Schieb Report

Ausgabe 2022.46

Bandbreite teilen: Ganz einfach – aber auch sicher?

Gelegentlich teilen wir unsere Bandbreite: Durch Einrichten eines offenen Hotspots, oder indem wir unser WLAN aufmachen. Das ist relativ einfach - und rechtlich auch weitgehend sicher.

Online gehen zu können, das ist für die meisten von uns heute ungeheuer wichtig, für viele sogar regelrecht lebenswichtig. E-Mails abrufen, Chats absetzen, Nachrichten checken, sich mit Updates versorgen... Aber längst nicht überall gibt es ein Netz. Manchmal nur Mobilfunk, manchmal nur WLAN.

Da hilft es, wenn andere ein bisschen von ihrer Bandbreite teilen. Wenn uns ein offenes WLAN zur Verfügung steht oder der freundliche Sitznachbar an der S-Bahn-Station mal seinen Onlinezugang teilt, weil man selbst kein Netz hat. Bis hin zu Projekten wie Snowflake, wo wir Teile unserer DSL-Kapazität zu Hause mit Menschen im Iran teilen, damit die unzensiert ins Netz können.

Es gibt also viele verschiedene Arten, Bandbreite zu teilen. Doch welche Risiken sind damit eigentlich verbunden?

Freies WiFi: Gibt es nicht nur an öffentlichen Plätzen

Tethering: Einen persönlichen Hotspot einrichten

Es gibt ja Situationen, da hat man selbst Zugang zum Netz – andere aber nicht. Oft die Kinder im Auto. Oder im Ausland, weil die einen Roaming haben, die anderen nicht. Oder, weil jemand ein Tablet benutzt, das nicht online gehen kann. Da kann ich doch auch meine Bandbreite teilen.

Das ist ein Vorgang, den man „Tethering“ nennt. Dazu geht man in die Mobil-Einstellungen seines Gerätes und sucht nach „Persönlicher Hotspot“ unter iOS oder „Hotspot“ unter Android.

Dort kann man festlegen, ob andere über mein Gerät online gehen dürfen. Ob sie quasi meine Mobilfunkverbindung nutzen dürfen, um online zu gehen. Wenn ich das möchte, richte ich einen solchen Hotspot ein, gebe ihm einen Namen und

hinterlege ein Passwort.

Die anderen können dann per WLAN über meinen Hotspot online gehen, sie müssen nur das richtige Passwort eingeben. Es empfiehlt sich, ein gutes Passwort zu nehmen, damit nicht jeder Fremde darüber rein kann. Wenn das einmal eingerichtet ist, geht das schnell und einfach. Aber man sollte im Blick behalten, wie intensiv der Hotspot genutzt wird – wegen des Datenvolumens.

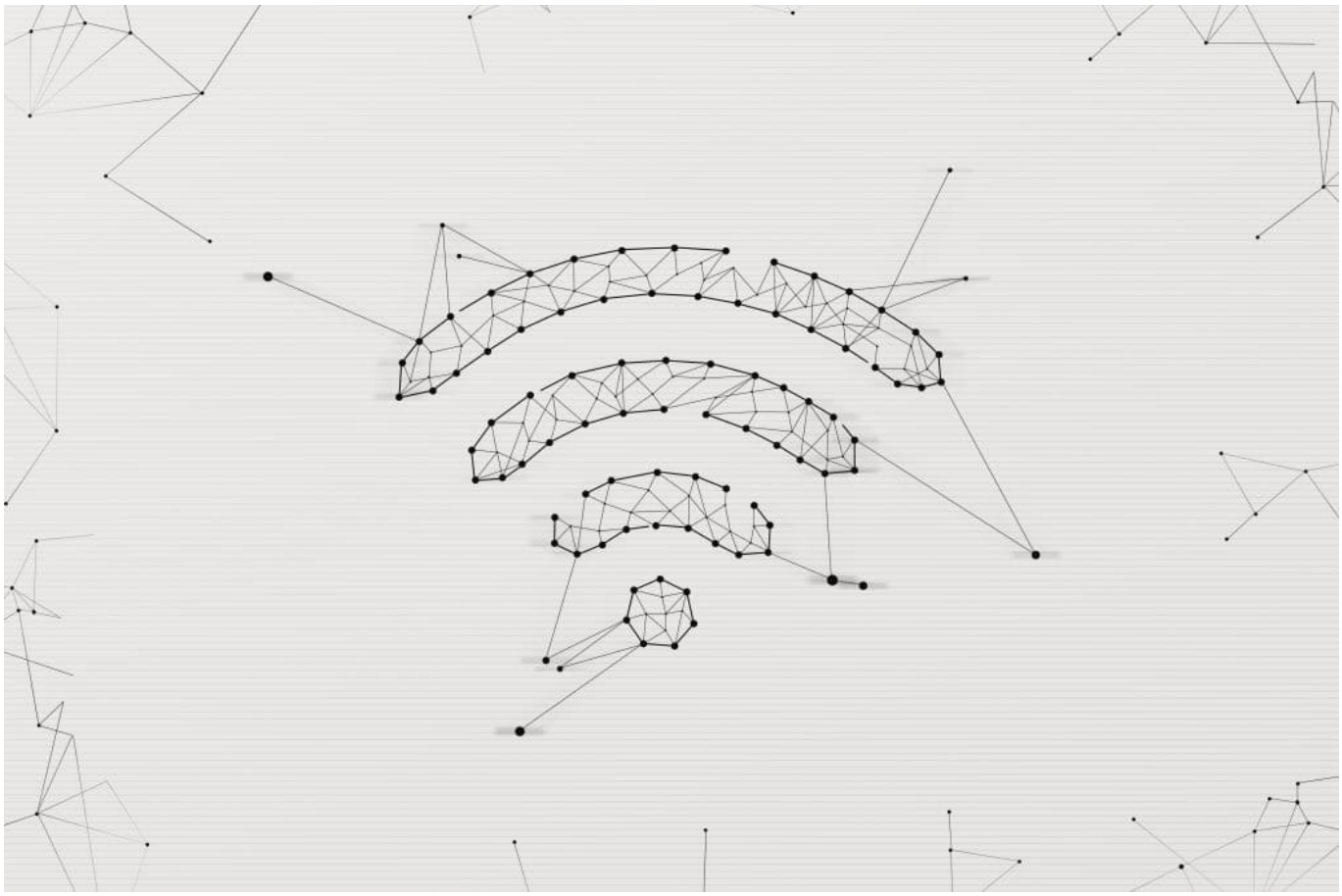
Wer eine Flatrate hat, muss sich da natürlich keine Gedanken machen. Das ist eine prima Lösung, um Familie oder Freunden Zugang zur Onlinewelt zu gewähren. Es gibt auch Geräte, die so etwas anbieten. Die kann man mitnehmen und zB im Urlaub aufstellen. Als WLAN-Hotspot. Meistens dann aber mit eigener SIM-Karte.

Offene WLANs

Es gibt ja auch offene WLANs: In Restaurants, im Bahnhof, teilweise auch in den Innenstädten, damit Menschen schnell und ohne große Kosten online gehen können. Wenn ich zu Hause schnelles Internet habe – wie kann ich das mit anderen teilen?

Da gibt es verschiedene Wege. Moderne Router bieten heute oft die Möglichkeit, einen Gast-Zugang einzurichten. Also quasi ein zweites WLAN. Das erste ist für mich und meine Familie, das zweite für Gäste, etwa die bei mir zu Hause sind – oder auch für Menschen vor der Tür.

Dieses zweite WLAN hat einen eigenen Namen. Und ich kann entscheiden, ob ich es mit Passwort schützen möchte oder nicht. Wenn es ohne Passwort ist, kann natürlich jeder rein. Trotzdem können die Gäste nicht auf meine Rechner oder Daten schauen, denn technisch ist es ein zweites, separates WLAN. Ich teile nur meine Bandbreite mit den Gästen. Oft besteht sogar die Möglichkeit, genau festzulegen, wieviel(!) der Bandbreite ich maximal mit den Gästen teilen möchte, damit ich nicht zu langsam surfe.



Abstract wifi symbol made in low polygonal style over light background, free space

Ich kann natürlich auch meinem Nachbarn mein Passwort verraten, das geht auch. Und wer es mit dem Teilen richtig ernst nimmt, der geht unter die Freifunker. Da kann man Mitglied werden, sich spezielle Software für den WLAN-Router holen und den dann ganz bewusst mit anderen teilen. Ein Projekt, um allen freien Zugang zum Netz zu ermöglichen.

Laut einer jüngsten Studie gibt es weltweit 549 Mio. offene Hotspots. Von den meisten weiß aber niemand. Vielleicht nicht mal die Betreiber selbst. In Europa ist das Land mit den meisten freien Hotspots – Russland. 280.000 Stück. Deutschland steht auf Platz 7 mit 56.000 Hotspots. Vergleichbar schlecht, das muss man sagen.

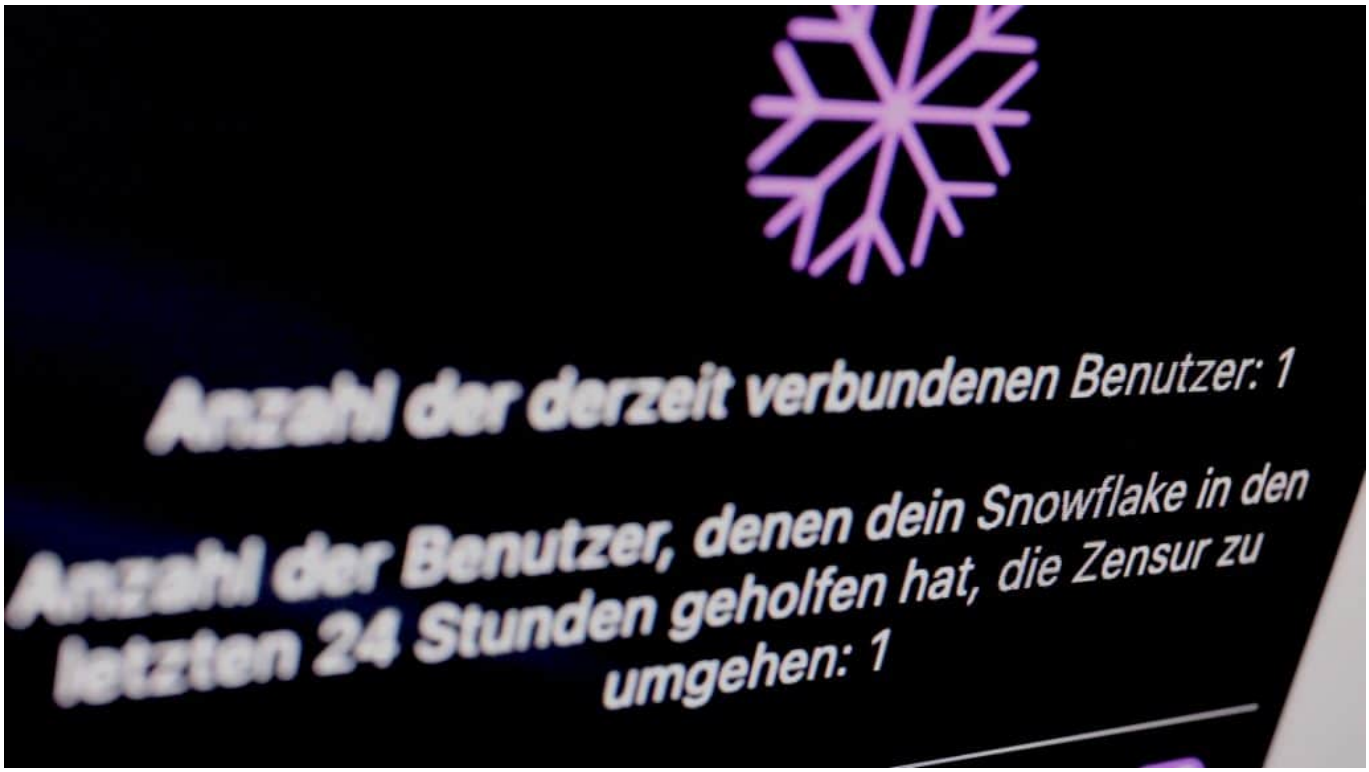
Bandbreite teilen: Juristische Konsequenzen

Aber woran liegt das? Möglicherweise an den juristischen Konsequenzen, die einem drohen können, wenn man einen Zugang frei gibt und andere können darüber online gehen, sie machen aber Unsinn?

Da muss man in der Tat aufpassen. Denn wenn ein Gast zum Beispiel Gesetze bricht, steht irgendwann die Polizei auf der Matte – weil die Spuren zu unserem WLAN-Router führen.

Aber für solche Fälle gibt es die „Störerhaftung“. Lange Zeit mussten Betreiber offener WLANs tatsächlich dann auch haften. Das wurde weitgehend abgeschafft – und hat erkennbar die Bereitschaft erhöhte, offene WLANs anzubieten. Heute muss ein Betreiber eines offenen WLANs kaum juristische Konsequenzen fürchten.

Allerdings müssen im Zweifel Sperren eingeführt werden, ein Missbrauch muss abgestellt werden, wenn er einem bekannt wird. Im Zweifel müsste man dann zB. den Nachbarn aussperren aus dem WLAN.



Die Browser-Erweiterung macht es leicht, seine Ressourcen zu teilen

Projekt Snowflake

Es gibt noch eine andere vielleicht etwas ungewöhnliche Art, eigene Bandbreite zu teilen. Zu Hause oder im Büro zum Beispiel, wenn man im LAN oder WLAN unterwegs ist. Wer mag, kann Bandbreite teilen mit Menschen im Iran oder in anderen Ländern mit eingeschränkten Zugang zum Internet – und ihnen quasi helfen, ins freie Netz zu gehen.

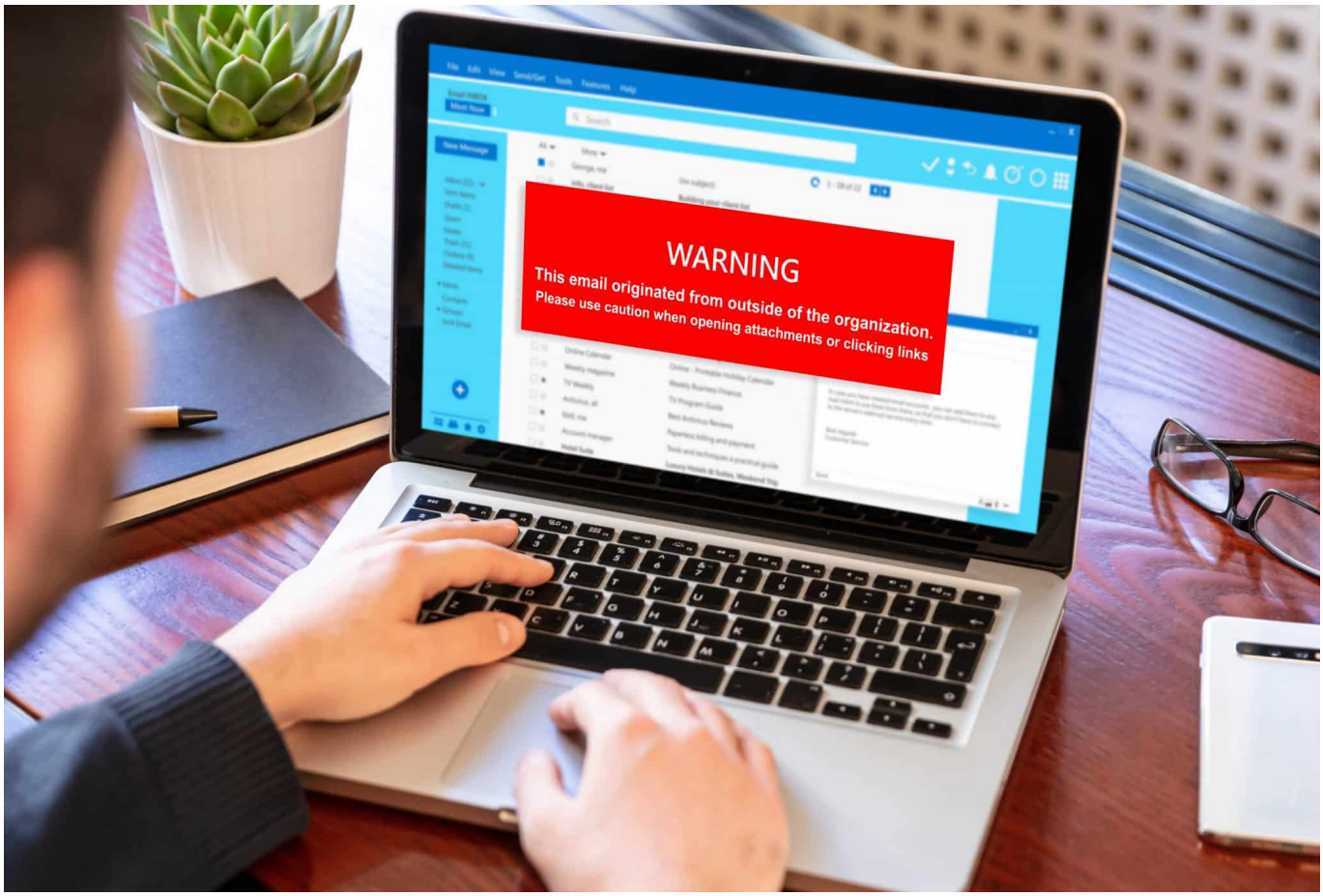
Im Prinzip sehr einfach: Man installiert eine Erweiterung (Plugin) für den Browser, derzeit Firefox und Chrome, namens „Snowflake“. Wenn die eingerichtet ist, können Menschen in Ländern wie Iran, aber auch China, Russland oder anderen Ländern mit zensiertem Internet über meinen Rechner ins unzensierte Netz.

Mein Rechner mit meinem Browser wird quasi zu einer Art Startrampe. Ein ausgeklügeltes System, das die Zensur umgehen hilft, denn mein Rechner steht nicht auf den Sperrlisten der Regierung – die Daten können frei fließen.

Das Ganze gehört zum TOR-Projekt, das unzensiertes und unbeobachtetes Surfen im Netz ermöglicht. Einach zu bedienen. Ich kann jederzeit sehen, wie viele Menschen gerade und in den letzten 24h darüber online gegangen sind.

Wenn ich meine Bandbreite für mich brauche, reicht ein Mausklick, um Snowflake zeitweise abzuschalten. Auch hier gilt: Störerhaftung. Man macht sich praktisch nie strafbar, muss den Dienst nur ggf. abschalten, falls Missbrauch gemeldet wird.

Schutz vor Ransomware: Die Sicherheit dort verbessern, wo sie am wichtigsten ist

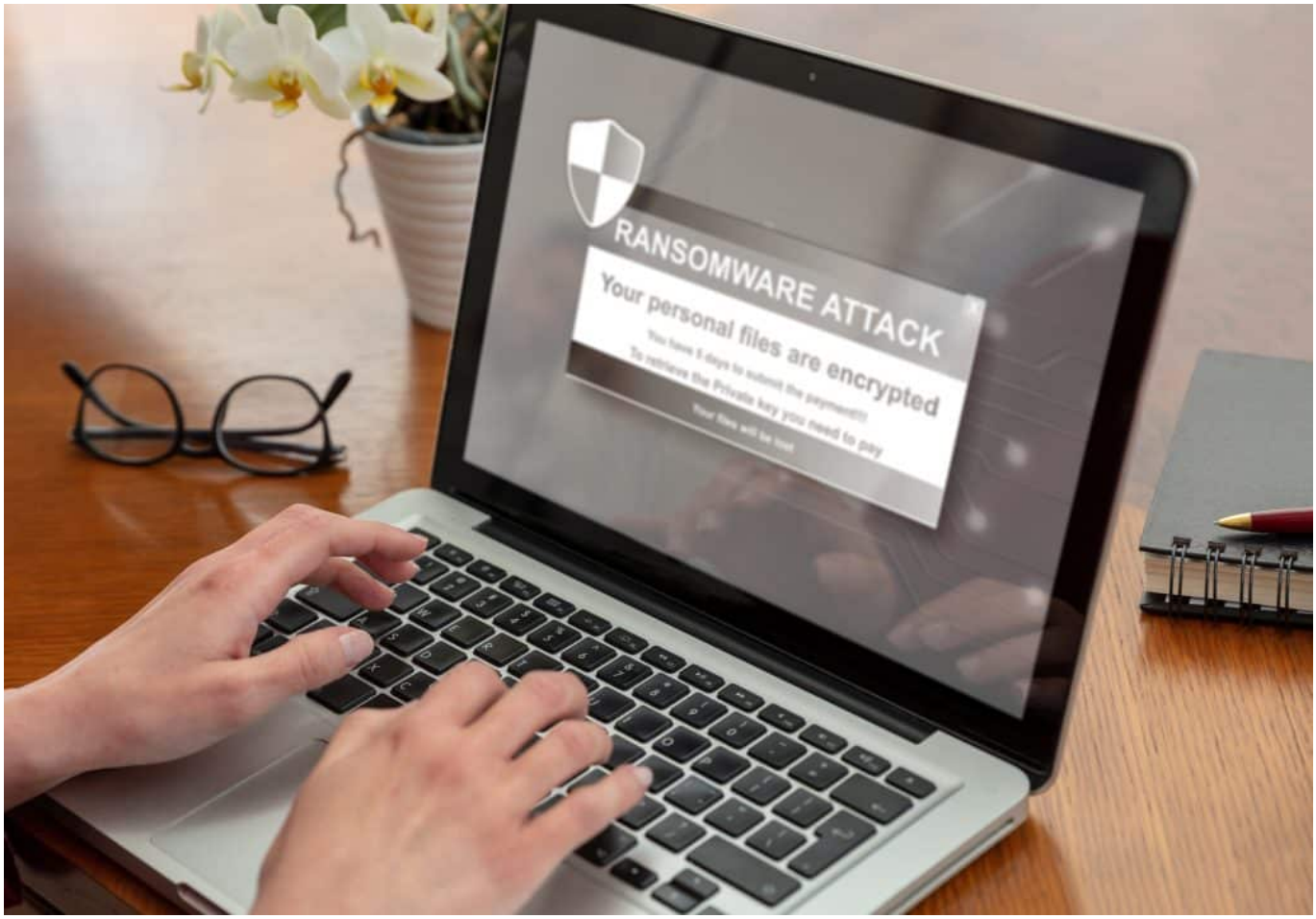


Eine der folgenreichsten Angriffsmethoden aus dem und im Netz sind Ransomware-Angriffe: Daten verschwinden, Geräte und Netzwerke lassen sich nicht mehr benutzen. Ein Albtraum - für Privatleute wie für Unternehmen und Institutionen. Wie sieht möglicher Schutz aus?

Wenn wir über Sicherheitsrisiken und Angriffsmethoden aus dem Netz sprechen, kommen wir nicht umhin, einige Fachbegriffe zu verwenden - um präzise zu sein.

In Zeiten von Ransomware, Insider Threats und Advanced Persistant Threats sind viele Unternehmen in puncto Security in der Defensive. Neben der eigentlichen Abwehr geht es im Kern darum, lange IT-Ausfallzeiten und Datenverluste zu vermeiden. Backups bieten bei der Wiederherstellung weniger wichtiger Daten eine einfache und praktikable Lösung.

Kritische Daten und Workloads benötigen allerdings eine ausgereiftere Wiederherstellungstechnologie. CDP (Continuous Data Protection, kontinuierliche Datensicherung) verbessert die Abwehr gegen Ransomware & Co. genau dort, wo es nicht nur auf Datensicherheit, sondern auch auf eine sehr schnelle Wiederherstellung ankommt.



Ransomware Angriffe haben folgenreiche Schäden

Präventiver Schutz alleine reicht nicht

Im Idealfall würden Ransomware-Angriffe das Netzwerk natürlich gar nicht erst erreichen. Um dieser Wunschvorstellung gerecht zu werden, arbeiten Anbieter von Sicherheitslösungen auch kontinuierlich daran mit den Angreifern schrittzuhalten. Allerdings ist es ihnen noch nicht gelungen, einen hunderprozentigen Schutz gegen neue Sicherheitsbedrohungen wie APTs (Advanced Persistent Threats) und Zero-Day-Exploits zu finden.

Aus der kürzlich veröffentlichten IDC-Studie The State of Ransomware and

Disaster Preparedness: 2022 geht hervor, dass 93 Prozent aller Unternehmen in den vergangenen 12 Monaten datenbedingte Störungen des Geschäftsbetriebs verzeichnet haben. Und 67,8 Prozent der befragten Unternehmen hatten über ein Kalenderjahr gar vier oder mehr solcher Unterbrechungen.

Die IT-Sicherheit stellt die erste Verteidigungslinie dar und ist offensichtlich nicht in der Lage, alle Angriffe abzuwehren. Entsprechend müssen sich alle Unternehmen für das Worst-Case-Szenario eines erfolgreichen Angriffs wappnen. Um sich auf einen erfolgreichen Angriff vorzubereiten, stützen sich die meisten Unternehmen auf eine altbekannte Technologie zur Wiederherstellung, die sie bereits implementiert haben: Backups.

Backups alleine garantieren keine schnelle Wiederherstellung

Organisationen nutzen Backups bereits seit langem als Standardtool zur Datensicherung ihrer Daten. Die Ansätze traditioneller Backups haben sich vom magnetischen Tape-Storage der 1950er bis zum modernen Cloud-Backup in den letzten Jahrzehnten auch überraschenderweise fast nicht verändert: Daten werden in festgelegten Intervallen auf einen zweiten Datenträger oder Datenort kopiert.

Zwar sind längere Intervalle mit Datenverlust verbunden, doch lassen sich mit der heute fast überall umgesetzten 3-2-1-Backup-Strategie in den allermeisten Fällen so gut wie alle Daten wiederherstellen. Backups haben jedoch die Schwäche, dass sie lediglich einzelne Server schützen, jedoch nicht komplette Applikationen als Ganzes, welche ja meist aus verschiedenen Komponenten (z.B. Datenbank, Webserver) bestehen.

Das Resultat dieser silo-basierten Fokussierung auf einzelne Server sind tage- bis wochenlange Wiederherstellungszeiten. Denn nach der Wiederherstellung der Daten muss eine funktionierende Applikation erst wieder manuell aus ihren zahlreichen Bestandteilen zusammengebaut werden. Es überrascht daher nicht, dass die meisten Unternehmen kein Vertrauen in ihre gegenwärtigen Backup- und DR-Lösungen haben.

Lediglich 28 Prozent der Befragten gaben im Rahmen der IDC-Studie an, dass sie

davon überzeugt sind, dass ihr Backup-System alle Daten zeitnah wiederherstellen können.

Angriffsmethoden werden immer ausgefeilter

Der vemeintliche Trade-Off: Komplexität verringern oder Sicherheit weiter erhöhen?

72 Prozent der Unternehmen erwarten mit ihrem auf Backups basierenden Ansatz folglich, dass sie ihre wichtigen Daten bei einem erfolgreichen Ransomware-Angriff nicht zeitnah wiederherstellen können. Dies ist natürlich langfristig kein tragbarer Zustand.

Die für Datensicherheit Zuständigen dieser Unternehmen suchen daher nach Möglichkeiten, ihre löchrige Strategie zu verbessern, damit sie Daten und Workloads schneller wiederherstellen können. Idealerweise sollte dies geschehen, ohne dabei die bereits hohe Komplexität der zahlreichen ineinandergreifenden Sicherheitslösungen noch weiter zu erhöhen.

Zu diesen Lösungen gehören neben den Backups auch spezielle Recovery-Software, Snapshots, Spiegelungen und Storage-basierte Replikationen sowie weitere **Disaster-Recovery-Strategien**. Diese mehrschichtige

Sicherheitsumgebung soll die Wiederherstellung von Daten bei Ausfällen gewährleisten.

Entsprechend würden Verantwortliche diesen komplexen Flickenteppich von Sicherheitslösungen am liebsten konsolidieren. Da Backups allein für eine schnelle Wiederherstellung jedoch nicht ausreichen, haben Unternehmen eine klaffende Sicherheitslücke in ihrer Abwehrreihe. Es gilt also strategisch abzuwägen, wie wichtig es für ein Unternehmen ist, größeren Datenverlust und lange Ausfallzeiten zu vermeiden.

CDP-basierte Lösungen eliminieren Komplexität und erhöhen die Sicherheit

In den meisten Unternehmen wäre die Abwägung für oder gegen eine Lösung zur Schliessung dieser Sicherheitslücke eindeutig: Laut IDC belaufen sich die durchschnittlichen Kosten für Ausfälle branchenübergreifend auf 250.000 US-Dollar pro Stunde.

Wenig überraschend gehen deshalb immer mehr Unternehmen dazu über, DR-Lösungen zur schnelleren Wiederherstellung ihrer wichtigsten Daten und Workloads einzusetzen, um diese Lücke zu schliessen. Das schöne daran ist, dass mit einer CDP-basierten Software-Lösung diese Unternehmen dann nicht nur effektiver geschützt sind, sondern oftmals auch Komplexität in ihrem bisherigen Lösungs-Stack abbauen können. Denn mit einer agnostischen CDP-Lösung wird weder mit Agenten noch mit Snapshots gearbeitet und es bestehen auch keine Hardware-Abhängigkeiten oder umfassende Schulungs- und Administrationsaufwände.

Auch haben diese Lösungen keinerlei Einfluss auf einen performanten Applikationsbetrieb und können so alle Datenänderungen erfassen, wenn sie geschrieben werden. So verringert sich der RPO auf Sekunden und Lücken bei der Sicherung, die zu den Hauptursachen für Datenverluste zählen, werden geschlossen. CDP macht es möglich, in Sekundenschnelle ohne nennenswerten Datenverlust zu einem Punkt zurückzukehren, der nur wenige Sekunden vor einem Angriff oder einer Störung lag, vollkommen unabhängig von der jeweiligen Ursache des Problems.

Fazit: Die Sicherheit mit CDP dort verbessern, wo sie am

wichtigsten ist

Angesichts der allgegenwärtigen Bedrohung und zahlreicher neuer Anwendungen, die im Core-, Cloud- und Edge-Bereich eingesetzt werden, sehen sich IT-Organisationen mit einer zunehmenden Komplexität bei der Implementierung von Datensicherheit- und Disaster Recovery-Lösungen konfrontiert. Mit CDP als letzte Evolutionsstufe von Recovery-Lösungen können Unternehmen ihre Sicherheit dort strategisch verbessern, wo sie am wichtigsten ist: Bei den wichtigsten Unternehmensdaten und den unternehmenskritischen Workloads.

Helft mit gegen Phishing!

Phishing ist ein immer schlimmer werdendes Übel. Auf unterschiedlichen Wegen versuchen Übeltäter, an Eure Zugangsdaten zu gelangen und diese entweder selbst zu verwenden oder in großem Stil zu verkaufen. Phishing E-Mails zu erkennen, ist nur die eine Seite der Medaille. Wichtig, um Euch zu schützen, aber Ihr könnt mehr tun: Beteiligt Euch aktiv an der Meldung von Phishing E-Mails!

"Tue Gutes und rede darüber"!

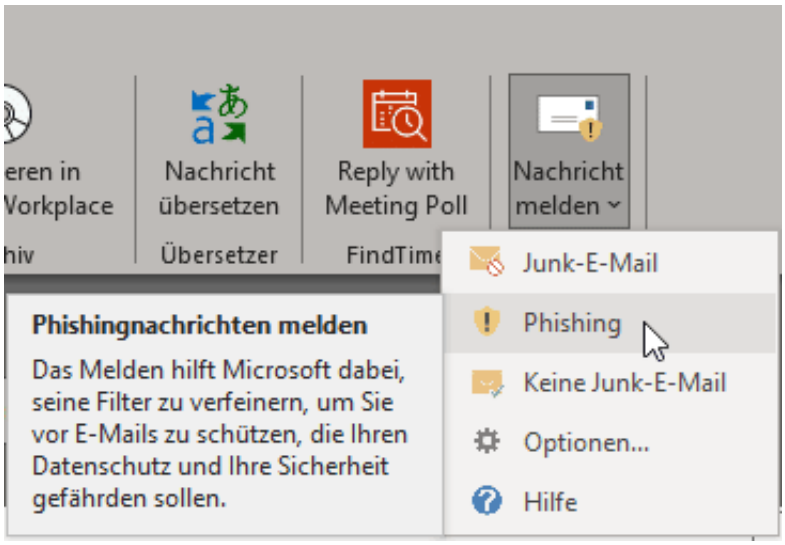
Am Ende sitzen alle Anwender im gleichen Boot: Unsere Daten sind wertvoll und schützenswert und der Schaden trifft jeden Anwender gleich. Warum sollen also andere Anwender in eine Falle tappen, die schon ein andere Anwender erkannt hat? Wäre es nicht viel sinnvoller, Phishing-E-Mails nicht einfach zu löschen, sondern an eine zentrale Stelle zu melden? Etwas Ähnliches bietet Microsoft schon mit dem Cloudbasierten Schutz im Windows Defender, wenn es um die Erkennung von Viren geht: Informationen von allen teilnehmenden PCs werden an einen Microsoft-Server geschickt, der dann wieder seine Informationen über neue Bedrohungen allen teilnehmenden PCs zur Verfügung stellt.

Für Phishing-E-Mails macht das ebenfalls Sinn: Diese kommen in Wellen, in denen die einzelnen E-Mails relativ ähnlich zueinander sind. Die Systematik dahinter können die Betreiber der E-Mail-Dienste wie Microsoft oder Google

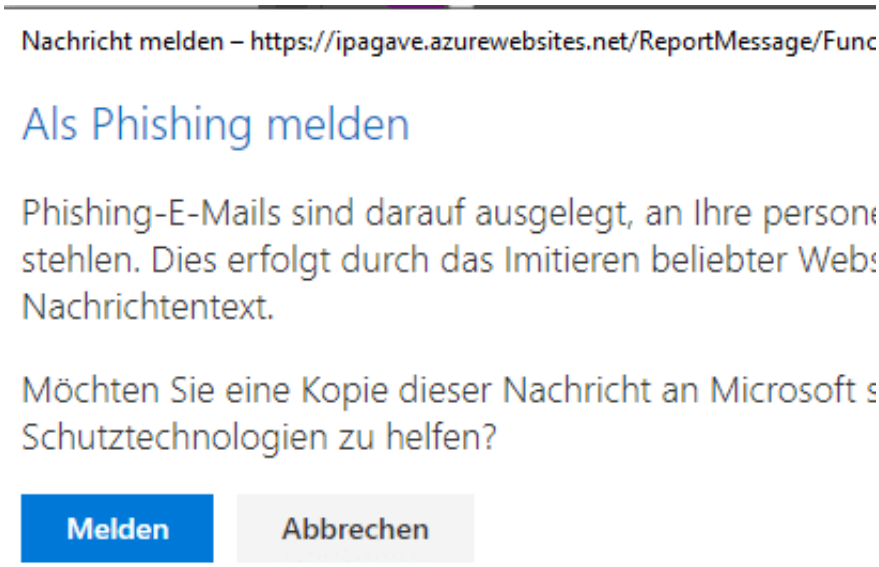
analysieren und die automatische Phishing-Erkennung damit verbessern.

Phishing-Meldung in Outlook

In allen Versionen von Outlook ist die Junk-Erkennung und die Konfiguration des Junk-E-Mail-Filters bereits integriert. Die regelt aber nur den Umgang mit SPAM-E-Mails, nicht mit Phishing E-Mails. Diese Funktion ist erst mit den aktuellen Versionen von Outlook 365 integriert worden.



- In den unterstützten Versionen von Outlook findet Ihr oben rechts in der Symbolleiste ein Symbol **Nachricht melden**.
- Gegebenenfalls müsst Ihr bei einer großen Symbolleiste das Outlook-Fenster maximieren, um das Symbol zu sehen.
- Klickt in der Phishing-E-Mail auf **Nachricht melden**.
- Die E-Mail wird an Microsoft gesendet und dort verarbeitet.
- Nach einigen Sekunden müsst Ihr noch einmal in dem erscheinenden Info-Fenster auf **Melden** klicken.
- Die E-Mail wird dann direkt aus Eurem Posteingang gelöscht, damit Ihr nicht mehr in Gefahr geratet, einen Link darin anzuklicken.



Phishing-Meldung bei GMail und anderen

Die meisten E-Mail-Anbieter, die einen Zugang über eine Weboberfläche Zugang zu den E-Mails bieten, erlauben die Meldung von Phishing E-Mails über diese Oberfläche. Bei GMail funktioniert das beispielsweise so:

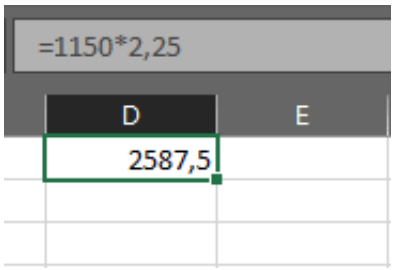
- Öffnet die E-Mail aus dem Posteingang.
- Klickt auf die drei Punkte oben rechts in der E-Mail.
- Wählt im Menü die Option **Phishing melden** aus.
- Ihr müsst diese Meldung noch einmal bestätigen, dann geht die E-Mail an das Sicherheits-Team von Google und wird dort verarbeitet.

Rechnen in Excel und OneNote

Ihr arbeitet an einer Tabelle in Excel oder einer Notiz in OneNote, listet darin Zahlenwerte auf, und müsst diese zusammenrechnen. Statt dafür den Windows-Taschenrechner zu verwenden, könnt Ihr das in den Programmen selber machen!

Berechnungen in Excel

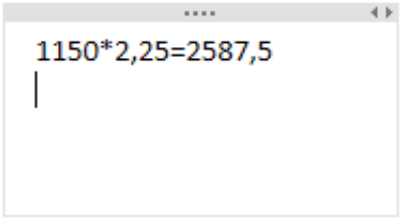
Excel ist ja schon von seiner eigentlichen Aufgabe prädestiniert für die Berechnung von Rechenaufgaben. Die Funktion der Berechnung findet Ihrin den Formeln. Die können über die Symbolleiste über **Formeln** einfügbar. Für einfachere Berechnungen aber könnt Ihr sie auch manuell eingeben: Eine Formel in Excel beginnt immer mit einem **=**, danach folgen - wie bei einem Taschenrechner - die Berechnungsschritte.



Wenn Ihr die Eingabetaste drückt, dann trägt Excel statt der "Rechenaufgabe" den berechneten Wert ein. Die Formel an sich ist aber nicht verloren: Wenn Ihr eine Zelle anklickt, dann erscheint über der Tabelle in der Bearbeitungszeile immer noch die Formel, die Ihr beliebig ändern könnt.

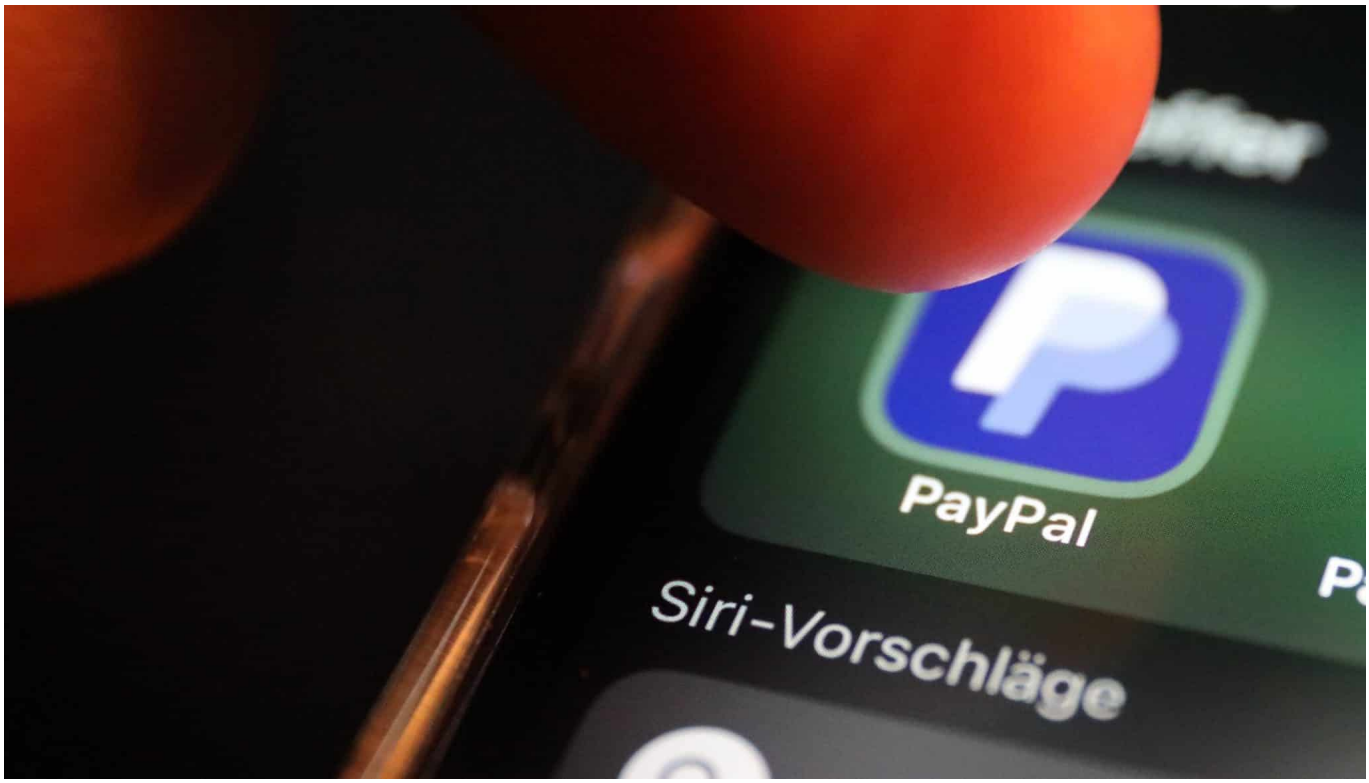
Berechnungen in OneNote

OneNote ist die Notizenapp von Microsoft und hat eigentlich wenig mit Zahlen und Berechnungen zu tun. Trotzdem könnt Ihr schnell Berechnungen durchführen: Gebt in einem Textfeld eine Rechenaufgabe ein und beendet diese mit dem **=-Zeichen**.



Wenn Ihr dann die Eingabetaste drückt, dann analysiert OneNote die Elemente der Berechnung. Sind diese auswertbar, dann fügt die App automatisch das Ergebnis hinter dem Gleichheitszeichen an.

Paypal: Bis zu 10 EUR Gebühren für inaktive Konten



Der bekannte Zahlungsanbieter für Online-Transaktionen will inaktive Konten mittelfristig auflösen und unter bestimmten Umständen auch Gebühren kassieren.

„Benutzen Sie Ihr Konto, um eine Gebühr für Inaktivität zu vermeiden“, heißt es in einer E-Mail, die der Zahlungsabwickler Paypal aktuell an alle Nutzer verschickt, die ihr Konto für längere Zeit nicht genutzt haben.

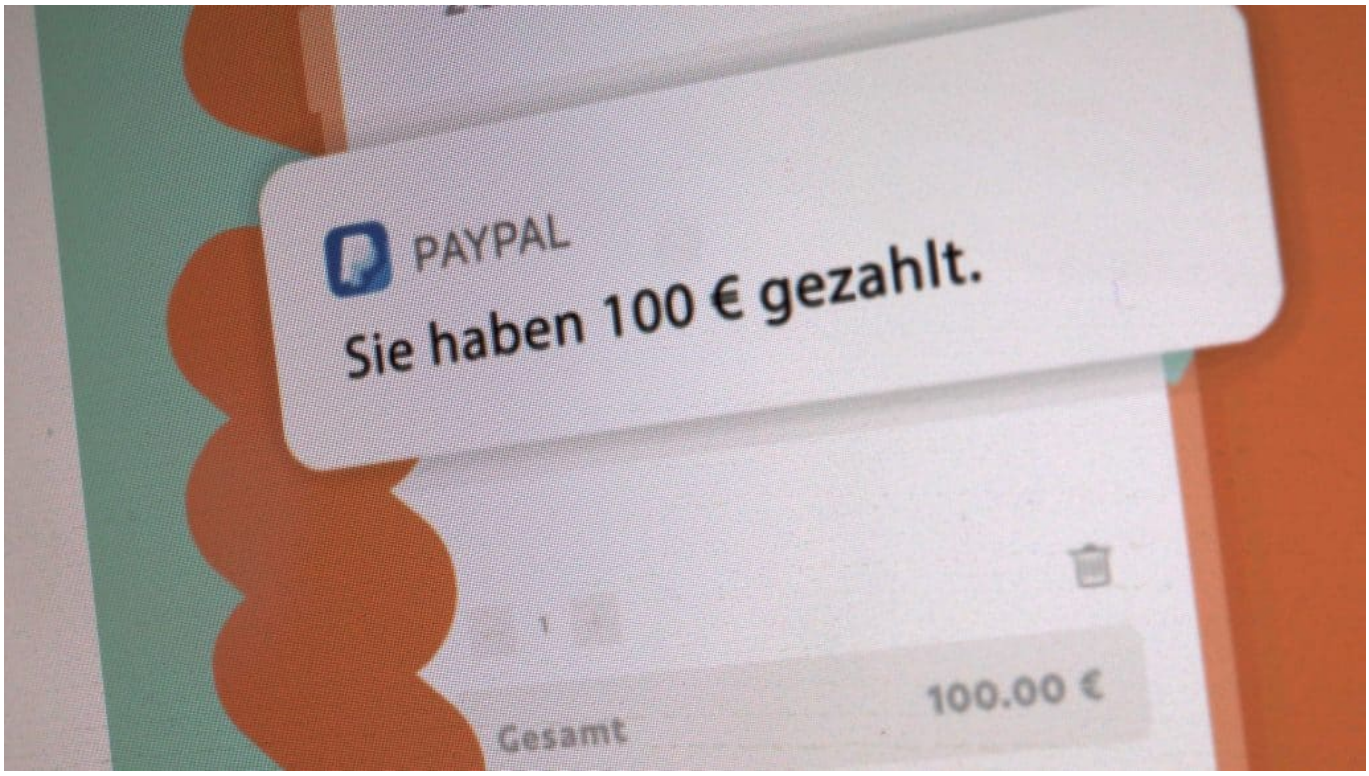
Ein Hinweis auf eine veränderte Situation. Denn Paypal hat gerade weltweit seine allgemeinen Nutzungsbedingungen angepasst: Nach den neuen Regeln kann Paypal bei inaktiven Konten eine Gebühr erheben. Das betrifft nicht nur Händler (da gibt es das bereits seit 2020), sondern jetzt auch alle Privatleute. Diese „Inaktivitätsgebühr“ genannten Kosten können bis zu 10 EUR betragen.

Inaktive Konten werden benachrichtigt

Seit Montag verschickt Paypal entsprechend lautende Hinweise an Nutzer, deren Konten „als inaktiv eingestuft“ wurden. „Inaktivität liegt vor, wenn Sie sich nicht in

Ihr Paypal-Konto eingeloggt oder Ihr PayPal-Konto anderweitig genutzt haben, um Geld zu senden, zu empfangen oder abzubuchen“, erklärt Paypal.

Betroffen sind laut neuen Regeln, die automatisch in Kraft treten, ausschließlich Konten, die in den letzten 12 Monaten inaktiv waren – also überhaupt nicht benutzt wurden. Wer zumindest einmal Geld überwiesen oder etwas bezahlt hat, muss keine Gebühren befürchten.



Wer regelmäßig etwas mit PayPal bezahlt, braucht keine Gebühren zu befürchten

Bis zu 10 EUR Gebühr

Berechnet werden bis zu 10 EUR pro Jahr. Aber auch nur dann, wenn das Konto ein Guthaben aufweist. Konten ohne Guthaben werden keine Gebühren berechnet. Bei Guthaben unter 10 EUR wird maximal das aktuelle Guthaben berechnet, bei Guthaben über 10 EUR maximal 10 EUR. Das Konto kann also nicht ins Saldo gehen.

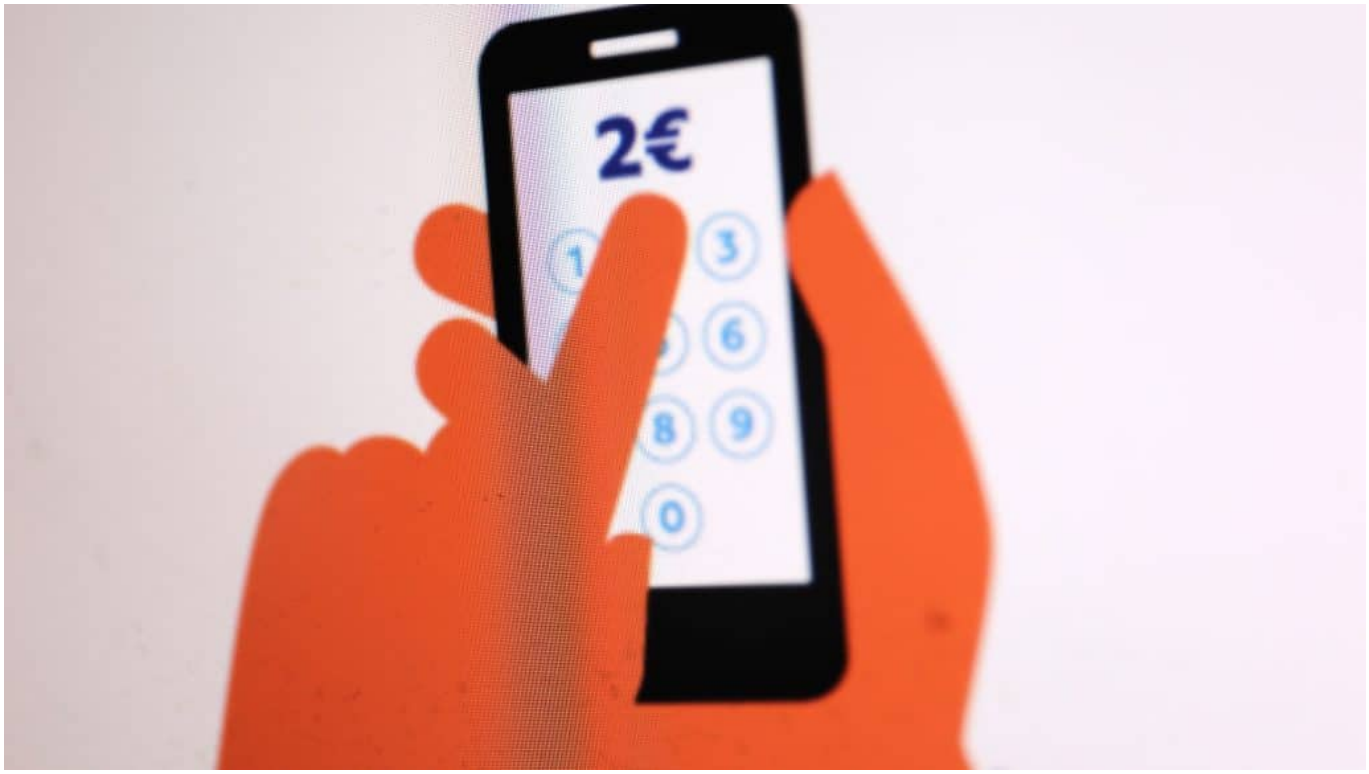
Wenn ein Konto nach Belastung der Inaktivitätsgebühr kein positives Saldo (also Guthaben) mehr aufweist und weitere 60 Tage nicht benutzt wird, dann löst Paypal das Konto auf. Es wird geschlossen.

Inaktive Konten werden benachrichtigt

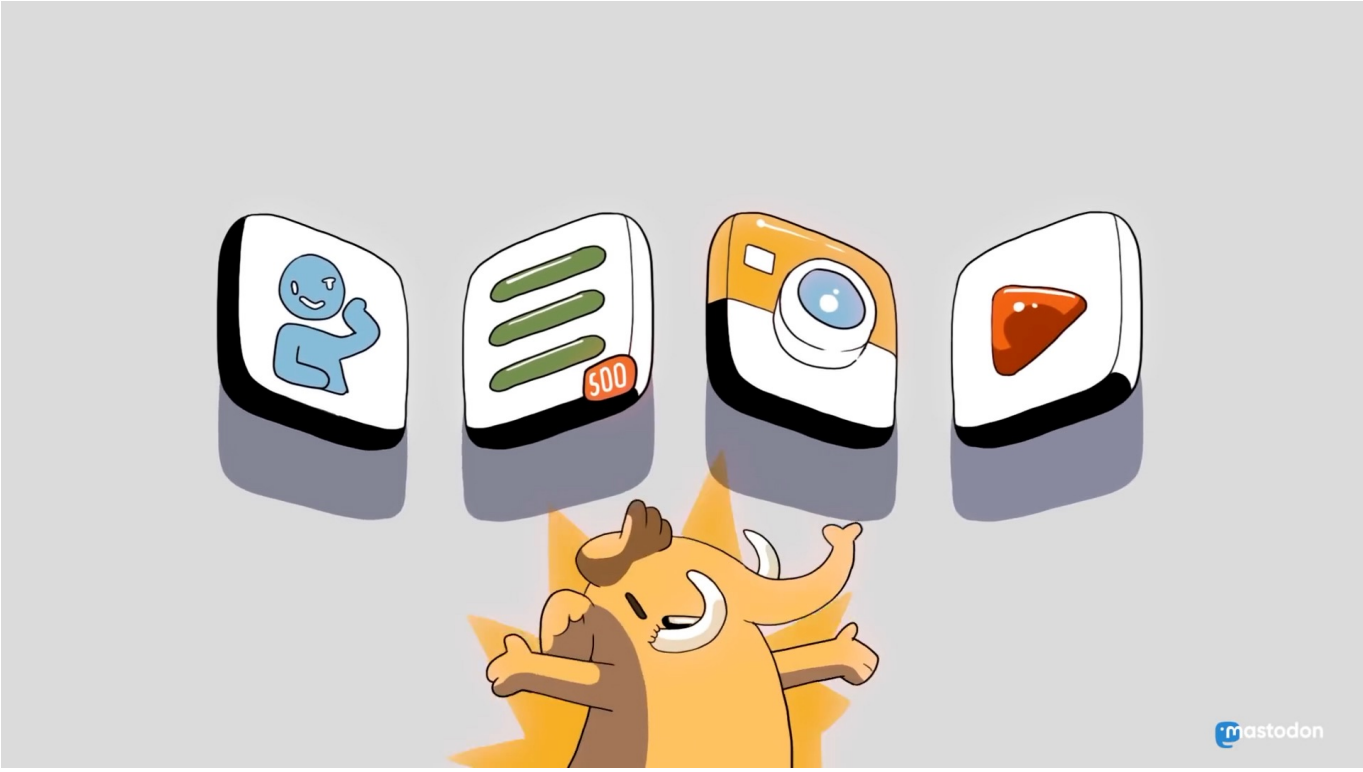
Die Inaktivitätskosten lassen sich schon durch ein einfaches Anmelden im Paypal-Konto vermeiden. Ebenso durch eine Überweisung an Freunde oder durch einen Kaufprozess oder durch Anweisung eines Guthabens auf ein eigenes Konto. Jede Form von Aktivität sorgt dafür, dass keine Inaktivitätsgbühr berechnet wird.

In vielen Ländern treten die neuen Regeln sofort in Kraft. In einer Fußnote weist Paypal darauf hin, dass private Konten, die in Deutschland, Österreich, Italien, Griechenland, Ungarn und Polen registriert sind, von der Inaktivitätsgebühr in diesem Jahr (2022) noch befreit sind.

Die Gebühr dürften dann ab 2023 eingehoben werden. "In Deutschland, Österreich, Italien, Griechenland, Ungarn und Polen registrierte Privatkonten sind von der Erhebung der Inaktivitätsgebühr für 2022 ausgenommen", heißt es in der Erklärung.



Toots und Tröts: So klappt der Einstieg bei Mastodon



Spätestens, seitdem Elon Musk bei Twitter die Kontrolle übernommen hat, denken viele darüber nach, Twitter zu verlassen. Aber ganz ohne Twitter? Da gibt es doch Mastodon - als "Alternative" gehandelt. Das musst Du wissen.

Mastodon sieht zwar in punkto Bedienung und Handhabung Twitter durchaus ähnlich, ist aber trotzdem fundamental anders - mit damit verbundenen Vor-. und Nachteilen.

Mastodon ist strikt dezentral aufgebaut. Twitter ebenso strikt zentral.

Bedeutet: Während Twitter eine Zentrale hat, wo alle Daten zentral gespeichert werden (etwa Nutzerdaten, Protokolle, Inhalte etc.), ist Mastodon dezentral aufgebaut. Es gibt - mittlerweile - Tausende von unabhängigen Knotenpunkten (Instanzen). Technisch gesehen Server, die mit der Software Mastodon laufen - und von Privatleuten, Institutionen oder Firmen betrieben werden. All diese Instanzen sind miteinander verbunden.

Der Mammut "Mastodon" ist das Maskottchen des gleichnamigen Dienstes

Twitter ist kommerziell. Mastodon basiert auf OpenSource und Communites.

Hinter Twitter steht ein (bislang) börsennotiertes Unternehmen mit Tausenden Mitarbeitern. Ziel der Veranstaltung: Gewinn erwirtschaften. Wie bei den meisten Online-Diensten heutzutage in erster Linie mit Werbung - mit all den damit verbundenen Seiteneffekten. So werden Daten erfasst, gespeichert und ausgewertet. Mehr, als den Menschen lieb ist.

Twitter wird von einem Mann "regiert". Mastodon dezentral von Tausenden.

Elon Musk hat sich vollständige Machtbefugnisse gesichert - und übt diese auch aus. Mastodon ist durch seine vollständig dezentrale Struktur komplett anders

organisiert. Jede einzelne Instanz wird separat geführt: Mit eigenen Regeln, die

auch vom Betreiber der jeweiligen Instanz durchgesetzt werden müssen.

Bei Twitter bestimmen Algorithmen die Inhalte. Bei Mastodon die Nutzer.

Twitter zeigt Postings chronologisch sortiert an, in der Regel von Konten, denen man folgt. Doch die Algorithmen präsentieren auch Inhalte, die von den Algorithmen ausgewählt werden - weil sie als interessant eingeschätzt werden.

Twitter-Nutzer erhalten bei entsprechenden Einstellungen sogar Hinweise per E-Mail, welche neuen Postings veröffentlicht wurden. Das gibt es bei Mastodon nicht. Nutzer bekommen ausschließlich Inhalte von Nutzern gezeigt, mit denen

man verbunden ist.

Twitter präsentiert Werbung. Mastodon nicht.

Viel mehr ist dazu nicht zu sagen. Twitter ist werbefinanziert, Mastodon spendenfinanziert.

Twitter beschränkt Postings auf 280 Zeichen. Mastodon auf 500 Zeichen.

Tweets sind heute maximal 280 Zeichen lang (anfangs waren es weniger, so viele wie in eine SMS passen). Mastodon beschränkt Postings auf 500 Zeichen. In beiden Netzwerken können Texte, Bilder und Videos gepostet werden. Oder auch Umfragen eingerichtet werden. Wer auf Twitter postet, erreicht alle Menschen. Bei Mastodon können Nutzer bei jedem einzelnen Posting individuell entscheiden, wer es sehen soll: Alle, nur Follower oder nur bestimmte Personen. Das bietet maximale Flexibilität.

Auf Twitter gibt es Tweets, auf Mastodon Toots (Tröts).

Einzelne Postings auf Twitter werden "Tweets" genannt (Gezwitscher), unter Mastodon "Toots" (Tröts). Das ist dem Maskottchen geschuldet, das Mastodon hat: eine Art Elefant. Denn "Mastodon" ist ein Mammut mit Rüssel.

https://www.youtube.com/watch?v=GSBrJwZbjUA&t=553s

Anmelden bei Mastodon

Wer sich bei Mastodon anmelden möchte - was kostenlos und unverbindlich ist -, muss wissen: Der Anmeldeprozess ist etwas mühsamer als bei Twitter. Und das aus einem ganz einfachen Grund: Ihr habt die Qual der Wahl. Und zwar die Qual der Wahl, bei welcher Instanz Ihr Mitglied werden wollt - um im Mastodon-Netzwerk dabei zu sein.

Es ist so, als wolltet Ihr der Gruppe "Tennisspieler" angehören - und müsstet überlegen, in welcher Stadt, in welchem Verein Ihr Euch anmelden wollt. Genauso ist es bei Mastodon: Es gibt mittlerweile über 6.000 Server/Instanzen. Nicht überall kann sich jeder anmelden. Manche funktionieren auf Einladung. Andere stehen jedem zur Verfügung.

In jeder Instanz gelten andere Regeln, die auch von den Betreibern der jeweiligen Instanz durchgesetzt werden. Was in der einen Instanz erlaubt ist, mag in einer anderen Instanz verboten sein - und umgekehrt. Das wird noch zu Problemen führen, wenn mehr Menschen ins Netzwerk strömen und die Grenzen ausloten.

Mastodon und Moderation

Aber was ist mit den Servern, die sich nicht an diese Maßgabe halten? Mastodon will zwar charmant und offen sein. Die Open-Source-Software steht jedem offen zur Verfu?gung. Das gilt auch für das soziale Netzwerk "Gab" in den USA, das sich vor allem an Rechte und Rassisten richtet, hat im Jahr 2019 auf Mastodon-Technik umgestellt.

Absolut zur Empo?rung der Entwickler, die sich davon distanzierten. Doch so etwas kann jederzeit passieren - auch bei uns. Und wird auch passieren. Verhindern lässt sich die Nutzung nicht. Allerdings kann jeder Server/jede Instanz andere Server blocken. Was aber bedeutet, dass man als User dann doch nicht alle Nutzer in Mastodon erreichen kann.

Gerüchteküche Twitter: Wie ein Raketeneinschlag Social Media zum Beben bringt

Der Raketeneinschlag auf polnischem Boden vor einigen Tagen hat mal wieder eindrucksvoll gezeigt: Auf Twitter verbreiten sich Gerüchte und Spekulationen im Eiltempo - und setzen traditionellen Medien unter Druck.

Vor einigen Tagen hat die Welt den Atem angehalten. Ein bisschen Kuba-Krise-Feeling. Denn in Polen sind auf polnischem Grund Raketen eingeschlagen, oder zumindest Überreste. Zwei Menschen sind dem zum Opfer gefallen. Und gleich Spekulationen: russische Raketen? Nato-Fall? Was passiert jetzt?

Auf Twitter und in anderen Social Media Diensten ist das normal. Aber auch die tradierten Medien wollten nicht abwarten und haben gleich spekuliert, es könnten russische Raken gewesen sein – mit den dann unvermeidlichen Konsequenzen.

Eine unbekannte Rakete, die auf russischem Boden einschlägt, bringt das Netz zum Beben – und Falschnachrichten schaffen es unwidersprochen in die linearen Medien. Ein Lehrstück dafür, wie Journalismus heute funktioniert – oder eben auch nicht funktioniert.

Einfluss auf traditionelle Medien ist groß

Chronologie der Ereignisse

Es war am Dienstag (15.11.2022) kurz nach 18 Uhr, als erste Meldungen über einen Einschlag einer Rakete in Polen kursierten. Unter dem Hashtag #Polen haben lokale polnische Medien Meldungen verbreitet, später sogar mit Fotos und Videos, die über einen Einschlag in einer Getreidetrocknungsanlage auf polnischem Gebiet nahe der ukrainischen Grenzen berichten. Zwei Tote.

"Möglicherweise russische Raketen", so der Verdacht. Schnell wurden diese Tweets weiterverbreitet, angereichert mit Hashtags wie **#Nato** und **#Bündnisfall**, was der Sache natürlich weiteren Nachdruck verleiht. Die Algorithmen der Social-Media-Netzwerke lieben solche Situationen: Schnelle Reaktionen, Retweets,

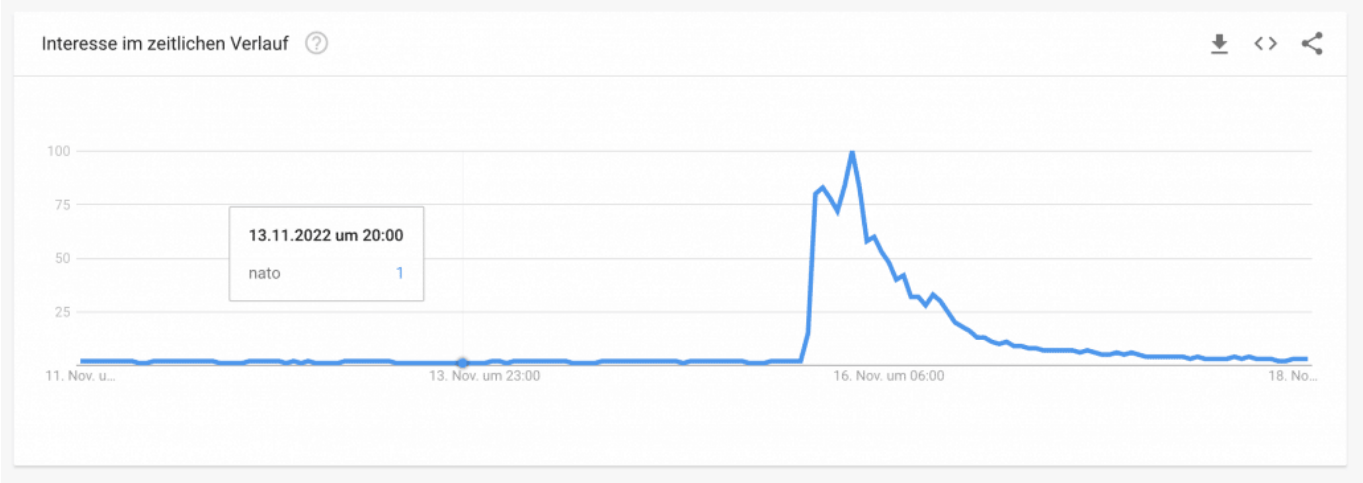
emotionale Reaktionen.

Das bekommt dann früher oder später jeder zu sehen. Und die Meldungen verbreitet sich – völlig ungeprüft – wie eine Wahrheit tausendfach, millionenfach. Weil sich der ukrainische Präsident Selenskij schnell sicher war: Das war eine russische Rakete – es besteht Handlungsbedarf, reichte vielen das schon als Beleg des Verdachts. Hashtags wie #Nato und #Bündnisfall trendeten explosionsartig. Schon um 19 Uhr war sozusagen #Weltkrieg.

Twitter ist ein Ticker für Politik und Medien

Nun könnte man ja sagen: Twitter – da sind gerade mal sechs bis sieben Millionen Deutsche. Das ist keine seriöse Nachrichtenquelle. Wieso hat sich das Thema dann so schnell weiterentwickelt?

Weil Twitter heute für viele eine Art „Nachrichten-Ticker“ ist. Man kann nachweisen, indem man bei Google Trends nachschaut – hier werden Suchanfragen auf Google chronologisch und nach Volumen eingeordnet: Ab Dienstag Abend, so 19 Uhr, haben die Menschen verstärkt nach „Nato“ gesucht. Es gab also augenblicklich einen deutlich erhöhten Bedarf nach Einordnung und Aufklärung – und da gab es noch keinen Hinweis auf das Ereignis in den linearen Medien.



Google Trends: Nato trendet - für 48h

Die Menschen wollten wissen, was da los ist. Das wissen auch Redaktionen – und versuchen dieses Interesse zu bedienen. Klicks sind Gold wert. Sie berichten dann ungeprüft, was auf Twitter gemeldet wird. Dadurch bekommen erste Tweets auf Twitter gleich einen seriöseren Anschein. Da die meisten Journalisten auf Twitter unterwegs sind – wir haben ja schon öfters darüber gesprochen –, bekommen sie mit, was auf Twitter trendet.

Um 20 Uhr wurde der Einschlag bereits in der Tagesschau gemeldet, freilich ohne zu behaupten, die Rakete wäre von den Russen. Es wurde aber auch nicht gesagt, dass man es eben nicht wisse – was jetzt kritisiert wird. Bild war natürlich auch sehr schnell – online und Print. Da hieß es gleich: „Putin feuer Raketen nach Polen“ und „Putin spielt mit dem Weltkrieg“. Es wurde auch geschrieben: „Die russische Armee hat Polen bombardiert“. Wie wir heute wissen: ~~alles falsch~~. Das war angesichts der Faktenlage viel zu voreilig.

Twitter ist ein Ticker für Politik und Medien

Selbst eine seriöse Sendung wie „Report aus Mainz“ (ARD) berichtet von russischen Raketen, die eingeschlagen seien, obwohl das noch gar nicht feststeht. Ebenso mehrere Zeitungen. Was führt dazu, dass so etwas passiert?

Das Problem ist: Nachrichten sind immer ein schnelles Geschäft. Im wahrsten Sinne des Wortes Geschäft: Journalisten wollen immer die ersten sein, die über etwas berichten. Seriöse Journalisten prüfen Quellen. Das Netz prüft nichts. Da kann jeder alles behaupten, ein Honk wie ein Präsident.

Und die Algorithmen entscheiden, was viral geht – natürlich auch die Nutzer, durch ihr Verhalten. Wahrheit hat keinen Wert. Emotionalität und Reaktion haben einen Wert. Das ist nicht journalistisch, aber Journalisten verspüren erkennbar einen Druck.

Sie wissen: Im Netz kursieren Nachrichten blitzschnell. Wir wollen nicht diejenigen sein, die nicht reagieren und nichts wissen. Also werden sogar Verdachtsfälle als vermeintliche Erkenntnisse erwähnt oder gemeldet. Ungeprüft. Das ist unter Qualitätsgesichtspunkten natürlich eine Katastrophe, weil die Unzulänglichkeiten der Netzwerke in die sogenannten Qualitätsmedien eindringen. Tempo kommt vor Gewissheit und Gewissenhaftigkeit.

Journalismus in einer Zwickmühle

Aber das Problem ist doch: Berichten Journalisten gar nichts, informieren sich die Menschen ausschließlich in den Social Media Diensten – und werden im Zweifel desinformiert, also mit interessengelenkten Falschinformationen ziemlich manipuliert. Das klingt nach einer ganz schönen Zwickmühle

Genau – und das ist auch der Druck, den Journalisten sehen. Aber hier müssen Redaktionen und Journalisten lernen, auch den Mut zu haben und zu erklären: Es gibt Gerüchte und bestenfalls Meldungen auf Twitter und Co., das muss aber nichts bedeuten.

Es könnte auch ganz anders sein. Wir müssen das erst seriös prüfen. Auch wenn es schwer fällt, müssen aber auch die Menschen, die sich informieren wollen, in Geduld üben. Es gibt nicht auf alles gleich Antworten – schon gar keine gesicherten und einfachen. Auch wir, die wir Medien konsumieren, haben uns angewöhnt, die Prinzipien der Social Networks zu übernehmen: Alles – sofort. Das ist ein riesiger Fehler.

[e2pdf-download id="1"]

Optimal mit Fenstern arbeiten auf dem iPad

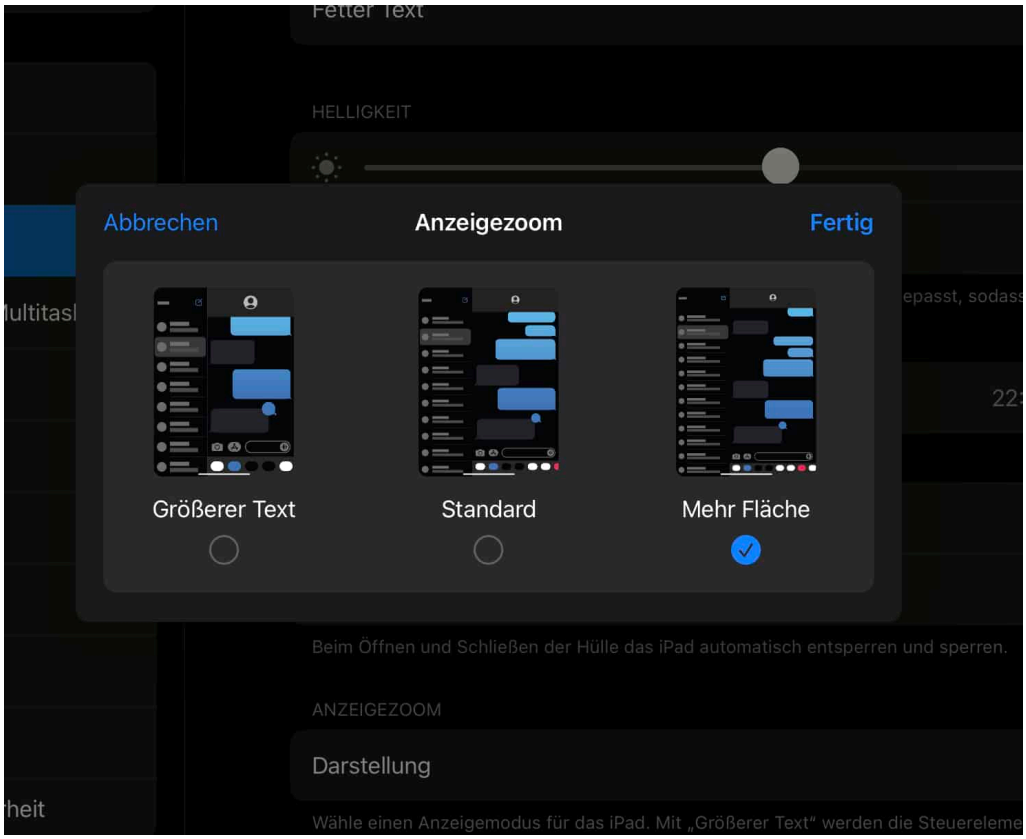
iPadOS 16 hat mit dem Stage Manager eine komplexe Funktion geschaffen, mit einem iPad eine Vielzahl von Fenstern parallel offen haben zu können und zwischen diesen Daten austauschen zu können. Es gibt einige Tricks, mit denen Ihr das Optimum aus Eurem iPad-Display herausholen könnt.

Das funktioniert allerdings nur auf iOS 16 und mit einem iPad-Modell, das von 2018 oder später ist. Habt Ihr den Stage Manager schon eingerichtet? Wenn nicht, dann holt das eben nach!

Auflösung der Fenster erhöhen

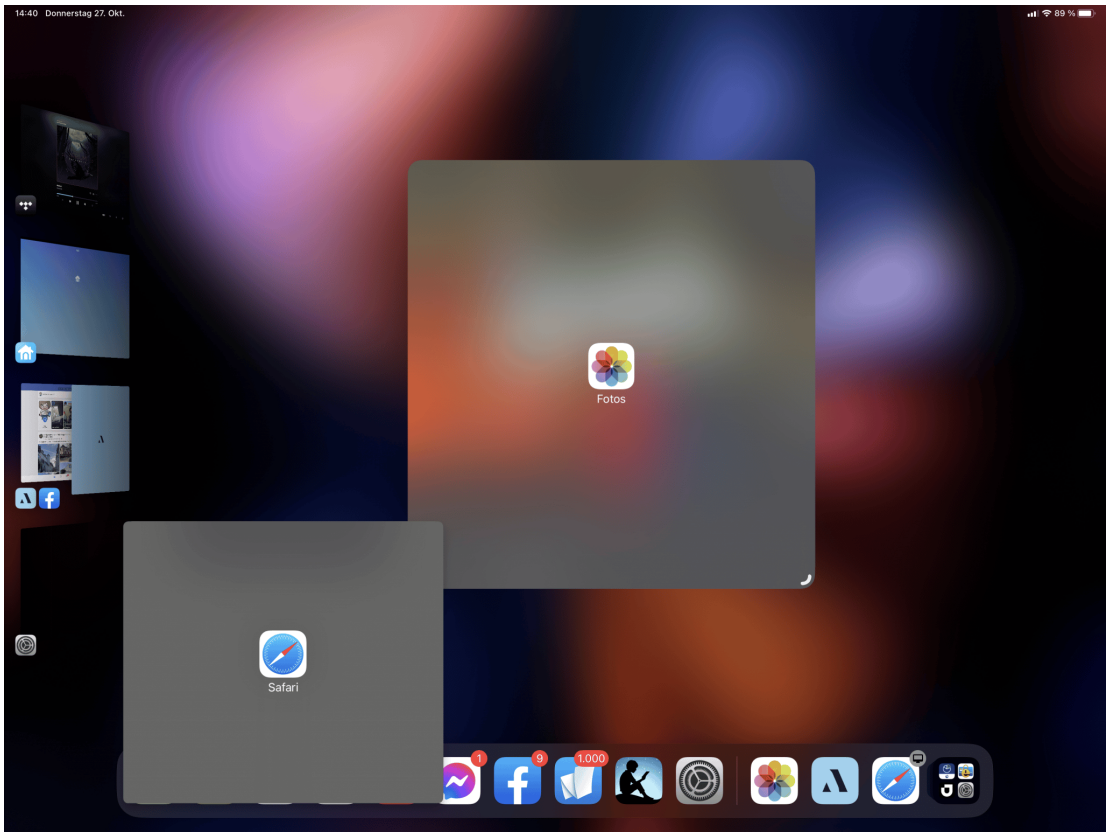
Das Display vieler moderner iPads kann mehr Pixel darstellen, als das

menschliche Auge sehen kann. Apple hat dies mit dem Begriff Retina-Display bezeichnet: Dabei werden Bildpunkte auf dem Display aus jeweils vier Pixeln gebildet, um gerade in Kanten- und Eckbereichen feinere Abgrenzungen darstellen zu können. Mit iOS 16 und den entsprechenden iPads könnt Ihr mehr Pixel für Inhalte verwenden lassen und damit die Darstellung verkleinern und mehr Fenster darstellen zu können.



- Dazu klickt in den Einstellungen von iPadOS auf **Anzeige & Helligkeit**.
- Rollt nach unten in den Bereich **Anzeigezoom** und klickt darin auf **Darstellung**.
- Wählt die Option **Mehr Fläche** aus.

Alle Elemente werden kleiner. So, als hättet Ihr auf einem externen Monitor die Auflösung erhöht.



Anordnen und Schließen von Fenstern

Um nun ein Fenster in die Multitasking-Ansicht zu bewegen, geht wie folgt vor:

- Dreht das iPad ins Querformat.
- Zieht ein Fenster aus der Taskleiste unten am Bildschirm nach oben in den Fensterbereich.
- Über den kleinen Viertelkreis unten rechts im Fenster könnt Ihr dieses mit dem Finger größer und kleiner machen.
- Bewegt das Fenster an die gewünschte Position, indem Ihr es mit dem Finger in der Titelleiste greift und bewegt.
- Um ein Fenster zu schließen, tippt oben in der Mitte auf die drei Punkte und dann auf **Schließen**.


Vollbild
Weiteres Fenster hinzufügen
Minimieren
Schließen