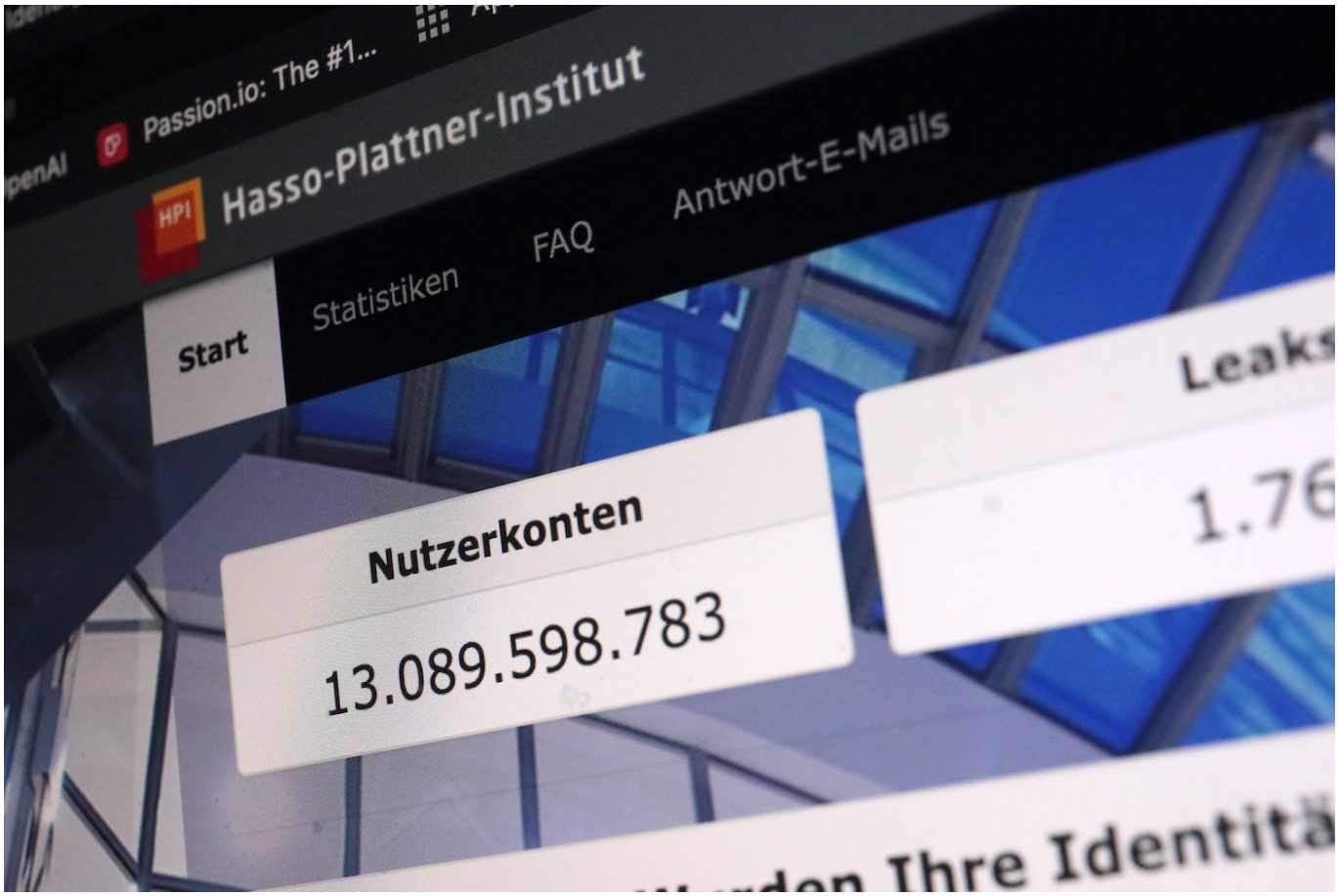
Schieb Report

Ausgabe 2023.08

Identity Leak Checker ermöglicht Abgleich mit 13 Milliarden gestohlenen Identitätsdaten im Internet



Hacker hacken sich nur vergleichsweise selten in das Smartphone von Privatleuten. Viel häufiger aber werden Zugangsdaten oder persönliche Daten "geklaut" - auf Servern von Unternehmen. Ob man selbst davon betroffen ist, verrät der HPI Identity Leak Cheker.

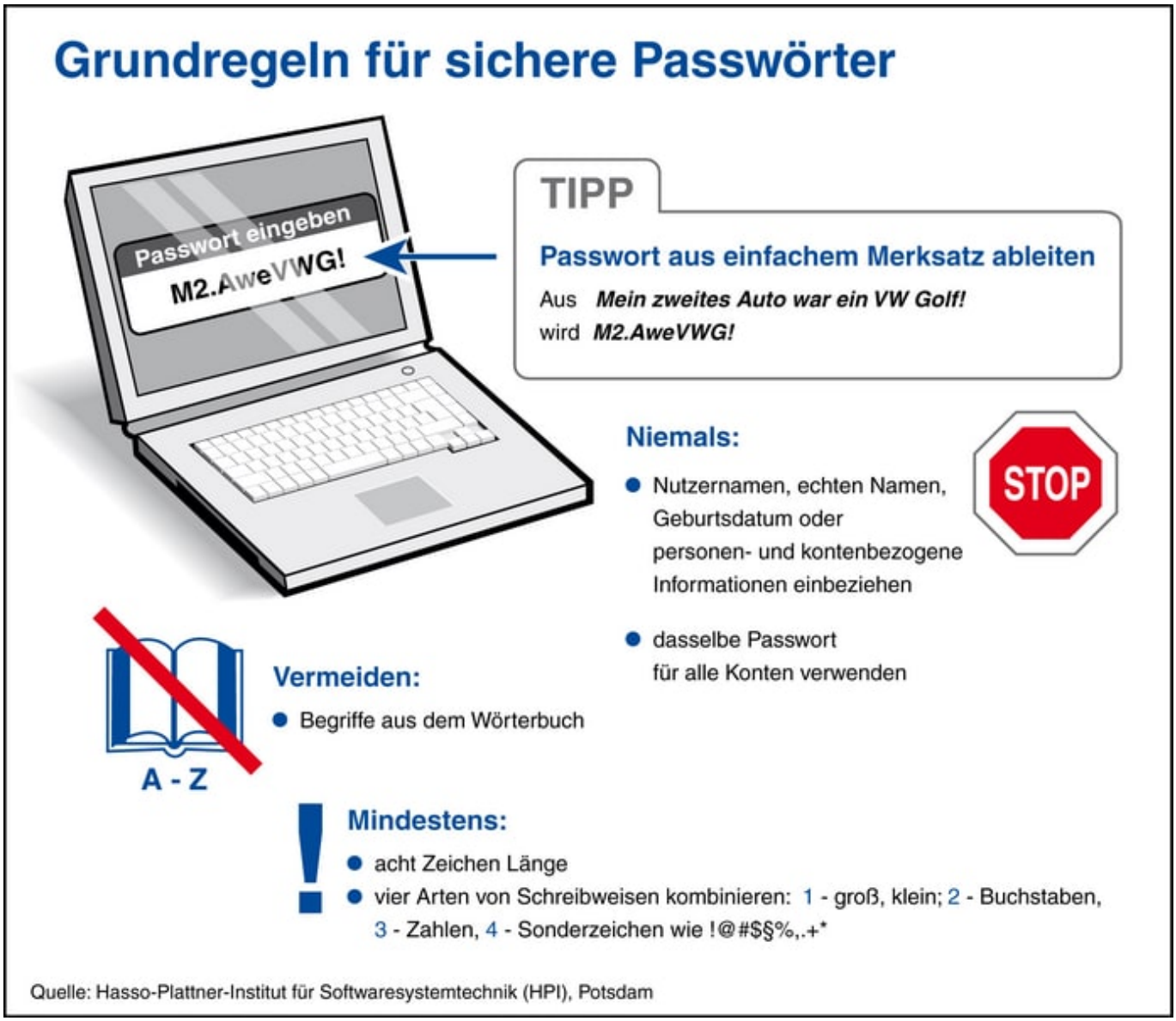
Ob man selbst schon mal Opfer eines Datendiebstahls geworden ist, lässt sich mit dem **Identity Leak Checker** sehr leicht überprüfen, einem Online-Sicherheitscheck des Hasso-Plattner-Instituts (HPI).

Jeder kann kostenlose seine Daten überprüfen

Seit 2014 kann dort jeder Internetnutzer unter https://sec.hpi.de/ilc kostenlos durch Eingabe seiner E-Mail-Adresse prüfen lassen, ob Identitätsdaten von ihm frei im Internet kursieren und missbraucht werden könnten. Mittlerweile ermöglichen die Sicherheitsforscher den Abgleich mit mehr als 13 Milliarden

gestohlener und im Internet verfügbarer Identitätsdaten.

Beinahe täglich gibt es Meldungen über neue Hackerangriffe oder Datenleaks, die uns zeigen, welche Risiken die Digitalisierung mit sich bringt. Mit dem Identity Leak Checker bieten wir allen Internetnutzern seit vielen Jahren die Möglichkeit, eines einfachen und kostenlosen Sicherheitschecks.



Identity Leak Checker

Seit 2014 haben mehr als 17,4 Millionen Nutzer mithilfe des Identity Leak Checkers die Sicherheit ihrer Daten überprüfen lassen. In mehr als 4,6 Millionen Fällen mussten sie darüber informiert werden, dass ihre E-Mail-Adresse in Verbindung mit anderen persönlichen Daten im Internet offen zugänglich

war. Allein im Jahr 2022 wurden 299 Datenlecks in den Identity Leak Checker eingepflegt - zuletzt knapp 230 Millionen Datensätze aus dem Datenleak des Musik-Streaminganbieters Deezer.

In Kombination mit den E-Mail-Adressen sind beim Deezer-Leak auch Angaben zu Vorname, Nachname, Geburtsdatum, Username, Stadt und Ländercode enthalten gewesen sofern Sie vom Nutzer bereitgestellt wurden.

Der Identity Leak Checker bildet auch die Datengrundlage für die meistgenutzten Passwörter der Deutschen, die das HPI jedes Jahr veröffentlicht.

Spezialangebot für Unternehmen und Organisationen: Identity Leak Checker Desktop Client

Der Identity Leak Checker Desktop Client ist ein kostenpflichtiges Angebot für Unternehmen und Organisationen, das sie bei der kontinuierlichen Überwachung der eigenen Domäne(n) unterstützt. Werden neue Datenlecks in den ILC importiert, prüft der Desktop Client automatisch, ob E-Mail-Adressen der überwachten Domäne(n) betroffen sind.

Die betroffene(n) E-Mail-Adresse(n) können dann sofort gewarnt werden. Weitere Informationen zum Angebot unter: https://sec.hpi.de/ilc/

https://www.youtube.com/watch?v=mEsDEVAgUKg&t=5s&ab_channel=NetzkennerJ%C3%B6rgSchieb

Browsererweiterungen: Turbo für Firefox und Chrome

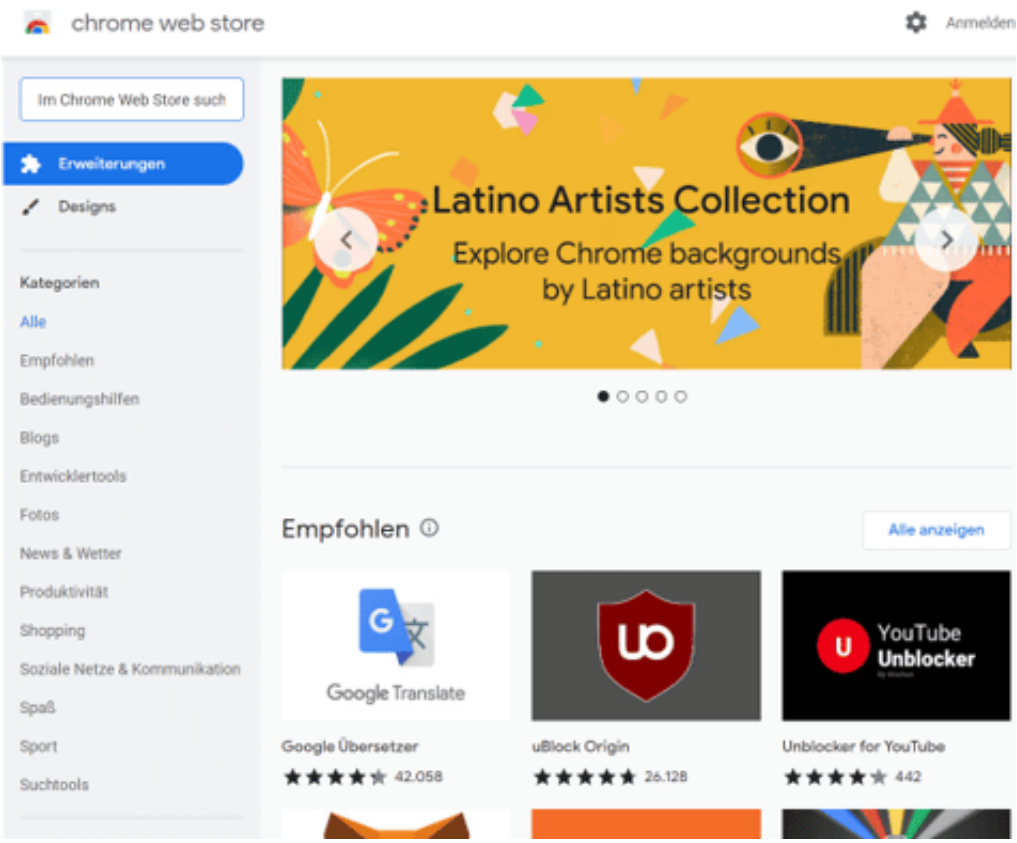
Browser lassen sich durch Erweiterungen vom Funktionsumfang her deutlich erweitern. Das gilt auch Für Google Chrome und Firefox. Wir zeigen Euch, wir Ihr das nutzt.

Funktionserweiterungen in Chrome

Auch bei Google Chrome könnt Ihr Erweiterungen installieren. Aufgrund der Tatsache, dass Chrome (wie Microsoft Edge) auf der Chromium Engine basiert, findet Ihr die meisten Erweiterungen ebenfalls im Chrome Web Store. Wenn Ihr einmal an einem PC ohne Chrome arbeiten müsst, dann könnt Ihr mit hoher Wahrscheinlichkeit die Erweiterung auch in Edge installieren.

- Klickt in Chrome oben rechts auf die drei Punkte, dann wählt **Einstellungen** aus und klickt auf **Erweiterungen**.
- Chrome zeigt Euch jetzt alle Erweiterungen an.

- Hier könnt Ihr die bestehenden Erweiterungen wie gewohnt aktivieren und deaktivieren und deren Einstellungen ändern, solange sie dies zulassen.
- Klickt auf die drei Striche oben links, dann unten auf **Chrome Web Store öffnen**. Um neue Erweiterungen zu laden. Die Funktionsweise ist dieselbe wie bei Edge.
- Wenn Ihr Erweiterungen aus dem Internet herunterladen wollt, dann aktiviert oben rechts in Chrome den Schalter für den Entwicklermodus.
- Durch einen Klick auf **Entpackte Erweiterung laden** könnt Ihr diese dann in Chrome installieren.

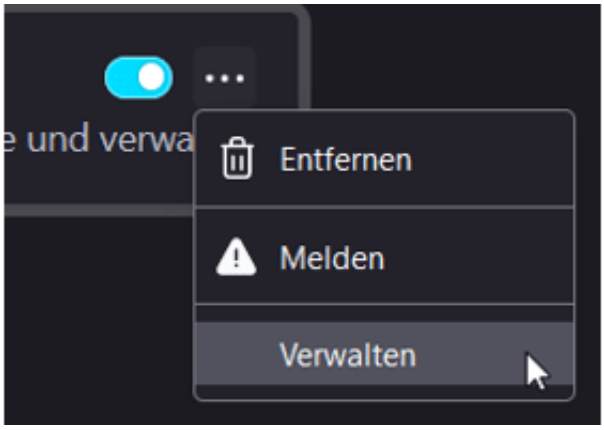


Funktionserweiterungen in Firefox

Firefox nutzt im Gegensatz zu Edge und Chrome nicht die Chromium-Erweiterung und hat aus diesem Grund ganz eigene Erweiterungen. Die findet Ihr im Firefox Add-on-Store.

- Klickt in Firefox oben rechts auf die drei Striche, dann wählt **Einstellungen** aus und klickt auf **Erweiterungen & Themes**, dann auf **Erweiterungen**.
- Firefox zeigt Euch jetzt alle Erweiterungen an.

- Hier könnt Ihr die bestehenden Erweiterungen wie gewohnt aktivieren und deaktivieren und deren Einstellungen ändern, solange sie dies zulassen.
- Wählt aus den angebotenen Erweiterungen aus oder klickt unten auf **Mehr Add-ons ansehen**, um neue Add-ons zu installieren. Die Funktionsweise ist dieselbe wie bei Chrome.



Weitere Infos zu Erweiterungen und auch der Nutzung in Microsoft Edge findet Ihr hier.

Was bitte ist eine DDoS-Attacke?

Regelmäßig informieren die Medien über sogenannte DDoS-Attacken auf Server, die dann zusammenbrechen. Wie zuletzt die Webseiten von deutschen Flughäfen.

Um eine Sache gleich zu klären: Ein DDoS-Angriff auf einen Server ist lästig und oft auch erfolgreich - es ist aber kein Hackangriff, wie häufig zu hören oder zu lesen ist. Denn ein Hack hat das Ziel, irgendwo reinzukommen (einfach gesprochen). Dieses Ziel lässt sich mit einer DDoS-Attacke nicht erreichen, denn der Ziel-Server wird lahmgelegt.

Der Begriff DDoS: Distributed Denial of Service

Aber wofür steht DDoS? Eine **Distributed Denial of Service** (DDoS)-Attacke ist eine gewöhnliche Form von Cyberangriff, bei dem ein Netzwerk oder eine Website durch die Überlastung durch Anfragen lahmgelegt wird. Im Wesentlichen versuchen Angreifer, ein System so zu überwältigen, dass es für normale Nutzer nicht mehr zugänglich ist.

Bei einer DDoS-Attacke verwenden Angreifer in der Regel eine Vielzahl von

infizierten Computern oder Geräten, die als "Botnet" bezeichnet werden. Mit Hilfe eines solchen Botnets - also einer Vielzahl zusammengeschlossener Rechner, die sich zentral steuern lassen, können die Angreifer eine enorme Menge an Traffic zeitgleich an das Ziel (Opfer) senden. Die meisten Geräte (nicht nur Rechner, es können auch ans Netz angebundene Geräte sein) wurden vorher mit Malware infiziert (Schadprogramme), die nur diese eine Aufgabe haben: Sie werden vom Angreifer ferngesteuert, ohne dass der Besitzer es bemerkt.

DDoS Angriffe sind kein Hack, sondern Betrug

Verschiedene Arten von DDoS-Angriffen

Es gibt verschiedene Arten von DDoS-Attacken, einschließlich Netzwerk- oder Bandbreitenüberlastungsangriffen, Anwendungsüberlastungsangriffen und Angriffen auf Infrastrukturebenen wie DNS-Server. Netzwerküberlastungsangriffe zielen darauf ab, die Netzwerkbandbreite zu überlasten, um das System zu verlangsamen oder auszuschalten.

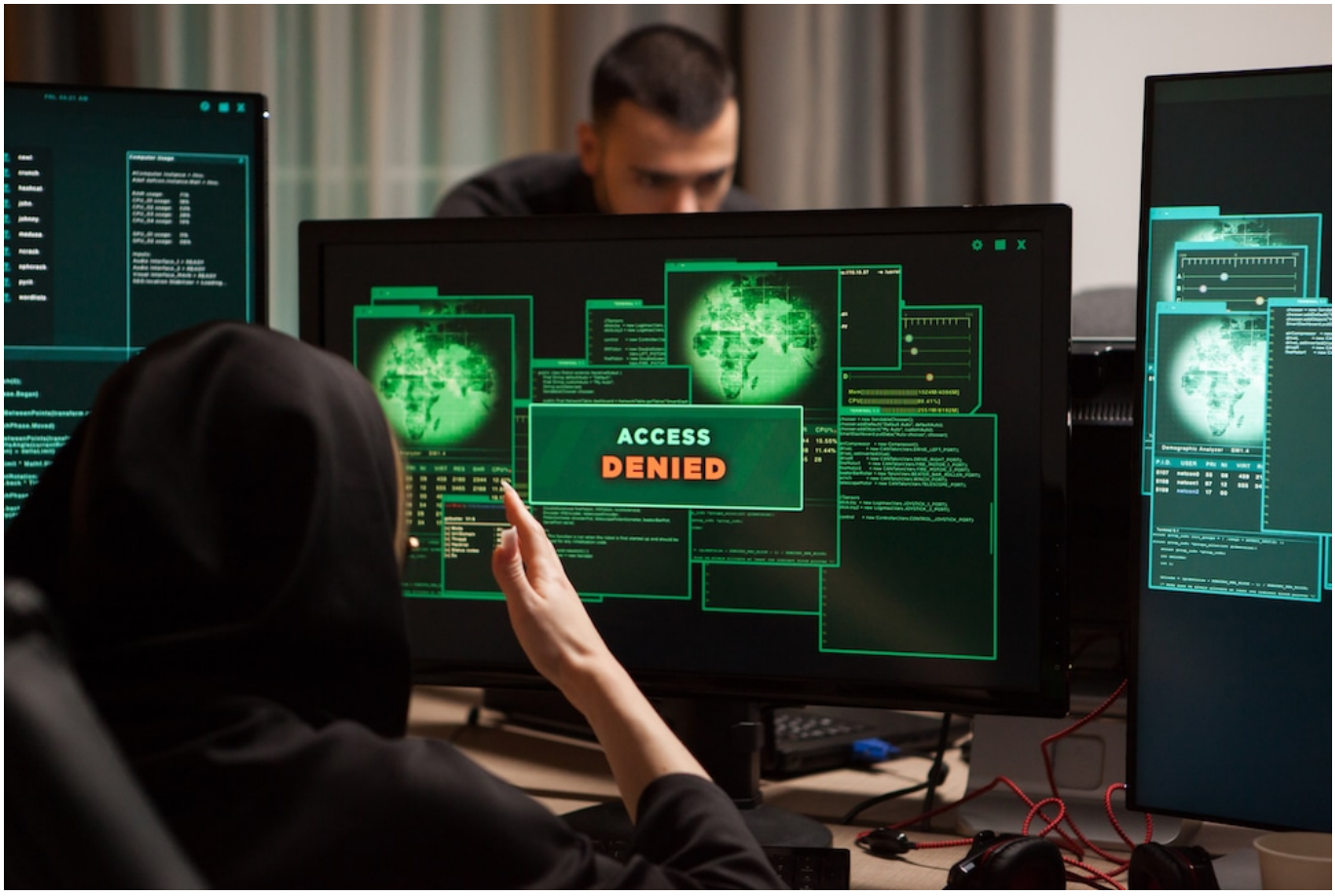
Anwendungsüberlastungsangriffe zielen darauf ab, spezifische Anwendungen

oder Ressourcen zu überlasten, um sie zu deaktivieren oder unzugänglich zu machen. Infrastrukturangriffe zielen darauf ab, die DNS-Server oder andere kritische Komponenten des Systems auszuschalten.

Auswirkungen von DDoS-Angriffen

Die Auswirkungen einer erfolgreichen DDoS-Attacke können durchaus verheerend sein. Denn wenn ein Unternehmen oder eine Organisation nicht in der Lage ist, seine Dienste bereitzustellen, kann es zu erheblichen finanziellen Verlusten kommen. Ein Onlineshop kann keine Waren verkaufen, ein Reisebüro keine Tickets - und der Flughafen kann keine Fluginformationen anzeigen. Darüber hinaus kann es auch zu einem Vertrauensverlust und Rückgang der Markenreputation führen.

Genau das ist der Grund, wieso viele Unternehmen eine solche DDoS-Attacke fürchten. Nicht wenige Cyberbetrüger drohen damit - und fordern Lösegeld, damit ein DDoS-Angriff aufhört oder ausbleibt. DDoS-Angriffe sind ein Drohmittel!



Bei einem DDoS-Angriff werden mit Malware infizierte Rechner eingesetzt

Schutz vor DDoS-Angriffen

Es gibt verschiedene Methoden, um sich vor DDoS-Attacken zu schützen. Für Privatleute in aller Regel völlig unnötig, sich Gedanken zu machen. Wer jedoch ein Geschäft betreibt und/oder von seinen Onlinediensten abhängig ist, sollte sich das ggf. überlegen.

Eine Möglichkeit ist die Verwendung von speziellen DDoS-Schutzdiensten, die den Datenverkehr überwachen und ungewöhnliche Aktivitäten erkennen und blockieren können. Eine andere Möglichkeit besteht darin, das Netzwerk oder die Website zu skalieren, um einen größeren Traffic zu bewältigen, als dies normalerweise der Fall ist.

Insgesamt ist es wichtig, sich der Gefahren von DDoS-Attacken bewusst zu sein und geeignete Maßnahmen zu ergreifen, um sich vor ihnen zu schützen. Unternehmen und Organisationen sollten regelmäßig ihre IT-Systeme und Netzwerke überwachen, um Anzeichen von Angriffen zu erkennen und schnell darauf zu reagieren, um ihre Systeme und ihre Kunden zu schützen

Daten aus der Apple Watch für die Forschung

Die Apple Watch ist ein leistungsfähiger Sensor für die Herzgesundheit: Die Smartwatch erkennt Puls und Rhythmus. Diese Daten kann jetzt die Forschung nutzen - wenn User sie freigeben.

Smartwatches für die Wissenschaft: Apple hat ein neues Programm für Forscher aufgelegt, über das sich die Smartwatches des Herstellers in größerem Umfang für Studienzwecke beziehen lassen. Die Idee: Es gibt Millionen Menschen mit validen Daten da draußen. Warum die nicht für die Forschung nutzen!

Ein guter Gedanke, sofern die Daten anonymisiert sind.

Das Herz eines durchschnittlichen, gesunden Erwachsenen schlägt mehr als 100.000 Mal pro Tag. Schlag für Schlag, Tag für Tag, entsteht ein Bild — ein Bild, das weitgehend unsichtbar bleibt.

Die Apple Watch kann helfen, das Unsichtbare sichtbar zu machen. Mit Funktionen für die Herzgesundheit — darunter Mitteilungen über hohe und niedrige Herzfrequenzen, Cardio Fitness, Mitteilungen über unregelmäßigen Herzrhythmus, die EKG App und das Vorhofflimmern-Protokoll. Auf diese Weise lassen sich Rückschlüsse auf die Fitness und die Herzgesundheit ziehen.

Daten von vielen erlauben Erkenntnisse

Die gleiche fortschrittliche Technologie, die den Nutzern Einblicke in ihre individuelle Gesundheit gewährt, hat auch das Potenzial, der Forschung und medizinischen Communitys die Tür zu neuen Entdeckungen zu öffnen. Seit der Einführung von ResearchKit und CareKit durch Apple im Jahr 2015 haben Forscher, Krankenhausärze und Entwickler innovative neue Wege gefunden, um eine breite Palette von Erkrankungen zu untersuchen, zu verfolgen und zu behandeln.

Um Entdeckungen voranzutreiben, die die Gesundheit in großem Umfang verbessern, hat Apple das Investigator Support Program ins Leben gerufen. Im Rahmen dieses Programms stellt Apple Forscherm Apple Watch Geräte zur Verfügung, mit denen sie neue Wege in der Gesundheitsforschung beschreiten können, unter anderem zum wissenschaftlichen Verständnis des Herzens.

Apple stellt die wegweisende Arbeit von Gesundheitsforschern auf der ganzen Welt, die die Apple Watch nutzen, um das Herz wie nie zuvor zu untersuchen, in den Mittelpunkt.

Konkrete Forschung mit Watch als Sensor

Die assoziierte Professorin Rachel Conyers und Dr. Claudia Toro sind leitende pädiatrische Onkologen aus Melbourne, Australien. Sie verbringen ihre Tage hauptsächlich mit der Betreuung von Kindern in einer tertiären pädiatrischen Onkologieklinik und der Erforschung von Toxizitäten im Zusammenhang mit Krebstherapien bei Kindern.

Gemeinsam untersuchen sie, wie sich die Behandlung auf den Herzrhythmus auswirken kann, und versuchen, innovative Wege zur Intervention zu finden. Die Inspiration für ihre Arbeit kommt von ihren Patient:innen — sowohl von Erfolgs- als auch herzzerreißenden Geschichten.

Toxizitäten bei der Krebsbehandlung können zu Herzrhythmusstörungen wie dem verlängerten QT-Syndrom führen, das potenziell lebensbedrohlich sein kann. Eine QT-Verlängerung führt zu einem unregelmäßigen Herzrhythmus und verlängert die Zeit, die das Blut zum Fließen durch das Herz benötigt.

Aufgrund ihrer Anfälligkeit für eine lange QT-Zeit werden Kinder, die eine Krebsbehandlung erhalten, routinemäßig mindestens einmal pro Woche einem 12-Kanal-EKG unterzogen, sagt Dr. Conyers. Ambulante Patienten benötigen jedoch weiterhin Zugang zur Überwachung.

Apple hat verschiedene neue Watch 8 Modelle vorgestellt

Mehr über die Herzgesundheit lernen

In den kommenden Monaten werden die Mediziner am Murdoch Children's Research Institute zunächst die Empfindlichkeit der Apple Watch EKG App bei 40 Kindern und Jugendlichen untersuchen. Danach wird das Team nach Möglichkeiten suchen, wie die Patienten ihre EKGs überall und jederzeit aufzeichnen können. Mit diesen Erkenntnissen hofft das Team, die Realität der kardialen Toxizität besser zu verstehen und mögliche Interventionsmöglichkeiten zu identifizieren.

Bewohner der Bay Area erinnern sich an den Tag, an dem sich der Himmel orange gefärbt hat. Es geschah am 9. September 2020. Dr. So-Min Cheong, eine assoziierte Professorin im Fachbereich Öffentlicher Dienst und Verwaltung an der Bush School der Texas A&M University, ist in Palo Alto, Kalifornien, gewesen.

In den Jahren 2020 und 2021 ist es in Kalifornien zu einer Reihe von verheerenden Waldbränden gekommen. Dr. Cheong, die die sozialen und gesundheitlichen Folgen von Umweltkatastrophen und Klimawandel erforscht, hat eine Möglichkeit gesehen, die Auswirkungen des Rauchs von Waldbränden auf die Herzgesundheit von Feuerwehrleuten zu untersuchen.

„Allgemeine Gesundheitsempfehlungen oder Interventionen von der Stange waren mir nicht genug“, erklärt Dr. Cheong. „Menschen sind einzigartig. Jeder Mensch ist anders, wenn es um seine Gesundheit geht, und ich wollte mehr erfahren.“

Nächsten Monat werden Dr. Cheong von der Texas A&M University und Dr. Brian Kim und Dr. Marco Perez der Stanford Medicine damit beginnen, Feuerwehrleute mit der Apple Watch auszustatten, um die Auswirkungen von Waldbrandrauch auf die Herzgesundheit zu untersuchen. Die Waldbrandsaison beginnt im Frühjahr in Texas und im Sommer in Kalifornien, und bis zu 200 Feuerwehrleute in diesen Gebieten werden an der Studie teilnehmen.

Die Studie sieht vor, mit der Apple Watch Herzfrequenz und -rhythmus, Schlaf, Blutsauerstoff, Aktivitätsdaten und mehr zu überwachen. Die Feuerwehrleute werden außerdem einen Luftqualitätsmonitor tragen und Umfragebögen zu Schlaf, Aktivität und Symptomen im Zusammenhang mit Waldbrandrauch ausfüllen.

Erkennen und Bekämpfen von Vorhofflimmern

„Die Feuerwehrleute werden von der Studie profitieren“, sagt Dr. Cheong. „Wir wissen, dass der Rauch von Waldbränden direkte Auswirkungen auf ihre Gesundheit hat, und mit einer Studie wie dieser können sie ihre Ergebnisse in Echtzeit sehen.“

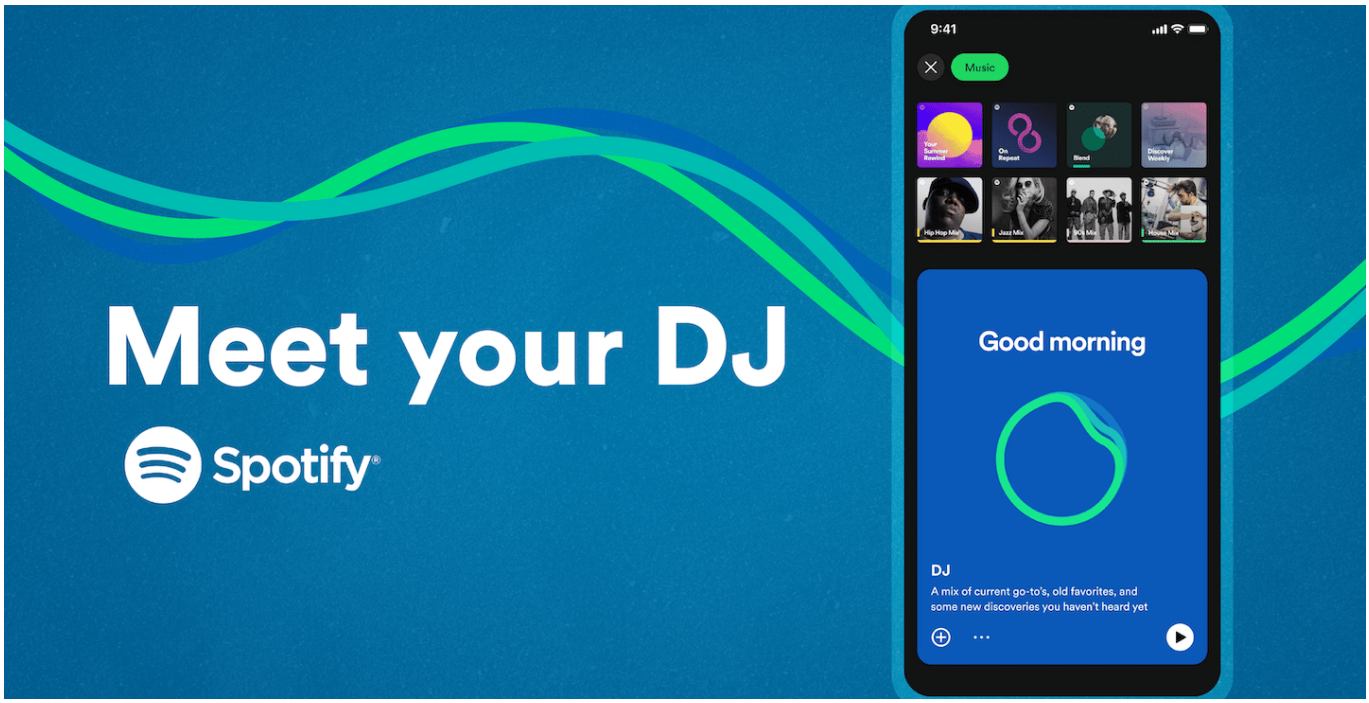
Allerdings möchte sie die möglichen Ergebnisse der Studie noch nicht verallgemeinern, vor allem, wenn der Schwerpunkt der Forschung auf der Art von individualisierten und präzisen Gesundheitsdaten liegt, die die Apple Watch liefern kann.

Nach Angaben von Epidemiologie-Experten Europa wird sich die Rate an Vorhofflimmern (AFib) in der Europäischen Union bis 2060 verdoppeln. Vorhofflimmern ist eine weit verbreitete Herzrhythmusstörung, die unbehandelt schwerwiegende Folgen haben kann, beispielsweise ein erhöhtes Risiko für Schlaganfälle oder Herzversagen.

An den Amsterdam University Medical Centers erforschen Dr. Sebastiaan Blok, Leiter der Abteilung eHealth der Cardiology Centers of the Netherlands, und seine Kolleg:innen Möglichkeiten, Vorhofflimmern früher zu erkennen. Die

Forscher:innen haben eine auf dem Zufallsprinzip basierte Kontrollstudie als Teil einer größeren Initiative namens HartWacht entwickelt, dem ersten erstattungsfähigen eHealth-Konzept.

Spotify führt virtuellen KI-DJ ein



Der Streamingdienst Spotify führt für Premium-Nutzer einen Discjockey ein, der auf Künstlicher Intelligenz basiert - und individuelle Playlists spielt. Zunächst aber nur in Englisch.

Das wird aber auch mal Zeit, dass sich die Streamingdienste etwas fundamental Neues einfallen lassen. Denn egal ob Audio oder Video Streaming: Durch innovative Konzepte sind die erfolgsverwöhnten Dienste in den letzten Monaten und Jahren nicht gerade aufgefallen.

Das, was Spotify da jetzt angekündigt hat, ist aber in der Tat etwas völlig Neues: Premium-Kunden sollen schon bald in den Genuss eines individuellen DJs kommen, der mit natürlicher Sprache spricht, individuelle Playlisten kuratiert - und auch anmoderiert.

Dahinter steckt natürlich Künstliche Intelligenz (KI), die nicht nur - à la ChatGPT - entsprechende Texte generiert, die der DJ sagt, sondern auch den Musikgeschmack jedes einzelnen Users ermitteln und treffen soll.

Künftig können Nutzer eine neue DJ-Taste in der App antippen und wechseln so in den interaktiven KI-Modus. Hier begrüßt der DJ - mittelfristig bestimmt einen mit wählbarem Temperament, Geschlecht und Slang - und kündigt den jeweils

nächsten Track an. Eine Kombination aus Party-DJ und Radiomoderation, wie es sie auf Apple Music ja gibt.

Individuelle Playlist - ebenfalls erstellt durch KI

Individuelle Playlist und live generierte Stimme

Jetzt aber nicht zu früh gefreut: Das Smartphone kann in der Hosentasche bleiben. Die neue Funktion wird erst mal in USA und Kanada angeboten. Es dauert sicher eine Weile, bis dieser Service auch in anderen Sprachen wie Deutsch angeboten wird.

Besonders interessant ist die Frage, wie Spotify es hinbekommt, quasi in Echtzeit die Moderationsstimme des DJ zu generieren. Dazu verwendet Spotify nach eigenen Aussagen auf die Technik von Sonantic zurück. Ein Unternehmen, das der skandinavische Musik-Streamingdienst im Juni 2022 akquiriert und übernommen hat.

Sonantic hatte sich auf nunanciert sprechende, realistisch klingende KI-Spracherzeugung spezialisiert. Wem der typische Klang der Moderationsstimme bekannt vorkommt: Das Unternehmen hat für das Training der KI die Stimme von Xavier "X" Jernigan analysiert, bekannt als Moderator der Morgenshow "The Get Up" in den USA.

Mit gefällt dieser personalisierende Ansatz von Spotify - endlich mal was Neues, was wirklich niemandem weh tut, aber Spaß bringen kann. Laut Spotify befindet sich die DJ-Funktion zunächst im Betatest. Klar, dass das Unternehmen da erst mal Erfahrungen sammeln muss.

Die Stimmt der Moderation wird von Sonantic erzeugt - von Spotify gekauft

KI erlernt Musikgeschmack der Nutzer

Aber nicht nur hinter der künstlich erzeugten Stimme steckt KI. Auch will Spotify mit Hilfe von KI den Musikgeschmack jedes einzelnen Users besser verstehen. Dazu kommt ein KI-System von OpenAI zum Einsatz - und: nein, diesmal nicht ChatGPT.

Die KI analysiert das Hörverhalten und wählt passende Musikstücke aus. Das spült dem Nutzer nicht nur Neuvorstellung in die Timeline, die er oder sie vielleicht noch nicht gehört hat, sondern auch Songs, die gerne immer wieder angehört werden. Auf diese Weise soll ein interessanter Mix entstehen.

Und noch etwas ist geplant: Zum Jahresende will Spotify seinen Usern künftig individuell generierte Jahresrückblicke anbieten: Das hast Du im Sommer gehört, da ging die Party richtig ab - und da warst Du verliebt.

So spannend das mitunter klingt: Es braucht auch einen kritischen Blick darauf,

ob und welche persönlichen Daten (Stimmung, Verfassung) gesammelt, gespeichert und ausgewertet werden.

Ob und wann die Funktion auch in deutscher Sprache und in Europa verfügbar ist? Spotify will nichts verraten.

https://www.youtube.com/watch?v=ok-aNnc0Dko

Microsoft Outlook: Signaturen richtig setzen

Wenn Ihr Outlook als E-Mail-Programm nutzt, dann unterschreibt Ihr in jeder E-Mail erneut. Je länger der Titel und der Name, desto mehr Aufwand ist das. Unnötig, wenn Ihr eine Signatur verwendet!

Mail-Unterschrift: Teil der Netiquette

Vor allem die hohe Frequenz der Kommunikation führt häufig dazu, dass man Höflichkeitsformeln wie einen Gruß oder eine Unterschrift vermeidet oder vergisst. Das mag in manchen Situationen angemessen sein, birgt aber auch ein Risiko: Es wirkt schnell unhöflich und kann bei der einen oder anderen Gelegenheit dazu führen, dass eure E-Mail nicht die gewünschte Wirkung erzielt. Wenn Ihr Euch informieren wollt, worauf Ihr bei der Kommunikation im Internet achten solltet, sucht nach dem Begriff Netiquette. auch der höfliche Abschluss einer E-Mail gehört dazu.

Microsoft Outlook: Signaturen als Vorlage

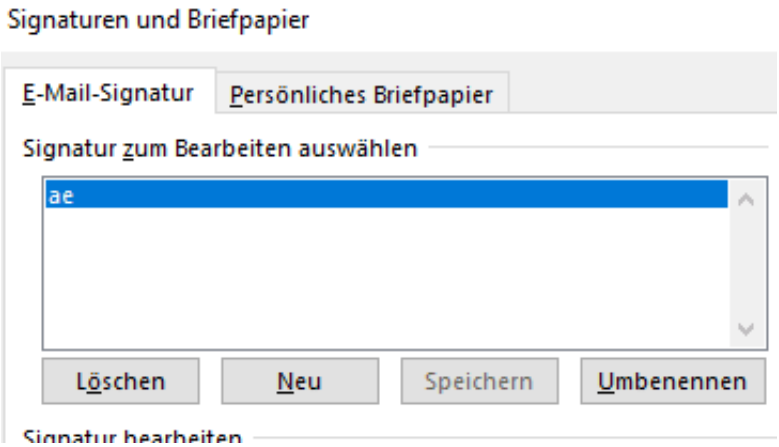
Nun werdet Ihr Eure E-Mails eher selten unterschiedlich unterschreiben, und da kommt die Signatur ins Spiel. So gut wie jedes E-Mail-Programm unterstützt die automatische Verwendung einer Signatur. Die ist nichts anderes als ein kleiner

Textblock, der automatisiert ans Ende einer jeden E-Mail gehängt wird. Um diese zu verwenden, solltet Ihr Euch vorher überlegen, zu welchen Gelegenheiten Ihr diese braucht.

- Überlegt Euch, ob Ihr eher eine formelle oder eine lockere Kommunikation nutzt.
- Viele Programme unterstützen auch mehrere Signaturen, sodass Ihr beispielsweise eine für die private, eine andere für die berufliche Kommunikation einrichten könnt.
- Schreibt Euch die Signatur in einem Textverarbeitungsprogramm vor, dann müsst Ihr sie nur noch in Outlook hineinkopieren.

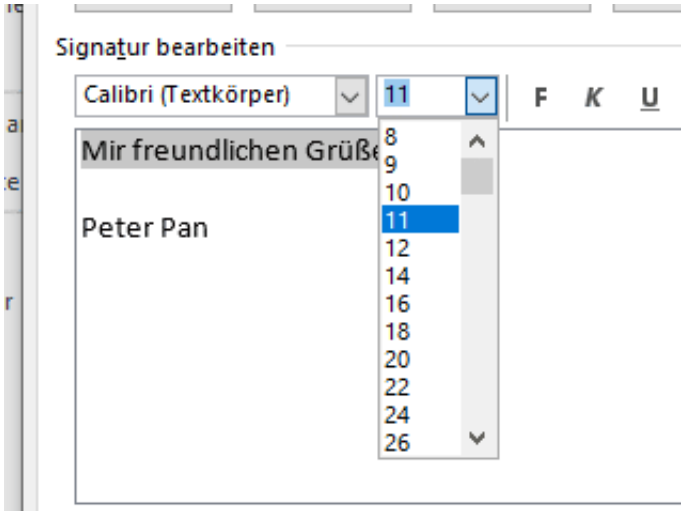
Signaturen in Outlook einrichten

Das Einrichten Eurer Signaturen in Outlook ist in wenigen Schritten erledigt. Auch bei anderen E-Mail-Programmen funktioniert die Konfiguration ähnlich:



- Klickt auf **Datei** > **Optionen** > **E-Mail**, um in die E-Mail-Einstellungen zu gelangen
- Rollt nach unten in den Bereich **Nachrichten verfassen** und klickt auf **Signaturen...**
- Wenn Ihr eine neue Signatur anlegen wollt, dann klickt auf **Neu**.
- Habt Ihr die Signatur schon als Text in Word oder einer anderen Textverarbeitung vorbereitet? Dann könnt Ihr ihn direkt über die Zwischenablage in den Eingabebereich der Signatur einfügen.
- Gebt der Signatur einen sprechenden Namen, damit Ihr sie identifizieren könnt, wenn Ihr verschiedene verwendet.
- In diesem Eingabebereich findet Ihr einfache Formatierungsmöglichkeiten:

Schriftart, Schriftgröße, Textattribute wie fett, kursiv und unterstrichen könnt Ihr in den Text einfügen. Durch einen Klick auf **OK** speichert Ihr die Änderungen.

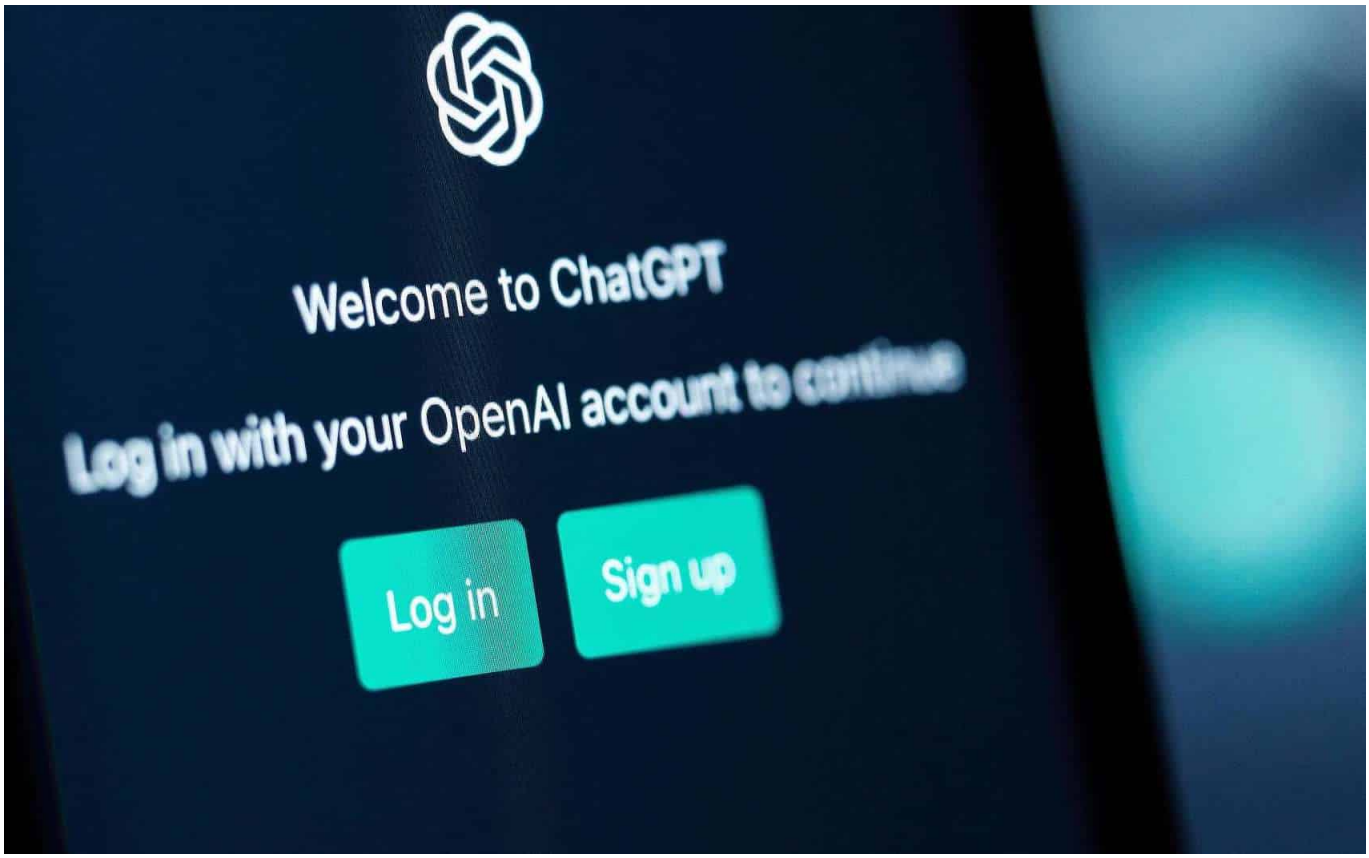


Signaturen in Outlook verwenden

Wenn Ihr einmal die Signaturen eingegeben habt, dann könnt Ihr diese entweder manuell oder automatisch verwenden:

- Unter **Standardsignatur auswählen** könnt Ihr erst das E-Mail-Konto (wenn es mehr als eines ist), dann die Signatur, die automatisch in E-Mails eingefügt werden soll, auswählen.
- Letztere könnt Ihr unterschiedlich für neue und beantwortetet/weitergeleitete E-Mails verwenden. Das macht Sinn, wenn bei neuen E-Mails eine formelle Signatur nötig ist, bei einer Antwort aber beispielsweise ein "Gruß, Jörg" reicht, dass Ihr gegebenenfalls dann doch selbst tippt.

KI-System "Luminous" aus Deutschland

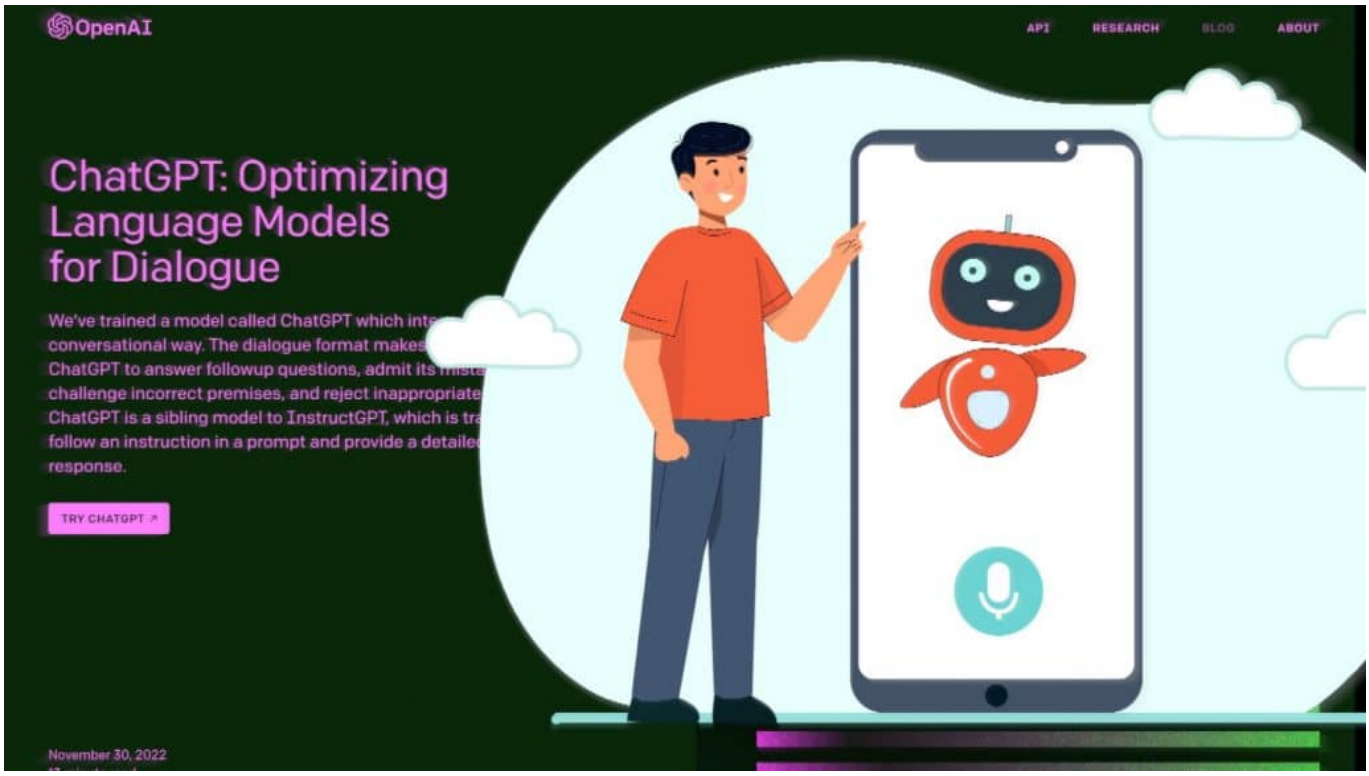


Der Wettbewerb um die leistungsfähigsten und schnellsten KI-Systeme nimmt Fahrt auf. Die meisten kommen aus den USA. Mit "Luminous" gibt es aber auch ein vielversprechendes Angebot aus Deutschland - und das ist effizienter und verbraucht weniger Energie.

Noch schreibt hier ein echter Autor aus Fleisch und Blut.

Muss man heutzutage betonen, denn man könnte den Eindruck bekommen, die KI übernimmt im Eiltempo so ziemlich alle kreativen Aufgaben. ChatGPT schreibt Texte, Midjourney erstellt Bilder. Es gibt Apps, um Stimmen oder Videos zu bauen, die echt aussehen...

Es ist gerade wahnsinnig viel Bewegung in dem Thema. Spotify zum Beispiel hat einen virtuellen DJ angekündigt: KI spricht mit künstlicher Stimme zum User und spielt nur für ihn oder sie eine individuelle Playlist. Abgestimmt auf Geschmack und aktuelle Stimmung. Die KI drängt also in alle Bereiche unsere Lebenswelt. Aber wo stehen wir in Deutschland da – und wie viel Strom/Energie kostet das alles eigentlich?



ChatGPT3 macht aktuell von sich reden und ist wohl die beliebteste KI aller Zeiten

Ein KI-System aus Heidelberg: "Luminous" von Aleph Alpha

Im Augenblick macht ja vor allem ChatGPT von sich Reden: Dieser Chat-Bot von OpenAI, der nicht nur Fragen beantwortet oder Hausaufgaben schreibt, sondern irgendwie alles kann. Auch Google und Microsoft haben hektisch KI in ihre Suchmaschinen integriert. Alles US-Konzerne - nix aus Europa oder gar Deutschland.

Es gibt einen Lichtblick: Das KI-Unternehmen Aleph Alpha aus Heidelberg hat ein KI-Modell entwickelt, das sich „Luminous“ nennt – also übersetzt „leuchtend“, das es durchaus mit ChatGPT und vergleichbar leistungsfähigen KI-Systemen aufnehmen kann. Laut aktuellen Vergleichstests ist das deutsche System sogar doppelt so effizient wie das von OpenAI, über das derzeit alle reden.

Man müsste sehr ins Detail gehen, um die Testweise zu erklären und wie sich solche Systeme vergleichen lassen. Aber Luminous ist ein 70 Milliarden Parameter großes Modell – das erklärt, wie viel und wie lange trainiert werden muss –, während die gängigen Systeme wie ChatGPT aus 175 Milliarden Parameter bestehen. Demnächst wollen die Deutschen ein deutlich besser

trainiertes System vorstellen. Das könnte und müsste der Logik folgend dann schneller sein und bessere Ergebnisse liefern. Besser bedeutet: Besseres Verständnis, was gewünscht ist – und bessere Ergebnisse.

Luminous ist eine extrem leistungsfähige KI aus Deutschland

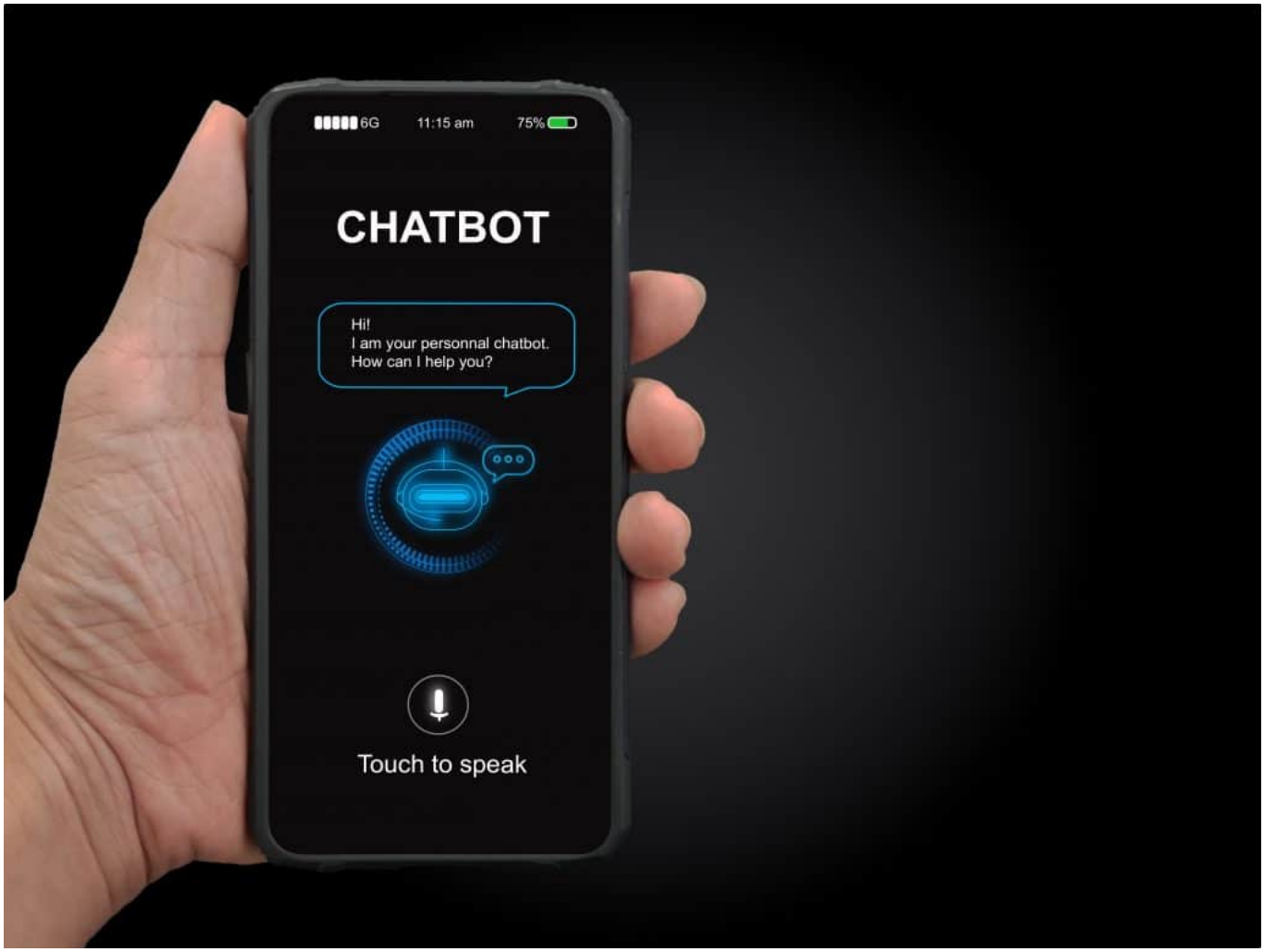
KI-System verbrauchen beim Training eine Menge Energie

Für einen in Computerdingen eher unerfahrenen Menschen ist es ja schwer vorstellbar, wie KI-Systeme überhaupt funktionieren. Wie schaffen sie sich das Wissen drauf und wieso ist es so aufwändig und teuer?

Es gibt verschiedene Konzepte für KI-Systeme. ChatGPT und vergleichbare Systeme werden nicht programmiert, wie bei Computern sonst üblich, sondern sie werden „trainiert“: Experten „füttern“ die Systeme mit Inhalten. In diesem Fall mit Milliarden von Texten aus den unterschiedlichsten Quellen. Der Lernprozess wird von Menschen begleitet und gesteuert (bei anderen KI-Systemen ist das nicht so), deshalb wird hier von „pretrained“ Modellen gesprochen.

Diese Lernphase ist besonders zeit- und kostspielig: Es braucht unzählige Rechner und zigtausende Stunden, um das Material zu importieren und analysieren zu lassen. Das alles lange bevor die KI überhaupt benutzt werden

kann. Später müssen noch Ebenen (Layer) eingezogen werden, um das Material zu kategorisieren: Etwa, so sehen Radiotexte aus, so Lyrik, so Texte für Blogposts. Wenn wir einen ChatBot nutzen, greifen wir auf dieses vorbereitete Material zurück.



Chat-Bot ChatGPT erstellt auf Wunsch eigenständig Texte

Enormer Energieaufwand

Klingt nicht nur nach einem enormen Energieaufwand, sondern ist auch einer.

Es kann Monate dauern, ein komplexes System zu trainieren – und komplette Rechenzentren auslasten. Leider machen die großen Betreiber wie Google, Facebook, OpenAI keine konkreten Aussagen über den tatsächlichen Aufwand. Das macht es schwer, das einzuschätzen.

Das Training eines einzelnen Modells erzeugt nach einer aktuellen Studie so viel

Emissionen wie ein durchschnittlicher Amerikaner in 17 Jahren – oder in etwa so viel wie 300 Flüge von New York nach San Francisco. Eine Untersuchung, die das Magazin „Wired“ zitiert, sieht einen Verbrauch von über 1.200 Megawattstunden und so viel CO2-Emissionen wie 550 Flüge zwischen New York und San Francisco.

Je mehr die KI können soll, desto mehr Strom frisst sie letztlich. Und da jetzt überall KI rein soll, nicht nur in die Suchmaschinen Google und Bing, sondern auch in Apps, wird der Energiebedarf explodieren. Es wird Zeit, dass das transparent gemacht wird. Wie viel CO2 ausgestoßen wird, hängt natürlich davon ab, ob vor allem fossile oder grüne Energie zum Einsatz kommt.

Kosten: Wer soll das alles bezahlen?

ChatGPT und auch die KI-Dienste in Bing und Google werden Unternehmenskunden berechnet. Die Preise sind ordentlich. Ich bezahlt auch für ChatGPT, 20 EUR im Monat – damit ich keine Einschränkungen habe und alles nutzen kann. Das Problem, das wir hier haben: Strom ist in Europa und besonders in Deutschland teurer als anderswo.

Wenn ein Startup wie Aleph Alpha kommt und ein neues Modell aufsetzen will, sind es vor allem die Stromkosten, die schnell in die Millionen gehen können. Wir haben also einen doppelten Standortnachteil in Deutschland: Wenig Know-how, wenige Experten – und hohe Stromkosten. Nun hat das deutsche Startup mit seinem „Luminous“-KI-Modell einen fetten Vorteil: Es ist sehr viel effizienter, verbraucht also deutlich weniger Strom als andere Systeme – bei gleicher oder sogar besserer Leistung.

Das ist bemerkenswert und kann sich zu einem großen Wettbewerbsvorteil für dieses Startup entwickeln. Wir brauchen mehr solcher Systeme, die weniger Strom verbrauchen, damit günstiger sind und die Umwelt nicht so stark belasten.

Autonomes Fahren soll schlecht fürs Klima sein

In den USA gibt es sie schon - und viele sehen darin die Zukunft: Selbstfahrende Autos, die eigenständig von A nach B fahren. Wissenschaftler haben jetzt den Energiebedarf des autonomen Fahrens untersucht.

Mit dem Auto zu fahren belastet die Umwelt - das ist unbestreitbar. Nun entwickelt sich aber gerade eine vergleichsweise neue Form der Fortbewegung, die das Klima auf eine andere Weise belastet: Autonomes Fahren - auch "Selfdriving Cars" genannt.

Selfdriving Cars oder auch Autonomous Autos sind Fahrzeuge, die in der Lage sind, ohne menschliches Eingreifen zu fahren. Sie werden mit Künstlicher Intelligenz (KI) und Sensoren ausgestattet, um ihre Umgebung wahrzunehmen, zu analysieren und Entscheidungen zu treffen.

Gps navigation system on a phone in a self-driving car

Selbstfahrende Autos benötigen KI

Selbstfahrende Autos haben das Potenzial, den Verkehr sicherer und effizienter zu gestalten, indem sie menschliche Fehler reduzieren und weil sie eine schnellere Reaktionszeit als der Mensch haben. Sie könnten auch den Verkehr auf den Straßen entlasten, indem sie in der Lage sind, den Abstand zwischen den Fahrzeugen zu optimieren und dadurch die Anzahl der benötigten Fahrspuren zu reduzieren.

Allerdings sind selbstfahrende Autos selbst auch nicht perfekt: Noch bauen sie immer wieder Unfälle, weil sie noch nicht auf jede Situation optimal trainiert sind.

Jetzt haben Wissenschaftler untersucht, wie energieaufwändig das autonome Fahren ist. Laut einer Studie des Massachusetts Institute of Technology (MIT) wird autonomes Fahren in der heutigen Form zukünftig einen enormen CO2-Ausstoß verursachen. Grund dafür sei laut Forschern die vergleichsweise hohe Rechenleistung der Fahrzeuge, die zu einem sehr hohen Energieverbrauch

führt.

CO2-Ausstoß durch selbstfahrende Autos

Die Wissenschaftler gehen in der Studie davon aus, dass im Jahr 2050 rund eine Milliarde selbständig fahrende Autos unterwegs sind. Eine Schätzen, die nicht genau so eintreffen muss. In diesem Fall würden diese 1 Mrd. autonomen Fahrzeuge bei einer Fahrzeit von einer Stunde am Tag alleine durch ihre KI 0,14 Gigatonnen CO2 pro Jahr verursachen. Eine Menge, wie sie das Land Argentinien produziert derzeit ein Land - oder sämtliche Rechenzentren der Welt zusammen. Dabei sind die Sensorentätigkeiten der Autos und die Herstellungs-Emissionen noch gar nicht eingerechnet.

Allerdings muss man zur Datenlage sagen: Niemand kann wissen, wie viel CO2 im Jahr 2050 überhaupt noch durch Rechenzentren ausgestoßen werden (hoffentlich gar keins) - und wie sich Rechnereffizienz und KI bis dahin weiter entwickelt. Die Studie darf und sollte daher nicht zu penibel interpretiert werden, sondern vielmehr nur als Richtschnur verstanden werden.

Chancen durch selbstfahrende Autos

Nicht zu vergessen sind auch die Chancen durch selbstfahrende Autos - sie können Energie einsparen helfen.

Denn Selfdriving Cars haben das Potenzial, die Art und Weise zu verändern, wie wir uns fortbewegen und wie wir unser Leben organisieren. Sie können für Menschen von unschätzbarem Wert sein, die nicht in der Lage sind, selbst zu fahren, wie zum Beispiel ältere Menschen oder Menschen mit Behinderungen.

Auch für Berufspendler könnten selbstfahrende Autos von Vorteil sein, da sie während der Fahrt arbeiten oder entspannen können, anstatt sich auf die Straße konzentrieren zu müssen. Allerdings gibt es noch viele Herausforderungen zu bewältigen, bevor Selfdriving Cars weit verbreitet werden können, wie beispielsweise die Entwicklung zuverlässiger Technologien und die Regulierung des Straßenverkehrs.

Wir brauchen mehr Resilienz!

Webseiten deutscher Flughäfen werden durch Hacker ("Russian Anonymous") lahmgelegt. Die IT der Lufthansa durch einen Bagger. Das kann doch alles gar nicht wahr sein... Wir brauchen mehr Resilienz.

Fliegen, also das Reisen per Flugzeug – war in den vergangenen Tagen alles andere als vergnügungssteuerpflichtig. Einige Flughäfen wurden bestreikt. Das kommt ja immer wieder vor. Aber dann gab es auch noch Ärger und Schwierigkeiten mit der IT: Die Webseiten von diversen Flughäfen, darunter Düsseldorf, Hannover, Nürnberg, Dortmund, wurden angriffen und damit lahmgelegt.

Reisende konnten also nicht mal nachschauen, ob ihre Flüge pünktlich abgehen oder die Flüge von Freunden oder Verwandten pünktlich ankommen. Und einige Tage vorher war in Frankfurt Chaos wegen eines durchtrennten Datenkabels bei der Lufthansa. Irgendwie kann das doch alles gar nicht wahr sein: Wichtige Verkehrsdienste liegen wegen Kleinigkeiten lahm.

Komplette Flughäfen wurden lahmgelegt

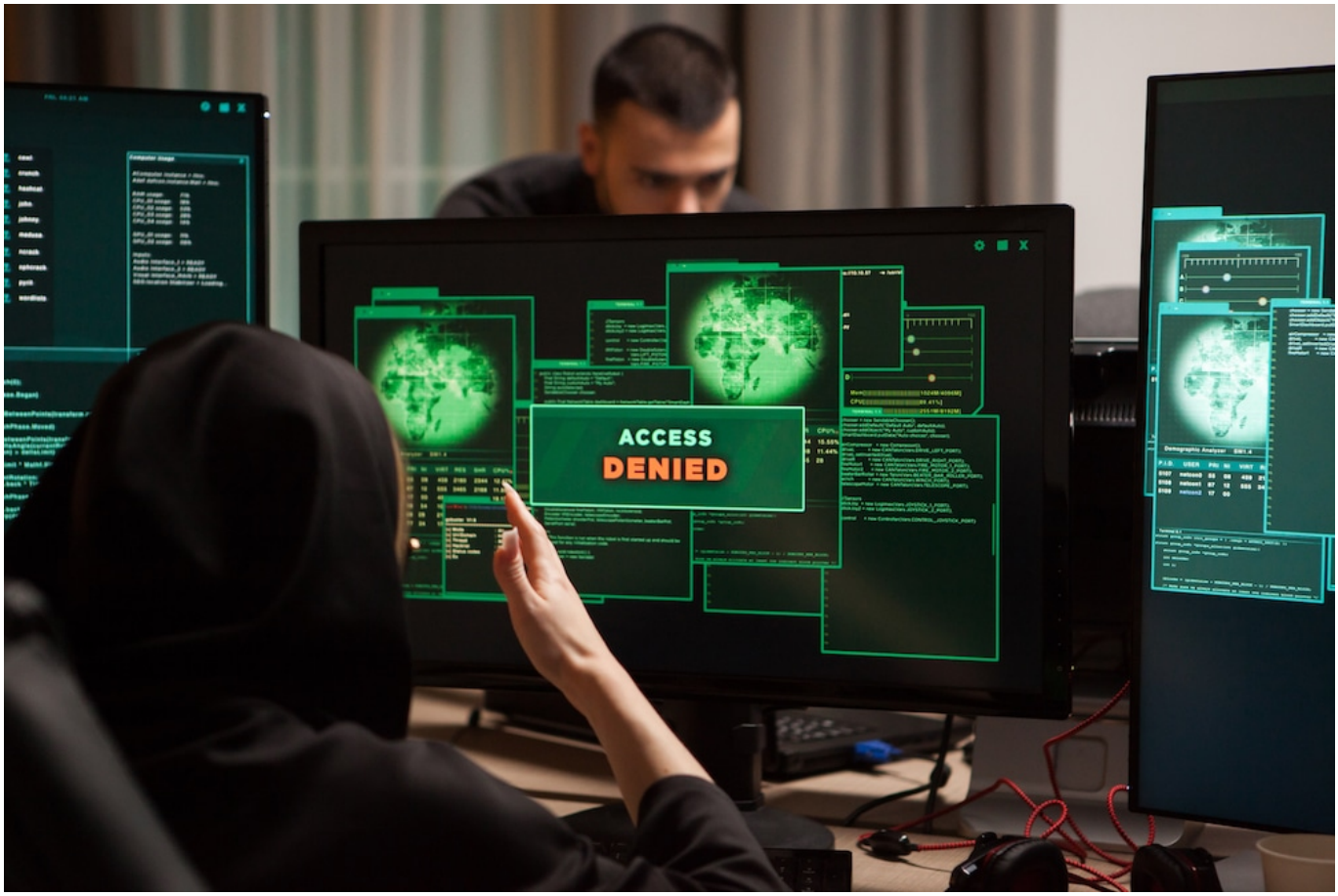
Gezielte DDoS-Angriffe durch russischen Hackverband

Die Webseiten gleich mehrere Webseiten von deutschen Flughäfen waren stundenlang nicht zu erreichen – das kann doch kein Zufall sein.

Ursache waren gezielte Angriffe auf die Webseiten und Onlinepräsenzen einiger großer deutschen Flughäfen. Es handelt sich dabei um sogenannte DDoS-Angriffe. DDoS steht für „Distributed Denial of Service“. Darunter verstehen Experten einen Angriff auf einen Server, bei dem eine große Anzahl von Computern gleichzeitig versuchen, den Zielcomputer oder die Website durch eine Flut von Anfragen zu überlasten.

Das ist so, als ob 10.000 Menschen gleichzeitig im Bundeskanzleramt anrufen. Da geht dann auch kein Anruf mehr durch. Diese Anfragen werden in der Regel von infizierten und miteinander verbundenen Computern ("Botnetz" genannt) durchgeführt.

Die Angriffe werden im Vorfeld vorbereitet, indem Rechner oder Gerte infiziert und dann ferngesteuert zum „Angriff“ genutzt werden. Für die Besitzer der Geräte unbemerkt. Dadurch entsteht eine Überlastung – der Server geht in die Knie. Die Webseite antwortet nicht mehr. Ziel erreicht.



Bei einem DDoS-Angriff werden mit Malware infizierte Rechner eingesetzt

Angreifer wissen genau, was sie tun

Ein DDoS-Angriff legt alles lahm. DDoS-Angriffe werden von Kriminellen oder Regierungen eingesetzt, um Dienste lahmzulegen, Erpressungen durchzuführen oder um ablenkende Taktiken einzusetzen, etwa um Sicherheitslücken auszunutzen. Im aktuellen Fall muss man davon ausgehen, dass russische Kräfte dahinterstecken.

Schon vor Wochen hat das Bundesamt für Sicherheit in der Informationstechnik vor genau solchen Angriffen gewarnt: Als Maßnahme Russlands, die Infrastruktur in Deutschland zu stören oder lahmzulegen – quasi als „Vergeltung“.

Eine russische Hackergruppe namens „Russian Anonymous“ hat sich zu den Angriffen bekannt. Die Wahrscheinlichkeit ist also tatsächlich extrem hoch, dass es russische Kräfte waren. Denn es wurde kein Lösegeld gefordert, was durchaus auch gelegentlich vorkommt. Nach dem Motto: Ihr habt gesehen, was wir können. Zahlt Lösegeld – oder Euer Dienst ist tagelang nicht zu erreichen.

Bagger legt IT der Lufthansa lahm

Nun war das nicht das einzige Problem im Luftverkehr in den vergangenen Tagen. Die Lufthansa musste Dutzende Flüge streichen, der Frankfurter Airport wurde gesperrt – wegen eines Totalausfalls.

Offensichtlich wurde bei Bauarbeiten an einer Bahnstrecke(!) durch einen Bagger ein wichtiges Datenkabel durchtrennt. Ein Glasfaserkabel, das bei Bohrarbeiten einfach durchbohrt wurde. Das hat schon gereicht, um das üppige Rechenzentrum der Lufthansa so stark zu schädigen, dass nichts mehr ging. Eine wichtige Datentrasse der IT der Lufthansa war damit nicht mehr am Netz. Sicher nicht das einzige Datenkabel. Aber ausreichend, um die Rechenzentren der Lufthansa lahmzulegen.

Es braucht dringend mehr Resilienz

Wir brauchen dringend mehr Resilienz

Ich weiß nicht wie es Euch geht: Aber mich macht es nervös, wenn es so einfach passieren kann, dass wichtige Webseiten von Flughäfen oder die Lufthansa komplett in die Knie gezwungen werden kann.

Je wichtiger ein Dienst, ein Server ist, desto mehr muss in den Schutz investiert werden. Wenn eine private Webseite mal ausfällt, ist das nicht tragisch. Aber wie offizielle Webseite eines Flughafens oder sogar die IT-Infrastruktur einer Fluggesellschaft – das ist ein Drama. Der Ausfall kostet verheerende Summen. Diese Ausfälle in einer Woche zeigen deutlich: Deutsche IT-Infrastruktur ist nicht ausreichend geschützt.

Es braucht **Resilienz**: Es darf nicht sein, dass ein ausgefallenes Glasfaserkabel die IT der Lufthansa lahmlegt. Solche Situationen müssen mitgedacht und

eingeplant werden, damit wenigstens ein Notbetrieb aufrechterhalten bleibt. Wichtige Infrastruktur muss auf solche Situationen vorbereitet sein. Es muss auch geübt werden, wie eine Feuerübung. Doch da sind wir in Deutschland – ob in Behörden, Unternehmen oder privat – völlig naiv. Es braucht ein Umdenken. Das kann nur durch Vorschriften und Schulung kommen.

Die besten Add-Ons und Plugins

Add-Ons und Plugins sind praktische Erweiterungen für Browser, Office, Anwendungen oder Apps. Sie erweitern den Funktionsumfang. Hier meine Auswahl der besten Erweiterungen für Euch.

Plugins und Add-Ons sind Erweiterungen von Software, die spezielle Funktionen hinzufügen oder das Verhalten der zugrunde liegenden Anwendung ändern. Sie sind in der Regel von Drittanbietern entwickelt und können kostenlos oder kostenpflichtig sein. Im Folgenden sind einige Gründe aufgeführt, wozu Plugins und Add-Ons gut sind:

1. Erweiterte Funktionalität: Plugins und Add-Ons bieten zusätzliche Funktionen, die nicht in der ursprünglichen Anwendung enthalten sind. Zum Beispiel können Browser-Add-Ons wie Adblocker verwendet werden, um unerwünschte Anzeigen auf Webseiten zu blockieren.
2. Anpassungsmöglichkeiten: Plugins und Add-Ons ermöglichen es den Benutzern, die Anwendung an ihre spezifischen Bedürfnisse anzupassen. Ein Beispiel dafür ist ein Plugin, das die Benutzeroberfläche von Photoshop ändert, um die Bedienung zu vereinfachen.
3. Verbesserte Leistung: Einige Plugins und Add-Ons können die Leistung einer Anwendung verbessern, indem sie bestimmte Aufgaben schneller oder effizienter ausführen. Beispielsweise können Kompressions-Plugins die Dateigröße von Bildern reduzieren, um den Speicherbedarf zu

verringern.

4. Nahtlose Integration: Plugins und Add-Ons können nahtlos in die zugrunde liegende Anwendung integriert werden, um die Benutzererfahrung zu verbessern. Zum Beispiel können Social-Media-Plugins in eine Website integriert werden, um das Teilen von Inhalten auf verschiedenen Plattformen zu erleichtern.

Aktualisierungen: Da Plugins und Add-Ons von Drittanbietern entwickelt werden, können sie aktualisiert werden, um Sicherheitslücken zu schließen oder neue Funktionen hinzuzufügen. Die Verwendung von Plugins und Add-Ons kann daher dazu beitragen, dass die Anwendung auf dem neuesten Stand bleibt und vor Sicherheitsbedrohungen geschützt ist.

Hier mein eBook **Die besten Plugins und Add-Ons** zum Durchstöbern.

Wer das eBook als PDF oder ePub haben will: Als Abonnent von So geht's leichter bekommt Ihr jeden Monat eine neue Ausgabe zugestellt - und habt Zugriff auf Dutzende solcher randvoll mit Tipps und Hacks gefüllten Ratgeber. Eine wahre Fundgrube, kann ich Euch versprechen!

Jetzt Abonnent von So geht's leichter werden!

Blauer Haken bei Instagram und Facebook: Kostenpflichtige Abos

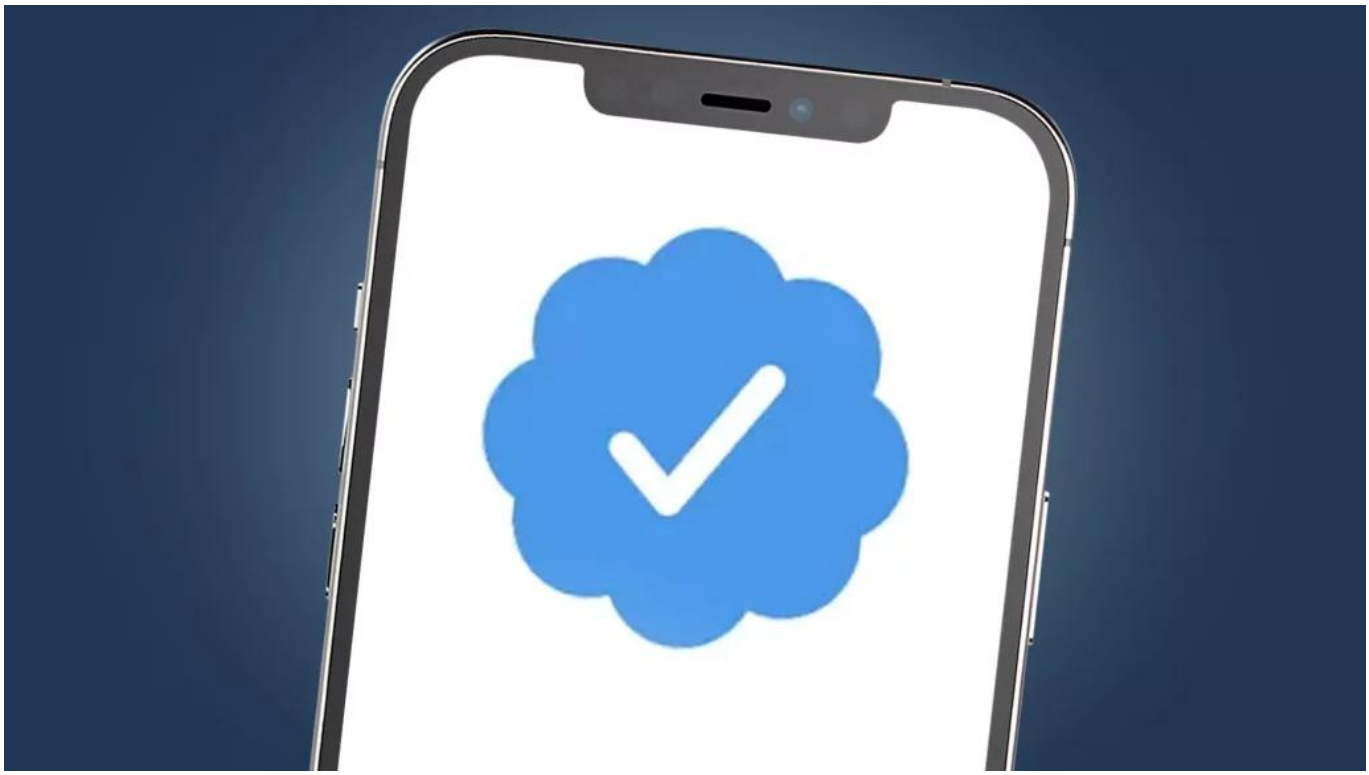
Bislang sind Social Media Dienste konsequent kostenlos. Doch das ändert sich gerade. Twitter hat seinen "Blue Verified"-Dienst bereits eingeführt. Als nächstes bieten auch Facebook und Instagram blaue Haken und Extradienste gegen Bezahlung an.

- Meta-Chef Mark Zuckerberg hat ein kostenpflichtiges Abonnement für Instagram und Facebook namens "Meta Verified" angekündigt
- Meta Verified soll 11,99 US-Dollar für Webnutzer oder 14,99 Dollar auf dem iPhone kosten
- Das Abo-Modell startet in Australien und Neuseeland und soll bald in weiteren Ländern eingeführt werden

Privilegien für Blue-Abonnenten

Twitter hat bereits kostenpflichtige Accounts eingeführt: Gegen entsprechende Bezahlung werden Accounts verifiziert und mit einem blauen Haken ausgerüstet. Darüber hinaus erhalten Blue-Kunden die Möglichkeit, Tweets mehrmals bearbeiten zu können. Tweets werden sichtbarer. Es wird 50% Werbung gestrichen. Und Videos können in Full-HD hochgeladen werden.

Jetzt will auch die Facebook-Mutter Meta ein Bezahlmodell für ihre Plattformen einführen. Meta-Chef Mark Zuckerberg kündigte für Instagram und Facebook ein neues kostenpflichtiges Abonnement namens "Meta Verified" an. Damit können zahlende Nutzer ihre Accounts verifizieren lassen - und bekommen ebenfalls einen blauen Haken.



Twitter hat damit angefangen, blaue Haken gegen Bezahlung anzubieten

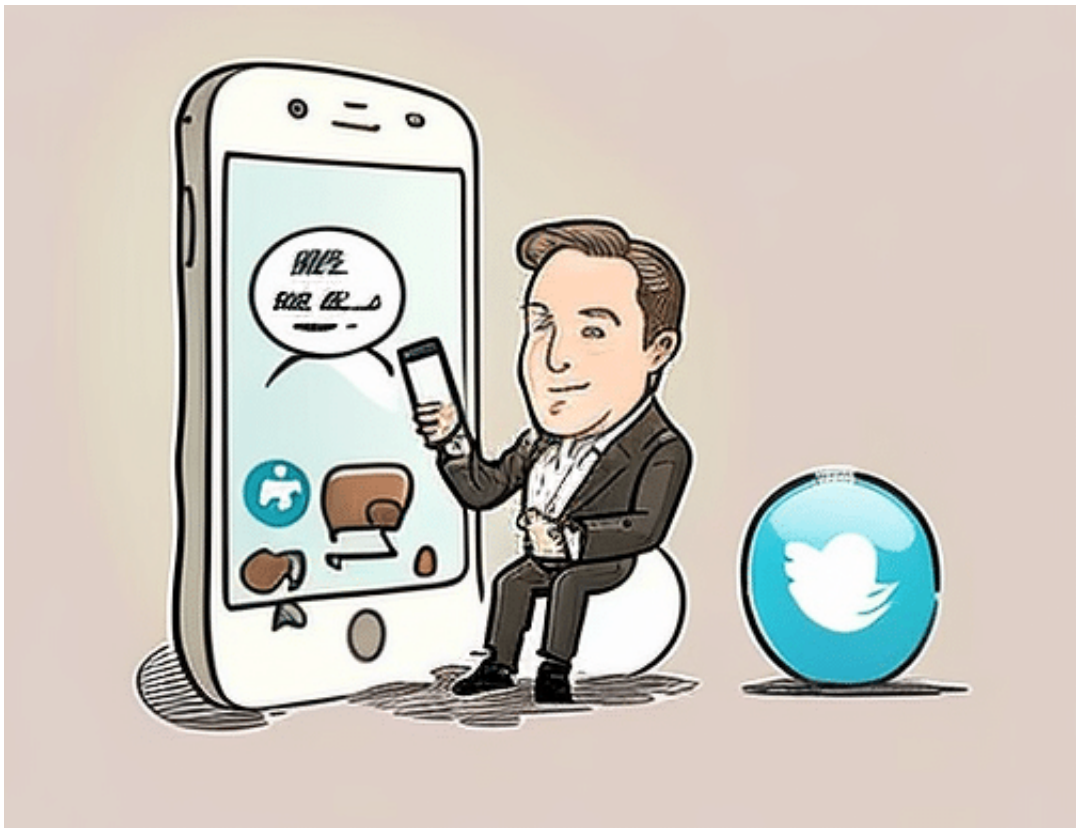
Meta führt verifizierte Konten ein

Neben dem blauen Häkchen gibt es noch zusätzlichen Schutz vor Fake-Profilen (eher für Influencer, Promis und Formen interessant) und direkten Kunden-Support. Dazu wird sogar der Pass des Profilinhabers überprüft.

Wie bei Twitter lockt Meta zahlende Nutzer auch mit mehr Sichtbarkeit auf den Plattformen.

Meta will das neue Abo-Modell in dieser Woche in Australien und Neuseeland sowie „bald in weiteren Ländern“ einführen, schrieb Zuckerberg auf Facebook. Mit der neuen Funktion wolle der Konzern die „Authentizität und Sicherheit“ seiner Dienste erhöhen. Meta Verified soll für Web-Nutzer monatlich 11,99 US-Dollar (umgerechnet 11,21 Euro) und 14,99 Dollar (14 Euro) für das Apple-Betriebssystem iOS kosten.

Twitter schaltet Zwei-Faktor-Authentifizierung per SMS ab



Elon Musk bestätigt: Ab 20. März bekommen nur noch Zahlkunden von Twitter die Möglichkeit, ihre Konten per Zwei-Faktor-Authentifizierung abzusichern. Keine guten Nachrichten für die Sicherheit!

Wer sein Twitter-Konto zusätzlich mit einer SMS als Zwei-Faktor-Authentifizierung absichern will, muss bald dafür bezahlen: Twitter bietet die Absicherung per SMS nur noch seinen Zahlkunden mit blauem Haken an. Alle anderen müssen ihre Konten anders absichern. Am besten schnell, sonst geht der Schutz verloren.

Absicherung der Konten per SMS wird abgeschaltet

SMS als Absicherung bei Twitter wird abgeschaltet

Denn Twitter erlaubt ab 20. März 2023 nur noch zahlenden Nutzern, SMS als Zwei-Faktor-Authentifizierungsmethode (2FA) zur Sicherung der Online-Konten zu benutzen. Danach werden laut Twitter "nur noch Twitter Blue-Abonnenten in der Lage sein, Textnachrichten als ihre Zwei-Faktor-Authentifizierungsmethode zu verwenden".

Die offizielle Begründung überrascht ein wenig - lässt aber sogar ein wenig Verständnis aufkommen: Laut Twitter hätten einige "Telekommunikationsunternehmen Roboterkonten benutzt, um 2FA-SMS zu pumpen". Bedeutet übersetzt: Offensichtlich haben Telekommunikationskonzerne Konten bei Twitter eröffnet und den Versand von SMS erzwungen. Das ergibt Sinn, denn sie erhalten für das Verteilen von SMS einen kleinen Geldbetrag.

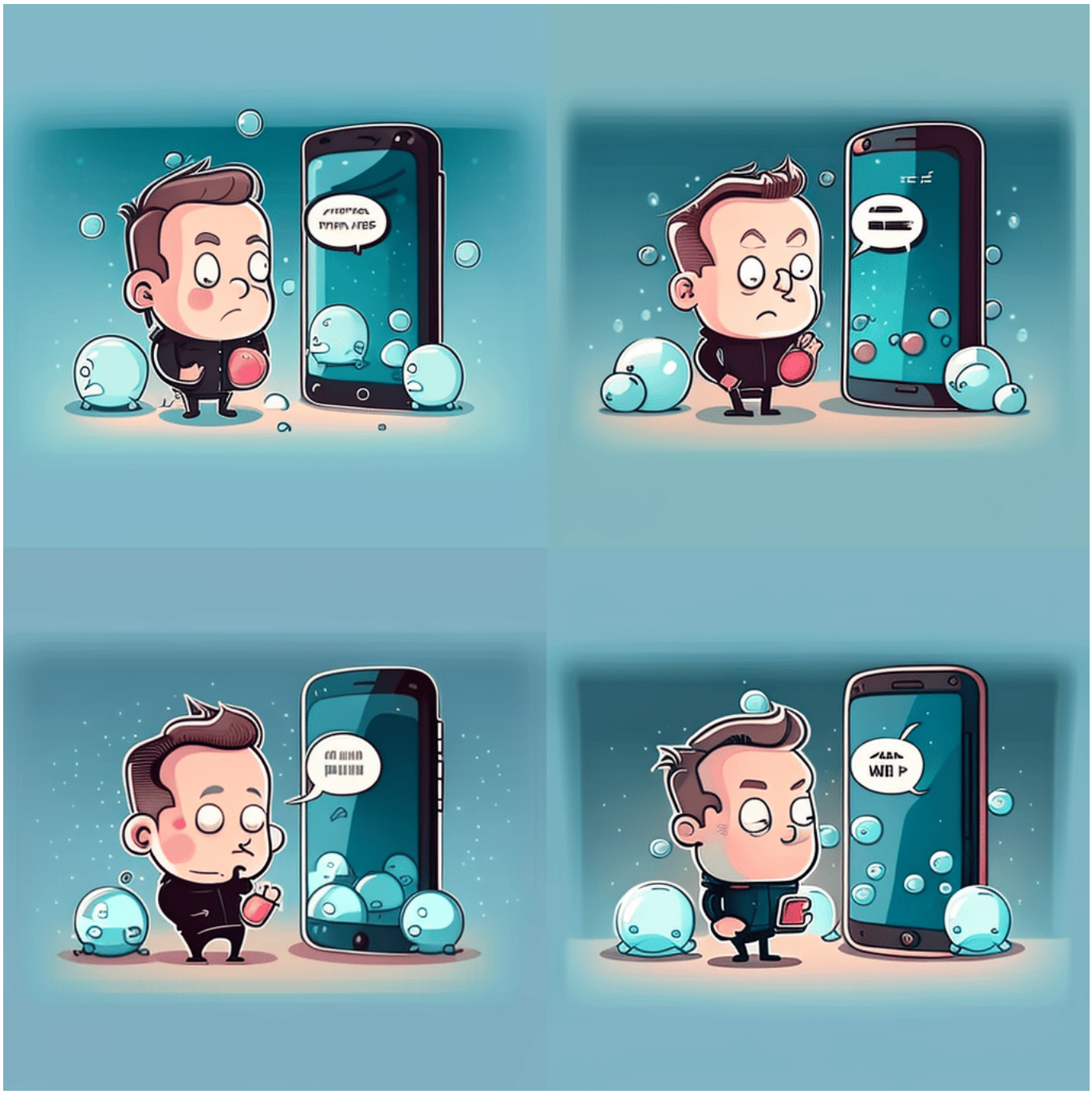
Die jährlichen Kosten "durch betrügerische SMS" sollen sich für Twitter auf 60 Millionen Dollar pro Jahr belaufen. Ein ordentlicher Batzen Geld.

Alternative Absicherungen für 2FA wählen

Doch anstatt diese wichtige Möglichkeit, seine Online-Konten einfach so abzuschalten, sollte Twitter lieber erst mal offensiv für andere Absicherungswege werben, etwa mit Apps wie den "Google Authenticator". Auch wäre es möglich, die Twitter-App selbst zum Absichern zu nutzen (macht Facebook auch so) - oder andere Wege zu entwickeln.

Den Menschen eine wichtige Methode zum Absichern ihrer Konten wegzunehmen, erhöht das Risiko für gekaperte Konten enorm. Viele User werden gar nichts unternehmen und dann entweder ausgesperrt - oder sie lassen ihre Konten ungeschützt. Ein Leckerbissen für Hacker, die dann verstärkt versuchen werden, Twitter-Accounts zu kapern.

Man sollte nicht vergessen: Mit einem gekaperten Twitter-Konto ließe sich nicht nur der dazugehörige Kanal befüllen. Angreifer könnten sich auch überall einloggen, wo das Twitter-Konto als Login benutzt wird (ist bei vielen Online-Diensten möglich).



Twitter-User sollten schnell handeln

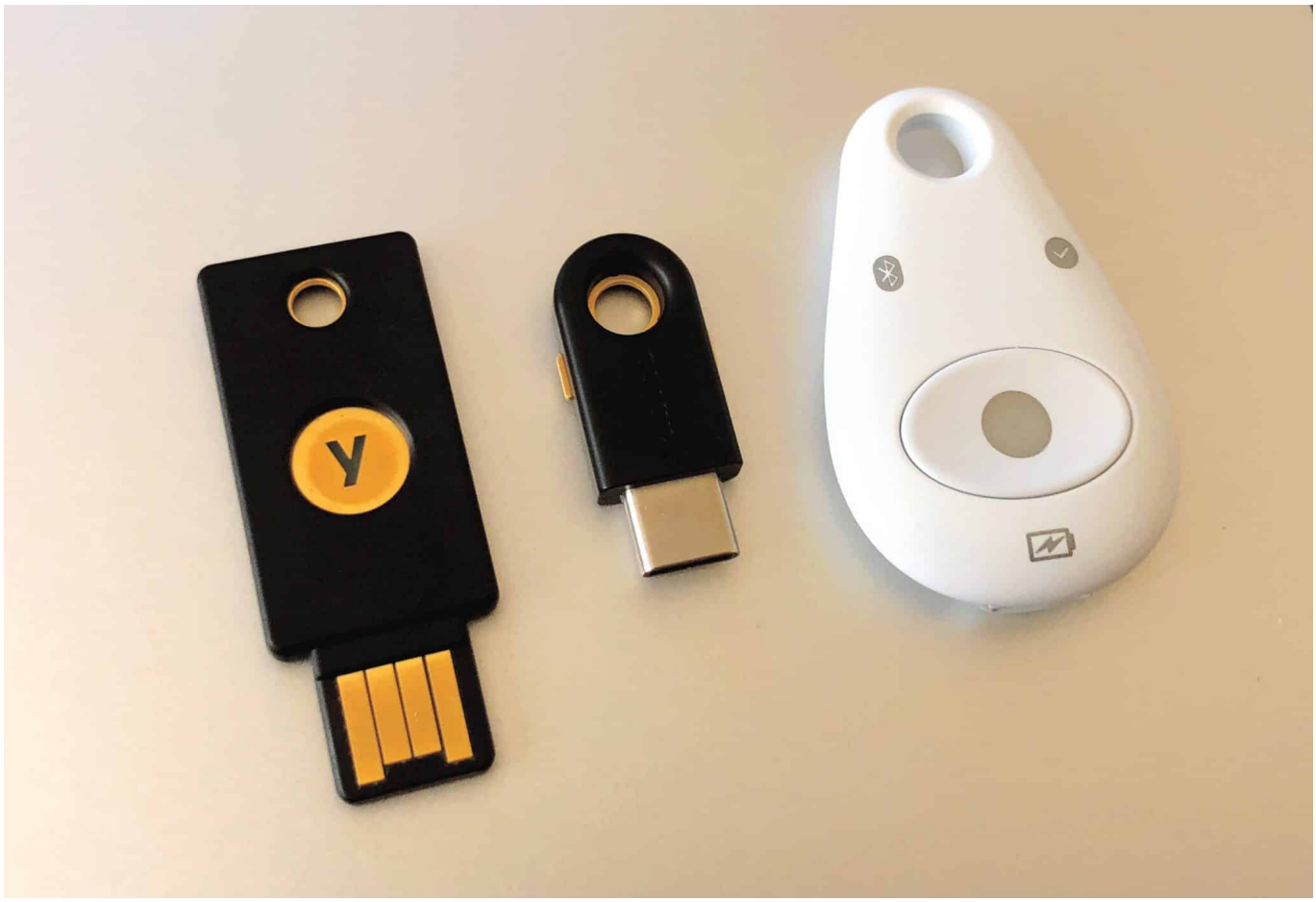
Die Zwei-Faktor-Authentifizierung macht Konten eindeutig sicherer. Kontoinhaber müssen neben Benutzername und Passwort eine zweite Authentifizierungsmethode verwenden. Twitter erlaubt als 2FA die Textnachricht als SMS, aber auch die Verwendung eines Sicherheitsschlüssel (USB-Key) oder -

das empfehle ich als Alternative! - eine bewährte Authentifizierungs-App wie "Google Authenticator", "Duo Mobile" oder "1Password".

Wer kein kostenpflichtiges **Twitter-Blue-Abo** hat, und das dürften die meisten sein, sollte zeitnah handeln. Twitter räumt nur bis Mitte März die Möglichkeit ein, die 2FA-Methode im Konto zu deaktivieren und/oder eine andere Methode zu aktivieren.

"Nach dem 20. März 2023 gestatten wir Nicht-Twitter Blue-Abonnenten nicht mehr, Textnachrichten als 2FA-Methode zu verwenden. Zu diesem Zeitpunkt wird es für Konten mit noch aktivierter SMS-2FA deaktiviert", erklärt das Unternehmen. Es droht also sogar eine Abschaltung des Kontos!

Passkey statt Passwort: FIDO Keys



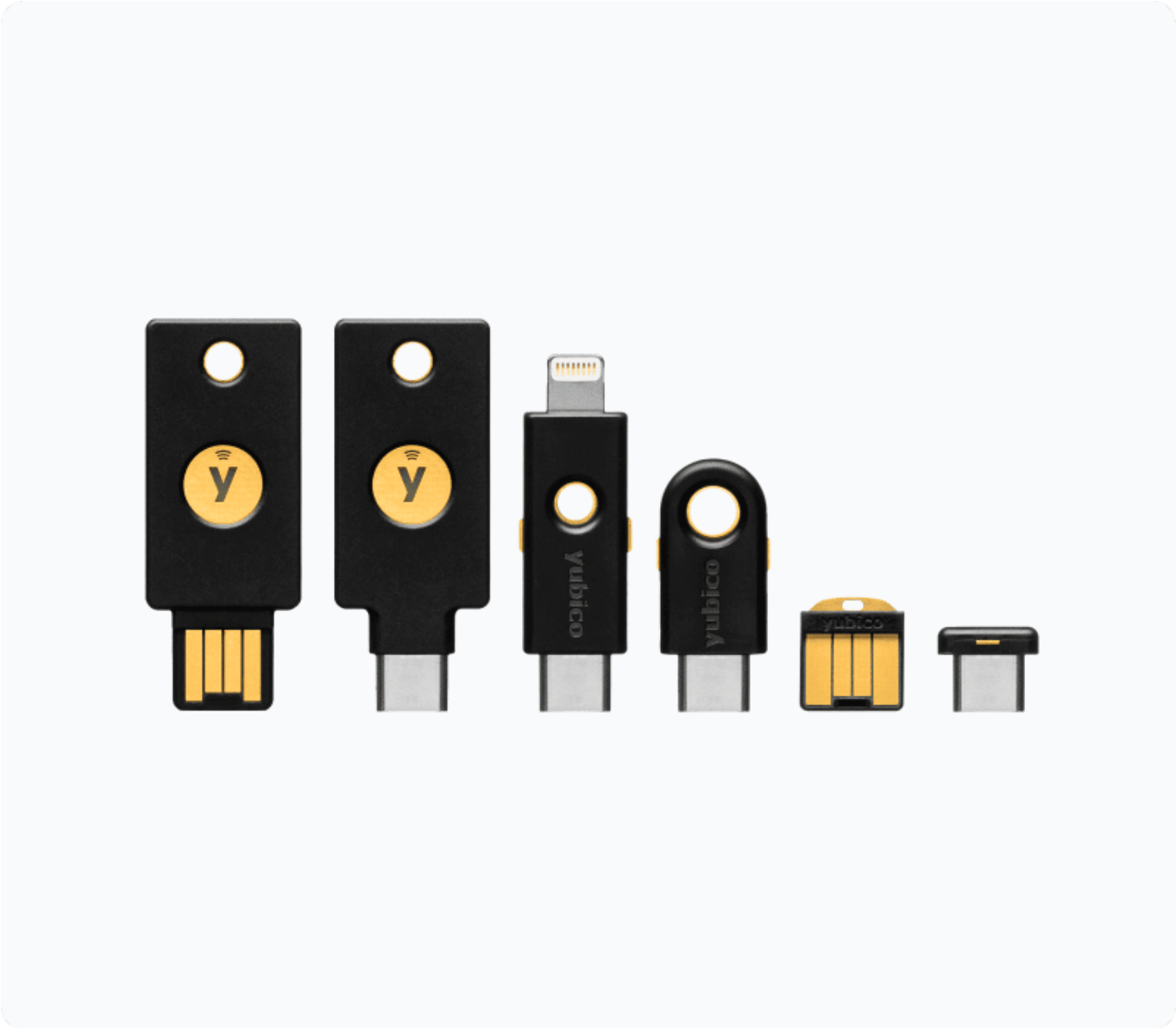
Passwörter haben eigentlich ausgedient: Sie sind unsicher, unpraktisch und leicht zu knacken/klauen. Längst gibt es bessere Methoden, Online-Accounts abzusichern. Vor allem: Passkeys.

Passwörter gehören eigentlich auf den Müll der Geschichte. Längst gibt es bessere Methoden, um sich auszuweisen - etwa mit biometrischen Daten an den Geräten (Gesicht, Fingerabdruck) - und technisch durch den Austausch von Schlüsseln. Ein bewährtes System, das wir auch zum Einloggen verwenden könnten.

Am bequemsten ist es, einen USB-Key zu verwenden. Ein kleines Gadget, das man auf eine USB-Buchse steckt, um anstelle eines Passworts vollkommen automatisch die geheimen Schlüssel zu übertragen.

Das geht auch bei Smartphones. Es gibt auch USB-Keys mit Lightning-Stecker für iPhones. Oder mit NFC, um drahtlos die nötigen Schlüssel ans Mobilgerät zu

übertragen. Eine Methode sich auszuweisen, die viele große Onlinedienste (Google, Microsoft, Amazon etc.) längst wie selbstverständlich anbieten.



Yubikeys: Eine Auswahl an USB-Keys

Fido USB Key

Ein FIDO USB Key ist ein kleines Gerät, das zur Zwei-Faktor-Authentifizierung verwendet wird und die Sicherheit von Online-Konten erhöht. In diesem Blogpost werde ich in sieben Absätzen erklären, wie ein FIDO USB Key funktioniert.

1. Einleitung FIDO steht für Fast Identity Online und ist ein Industriestandard, der von der FIDO-Allianz entwickelt wurde. Die FIDO-Allianz ist eine Non-Profit-

Organisation, die sich dafür einsetzt, die Sicherheit von Online-Identitäten zu erhöhen. Ein FIDO USB Key ist ein Hardware-Token, das die Identität des Benutzers bestätigt und den Zugriff auf ein Online-Konto ermöglicht.

2. Zwei-Faktor-Authentifizierung Die Zwei-Faktor-Authentifizierung (2FA) ist eine Sicherheitsmethode, bei der der Benutzer neben seinem Passwort einen weiteren Faktor zur Identitätsbestätigung eingeben muss. Ein FIDO USB Key ist ein Beispiel für einen zweiten Faktor, der oft als etwas Besitzes bezeichnet wird, da er physisch vorhanden ist.

3. Öffentliche und private Schlüssel Ein FIDO USB Key verwendet eine asymmetrische Verschlüsselung, bei der der Benutzer einen öffentlichen und einen privaten Schlüssel besitzt. Der öffentliche Schlüssel wird an den Online-Service gesendet, während der private Schlüssel auf dem USB Key gespeichert wird.

4. WebAuthn-Protokoll Um die Authentifizierung zu erleichtern, verwendet ein FIDO USB Key das WebAuthn-Protokoll, das von der FIDO-Allianz entwickelt wurde. Das Protokoll ermöglicht es, die Authentifizierung über Webbrowser durchzuführen und ist in den meisten gängigen Browsern integriert.

5. Authentifizierungsprozess Wenn ein Benutzer sich bei einem Online-Service anmeldet, fordert der Service den Benutzer auf, den FIDO USB Key anzuschließen. Der Key sendet dann eine öffentliche Anfrage an den Service, die der Service mit einer Herausforderung beantwortet. Der Key verwendet dann den privaten Schlüssel, um die Herausforderung zu signieren und sendet die Antwort an den Service zurück.

6. Keine Passwortweitergabe Ein FIDO USB Key bietet den Vorteil, dass der Benutzer das Passwort nicht an den Online-Service weitergeben muss. Da der private Schlüssel nur auf dem Key gespeichert ist, kann der Benutzer sicher sein, dass seine Anmeldedaten nicht durch den Service kompromittiert werden.

7. Vorteile von FIDO USB Keys Ein FIDO USB Key bietet eine höhere Sicherheit als herkömmliche Authentifizierungsmethoden, da er ein zusätzliches Element zur Identitätsbestätigung verwendet. Der Key kann auch für mehrere Online-Konten verwendet werden, wodurch der Benutzer eine einfache und sichere Möglichkeit hat, auf verschiedene Konten zuzugreifen. Schließlich ist ein FIDO USB Key einfach zu verwenden und erfordert nur das Anschließen des Geräts, um sich bei

einem Online-Service anzumelden.

In Gefahrensituationen: Stiller Notruf bei iOS

Der Ruf nach Hilfe in einer Bedrohungssituation scheitert oft daran, dass niemand in der Nähe ist. Aus dem Grund bietet iOS den Notruf, der mit Positionsangabe Hilfe alarmiert. Seit iOS 16.3 auch unauffällig.

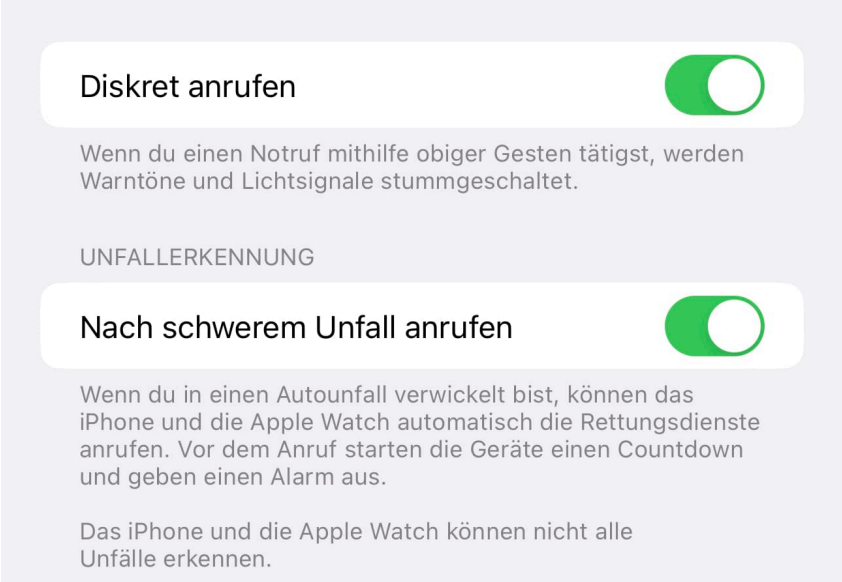
Der normale Notruf bei iOS

Es gibt verschiedene Situationen, in denen Ihr Hilfe holen müsst: Nach einem Verkehrsunfall, wenn Ihr nicht mehr voll beweglich oder konzentriert seid. Da reicht es, wenn Ihr auf dem Handy aktiv die Notruffunktion nutzt, das kann jeder in der Umgegend sehen. Und der Weg bei iOS ist ein wenig hakelig, wenn man ihn nicht kennt.

- Unter **Einstellungen** > **Notruf SOS** könnt Ihr die Konfiguration des Notrufes vornehmen.
- Im Standard ist es so, dass Ihr durch längere Drücken des Einschalters und der Leiser-Taste in das Menü gelangt, in dem Ihr durch Streichen des SOS-Reglers einen Notruf auslösen könnt.
- Dieses Verfahren ist einfach als das manuelle Auslösen eines Notrufs, bedarf aber immer noch manueller Koordination.
- Schaltet **Durch 5-maliges Drücken der Taste anrufen** ein, dann braucht Ihr nur fünfmal hintereinander die Seitentaste drücken, das geht im Zweifel einfacher, als zwei Tasten drücken zu müssen.
- Der so ausgelöste Notruf wird dann von einer Sirene und Lichtsignalen begleitet, was hilfreich ist, wenn Ihr so viel Aufmerksamkeit wie möglich erregen wollt. Das ist aber nicht immer der Fall!

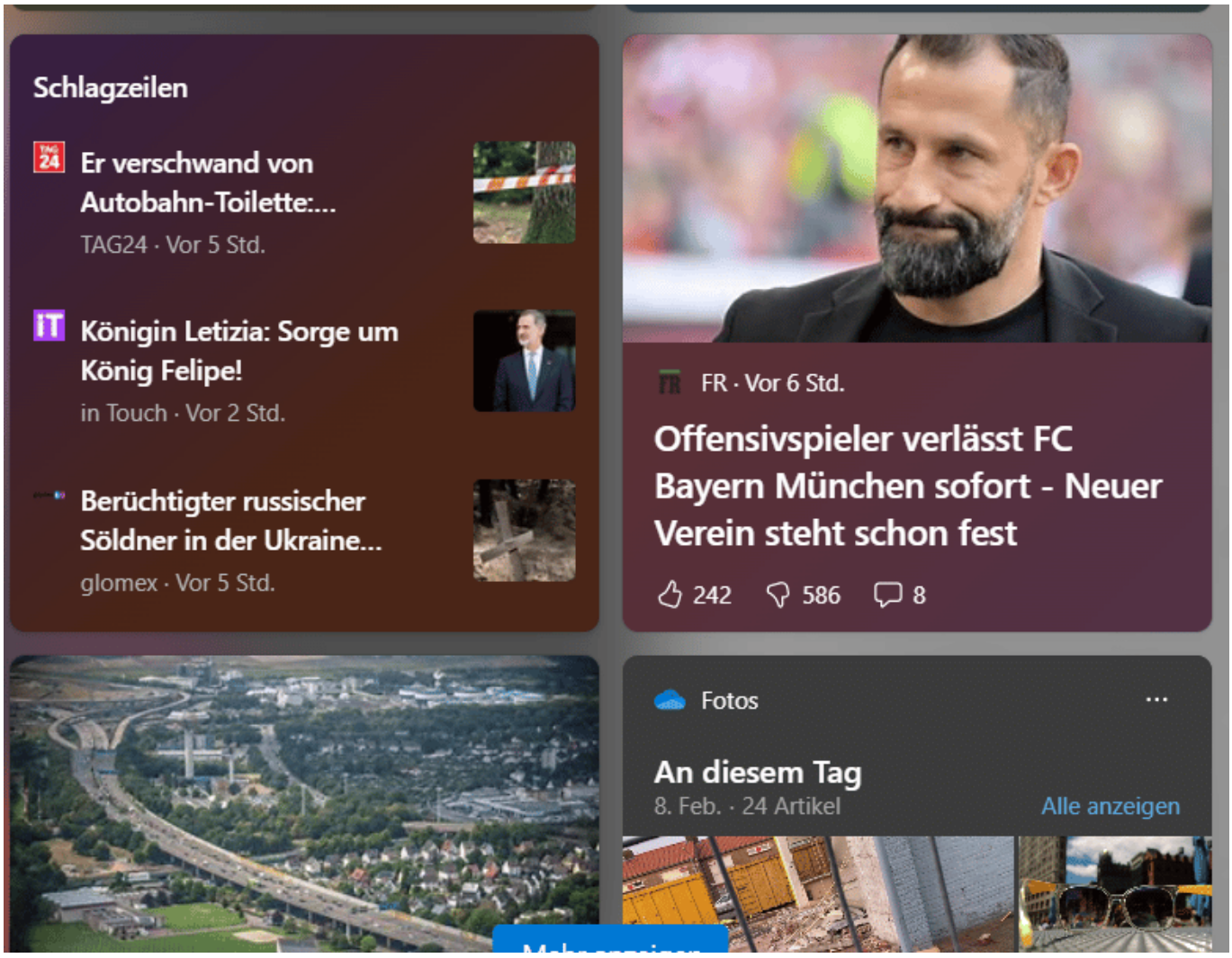
Neu in iOS 16.3: der stumme Notruf

Es gibt Situationen, da wollt Ihr um Hilfe rufen, habt aber Sorge, dass das die Situation noch verschlimmern könnte. Beispielsweise bei einem Überfall, wo der Angreifer nicht auch noch aufmerksam wird. Da sind Töne und Lichtblitze nicht hilfreich. iOS 16.3 hat hier eine neue Funktion integriert, die in einer solchen Situation hilft.



- Unter **Einstellungen** > **Notruf SOS** könnt Ihr die Konfiguration des Notrufes vornehmen.
- Aktiviert den Haken neben Diskret anrufen, dann löst Ihr den Notruf - immer noch in den Methoden oben - so aus, dass er ohne Ton- und Lichtsignale erfolgt, also stumm und unsichtbar.
- Die Alarmierung an sich ist dieselbe, nur die Signalisierung nach außen an Eurem, Telefon eine andere. Ihr müsst also entscheiden, ob Ihr eher bei einem Unfall einen Notruf absetzen müsst oder bei einem Überfall. Abhängig davon solltet Ihr den Schalter setzen.

Windows 11: Widgets richtig verwenden

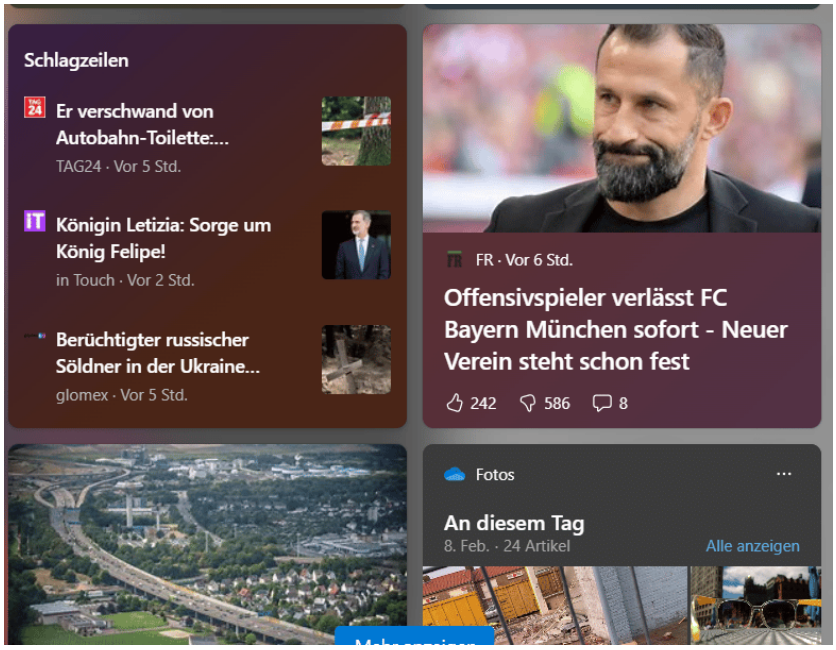


Die Kacheln von Windows sind Geschichte, vielen Anwendern fehlt allerdings deren Informationsgehalt. Dafür hat Windows 11 die Widgets, mit denen Ihr viele Informationen zusammenführen könnt!

Widgets - Was ist das?

Widgets sind keine neue Erfindung. Wenn Ihr ein Smartphone mit Android oder iOS nutzt, dann kennt Ihr die: Kleine Informationsfelder, die aktuelle Informationen aus den einzelnen Programmen enthalten: Wetter, Nachrichten, Warnungen, all das könnt Ihr auf dem Handy auf den Startbildschirmen anzeigen lassen. Die Inhalte aktualisieren sich regelmäßig, entweder beim Vorliegen neuer Inhalte oder in festen Abständen.

- In Windows wäre die Nutzung von Widgets auf dem Desktop eher störend, darum verstecken sich diese im sogenannten Widget Board (im Deutschen eher unschön "Widget-Tafel" genannt).
- Die öffnet Ihr durch Drücken von **Windows** + **W** oder Wischen von links nach rechts über den Bildschirm.



Widgets - Erweitern des Widget Boards

Windows bringt schon im Standard eine Vielzahl an Widgets mit, die auf dem Widget Board angeordnet sind. Damit aber natürlich nicht genug: Ihr könnt weitere hinzufügen und bestehende entfernen bzw. verändern.

- Öffnet das Widget Board durch Drücken von **Windows** + **W** oder Wischen von links nach rechts über den Bildschirm.
- Klickt auf das **Plus-Zeichen** oben rechts, um die Übersicht der verfügbaren Widgets zu öffnen.
- Klickt auf das **Plus-Zeichen** neben der Kategorie, dann wird das Widget eingefügt und bekommt einen Haken in der Übersicht.
- Um ein Widget zu bewegen, greift es mit der Maus und bewegt es an die Zielposition.

Entfernen von Widgets

Nicht alle Widgets sind für Euch wertvoll, und manchmal wollt Ihr sie deshalb loswerden. Da ist Windows nicht immer kooperativ. Nicht alle Widgets sind entfernbar. Besonders die diversen News-Widgets sind im Widget Board fest verankert. Für die meisten anderen habt Ihr zwei Möglichkeiten:

- Um ein Widget zu entfernen, das das anbietet, klickt auf die Stecknadel oben rechts im Widget. Das Widget verschwindet automatisch, die anderen Widgets rücken auf.
- Manche Widgets könnt Ihr nicht komplett entfernen, beispielsweise das Fotos-Widget, dann hilft aber vielleicht das folgende Vorgehen: Klickt auf die drei Punkte oben rechts im Widget, dann auf **Dieses Widget ausblenden**.