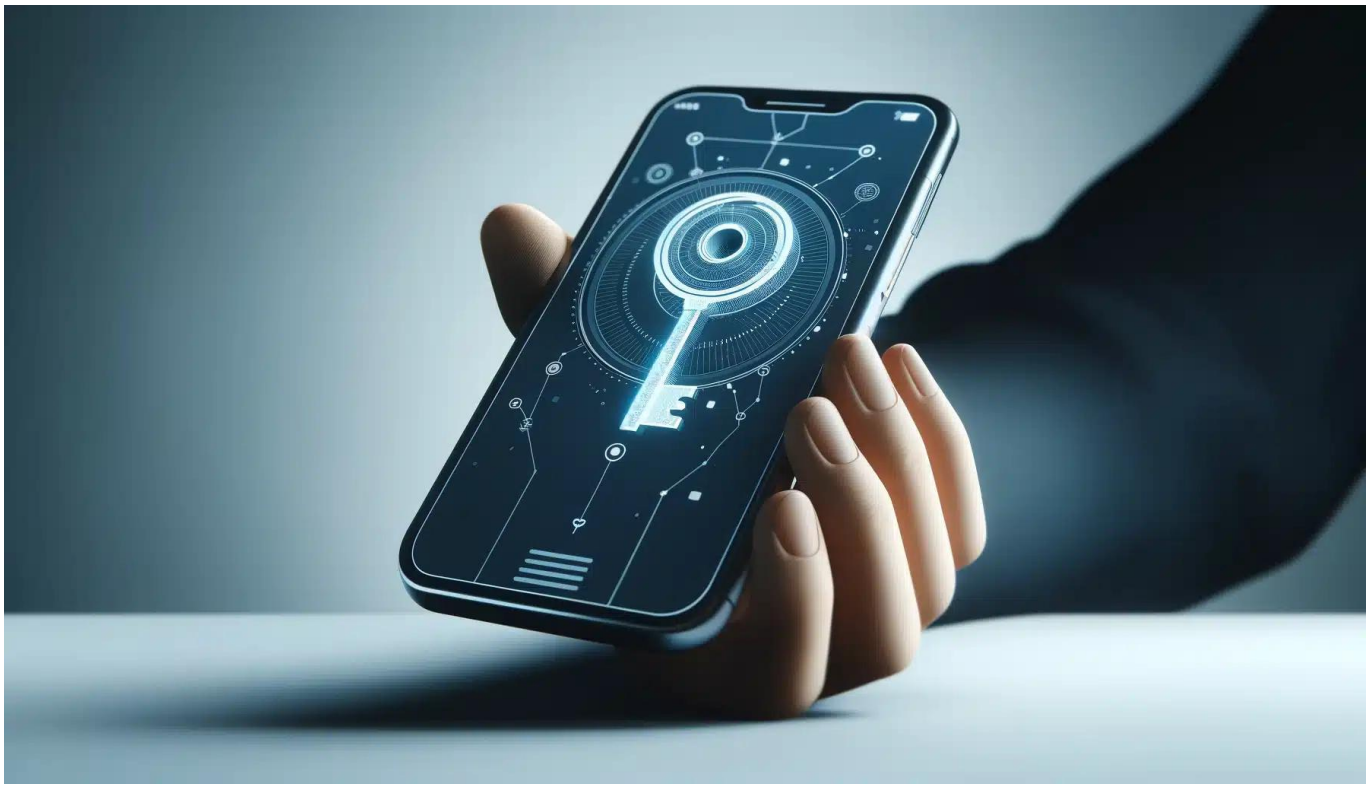
Schieb Report

Ausgabe 2024.26

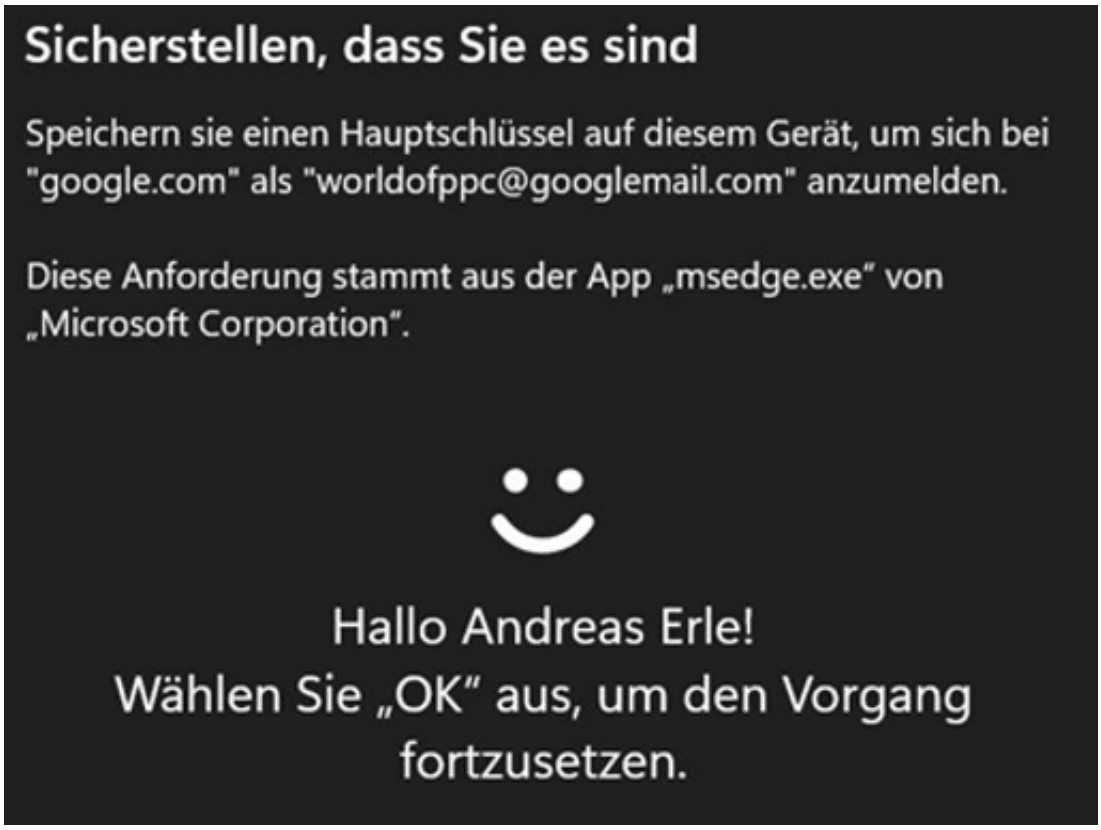
Passkeys bei Google verwenden



Schon 2023 hat sich Google entschieden, für alle seine Dienste und alle Google-Konten weltweit die Verwendung von Passkeys zu aktivieren. Wir zeigen euch, wie ihr diese mit wenig Aufwand erzeugen und nutzen könnt.

Erzeugen von Passkeys bei Google

Zum Anlegen eines Passkeys benötigt ihr nur die Zugangsdaten zu eurem Google-Account und ein Gerät, das die oben beschriebenen Anforderungen für Passkeys erfüllt.



- Öffnet die Passkey-Webseite von Google.

- Solltet ihr bisher nicht mit eurem Google-Konto angemeldet sein, dann holt das auf Aufforderung nach.

- Um einen neuen Passkey anzulegen, klickt auf der Seite unter dem Text auf **+ Passkey erstellen**.

- Ihr könnt jetzt entscheiden, ob ihr den Passkey auf dem aktuellen Gerät erstellen wollt. In dem, Fall klickt auf **Passkey erstellen**.

- Bestätigt, dass ihr einen Passkey erstellen wollt.

- Google nutzt nun die Sicherheitsmechanismen des Geräts, auf dem ihr euch anmeldet: Bei Windows Hello (mit Gesichtserkennung, PIN, Fingerabdruck), bei macOS den Schlüsselbund etc.

- Wenn ihr eine Fehlermeldung bekommt, dass auf dem entsprechenden Gerät kein Passkey erstellt werden kann, dann liegt das meist daran, dass dieses gerade nicht auf die biometrischen Sensoren zugreifen kann. Ein beliebter Fehler: Ihr habt euer Notebook mit Windows Hello-Gesichtserkennung zugeklappt und an einen Monitor angeschlossen. In dem Fall kann die Gesichtserkennung nicht gestartet werden, die ist aber für die Erzeugung des Passkeys nötig!

- Die Lösung: Klappt das Notebook auf und startet den Prozess neu!

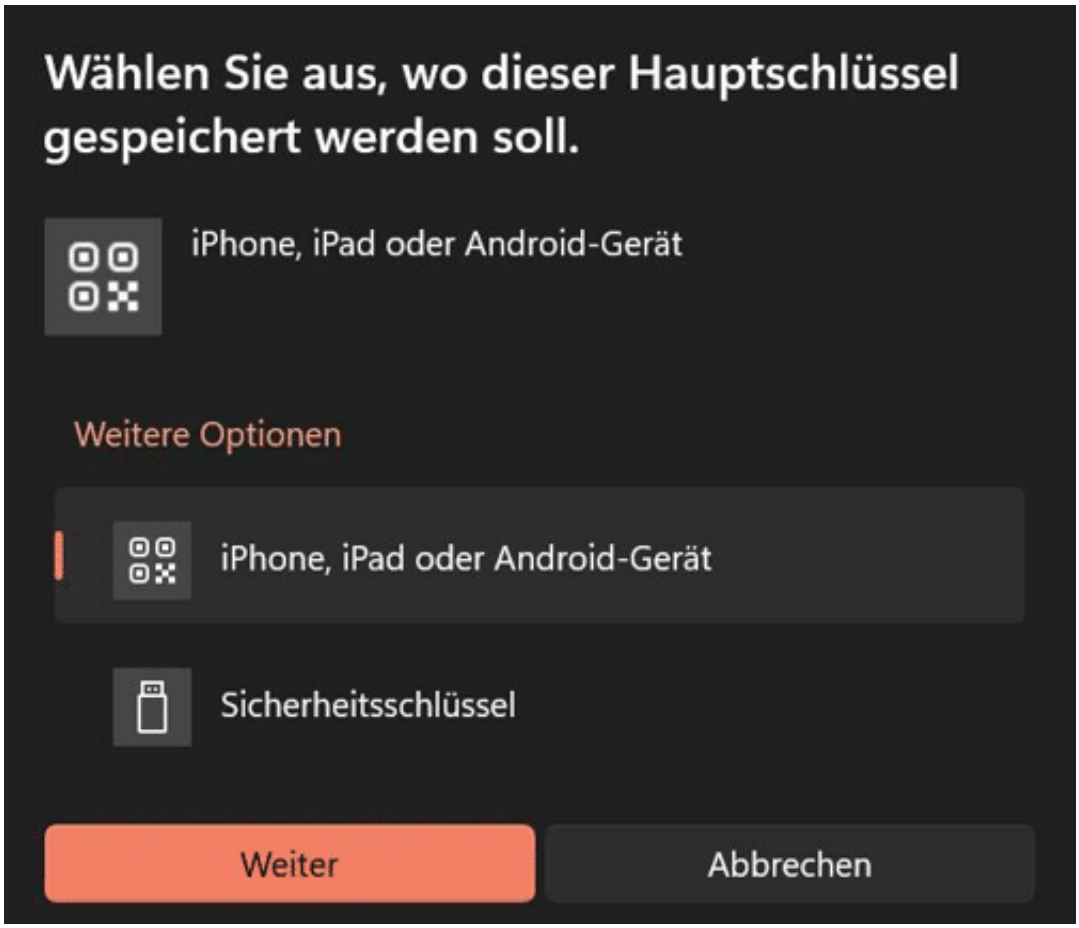
Speichern eines Passkeys auf einem anderen Gerät

Wenn ihr möchtet, dass der Passkey/Hauptschlüssel nicht auf dem Desktop gespeichert wird, sondern auf einem anderen Gerät, dann müsst ihr etwas anders vorgehen:

- Klickt im ersten Menü auf **Anderes Gerät verwenden**.
- Ihr könnt nun auswählen, ob ihr ein Android-, ein iOS-Gerät oder einen Hardware-Sicherheitsschlüssel verwenden wollt. Im Normalfall werdet ihr euer Handy verwenden.
- Klickt auf **Weiter**.
- Google zeigt euch nun einen QR-Code an. Öffnet die Kamera-App auf dem Handy und richtet die Kamera auf den QR-Code.
- Dieser wird von allen gängigen mobilen Betriebssystemen erkannt und gelb eingerahmt. Darunter seht ihr einen gelben Text „Einen Passkey sichern“. Tippt darauf.
- Je nach der Konfiguration eures Smartphones fragt Google euch jetzt, wo ihr den Schlüssel speichern wollt. Normalerweise ist das der Standard-Passwortspeicher des Geräts, bei iOS also der Schlüsselbund. Wenn ihr

aber den Microsoft Authenticator installiert habt, dann könnt ihr auch festlegen, dass dieser stattdessen verwendet wird.

- Ihr müsst euch dann am Gerät einmal authentifizieren (indem ihr den Fingerabdruck auflegt oder das Gesicht scannen lasst), dann wird der Passkey im Google-Konto gespeichert.



Tritt dabei ein Fehler auf, dass der Schlüssel nicht gespeichert werden kann, dann liegt das meist daran, dass ihr nicht mehrere Schlüssel für ein Gerät anlegen könnt:

- Wenn ihr erst den Passkey direkt auf dem PC anlegt, dann wird dieser dort gespeichert.

- Wenn ihr dann auf demselben PC einen Passkey anlegt und dafür das iPhone nutzt, dann ist das ja immer noch dasselbe Konto und dasselbe Gerät, das ihr mit einem Passkey schützt.

- In einem solchen Fall löscht den Passkey, den ihr auf dem PC angelegt habt und erstellt ihn dann neu auf dem Smartphone, wie oben beschrieben.

Wie funktionieren Passkeys?

Im Kern handelt es sich bei Passkeys um digitale Schlüssel, die das herkömmliche Passwort ersetzen sollen. Statt sich einen kryptischen Mix aus Buchstaben, Zahlen und Sonderzeichen merken zu müssen, übernimmt das Smartphone oder der Computer die sichere Anmeldung. Aber wie?

Des Rätsels Lösung als Sicherheitsfaktor

Das Prinzip: Für jede Website, bei der man sich registriert, wird ein eigenes Schlüsselpaar erzeugt. Der öffentliche Schlüssel liegt auf den Servern des Anbieters, während der private Schlüssel das Gerät nicht verlässt. Beim Login gleichen sich die beiden Hälften ab und gewähren nur bei Übereinstimmung den Zugang zum Konto – einfach per Fingerabdruck, Gesichtsscan oder PIN-Eingabe.

Ein wichtiger Aspekt bei der Funktionsweise von Passkeys ist die Ende-zu-Ende-Verschlüsselung. Die privaten Schlüssel verlassen nie das eigene Gerät und werden auch nicht an die Server des Anbieters übertragen. Selbst wenn diese gehackt werden, sind die Anmeldedaten nicht kompromittiert:

- Wenn ihr euch auf einer Webseite per Passkey anmeldet, dann müsst ihr euch mit dem Gerät erst einmal für die Nutzung des Passkeys registrieren.

- Die Webseite erzeugt ein neues Schlüsselpaar, das aus einem öffentlichen und einem privaten, geheimen Schlüssel besteht. Das Verfahren kennt ihr vielleicht aus der Verschlüsselung bzw. Signierung von E-Mails.

- Der private Schlüssel bleibt sicher bei euch, der öffentliche Schlüssel wird auf der Webseite hinterlegt.

- Für jede Webseite wird für jeden Benutzer ein eigenes Schlüsselpaar erzeigt, jeder Passkey ist also einzigartig und damit so gut wie nicht zu fälschen.

Wenn ihr euch nach der initialen Anmeldung an der Webseite mit eurem Passkey anmeldet, dann funktioniert es wie bei einem Ratespiel:

- Die Webseite schickt eine zu lösende Aufgabe an das Gerät, das sich anmelden soll.

- Das Gerät löst diese Aufgabe und nutzt dafür den geheimen Schlüssel, der ja auf ihm selbst gespeichert ist. Die so erzeugte Antwort schickt es wieder zurück.

- Die Webseite wiederum kann über den bei ihr vorliegenden öffentlichen Schlüssel diese Antwort entschlüsseln und überprüfen, ohne den privaten

Schlüssel zu kennen.

- Ist die Antwort korrekt, dann hat sich euer Gerät erfolgreich „ausgewiesen“ und die Webseite gewährt ihm (und damit euch) Zugriff.

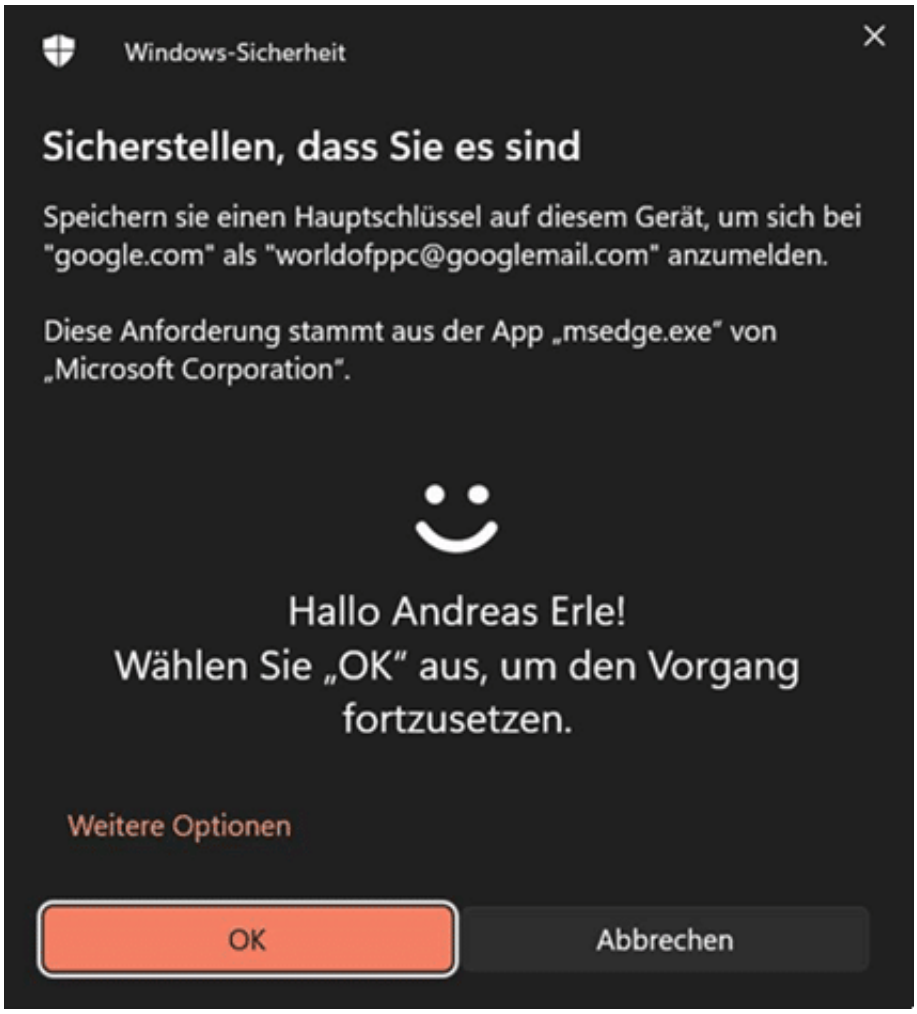
Kein Verzicht auf den zweiten Faktor

Was auf den ersten Blick wie eine runde Lösung klingt, die alle anderen Sicherungsmechanismen überflüssig macht, hat natürlich auch einen kleinen Haken, der sich aber über bekannte Maßnahmen beseitigen lässt:

Schon bei den Passwörtern war das Prinzip von Wissen und Besitz ein zusätzlicher Sicherheitsfaktor:

- Das Passwort müsst ihr kennen, um es eingeben zu können („Wissen“). Das können aber natürlich auch Unbefugte erfahren, dies es dann auch wissen.

- Um das zu umgehen, wird als zweiter Faktor oft das Smartphone verwendet, dem zusätzlich nach Eingabe des Passworts eine SMS mit einem zufälligen Zahlencode geschickt wird. Euer Smartphone hat ein Angreifer natürlich nicht („Besitz“).



Passkeys konzentrieren sich vor allem auf den Besitz, denn der private Schlüssel ist ja auch eurem Gerät gespeichert. Kommt das abhanden, dann könnte sich der neue Besitzer damit an den per Passkey gesicherten Webseiten anmelden. Aus diesem Grund verlangt die Anmeldung per Passkey ebenfalls einen zweiten Faktor und nutzt dabei die Mechanismen, die auf dem Smartphone sowieso genutzt werden: Die PIN oder Biometrie wie Gesichtserkennung oder der Fingerabdruck. Ihr müsst eine dieser Sicherheitsmethoden aktiviert haben und nutzen, wenn ihr euch per Passkey anmeldet.

Eigene Vorlagen mit Google Docs erstellen

Die verbreiteten Textverarbeitungen unterstützen das Erstellen eigener Vorlagen zur Wiederverwendung häufig genutzter Dokumente an. Google hat diese für Docs gestrichen. Keine Sorge: Wir haben die Lösung!

Wie ihr vorgefertigte Vorlagen verwendet, habt ihr ja bereits hier gelesen. Ihr könnt aber auch eigene anlegen. Das bietet sich für Dokumente an, die ihr immer wieder in derselben Struktur, aber mit anderen Inhalten verwendet, beispielsweise Protokolle, Einladungen, Handbücher und andere Dokumente.

Erstellen eigener Vorlagen

Der Weg ist ein wenig komplizierter als bei Microsoft Office und anderen Office-Programmen. Das Speichern in einem eigenen Vorlagenformat ist für die Webversion von Google Docs nicht möglich.

- Stattdessen sucht euch das Dokument, dessen Struktur ihr wiederverwenden wollt, aus der Startseite von Google Docs oder auf eurem Google Drive heraus.

- Klickt auf die drei Punkte neben der Datei, dann auf **Kopie erstellen**.

- Öffnet nun diese kopierte Datei und entfernt alle Elemente, die ihr nicht bei jedem Verwenden braucht, unter anderem Adressen oder persönliche Daten.

- Benennt die Datei dann um als „Vorlage_“, zum Beispiel Vorlage_Protokoll.

- Jetzt solltet ihr noch die Datei davor schützen, verändert zu werden. Klickt dazu in Google Drive auf die drei Punkte neben der Datei, dann auf **Dateiinformationen** > **Sperren**. Selbst wenn ihr sie öffnet und versehentlich hineinschreibt, verändert ihr sie nicht, Google Docs meldet stattdessen „Dokument gesperrt“.

- Aus dieser Vorlage könnt ihr immer wieder eine Kopie anlegen und diese

bearbeiten, die Kopie ist dann nicht gesperrt!

Ich weiss, wo Du Deine Fotos gemacht hast: Metadaten und KI veraten eine Menge

Wer Fotos macht, hinterlässt Spuren – zum Beispiel in den Metadaten. Die lassen Rückschlüsse auf den Ort der Aufnahme zu. Aber auch KI kann den herausfinden.

Fotos in Sozialen Netzwerken

Wir alle machen heute unzählige Fotos. Andauernd. Schließlich haben wir unsere Kamera immer mit dabei. Mit dem Smartphone. Oft genug verteilen wir viele der Fotos dann gleich, vor allem auf Social Media, vielleicht aber auch über Messenger wie WhatsApp oder Signal.

Schnell verliert man die Kontrolle darüber, wo die Fotos landen – und wer sie

sehen kann. Dabei sollten wir unsere Fotos vielleicht nicht so freizügig verteilen. Denn die meisten Fotos enthalten Daten, die Rückschlüsse erlauben, wo ein Foto entstanden ist.

Und wer jetzt abwinkt und meint: Kenne ich doch… Moment. Mittlerweile gibt es sogar eine KI, die nur durch Analyse des Fotos, vor allem des Hintergrunds sagen kann, wo es aufgenommen wurde. Klingt spooky genug?

Metadaten sind zahlreiche Daten und Informationen, die unsichtbar im Foto gespeichert werden

Fast jedes Foto hat Metadaten

Man sieht diese Angaben normalerweise auch nicht. Wir sprechen hier über

sogenannte Metadaten, die in der Bilddatei enthalten sind, aber nicht im sichtbaren Bereich. Wer sich Metadaten eines Fotos anschauen will, muss etwas Aufwand betreiben.

Doch in allen Betriebssystemen – ob Windows, MacOS, iOS oder Android – ist es möglich, sich die Metadaten anzuschauen. In der Regel muss man das Foto auswählen und dann eine Funktion „Info“ oder „Eigenschaften“ aufrufen, dann erscheinen die Metadaten – auch die sogenannten „Exif“-Daten.

Da steht unter anderen auch, wo die Aufnahme entstanden ist – mit Längen- und Breitengrad. Auch eine Menge weiterer Infos, etwa, mit welcher Kamera oder mit welchem Smartphone ich fotografiert habe. Sogar, welche Blende die Kamera verwendet hat und ob der Blitz ausgelöst wurde.

Wer Fotos teilt, teilt oft auch den Standort

Und wenn ich meine Fotos teile, dann gebe ich all diese Informationen auch weiter?

Prinzipiell schon – aber nicht immer. Wenn du die Fotos mit einem Messenger verschickst, passiert es häufig, dass die Empfänger der Fotos die Metadaten nicht mehr erhalten, der Anbieter der App allerdings schon. So ist es zum Beispiel bei WhatsApp und Facebook Messenger. Signal hingegen entfernt die Metadaten noch vor dem Absenden. Es kommt also drauf an.

Wer ein Foto per E-Mail verschickt oder in die Cloud hochlädt und dann den Link teilt, der teilt auch die Metadaten. Wer hingegen seine Fotos bei Facebook oder Instagram hochlädt, kann sicher sein: Alle, die sich die Fotos anschauen, können den Aufnahmeort nicht sehen, da Facebook und Instagram die Daten vorher entfernen.

Der Meta-Konzern bekommt sie aber schon. Der sammelt alle Daten, auch die Standortdaten der Fotos und weiß also so, wo man sich aufgehalten hat und wo man Fotos macht.

Prinzipiell ist es auch bei Videos möglich; aber viele Apps oder Kameras speichern diese Daten nur, wenn man es ausdrücklich will.

Klare Vorteile von Meta- und Geodaten

Jeder kann die Metadaten aber auch für eigene Zwecke nutzen.

Die Metadaten bieten viele Vorteile. Wer mit hochwertigen Kameras fotografiert und seine Fotos später bearbeiten will, sieht sogar, mit welcher Blende, welchem Objektiv, welcher Belichtungszeit fotografiert wurde – das kann ungeheuer hilfreich sein.

Aber auch wer nur mit dem Smartphone fotografiert, kann Vorteile haben. iPhones und Android-Handys und auch die Cloud-Dienste für Fotos bieten die Möglichkeit, ganz gezielt Fotos herauszusuchen, die an einem bestimmten Ort aufgenommen wurden.

Gib einfach mal „Mallorca“ oder „Bordeaux“ ein in der Foto-Suche – Du wirst dann schon sehen, was ich meine. Die App zeigt dir nur die Fotos, die vor Ort gemacht wurden – oder zeigt in einer Landkarte an, wo welche Fotos entstanden sind. Das ist sehr praktisch.

Aber auch Polizei oder Strafverfolgungsbehörden können diese Geodaten in Fotos im Einzelfall nutzen, etwa wenn sie herausfinden wollen oder müssen, wo ein Foto entstanden ist. In solchen Fällen ist es natürlich hilfreich, wenn die Metadaten noch da sind.

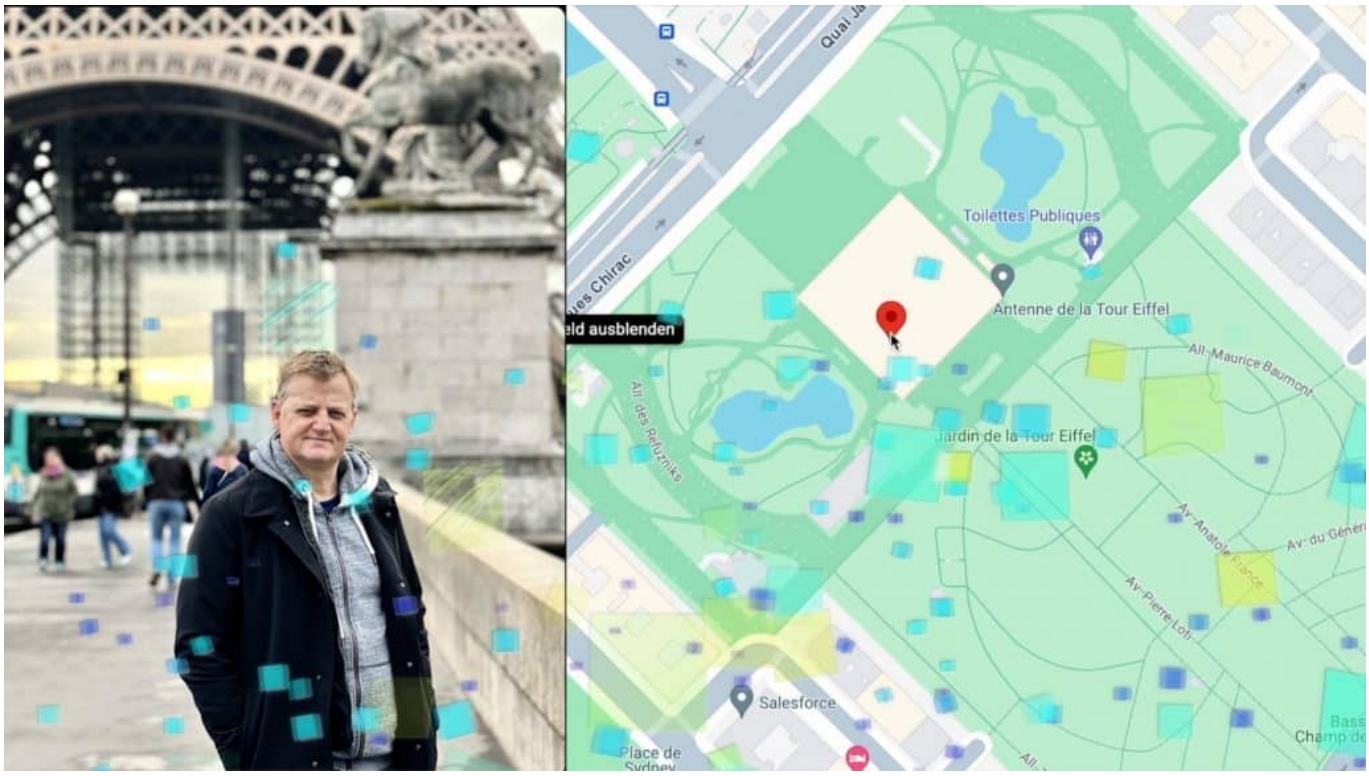
Wenn Metadaten geteilt werden

Kommen wir auf die Nachteile zu sprechen: Was bedeutet es, wenn ich diese Metadaten teile?

Mark Zuckerberg bedankt sich: Je mehr Daten, desto besser. Das gilt ganz besonders für Metadaten. Aber nicht nur der Meta-Konzern, jeder, der viele Fotos von dir in die Hände bekommt, kann Bewegungsprofile anfertigen. Weiss, wann du Tennis spielst und wo, an welchen Orten du bevorzugt Urlaub machst und wo deine Freunde wohnen.

Standortdaten sind vielleicht die sensibelsten Informationen, die man teilen kann. Weil man gewiss nicht möchte, dass Fremde wissen, wo man sich aufhält – außer vielleicht, wenn man gerade in Paris ist und den Eiffelturm postet. Da ist es offensichtlich, dass man möchte, dass jeder weiß, wo man gerade ist.

Aber wer ein Refugium hat, von dem niemand erfahren soll, der ist gut beraten, dort keine Fotos zu machen und die zu teilen.



KI kann heute ziemlich genau den Ort einer Aufnahme ermitteln – auch ohne Metadaten

Metadaten los werden

Wenn ich also nicht möchte, dass andere meine Standortdaten teilen, muss ich diese Metadaten loswerden.

Sagen wir mal so: Facebook, Whatsapp und Instagram sind so freundlich, die Metadaten abzuschneiden, bevor sie an Dritte weitergegeben werden. Doch Meta sammelt die Daten, wie bereits erwähnt.

Wer die Metadaten entfernen möchte, kann das bei jedem Foto manuell machen – oder Tools benutzen, die das schneller erledigen und bei vielen Fotos gleichzeitig.

Solche Tools nennen sich ExifTool oder Gimp auf dem Desktop, oder Metapho (iOS) oder Photo Exif Editor (Android) – oder man geht auf eine Webseite wie EXIF.tools.

Es macht also Mühe. Aber wenn man Fotos von seinem Refugium publizieren möchte oder einfach nicht möchte, dass andere wissen wo man ist, gilt: Entweder gar keine Fotos veröffentlichen oder sich vorher die Mühe machen, die Metadaten zu entfernen.

Geospy: Eine KI erkennt den Aufnahmeort

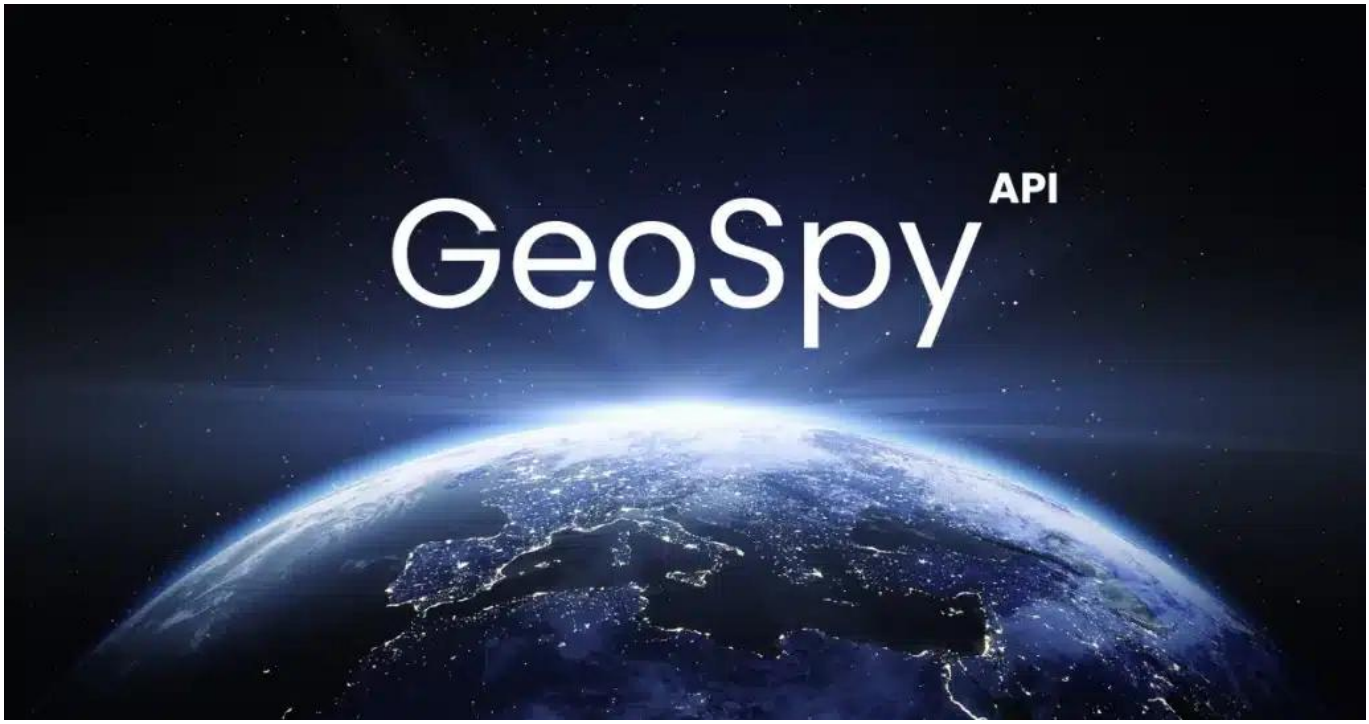
Es gibt jetzt aber auch KIs, auch ohne Metadaten rausfinden, wo ein Foto aufgenommen wurde. Klingt irgendwie spooky.

Die KI nennt sich Geospy AI und wurde von einem kleinen Team von drei Brüdern in den USA entwickelt. Ich habe mit den Gründern gesprochen, um die genaue Funktionsweise und auch die Motivation zu verstehen.

Die Handhabung ist wirklich einfach: Webseite aufrufen – die ist für jeden frei zugänglich –, ein Foto hochladen. Fertig, das Ergebnis steht auf dem Bildschirm, Zum Beispiel ein Foto vom letzten Trip, ein Straßenzug mit schicken Häusern. Man ahnt, das könnte England sein. Doch die KI zeigt tatsächlich die genaue Position in London.

Jeder kann Geospy benutzen, im Web. Es kostet nicht mal was.

Einzige Bedingung: Die Fotos müssen draußen aufgenommen worden sein. Man muss etwas von der Landschaft und der Stadt sehen.



Geospy: Eine KI, die Fotos auf Hinweise untersucht

Noch keine perfekte Genauigkeit

Die Genauigkeit ist im Augenblick noch sehr durchwachsen. Manchmal klappt das erstaunlich gut, manchmal liegt sie aber auch total daneben. Ein Foto aus London oder Paris funktioniert super, vor allem wenn Häuser oder markante Punkte zu sehen sind, und sei es nur angedeutet. Auf dem Land funktioniert es noch nicht so gut.

Die Betreiber sagen aber auch: Die KI steht ganz am Anfang. Sie befindet sich noch im Testbetrieb, Betastadium, und muss noch lernen. So ist das bei jeder KI.

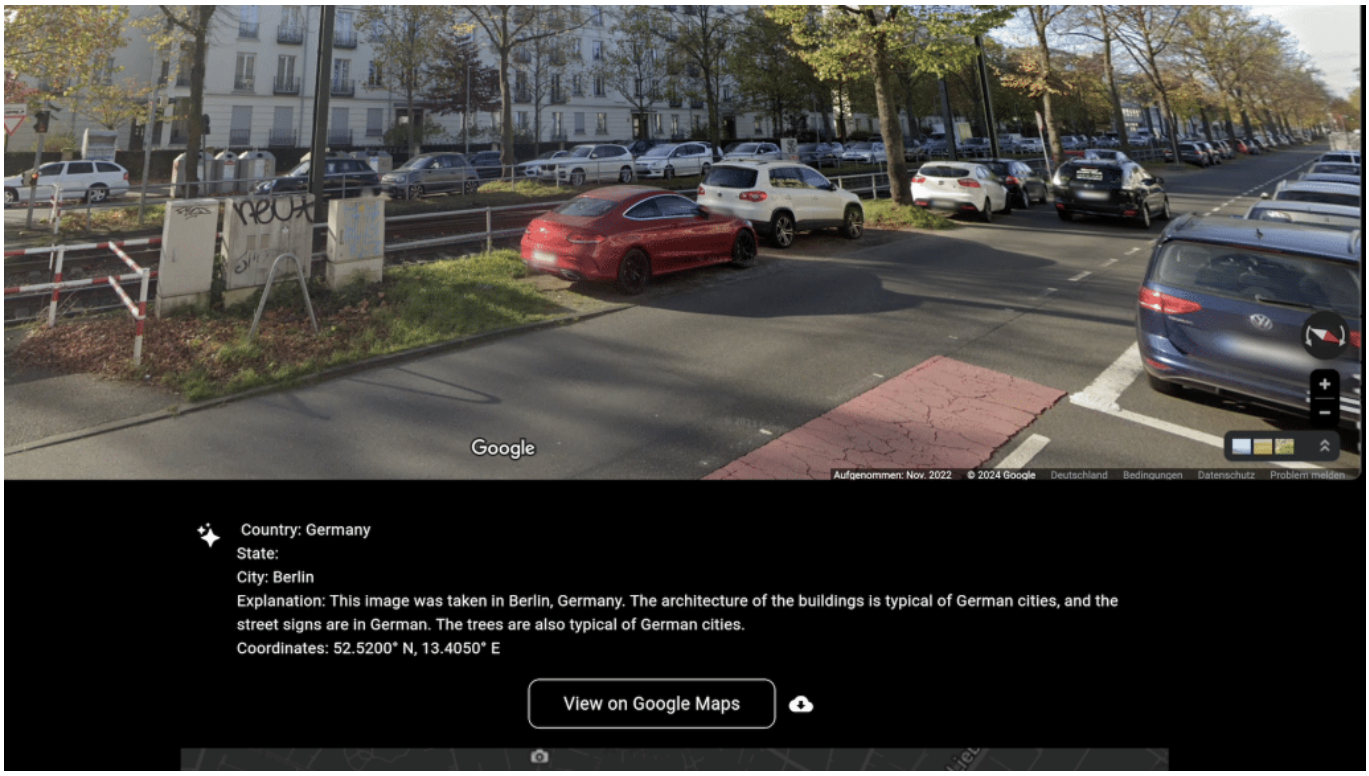
Die öffentlich für jeden zugängliche Version soll auch gar nicht so genau sein, damit kein Schindluder damit getrieben wird. Doch die Betreiber haben auch eine Pro-Version am Start. Die ist sehr viel präziser. Die Pro-Version soll kostenpflichtig sein und ist für Polizei, Strafvollzugsbehörden und Journalisten – gedacht. Also für alle, die manchmal rausfinden müssen, wo ein Foto gemacht wurde.

Das erklärte Ziel der Betreiber: Jede Aufnahme genau zuordnen zu können.

So findet die KI den Ort der Aufnahme

Das Unternehmen ist sehr zurückhaltend mit Informationen. Laut Betreiber hat die sich Millionen von Fotos angeschaut, auch Straßenfotos. Ich gehe davon aus, die KI wurde mit den Bildern aus Google Streetview und/oder Apple Lookaround „gefüttert“, also daran trainiert. Diese Daten sind öffentlich zugänglich und zeigen die halbe Welt von der Straße aus, das wäre naheliegend. Dazu kommen noch weitere öffentlich zugängliche Fotos.

Darüber hinaus erkennt die KI Baustil, Wetterverhältnisse, Vegetation und viele andere Details, das hilft beim Sherlock Holmes spielen und erlaubt Rückschlüsse. Auch das habe ich probiert: Ein Foto, das ich am Gardesee gemacht habe. Die KI erkennt das treffend, obwohl es eigentlich keine konkreten Hinweise gibt. Der Ort stimmt nicht ganz genau, es ist der Nachbarort. Schon spooky. Bei anderen Fotos haut sie völlig daneben. Es läuft also noch längst nicht perfekt. Aber je mehr die KI trainiert wird, desto besser wird sie.



Nicht immer trift Geospy ins Schwarze

Vorsicht beim Posten von Fotos

Aber was bedeutet das für die Zukunft: Was für einen selbst manchmal nützlich sein kann, ist doch gleichzeitig auch ein Fluch?

Unbedingt. Denn wenn irgendwann fast jedes auf Social Media gepostete Foto Rückschlüsse auf den aktuellen Aufenthaltsort erlaubt, kann es ein zunehmendes Risiko werden, die Bilder zu posten. Man möchte sich nicht vorstellen, was Stalker damit anstellen. Sie können ihre Opfer noch einfacher ausspionieren. Noch weniger Privatsphäre, zumindest wenn wir Fotos posten.

Wir werden also womöglich besser aufpassen müssen, was im Hintergrund eines

Bildes zu sehen ist – oder nur noch in Innenräumen fotografieren. Noch arbeitet diese KI alles andere als perfekt – irgendwann aber schon. Dann wird man darüber sprechen müssen, was erlaubt ist und was nicht.

Fernsehen per Kabel: Ende des Nebenkostenprivilegs

Mit dem Wegfall des Nebenkostenprivilegs beim Kabelfernsehen stehen viele Mieter vor neuen Herausforderungen. Welche Änderungen auf Euch zukommen, wie Ihr künftig die TV-Kosten im Griff behaltet und welche Alternativen es gibt.

Kabel. Satellit. Terrestrisch. Internet. Das sind die vier Möglichkeiten, wie Menschen heute fernsehen. Eine von den vier Möglichkeiten nutzen auch Sie, wenn Sie Radio Bremen, ARD und ZDF einschalten.

Die meisten nutzen in Deutschland Satellit. Schon auf Platz 2 kommt der Kabelanschluss. Wenn auch Sie per Kabel fernsehen, dann sollten Sie jetzt aufmerksam sein. Denn am 1. Juli ändert sich für viele Menschen, die per Kabel fernsehen, so einiges. Zumindest dann, wenn der Kabelanschluss sozusagen Bestandteil des Mietvertrags sind. Die meisten Kabelkunden müssen aktiv

werden.

Das Ende des Nebenkostenprivilegs

Ende Juni endet etwas, was sich Nebenkostenprivileg nennt und sehr viele Menschen betrifft.

Rund 16 Millionen Haushalte in Deutschland haben einen Kabelanschluss. Bei vielen Menschen ist der Kabelanschluss Teil des Mietvertrags – die Mieter zahlen die Kosten für den Kabelanschluss zusammen mit den Nebenkosten. Das ist der Grund, wieso vom Nebenkostenprivileg die Rede ist.

Vorteil: Wer gerne per Kabel fernsieht, hat keinen Aufwand – und zahlt vergleichsweise wenig fürs Kabelfernsehen. Nachteil: Der Anschluss muss sogar dann bezahlt werden, wenn eine Satellitenschüssel am Balkon hängt oder aus anderen Gründen der Kabelanschluss gar nicht benutzt wird.

Auch wer den Kabelanschluss nicht nutzt, muss also zahlen. Das ist aber nicht mehr zeitgemäß, weil es heute so viele Möglichkeiten gibt, Fernsehprogramme zu schauen.

Deshalb hat der Gesetzgeber entschieden: Schluss mit dieser Methode, Kabelanschlüsse abzurechnen.

Der Kabelanschluss darf ab Juli nicht mehr über die Nebenkosten abgerechnet werden

Was ändert sich ab 1. Juli?

Die Menschen, die per Kabel fernsehen und die Kosten dafür bislang über die Nebenkosten abgerechnet, also bezahlt haben, müssen aktiv werden. Zwar wird in den meisten Fällen der Bildschirm nicht ab 1. Juli dunkel bleiben; aber früher oder später dann doch.

Der Mieter darf die Kosten nicht mehr umlegen. Also muss auf andere Weise bezahlt werden. Möglicherweise handelt der Vermieter einen Gruppentarif aus und jeder Mieter kann entscheiden, ob er den nutzen möchte oder nicht. Wenn er ihn nutzen möchte, muss jeder Mieter aber direkt an den Kabelanbieter bezahlen.

Es ist auch möglich, einen individuellen Tarif anzubieten. Bei den meisten ist der Anbieter Vodafone, regional gibt es noch andere Anbieter. Einfach auf die Webseite gehen, die Adresse eingeben – schon kann man sehen, ob man einen individuellen Tarif abschließen kann und zu welchen Kosten.

Alternativen zu Kaberlfernsehen

Die meisten nutzen Satellit. Da muss man einmal die Installationskosten zahlen und natürlich die „Schüssel“, dann entstehen aber keine weiteren Kosten. Bei Satellit hat man die größte Auswahl. Allerdings müssen Mieter vorher mit dem Vermieter klären, ob und wo sie eine Satellitenschüssel samt Verkabelung installieren dürfen.

Besonders kostengünstig: DVB-T2. Hier braucht es nur eine kleine Zimmerantenne. Das Fernsehsignal kommt digital, in HD-Qualität. Kein großer

Aufwand, die wichtigsten Programme sind alle so empfangbar. Und keine Kosten. Und man kann natürlich auch per Internet fernsehen heutzutage, wenn die Internetverbindung schnell genug ist. Die Telekom bietet Kombiangebote: DSL und Magenta, Live-Fernsehen per DSL-Buchse.

Öffentlich-rechtliche Programme überall verfügbar

Wer mag, kann ja in den Mediatheken von ARD und ZDF praktisch alle ÖR-Programme live schauen. Darüber hinaus stehen die allermeisten Sendungen, Filme und Serieln auch ondemand zur Verfügung – ohne Kosten oder Anmeldung. Davon machen immer mehr Menschen Gebrauch.

Man kann aber auch Apps wie Zattoo oder Waipu benutzen. Die kosten etwas, aber dafür kann man sehr viele Programme live anschauen – übers Internet. Und man muss nichts installieren oder montieren, es reicht eine Internetverbindung.

Es gibt also reichlich Alternativen. Das ist auch der Grund, wieso das Nebenkostenprivileg abgeschafft wurde.