit dem Namen an: Google hat das KI-Modell „Lumière“ getauft. Eine Verneigung vor den Brüdern Lumière.

Die beiden Franzosen entwickelten 1895 die erste funktionstüchtige Filmkamera – und das erste Abspielgerät. Der Grundstein des Kinos. Google Lumiere will der Grundstein für Videos generierende KI sein.

Mit der KI, die noch nicht öffentlich zugänglich ist, wohl aber technischen Dokumente und Beispiele, die mit der KI erzeugt wurden, kann fünf Sekunden lange Videosequenzen erzeugen. Aus dem Nichts.

Es reicht, der KI zu sagen, was man sehen möchte. Zum Beispiel: Ein Hund mit roter Brille, der seine Nase beim Autofahren aus dem Fenster hält. Fertig. Oder eine Schildkröte, die an den Strand krabbelt. Fertig. Ein tanzender Bär. Ein Sonnenuntergang in Paris. Das können Bilder generierende KIs ja schon lange. Aber nun gibt es die erste KI, die durchaus real wirkende Videos generiert.



Das Konzept hinter Google Lumiere erklärt

Google Lumiere verwendet anderen Ansatz

Die aller erste KI, die Videosequenzen erzeugt, ist Google Lumiere ja nicht.

Die bisherigen KI-Modelle sind daran gescheitert, Bewegungen wirklich gut zu simulieren. Man könnte sagen, die KI scheitert an der Zeit. Denn wenn sich etwas bewegt, dann verändert sich oft auch die Perspektive, das Licht.

Die Google-Ingenieure verfolgen eine ganz andere Philosophie als bisherige KI-Modelle. Bislang haben Video-KIs das erste Bild erzeugt, dann das zweite, dann das dritte – und immer Kleinigkeiten verändert.

Google Lumiere erzeugt alle Bilder gleichzeitig. Das sorgt für mehr „Kohärenz“, wie Ingenieure sagen. Alles bewegt sich natürlich, es gibt nichts, was unnatürlich wirkt. Die KI wurde mit 30 Millionen Videos trainiert, um natürliche Bewegungen zu erlernen.

Die KI kann nicht alles erzeugen, aber Natur und Tiere funktionieren schon sehr überzeugend. Ein erster Schritt ist gemacht: Alle KI-Entwickler werden jetzt auf diese neue Methode setzen, weil sie am erfolgversprechendsten ist.

[video width="512" height="512" webm="https://www.schieb.de/wp-content/uploads/2024/01/origami_woman.webm"][/video]

Durchbruch gelungen: Missbrauch vorherzusehen

Das klingt jetzt erst mal sehr beeindruckend, man könnte auch sagen viel versprechend. Aber natürlich auch beängstigend: Drohen uns nach Fake-Bildern nun auch Fake-Videos?

Das ist wohl unausweichlich – früher oder später. Es gibt durchaus schon Fake-Videos. Etwa Videos, die Personen zeigen, die reden – und ihnen werden andere Wörter in den Mund gelegt. Oder KI tauscht das eine Gesicht im Film gegen ein anderes Gesicht aus.

Aber dass eine KI tatsächlich eine komplette Bildsequenz aus dem Nichts erstellt und es sieht echt aus: Das ist neu! Sobald diese Technologie frei zugänglich ist oder von anderen kopiert wurde, wird ohne jeden Zweifel Missbrauch stattfinden.

So wie auch mit Bildern und Audios schon geschehen. Allerdings wird es noch eine Weile dauern, bis wirklich längere Sequenzen erstellt werden können. So sind zum Beispiel im Augenblick noch keine Umschnitte möglich.

Nur eine Einstellung und Sequenz. Aber das ist alles eine Frage der Zeit. Denn mit dieser Technologie lassen sich auch Objekte in einem vorhandenen Video austauschen. Eine Person gegen eine andere. Eine Uhr der Marke A gegen eine der Marke B. Das perfekte Werkzeug für Werbung, Spaß, Unterhaltung und Kino – aber eben auch für die Giftküche von Betrügern und Staaten.

Wie geht es mit Google Lumiere weiter

Stellt sich die Frage: Lässt sich der Geist denn wieder in die Flasche bekommen oder so „zähmen“, dass Missbrauch ausgeschlossen ist.

Das kommt darauf an, wie schnell sich die KI-Technologie entwickelt – und wer sie kopieren kann. Durch die Möglichkeiten bisheriger KI-Technologien ist die Politik und Gesellschaft aufgewacht und gewarnt.

Es ist wahrscheinlich, dass Grenzen gezogen werden, was mit so einer KI möglich sein darf – und was damit gemacht werden darf. Oder wer sie benutzen

darf. Das wird Missbrauch allerdings niemals vollständig verhindern können, bestenfalls erschweren.

Einige KI-Modelle, die Bilder generieren können, erlauben es zum Beispiel nicht mehr, Fake-Bilder von einem verhafteten Donald Trump zu erzeugen.

Gut möglich aber trotzdem, dass schon bald KI-erzeugte Videos zu sehen sind, die genau so etwas zeigen – und für Manipulationen bei Wahlen verwendet werden. Wir müssen also wachsam bleiben – zunehmend.