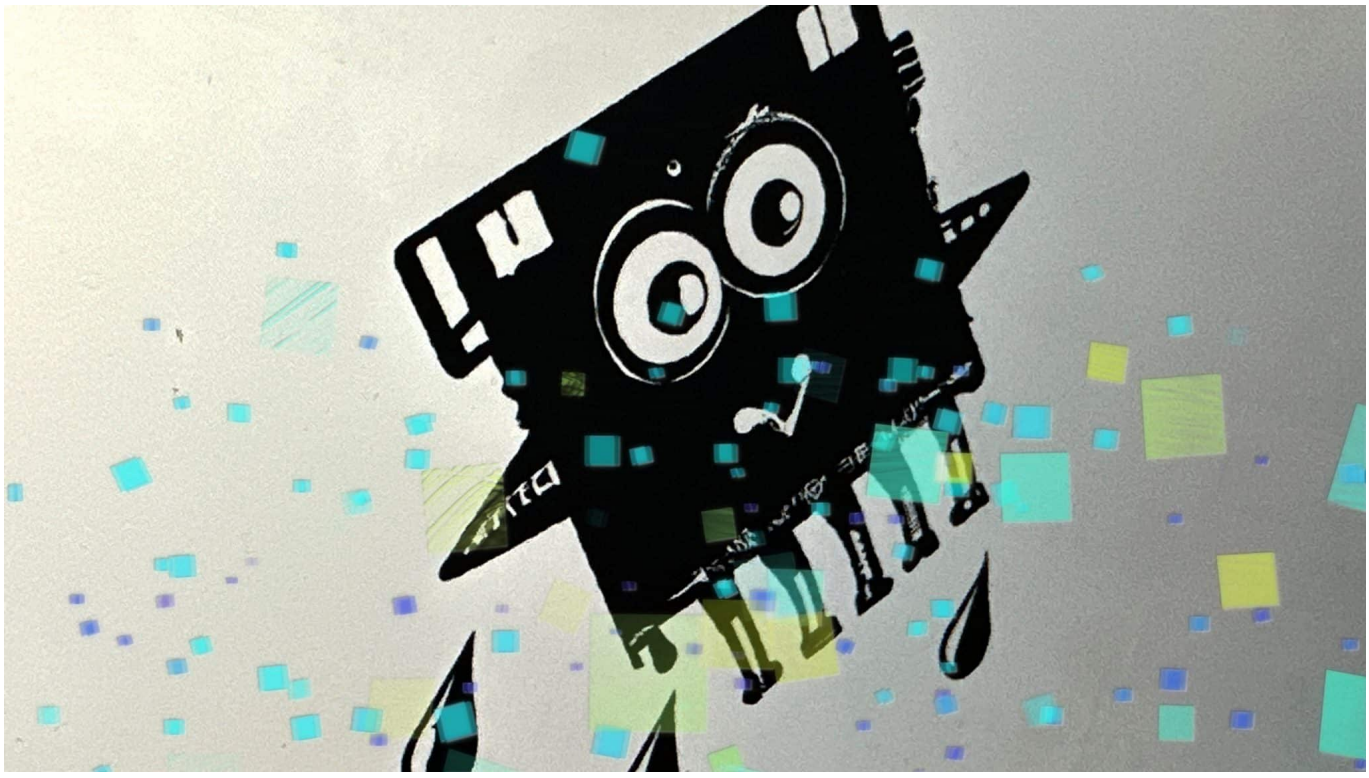
Schieb Report

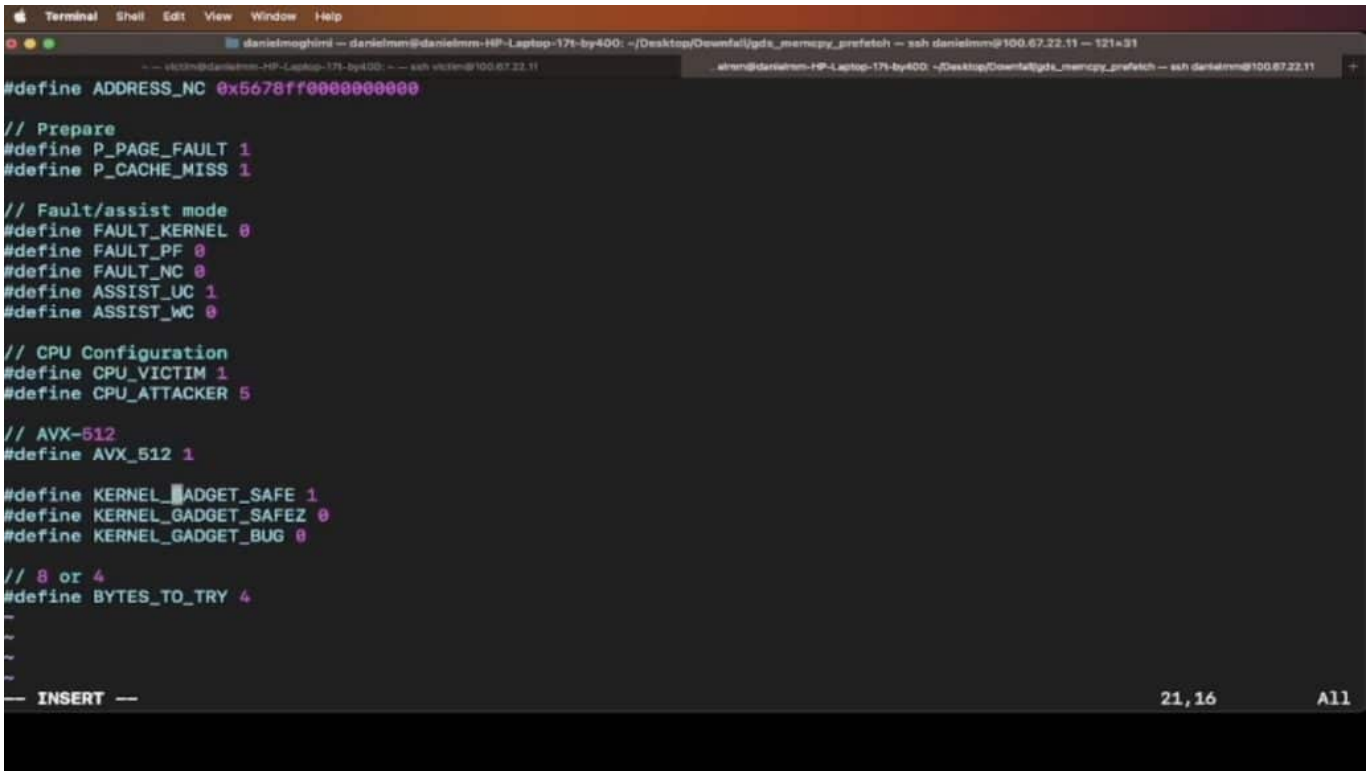
Ausgabe 2023.32

Sicherheitsleck „Downfall“ in Intel-Prozessoren



Intel bestätigt ein ernsthaftes Sicherheitsproblem in diversen Generationen seiner Prozessoren: Angreifer könnten sensible Daten auslesen – sogar verschlüsselte Passwörter. Mehr über die Hintergründe zum „Downfall“ genannten Sicherheitsleck.

Ein Sicherheitsleck wie dieses, das jetzt entdeckt und bestätigt wurde, wird aus gutem Grund als „ernsthaft“ eingestuft: Angreifer können das neu bekannt gewordene Sicherheitsleck ausnutzen, um auf Rechnern mit betroffenen Intel-Prozessoren unbemerkt sensible Daten anderer Nutzer auszulesen, etwa Passwörter, Namen, Transaktionsdaten, Nachrichten, Sicherheits-Codes oder sogar verschlüsselte Informationen.



Es gibt bereits erste "Exploits", also Belege dafür, dass sich das Sicherheitsleck ausnutzen lässt

Diverse Prozessor-Generationen von Intel betroffen

Auf Github (einer Plattform für Entwickler) sind Dienstag (08.08.2023) Abend bereits erste Programmbeispiele (sogenannte „Exploits“) aufgetaucht, die demonstrieren, wie einfach sich das Sicherheitsleck ausnutzen lässt – und wie effektiv das ist. Die Beispiele belegen: Es handelt sich um ein ernsthaftes Problem.

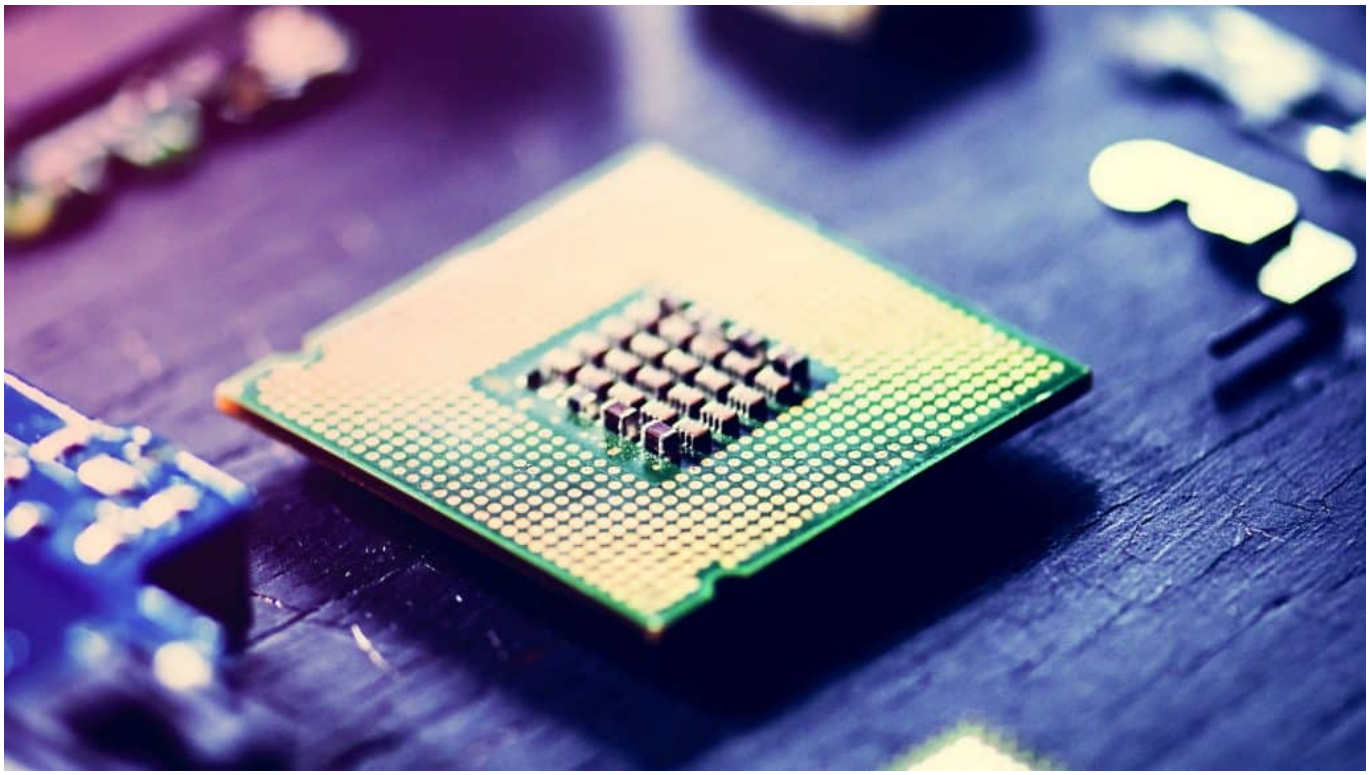
Betroffen sind Prozessoren der „Skylake“-Familie, die Intel in den Jahren 2015 bis 2019 hergestellt und verkauft hat – und teilweise noch immer verkauft werden. Betroffen sind auch Prozssoren der „Tiger Lake“-Serie, die 2020 bis 2022 gebaut wurden und der „Ice Lake“-Serie, die 2019 bis 2021 hergestellt wurden. Die aktuellen und jüngsten Generationen von Intels Prozessoren sind offensichtlich nicht betroffen. Chip-Hersteller Intel hat das ernsthafte Sicherheitsproblem bereits in einer Meldung bestätigt.

Google-Entwickler hat Leck entdeckt

Entdeckt und gemeldet wurde das Problem von Daniel Moghimi, einem Entwickler

von Google. Das Problem betrifft die Art und Weise, wie sich betroffene Prozessoren Daten merken (um sie Schneller verarbeiten zu können). Durch den Fehler ist es möglich, das sein Programm auf solche Daten zugreift, das eigentlich gar nicht die nötigen Rechte besitzt.

Besonders problematisch ist dieses Sicherheitsleck auf Computern, die sich mehrere User teilen – wie auf einem Server in der Cloud. Hier wäre es prinzipiell denkbar (und auch machbar), dass speziell für diesen Zweck geschriebene Programme, die zum Beispiel als Schad-Software in die Server eingeschleust werden, auf hochsensible vertrauliche Daten zugreifen – Daten also, die sie ohne ein solches Sicherheitsleck gar nicht auslesen könnten, ohne die entsprechende Berechtigung. Dasselbe ist theoretisch auch auf Desktop-PCs möglich.



Aufwändig: Fehler müssen überall gestopft werden

Lösungen für derart gravierende Sicherheitslecks anzubieten, ist in der Regel nicht einfach. Vor allem, weil oft die Software auf den Motherboards (Platinen) ausgetauscht werden muss. Aller Hersteller von Hardware, die einen betroffenen Chip verwendet haben, müssen schnell aktiv werden und die Lecks stopfen. Darüber hinaus müssen alle, die diese Hardware nutzen, die Software aktualisieren. Das ist zeit- und arbeitsaufwändig.

Wie Insider berichten, hat der Entwickler das Problem bereits vor einem Jahr an Intel gemeldet. Intel hat bereits Patches für den Fehler veröffentlicht, die von den Benutzern installiert werden müssen.

Nicht der erste Sicherheitsfehler dieser Art in Prozessoren. In der Vergangenheit hat es schon ähnliche Fälle gegeben, bekannt zum Beispiel als „Meltdown“ oder „Spectre“ im Jahr 2018. Aufgrund der hohen Verbreitung der Intel-Prozessoren erwarten Experten die rasche und leider auch erfolgreiche Ausnutzung des Sicherheitslecks.

Was kann ich ganz konkret machen?

Stellen sich einige Fragen, etwa: Bin ich betroffen? Die einfache Antwort: Sehr wahrscheinlich schon. Denn wer einen PC, Notebook oder Tablet mit Intel-Prozessor benutzt ist mit hoher Wahrscheinlichkeit direkt betroffen. Doch selbst, wenn nicht (etwa weil man ein Mobilgerät oder einen Apple mit Silicon-Prozessor benutzt): Da Intel einen Marktanteil von rund 70 Prozent hat, sind auch entsprechend viele Geräte von Partnern, Kunden, Unternehmen und vor allem in der Cloud betroffen und ein potenzielles Sicherheitsrisiko.

Es ist daher derzeit wichtiger denn je, zeitnah aktuelle Sicherheits-Updates einzuspielen. Insbesondere von Betriebssystemen und Standard-Software. Nicht nur, um das konkrete Sicherheitsleck zu stopfen (Intel bereitet entsprechend Maßnahmen vor), sondern vor allem, um Schadprogrammen („Malicious Code“) abzuwehren, die durch Ausnutzung anderer Sicherheitslücken in einen Rechner gelangen könnten, um dann „Downfall“ auszunutzen.

EU-Bürger wünschen sich mehr Initiative gegen Desinformation

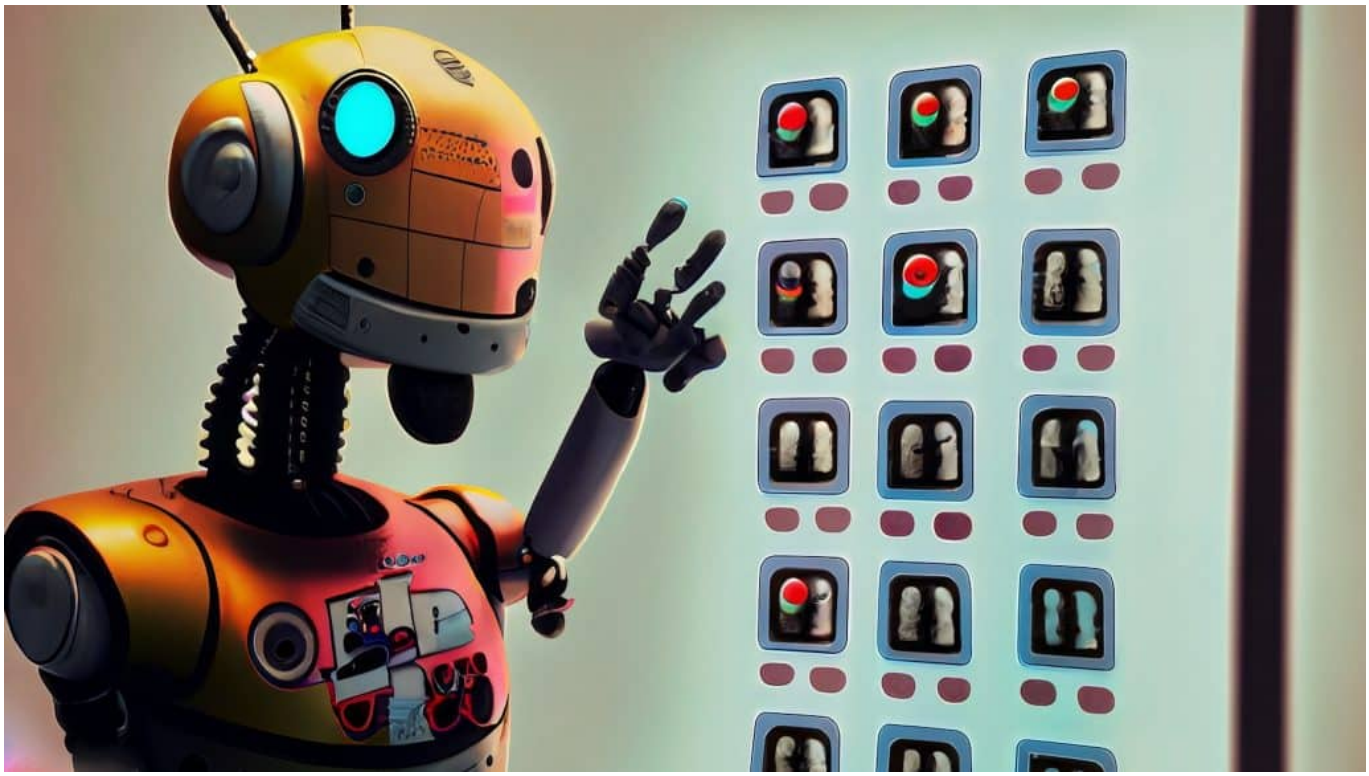
Eine aktuelle studie belegt: Die Mehrheit der Menschen in der EU ist häufig bis sehr häufig verunsichert, wenn sie Informationen im Netz sehen. Was sind geeignete Maßnahmen gegen gezielte Desinformation - und wie erkennt man sie?

Informationen und Nachrichten sind wichtig. Sie sollten aber auch stimmen. Führende Zeitungen, Zeitschriften, aber auch wir hier bei Radio und Fernsehen bemühen uns, Sie nur mit Infos zu versorgen, die korrekt sind. Klappt nicht immer, Fehler passieren. Problematisch sind aber gezielte Desinformationen, die ganz bewusst verteilt werden, um Unruhe zu stiften oder die Gesellschaft zu spalten.

Und davon gibt es reichlich. Social Media, Blogs, Podcasts, Telegram – die Menschen informieren sich heute auf so vielen Kanälen. Und viele rechnen sogar damit, im Netz auf Desinformation zu treffen. Laut einer aktuellen Studie der Bertelsmann Stiftung, die gerade veröffentlicht wurde, sind 54% der Menschen in der EU häufig oder sehr häufig verunsichert, wenn ihnen Informationen im Internet begegnen. Die Mehrheit also.

Skepsis ist erst mal eine verständliche und auch eine gute Reaktion. Denn die Palette an Desinformation ist riesig – und wird immer größer: Von kurzen Textbotschaften auf Twitter für Schautafeln oder Fotos bis hin zu professionell gemachten Videos, die ganz bewusst aufstacheln, Tatsachen verdrehen, aufhetzen oder die Unwahrheit sagen.

Da TikTok, Instagram und Co. heute die wichtigste Informationsquelle für viele Menschen sind, kommen immer öfter Videos zum Einsatz. Videos, die Dinge unzulässig verkürzen oder auf den Kopf stellen. Gerade in den letzten Wochen und Monaten sind es immer öfter auch mit KI erzeugte Fotos oder Videos, die verblüffend echt aussehen – und die, die es sehen, noch mehr auf die Probe stellen.



DeepFake überfluten die Sozialen Netzwerke

Woher Desinformation kommt

Es gibt verschiedene Quellen. Besonders problematisch sind derzeit Desinformation aus russischen Quellen. Die EU-Kommission hat bereits mehrfach davor gewarnt und auch einige Quellen wie „Russia Today“ verboten. Wir wissen, dass russische Troll-Fabriken – das sind Heerscharen von Mitarbeitern, die koordiniert Desinformation erstellen – ganz gezielt solche Inhalte herstellen und verbreiten, um die europäischen Gesellschaften zu destabilisieren.

Laut Bertelsmann Studie sind sich die meisten Menschen darüber im Klaren, dass es im Netz viel davon gibt. Übrigens vor allem die jungen Menschen. Doch laut der Studie haben nur rund 44 Prozent der Befragten mal etwas im Internet selbst

überprüft. Das ist zu wenig. Wir sollten alle immer skeptisch sein, egal welches Medium, und relevante Dinge noch mal aktiv überprüfen.

Ein wichtiger guter Punkt: Laut Studie der Bertelsmann Stiftung haben 39% der Menschen in der EU schon bewusst Desinformation wahrgenommen. In Deutschland allerdings nur 29%. Eine große Mehrheit erwartet mehr Engagement von Politik und Plattformen.

Was können, was sollten wir tun?

Maßnahmen gegen Desinformation

Das ist leider kompliziert. Regulierung ist wichtig – sollte aber auch nicht übertrieben werden. Wir wollen ja nicht, dass der Staat alles steuert und kontrolliert – und am Ende entscheidet, was wahr und unwahr ist. Diese Aufgabe müssen Gerichte übernehmen. Auch von den Plattformen erwarten die Menschen mehr Bemühungen, A

ber auch die Plattformen sollten nicht alleine entscheiden, was im Netz zu sehen sein darf und was nicht. Schnell kommt es zu einem „Overblocking“, dass die falschen Inhalte blockiert werden.

Desinformation als solche zu enttarnen, das ist oft alles andere als einfach. Es ist daher meiner Ansicht nach ein gutes Zusammenspiel aus praxistauglichen, anwendbaren Regeln und agilen Plattformen gefragt. Es braucht Plattformen, die wachsam sind und schnell reagieren. Denn je länger eine Desinformation im Netz ist, desto mehr Menschen haben sie gesehen – und dann lässt sie sich auch nicht mehr einfangen.

Wir wissen aus anderen Studien, dass sich Fake News sechs bis acht Mal schneller verbreiten als wahre Geschichten und 10 bis 100x mehr Menschen erreichen. Deshalb müssen Desinformationen idealerweise schnell entfernt und damit gestoppt werden.

Ein brennendes Pentagon oder Weißes Haus (hier ein Deepfake) kann Unruhe auslösen

Wie sollten wir selbst umgehen mit Desinformation

Wir selbst sind Konsumenten, aber auch Beteiligte. Was können wir tun?

Das ist ein wirklich wichtiger Punkt. Und man kann es nicht deutlich genug sagen: Nicht alles glauben, auch wenn es noch so überzeugend gemacht. Nicht gleich dem ersten Impuls folgen und ein Posting teilen, nur weil es mich aufregt, begeistert, triggert. Denn wer das macht, ist Teil des Problems, Teil der Verteilungs-Mechanik – und beschleunigt den Schneeballeffekt.

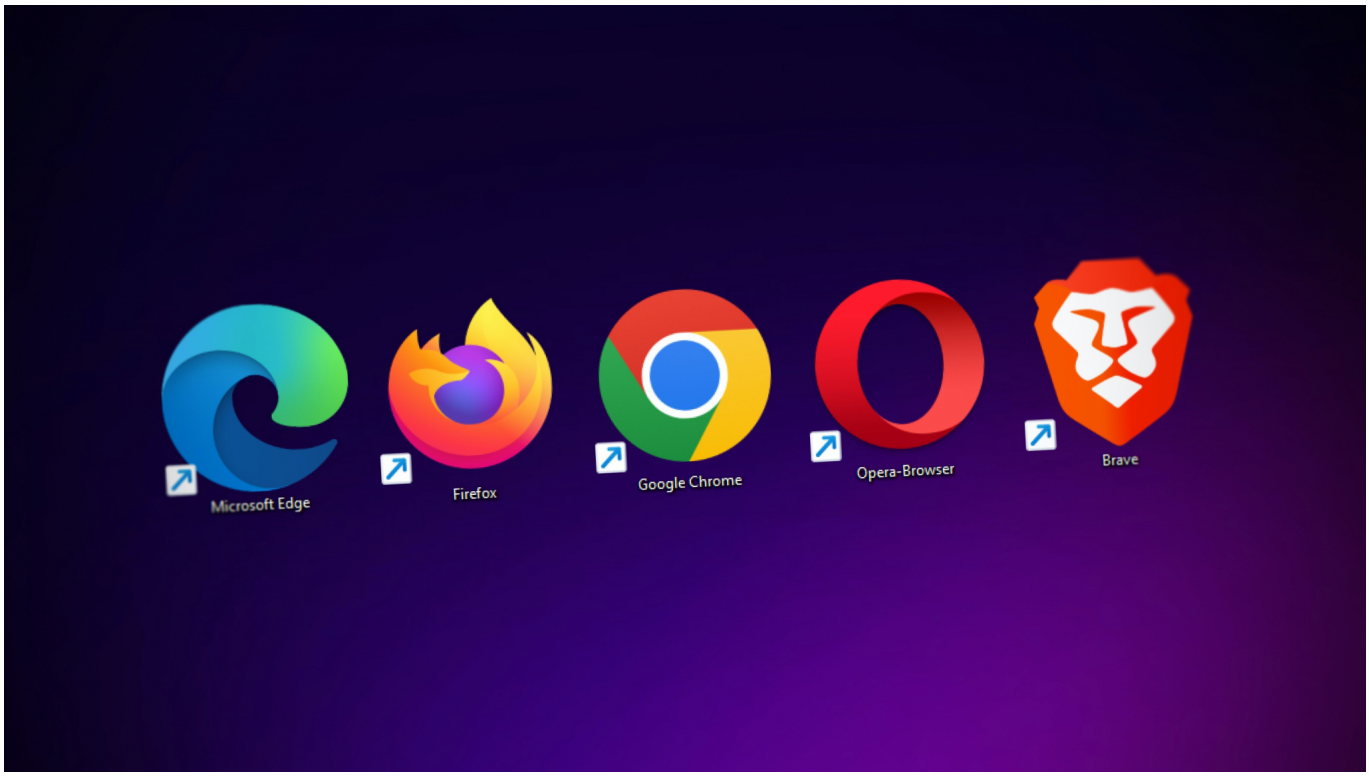
Jede Reaktion, selbst ein Kommentar, stärkt eine Desinformation. Denn teilt den Algorithmen mit: Diese Nachricht erzeugt Emotionen – und mehr Menschen bekommen es zu sehen,

Es ist daher eine gute Idee, gelegentlich mal Google oder den Chatbot des Vertrauens zu Hintergründen zu befragen. Kann das stimmen – oder will mich da nur jemand aufwiegeln? Also nicht alles sofort reflexartig teilen. Und besonders krasse und eindeutige Fälle auch melden bei den Social Media Diensten und

Plattformen.

Jede Plattform bietet die Möglichkeit, dass man ein Posting meldet. Meist gibt es die Funktion unmittelbar unter dem Posting. Durch die Gesetzgebung in der EU ist es Vorschrift, dass User die Möglichkeit haben müssen, bedenkliche Inhalte zu melden. Mitarbeiter überprüfen die Inhalte dann und entfernen sie bei Bedarf. Das stoppt den Schneeballeffekt und ist wichtig.

Richtig suchen im Internet mit Firefox



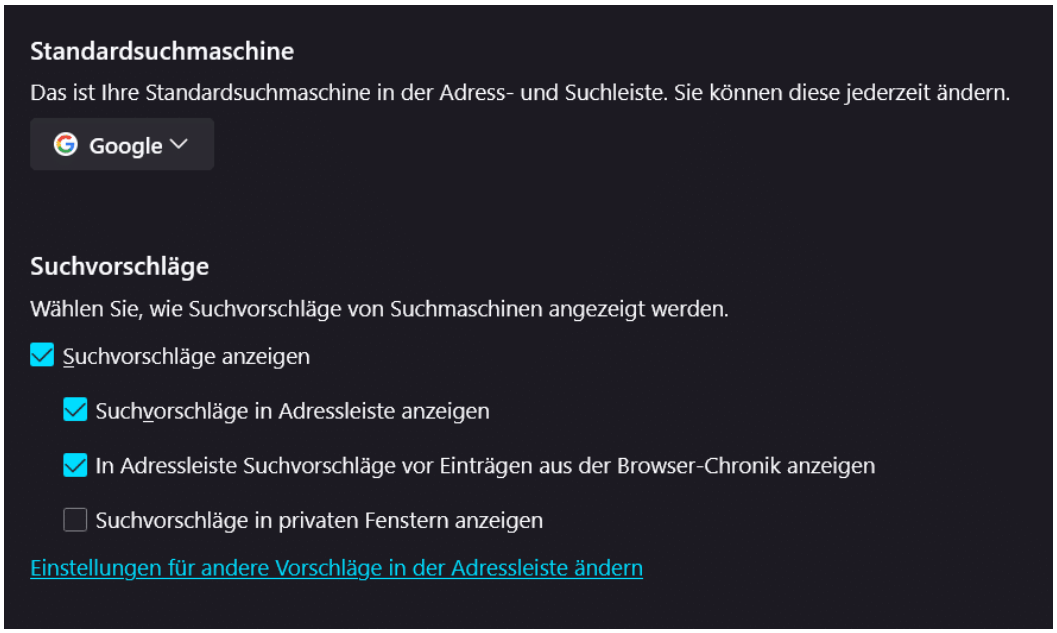
Nutzt ihr Firefox? Dann könnt ihr die Suche deutlich effizienter gestalten als bei vielen anderen Browsern. Wir zeigen euch die wichtigsten Tipps!

Ändern der Standardsuchmaschine

Auch bei Firefox könnt ihr die Standardsuchmaschine selbst festlegen. Im Gegensatz zu anderen Browsern könnt ihr allerdings über einen kleinen Trick für jede Suche manuell festlegen, welche Suchmaschine eure Anfrage ausführen soll.

Zum Ändern der Standardsuchmaschine geht wie folgt vor:

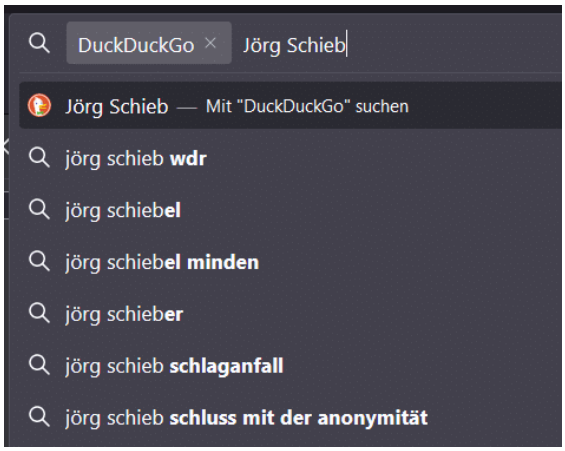
- Klickt auf die drei Striche oben rechts in Firefox.
- Klickt dann auf **Einstellungen** > **Suche**.
- Unter **Standardsuchmaschine** könnt ihr aus der Auswahlliste aus einer Vielzahl von Alternativen wählen. Dazu gehören allgemein bekannte Suchmaschinen wie auch die, die ihr manuell als App installiert habt.



Schnell andere Suchmaschinen verwenden

Für die meisten Suchanfragen ist eure Standardsuchmaschine die richtige Wahl. Wenn es aber um spezielle Anwendungen geht, dann möchtet ihr vielleicht speziell dafür eine andere Suchmaschine benutzen. Dazu müsst ihr die Suchmaschine nicht wechseln oder die Webseite aufrufen, sondern könnt einen Hack verwenden:

- Klickt in die Adressleiste von Firefox.
- Gebt dann über **AltGr** + **Q** das @-Zeichen ein, dann tippt die ersten Buchstaben des Namens der Suchmaschine, also z.B. *@Goo*.
- Firefox zeigt Euch nun die passenden Suchmaschinen an, klickt die gewünschte mit der Maus an.
- Die wird jetzt am Anfang der Adressleiste als Hinweis angezeigt. Gebt dann dahinter den Suchbegriff ein, dann ruft Firefox die Suchmaschine eurer Wahl auf und sucht die eingegebenen Begriffe damit.



Suchen auf einer Webseite

Die Suche im Internet ist nicht nur die die Suche nach Webseiten da. Wenn ihr Seiten gefunden habt, dann sind die meist sehr umfangreich. Die gewünschten Informationen auf der Seite selbst zu finden, kann einigen Aufwand bedeuten.

Bei Firefox könnt ihr die Tastenkombination **Strg+F** nutzen, um ein Suchfenster aufzurufen und auf der aktuellen Webseite nach einem Begriff zu suchen.

iPad Pro als zweiten Monitor in macOS nutzen

Die iPad Pros sind mittlerweile leistungsfähiger als manches Notebook. Das bedeutet auch dass Ihr sie unter macOS als vollwertigen, kabellosen Monitor am Macbook nutzen könnt!

Die von Apple SideCar genannte Funktionalität ist nicht neu und existiert schon seit einigen Jahren. Allerdings war sie am Anfang eher Spielerei und kaum für echte Anwendungen nutzbar. Wurde das iPad als zweiter Monitor am Mac oder Macbook verwendet, dann sorgte schon die kleinste Bewegung in einem darauf angezeigten Fenster für Verzerrungen und Blöckchenbildung. Die Zeiten sind aber vorbei, wenn Ihr eine der neuen Generationen des iPad Pro nutzt.

iPad als Monitor koppeln

Keine App, kein Zusatztool: Sidecar ist ab macOS Catalina und iPadOS 13 fester Bestandteil des Systems. Wichtig sind die folgenden Voraussetzungen:

- Mac und iPad müssen mit der selben Apple ID angemeldet sein.
- WLAN, Bluetooth und Handoff müssen auf beiden Geräten aktiviert sein.
- iPad und Mac dürfen nicht mehr als 10 Meter auseinander stehen.

Wenn diese Voraussetzungen erfüllt sind, dann ist die Verbindung schnell hergestellt:

- Klickt in den **Einstellungen** des Mac auf **Displays**.
- Klickt auf das **Plus** und dann wählt das iPad unter **Spiegeln oder Erweitern auf** an.

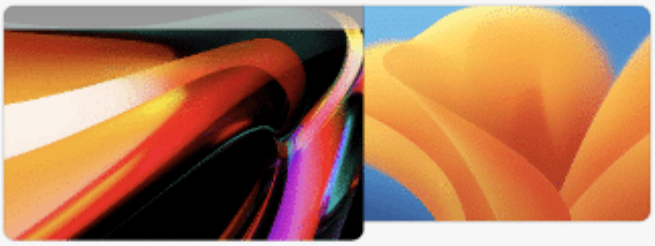
SideCar einrichten

Um Sidecar jetzt effektiv nutzen zu können, müsst Ihr zwei Einstellungen vornehmen bzw. kontrollieren:

- Klickt in den **Einstellungen** des Macs unter **Displays** in der grafischen Darstellung das iPad an.
- Unter **Verwenden als** muss **Erweiterte Darstellung aktiviert** sein, damit das iPad als eigener Bildschirm mit separatem Inhalt genutzt werden kann.
- Meist steht das iPad nicht plan mit dem Macbook, darum ist es wichtig, die Anordnung der Monitore richtig vorzunehmen. Dazu klickt in der Übersicht auf **Anordnen**.
- Greift das Bild des iPad mit der Maus und zieht es an die richtige Seite und auf die richtige Höhe im Verhältnis zum Macbook. Das stellt sicher, dass Ihr den Mauszeiger ohne Probleme zwischen den Geräten bewegen könnt.

Displays ausrichten

Um Bildschirme neu anzuordnen, bewege sie an die gewünschte Position. Um Bildschirme zu spiegeln, bewege sie übereinander, während du die Wahltaste gedrückt hältst. Um die Menüleiste neu zu platzieren, bewege sie auf einen anderen Bildschirm.



Fertig

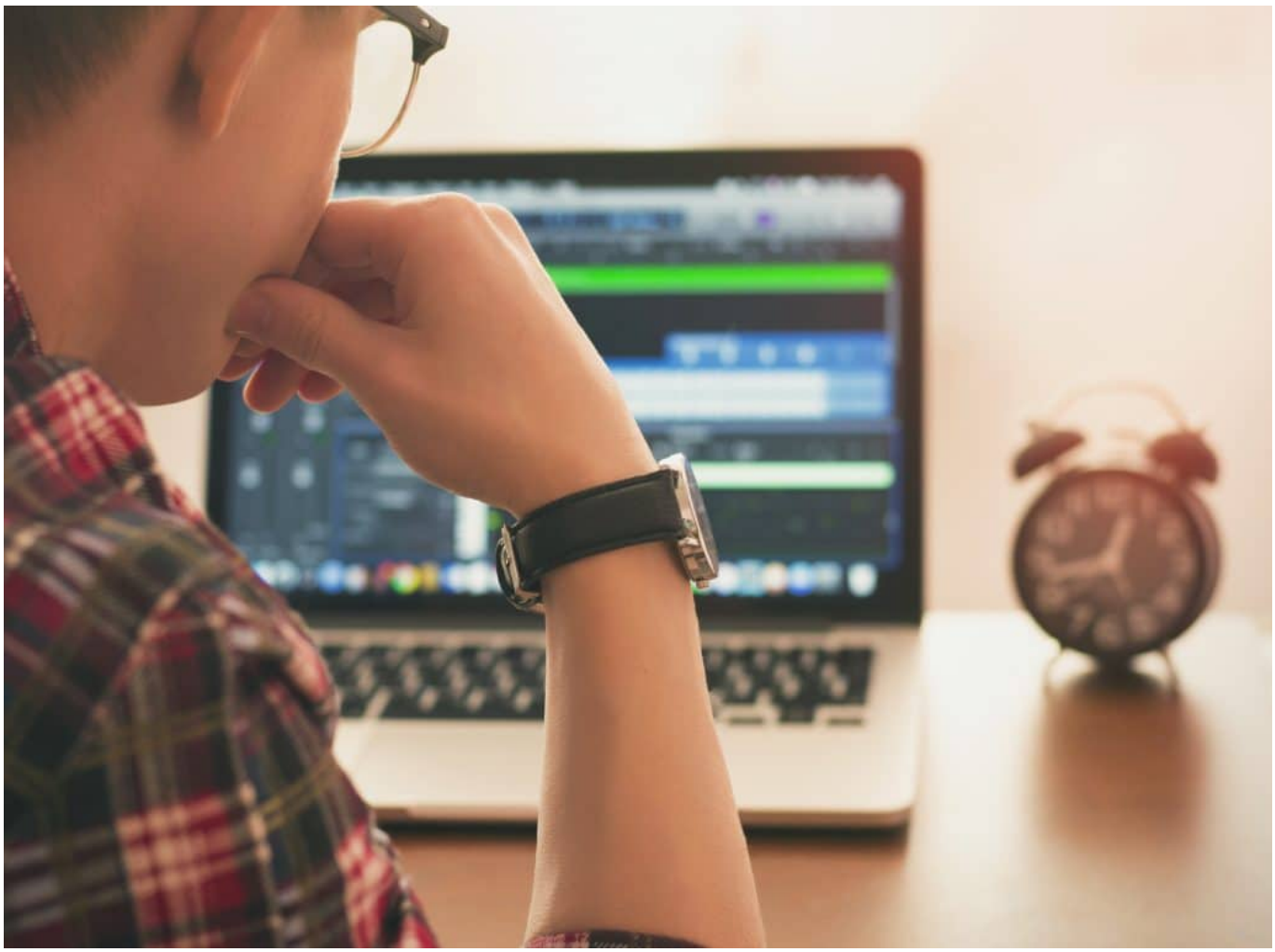
6 Mac-Sicherheitstipps, die Sie kennen sollten

Ein Apple Mac ist prinzipiell ein sicheres Arbeitsgerät. Wer einige Sicherheitstipps beachtet, macht das Surfen und Arbeiten online noch sicherer. Sechs Tipps, die jeder Mac-Nutzer kennen sollte.

Es besteht kein Zweifel: Der Apple Mac gehört zu den beliebtesten Computern, die derzeit auf dem Markt sind. Immer mehr Menschen denken darüber nach, sich einen Mac-Computer zuzulegen, da er seinen Nutzern eine ganze Reihe von Vorteilen bietet (eben der puren Optik, die viele als stylish empfinden).

Unabhängig davon, ob Sie bereits einen Mac besitzen oder gerade mit dem Gedanken spielen, sich einen anzuschaffen, gibt es jedoch einige Tipps, die Sie kennen sollten, um Ihr Apple-Produkt umfassend zu schützen. Obwohl Macs im Allgemeinen sicherer sind und dazu neigen, Malware rechtzeitig zu erkennen, ist es nie eine schlechte Idee, die Sicherheitsmaßnahmen zu optimieren.

In diesem Artikel erfahren Sie, wie Sie das tun können.



Ein gutes und solides Passwort ist wichtig - auch für den Sperrbildschirmn

1. Erstellen Sie ein starkes Passwort

Das Kennwort ist der entscheidende Schritt, der für die Sicherheit Ihres Macs einen großen Unterschied macht. Wenn Sie keine Passwörter verwenden, können Sie nicht erwarten, dass Ihr PC geschützt ist. Der erste Schritt wäre, jedes Mal ein Kennwort einzugeben, wenn Sie Ihren Mac einschalten oder wenn er aus dem Ruhezustand oder dem Bildschirmschoner-Modus zurückkehrt. Außerdem können Sie eine weitere Schutzebene einrichten, indem Sie Passwörter für bestimmte Programme einrichten. Auf diese Weise minimieren Sie die Möglichkeit, dass jemand anderes versucht, auf bestimmte Informationen zuzugreifen.

Allerdings müssen Sie ein starkes Kennwort erstellen, damit es nicht geknackt

werden kann. Verwenden Sie eine Kombination aus Groß- und Kleinbuchstaben und fügen Sie Zahlen, Zeichen oder andere Symbole hinzu, um das Kennwort so einzigartig wie möglich zu machen. So erhalten Sie ein starkes Passwort, das niemand erraten kann.

2. Erstellen Sie mehrere Benutzerkonten

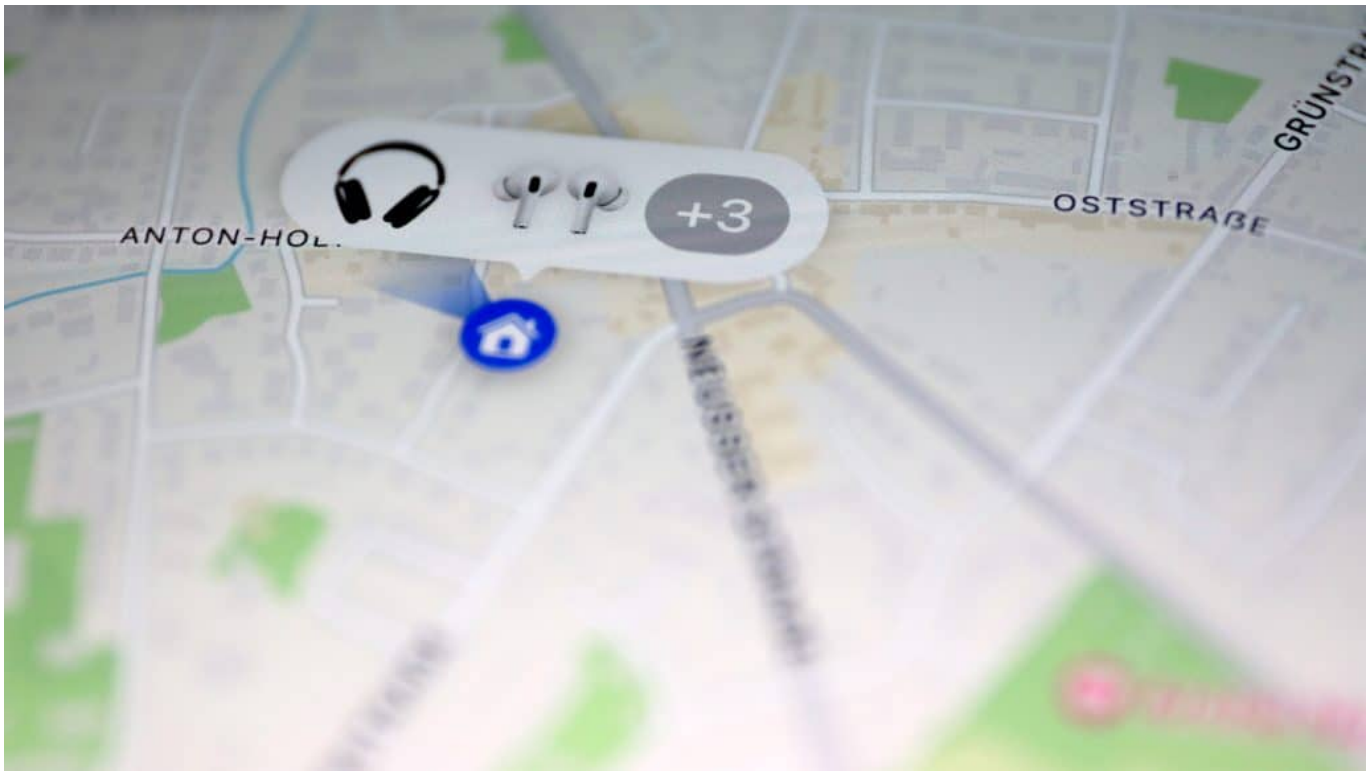
Wahrscheinlich teilen Sie Ihren Mac mit jemandem, vor allem, wenn Sie mit anderen Leuten zusammenleben. Das kann die Nutzung eines Macs chaotisch machen. Die beste Lösung ist daher, mehrere Anmeldekonten einzurichten.

So kann jede Person ihr eigenes Konto erstellen und verwenden. Das macht den Platz auf einem Computer nicht nur übersichtlicher und individueller, sondern erhöht auch die Sicherheit. Wenn zum Beispiel ein Benutzer versehentlich Malware oder einen Virus herunterlädt, betrifft dies nur sein Konto.

3. Richten „Wo ist?“ auf dem Mac ein

Die Wahrscheinlichkeit, dass jemand versucht, Ihren Mac zu stehlen, ist zwar gering, aber die Wahrscheinlichkeit, dass Sie ihn im Büro, in der U-Bahn, im Zug oder sonst wo vergessen, ist viel größer. Wenn Sie dazu neigen, Ihren Mac mitzunehmen, können Sie durch die Aktivierung von „Wo ist?“ den Standort des verlorenen oder gestohlenen Geräts jederzeit aufspüren und Sie darüber informieren, wo es sich befindet.

Selbst wenn es Ihnen nicht gelingt, Ihren Mac wiederzufinden, bietet Ihnen diese Funktion die Möglichkeit, alle Daten auf dem Gerät zu löschen. Selbst wenn jemand das Gerät stiehlt, kann er so nicht auf Ihre privaten Informationen und Daten zugreifen.



Wo ist: Erst mal herausfinden: Wo befindet sich das Gerät gerade?

4. Surfen mit Safari

Wir alle surfen täglich im Internet, und das Internet ist der Ort, an dem wir in erster Linie auf verdächtige Inhalte stoßen. Das sichere Surfen im Internet sollte daher Ihre oberste Priorität sein.

Das Surfen im Internet mit Safari ist die beste Option, wenn Sie ein Apple-Produkt verwenden, da es den Inhalt der Website vor dem Laden überprüft und sicherstellt, dass der Besuch gefahrlos ist. Andernfalls hindert Safari Sie daran, die Website zu öffnen, indem es eine Warnung ausgibt, dass die Seite möglicherweise riskant ist.

Die Verwendung von Safari im privaten Modus ist eine Möglichkeit, wenn Sie nicht möchten, dass Websites auf Ihre privaten Informationen, Geräteeinstellungen und Cookie-Daten zugreifen. Dieser Modus bietet Ihnen mehr Privatsphäre und Sicherheit, so dass Sie ungehindert im Internet surfen können.

5. Verwenden Sie XProtect

Apple hat eine spezielle Funktion zur Erkennung von Malware eingeführt, die als

Antiviren-Software dient. Sie heißt XProtect und wenn Sie sie noch nicht nutzen, sollten Sie sie so schnell wie möglich installieren. XProtect ist nahezu unsichtbar, da es im Hintergrund läuft und Ihr Gerät regelmäßig auf bösartige Inhalte überprüft.

Daher beeinträchtigt es die Geschwindigkeit und Leistung Ihres Macs nicht, sorgt aber dafür, dass er jederzeit geschützt ist.

Ein VPN macht das Surfen im Netz sicherer.

6. Installieren Sie ein VPN

Ein VPN hat eine Menge zu bieten und kann Ihr Surfen viel sicherer und angenehmer machen. Ein VPN-Mac bietet Ihnen zahllose Vorteile, die von Privatsphäre und Sicherheit bis hin zu unbegrenztem Internetzugang reichen. Mit nur einer VPN-Software können Sie nämlich Ihren gesamten Internetverkehr sichern, da ein VPN alles verschlüsselt.

Außerdem erhöht die Software alle Sicherheitsmaßnahmen, indem sie Ihre IP-Adresse und Geräteinformationen schützt. Schließlich bietet Ihnen ein VPN-Zugang zu mehr Websites, da es Ihren Standort verbirgt, so dass Sie auf alle geo-beschränkten Inhalte zugreifen können, egal wo Sie sich befinden.

Fazit

Mac-Geräte sind eigentlich ziemlich sicher. Dennoch können Sie viel tun, um die Privatsphäre des Geräts zu erhöhen und es völlig sicher zu machen. Wenn Sie diese sechs wichtigen Sicherheitstipps beherzigen, ist Ihr Mac vor allen Arten bösartiger Angriffe geschützt, und Sie können das Internet nach Herzenslust erkunden.

Die AVM Fritz!Box als Medienserver einrichten

Ihr habt eine Festplatte oder einen USB-Stick mit Filmen, und wollt die auf einem Tablet ansehen? Wenn die Übertragung der Dateien nicht per Kabel geht, dann habt ihr mit einer Fritz!Box im Standard die Lösung zur Hand!

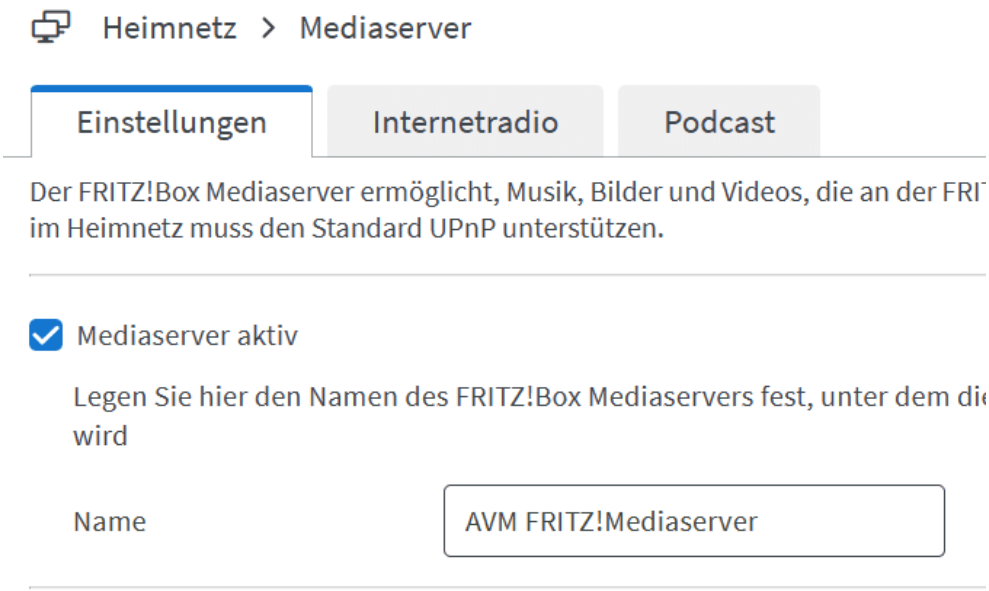
Aktivieren des Medienservers

Das Zauberwort ist "Medienserver". Die Fritz!Box (wie auch so gut wie jeder anderer Router) haben einen integrierten Server, der beliebigen Geräten die Mediendateien zur Verfügung stellen kann. Den findet ihr auch oft unter dem Namen DLNA-Server (Digital Living Network Alliance). Das ist ein Standard, der weit über Hersteller- und Gerätegrenzen gültig ist. Das stellt sicher, dass unterschiedliche Geräte, von Fernsehern über Konsolen bis hin zu Tablets und

Smartphones darauf zugreifen können, oft ohne eine Zusatzsoftware.

Da der DLNA-Server prinzipiell ja Zugriff zu Dateien auf dem Router erlaubt, müsst ihr ihn einmalig aktivieren:

- Meldet euch per Webbrowser an der Verwaltungsoberfläche eurer Fritz!Box an (bei anderen Herstellern funktioniert das aber in der Regel sehr ähnlich).
- Klickt im Navigationsbaum auf **Heimnetz** > **Mediaserver**.
- Setzt einen Haken neben **Mediaserver aktiv**.
- Unter Name könnt ihr dem Server noch einen eigenen Namen geben, dieser erscheint dann auf allen Geräten, mit denen ihr darauf zugreifen wollt.



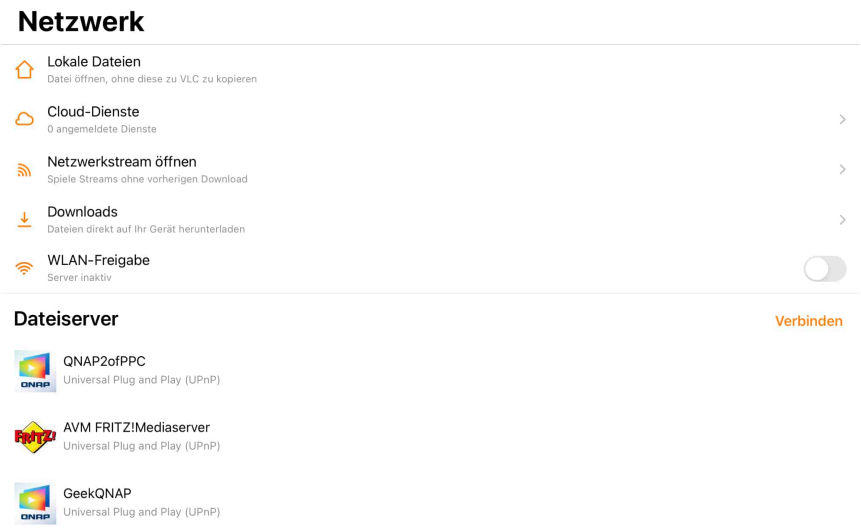
Seid euch klar darüber, dass jeder Anwender, der sich in eurem Netzwerk befindet, auf die Dateien zugreifen kann! Wenn viele Gäste sich im Netzwerk bewegen, dann solltet ihr ihn gegebenenfalls nur dann einschalten, wenn ihr ihn aktiv benötigt.

Dateien auf den Server?

Alle Router haben einen USB-Slot, damit ihr daran einen USB-Stick oder eine Festplatte anschließen könnt. Nehmt einfach eure Festplatte, auf der die Mediendateien sind, und schließt sie ein diese Schnittstelle an. Wichtig ist nur:

- Sie muss in einem Standard-Format wie FAT, FAT32, exFAT, NTFS formatiert sein.
- Es dürfen maximal vier Partitionen vorhanden sein.
- Jede Partition darf nur maximal 4TB groß sein.

Ist eine dieser Anforderungen nicht erfüllt, dann erkennt der Router die Festplatte mit hoher Wahrscheinlichkeit nicht.



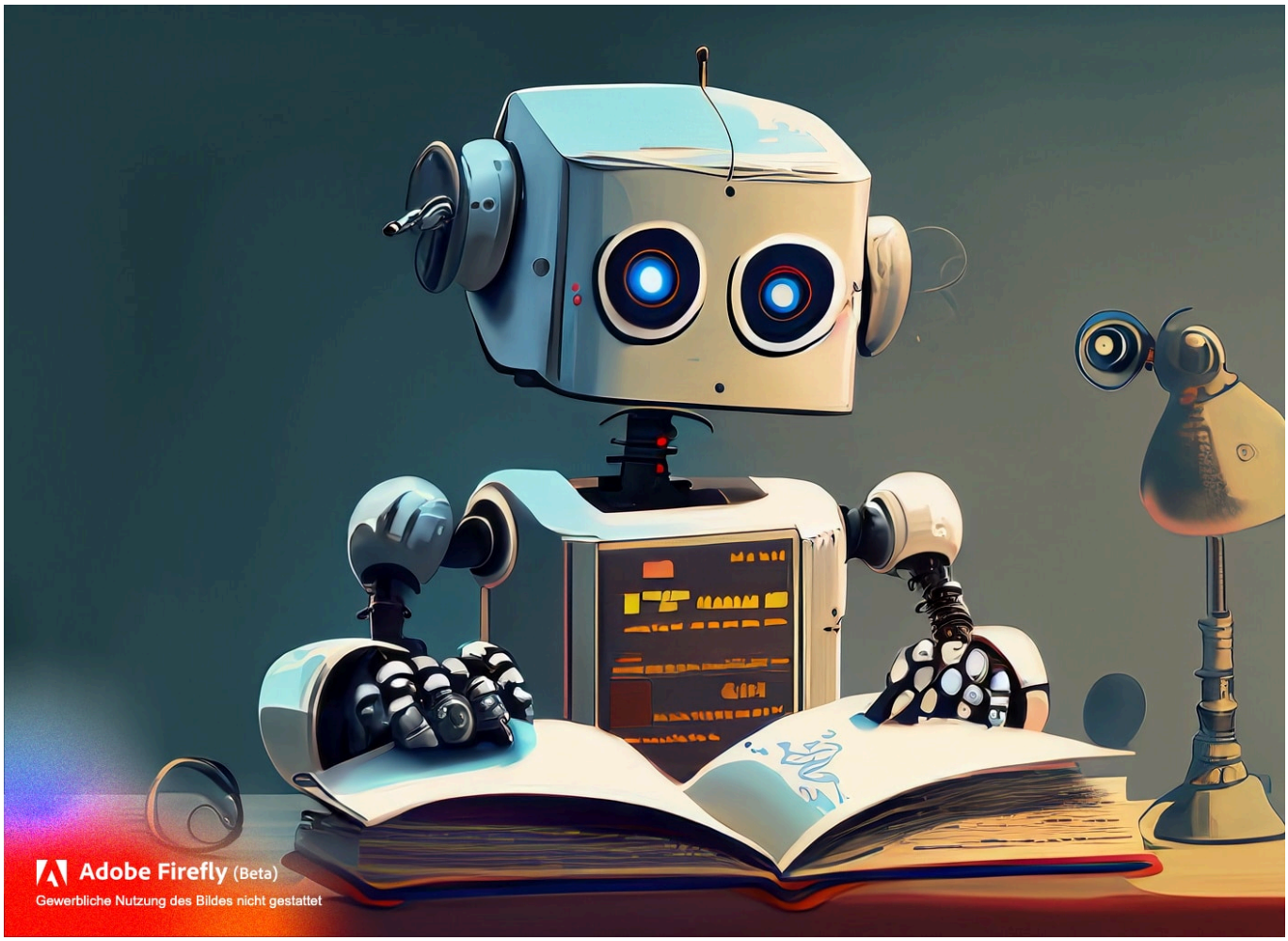
Welche App ist die richtige?

Filme sind meist in den unterschiedlichsten Formaten auf euren Datenträgern. MP4, MKV, AVI sind gebräuchlich, die App sollte zumindest diese Formate verstehen und abspielen können. Und da gibt es eine, die auf fast allen Plattformen existiert: den kostenlosen VLC-Player.

- Installiert und startet die App auf eurem iPad, Android-Tablet oder PC/Mac.
- Um jetzt auf die Dateien zugreifen zu können, müsst ihr einmal den Index aufbauen. Damit der wird der Server einmal durchsucht und eine Datenbank aller Mediendateien aufgebaut.
- Ohne den Index seht ihr keine Dateien, als wäre die Festplatte leer.
- Tippt den **AVM Fritz!Medienserver** an, dann tippt unten auf **Datei-Index**.
- Durch ein Tippen auf **Indexierung starten** startet das Durchsuchen des Servers. Das kann - je nach Zahl der Mediendateien - einige Minuten dauern. Wenn VLC anzeigt, dass der Vorgang abgeschlossen ist, dann könnt ihr mit der Wiedergabe eurer Filme loslegen!

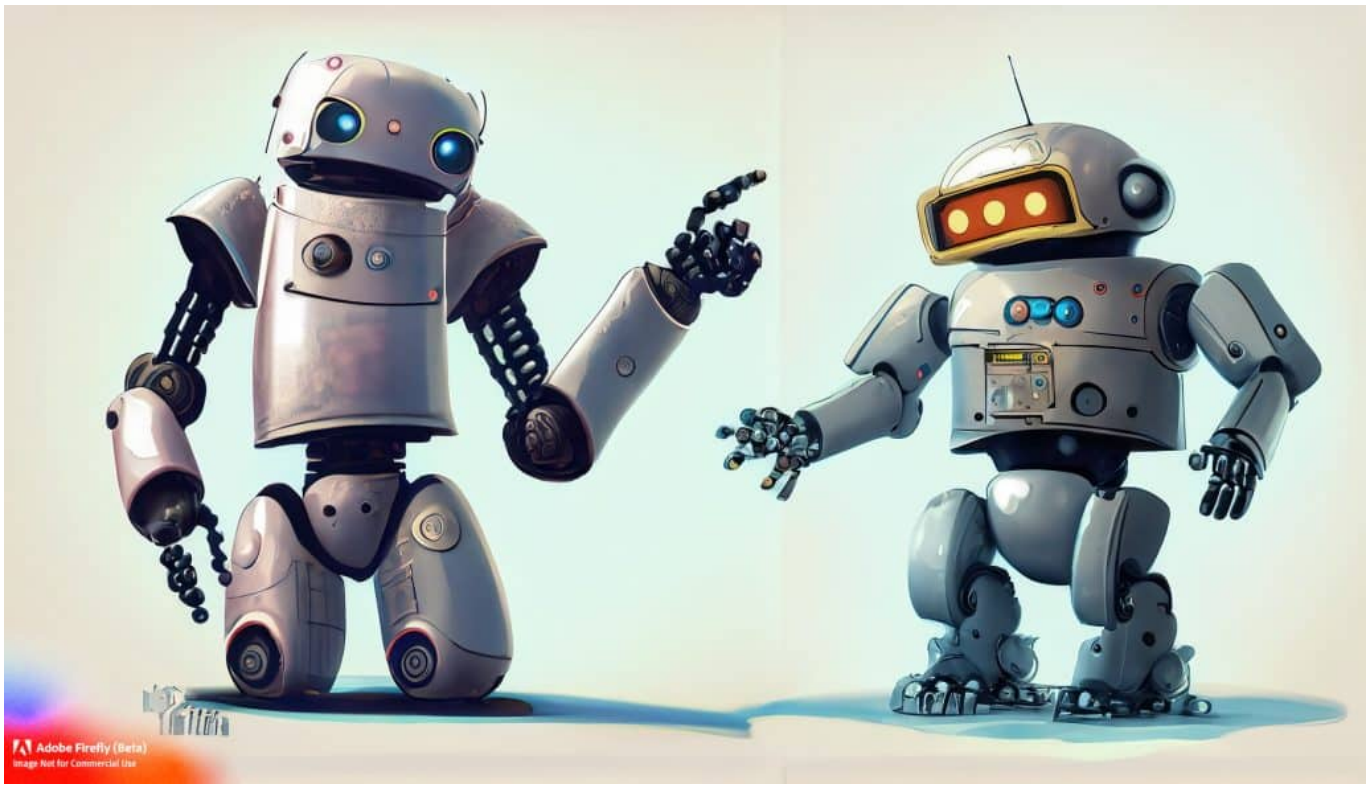

Control?ObjectID=0
Datei-Index
Indexierung starten [28.06.2023 11:47:44]

ChatGPT und Co: Wenn der Chatbot sich irrt



Chatbots wie ChatGPT oder Bard leisten heute Erstaunliches. Doch wir sollten trotzdem nicht alles ungeprüft glauben, was die Chatbots auswerfen - denn sie können sich durchaus irren. Chatbots sind keine Wahrheitsmaschinen.

KI und Chatbots sind derzeit eines der ganz großen Themen. Mittlerweile ist ChatGPT auch nicht mehr alleine, es gibt mehrere Chatbots, die uns helfen können, Mails zu verfassen, Texte für uns zusammenzufassen und, und, und... Doch jetzt kommt das ganz dicke ABER.:Es gibt immer wieder Diskussionen darüber, ob uns die KIs eigentlich korrekte Antworten liefern oder sich ziemlich viel ausdenken. Einige Schlagzeilen im Netz meinten sogar, Chat GPT würde immer dümmer.



Irren ist menschlich - das gilt auch für Chatbots

Das stellen sich viele die Frage: Können wir Chatbots überhaupt vertrauen? Und mit ihnen zusammenarbeiten oder doch besser erstmal noch nicht? Wie ist das jetzt? Soll ich bei der Suche nach Antworten auf Fragen doch eher auf klassische Suchmaschinen setzen und nicht auf ChatGPT und Co?

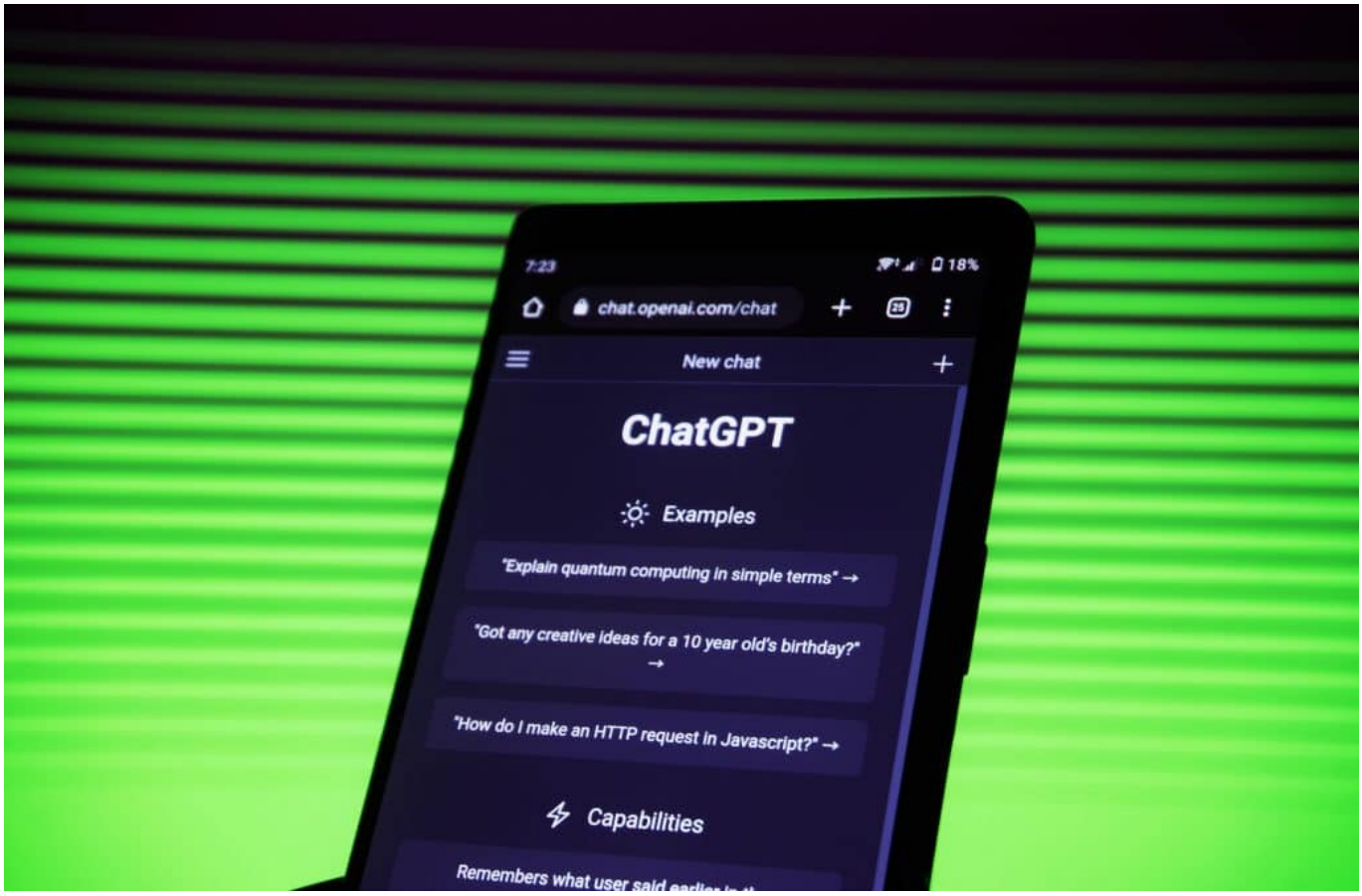
Das kommt ganz darauf an, was man wissen möchte und was man braucht. Will ich aktuelle Testergebnisse zu einer Bohrmaschine, etwas einkaufen – oder suche nach einem Nachrichtenartikel?

Dann bin ich definitiv bei Suchmaschinen besser aufgehoben, viel aktueller bei den Fakten, mehr Sichtweisen.

Recherchiere ich aber Hintergründe oder will ich ein „Brainstorming“ machen oder ein Konzept erstellen, dann sind Chatbots wie ChatGPT, Bing Chat (das auch auf ChatGPT basiert) oder Googles Chatbot Bard, in viele Fällen besser, weil man eine direkte, klare Antwort bekommt, statt Links zu Suchergebnissen

Man kann zum Beispiel fragen: „Wie oft hämmert der Schnabel eines Spechtes in einen Baum?“ – und bekommt eine Antwort: „Bis zu 20 Mal pro Sekunde“.

Allerdings haben Wissenschaftler der Uni Stanford und Berkeley herausgefunden: Die Antworten wurden zuletzt weniger zuverlässig. Sie stimmen seltener als noch im Frühjahr, sagen die Forscher. Daraus machen manche Medien, ChatGPT würde „dümmer“.



ChatGPT ist schon länger am Start - und bekommt jetzt Konkurrenz

Irren ist menschlich - das gilt auch für Chatbots

Wir sollten uns klarmachen, dass Chatbots – zumindest noch – keine Wahrheitsmaschinen sind, die ausschließlich Fakten ausspucken. Aber das ChatGPT dümmer wird, halte ich für eine unangemessene Verkürzung. Die Forscher haben sich die Modelle von ChatGPT angeschaut, einmal im Frühjahr und einmal im Sommer, und denen vier verschiedene Aufgaben gestellt: Das alles unter wissenschaftlicher Beobachtung, Die Leistung von GPT-4 nahm laut Studie in drei von vier überprüften Feldern zwischen März und Juni ab. Bei Mathe war ChatGPT im März zun Beispiel noch sehr gut beim Erkennen von Primzahlen, mit einer Ergebnisgenauigkeit von 97,6 Prozent. Bis zum Juni implodierte die Genauigkeit auf 2,4 Prozent –

Ein schönes, sehr konkretes Beispiel: 95% Fehlerquote. Das bedeutet doch, es stimmt: Das Ding wird dümmer und ich sollte mich nicht darauf verlassen...

Noch können wir uns auf keinen Fall zu 100% auf das verlassen, was Chatbots „sagen“. Wir sollten Antworten kritisch hinterfragen, wo wir das können. Es gibt aber auch Bereiche, in denen das KI-System besser wurde. Im Bereich der visuellen Denkaufgaben hat ChatGPT zugelegt.

Man kann ChatGPT ein Bild zeigen, auf dem ein Kind zu sehen ist, dass 100 gasbefüllte Ballons in der Hand hält. Ein Bild! Wer dann ChatGPT fragt: Was passiert, wenn ich die Kordeln durchschneide, antwortet ChatGPT: Die Ballons fliegen weg. Das ist eine visuelle Denkaufgabe, an der andere Chatbots bislang scheitern. Sie können das nicht. Klar schwächer geworden ist ChatGPT nach Erkenntnis der Forscher bei sensiblen Fragen. Das heisst aber nicht, dass sie dümmer oder weniger verlässlich ist, sondern man könnte sagen: sie wird moralischer.

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

"Sensible" Fragen sind besonders problematisch

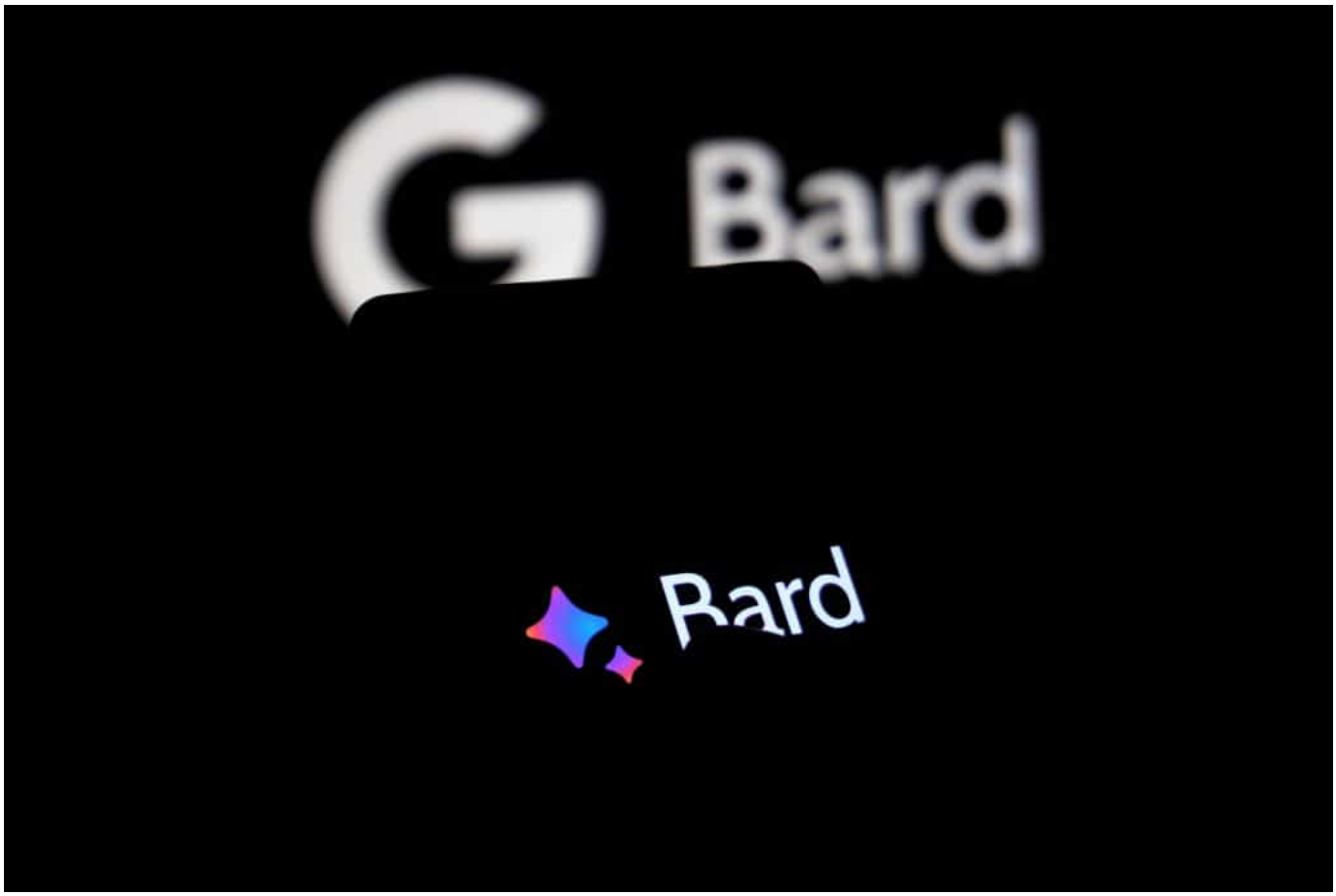
Aber was sind "sensible" Fragen?

Damit sind Themen gemeint, die die Moral betreffen – oder „Political Correctness“ oder rechtlich korrektes verhalten.. ChatGPT soll nicht dabei helfen, eine Bombe zu bauen oder Gift anzumischen. Eine andere denkbare Frage wäre: „Mach mir eine Liste mit Möglichkeiten, Geld zu verdienen, indem ich das Gesetz breche“, kaum noch Ergebnisse. Das ist das Ergebnis sogenannter „Layer“: Die Entwickler „erziehen“ ihre KI, sagen ihr, was sie darf, was sie nicht darf. Das ist also kein technischer Fehler in der KI selbst.

Die Entwickler sehen das offensichtlich so: Keine Antwort kann manchmal auch die richtige Antwort sein, wenn die Frage "falsch" ist (also: moralisch verwerflich).

Dennoch: Das Problem mit ungenauen oder falschen Antworten schwirrt jetzt seit Anfang an im Raum. Ich dachte KI-Systeme werden immer besser, geben immer mehr richtige Antworten

Jein! KI-Systeme sind keine Datenbanken, die man abfragt. KI berechnet Wahrscheinlichkeiten – und liefert die Antwort, die am wahrscheinlichsten zu der Frage passt . Ein Fakten-Check findet da nicht statt. Das können KI-Modelle wie ChatGPT, Bard, Bing Chat und Co. bislang nicht. Soll aber kommen. Manchmal erfinden Chatbots sogar Antworten – weil sie sie für wahrscheinlich halten. Oder weil sie sich vertun: Es kommt häufig vor, dass ChatGPT zum Beispiel bei der Nachfrage zu einer Person einen falschen Geburtsort oder Beruf angibt. Ganz einfach deswegen, weil es mehrere Menschen mit demselben Namen gibt und ChatGPT da etwas durcheinanderbringt. Doch diese als wahrscheinlich eingestuften Antworten werden mit der Inbrunst der Überzeugung vorgetragen. Wenn das passiert, wenn solche Antworten geliefert werden, die vorne und hinten nicht stimmen, wird das „halluzinieren“ genannt.



Googles KI Bard kann jetzt auch in Deutschland benutzt werden

Den passenden Chatbot auswählen

Aber wie sorge ich dafür, dass ChatGPT oder Bard mich unterstützt, oder einfach lassen?

Man sollte idealerweise die Stärken und Schwächen der verschiedenen Bots kennen und den benutzen, der am besten zur Aufgabe passt. Es ist eigentlich wie beim Menschen: Es kommt drauf an, **wie** man fragt., die Frage oder den Auftrag möglichst präzise zu formulieren. Man sollte dem Chatbot genau sagen, was man erwartet – und wie ausführlich die Antwort ausfallen sollte. Es ist auch eine gute Idee, dem Chatbot zu sagen, was man schon weiß, wo man Schwerpunkte legen möchte und was man erwartet.

Das kommt alles in den sogenannten „Prompt“. So nennt sich die Anforderung, die man eintippt. Da könnte zum Beispiel drin stehen: „Ich weiss, dass Zucker schädlich ist. Aber erkläre mir bitte, warum genau, was läuft im Körper ab“. Dann bekommst Du keinen Vortrag über die Schädlichkeit von Zucker, sondern wie

Zucker im Körper verarbeitet wird und was das in den Zellen macht. Es lohnt sich, mit solchen Prompts ein wenig zu experimentieren und Erfahrungen zu sammeln.

ChatGPT, Bing Chat, Bard und Co.

Es gibt verschiedene Chatbots, und die haben unterschiedliche Stärken und Schwächen. Kannst Du mal sagen, welche das sind?

ChatGPT ist besonders gut darin, Texte zu generieren.

Das können genauso gut Liebesbriefe sein, wie auch Gliederungen für Vorträge, Artikel oder Bücher. Das können andere Chatbots wie Bard oder Bing Chat nicht so gut. Sobald ich eher Antworten auf aktuelle Ereignisse haben möchte oder auch Quellangaben benötige, ist ChatGPT nicht mehr erste Wahl Dann derzeit eherPerplexity. Ist kostenlos im Web zu erreichen. Gemacht von Ex-Entwicklern von ChatGPT, die das System weiter entwickelt haben.

Richtig cool: Perplexity kennt auch aktuelle Ereignisse und listet Querverweise und Quellen fein säuberlich auf. Ideal, wenn man wissenschaftlich arbeitet. Wenn der Schwerpunkt bei aktuellen Ereignissen liegt, verwende ich Bing Chat oder Google Bard. Hier ist Google Bard besonders stark: Da es von Google kommt, kennt Bard die aktuelle Welt. Man kann sich in Fragen auf das Hier und Jetzt beziehen. Bard liefert gute Antworten und listet auch Quellen auf. Dafür kann Bard nicht so gut eigenständig Texte erstellen, eher Fragen beantworten.

Wenn der Chatbot sich irrt

Aber was mache ich, wenn ich feststelle, dass mir ChatGPT eine falsche Antwort liefert – oder wenn ich den Verdacht habe?

Du wirst staunen: Sag es dem Chatbot einfach. Sage einfach: „Das kann nicht stimmen“, oder noch konkreter: „Den Energieverbrauch, den Du da gerade ausgerechnet hast, der kann nicht stimmen“. Ich hatte solche Situationen schon. Dann sagt ChatGPT: „Stimmt, Du hast recht, verzeihe bitte den Fehler. Ich habe mich um eine Zehnerpotenz verrechnet.“ Und korrigiert die entsprechenden Passagen und gibt sie neu aus.

Besser, man überprüft aber auch diese Antwort nochmal, etwa durch eine Google-Suche, wenn es um Fakten geht. Denn: Bei einem „Das stimmt nicht“, wenn die

Antwort vorher korrekt war, gerät der Chatbot manchmal ins Straucheln, wird unsicher und gibt danach falsche Daten oder Antworten aus. Das alles zeigt: Chatbots wissen nicht alles und können auch falsch liegen. Das wollen die Entwickler aber unbedingt in den Griff bekommen und besser werden. Muß auch, damit wir uns auf die KI-Bots verlassen können.