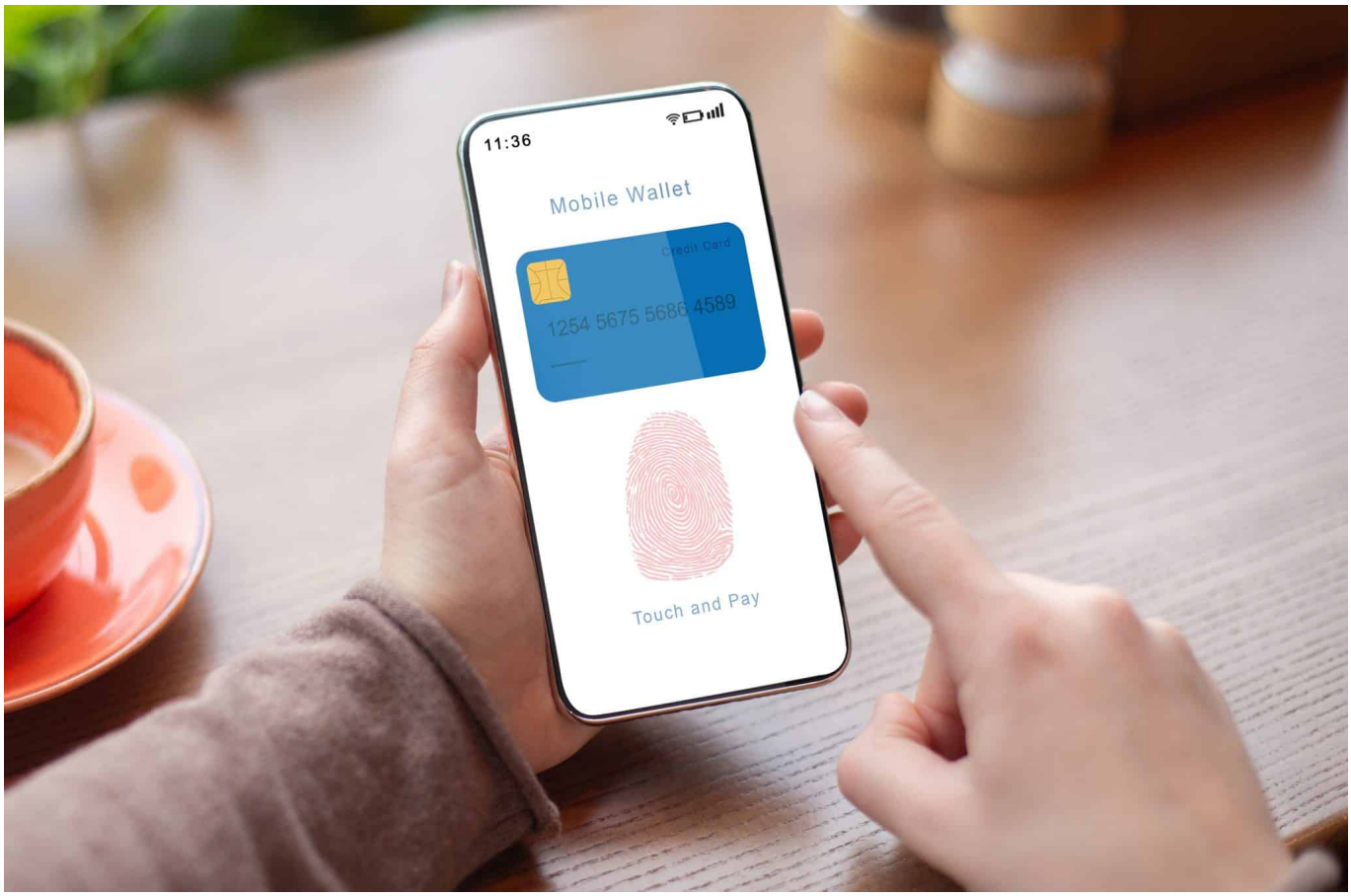
Schieb Report

Ausgabe 2023-22

Schieb Report

Ausgabe 2023-22

Attacke auf Fingerabdruck-Sensoren bei Android

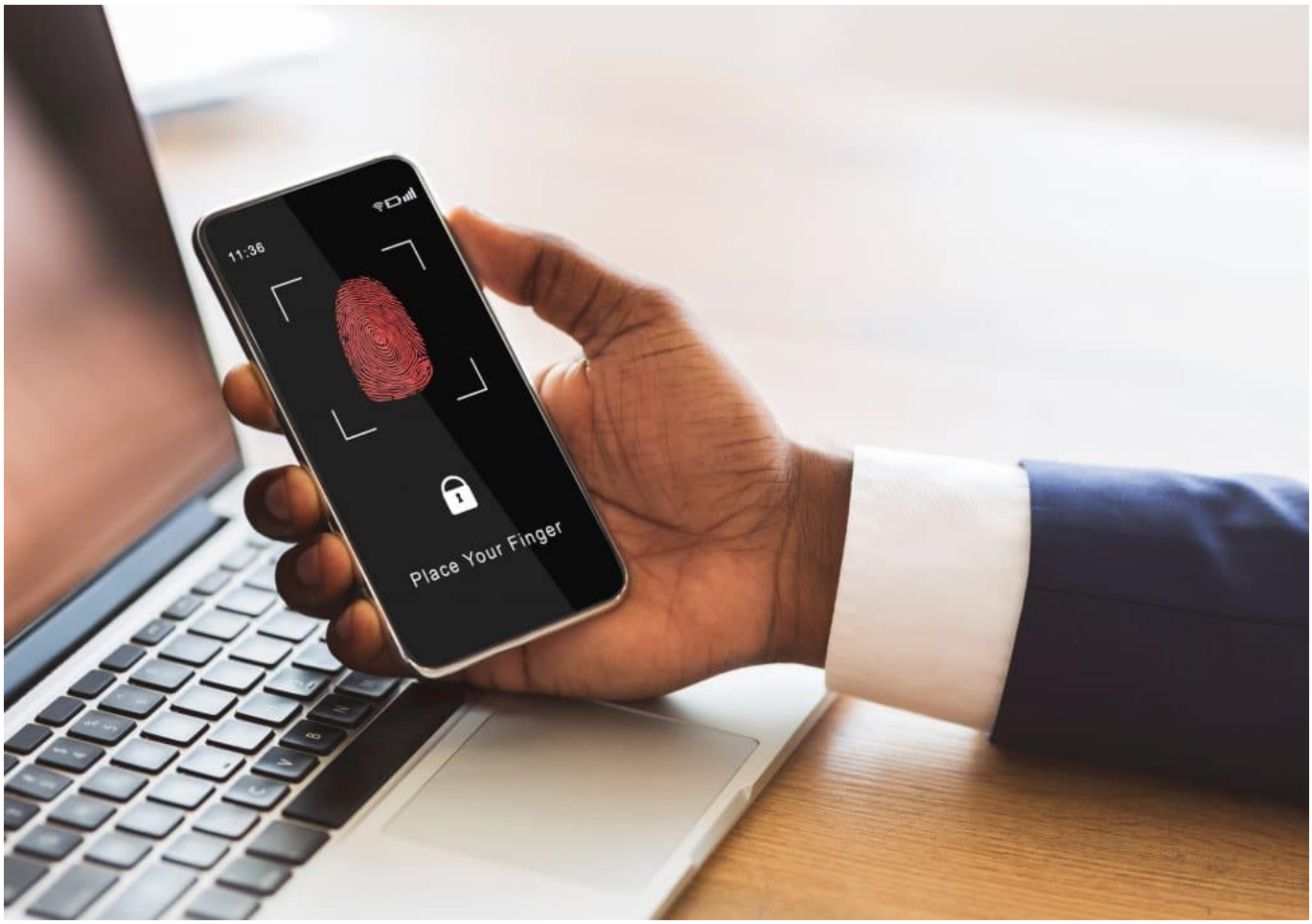


Ein Smartphone per Fingerabdruck abzusichern und dort anzumelden ist praktisch - und bislang auch vergleichsweise sicher. Doch jetzt gibt es eine "Bruteprint" genannte Methode, um sich Zugang zu verschaffen.

Stell dir vor, du hast dein Android-Smartphone mit einer sicheren Fingerabdrucksperre gesichert, doch plötzlich knacken Hacker innerhalb von Minuten deine Sicherheitsmaßnahme.

Klingt unglaublich, oder? Doch genau das haben Forscher der Universität Zhejiang in China geschafft und eine Methode namens **Bruteprint** entwickelt, um die Fingerabdrucksperre mit minimalen Mitteln und akzeptablem Zeitaufwand zu umgehen.

Wie machen sie das?



Per Fingerabdruck im Smartphone anmelden: Praktisch, aber nicht mehr sicher

Bruteprint: Einbruch per Fingerabdruck

Statt exakter Übereinstimmungen reicht eine Schwelle an Gemeinsamkeiten aus. Bruteprint nutzt eine Datenbank an Fingerabdrücken, um einen passenden Abdruck zu finden, der den gespeicherten Abdrücken ausreichend entspricht. Und woher kommen diese Datenbanken? Durch Leaks sind sie für Hacker verfügbar.

Aber bevor du jetzt in Panik gerätst, solltest du wissen, dass Bruteprint aus einem kleinen Board besteht, das mit einem STM32F412-Microcontroller und einer Fingerabdruckdatenbank ausgestattet ist. Das Board muss mit dem Smartphone verbunden werden, wofür es geöffnet werden muss. Das dürfte unbemerkte Attacken ausschließen.

Die Forscher testeten ihr Vorgehen mit zehn verschiedenen Smartphone-Modellen, darunter einem Galaxy S10+, einem Xiaomi Mi 11 Ultra, einem Oneplus 7 Pro und einem iPhone 7 und SE. Doch bei den iPhones funktioniert die Attacke

nicht, da die Fingerabdruckdaten verschlüsselt gespeichert werden.

Keine Panik!

Also, keine Panik! Aber sei wachsam und schütze deine Daten auf deinem Android-Smartphone so gut wie möglich. Wie sicher ist deine Sicherheitsmaßnahme? Bist du bereit für die Herausforderung?

Übrigens: Die Zeit, die jeweils für eine erfolgreiche Attacke nötig war, war sehr unterschiedlich, abhängig vom verwendeten Gerät. Der Zeitaufwand betrug zwischen rund 40 Minuten und 14 Stunden. Nicht “mal eben” gemacht; aber für den Fall, dass eine gezielte Attacke das Ziel ist, durchaus vertretbar. Der verhältnismäßig niedrige Kostenaufwand von 15 US-Dollar für die Elektronik ist sicher auch keine Hürde.

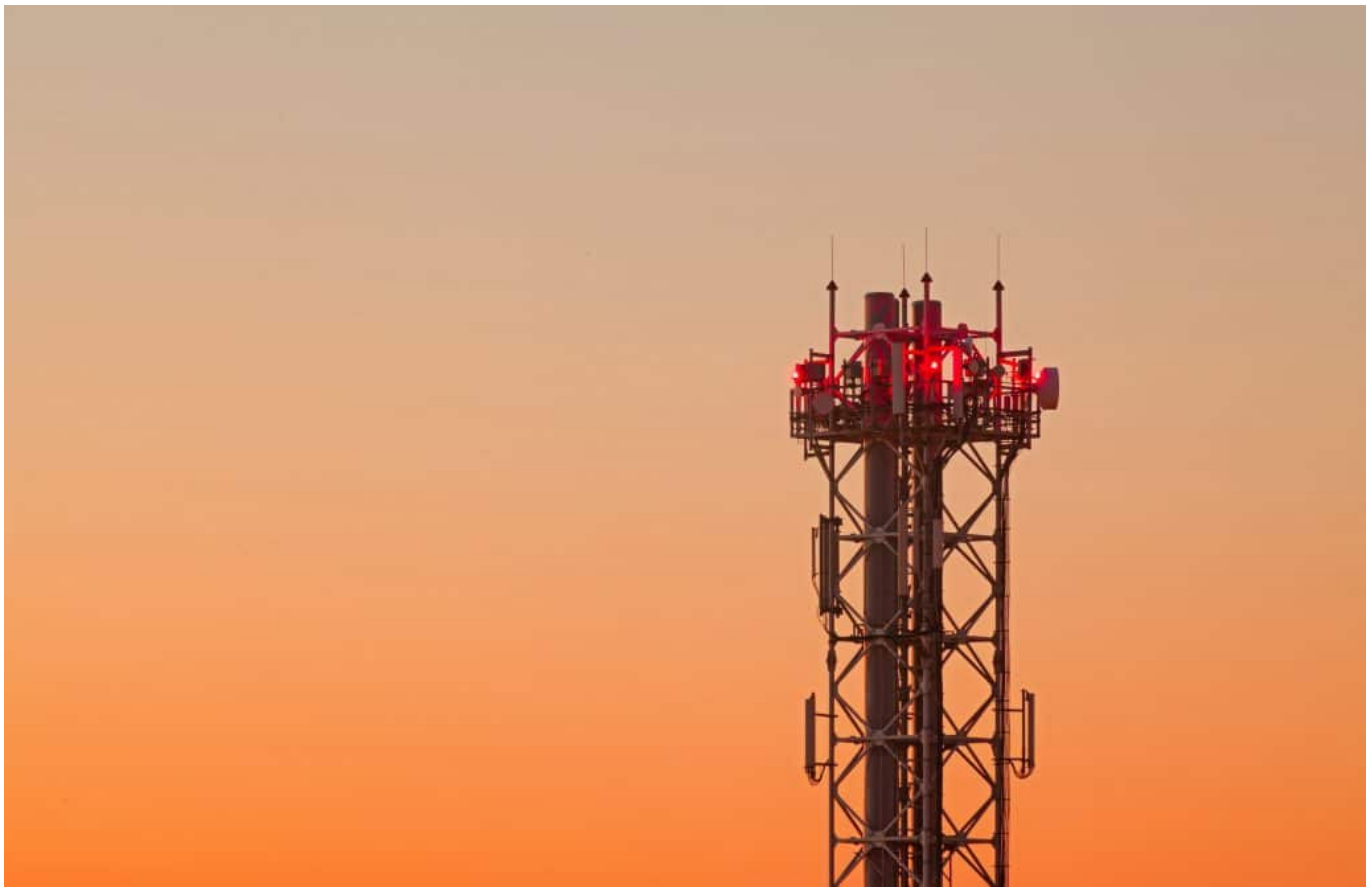
Stichwort: Netzabdeckung und Funklöcher

Wir sprechen im Zusammenhang mit Mobilfunk gerne von "Funklöchern" und "grauen Flecken". Aber was ist das eigentlich?

Funkloch, das – ein Ort oder Bereich, an dem es kaum, gar keinen oder nur sehr schlechten Empfang gibt. Und seien wir ehrlich: Solche Funklöcher kennen wir doch alle.

Funkloch: Wenn gar nichts geht

Ein Funkloch auf dem sogenannten platten Land oder auf dem Berg – da wundern sich die meisten nicht. Ärgerlich, aber keine Überraschung. Doch Funklöcher gibt es überall. Selbst dort, wo man sie nicht vermuten oder in einem führenden Industrieland erwarten dürfte. Im Bahnhof. Auf der Zugstrecke. Entlang der Autobahn. Aber auch im Büro, wenn man Pech hat.



Im schlechtesten Fall sind nur 90% der Fläche abgedeckt (O2)

Smartphone oder Mobilgerät bekommen keinen Kontakt zum Mobilfunknetz.

Dabei sehen die offiziellen Zahlen doch so gut aus. Nach Angaben der Bundesnetzagentur war der Funkstandard 4G Anfang des Jahres auf 97,9 Prozent der Fläche von NRW von mindestens einem Netzbetreiber zu empfangen. Das Problem ist: Kann ein Smartphone keinen Empfang zum eigenen Netzwerk herstellen, gibt es keinen Empfang. Ein grauer Fleck: Manche können mobil telefonieren, andere nicht. Abhängig vom Mobilfunknetzwerk.

Die Ironie: Ausländische Besucher können sich dank Roaming überall einbuchen. Einheimische können es nicht.

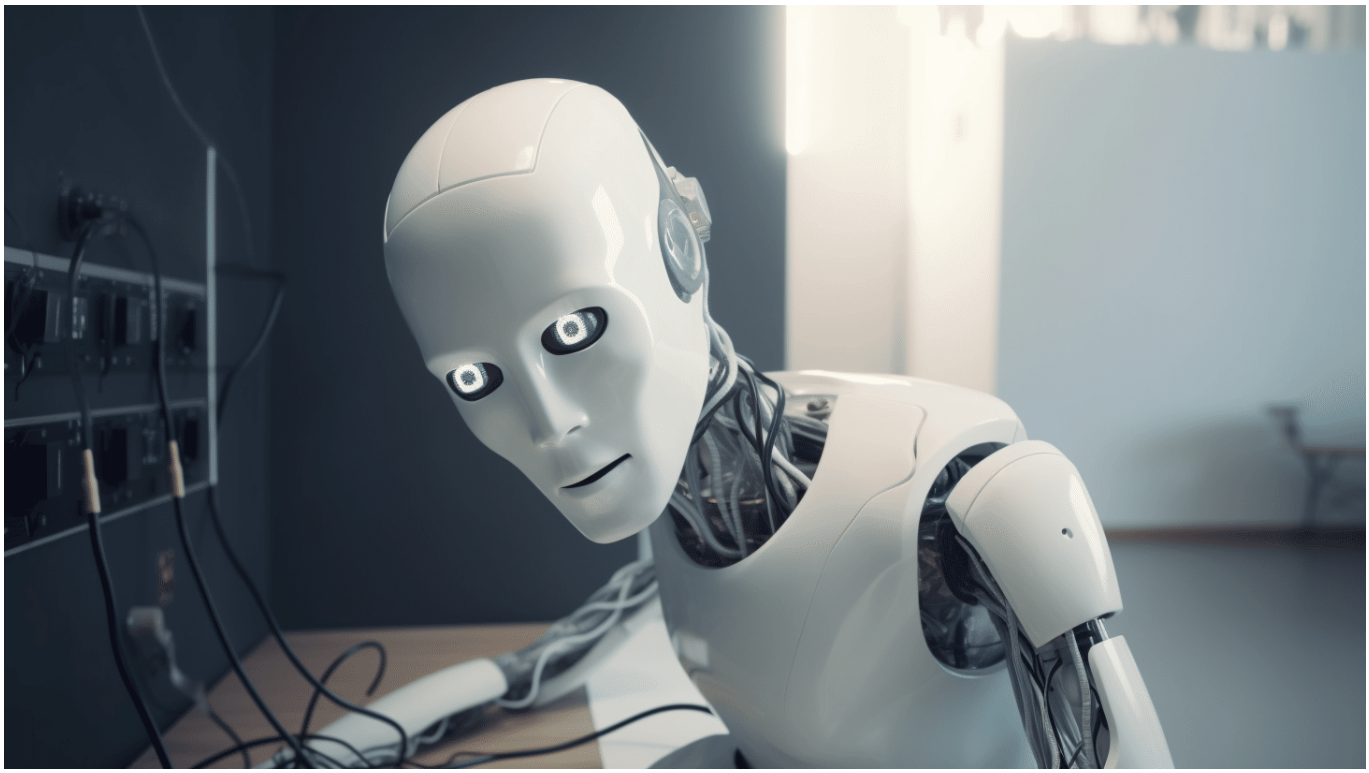
Roaming deckt alles ab

Schaut man auf die einzelnen Mobilfunkanbieter, sehen die Zahlen schon anders aus. Die Telekom bringt es auf 94,3% Netzabdeckung, Vodafone auf 90,2% und Telefonica auf 89,6%. Da sind also schon knapp 10% der gesamten Fläche ein Funkloch. Die Abdeckung mit dem modernen 5G ist noch deutlich niedriger.

Und selbst wenn man Empfang hat, muss das nicht bedeuten, dass Telefongespräche gut klingen – und die Daten rasant fließen. Das tun sie nur in der Werbung.

Auf knapp 2 Prozent der Fläche NRWs gibt es gar kein Netz, weder 4G, noch 5G.

Deepfakes: Wir können unseren Augen und Ohren nicht mehr trauen



KI-Systeme erstellen längst nicht mehr nur Texte und Bilder, sondern auch Audios und Videos. Und die sind von echten Aufnahmen kaum noch zu unterscheiden. Was solche KI-Systeme heute schon können – und worauf wir achten müssen, um nicht auf Deepfakes hereinzufallen.

Deepfakes bestimmen jetzt schon die Schlagzeiten: Zum Beispiel das Fake-Foto, das den in einer Luxus-Daunenjacke zeigt. Oder vor einigen Tagen die Fake-Aufnahmen einer angeblichen Explosion am Pentagon: Die Aufnahmen kursierten in Social Media und reichten schon, um zumindest kurzzeitig die Börsenkurse einbrechen zu lassen. Auch kursierte schon ein Fake-Video von Wolodymyr Selenskyj, der sein ukrainisches Militär zur Niederlegung der Waffen aufgefordert hat.

Es gibt immer mehr, technisch immer besser gemachte Fakes – erzeugt mit Hilfe von KI.

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

Deepfake - der Begriff

Ein **Deepfake** ist ein realistisch wirkender Medieninhalt, der mithilfe von künstlicher Intelligenz (KI) manipuliert, erzeugt oder verfälscht wurde. Es handelt sich um eine Form der Medienmanipulation, die auf maschinellem Lernen basiert, insbesondere auf künstlichen neuronalen Netzwerken. Deepfakes sind Videos, bei denen das Gesicht einer Person auf den Körper einer anderen Person gesetzt wurde, wobei diese Manipulation in der Regel so überzeugend ist, dass sie schwer von echten Inhalten zu unterscheiden sind.

Die Technologie hinter Deepfakes nutzt fortschrittliche Algorithmen, um Gesichter in Videos auszutauschen oder andere Veränderungen vorzunehmen. Dabei werden große Mengen an Trainingsdaten verwendet, um das neuronale Netzwerk zu trainieren, Gesichter zu erkennen und realistische Manipulationen vorzunehmen.

Die Manipulation von Videos und Bildern ist an sich nichts Neues, aber Deepfakes haben die Fähigkeit, diese Manipulationen weitgehend autonom durchzuführen und dabei äußerst überzeugende Ergebnisse zu erzielen. Insbesondere der

Tausch von Gesichtern, auch bekannt als "faceswap", ist eine gängige Form der Deepfake-Manipulation.

Es ist wichtig zu beachten, dass Deepfakes potenziell negative Auswirkungen haben können. Sie können dazu verwendet werden, Falschinformationen zu verbreiten, das Ansehen von Personen zu schädigen oder in betrügerischer Absicht eingesetzt werden. Daher besteht ein wachsendes Interesse daran, Technologien zur Erkennung von Deepfakes zu entwickeln und Maßnahmen zum Schutz vor ihrer missbräuchlichen Verwendung zu ergreifen.

Ein Papst in Luxusjacke: Ein Hingucker - aber DeepFake

KI auf dem Vormarsch

Künstliche Intelligenz (KI) ist auf dem Vormarsch: Chatbots wie ChatGPT von OpenAI oder Bard von Google erstellen auf Knopfdruck Texte zu jedem beliebigen Thema und in jeder gewünschten Länge und Ausführlichkeit. Meist in guter Qualität. KI-Systeme wie Midjourney oder Stable Diffusion hingegen erzeugen nach Eingabe entsprechender Kommandos innerhalb weniger Sekunden Fotos, Bilder, Cartoons oder Illustrationen – die mitunter aussehen, als hätten sie Menschen erdacht und gemacht.

Solche KI-Systeme sind allgemein verfügbar – teilweise sogar kostenlos, die besseren kosten einige EUR pro Monat. Mittlerweile gibt es eine regelrechte Flut von Apps, die Brücken zu solchen Inhalte generierenden KI-Systemen baut und sie für alle verfügbar macht, ohne jede Vorkenntnisse (allerdings zu teilweise gepfefferten Preise).

Olaf Scholz am Mikro: Kommt selten vor - deshalb hier ein Deepfake

Text to Speech: Wenn die KI mit synthetischer Stimme spricht

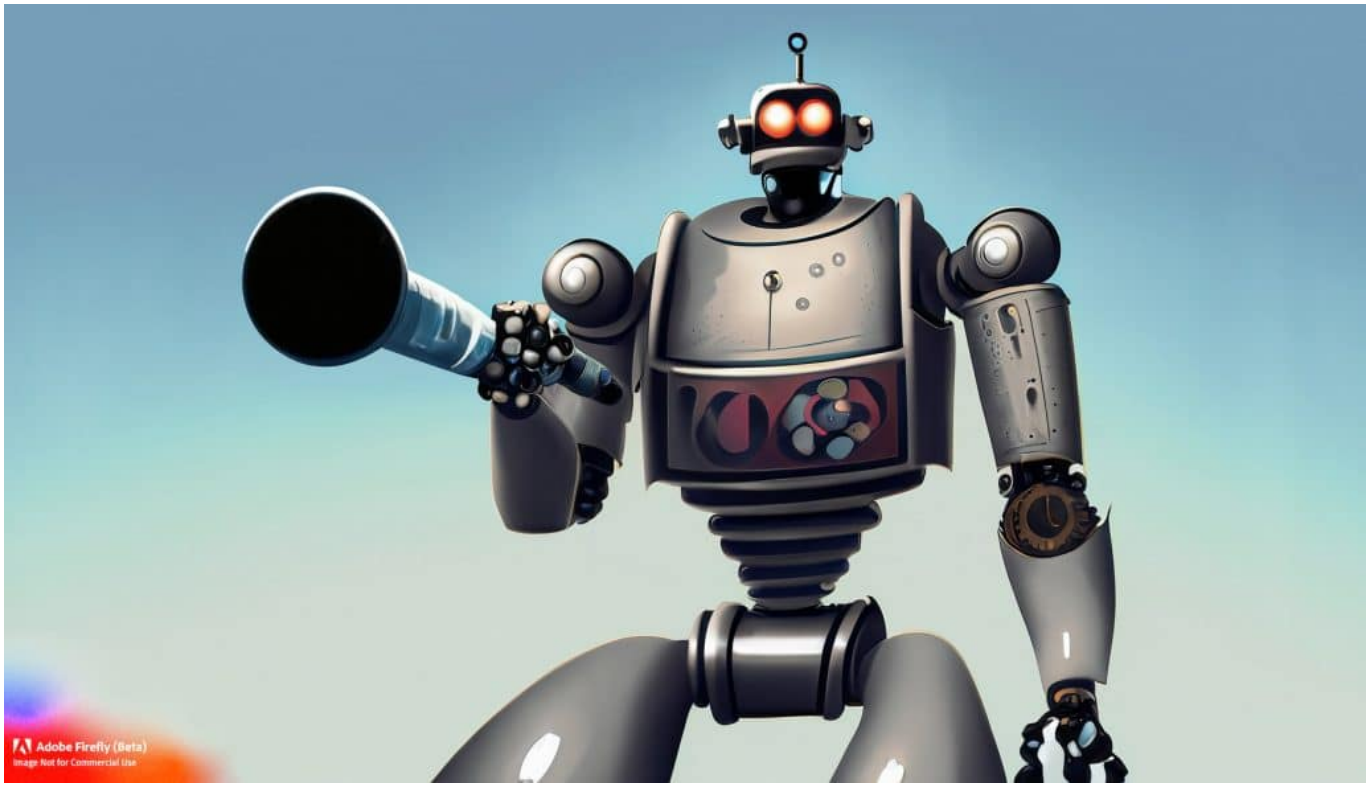
Die nächste Stufe sind Audios und Videos, die mit Hilfe von KI erzeugt werden – und ebenfalls mittlerweile ein bemerkenswertes technisches Niveau erreichen. Eine Unterscheidung zwischen echt und unecht, zwischen wahr und Fake ist für den Laien kaum noch möglich – und schon bald selbst für Experten nicht mehr. Bislang lassen sich durch den Einsatz forensischer Methoden Hinweise für die Erzeugung durch KI finden. Da die KI-Syste,e immer besser werden, ist das schon bald möglicherweise nicht mehr möglich.

So gibt es mittlerweile Dutzende KI-Systeme, die „Text to Speech“-Dienste anbieten: Wer mag, wählt eine Stimme aus, gibt einen Text ein – und die KI erzeugt ein wohlklingendes Audio. Benutzer haben die Auswahl aus Dutzenden

von Stimmen – und oft auch Sprechsituationen. Es macht einen Unterschied, ob man ein „Voice over“ – also einen Sprechtext – für ein Video benötigt, oder eine Stimme für einen Podcast erzeugen möchte.

Mit jeder Generation werden solche KI-Systeme, die Elevenlabs, Speechify oder Murf heißen, immer besser und leistungsfähiger. Die KI-Systeme machen vor allem in englischer Sprache riesige Fortschritte: Einen langen Text mit einer synthetischen Stimme sprechen zu lassen, etwa für einen Podcast, ist heute auf einem Niveau möglich, dass niemand auf die Idee käme, die Stimme wäre nicht echt.

Moderne KI-Systeme variieren das Sprechtempo, können auch Emotionen einbringen – sie erzeugen so verblüffend echt wirkende Audios. In der deutschen Sprache bewegen sich die Ergebnisse noch nicht auf diesem Niveau – aber das ist nur eine Frage der Zeit.



Achtung, App hört mit

Fake: KI kann die Stimme eines jeden anderen nachbilden

Doch jetzt wird es problematisch: Immer mehr KI-Systeme bieten die Möglichkeit an, völlig frei eine eigene synthetische Stimmen zu trainieren. Wer nun eigene

Sprachproben einspielt, kann zum Beispiel seine eigene Stimme trainieren – oder die jeder anderen Person. Es braucht nur wenige Minuten Sprachtext – möglichst ohne Nebengeräusche –, und schon kann ein System wie Elevenlabs mit der Stimme der Person sprechen.

Bundeskanzler Olaf Scholz aus dem „Kleinen Prinzen“ vorlesen oder die Stauschau vortragen lassen? Gar kein Problem... (siehe Video). Wer nicht genau hinhört, bemerkt den Unterschied kaum oder gar nicht.

Deepfakes: Audios lassen sich leicht fälschen

Komplett monoton klingende KI-Stimmen gehören längst der Vergangenheit an. Heute muss man auf „Natürlichkeit“ achten: Klingen die Stimmen variantenreich und natürlich? Noch kriegen das KI-Systeme mit deutscher Sprache nicht perfekt hin. Aber schon bald wird auch hier kein Unterschied mehr zu hören sein.

Das Risiko liegt auf der Hand: Entsprechend trainiert, lässt sich mit modernen KI-Systemen mit den Stimmen von Prominenten oder Politikern so ziemlich alles sagen. Dem Einsatz manipulativer Deepfakes sind Tür und Tor geöffnet. Durch die weite Verbreitung solcher Systeme und den niederschwelligen Einsatz erhöht sich das Risiko, das Nachrichten mit Deepfakes verbreitet werden. Etwa, indem behauptet wird, ein Politiker hätte etwas gesagt – und als Beleg wird ein Audio verteilt.

KI-Systeme erzeugen Videos – oder tauschen Gesichter aus

Ganz ähnlich verhält es sich mit Videos. Bis vor einigen Monaten waren überzeugende Deepfake-Videos nur im Labor zu erzeugen. Doch die Fortschritte der KI-Systeme sind rasant: Es ist mittlerweile möglich, künstliche Avatare sprechen zu lassen. Oder eigene Avatare zu erzeugen, einer echten Person nachgeahmt, die ebenfalls alles tun und sagen können.

Last not least gibt es bereits KI-Systeme wie „Deepfakesweb.com“, die einen „Face Swap“ anbieten: Das Gesicht in einem A-Video wird durch ein anderes Gesicht aus einem B-Video ausgetauscht. Auf Wunsch kann dieses dann reinmontierte Gesicht alles sagen, was es soll – lippensynchron. Das erfordert einiges an Rechenaufwand, Zeit und Kosten – ist aber eben mittlerweile möglich.

Dabei kommen Videos in technisch guter Qualität heraus. Auch mit solchen Systemen lassen sich mühelos Deepfakes erzeugen, die Menschen in kompromittierenden Situationen zeigen – oder die Dinge sagen (mit synthetischer Stimme kombiniert), die sie nie gesagt haben.

Doch durch KI erzeugte Audios und Videos kommen auch im kriminellen Umfeld

zum Einsatz – schon jetzt. So wird der bekannte „Enkeltrick“ erweitert: Potenzielle Opfer bekommen nicht nur einen angeblichen Hilferuf als Textnachricht per Whatsapp zugeschickt, sondern auch schon durch KI erzeugte Hilfeaufrufe in gesprochener Form. Der Aufwand ist zwar etwas höher, der Effekt aber durchschlagend – denn wer misstraut einer Stimme, die er kennt? In den USA haben Kriminelle diese Methode bereits erfolgreich angewandt.

Ein Problem, denn die Polizei ist auf solche kriminelle Methoden noch nicht vorbereitet. Gerhard Schabhüser von „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) sagt:

> „Eine technische Unterstützung auf großem Qualitätsniveau gibt es leider noch nicht. Aber ich bin mir sicher, dass wir an dieser Stelle Forschung und Entwicklung vorantreiben müssen, um künftig unseren Bürgerinnen und Bürgern Detektions-Tools von Deepfakes an die Hand zu geben, damit sie das besser bewerten können.“

Bedeutet: Der Experte wünscht sich, dass Bürger selbst mit geeigneten Werkzeugen überprüfen können, ob ein Audio oder Video mit KI erzeugt wurde.

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

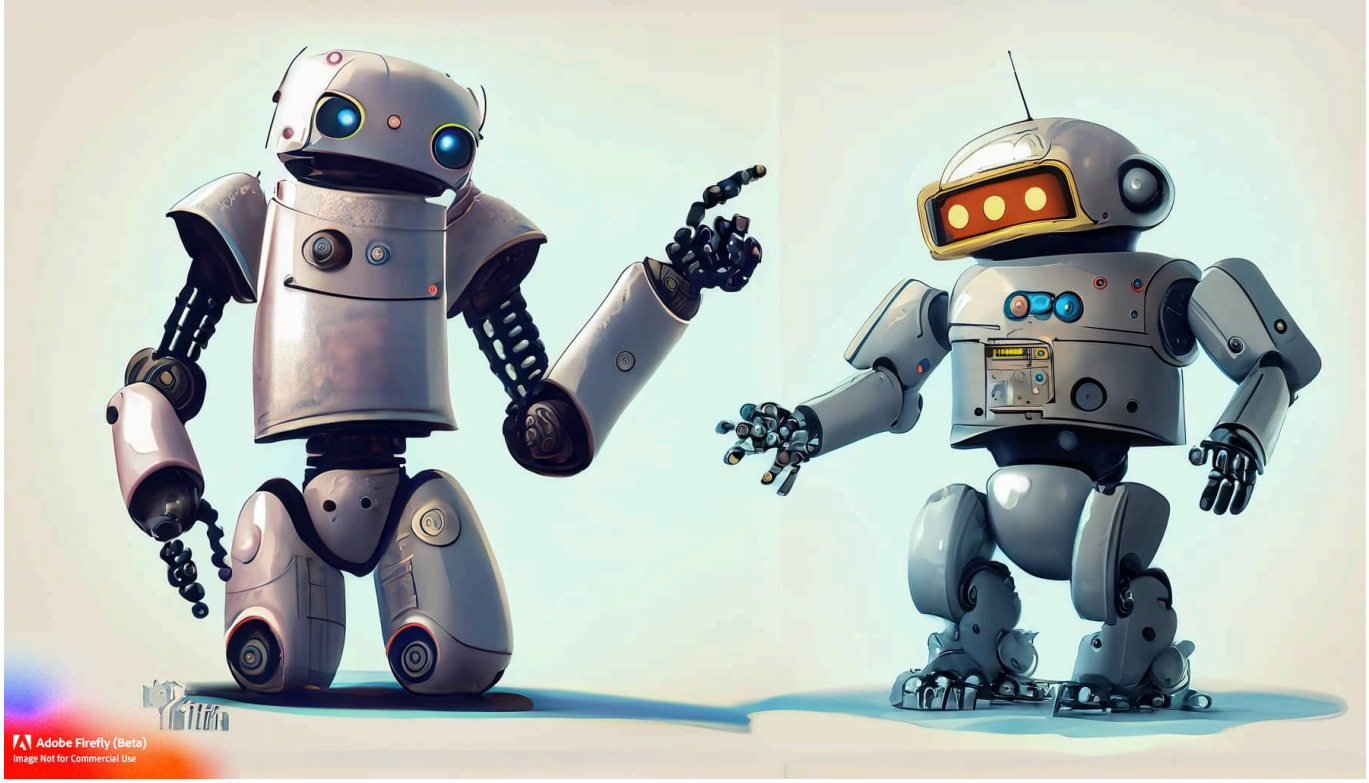
Mehr gesundes Misstrauen nötig

Noch gibt es solche Werkzeuge nicht. Bei Audios deshalb auf Sprechtempo und Sprachrhythmus achten: Noch verraten sich manche KI-Systeme durch eine gewisse Monotonie. Bei Videos empfiehlt es sich, ganz genau darauf zu achten, ob lippensynchron gesprochen wird. Auch sind KI-Videos häufig (nicht immer!) etwas „matschig“: Das erfordert weniger Rechenzeit und könnte ein Hinweis auf ein Deepfake sein.

Wir Menschen neigen dazu, unseren Sinnen zu vertrauen. Doch wir leben in einer Zeit, in der nicht nur Fotos, sondern eben auch Audios und Videos leicht zu manipulieren sind – oder sogar komplette Deepfakes erzeugt werden können. Wir sind daher gut beraten, unseren Augen und Ohren nicht einfach mehr so zu trauen. Ein Quellen-Check wird immer wichtiger.

https://www.youtube.com/watch?v=56kbryM17TQ

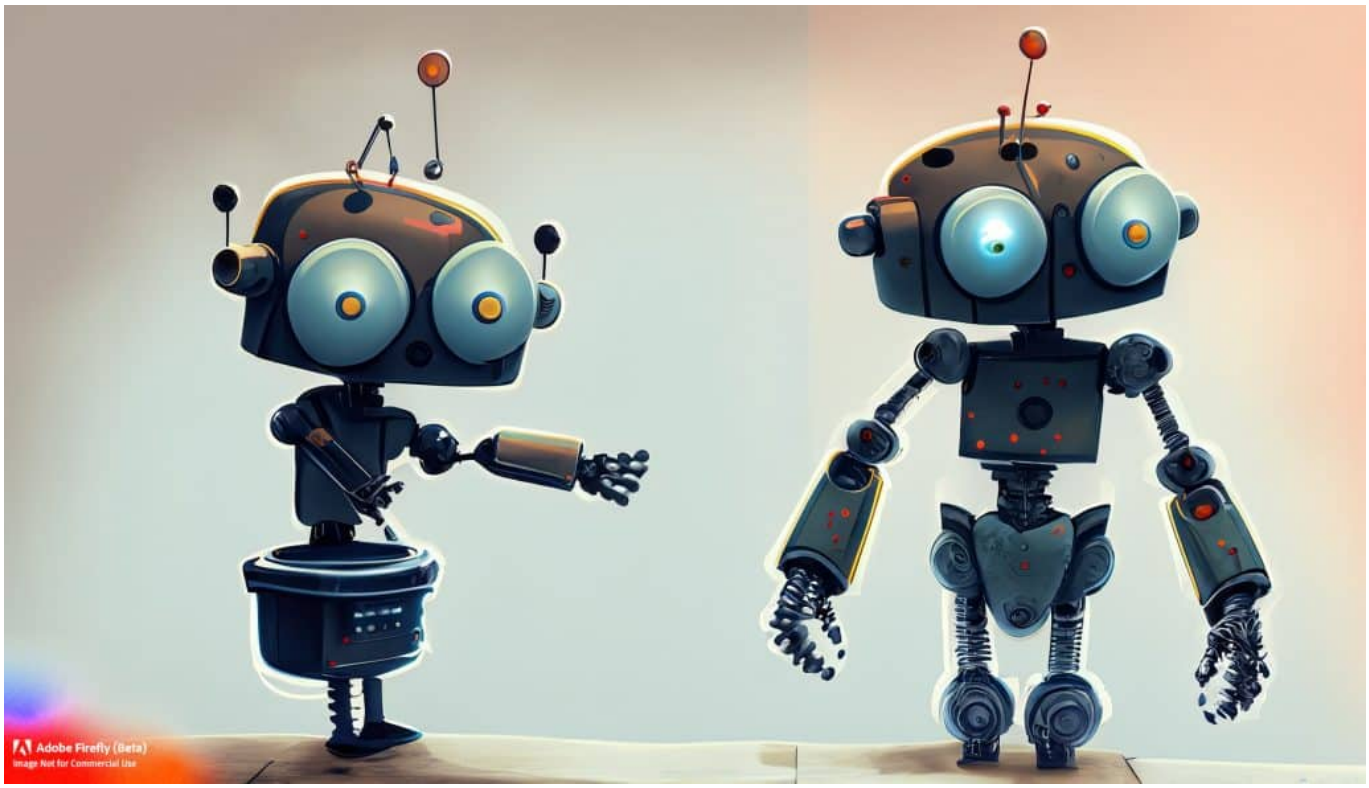
Das Geniale am GAN: Wenn Künstliche Intelligenz zu Kunst wird!



"Generative Adverarial Network": So werden KI-Systeme genannt, die eigenständig trainieren und so immer besser werden. Dabei kommen KI-Systeme wie ChatGPT, Midjourney und andere heraus, die Inhalte generieren können.

Künstliche Intelligenz (KI) hat die Welt im Sturm erobert und bringt ständig neue aufregende Technologien hervor. Eine dieser Technologien, die mit ihrem kreativen Potenzial beeindruckt, ist das **GAN** (Generative Adversarial Network).

Doch was genau ist ein GAN? Lass mich das in einfacher Sprache und mit einem Augenzwinkern erklären.



GAN: KI-Systeme trainieren sich gegenseitig

So funktioniert ein GAN

Stell dir vor, du hast zwei Kontrahenten: den Generator und den Diskriminator. Sie sind wie Rivalen in einem Kunstwettbewerb. Der Generator ist ein angehender Künstler, der neue Bilder malen möchte, und der Diskriminator ist der strenge Kunstkritiker, der entscheidet, ob das Gemälde echt oder gefälscht ist. Das Ganze spielt sich in einem spannenden Hin und Her ab.

Der Generator fängt an und malt sein erstes Bild. Aber hey, es sieht noch ziemlich schlecht aus - eher wie ein Kunstkurs für Anfänger. Der Diskriminator erkennt sofort, dass es sich um ein künstliches Bild handelt und gibt dem Generator sein Feedback.

Jetzt kommt der Trick: Der Generator lernt aus diesem Feedback und versucht, sein nächstes Bild besser zu machen. Er verfeinert seine Pinselstriche und fügt mehr Details hinzu. Der Diskriminator ist beeindruckt und muss zugeben, dass es schon viel realistischer aussieht. Das geht so weiter, immer hin und her, bis der Generator schließlich Bilder erzeugt, die so überzeugend sind, dass selbst der Diskriminator nicht mehr zwischen echten und künstlichen Bildern unterscheiden kann.

GAN erzeugen selbständig Inhalte

Das GAN ist wie ein Tanz zwischen Generator und Diskriminator, bei dem sie sich ständig verbessern und herausfordern. Der Generator versucht, den Diskriminator zu täuschen, während der Diskriminator versucht, die Fälschungen zu entlarven. Dieses Katz-und-Maus-Spiel führt zu immer realistischeren und ansprechenderen Ergebnissen.

Das Geniale an GANs ist ihre Vielseitigkeit. Sie können nicht nur Bilder generieren, sondern auch Videos, Musik oder sogar Texte. Sie sind echte Kreativitätsmaschinen! Obwohl sie im Bereich der Kunst oft eingesetzt werden, haben sie auch Anwendungen in anderen Bereichen wie der medizinischen Bildgebung, der Datensynthese und der Sprachverarbeitung.

Ein Papst in Luxusjacke: Ein Hingucker - aber DeepFake

Deepfakes: Fälschungen drohen

Natürlich gibt es auch Risiken. Denn wenn GANs so gut darin sind, Fälschungen zu erzeugen, könnten sie auch für betrügerische Zwecke missbraucht werden. Man denke nur an gefälschte Nachrichten oder manipulierte Beweismittel. Es ist also wichtig, dass wir uns bewusst sind, wie mächtig diese Technologie ist, und

entsprechende Schutzmechanismen entwickeln, um den Missbrauch zu verhindern.

Insgesamt ist das GAN eine faszinierende Technologie, die uns zeigt, wie Künstliche Intelligenz zu echter Kunst werden kann. Es ist wie ein magisches Duo, das unsere Vorstellungskraft beflügelt und uns in eine Welt voller kreativer Möglichkeiten entführt. Also halte Ausschau nach den Werken von GANs - wer weiß, vielleicht hast du schon einmal ein von ihnen generiertes Bild bewundert, ohne es zu wissen!

Star Wars als ASCII-Film

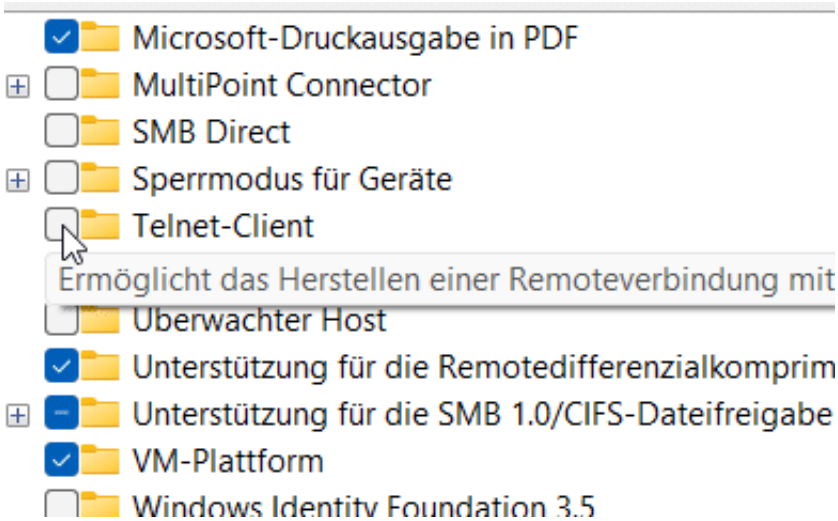
Star Wars ist überall: Filme, Computerspiele, Merchandise, an manchen Tagen - wie dem 4. Mai, dem (in)offiziellen Star Wars-Tag - könnt Ihr das Thema kaum vermeiden. Wusstet Ihr, dass Ihr mit ein wenig Unterstützung von Windows einen Star Wars-Film im ASCII-Format ansehen könnt?

Windows Features aktualisieren

Dieser kleine Trick benötigt vor allem die Telnet-Funktionalität von Windows, mit der Ihr die Verbindung zu anderen Rechnern auf sehr rudimentärer Basis aufbauen könnt. Die ist in den Standard-Windows-Installationen nicht automatisch vorhanden. Dafür gibt es in Windows eine sehr hilfreiche Funktion, mit der Ihr Windows-Funktionen schnell hinzufügen könnt.

Die sogenannten Windows-Features sind Funktionen, die zu Windows gehören, aber nur in bestimmten Fällen gebraucht werden. Daher sind einige davon aktiviert, andere deaktiviert. Ihr könnt sie aber ohne komplizierte Windows-Neuinstallation direkt im laufenden Betrieb anpassen:

- Gebt im Suchfeld **Windows Features** ein und klickt dann auf **Windows-Features aktivieren oder deaktivieren**.
- Ihr bekommt eine Liste der Windows-Features angezeigt. Die, die einen Haken neben dem Eintrag haben, sind bereits aktiviert (und können durch Entfernen des Hakens deaktiviert werden), die ohne Haken sind nicht aktiviert.
- Rollt nach unten bis zum Eintrag **Telnet-Client** und aktiviert diesen.
- Windows lädt nun gegebenenfalls fehlende Komponenten nach und installiert/aktiviert den TelNet-Client.

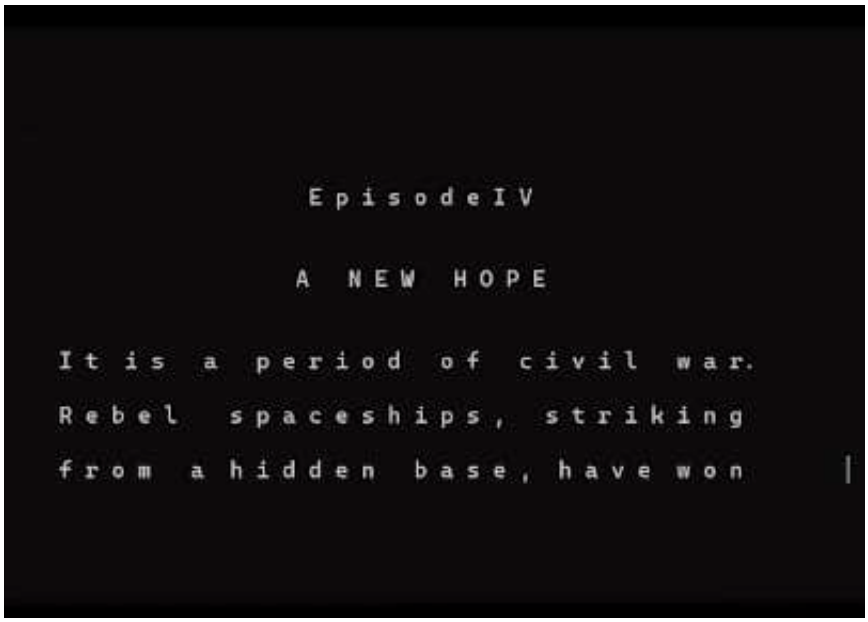


Auf diesem Weg könnt Ihr alle Windows-Features verwalten. Ihr wolltet allerdings nur Features deaktivieren, von denen Ihr sicher seid, dass diese nicht benötigt werden!

Star Wars als ASCII-Film

Nachdem Ihr den Telnet-Client auf Eurem Rechner aktiviert habt, könnt Ihr nun zum lustigen Teil kommen: Ruft den Star Wars-Film im ASCII-Format auf. Um Eure Erwartungshaltung anzupassen: ASCII-Film heißt, dass Ihr keine echten, hochauflösenden Bilder sehen werdet, sondern der ganze Film aus Textzeichen zusammengesetzt ist. Was auf den ersten Blick langweilig klingt, hat tatsächlich seinen ganz eigenen Reiz!

- Gebt im Suchfeld **Eingabe** ein und klickt dann auf **Eingabeaufforderung**.
- An der nun erscheinenden Eingabeaufforderung tippt als Befehl **telnet towel.blinkenlights.nl** ein und drückt die Eingabetaste.
- Nach einem Moment erscheint der bekannte Anfang von Star Wars: Episode IV auf Eurem Bildschirm und danach die Filmsequenzen. Viel Spaß!

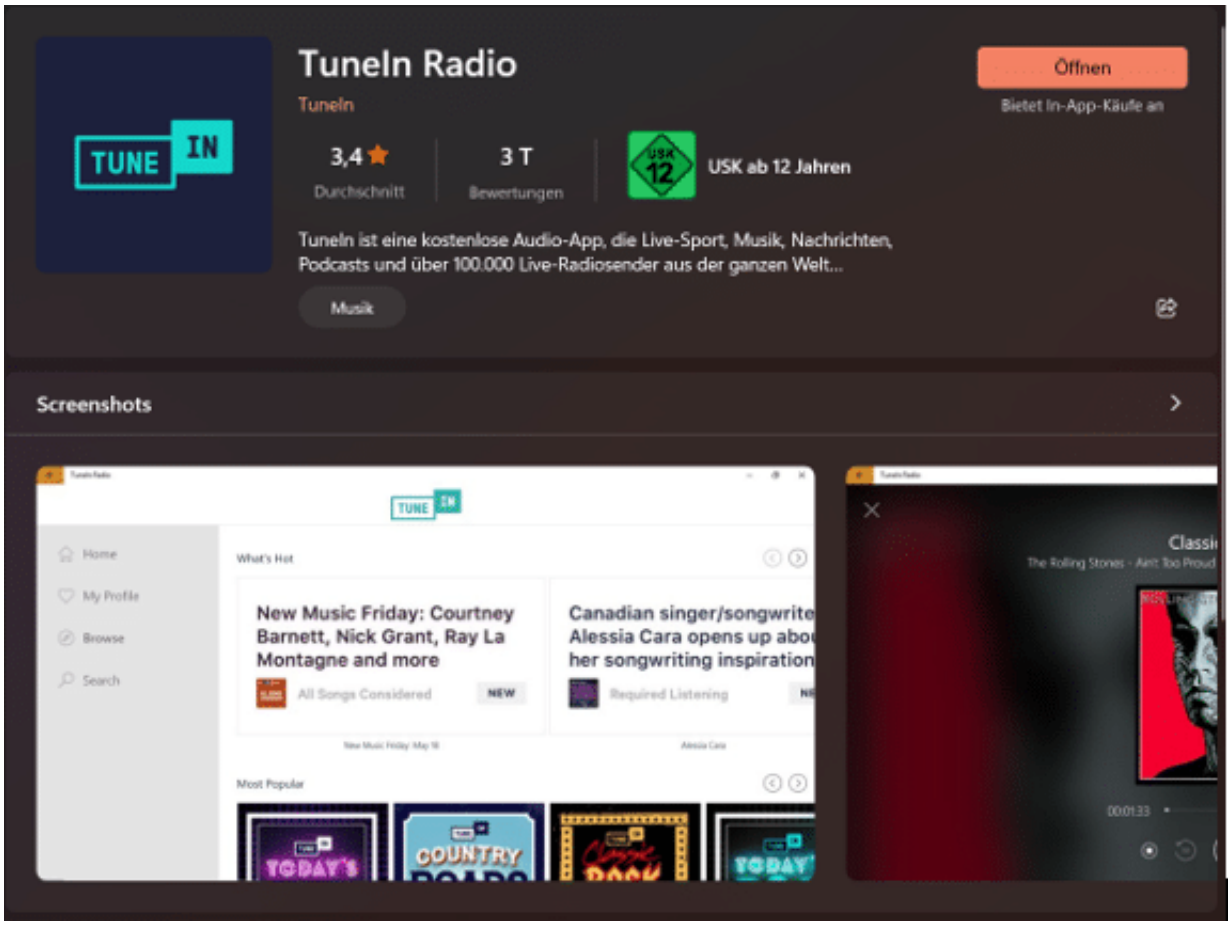

EpisodeIV
A NEW HOPE
It is a period of civil war.
Rebel spaceships, striking
from a hidden base, have won

Radio- und Video-Mediatheken nutzen unterwegs

Habt Ihr immer noch nicht genug Unterhaltung auf Eurem PC? Dem können wir abhelfen: Lust auf Radio? Kein Problem! Und habt Ihr eine Fernsehsendung verpasst? Dann schaut sie einfach nachträglich!

Radio hören auf dem PC

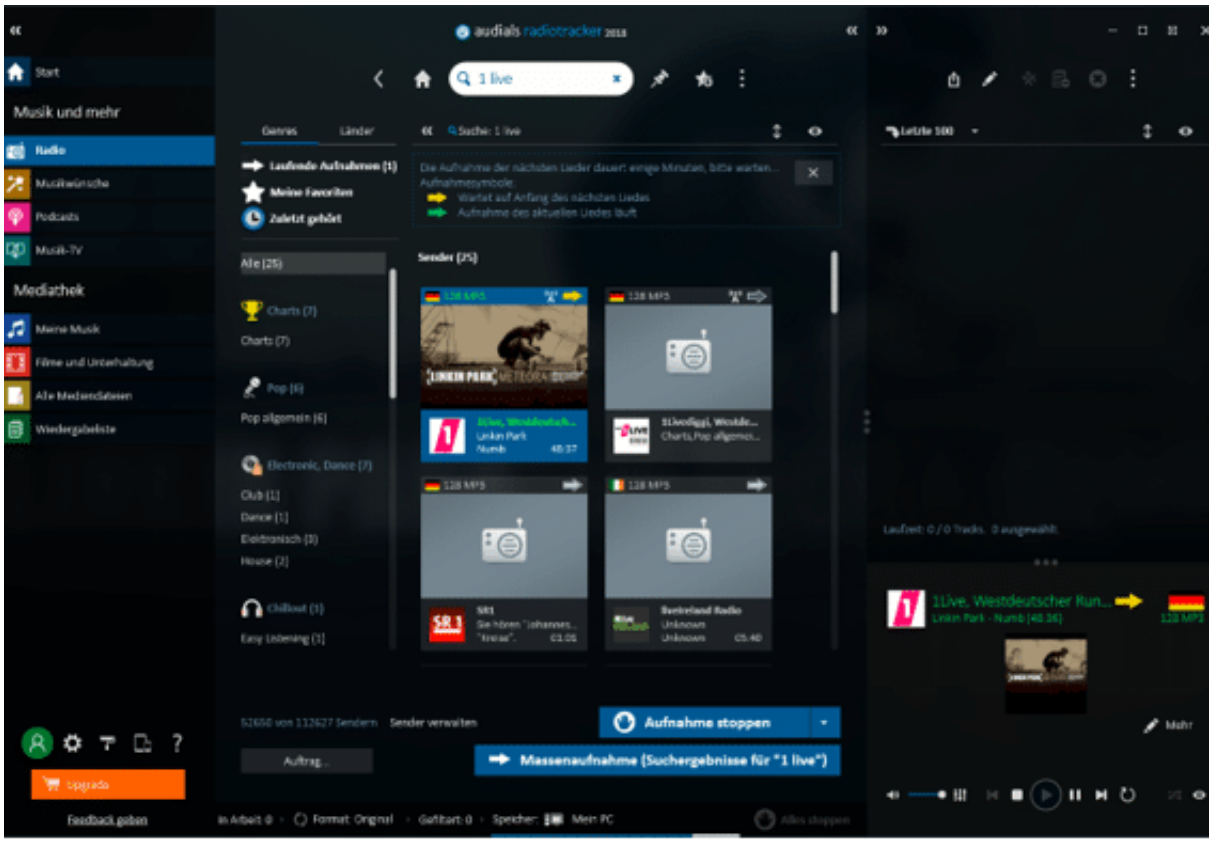
Die einfachste Möglichkeit, auf Eurem PC Radio zu hören, ist die kostenlose Tune-In-App. Die könnt Ihr direkt im Windows Store herunterladen.



Gebt unter **Suche** einen Sendernamen ein, klickt den Sender an und danach das Wiedergabesymbol, und schon hört Ihr das Live-Programm.

Radiosendungen aufnehmen

Erinnert Ihr Euch noch an die gute, alte Zeit, in der Ihr mit dem Kassettenrekorder vor dem Radio gehockt habt, um Eurer Lieblingslied aus dem Radio aufzunehmen? Selbst so etwas gibt es für Windows 11!



- Der Audials Radiotracker kennt über 100.000 Sender, die Ihr Euch live anhören können.
- Habt Ihr einen Sender ausgewählt, dann könnt Ihr mit der rechten Maustaste hineinklicken und dann Aufnehmen und Songs schneiden auswählen.
- Das Programm versucht dann, aus dem laufenden Programm die Musikstücke zu erkennen und als einzelne Dateien abzuspeichern.
- Wenn Ihr dem Automatismus nicht vertraut, dann könnt Ihr stattdessen eine Durchgehende Aufnahme starten und dann beispielsweise mit dem schon beschriebenen Programm Audacity das hinausschneiden, was Euch wirklich interessiert.
- Die kostenlose Testversion erlaubt die Aufnahme von 25 Musikstücken und das freie Radiohören. Wenn Sie mehr Aufnahmen machen wollen, fallen EUR 50,- als Einmalgebühr an. Alternativ könnt Ihr auch eine monatliche Gebühr entrichten.

Herunterladen von Sendungen aus Mediatheken

Habt Ihr noch einen Videorecorder? Und ärgert Euch darüber, dass Ihr nur zu Hause schauen könnt? Dann solltet Ihr dringend einmal die Mediatheken

anschauen.

- Die meisten Sender bieten Euch die Sendungen nach Ausstrahlung für eine gewisse Zeit als gespeicherte Version an, die Sie im Browser ansehen können.
- Sucht einfach mit Eurer bevorzugten Suchmaschine nach „ Mediathek“ (und ersetzt durch den Sender, den Ihr im Sinn habt).
- Um noch komfortabler auch unterwegs eine verpasste Sendung anschauen zu können, nutzt doch die Webseite https://mediathekviewweb.de/.
- Hier findet Ihr die Sendungen der Mediatheken der öffentlich-rechtlichen Sender aufgeführt.
- Sucht nach der Euch interessierenden Sendung. Rechts neben dem Video könnt Ihre dann auf das kleine Filmsymbol rechts neben dem Eintrag klicken und die Videogröße (und damit -Qualität) der herunterzuladenden Datei festlegen.
- Sobald diese auf Eurer Festplatte angekommen ist, könnt Ihr sie auf ein beliebiges Gerät übertragen und dort ansehen.

Windows: Das Touchpad beherrschen

Nicht nur am Notebook ist das Touchpad eine echte Alternative zur Maus. Es benötigt weniger Platz und ist für viele Anwender präziser in der Bedienung. Allerdings hat es auch seine Tücken. Wir zeigen Euch, wie Ihr es optimal nutzt.

Touchpad einschalten und konfigurieren

Für das Touchpad gibt es zwei Varianten unter Windows:

- Die Hardware-Version, die integriert (in einem Notebook) oder extern (per USB oder Bluetooth angeschlossen) sein kann.
- Das virtuelle Touchpad, das Windows für Touchscreens anbietet.

Die Einstellungen für das Touchpad findet Ihr, wenn Ihr nach Touchpad" sucht

und auf die **Touchpad-Eigenschaften** klickt.

- Schaltet das Touchpad ein, um es nutzen zu können.
- Es kann Sinn machen, das Touchpad auszuschalten, wenn Ihr eine Maus angeschlossen habt. Beispielsweise, weil Euch das Touchpad stört, wenn Ihr tippt. Das könnt Ihr ein den Einstellungen aktivieren oder deaktivieren.
- Darunter findet Ihr eine Vielzahl von Einstellungen, die das Verhalten des Touchpads beeinflussen. Die können Euch bei falscher Einstellung ärgern:

Fehler beim Touchpad identifizieren und lösen

Eigentlich sollte ein Touchpad intuitiv funktionieren. Das ist in den meisten Fällen auch so, allerdings gibt es einige Fehler, die immer wieder vorkommen:

Wenn das TouchPad nicht funktioniert, dann prüft folgendes:

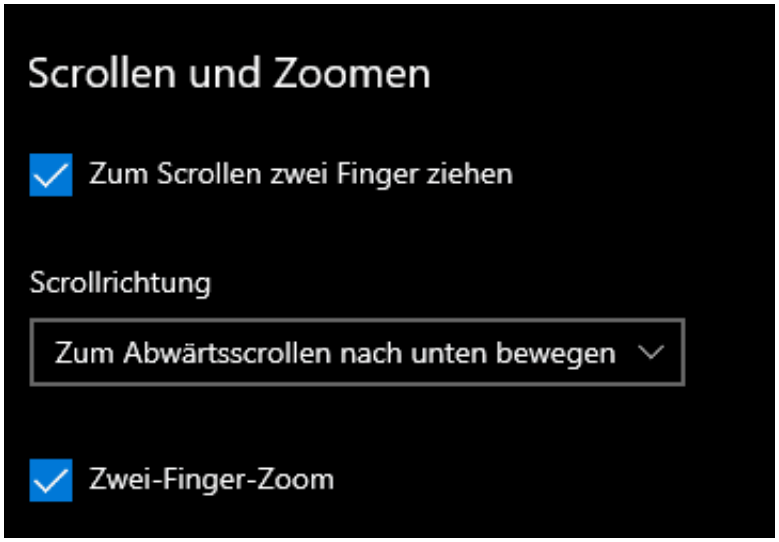
- Ist es eingeschaltet? Akku-betriebene TouchPads haben einen Ein-/Ausschalter.
- Ist die Kabelverbindung richtig hergestellt?
- Ist das Touchpad in den Einstellungen von Windows (siehe oben) aktiviert?

Wenn der Mauszeiger bei Nutzung des Touchpads hakelt, dann prüft folgendes:

- Sind die Oberfläche des Touchpads oder Eure Finger verschmiert? Das

beeinträchtigt die Leitfähigkeit, säubert die Oberflächen.

- Ist bei einem Bluetooth-TouchPad der Abstand zwischen dem Gerät und dem Touchpad zu groß oder sind störende Geräte mit Funksendern in der Nähe, die die Qualität beeinflussen? Ändert, wenn möglich, die Positionierung des Touchpads.



Wenn die Scrollrichtung des Touchpads nicht stimmt, dann könnt Ihr folgendes tun:

- Rollt in den Einstellungen des TouchPads nach unten bis zum Bereich **Scrollen und Zoomen**.
- Unter Scrollrichtung könnt Ihr einstellen, ob die Bewegung der Finger nach unten den Bildschirminhalt nach oben oder unten bewegt.