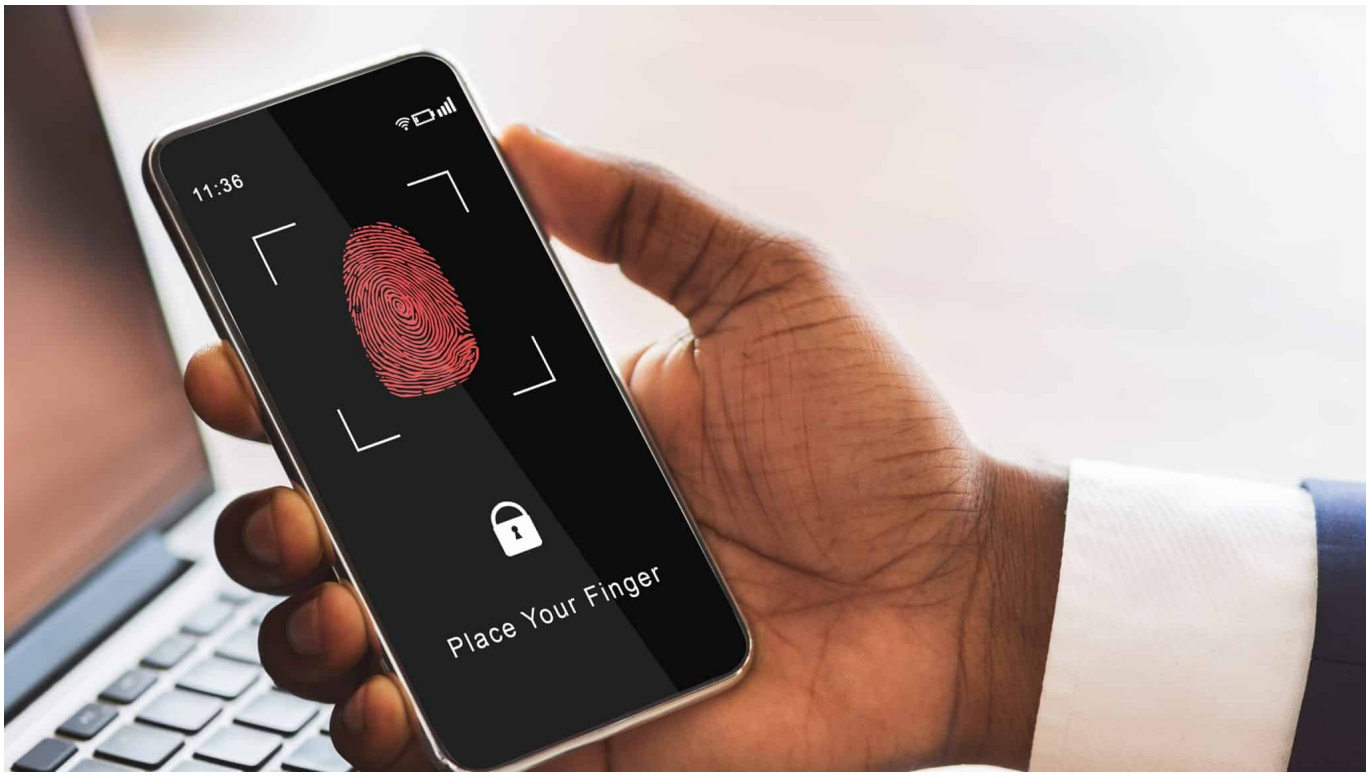
Schieb Report

Ausgabe 2023.18

Ganz ohne Passwörter: Google setzt auf Passkey



Branchenriese Google führt eine neue Methode zum Einloggen in Google-Konten ein, die sich „Passkey“ nennt – und ohne Passwort auskommt.

Wie schnell hat man ein Passwort vergessen, es falsch eingetippt – oder es wurde bei einem Hack irgendwo erbeutet und schon ist die digitale Identität gefährdet. Passwörter sind zweifellos eine Qual – aber bislang unvermeidlich. Menschen müssen sich überall per Benutzername und Passwort registrieren und anmelden.

Schon lange ist klar, dass es einen Nachfolger für diese umständliche und vor allem alles andere als sichere Methode zum „Ausweisen“ im Netz braucht. Große Unternehmen wie Google, Apple, Microsoft und Co. arbeiten deshalb schon länger an alltagstauglichen Lösungen, die einfach zu nutzen, sicher und massentauglich sind.

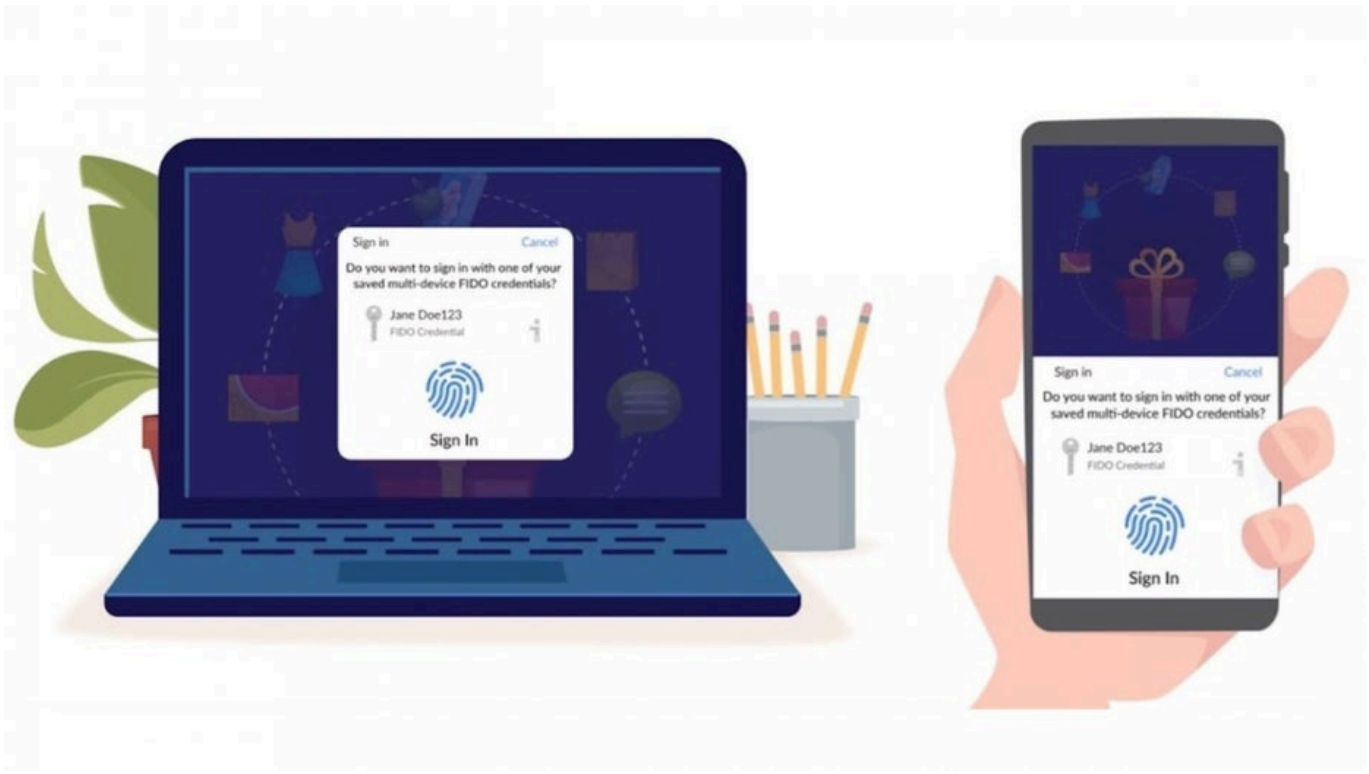
Lästig: Passwörter sind leicht angreifbar und die guten schwer zu merken

Gute Nachrichten am Weltpasswortag

Vor genau einem Jahr haben die großen IT-Konzerne zusammen mit der Fido-Alliance eine Lösung für das Passwort-Problem angekündigt. Die „Fast Identity Online“ (FIDO) Alliance ist ein Konsortium führender Technologieunternehmen, Regierungsbehörden, Dienstleister, Finanzinstitute, Zahlungsabwickler und anderer Branchen, das 2013 mit dem Ziel gegründet wurde, die Verwendung von Passwörtern auf Websites, Apps und Websites zu vermeiden.

Am Weltpasswortag (04. Mai 2023) hat Google nun für Passwort-Muffel eine gute Nachricht: Ab sofort lassen sich bei allen Google-Konten weltweit ganz ohne Passwort benutzen. Jeder, der mag, kann darauf verzichten. Stattdessen kommen sogenannte „Passkeys“ zum Einsatz.

Bei Passkeys handelt es sich um einen kryptografischen Schlüssel (verschlüsselter, einzigartiger Code). Alles, was es dazu braucht, ist ein „vertrauenswürdiges“ Gerät, das einmal eingerichtet werden muss. Das kann zum Beispiel ein Smartphone sein. Es reicht dann aus, dort einen PIN einzugeben – oder sich einfach per Gesichts-Scan oder Fingerabdruck „auszuweisen“ und somit anzumelden.



Passkey: Einmal generiert machen sie ein Login kinderleicht und sicher

Biometrischer Login: Bequemer und sicherer

Das ist nicht nur deutlich bequemer, sondern obendrein sicherer. Denn biometrische Systeme, die Fingerabdruck scannen und abgleichen oder ein Gesicht erkennen, funktionieren heute sehr zuverlässig. Die Trefferquote liegt laut aktuellen Studien bei weit über 99%. Einen Fingerabdruck zu „entwenden“ oder ein Gesicht zu fälschen und Scanner zu überlisten ist zwar nicht unmöglich, aber ungeheuer aufwändig.

Google-Nutzer können ab sofort bei allen Google-Konten zu Passkeys wechseln – und damit Passwörter und zweistufige Verifizierungen per „Multifaktor Authentifizierung“ bei der Anmeldung endgültig vergessen. Alles, was zum Anmelden nötig ist, wird verschlüsselt auf dem lokalen Gerät gespeichert. Biometrische Daten bleiben geschützt und werden niemals rausgegeben. Ob man sich per PIN, Fingerabdruck oder Gesichts-Scan ausweist, bleibt jedem selbst überlassen.

Passkey: Google ist der erste große Dienst, der Passkeys flächendeckend anbietet

Mehr Sicherheit: Phishing läuft ins Leere

Großer Vorteil: Es ist völlig unmöglich, einen Passkey zu stehlen – und zu missbrauchen. Denn ein Passkey ist immer zwingend an das jeweilige Gerät gebunden. So laufen Phishing-Angriffs ins Leere: Dritte erhalten niemals Zugriff auf den Passkey, ohne physisch Zugriff auf das jeweilige Gerät zu haben.

Praktisch funktioniert es so: Wer einmal sein Smartphone mit seinem Google-Konto verbunden hat (was nur wenige Augenblicke dauert), kann sich darüber jederzeit ausweisen. Gesichts-Scan genügt. Auch ein Login am PC lässt sich dann über das Smartphone freischalten.

Ebenso ist es denkbar, einen speziellen USB-Key zu verwenden: Der wird mit dem Google-Konto verbunden und speichert den Passkey. Immer dann, wenn man sich einloggen möchte, reicht es, den Key einmal kurz zu berühren (etwa mit Fingerabdruck-Scanner). Auf diese Weise kann man sich dann – passwortlos – in jedem Rechner einloggen.

Google ist der erste größte Anbieter, der das neue Verfahren konsequent einsetzt.

Es ist damit zu rechnen, dass andere Anbieter wie Apple oder Microsoft schon sehr bald folgen werden. Da es heute möglich ist, sich über ein Google-Konto bei vielen Drittdiensten anzumelden, erspart einen das die Eingabe von Passwörtern längst nicht nur bei Google-Diensten.

Wer sich – alternativ – weiterhin mit Passwort anmelden möchte, kann das tun.

„Schnelle Sicherheitsmaßnahmen“: Apple verteilt iOS 16.4.1 (a) und macOS 13.3.1 (a)

Updates sind wichtig, um Sicherheitslecks zu schließen - aber auch manchmal lästig, weil sie lange Ladezeiten bedeuten. Apple will das ändern und führt eine Art Turbo-Updates ein.

Apple hat mit **iOS 16.4.1** und **macOS 13.3.1** eine neue Form der Software-Updates erstmals für alle Nutzer eines iPhones und Macs veröffentlicht. Mit den sogenannten **Rapid-Security-Response-Updates** (RSR-Updates, in deutsch: **Schnelle Sicherheitsmaßnahme**) muss Apple bei Sicherheitslücken nicht jedes Mal ein großes OS-Update verteilen.

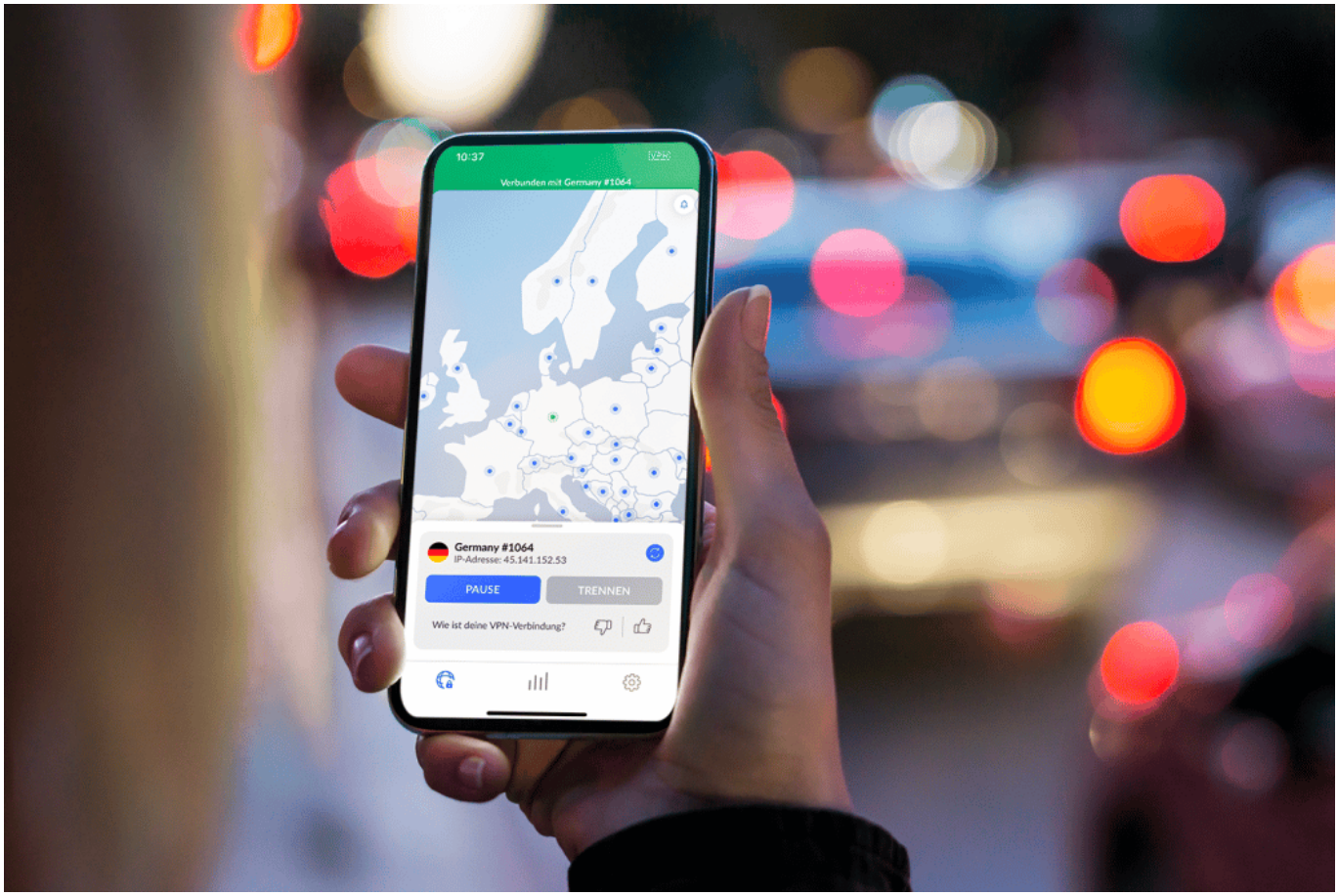
Apple hat einen ersten Testlauf der neuen "schnellen Sicherheitsmaßnahmen" durchgeführt. Vorteil: Der Mechanismus erlaubt es dem Hersteller, Schwachstellen und Fehler künftig auch unabhängig von größeren

Betriebssystem-Updates und dadurch deutlich schneller und einfacher zu beheben. Wer mag, aktiviert die Funktion in den Einstellungen.

Die Patches werden dann mit über die in iOS, iPadOS und macOS integrierte Softwareupdate-Funktion zum Download angeboten und standardmäßig automatisch installiert. Nutzer erhalten im Anschluss einen Hinweis

Für uns bedeutet das: Updates, ohne lange Wartezeiten und vor allem ohne Reboot.

Ich betone das hier immer wieder: Sicherheit ist ein wichtiges Thema in der Technologiebranche. Apple hat sich in dieser Hinsicht immer wieder als Vorreiter erwiesen. Mit dieser neuen Form von Updates hat Apple erneut bewiesen, dass sie die Sicherheit ihrer Nutzer ernst nehmen.



Update schließt viele Sicherheitslecks

Die iOS 16.4.1 und macOS 13.3.1 Updates enthalten mehrere wichtige

Sicherheitspatches, die potenzielle Schwachstellen im Betriebssystem beseitigen. Einige der wichtigsten Sicherheitsverbesserungen, die mit diesen Updates eingeführt wurden, sind:

1. Schutz vor Zero-Day-Exploits: Diese Exploits sind Schwachstellen im Betriebssystem, die von Hackern genutzt werden können, um unautorisierten Zugriff auf das System zu erhalten. Die iOS 16.4.1 und macOS 13.3.1 Updates enthalten Patches, die bekannte Zero-Day-Exploits beseitigen, um die Sicherheit der Nutzer zu gewährleisten.
2. Verbesserte Privatsphäre: Mit diesen Updates hat Apple auch die Privatsphäre der Nutzer verbessert. Einige der Änderungen umfassen die Verbesserung der Passwortverwaltungsfunktionen und die Möglichkeit, die Verwendung von Standortdaten durch Apps zu beschränken.
3. Schutz vor Phishing-Angriffen: Phishing-Angriffe sind eine der häufigsten Arten von Cyberangriffen. Mit den neuesten Updates hat Apple die Anti-Phishing-Funktionen verbessert, um Nutzer vor gefälschten Websites und Betrugsversuchen zu schützen.
4. Verbesserter Schutz vor Malware: Die iOS 16.4.1 und macOS 13.3.1 Updates enthalten auch Patches, die die Nutzer vor Malware-Angriffen schützen. Dies wird durch die Verbesserung der Sicherheitsfunktionen von Safari und anderen Apps erreicht.

Insgesamt sind die iOS 16.4.1 und macOS 13.3.1 Updates wichtige Schritte in Richtung einer besseren Sicherheit und Privatsphäre für Apple-Nutzer. Es ist jedoch immer noch wichtig, dass Nutzer ihre Geräte regelmäßig auf Updates überprüfen und sicherstellen, dass sie die neuesten Sicherheitspatches installiert haben.

Das war's für heute, vielen Dank fürs Lesen meines Techblogs! Wenn Sie Fragen oder Anregungen haben, zögern Sie nicht, diese in den Kommentaren unten zu hinterlassen

Weitere Verbesserungen

Ich möchte noch einige weitere Punkte hinzufügen, die die neuesten Sicherheitsupdates von Apple betreffen.

1. Verbesserte Passwortsicherheit: Mit iOS 16.4.1 und macOS 13.3.1 hat Apple die Passwortsicherheit verbessert. Die neue Funktion "Sichere

Empfehlungen" schlägt Nutzern sichere und einzigartige Passwörter vor, die schwer zu knacken sind. Dadurch wird die Sicherheit der Nutzerkonten auf verschiedenen Plattformen verbessert.
2. Verbesserte Kommunikationssicherheit: Die Updates von Apple verbessern auch die Kommunikationssicherheit von iMessage und FaceTime. Sie verschlüsseln automatisch alle eingehenden und ausgehenden Nachrichten und Anrufe, um sie vor unbefugtem Zugriff zu schützen.
3. Patches für Schwachstellen in Drittanbieter-Apps: Apple hat auch Patches für bekannte Schwachstellen in Drittanbieter-Apps bereitgestellt, um die Sicherheit der Nutzer zu verbessern. Diese Schwachstellen können von Hackern genutzt werden, um auf das Betriebssystem und die persönlichen Daten der Nutzer zuzugreifen.

Abschließend lässt sich sagen, dass die neuesten Sicherheitsupdates von Apple ein wichtiger Schritt in Richtung einer besseren Sicherheit und Privatsphäre für Nutzer sind. Es ist jedoch wichtig zu beachten, dass es keine 100%ige Sicherheit gibt, da es immer wieder neue Bedrohungen gibt. Daher ist es wichtig, dass Nutzer vorsichtig sind und sich bewusst bleiben, wenn sie ihre Geräte verwenden und auf verdächtige Aktivitäten achten.

Erzwungene Aktivierung von Sicherheitsstandards bei Microsoft 365

Alle Benutzer der Microsoft 365-Pläne (ehemals Office 365) bekommen dieser Tage eine E-Mail, dass zum 11. Mai die Sicherheitsstandards aktiviert werden. Was bedeutet das?

Die Mail von Microsoft

Ein Mailtitel, den man eigentlich als SPAM abtun würde: "Wichtig: Wir werden bis zum May 11, 2023 die Sicherheitsverbesserungen für Ihre Organisation aktivieren." Diese E-Mail ist allerdings tatsächlich von Microsoft, und sie weist Euch auf eine wichtige Änderung hin: Bei älteren Konten ist es so, dass die Benutzer sich alleine mit der Kombination E-Mail-Adresse/Passwort anmelden können. Das ist unsicher, die Zwei-Faktor-Authentifizierung (2FA) ist mittlerweile Standard. Um genau diese geht es.

Microsoft 365 geht normalerweise davon aus, dass es einen Administrator gibt und mehrere Benutzer, und dass dieser die Änderungen für alle Benutzer zentral

vornimmt. Wenn Ihr in der Familie oder in einem kleinen Unternehmen Microsoft 365 nutzt, dann ist das Prinzip dasselbe. Ihr müsst also gegebenenfalls tätig werden.

Microsoft

Die Einstellung Sicherheitsstandards für Ihren WoPPC-Mandanten wird bis zum May 11, 2023 aktiviert.

Sie erhalten diese E-Mail, weil Sie ein globaler Administrator für WoPPC sind.

Zum Schutz Ihrer Organisation arbeiten wir stetig an der Verbesserung der Sicherheit von Microsoft Cloud Services. In diesem Zusammenhang **aktivieren wir die Einstellung „Sicherheitsstandards" in Ihrem Mandanten, die die mehrstufige Authentifizierung umfasst**. Dies kann mehr als 99,9 Prozent der Identitätsangriffe blockieren, die versuchen, Ihre Konten zu kompromittieren.

Wenn Sie sich zwischen April 27, 2023 und May 11, 2023 an Ihrem Konto anmelden, werden Sie dazu aufgefordert, die Sicherheitsstandards proaktiv zu aktivieren. Wenn Sie sich bei Ablauf dieses Zeitrahmens nicht angemeldet oder diese Einstellung nicht aktiviert haben, aktivieren wir sie automatisch für Sie.

Welche Einstellungen müsst Ihr vornehmen?

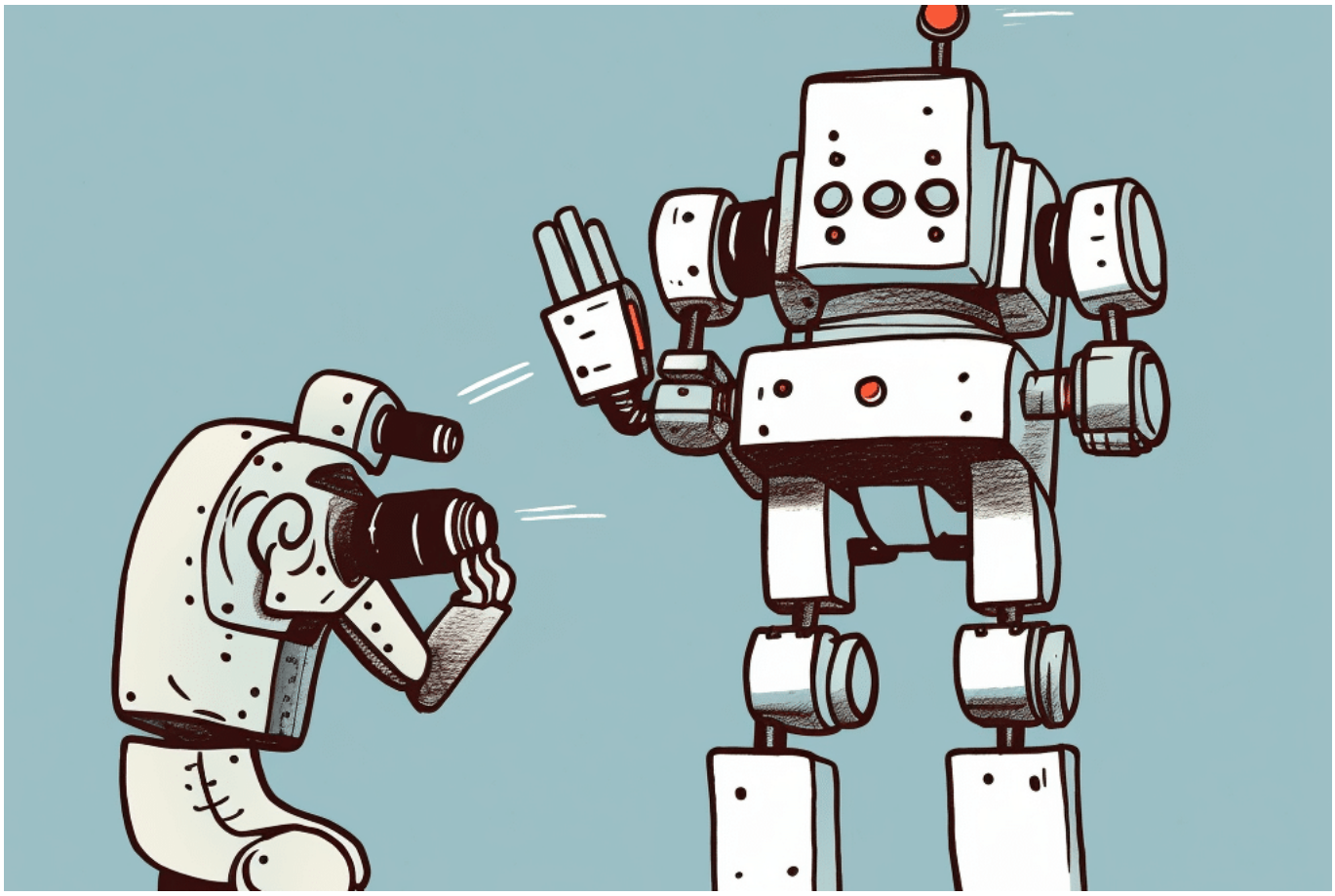
Die kompletten Organisationseinstellungen findet Ihr im Azure-Portal.

- Meldet Euch am Portal als Administrator an, dann klickt oben links auf die **drei Striche**.
- Klickt links in der Spalte der Optionen auf **Azure Active Directory**.
- Klickt auf **Eigenschaften** unten in der Liste.
- Unten im Detailbereich des Fensters findet Ihr einen Link zu **Sicherheitsstandards verwalten**. Klickt darauf.

- Aktiviert unter Sicherheitsstandards durch einen Klick auf das Auswahlmenü **Aktiviert (empfohlen)**.
- Klickt auf **Speichern**.

Nun solltet Ihr jeden Anwender die Microsoft Authenticator-App einrichten lassen. Mit der könnt Ihr den zweiten Faktor, der die Anmeldung an Eurem Konto absichert, wenn das Passwort bekannt geworden ist.

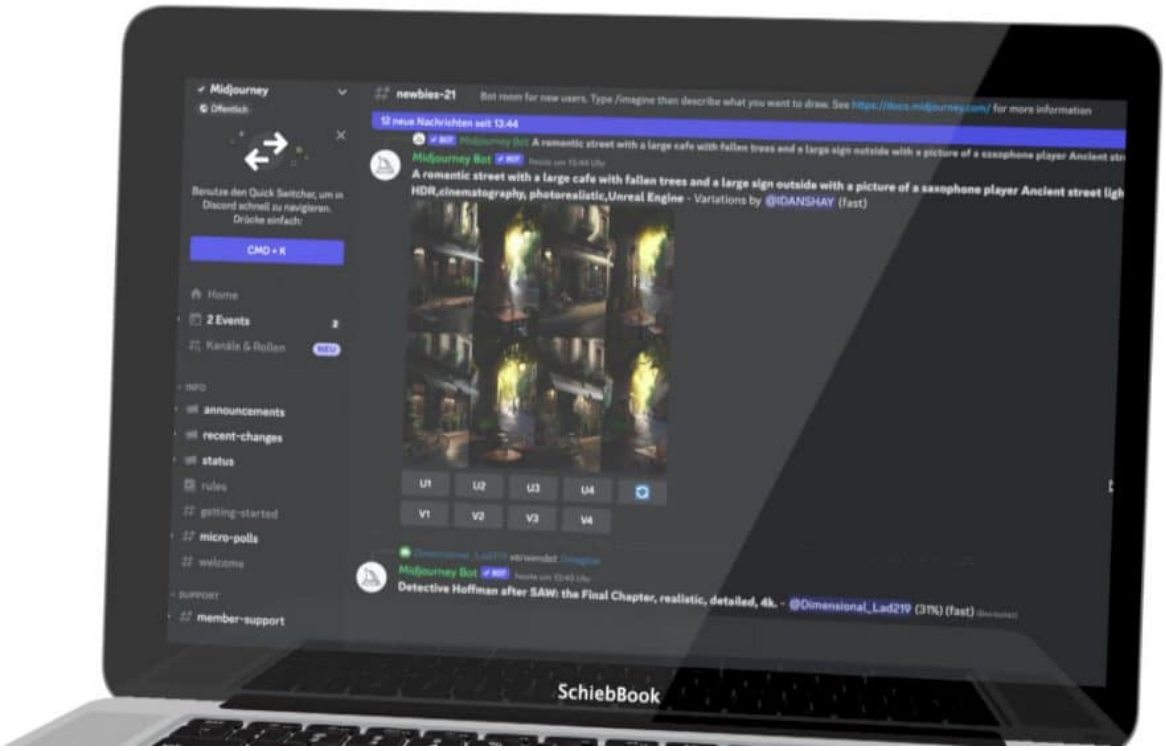
KI Training: Fotograf verlangt Löschung seiner Fotos



KI-Systeme wie ChatGPT oder Midjourney werden aufwändig trainiert: mit Inhalten, die frei im Netz zugänglich sind. Ob das OK ist, ist umstritten. Jetzt hat ein Fotograf verlangt, dass seine Fotos aus einem KI-Gedächtnis gelöscht werden.

Künstliche Intelligenz spielt in unserer Welt eine immer größere Rolle. Egal ob bei der Erstellung von Texten, der Bilderkennung oder der Spracherkennung - überall wird KI eingesetzt.

Doch was passiert eigentlich mit den Daten, die von KI-Systemen verarbeitet werden? Ein aktueller Fall zeigt, dass es hierbei auch ethische Fragen gibt, die diskutiert werden müssen.



Midjourney produziert erstaunliche Fotos und Aufnahmen

Fotograf aus Berlin wehrt sich

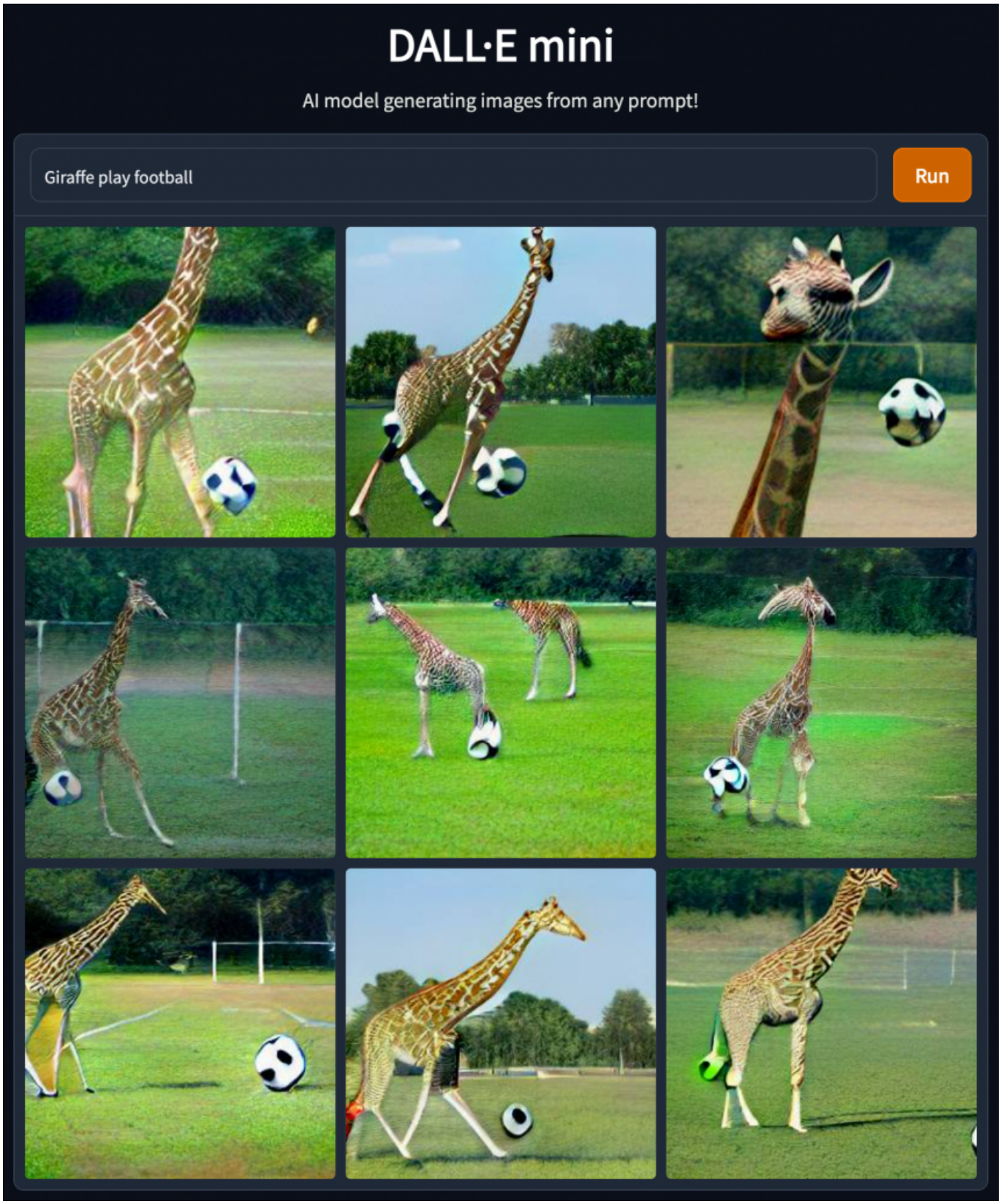
Ein Fotograf aus Berlin hat vor kurzem eine Rechnung von einem Unternehmen namens "V7 Labs" erhalten. Dieses Unternehmen betreibt eine Plattform zur Bilderkennung, auf der Nutzer Fotos hochladen können, die dann von KI-Algorithmen analysiert werden. Das Ziel ist es, die Bilderkennung von KI-Systemen zu verbessern.

Doch was hat das mit dem Fotografen zu tun? Nun, es stellte sich heraus, dass einige der Bilder, die von V7 Labs verwendet wurden, von dem Fotografen stammten. Er hatte diese Bilder in der Vergangenheit auf einer Stockfoto-Plattform hochgeladen und war davon ausgegangen, dass sie nur von anderen Nutzern zu kommerziellen Zwecken genutzt werden würden.

Welche Bilder dürfen KIs benutzen?

Als er nun erfuhr, dass seine Bilder von V7 Labs verwendet wurden, fühlte er sich unwohl. Er hatte keine Kontrolle darüber, wie seine Bilder verwendet wurden und wollte nicht, dass sie Teil eines KI-Bilddatensatzes sind. Aus diesem Grund forderte er V7 Labs auf, seine Bilder aus ihrem Datensatz zu entfernen.

Doch V7 Labs lehnte dies ab. Sie argumentierten, dass sie das Recht hätten, die Bilder zu verwenden, da sie auf einer öffentlich zugänglichen Plattform verfügbar waren. Außerdem sei die Verwendung der Bilder für die Verbesserung von KI-Systemen von großem Nutzen für die Gesellschaft.



Rechte durchgesetzt

Diese Antwort stieß bei dem Fotografen auf Unverständnis. Er argumentierte,

dass er als Urheber der Bilder das Recht habe, zu entscheiden, wie sie verwendet werden. Außerdem sei es nicht seine Verantwortung, dass seine Bilder Teil eines KI-Datensatzes werden. Er befürchtet, dass seine Bilder für Zwecke genutzt werden könnten, die er nicht gutheißen würde, wie etwa die Überwachung von Personen.

Dieser Fall wirft einige wichtige ethische Fragen auf. Auf der einen Seite gibt es das Recht des Fotografen als Urheber seiner Bilder. Er sollte entscheiden können, wie seine Bilder verwendet werden. Auf der anderen Seite gibt es jedoch das Argument, dass die Verwendung von KI-Systemen für die Gesellschaft von großem Nutzen sein kann. Wenn wir KI-Systeme verbessern wollen, müssen wir ihnen große Mengen an Daten zur Verfügung stellen. Es ist jedoch fraglich, ob diese Daten immer ethisch einwandfrei erhoben werden können.

Wir brauchen Lösungen

Es ist wichtig, dass wir diese Fragen diskutieren und Lösungen finden, die sowohl die Rechte der Urheber schützen als auch die Entwicklung von KI-Systemen ermöglichen. Eine Möglichkeit wäre zum Beispiel, dass Urheber ihre Bilder mit speziellen Lizenzen versehen können, die den Einsatz in KI-Systemen ausschließen. Eine andere Möglichkeit wäre, dass Unternehmen wie V7 Labs transparenter darüber informieren, welche Bilder sie verwenden und wie sie diese verwenden.

In jedem Fall sollten wir uns bewusst sein, dass unsere Daten und Bilder in der heutigen digitalen Welt oft nicht mehr unter unserer Kontrolle sind. Wir sollten uns daher genau überlegen, welche Daten wir teilen und wie wir sie teilen. Unternehmen sollten auch ihre Verantwortung wahrnehmen und sicherstellen, dass sie Daten ethisch einwandfrei erheben und verwenden.

Insgesamt zeigt dieser Fall, dass die Diskussion um die ethischen Aspekte der künstlichen Intelligenz und der Verwendung von Daten noch lange nicht abgeschlossen ist. Wir müssen uns weiterhin damit beschäftigen und Lösungen finden, die die Rechte der Urheber schützen und gleichzeitig die Entwicklung von KI-Systemen ermöglichen. Nur so können wir sicherstellen, dass KI-Systeme auf eine ethisch einwandfreie Art und Weise entwickelt werden und einen Nutzen für die Gesellschaft haben.

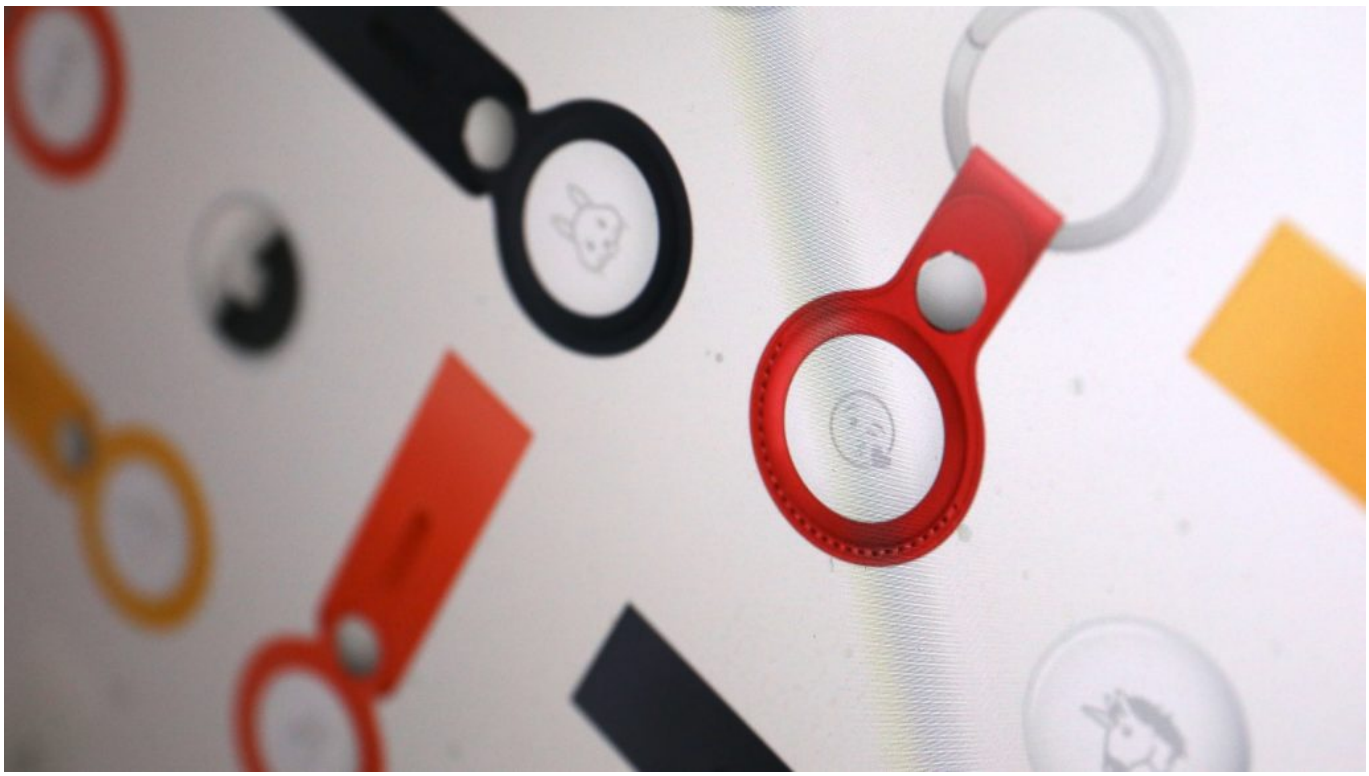
Apple und Google unternehmen etwas gegen unerwünschtes Tracking

Die kleinen Tracker von Apple und Google können extrem praktisch sein - aber auch missbraucht werden. Jetzt schließt sich Apple mit Google und anderen Unternehmen zusammen, um dem Missbrauch von Bluetooth-Ortungsgeräten wie den AirTags zu begegnen. Ein Industriestandard soll helfen.

Vielleicht kennt Ihr die Minigeräte, die nicht viel größer als eine 2-EUR-Münze (aber etwas dicker) sind und ein jederzeitiges Orten von Gegenständen ermöglichen: Einfach den AirTag von Apple in eine Tasche legen - und Ihr findet sie immer wieder. Google hat ähnliche Technologie im Angebot. Das Problem: Es gibt Menschen, Stalker zum Beispiel, die missbrauchen diese Technologie, um andere Menschen zu überwachen.

Nun wollen Apple und Google unerwünschtes Tracking zu einem Industriestandard machen. Dies ist eine wichtige Entwicklung in der Tech-Branche, da sie dazu beitragen kann, die Privatsphäre von Nutzern im Internet zu

schützen und die Akzeptanz dieser wirklich praktischen Gadgets zu verbessern.



Zusätzliche Bänder zum Anbringen der AirTags

Unerwünschte Nachverfolgung soll erschwert werden

Die beiden Tech-Konzerne haben angekündigt, dass sie ihre Betriebssysteme so aktualisieren werden, dass sie es Websites und Apps schwerer machen, Nutzer ohne deren ausdrückliche Zustimmung zu verfolgen. Konkret: Sowohl Apples iOS 14.5 als auch Android 12 sollen eine neue Funktion enthalten, die es Nutzern ermöglicht, dem Tracking zu widersprechen. Man könnte auch sagen, sie sollen Stalking unterbinden.

Wie Apple erklärt, machen auch weitere Unternehmen wie Samsung, Tile, Chipolo, eufy Security und Pebblebee mit und haben ihre Unterstützung für den Entwurf der Spezifikation angekündigt. Das gemeinsame Projekt soll sicherstellen, dass Bluetooth-Ortungsgeräte wie AirTags nicht missbraucht werden können. Der Trick: Die Betriebssysteme sollen unerwünschtes Tracking erkennen und Warnhinweise über iOS- und Android-Plattformen hinweg anzeigen.

Stalking verhindern

Schon seit es AirTags und vergleichbare Produkte gibt, kommt es immer wieder zu Fällen von Missbrauch. Stalker stecken (meist) Frauen unbemerkt einen Airtag in die Tasche - und können dann sehen, wo sie wohnen oder wohin sie gehen. Eifersüchtige Partner können sich gegenseitig überwachen. All das ist strafbar, weil die Überwachung ohne Zustimmung verboten ist.

Apple hat zwar verschiedene technische Maßnahmen eingeführt, um Stalking mit AirTags zu verhindern oder zumindest erschweren, wie zum Beispiel das Ertönen eines Warntons, wenn sich ein fremder AirTag für eine gewisse Zeit in der Nähe befindet. So erhalten potenzielle Opfer einer Überwachung auf ihrem iPhone Anweisungen, wie sie den fremden AirTag in ihrer Nähe erkennen und ausschalten können. Allerdings funktioniert dieser durchaus sinnvolle Anti-Stalking-Schutz nur dann, wenn alle Beteiligten ein iPhone verwenden - was wohl kaum vorausgesetzt werden kann.

Genau das soll sich durch die Kooperation ändern.

Apple hat AirTag und das "Wo ist?"-Netzwerk mit einer Reihe von proaktiven Funktionen ausgestattet, um unerwünschtes Tracking zu verhindern. Jetzt sollen Maßnahmen kommen, um sicherzustellen, dass die Technologie wie vorgesehen genutzt wird. Dieser neue Industriestandard baut auf den Schutzmaßnahmen von AirTag auf und ist durch die Zusammenarbeit mit Google ein entscheidender Schritt nach vorn, um unerwünschtes Tracking unter iOS und Android zu bekämpfen.

Breite Zusammenarbeit

„Bluetooth-Tracker haben Nutzern enorme Vorteile gebracht, aber sie bergen auch das Potenzial für unerwünschtes Tracking, das nur durch industrieübergreifende Maßnahmen gelöst werden kann“, sagte Dave Burke, Vice President of Engineering for Android bei Google. „Android setzt sich unermüdlich für den Schutz der Nutzer ein und wird auch weiterhin strenge Schutzmaßnahmen entwickeln und mit der Industrie zusammenarbeiten, um den Missbrauch von Bluetooth-Trackern zu bekämpfen.“

Neben dem Feedback von Geräteherstellern sind auch Beiträge von verschiedenen Sicherheits- und Interessengruppen in die Entwicklung des Standards einbezogen worden. „The National Network to End Domestic Violence hat sich für universelle Standards eingesetzt, um Überlebende — und alle

Menschen — vor dem Missbrauch von Bluetooth-Ortungsgeräten zu schützen. Diese Zusammenarbeit und die daraus resultierenden Standards sind ein bedeutender Schritt nach vorn.

Ein Schlüsselelement zur Verringerung des Missbrauchs ist eine universelle Lösung auf Betriebssystemebene, die in der Lage ist, Tracker von verschiedenen Unternehmen auf der Vielzahl von Smartphones zu erkennen, die die Menschen täglich verwenden.

Die Spezifikation ist als Entwurf über die Internet Engineering Task Force (IETF), eine führende Organisation für die Entwicklung von Standards, im Internet eingereicht worden. Interessierte Unternehmen sind eingeladen und aufgefordert, die Spezifikation in den nächsten drei Monaten zu prüfen und zu kommentieren. Nach der Kommentierungsphase werden Apple und Google gemeinsam auf das Feedback eingehen und bis Ende 2023 eine Implementierung des Standards bei der Produktion für unerwünschte Tracking-Warnhinweise veröffentlichen, die dann in künftigen Versionen von iOS und Android unterstützt wird.

Onlinekurs hilft, Whistleblower rechtskonform zu schützen

Wir sind meist dankbar, wenn Whistleblower die Öffentlichkeit informieren. Es braucht aber geeignete technische Möglichkeiten, um sie zu schützen. Ein Onlinekurs des HPI klärt auf.

Wie Unternehmen und Organisationen sich in der Praxis auf die kommenden Anforderungen des Hinweisgeberschutzgesetzes (HinSchG) einstellen sollten, ist Thema eines neuen kostenlosen Online-Kurses des Hasso-Plattner-Instituts (HPI). Dessen Justiziarin Dr. Ina Haarhoff startet das zweiwöchige Angebot am 3. Mai. Der Gratiskurs trägt den Titel "Compliance Management: Die Umsetzung der Whistleblower-Richtlinie". Anmelden kann man sich online auf der Lernplattform openHPI unter https://open.hpi.de/courses/compliance2023.

EU-Richtlinie schützt Whistleblower

"Schon seit Ende 2019 müsste im deutschen Recht ein umfassender Schutz von Whistleblowern verankert sein. Das verlangt eine EU-Richtlinie. Aber der deutsche Gesetzgeber tut sich extrem schwer damit", sagt die HPI-Juristin. Bis heute sei es trotz mehrerer Anläufe nicht gelungen, die deutsche Umsetzung zu beschließen. Der Druck steige aber, weil die EU inzwischen sogar schon ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet hat. Das deutsche Hinweisgeberschutzgesetz werde also voraussichtlich zeitnah beschlossen werden, so Haarhoff.

Beschäftigte müssen danach die Möglichkeit erhalten, Regelverstöße oder Missstände zu melden, damit die Unternehmensführung darauf reagieren kann. Wer wie die berühmte Whistleblowerin Frances Haugen, die geheime Praktiken ihres Arbeitgebers Facebook enthüllte, entsprechende Hinweise gibt, darf dadurch keine Repressionen erleiden, etwa durch Mobbing oder Kündigung.

Whistleblower informieren die Öffentlichkeit

Unternehmen müssen Maßnahmen vorsehen

"Spätestens mit Ablauf der Fristen, die im Hinweisgeberschutzgesetz festgelegt werden, müssen auch deutsche Unternehmen die Vorgaben beachten, wenn sie empfindliche Strafen vermeiden wollen. Gerade für solche Unternehmen, die verpflichtet sein werden, interne Meldestellen einzurichten, drängt die Zeit. Das betrifft vor allem Unternehmen mit mindestens 50 Mitarbeitern", betont Haarhoff. Sie will in ihrem Onlinekurs nicht nur den zusätzlichen Aufwand bei der Umsetzung behandeln, sondern auch den Mehrwert, von dem Unternehmen langfristig profitieren können.

Konkrete Antworten verspricht die Kursleiterin zum Beispiel auf folgende Fragen: Welche Stellen muss ein Unternehmen neu einrichten, um Hinweise entgegenzunehmen? Welche Meldungen fallen überhaupt unter die neuen Vorgaben? Inwieweit sind die Datenschutzbeauftragten und Betriebsräte zu beteiligen? Und wie schützt man die Identität des Whistleblowers?

Hintergrund zur Bildungsplattform openHPI

https://open.hpi.de ist Europas Pionier unter den offenen Lernplattformen, die für alle Interessierten zugänglich sind. Seine kostenlosen Onlinekurse zu Informationstechnologie- und Innovationsthemen startete das Hasso-Plattner-Institut am 5. September 2012. Mittlerweile wurden auf openHPI rund 1,2 Millionen Kurseinschreibungen registriert - sowohl von IT-Einsteigern, als auch von Experten für digitale Transformation.

Mehr als 328.000 Personen aus 180 Ländern gehören derzeit auf der Plattform zum festen Nutzerkreis dieser Massive Open Online Courses (MOOC). Er wächst täglich. Für besonders erfolgreiche Teilnehmende stellte das Institut bisher rund 132.000 Zertifikate aus. Auch die bislang angebotenen gut 100 Kurse stehen im Archivmodus nach wie vor kostenfrei zur Verfügung. Studierende können sich für das Absolvieren von openHPI-Kursen auch Leistungspunkte an ihrer Universität anrechnen lassen. Partnerplattformen, die mit derselben Lerntechnologie arbeiten, sind neben openSAP und OpenWHO zum Beispiel auch KI-Campus, eGov-Campus und Kommunalcampus.

Big Brother Award 2023: Warum DHL und Zoom als Datensünder gelten

Einmal im Jahr vergibt der Bielefelder Verein Digitalcourage den „Big Brother Award“. Unter den diesjährigen Preisträgern sind DHL und Zoom – zwei Anbieter, mit denen wir alle im Alltag zu tun haben.

Datenschutz: Für viele nur ein Wort, für andere eine ernsthafte Angelegenheit. Durch die zunehmende Vernetzung der Welt und der Geräte fallen immer mehr Daten an – und der Datenschutz häufig hinten über. Doch der Verein Digitalcourage aus Bielefeld spürt jedes Jahr besonders krasse Fälle von Datenschutz-Verstößen auf – und vergibt den "Big Brother Award".

Es geht den Machern hinter dem Preis darum (der Verein Digitalcourage aus Bielefeld), Missstände zu brandmarken, bedrohliche Entwicklungen aufzuzeigen: Da, wo sich neue Datensammlungen auftun, die missbraucht werden könnten – und worüber die Gesellschaft unbedingt sprechen muss. Die Jury von Big Brother beweist immer ein sicheres Händchen bei der Auswahl der Preisträger in den verschiedenen Kategorien. In der Regel kommen die "Preisträger" auch nicht, um sich ihren Preis abzuholen. Das kommt nur selten vor – was dann aber auch eine

gewisse Größe zeigt.

Packstationen sind praktisch - zwingen die Menschen aber dazu, eine App zu installieren

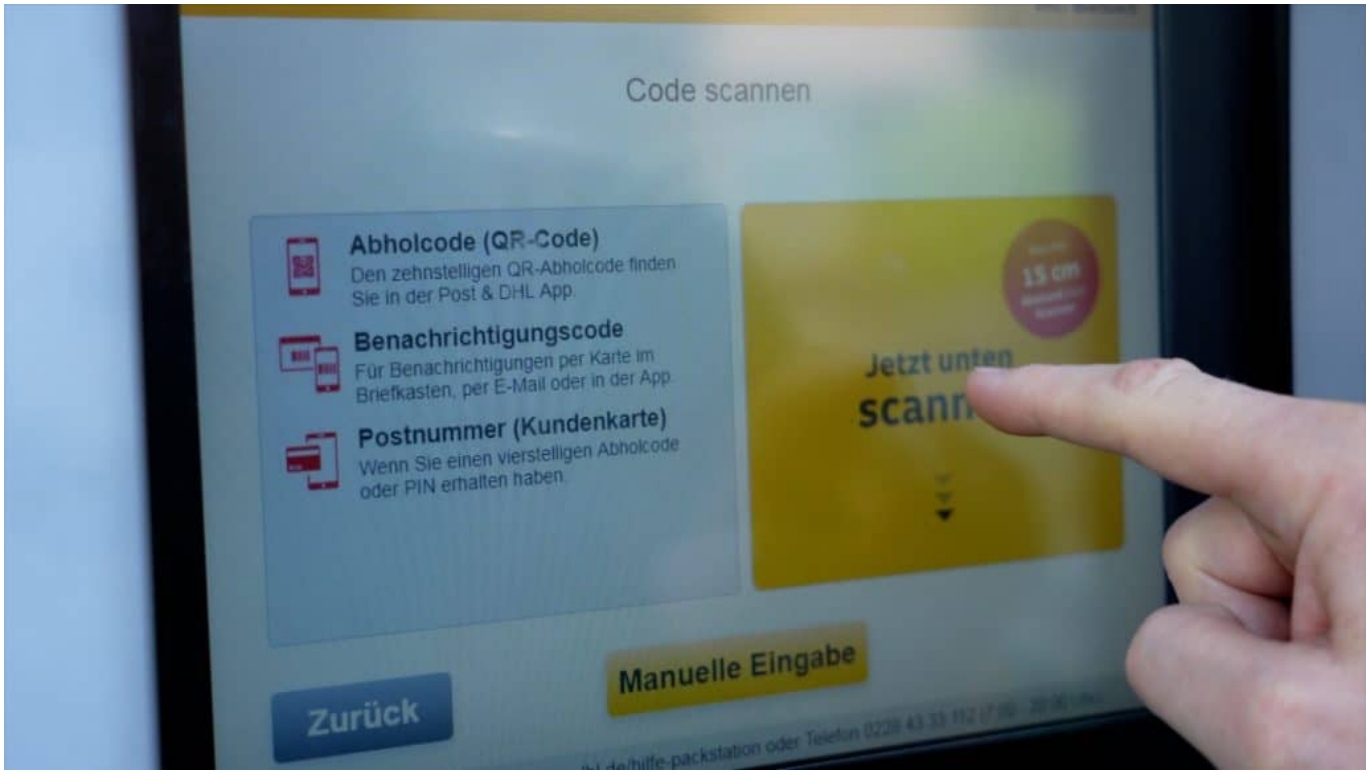
„Digitalzwang“: Ohne Smartphone keine Pakete

Ein konkreter Fall ist aus Sicht der Jury die Packstation bei DHL. Es bestehe mittlerweile ein „Digitalzwang“ für DHL-Kunden, begründet Rena Tanges. Wer ein Paket bestellt und vom Boten zu Hause nicht angetroffen wird, muss immer öfter erleben, dass die Sendung in einer „Packstation“ abgelegt wird. Dort konnten sich Kunden früher mit Kundenkarte und PIN ausweisen und so Zugriff auf das Paket erhalten.

Doch die Packstationen der neuen Generation funktionieren anders. Es gibt kein Display mehr, an dem ein PIN eingetippt werden könnte. Stattdessen wir erwartet, dass die Menschen ein Smartphone haben – und die App von „Post/DHL“ installieren. Nur damit lässt sich bei den Packstationen der neuesten Generation die passende Türe öffnen. Die Menschen werden laut Jury „gezwungen“, ein Smartphone zu besitzen – und eine App zu benutzen. Die darüber hinaus Daten

sammle und verschiedene Tracker-Unternehmen in den USA mit Daten versorge.

Darüber hinaus beklagt die Jury den zunehmenden Abbau von tatsächlichen Postfilialen, die durch Packstationen ersetzt werden.



Früher konnte man einen PIN Code eingeben - ohne Smartphone

„Zoom“: Zu viele Daten gehen nach USA

Weiterer prominenter Preisträger ist das Videokonferenz-System „Zoom“ des gleichnamigen US-Unternehmens. Hier redet sich Padeluun, einer der Gründer und Leiter des Big Brother-Award, regelrecht in Rage: „Selbst da, wo Zoom behauptet, die Server stehen in Deutschland werden Daten in die USA übertragen – das heißt: Zoom lügt an dieser Stelle“. Gemeint ist, dass bei der Nutzung des weit verbreiteten Videokonferenz-Systems Daten nach USA fließen und dort, so die Befürchtung, von US-Geheimdiensten abgegriffen werden könnten.

Dabei geht es nicht um die Inhalte der Videogespräche, die verschlüsselt übertragen werden, sondern um die sozialen Kontakte: Wer spricht wann mit wem – diese Daten fallen zweifellos an, da Zoom eine Registrierung erfordert und somit die persönlichen Daten vorliegen.

Padeluun rügt, wie unbesorgt selbst Ministerien und Organisationen mit Zoom arbeiteten. Dabei gäbe es datenschutzfreundlicher Alternativen wie Jitsi oder kMeet. Beides Systeme, die anders als Zoom, Teams oder Skype nicht in der Hand eines Konzerns sind und teilweise sogar eigenständig betrieben werden können. Solche Systeme einzusetzen, ist am Ende nur eine Frage der Gewohnheit – und der Verständigung untereinander.

Zoom: Extrem populär - aber alles andere als diskret

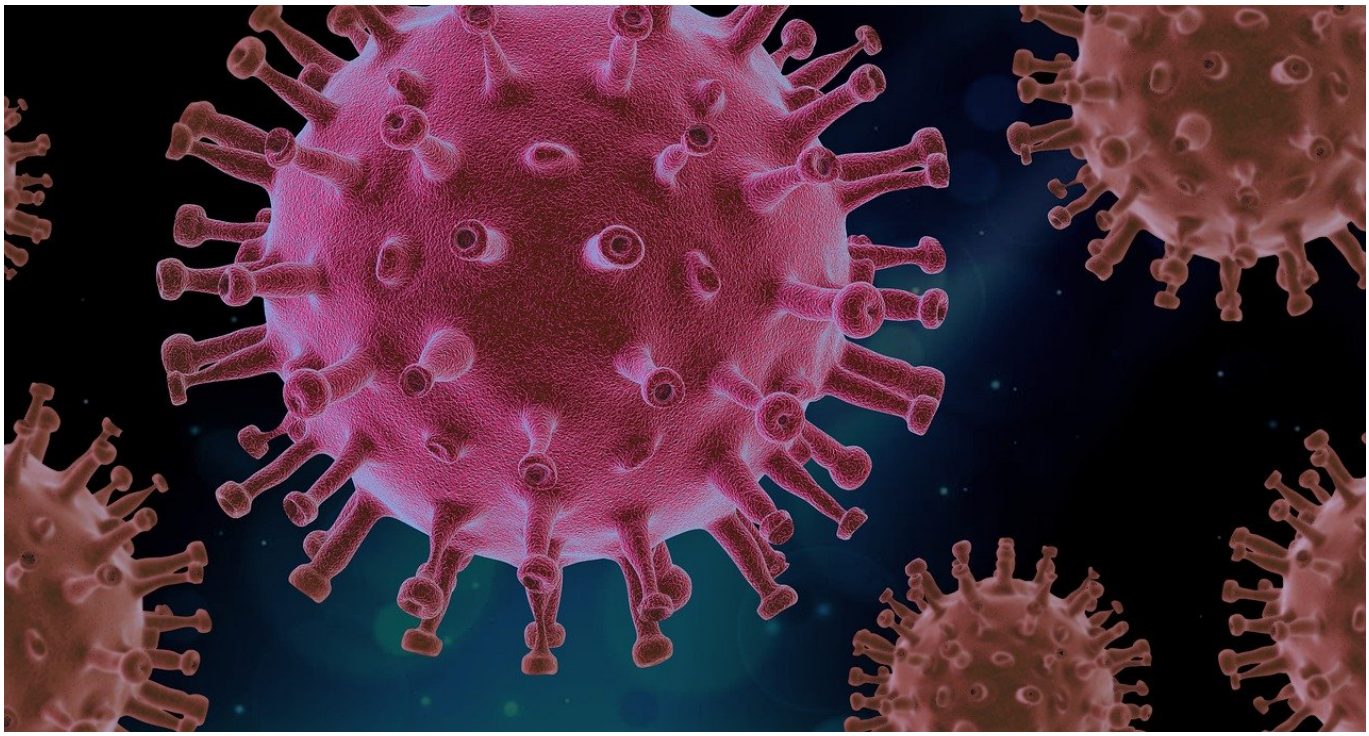
Auch Microsoft für Datenweitergabe gerügt

Mit ganz ähnlichen Argumenten wird auch Microsoft in der Kategorie „Lebenswerk“ mit dem Big Brother Award ausgezeichnet. Das Unternehmen sorge schon seit Jahren dafür, dass Daten von EU-Bürgern in die USA fließen. Denn die meisten Online-Dienste von Microsoft erfordern eine Registrierung und Anmeldung. Und selbst, wenn Daten auf EU-Servern gespeichert seien, müssten US-Unternehmen sie oft auf gerichtliche Anordnung herausgeben. Das stimmt – allerdings wehrt sich Microsoft auch juristisch gegen solche Anliegen.

Man muss schon sagen, dass die Argumentation des Big Brother Award schon sehr strikt und streng ist, ein bisschen deutsch muss man sagen: Datenschutz maximus. Aber auf jeden Fall legt der Big Brother Award einen Finger in die

Wunde und bringt so wichtige Debatten in Gang. Es ist gut, dass wir das jedes Jahr haben – und das schon seit 23 Jahren.

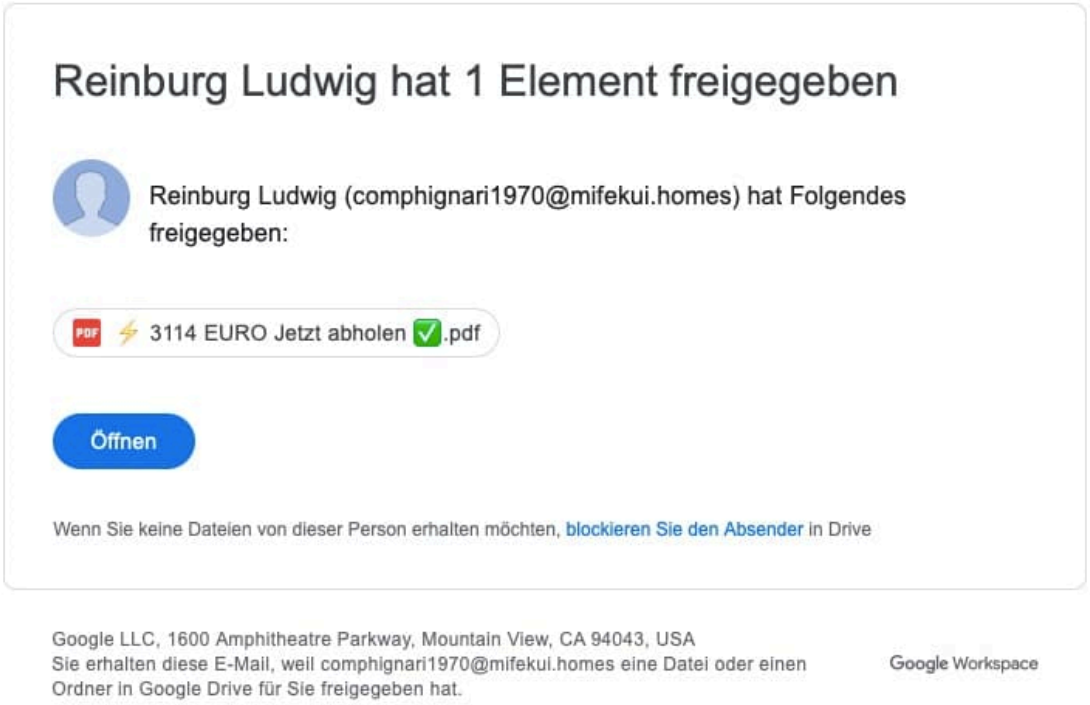
Vorsicht bei vermeintlich tollen Angeboten: SCAM-Mails



Das Internet wäre ein so toller Ort. Wenn da nicht die Betrüger wären, die Euch Daten stehlen, zu Käufen von nicht existierender Ware verleiten oder andere Gemeinheiten planen. Gerade gehen wieder zwei fiese Maschen um, die Ihr erkennen solltet!

Die freigegebene Datei per Google Drive

Jemand gibt Euch eine Datei frei. Da muss ja eine wichtige Information drin sein, oder? Nicht immer ist es eine so offensichtliche Falle wie unten, wo Ihr schon auf den ersten Blick erkennt, dass das eine Betrugsmasche ist.



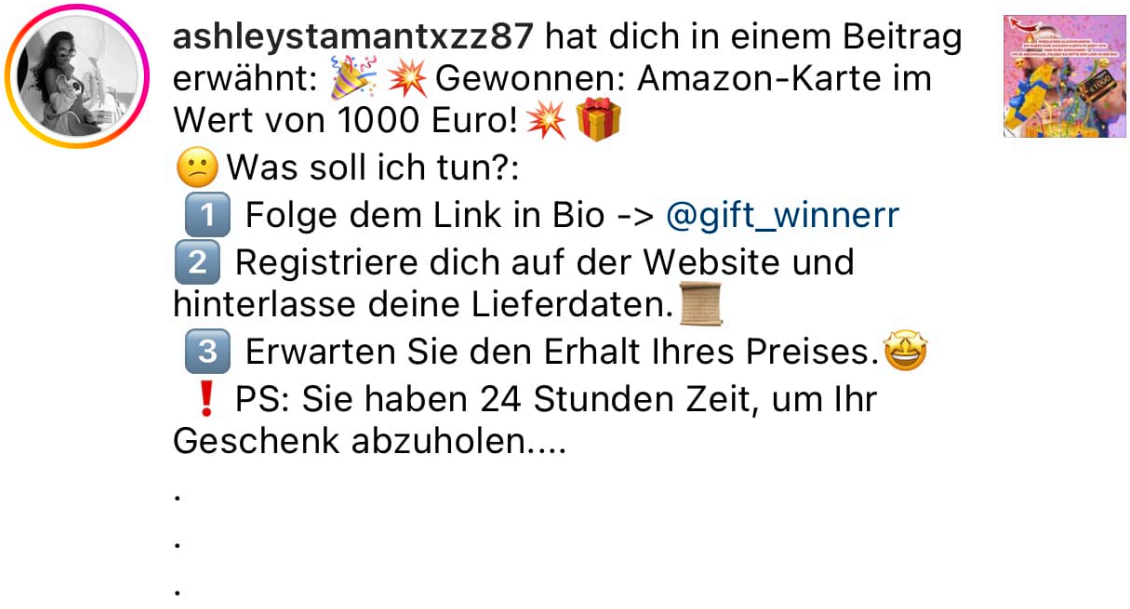
Google Drive, OneDrive, solche E-Mails bekommt Ihr gerade von verschiedenen Cloud-Diensten. Das Gemeine: Dadurch, dass die Datei nicht angehängt, sondern verlinkt ist, kann Euer Virenscanner genauso wenig eingreifen wie die Sicherheitsmechanismen Eures Mail-Anbieters. Bevor Ihr auf irgendeinen Link klickt, kontrolliert Folgendes:

- Kennt Ihr den Absender der E-Mail? Wenn diese vom Betreff her dubios erscheint, dann fragt trotzdem noch einmal bei diesem nach, vielleicht wurde sein Konto gehackt.
- Wartet Ihr auf ein Dokument von einem Absender, den Ihr im Detail nicht kennt? Dann versucht das zu validieren, indem Ihr die E-Mail-Adresse prüft (ist sie von der Firma, zu der der Sender gehört? Passt der Betreff/der Dateiname?).
- Stellt sicher, dass auf jeden Fall Euer Virenscanner aktiv und aktuell ist, wenn Ihr die Datei öffnen müsst und nicht 100% sicher seid, dass der Absender echt ist.
- Wenn Ihr nur den leisesten Zweifel habt, dann ignoriert die Nachricht.

WhatsApp, Twitter, FaceBook-SCAMs

Eine zweite, immer häufiger vorkommende Variante des SCAMs ist eine Nachricht auf einem sozialen Netzwerk. Ihr habt gerade auf Instagram ein Bild

hochgeladen und bekommt kurze Zeit später eine Nachricht, dass das Bild so toll ist, dass Ihr Geld dafür bekommen sollt. Oder eine Amazon-Geschenkkarte. Ihr müsst nur auf einen Link klicken und Euch anmelden.



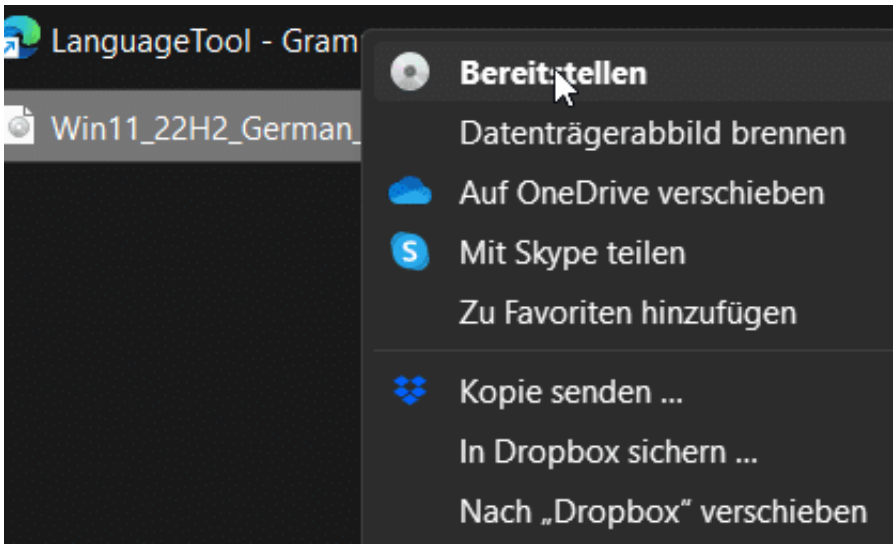
- Kontrolliert genau, wer der Absender der Nachricht ist. Wenn es ein offizieller Account ist (meist durch ein Häkchen zu erkennen), dann könnt Ihr reagieren.
- Bei allen anderen Absendern - besonders bei so komischen Namen wie im Beispiel - lasst die Finger davon. Am Ende des Links wartet nichts Gutes auf Euch: Ob ein Virus, eine Seite, die Eure Daten abgreifen möchte oder was auch immer, geschenkt bekommt Ihr nichts und habt höchstens Ärger.

ISO-Dateien: Virtuelle Datenträger optimal genutzt

Habt Ihr noch Installationsdatenträger wie CDs oder DVDs? So schön die Gewissheit eines anfassbaren Mediums ist, es ist unhandlich und anfällig. Das geht auch einfacher!

Ganze DVDs in einer Datei: ISOs

In den allermeisten Fällen sind CDs und DVDs ja nichts anderes als ein Datenträger, der im Gegensatz zu einer Festplatte geringere Kapazität hat und vor allem nicht beschreibbar ist. Der Vorteil: Ihr könnt nicht versehentlich etwas davon löschen, die Dateien darauf bleiben unverändert. Meist enthält eine DVD eine so große Zahl von Dateien, dass Ihr sie nicht mit vertretbarem Aufwand auf eine externe Festplatte kopieren könnt. Die Lösung in Windows: So genannte ISO-Dateien. Das ist ein Standard-Format, das die Dateien in ihrer Ordnerstruktur in einer einzigen Datei zusammenfasst.



Öffnen einer ISO-Datei

ISO-Dateien findet Ihr bei vielen Anbietern direkt auf der Webseite. Die meisten Programme sind nicht lauffähig, wenn Ihr nur die Dateien und nicht zusätzlich noch einen Lizenzcode habt. Der Download alleine nützt Euch also nichts, hat aber einen großen Vorteil: Ihr bekommt immer die aktuellste Version der Software, statt nach der Installation von einem vor Monaten gebrannten Datenträger gleich mehrere Updates machen zu müssen. Wenn Ihr nun eine solche ISO-Datei bekommen habt, dann könnt Ihr die wie eine DVD in Windows verwenden:

- Öffnet den Explorer und navigiert zu dem Ordner, in dem die ISO abgelegt ist.
- Klickt mit der rechten Maustaste auf die ISO-Datei.
- Klickt dann im sich öffnenden Kontext-Menü auf **Bereitstellen**.
- Ihr habt dann im Explorer ein neues (virtuelles) DVD-Laufwerk, das die Dateien enthält.

Erstellen einer ISO-Datei

Nun kann es ja auch andersherum Sinn machen, aus bestimmten Dateien oder einer eigenen CD/DVD eine ISO-Datei zu erstellen. Da habt Ihr zwei Möglichkeiten:

- Wenn es darum geht, Windows in eine ISO-Datei zu sichern, dann könnt Ihr Euch direkt bei Microsoft bedienen: Hier findet Ihr die aktuellen Windows-Versionen direkt zum Download.
- Alternativ könnt Ihr Programme wie den Infrarecorder oder IMGBurn verwenden, um aus einer CD/DVD oder einer Verzeichnisstruktur auf Eurer Festplatte eine ISO-Datei zu erstellen.
- ISO-Dateien gelten für Windows (und andere Betriebssysteme) als normale Dateien und können beliebig kopiert und einsortiert werden.
- Achtet aber darauf: Wenn Ihr Verzeichnisse von Eurer Festplatte als ISO sichert, dann enthalten diese auch alle Eure persönlichen Dateien und Einstellungen!