Schieb Report

Ausgabe 2024-02

CES2024 Trend: transparente Fernseher

Die Geräte von LG und Samsung sind der Hingucker auf der CES2024: Ausgeschaltet sieht man nur eine transparente Glasscheibe, eingeschaltet ein kristallklares Bild.

Die transparenten Fernseher sind die Sensation auf der CES 2024 in Las Vegas. Wenn sie ausgeschaltet sind, sehen die Geräte aus wie gewöhnliche Glasflächen. Doch sobald sie eingeschaltet werden, scheinen die Bilder darauf zu schweben.

Durchsichtige Hightech-Wunder

Sowohl Samsung als auch LG haben Modelle vorgestellt. Bei Samsungs transparentem MicroLED-Fernseher wird das Bild von winzigen LEDs auf die Glasoberfläche projiziert. LGs Signature OLED T nutzt die organische Leuchtdioden-Technologie, um die Pixel selbst leuchten zu lassen. Mit nur 5,7 Millimetern ist er extrem dünn.

Beide Hersteller setzen auf hochauflösende 4K-Bildschirme, die gestochen scharfe Bilder und lebendige Farben bieten. Die Diagonalen liegen zwischen 55 und 77 Zoll. Damit die Technik im Rahmen nicht stört, haben die Designer sie in den Sockeln der transparenten Fernseher untergebracht.

Funktionen: Unsichtbar und smart

Die durchsichtigen TV-Geräte punkten mit einzigartigen Funktionen, die bei herkömmlichen Modellen nicht möglich sind. Sie können wie digitale Gemälde oder Deko-Elemente in den Raum integriert werden, ohne die Sicht zu behindern.

Wenn der Fernseher ausgeschaltet ist, bleibt die Sicht durch das Display hindurch weitgehend erhalten. Filme, Serien und Spiele scheinen dann beim Einschalten wie 3D-Hologramme im Raum zu schweben.

Gleichzeitig bieten die Hightech-TVs alle Funktionen moderner Smart-TVs. Über WLAN und Bluetooth lassen sich Inhalte streamen, Sprachassistenten nutzen oder externe Lautsprecher anschließen. Einige Modelle kommen sogar ganz ohne Kabel aus.

Technologie: Die Zukunft des Fernsehens

Möglich machen dies modernste Display-Technologien. Sowohl Samsungs MicroLED als auch LGs OLED setzen auf selbstleuchtende Pixel. Im Gegensatz zu LCDs ist keine Hintergrundbeleuchtung nötig.

Bei MicroLEDs handelt es sich um winzige anorganische Leuchtdioden, die besonders kontrastreiche Bilder erzeugen können. OLEDs basieren auf organischen Materialien, die sich extrem dünn und flexibel verbauen lassen.

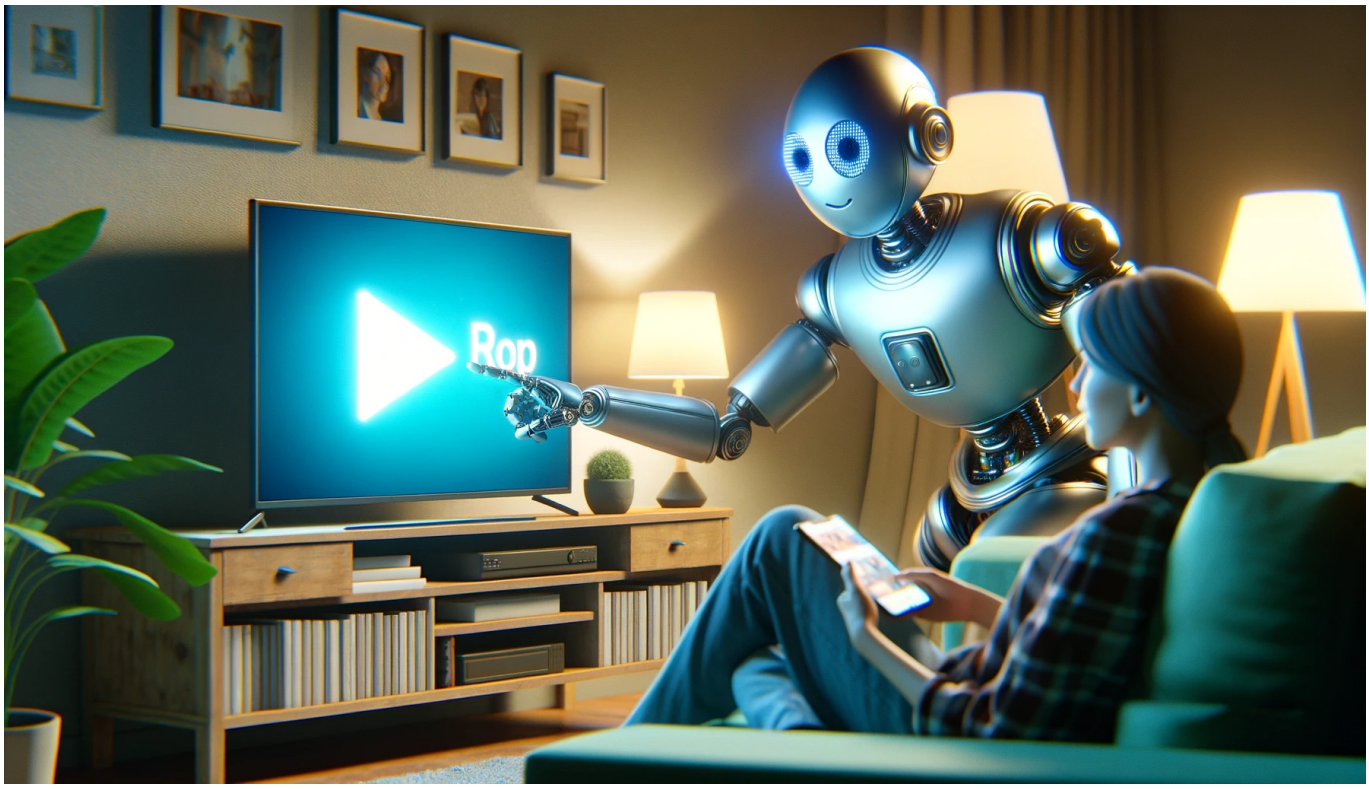
In Kombination mit transparenten Elektroden und Steuerelektronik entstehen so durchsichtige Fernseher, die den Blick durch das Display kaum beeinträchtigen. Sie gelten als Zukunftsvision für die Displaytechnik und dürften transparente Bildschirme schon bald auch in anderen Bereichen wie beim Auto oder in Schaufenstern ermöglichen.

Fazit: Fernseher werden unsichtbar

Die CES 2024 gibt einen Ausblick darauf, wohin die Reise beim Fernseher geht. Die Geräte werden immer größer, schärfer und smarter. Gleichzeitig verschwinden sie optisch mehr und mehr. Transparente OLED- und MicroLED-Displays sind ein wichtiger Schritt, um Displays komplett unsichtbar in Räume und Objekte zu integrieren.

Noch sind die durchsichtigen TV-Bildschirme sehr teuer und ein Nischenprodukt. Doch wie alle Display-Innovationen dürfte die Technik schnell erschwinglicher werden. In wenigen Jahren könnten transparente Fernseher dann zum Standard gehören.

Algorithmen in Streamingportalen und Social Media



Algorithmen bestimmen unser digitales Leben: Sie schlagen Produkte vor, neue Filme oder Serien, Musik - oder Postings und Meldungen auf Social Media. Das alles intransparent und keineswegs immer zu unserem Vorteil.

Algorithmen bestimmen unser Leben. Sie entscheiden, wann der Wecker klingelt, welche Nachrichten oder Meldungen in der Timeline von Social Media auftauchen – oder welche Bücher, Filme oder Serien uns empfohlen werden. Sie entscheiden also für uns – und wir wissen gar nicht, wer sie programmiert hat, wie sie funktionieren und ob sie wirklich uns dienen – oder den kommerziellen Betreibern.

Das ZDF ist mit gutem Beispiel vorangegangen: Der Sender hat die Entscheidungsalgorithmen der ZDF-Mediathek öffentlich gemacht.

Algorithmen sind Programmabläufe, die ständig Entscheidungen fällen

Algorithmen: die unsichtbaren Entscheider

Welche Rolle spielen Algorithmen ganz genau, zum Beispiel wenn ich mir bei Netflix etwas anschaue oder in einem Onlineshop etwas einkaufe – wie funktioniert das eigentlich?

Amazon war der erste Onlineshop, der diese Empfehlung hatte: Kunden, die das gekauft haben, die haben auch das gekauft“. Als das 1998 eingeführt haben, war das völlig neu. Experten sind sich einig: Dieses Konzept, dieser Algorithmus dahinter war der Schlüssel zum Erfolg und hat Amazon zu dem Riesen gemacht, den wir heute kennen.

Heute sind diese Algorithmen sehr viel ausgefeilter – und alle benutzen sie. Algorithmen sind Computerprogramme, die Daten sammeln und auswerten. Nach strengen Vorgaben. Heute begegnen wir solchen Algorithmen auch auf Social Media: Was bei Facebook, Instagram oder TikTok zu sehen ist, entscheidet der Algorithmus.

Er „weiß“, was uns sehr, sehr wahrscheinlich gefallen wird. Weil er uns kennt, und weil er Menschen kennt, die so ähnlich ticken wie wir – und das Verhalten

vergleicht und überträgt. So machen es auch die Empfehlungsalgorithmen bei Streamingdiensten.

Klar, wenn ich viel Action schaue – dann ist es eher unwahrscheinlich, dass ich Kuschelfilme anschaue – und umgekehrt. Nicht ganz so simpel, aber im Prinzip. Fertig sind die Empfehlungen.

Algorithmen sortieren Playlisten oder machen Vorschläge

KI ersetzt Algorithmen - teilweise

Viele fragen sich da: Aber übernimmt nicht zunehmend KI solche Aufgaben?

Das stimmt. Allerdings ist KI derzeit noch etwas zu träge, dass blitzschnell zu tun, etwa beim Scrollen in der Timeline. Aber das wird auch noch kommen.

Derzeit sind es noch eher Algorithmen. Wenn allerdings KI die Entscheidungen fällt, wird es noch schwieriger nachzuvollziehen, wie die Entscheidungen zustande kommen und welche Daten verwendet wurden – egal ob es sich um eine KI handelt, die Kreditanträge bearbeitet oder Empfehlungen im Streamingportal ausspricht.

Intransparente Algorithmen

Nun sind Empfehlungen doch etwas Gutes: Wir bekommen aus dem riesigen Angebot gezeigt, was uns noch gefallen oder interessieren könnte. Wieso ist das problematisch?

Das ist aus unterschiedlichen Gründen manchmal problematisch. Zum Beispiel dann, wenn Algorithmen uns in Social Media nur das zeigen, was in meiner Bubble passiert – und alles andere bleibt unsichtbar. Wenn Algorithmen nur das präsentieren, was erfahrungsgemäß aufregt – eher Fake News auf Social Media zB. –, aber nicht das, was richtig ist oder Qualität bietet.

Was leider genau so ist. Die Algorithmen sind so programmiert, den Anbietern den optimalen Nutzen zu bieten: Maximale Aufenthaltszeit im Netzwerk, maximale Einkaufskörbe, maximale Zufriedenheit mit dem Streamingdienst.

Dabei geht in der Regel Vielfalt verloren. Nicht gut für die Medienkompetenz, nicht gut für die Kultur. Das bedeutet am Ende eine Verarmung für die Gesellschaft. Ein weiteres Problem ist aber, dass wir nicht wissen, wie die Entscheidungen zustande kommen. Es gibt keine Transparenz.

Algorithmen sind in der Regel intransparent: Niemand versteht, wie sie

entscheiden

Öffentliche Algorithmen = Transparenz

Google, Meta und Co. machen ihre Algorithmen nicht öffentlich – sie sind wie der heilige Gral. Das ZDF ist nun aber einen ganz anderen Weg gegangen und hat den Entscheidungsalgorithmus von der ZDF Mediathek Ende 2023 öffentlich gemacht.

Jeder kann sich ansehen, welche Algorithmen das ZDF benutzt, um die vielen unterschiedlichen Empfehlungen auszusprechen. Sie sind frei zugänglich. Das ist hervorragend, denn so kann sich jeder anschauen, welche Daten das ZDF erhebt und verarbeitet und wie die Entscheidungen zustande kommen.

Das schafft Vertrauen und ist bei einem ÖR-Angebot enorm wichtig. Ein ZDF hat keine kommerziellen Interessen und macht seinen Zuschauern auch Empfehlungen außerhalb des üblichen Interessensspektrums, was Serendipität genannt wird – und hat damit Erfolg.

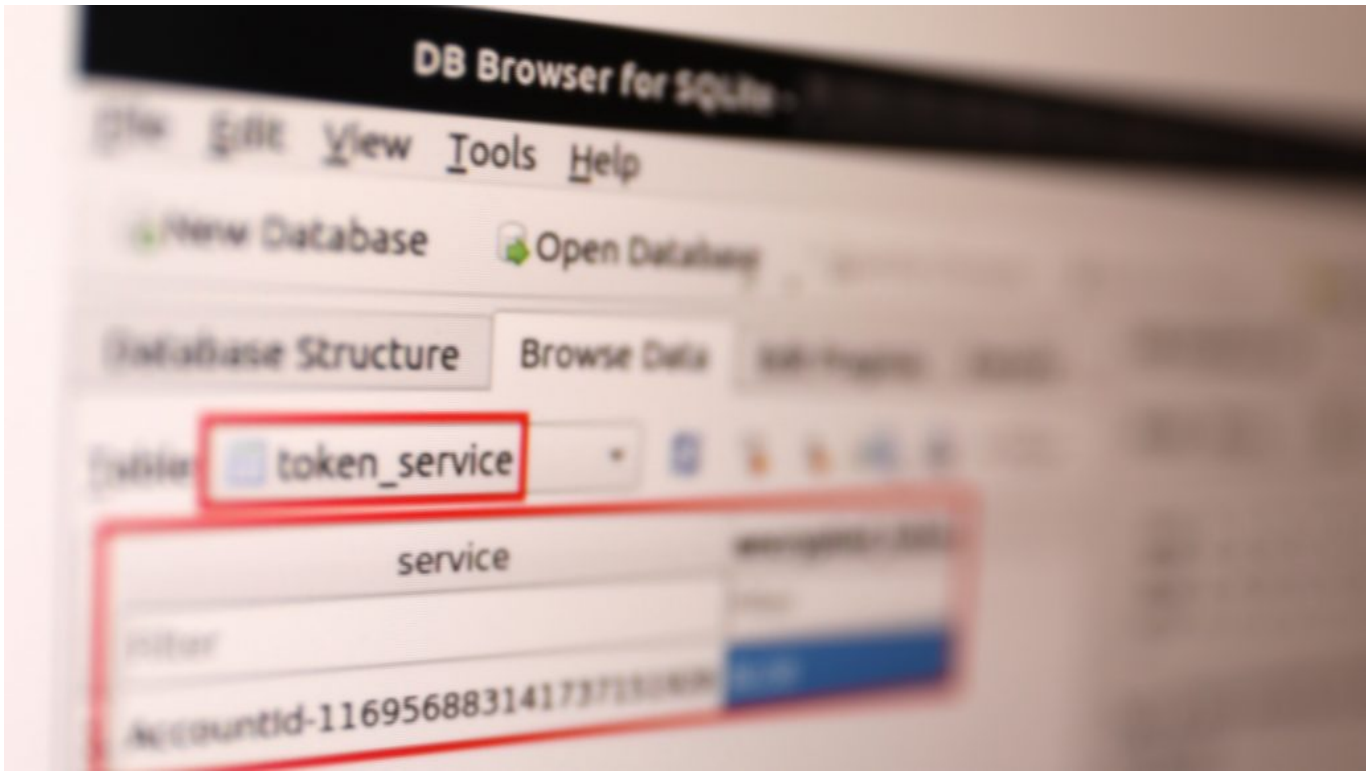
https://github.com/zdf-opensource/recommendations-pa-base

Netflix zB hat ganz andere Interessen. Sie wollen die Leute im Dienst halten und nutzen die Daten auch zur Optimierung von Konzepten und Drehbüchern, weil sie genau sehen, ob eine Szene doppelt angeschaut oder übersprungen wird zB. Hier wäre es sehr interessant, mal in die Algorithmen zu schauen. Die Vorgehensweise des ZDF ist vorbildlich.

Wieso alle Google-Dienste aktuell gefährdet sind

Ein neuer Trojaner ist im Umlauf: Die aggressive Malware nutzt Login-Informationen des Browsers und verschafft sich so unbemerkt Zugriff zu allen Google-Diensten. Die wichtigsten Hintergründe und Tipps, wie sich Nutzer von Google-Diensten effektiv schützen können.

Es gibt eine eiserne Regel: Wer sich auf dem PC oder Smartphone Malware eingefangen hat – also Schadprogramme, die Daten ausspionieren und missbrauchen –, sollte unverzüglich alle Passwörter ändern. Normalerweise empfehlenswert und effektiv. Doch beim neuen Trojaner namens „Lumma“ ist diese bewährte Maßnahme nicht zielführend: Cyberbetrüger kommen trotzdem noch in alle Google-Dienste.

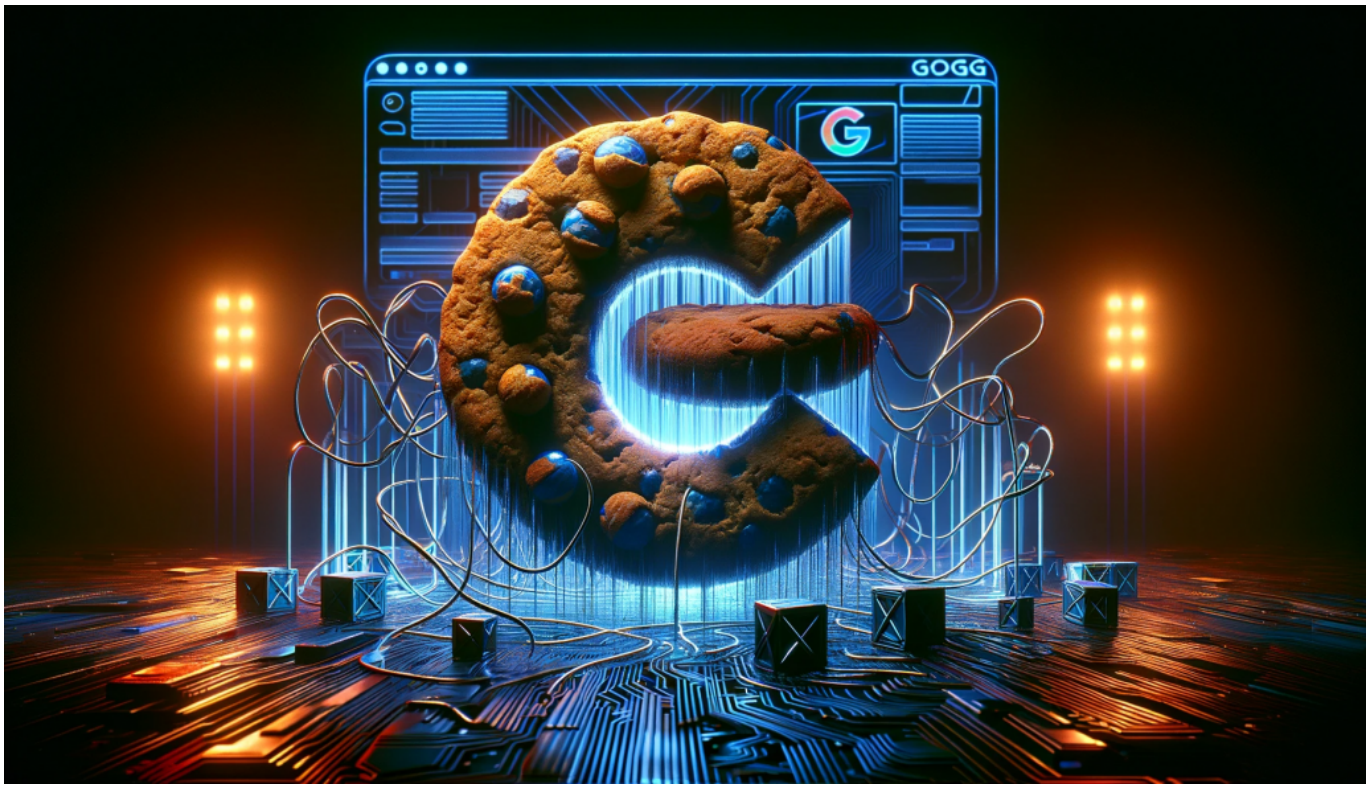


Grundlage für die neue Art des Angriffs sind Cookies

Alle Google-Dienste betroffen

Betroffen sind potenziell alle Menschen, die Google-Dienste wie Google Mail, Youtube, Google Docs, Google Play Store (etwa auf Android-Smartphones), Google Translator, Google Maps und vor allem die Google-Suche benutzen – und ein Google-Konto verwenden, um sich dort anzumelden und die Dienste individuell zu nutzen.

Durch eine Sicherheitslücke in der Art der Anmeldung („Oauth“ genannt) ist es Betrügern möglich, die auf Festplatten und Smartphones gespeicherten Cookies (kleine Infodateien) abzufangen und damit jederzeit selbständig neue zu generieren und sich Zugang zu allen Diensten zu verschaffen, selbst wenn ein User sein Passwort geändert haben sollte. Sie übernehmen quasi den Schlüsselbund und können alle Türen im Google-Universum damit öffnen.



Identitätsdiebstahl nicht ausgeschlossen

Da auch Google Mail davon betroffen ist, ein durchaus ernsthaftes Problem. Denn wenn sich Betrüger Zugang zum Mail-Postfach verschaffen, können sie nicht nur die E-Mails lesen, sondern schlimmstenfalls auch die Identität übernehmen (Identitätsdiebstahl) und durch Passwort-Reset-Funktion viele andere Online-Dienste kapern.

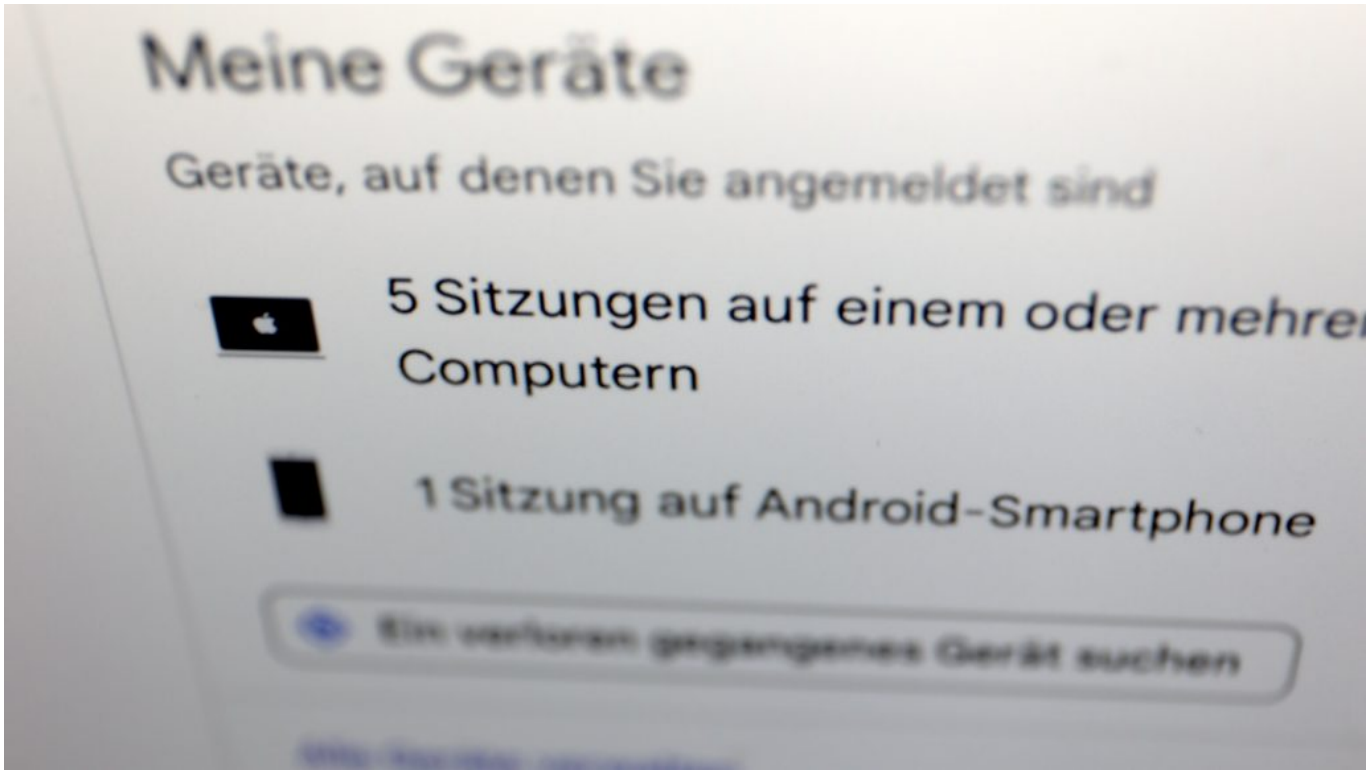
Verschiedene IT-Sicherheitsexperten haben nicht nur bereits dokumentiert, wie einfach das vorhandene Sicherheitsleck ausgenutzt werden kann, sondern auch, dass seit November 2023 bereits mindestens sechs Malware-Programme (also Trojaner) kursieren, die davon Gebrauch machen. Da es sich um noch eine relativ neue Masche handelt, ist damit zu rechnen, dass es noch mehr Trojaner werden.

Geeignete Gegenmaßahmen: Konten schützen

Die gute Nachricht: Nutzer sind nicht völlig wehrlos. Es ist wichtig, Google-Konten mit einer „Multi-Faktor-Authentifizierung“ abzusichern. Neben Benutzername und Passwort muss dann noch ein zusätzlicher Faktor eingegeben werden, etwa ein Code, der durch eine App erzeugt wird. Ein Verfahren, das normalerweise deutlich mehr Sicherheit bietet.

Ob die Multifaktor-Authentifizierung auch in diesem Fall hilft, ist allerdings noch nicht bestätigt – da die Angreifer den Cookie eines bestätigten Logins verwenden, möglicherweise nicht in jedem Fall.

Daher ist es wichtig, Rechner – und auch Smartphones – durch geeignete Schutz-Software auf Malware und Trojaner zu untersuchen. Noch viel wichtiger ist es, ab sofort im Browser nur im „Safe-Modus“ zu surfen: Dabei werden Cookies missachtet und nach der Arbeit automatisch wieder gelöscht. So hinterlässt man keine Spuren, die die Trojaner verwenden könnten.



Im Zweifel auf allen Geräten abmelden

Hilfreich ist auch, aktuell bewusst nach jeder Verwendung eines Google-Dienstes sich wieder aus dem Konto abzumelden (Logoff). Im Google Dashboard ist das sogar für alle Geräte gleichzeitig möglich. Das ist zwar unbequem, stellt aber sicher, dass die neuen Trojaner keine Möglichkeit zu haben, sich in den Google-Diensten unbemerkt anzumelden.

In jedem Fall sind Nutzer von Google-Diensten gut beraten, im Augenblick auf verdächtige Aktivitäten in ihren Konten zu achten. Unter myaccount.google.com kann man sich einen hervorragenden Überblick verschaffen. Sollten verdächtige Aktivitäten entdeckt werden: Ausnahmslos überall abmelden und alle(!) Browser und Apps schließen.

Google-Kontoaktivitäten überprüfen:
https://myaccount.google.com/data-and-privacy

Infostealer: Wie schützt du dich effektiv vor dieser digitalen Bedrohung?

Infostealer stellen eine ernsthafte Bedrohung für deine Daten und Informationen dar. Um dich effektiv davor zu schützen, gibt es verschiedene Maßnahmen, die du ergreifen kannst.

Dazu gehören beispielsweise die Nutzung von Cloud-Services, die Verwendung von Anti-Malware-Programmen und die Zusammenarbeit mit einem erfahrenen IT-Security-Partner. Informiere dich über aktuelle Trends und lerne, wie du dein System und Netzwerk sicherer machen kannst. Denn deine Daten sind wertvoll und sollten immer geschützt sein.

Was sind Infostealer und warum solltest du dich davor schützen?

Infostealer sind eine der größten digitalen Bedrohungen für die Sicherheit deiner Daten und Informationen. Diese Malware hat das Ziel, vertrauliche Daten wie Passwörter und Kreditkarteninformationen zu stehlen. Die Infostealer können auf

verschiedene Arten in dein System gelangen, zum Beispiel über E-Mails oder Downloads aus dem Internet.

Infostealer arbeiten im Hintergrund und sammeln Informationen, ohne dass du es bemerkst. Es ist wichtig, dich vor dieser Bedrohung zu schützen, da sie nicht nur deine persönlichen Informationen gefährdet, sondern auch Cloud-Daten und Netzwerke beeinträchtigen kann.

In diesem Artikel erfährst du alles Wichtige über Infostealer: Wie erkennst du sie? Welche Arten gibt es? Welche Daten werden gestohlen? Und vor allem: Wie kannst du dich effektiv davor schützen? Es ist von großer Bedeutung, dass du deine digitale Sicherheit ernst nimmst und Maßnahmen ergreifst, um dich vor den Gefahren der Infosteler zu schützen.

Neue Malware missbraucht Cookies und verschafft sich so Zugang zu Google Konten

Erkennungsmerkmale von Infostealern: Wie erkennst du, ob dein Gerät infiziert ist?

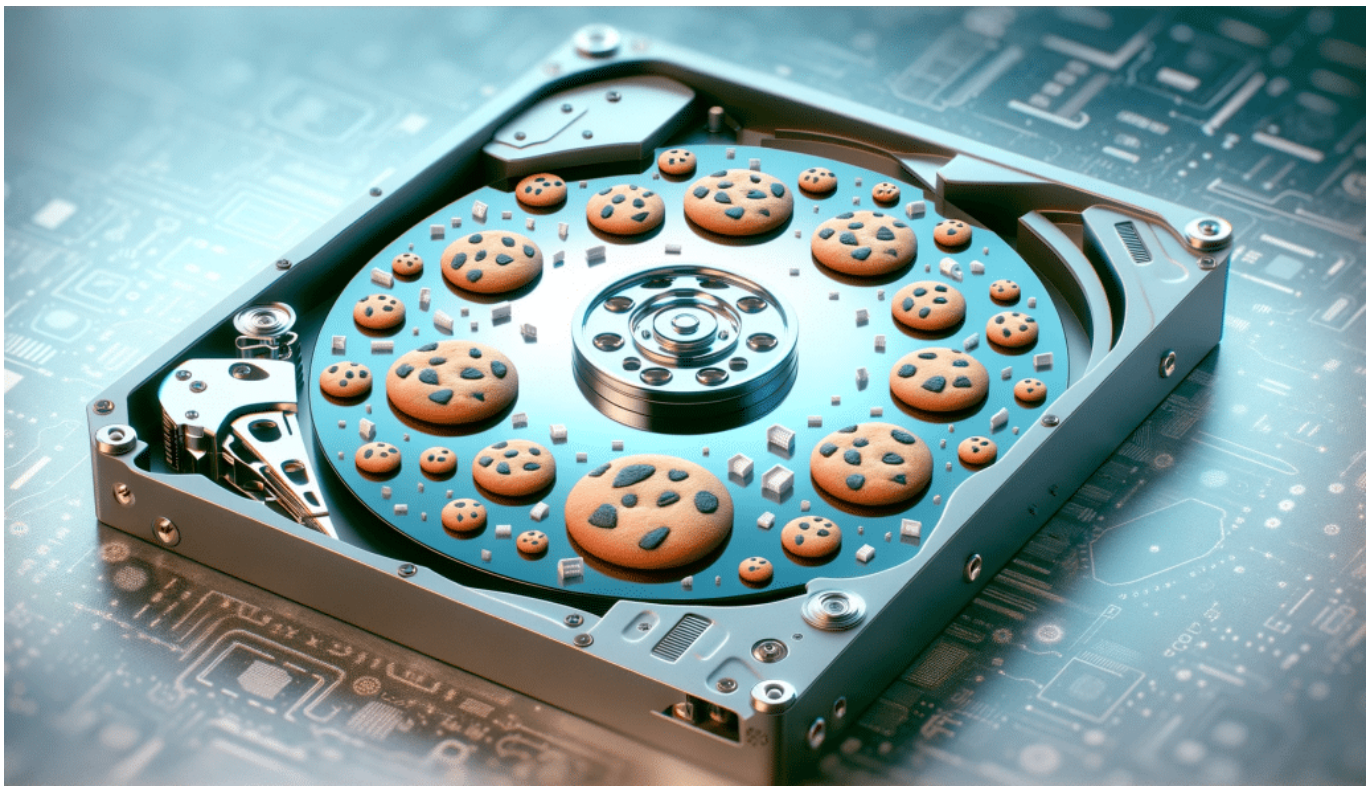
Infostealer stellen eine ernsthafte Bedrohung für die Sicherheit deiner Daten dar. Deshalb ist es wichtig, dass du weißt, wie du erkennen kannst, ob dein Gerät

infiziert ist. Ein Erkennungsmerkmal von Infostealern sind ungewöhnliche Aktivitäten auf deinem System oder Netzwerk.

Zum Beispiel kann ein Anstieg des Datenverkehrs oder der CPU-Auslastung ein Hinweis darauf sein, dass Malware im Hintergrund läuft und Informationen sammelt. Eine weitere Möglichkeit, um verdächtige Aktivitäten zu erkennen, besteht darin, deine Cloud-Dienste und -Konten regelmäßig zu überprüfen. Wenn du feststellst, dass sich unbekannte Dateien in der Cloud befinden oder Zugriffe auf deine Daten stattfinden, ohne dass du sie autorisiert hast, solltest du alarmiert sein und sofort Maßnahmen ergreifen.

Um dich effektiv vor Infostealern zu schützen, empfiehlt es sich auch immer aktuelle Antivirus-Software zu verwenden und regelmäßige Updates durchzuführen. Darüber hinaus solltest du sicherstellen, dass deine Passwörter sicher genug sind und immer auf dem neuesten Stand gehalten werden.

Indem du diese Vorsichtsmaßnahmen ergreifst und achtsam beim Umgang mit persönlichen Informationen bist, kannst du dich wirksam gegen die Bedrohung durch Infosteler schützen und deine digitalen Daten bewahren.



Die verschiedenen Arten von Infostealern und ihre

Funktionsweise

In diesem Abschnitt geht es um die verschiedenen Arten von Infostealern und ihre Funktionsweise. Es gibt eine Vielzahl von Infostealer-Malware, die alle unterschiedliche Funktionen haben.

Einige stehlen Daten aus der Cloud-Storage, während andere sich in das Netzwerk einklinken und Informationen über das System oder den Benutzer sammeln. Manche Infostealer-Stämme zielen auf spezifische Services ab, wie zum Beispiel Online-Banking-Dienste oder E-Mail-Clients. Die meisten Infostealer sammeln jedoch allgemeine Informationen wie Passwörter, Kreditkartennummern und persönliche Daten, um sie an einen Remote-Server zu senden.

Ein häufiger Typ von Infostealern ist der **Keylogger**. Diese Malware zeichnet Tastatureingaben auf und sendet sie an den Angreifer zurück. Andere Arten von Infostelers sind Formgrabber, die nach dem Ausfüllen eines Formulars im Browser die eingegebenen Informationen speichern und auch Screenshots machen können.

Eine weitere Art ist Backdoor-Infostealer, welche Hintertüren ins System öffnen können. Es gibt auch fortschrittlichere Varianten wie RATs (Remote Access Trojans), die einem Angreifer Zugriff auf ein infiziertes Gerät geben können.

Diese Art von Malware kann verwendet werden, um sensible Daten zu stehlen oder sogar das ganze System zu kontrollieren.

Um sich effektiv vor dieser digitalen Bedrohung zu schützen ist es wichtig zu verstehen, wie diese verschiedene Arten von Infostelers funktionieren und verbreitet werden könnten. Mit diesem Wissen kannst du geeignete Maßnahmen ergreifen um dich vor Infostealer-Angriffen zu schützen.

Trojaner: Kommen verdeckt - benannt nach dem berühmten Vorbild in der Antike

Welche Daten werden von Infostealern gestohlen?

Infostealer sind eine ernsthafte Bedrohung für unsere digitale Sicherheit. Sie können auf verschiedene Arten in unser System eindringen und vertrauliche Daten stehlen. Aber welche Daten werden von Infostealern gestohlen? Es gibt keine klare Antwort, da verschiedene Arten von Infostealern unterschiedliche Daten stehlen können.

In der Regel zielen sie jedoch auf unsere persönlichen Informationen ab, wie Login-Daten, Passwörter, Kontoinformationen und Kreditkartendaten. Einige können auch sensible Geschäftsdaten oder geistiges Eigentum stehlen.

Es ist wichtig zu verstehen, dass Infostealer nicht nur auf unseren lokalen Geräten agieren können, sondern auch über das Netzwerk oder die Cloud auf andere Systeme zugreifen können. Daher müssen wir uns bewusst sein, welche Art von

Daten wir speichern und wie wir diese schützen können.

Es ist ratsam, regelmäßig Backups unserer wichtigen Daten durchzuführen und starke Passwörter zu verwenden. Wir sollten auch sicherstellen, dass unsere Antivirus-Software immer auf dem neuesten Stand ist und alle Updates für unser Betriebssystem installiert wurden, um potenzielle Schwachstellen zu schließen und uns vor neuen Bedrohungen zu schützen.

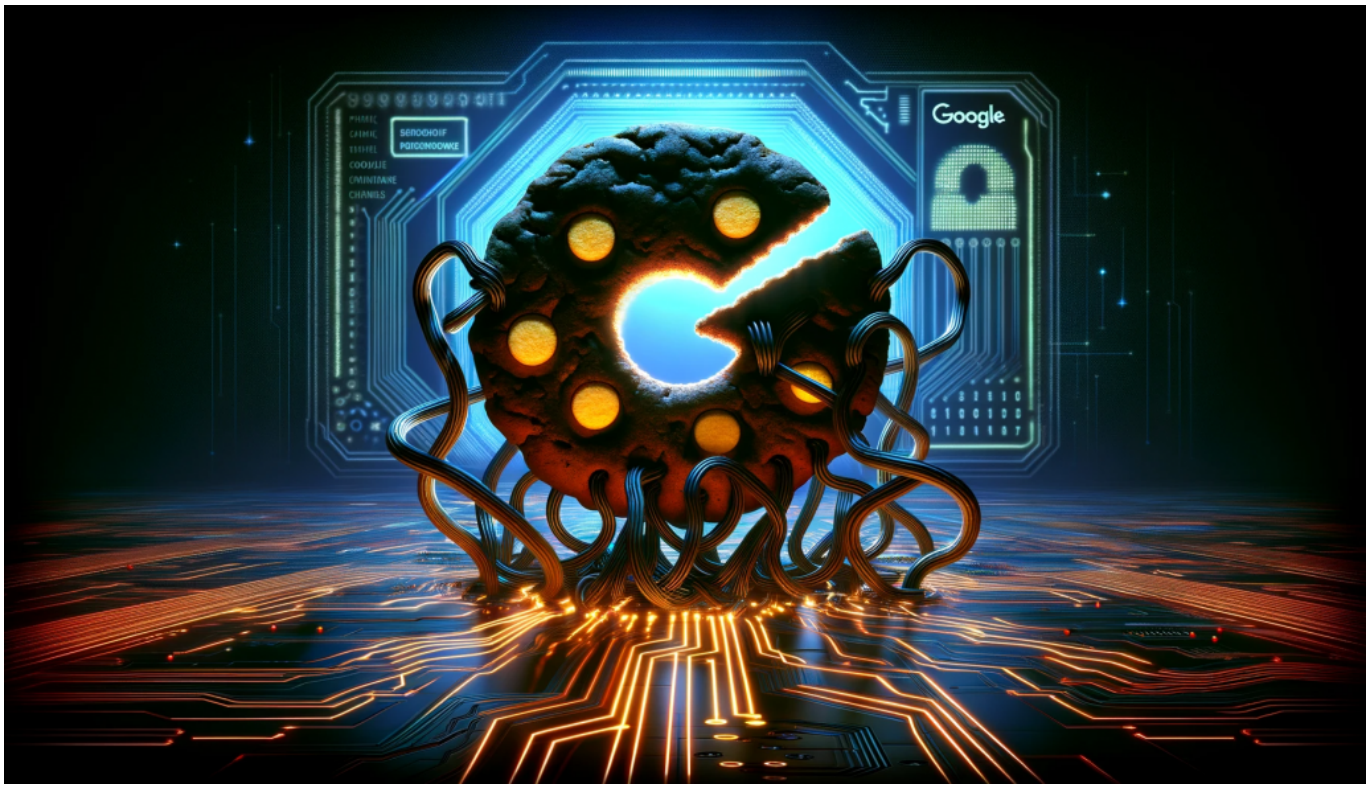
Vorsichtsmaßnahmen gegen Infostealer: Wie kannst du dich effektiv schützen?

Um dich effektiv vor Infostealern zu schützen, gibt es einige Vorsichtsmaßnahmen, die du unbedingt beachten solltest. Eine davon ist das regelmäßige Updaten deines Systems und deiner Antivirus-Software. So können bekannte Schwachstellen geschlossen werden und dein Gerät wird weniger anfällig für Angriffe von Infostealern.

Außerdem solltest du darauf achten, sichere Passwörter zu verwenden und diese regelmäßig zu ändern. Ein weiterer wichtiger Punkt ist das sensibilisierte Surfen im Internet sowie der vorsichtige Umgang mit persönlichen Informationen in E-Mails oder sozialen Medien.

Auch der Einsatz von Cloud-Services, die eine hohe Sicherheit bieten, kann eine gute Möglichkeit sein, um deine Daten vor Infostealern zu schützen. Es empfiehlt sich außerdem immer auf dem neuesten Stand in Bezug auf die verschiedenen Arten von Infostealern zu bleiben und dank trendMicro oder anderen Partnern stets über aktuelle Bedrohungen informiert zu sein.

Mit diesen Vorsichtsmaßnahmen kannst du dich effektiv gegen Infostealer schützen und sicher im digitalen Raum agieren.



Antivirus-Software als Schutz vor Infostealern

Als effektive Vorsichtsmaßnahme gegen Infostealer empfiehlt sich der Einsatz von Antivirus-Software. Diese kann dabei helfen, Schadsoftware zu erkennen und zu blockieren, bevor sie Daten stehlen oder Schaden anrichten kann. Dabei sollte die Software regelmäßig aktualisiert werden, um auch gegen neue Bedrohungen gewappnet zu sein.

Zudem ist es wichtig, auf einen vertrauenswürdigen Anbieter zu setzen und dessen Support-Services in Anspruch nehmen zu können. Einige Antivirus-Programme bieten auch Cloud-basierte Services und Netzwerk-Security an, um das gesamte System vor Bedrohungen zu schützen.

Darüber hinaus können Nutzer durch den sensiblen Umgang mit persönlichen Informationen sowie sichere Passwörter weitere Angriffsmöglichkeiten von Infostealern minimieren. Mit diesen Maßnahmen lässt sich das Risiko eines erfolgreichen Angriffs durch Infostealer deutlich verringern und ein sicherer Umgang mit Daten und Informationen gewährleisten.

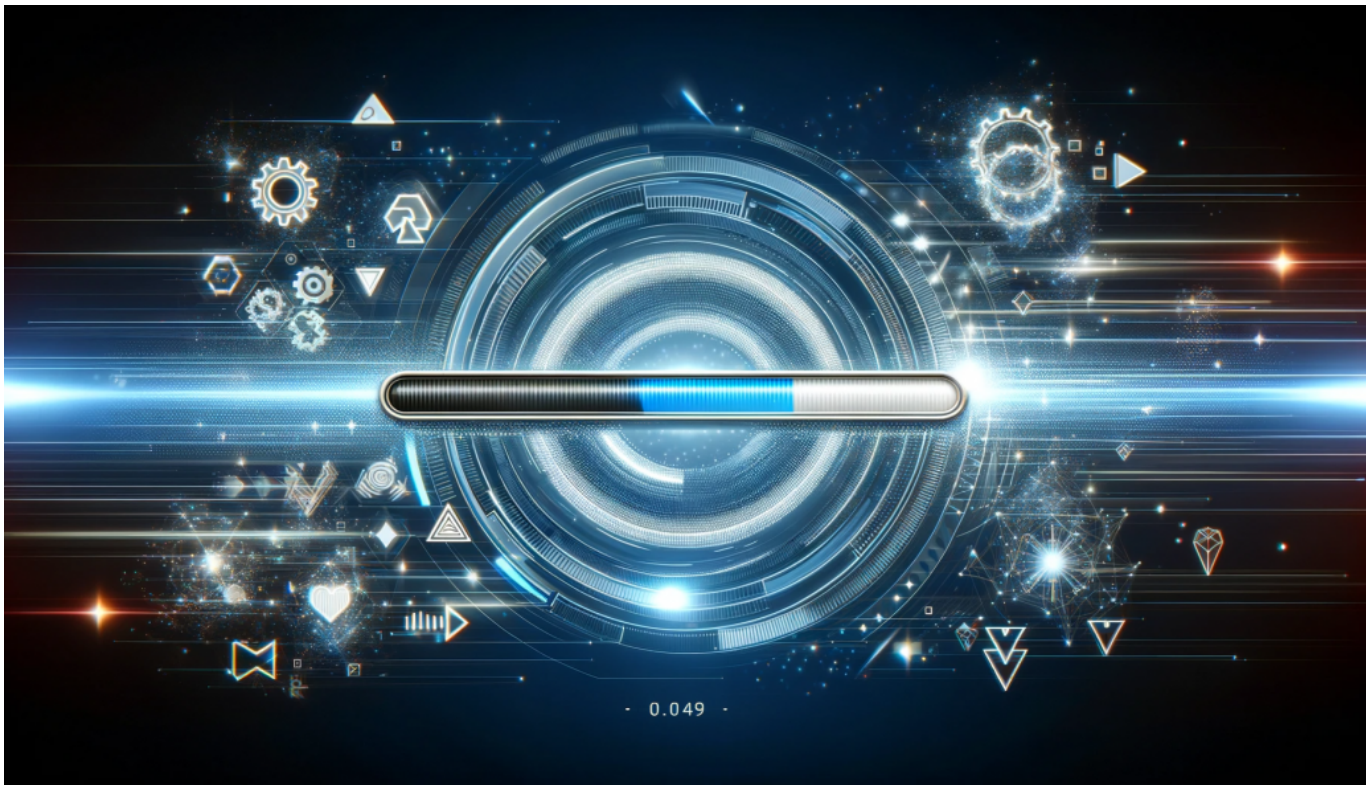
Regelmäßige Updates und sichere Passwörter zur Vermeidung von Angriffen durch Infostealer

Um sich effektiv vor Infostealern zu schützen, ist es wichtig regelmäßige Updates durchzuführen und sichere Passwörter zu verwenden. Denn Infostealer nutzen oft Sicherheitslücken in veralteter Software aus oder knacken schwache Passwörter, um an sensible Daten zu gelangen.

Regelmäßige Updates des Betriebssystems und der installierten Anwendungen können diese Lücken schließen und somit das Risiko eines Angriffs reduzieren. Auch die Verwendung von starken Passwörtern, die aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen, kann helfen, Angriffe durch Infostealer abzuwehren.

Zusätzlich empfiehlt es sich verschiedene Passwörter für unterschiedliche Dienste zu verwenden und diese regelmäßig zu ändern.

So wird das Risiko minimiert, dass ein Angreifer Zugang zu allen Konten erhält, wenn er nur ein Passwort knackt. Durch diese einfachen Vorsichtsmaßnahmen kannst du deine Daten besser schützen und dich vor den Gefahren der Infostealer bewahren.



Regelmäßige Updates helfen, Sicherheitslücken zu schließen

Sicherheitsbewusstes Surfen im Internet: Tipps zum

Schutz vor Phishing-Angriffen durch Infostealer

Ein weiterer wichtiger Aspekt, um sich vor Infostealern zu schützen, ist das Bewusstsein für Phishing-Angriffe. Dabei versuchen Cyberkriminelle, über gefälschte E-Mails oder Websites an persönliche Informationen wie Passwörter oder Kreditkartennummern zu gelangen.

Um dich davor zu schützen, solltest du immer misstrauisch sein bei E-Mails von unbekannten Absendern und niemals auf Links in solchen Nachrichten klicken. Auch wenn die Website vertraut aussieht, solltest du sicherstellen, dass die URL korrekt geschrieben ist und nicht irgendwelche Tippfehler oder zusätzliche Buchstaben enthält.

Um zusätzlichen Schutz zu bieten, kannst du auch eine Antiphishing-Software installieren. Es ist wichtig zu verstehen, dass Infostealer eine ernsthafte Bedrohung darstellen und sie können dein Leben stark beeinträchtigen, wenn sie erfolgreich sind.

Indem du diese Tipps befolgst und deinen digitalen Sicherheitsplan regelmäßig aktualisierst und überprüfst, kannst du sicherstellen dass deine Daten und Informationen geschützt bleiben und deine digitale Identität intakt bleibt.

Sensibler Umgang mit persönlichen Informationen in E-Mails und sozialen Medien, um nicht Opfer eines Datenlecks zu werden.

Ein weiterer wichtiger Faktor bei der Vermeidung von Datenlecks durch Infostealer ist der sorgsame Umgang mit persönlichen Informationen in E-Mails und sozialen Medien. Infostealer nutzen oft Phishing-Methoden, um Zugriff auf vertrauliche Daten wie Passwörter oder Bankdaten zu erhalten.

Achte darauf, keine verdächtigen Links anzuklicken oder auf Anfragen von unbekannten Personen zu antworten. Es ist auch ratsam, sensible Informationen nicht über unsichere Netzwerke oder Cloud-Services zu teilen.

Ein weiterer hilfreicher Tipp ist die Überprüfung von Datenschutzrichtlinien und Nutzungsbedingungen von Online-Diensten und -Partnern, um sicherzustellen, dass deine Daten sicher sind.

Eine regelmäßige Überprüfung deiner Kontoinformationen kann ebenfalls dazu beitragen, mögliche Angriffe frühzeitig zu erkennen und abzuwehren. Bleibe wachsam und achte darauf, wer Zugriff auf deine persönlichen Informationen hat - so kannst du dich effektiv vor den Gefahren von Infostelern schützen!

Effektiver Schutz vor digitaler Bedrohung: So bleibst du sicher vor den Gefahren der Infosteler!

Um dich effektiv vor den Gefahren der Infostealer zu schützen, gibt es einige Vorsichtsmaßnahmen, die du ergreifen kannst. Eine Möglichkeit ist die Verwendung von Antivirus-Software, um dein System auf mögliche Infektionen durch Malware und andere Bedrohungen zu überprüfen.

Regelmäßige Updates deiner Systeme und sichere Passwörter können auch dazu beitragen, Angriffe durch Infostealer zu vermeiden. Ein weiterer wichtiger Punkt ist das Bewusstsein für Sicherheit beim Surfen im Internet sowie ein sensibler Umgang mit persönlichen Informationen in E-Mails und sozialen Medien.

Durch diese Schritte kannst du bereits einen großen Schritt hin zu einem effektiven Schutz vor digitalen Bedrohungen machen.

Aber auch der Einsatz von Cloud-Services oder Netzwerksicherheits-Services kann dir helfen, deine Daten sicher zu halten und somit mögliche Diebstähle durch Infostealer zu verhindern. Zusammenfassend lässt sich sagen, dass es viele Möglichkeiten gibt, um dich gegen die Bedrohung durch Infostealer zu schützen - sei es durch den Einsatz von Software oder das Bewusstsein für Sicherheit im Umgang mit Daten und Informationen.

Neue Malware (Infostealer) ermöglicht Missbrauch von Google-Konten

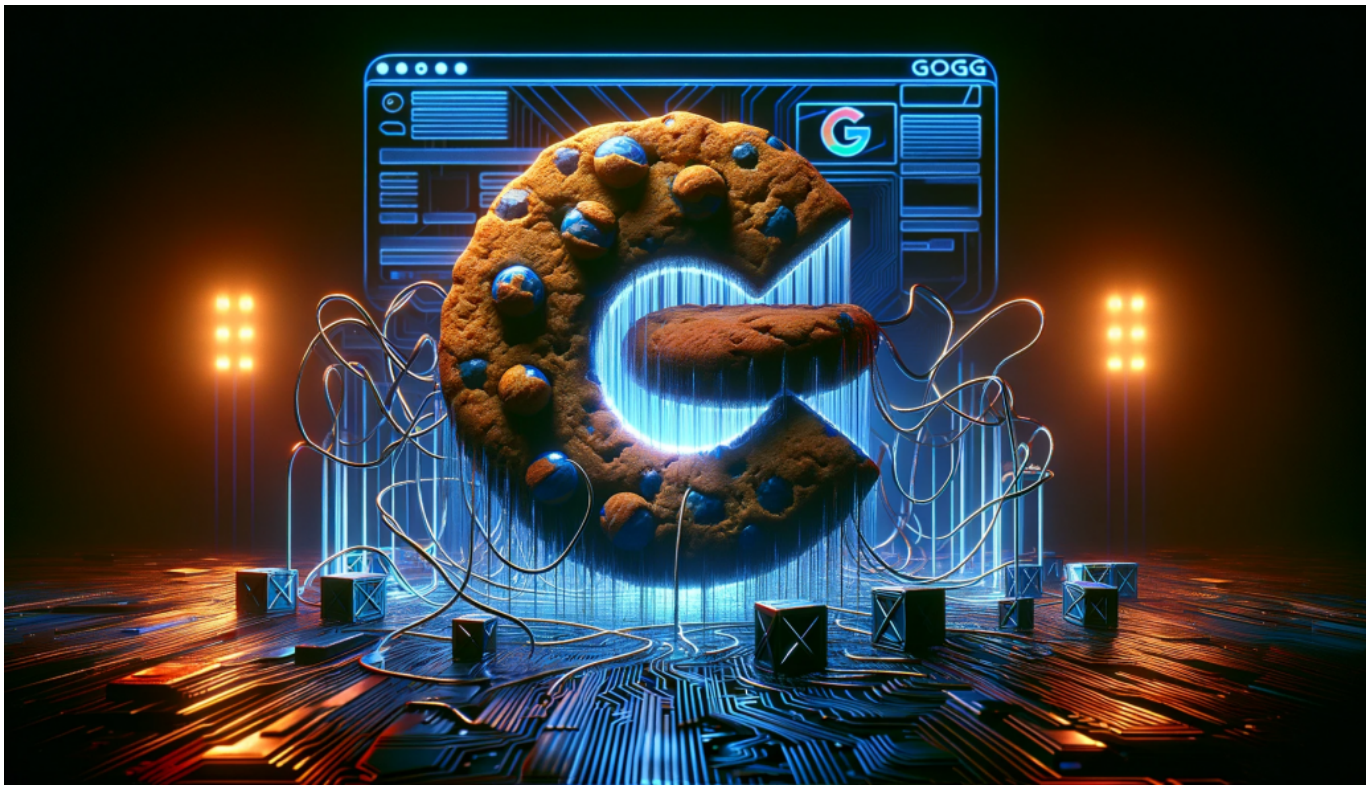
Eine neue entdeckt schädliche Software (Malware) umgeht den Passwortschutz von Google-Konten durch unbemerkte Übernahme von Google-Cookies – Passwortwechsel bleibt ohne Effekt.

Der Lumma-Trojaner greift auf Browser-Daten und eine unbekannte Google-Funktion zu, um sich fortwährenden Zugang zu Nutzerkonten zu verschaffen.

Lumma Trojaner wendet neuen Trick an

Wird ein Computer von Schadsoftware befallen, gilt es als eine der ersten Maßnahmen, sämtliche Passwörter neu zu setzen. Doch es zeigt sich, dass diese Aktion nicht immer geeignet ist, um Online-Konten vor unbefugtem Zugriff zu schützen. Aktuelle Versionen unterschiedlicher Malware-Typen haben die Fähigkeit entwickelt, die verschlüsselten Authentifizierungszusätze für Google-Konten wiederherzustellen, sogar nachdem Nutzer ihr Passwort geändert haben könnten.

Schon im letzten Herbst starteten mehrere Gruppen aus dem cyberkriminellen Milieu den Verkauf einer innovativen Funktion ihrer Diebstahl-orientierten Schadprogramme. Nach der Einrichtung sammeln diese Programme gezielt sensible Informationen wie Anmeldedaten und Authentifizierungszusätze. Einige Entwickler solcher Schadsoftware preisen nun eine Fähigkeit an, die die Authentifizierungszusätze aktualisieren kann, was Änderungen am Passwort nutzlos macht.



Malware nutzt Schwachstelle in Google API

Eine Untersuchung von IT-Sicherheitsexperten bestätigt, dass diese Fähigkeit keine Finte ist. Mithilfe einer nicht öffentlich dokumentierten Schnittstelle von Google, die ursprünglich für die Synchronisation von Konteninformationen über verschiedene Endgeräte hinweg vorgesehen ist, kann die Malware gültige Cookies für entwendete Konten generieren.

Die Schadsoftware lädt verschlüsselte Zugangstokens durch das API herunter und entschlüsselt sie, wobei sie die im Browser des Opfers entwendeten Schlüssel verwendet.

Passwortwechsel bieten keinen Schutz

Da die Authentifizierungstokens nicht an das Google-Passwort des Nutzers geknüpft sind, bleibt auch ein Passwortwechsel ohne Auswirkung und Täter erlangen weiterhin Zugang zu allen Google-Konten des Opfers, die während der Infektion aktiv waren.

Es ist bisher nicht bekannt, ob und wann Google diese Schwachstelle beheben wird, ebenso unklar ist, ob Nutzer effektive Schutzmaßnahmen ergreifen könnten. Angesichts der Tatsache, dass nun mehrere Schadsoftware-Varianten diesen Exploit nutzen, dürfte bei den Entwicklern von Google Alarmstimmung herrschen.

Probleme mit der Implementierung von OAuth oder das Abfangen von OAuth-Tokens haben bereits in der Vergangenheit zu Sicherheitsproblemen geführt, wie bei einem schwerwiegenden Angriff auf Github im Jahr 2022 deutlich wurde.

Selbst der Wechsel eines Passwortes macht keinen Unterschied

Das müssen Google-Nutzer jetzt tun

Es ist wichtiger denn je, darauf zu achten, sich keine Malware einzufangen. Also: Keine bedenklichen oder unsicheren Webseiten aufrufen, am besten Antiviren-Software benutzen und bei Bedenken mal den Rechner scannen. Sofern Malware entdeckt wurde, diese entfernen und anschließend die Passwörter aller Google-

Konten erneuern.

Ganz besonders wichtig: Multifaktor-Authentifizierung verwenden. Wer seine Online-Konten durch einen zweiten Code oder einen Hardware-Key absichert - was Google schon lange anbietet und auch empfiehlt -, kann seine Online-Konten deutlich besser schützen.

Eigene Benachrichtigungstöne festlegen bei iOS 17.2

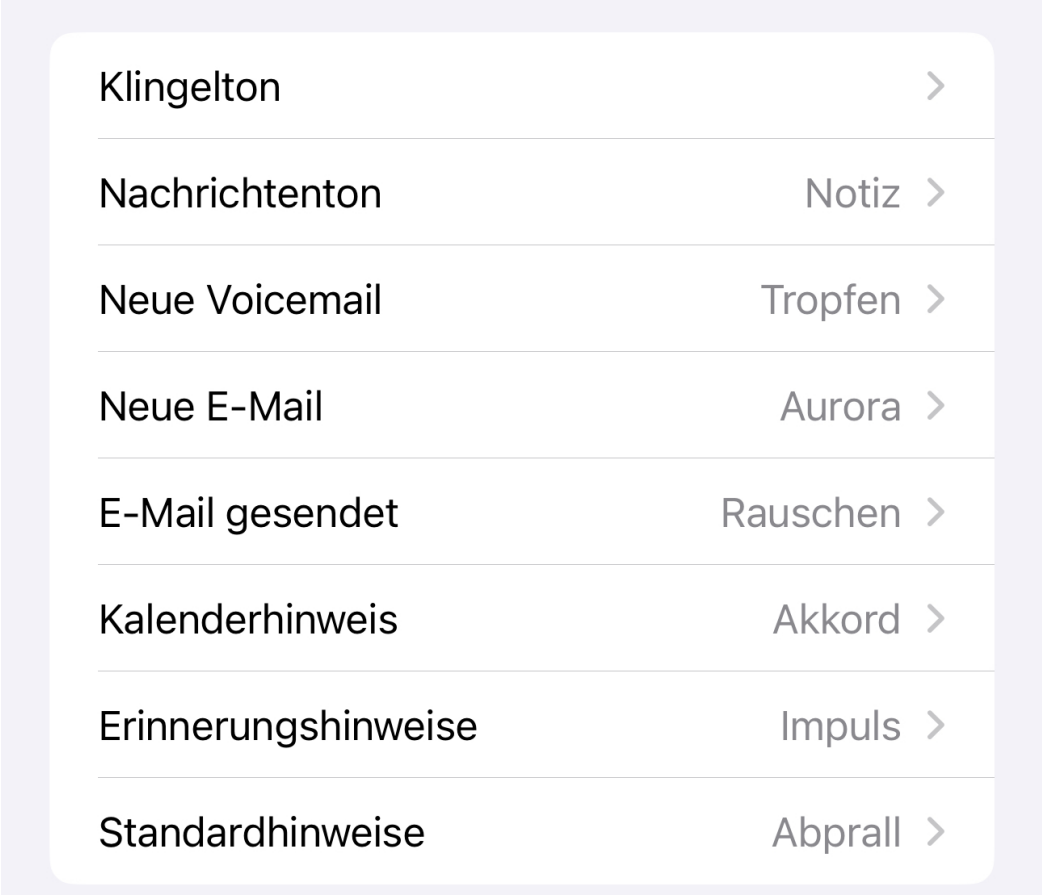
Über viele Jahre hatten iPhones die selben Benachrichtigungs- und Hinweistöne für Systemereignisse. Mit iOS 17 hat Apple diese geändert, nicht zur Freude aller Anwender. Wir zeigen Euch, wie ihr den alten Zustand wiederherstellen könnt!

Welche Töne könnt ihr einstellen?

iOS ist restriktiv, das ist nichts Neues. Das zeigt sich oft auch darin, dass weniger Einstellmöglichkeiten für Systemfunktionen angeboten werden als beispielsweise bei Android. Bei den Tönen war anfangs die Auswahl der Klingeltöne auf die mitgelieferte eingeschränkt, wurde aber dann schnell auch für den Store und GarageBand geöffnet.

Hinweistöne waren lange nur sehr eingeschränkt beeinflussbar, mit iOS 17 hat sich das en wenig geändert. "Ein wenig", weil in der ersten Version hauptsächlich

die Standardtöne geändert wurden. Wer sich also über Jahre an die Standard-Töne gewöhnt hatte, der verpasste Benachrichtigungen, weil er das Piepen seines iPhones nicht mehr auf sich bezog. Erst mit iOS 17.2 ist es möglich, diese Ton-Typen manuell anzupassen.

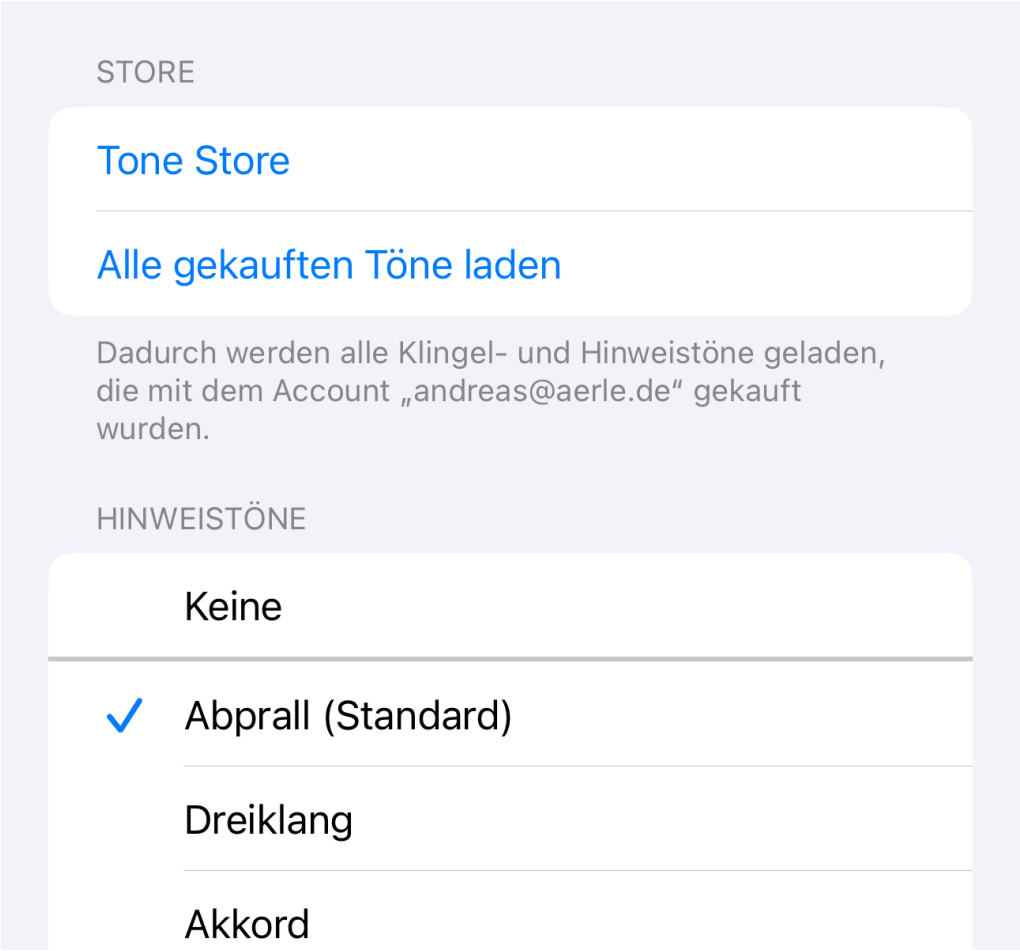


iOS 17.2: Ändern der Benachrichtigungstöne

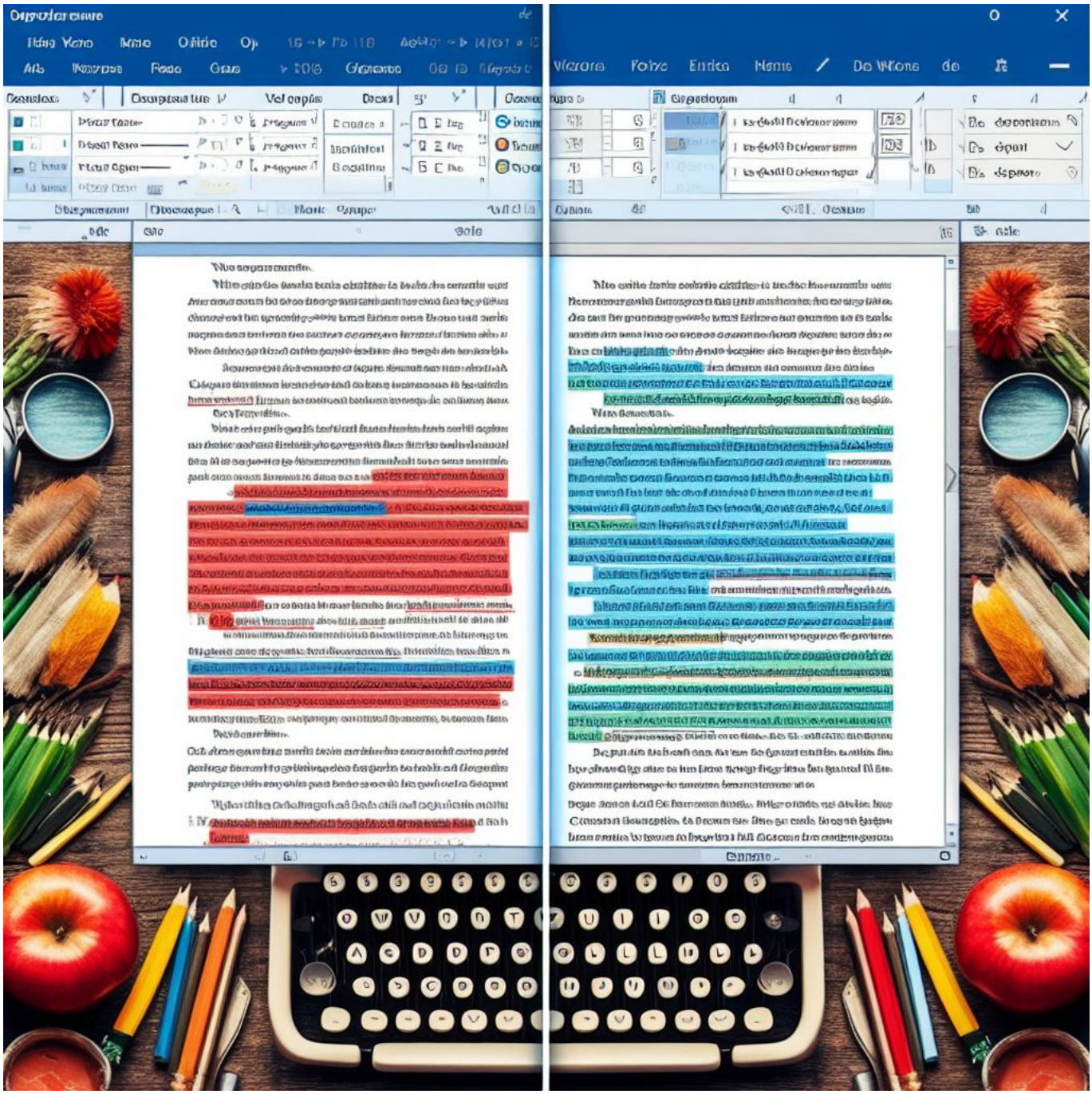
Wenn ihr das iOS 17.2-Update installiert habt, dann könnt Ihr auf diesem Weg die Benachrichtigungstöne verändern:

- Wechselt in die **Einstellungen**.
- Tippt dann auf **Töne und Haptik**.
- Unter iOS 17.2 findet ihr eine neue Option **Standardhinweise**, tippt diese an.
- Darunter könnt ihr aus den bestehenden Tönen auswählen oder über den Ton-Store neue installieren.
- Auch für die anderen Benachrichtigungsereignisse könnt ihr hier eigene Benachrichtigungstöne auswählen.
- Der bisherige Ton ist übrigens der **Dreiklang**, wenn ihr diesen

wiederhaben wollt.



Welches Word-Dokument ist aktueller? Schnelle Vergleiche



Viele Köche verderben den Brei. Das ist nichts Neues, und die Cloud macht es nicht besser: Je mehr Menschen an einer Word-Datei arbeiten, desto mehr Chaos entsteht potenziell. Wir zeigen Euch, wie ihr die richtige Version der Datei findet!

Eigenschaften von Dateien

Der erste Ansatz, zwei oder mehr Dateien miteinander zu vergleichen, ist der Blick auf die Dateieigenschaften. Wie Fotos haben auch Dateien unter Windows viele Metainformationen im Bauch, die euch dabei helfen können. So beispielsweise

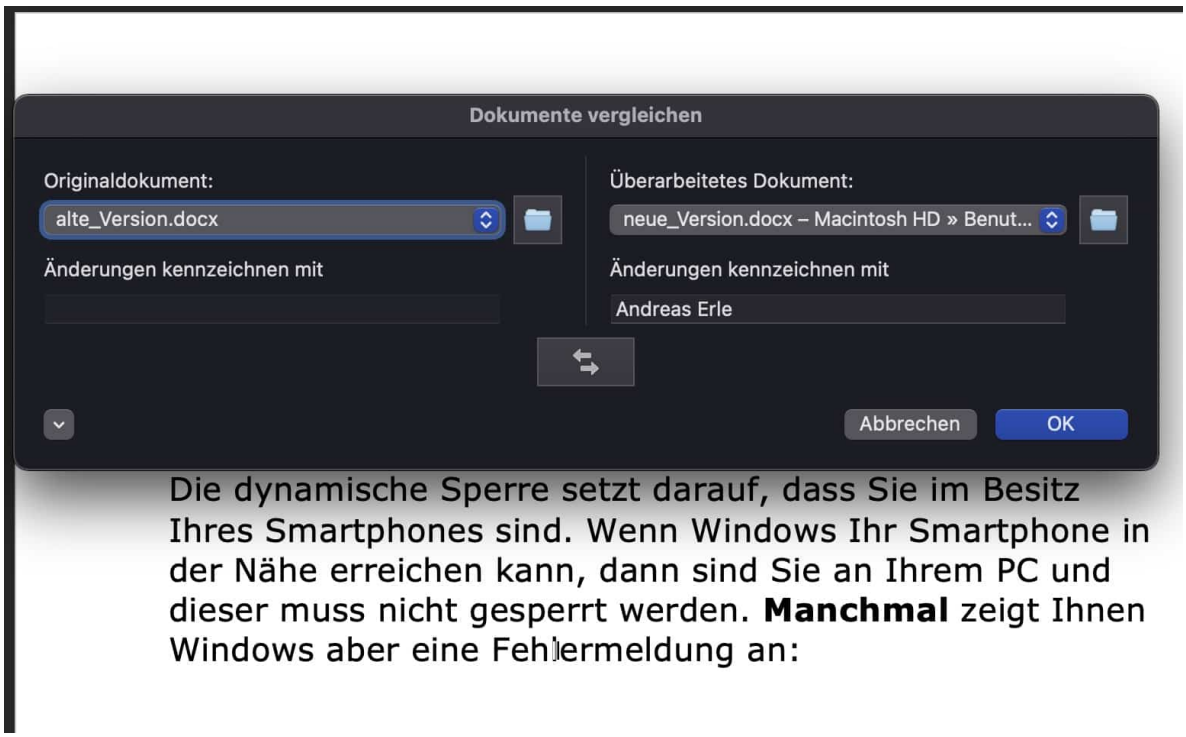
- Name
- Datum und Uhrzeit der letzten Änderung
- Größe

Diese Informationen findet ihr im Windows Explorer, wenn ihr auf **Anzeige** > **Details** klickt. Die Datei mit dem neuesten Datum wurde als letzte verändert und sollte den aktuellsten Stand haben. "Sollte"? Nicht jede Änderung ist absichtlich vorgenommen worden: Wenn die automatische Speicherung aktiviert ist, dann kann schon das Öffnen und Klicken in eine Datei zu einer neuen Version führen. Findet ihr also die gewünschte Dateiversion über den Vergleich der Metadaten nicht heraus, dann müsst Ihr anders herangehen:

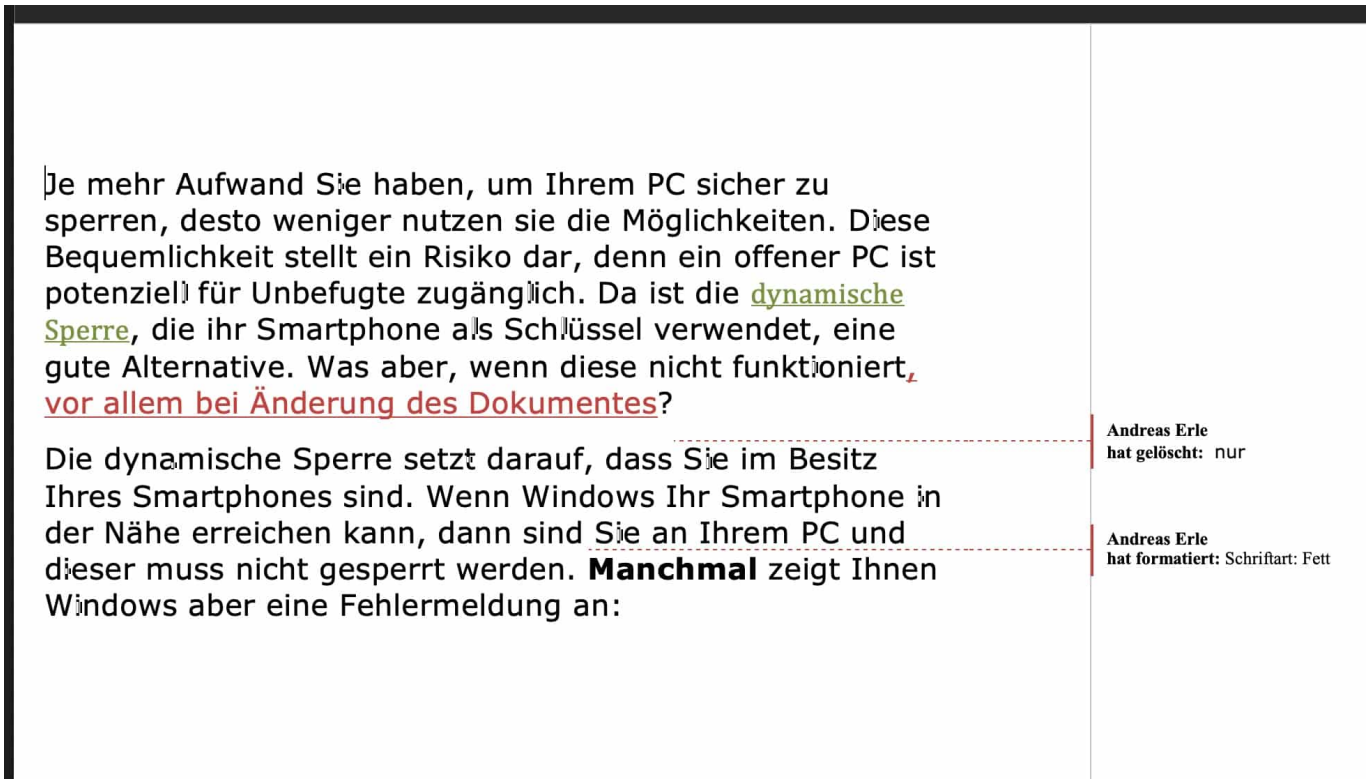
Name	Änderungsdatum	Typ	Größe
WP_20141212_20_57_28_Pro.mp4	12.12.2014 21:32	MP4-Datei	107.957 KB
WP_20141210_19_12_13_Pro.mp4	10.12.2014 19:16	MP4-Datei	10.663 KB
WP_20141119_22_27_26_Pro.mp4	20.11.2014 00:38	MP4-Datei	205.381 KB
WP_20141119_22_05_20_Pro.mp4	20.11.2014 00:04	MP4-Datei	100.444 KB
WP_20141119_21_07_44_Pro.mp4	19.11.2014 23:43	MP4-Datei	120.491 KB
WP_20141116_22_53_07_Pro.mp4	17.11.2014 01:53	MP4-Datei	307.507 KB
WP_20141116_22_09_23_Pro.mp4	17.11.2014 01:07	MP4-Datei	77.041 KB
WP_20141116_22_04_26_Pro.mp4	17.11.2014 00:55	MP4-Datei	74.513 KB
WP_20141116_20_54_37_Pro.mp4	17.11.2014 00:34	MP4-Datei	62.561 KB
WP_20141116_20_00_54_Pro.mp4	17.11.2014 00:24	MP4-Datei	29.596 KB
WP_20141020_20_39_07_Pro.mp4	20.10.2014 23:03	MP4-Datei	4.236 KB
WP_20141015_21_30_19_Pro.mp4	15.10.2014 21:37	MP4-Datei	24.676 KB

Vergleich von Dateiversionen

Wenn Datum und Größe einer Datei nicht zum Vergleich reichen, dann müsst ihr auf die inhaltliche Ebene gehen. Das ist nicht immer ganz so einfach. Word allerdings hat eine eigene Funktion dafür eingebaut: Den Dokumentenvergleich.



- Klickt auf **Überprüfen** > **Vergleichen** > **Dokumente vergleichen**.
- Unter **Originaldokument** wählt das aus, was für Euch die Basis des Vergleiches ist. Das muss nicht die jüngste Version sein, sondern die, die als letzte bearbeitete vorliegt.
- Unter **Überarbeitetes Dokument** wählt die Version aus, die Ihr als neuere Version bekommen habt. Habt Ihr Euch bei der Auswahl vertan, dann könnt Ihr durch den **Doppelpfeil** die Rolle der beiden Dokumente tauschen.
- Nach einem Klick auf **OK** startet Word den Vergleich und zeigt Euch die Änderungen im Dokument an. Diese könnt Ihr jetzt wie gewohnt annehmen oder verwerfen.



Wenn Ihr direkt ein zusammengeführtes Dokument erzeugen wollt, dann geht das direkt über **Überprüfen** > **Vergleichen** > **Dokumente zusammenfassen**.