

A portrait of a man with short brown hair and a slight smile, wearing a teal button-down shirt. He is positioned on the left side of the frame, with his arms crossed. The background is dark. The text 'Schieb Report' is overlaid on the right side in a large, white, sans-serif font.

Schieb Report

Ausgabe 2022.31

Festplatten zwischen Mac und PC austauschen



Viele Dateien auf Mac und PC sind auf beiden nutzbar. Wie aber bekommt Ihr sie zwischen den Geräten ausgetauscht? Wir zeigen es Euch!

Standard-Dateiformate wie Bilder, Office-Dokumente und mehr sind ohne Konvertierung auf Mac und PC gleichermaßen nutzbar. Ob Ihr nun von einem Mac auf den PC (oder umgekehrt) umzieht oder einfach nur einige Dateien zur weiteren Nutzung übertragen müsst, am Ende habt Ihr dafür zwei Möglichkeiten:

Externe Datenträger und deren Formatierung

Nicht jeder USB-Stick oder jede Festplatte lässt sich auf beiden Systemen lesen. Das liegt an verschiedenen Standards: Beim PC war lange Zeit NTFS die Formatierung der Wahl, bei einem Mac ist es Mac OS Extended Journaled. Das jeweils andere System zeigt Datenträger dieser Formatierung entweder gar nicht erst an oder kann sie nur lesen, aber nicht schreiben. Grund genug, einen Standard zu schaffen, der kompatibel ist und zusätzlich noch keine Einschränkungen in der Dateigröße kennt: [exFAT](#).

Sowohl Windows als auch macOS erlauben es, Datenträger in exFAT zu formatieren. Dateien auf einem solchen Datenträger können von beiden Geräten gelesen wie auch geschrieben werden.

Die Cloud als Online-Lösung

Der einzige Datenträger, der keine Formatierung in der Form kennt, ist die [Cloud](#). Wenn Ihr häufiger Dateien zwischen Rechnern austauschen müsst (unabhängig davon, ob es Macs oder PCs sind), dann macht es Sinn, die in der Cloud abzulegen. Ob OneDrive oder DropBox, Desktops, Notebooks, Tablets und Smartphones können auf die Dateien zugreifen und sie bearbeiten.

Was Ihr bei Powerbanks beachten müsst



Wenn der Akku zur Neige geht, werdet Ihr schnell: Datenverlust muss nicht sein, und darum muss schnell Strom her. Da sind Powerbanks eine Hilfe. Worauf Ihr achten solltet, lest Ihr hier.

Powerbanks gibt es wie Sand am Meer. Die nützen Euch aber relativ wenig, wenn sie nicht für das Gerät geeignet sind, was Ihr damit betreiben oder laden wollt.

Die Spannung

Normale USB-Powerbanks liefern nur die USB-Standardspannung von 5V über den USB-Anschluss aus. Das ist für Smartphones und Tablets, die ja im Standard über USB geladen werden, ausreichend. Ein Notebook könnt Ihr damit nicht laden. Es sei denn... das wurde per USB-C geladen und die PowerBank und das Kabel sind mit dem Kennzeichen PD (für **P**ower **D**elivery) versehen.

Eine weitere Alternative sind die Powerbanks von [OmniCharge](#) und [Anker](#), die neben den USB-Anschlüssen vollwertige 22V Netzteil-Anschlüsse bieten. In die

könnt Ihr dann das Originalnetzteil einstecken und das zum Laden des Gerätes verwenden. Einziger Unterschied: Statt einer Steckdose ist die Powerbank die Stromquelle.



Die Kapazität

Intuitiv würde man vermuten, dass die Kapazität einer Powerbank einfach der des zu ladenden Geräts entsprechen sollte. Das ist aber nicht ganz richtig: Auf dem Weg von der Powerbank ins Gerät geht Kapazität verloren. Grob lässt sich sagen: Die Powerbank sollte ca. 30% mehr Kapazität haben als der Akku des zu ladenden Geräts.

Abwägung zwischen Kapazität und Größe

Je mehr Kapazität eine Powerbank hat, desto schwerer ist sie. Ihr müsst also abwägen: Wollt Ihr für den Notfall Euer Smartphone oder Tablet nachladen? Dann reicht auch eine kleine Powerbank mit geringerer Kapazität, die den Akku für zwei, drei Stunden am Leben erhält und gleichzeitig hosen- oder handtaschenkompatibel ist. Wenn Ihr Euren Akku komplett laden wollt oder müsst, weil Ihr länger nicht an eine Steckdose kommt, dann bleibt Euch keine Alternative zur großen Powerbank.

Telefonprotokolle der Fritz!Box richtig lesen



Wenn Ihr einen Fritz!Box-Router einsetzt, dann telefoniert Ihr vermutlich auch darüber. Das Lesen der Rufprotokolle bedarf allerdings einiger Interpretationen!

Gerade bei mehreren Handapparaten kann das Rufprotokoll der [Fritz!Box](#) einige Fragen schnell beantworten. Jeder Anruf, ob eingehend, ausgehend oder verpasst wird darin vermerkt. Damit lassen sich beispielsweise auch Vorwürfe der Schwiegermutter, man würde ihre Anrufe ignorieren und nie zurückrufen, schnell entkräften!

Der aktuelle Anruf

Das Telefon klingelt, Ihr geht nicht dran, wollt aber wissen, ob jemand anders im Haus das Telefonat angenommen hat. Das zeigt die Fritz!Box ein wenig versteckt an, nämlich nicht im Rufprotokoll, sondern unter **Übersicht** im Hauptmenü. Unter

Anrufe heute findet Ihr die Telefonate, die zum aktuellen Datum geführt wurden. Läuft der Anruf noch, dann findet Ihr im obersten Eintrag **Eingang** und eine Zeitangabe.

Anrufe heute: 0

 Helga&Klaus Eingang 0:10

 Lukas

 , Helga&Klaus

Diese Zeitangabe gibt die Laufzeit des Anrufes in Stunden und Minuten an (hier würde man eher Minuten und Sekunden erwarten!). Erst nach Beendigung des Anrufes wird dieser ins normale Rufprotokoll übertragen.

Das Rufprotokoll

Für alle bereits abgeschlossenen Anrufe findet Ihr das Rufprotokoll unter **Telefonie > Anrufe**. Hier könnt Ihr die Anrufe über der Übersicht in den Registerkarten nach ausgehenden, ankommenden oder in Abwesenheit nicht angenommenen Anrufen filtern. Die der Schwiegermutter sollten sich - so sie wirklich erfolgt sind - unter **Anrufe in Abwesenheit** finden.

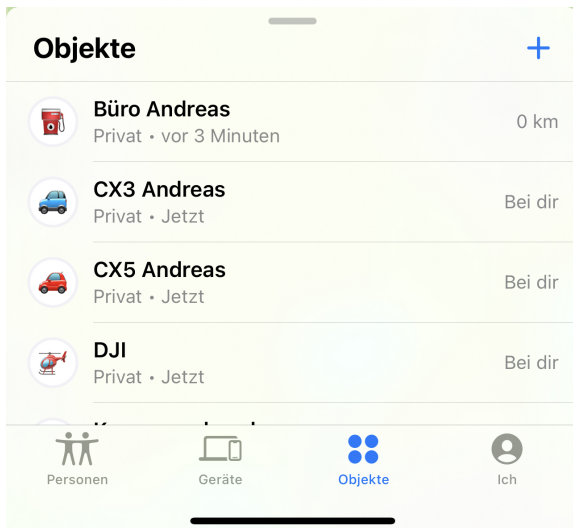
Aus dieser Ansicht könnt Ihr Anrufe schnell [in die Kontaktliste\(n\) der Fritz!Box übertragen](#).

Wenn AirTags nicht auffindbar sind



Die Apple [AirTags](#) werden von vielen Anwendern für die [Ortung von Gegenständen](#) eingesetzt. Auch aus der Ferne. Dumm, wenn eines dann seine Position nicht übermittelt!

Das Besondere an den AirTags ist, dass sie nicht nur ortbar sind, wenn das eigene Smartphone in Reichweite ist: Das [Find My-Netzwerk](#) von Apple, das unter anderem auch für die Ortung von iPhones, iPads und Macs gedacht ist, kann mehr. Sobald ein anderes iOS-Gerät eines fremden Benutzers sich in der Nähe befindet, wird die Position des AirTags aktualisiert. Anonym, nicht für den fremden Nutzer identifizierbar, aber für Euch sichtbar. Im Normalfall seht Ihr bei Euren AirTags, die nicht in Eurer Reichweite sind, aber in einem besiedelten Gebiet stehen, alle paar Minuten ein Update. Dann nämlich, wenn jemand mit seinem iPhone vorbeigegangen ist und die Position des AirTags automatisch gemeldet wurde.



Wenn Die nicht bestimmt werden kann, dann gibt es drei potenzielle Gründe:

- Die Batterie ist leer oder der Batteriedeckel nicht richtig geschlossen: Dreht einmal den silbernen Deckel mit dem Apple-Symbol auf und wieder zu. Wenn das nichts hilft, tauscht die Batterie aus (es handelt sich hier um eine handelsübliche CR2032 Knopfzelle).
- Bewegt das AirTag einmal kräftig. Manchmal kommt es vor, dass es seine Kopplung vergisst und dann zum Einsparen von Batteriestrom in den Standby-Modus geht. Nachdem es wieder aktiv ist, kann es neu gekoppelt und dann normal verwendet werden.
- Das AirTag wurde sehr lange nicht mehr von einem iPhone oder einem anderen Gerät gesehen worden und ist aus dem Grund nicht aktualisiert worden. Die Find My-App gibt dann die letzte Position an, bemängelt aber deren Aktualität. Sobald Ihr Euch mit Eurem iPhone in die Nähe bewegt, aktualisiert die Position wieder.

Wo kommt nur all der Hass her?



Über Monate haben Corona-Leugner und Impfgegner die österreichische Ärztin Dr. Lisa-Maria Kellermayr im Netz bedroht. Ihre wiederholte Bitte, die Polizei möge sie schützen, hat die Polizei nicht ernst genommen. Die Ärztin hat viel Geld in Sicherheitsmaßnahmen in ihrer Praxis investiert. Sie hat nun Selbstmord begangen.

Eine Ärztin [nimmt sich das Leben](#), weil der Hass, die Hetze, die eiskalte Bedrohung aus dem Netz schlichtweg unerträglich geworden ist. Weil hemmungslose Impfgegner sich immer und immer wieder ungestraft im Netz menschenverachtend äußern dürfen. Nicht ein Mal, nicht ein Dutzend Mal. Unzählige Male. Mit ganz konkreten Bedrohungen für Leib und Leben. Mit Todesdrohungen.

Shitstorms und Bedrohungen

Einfach nur furchtbar, was Dr. Lisa-Maria Kellermayer da monatelang aushalten musste – und ganz offensichtlich irgendwann nicht mehr aushalten konnte. Die zahlreichen Täter, die sie unentwegt bedrängten, haben Verachtung verdient – und ganz sicher strenge rechtliche Konsequenzen.

Viel schlimmer ist in meinen Augen aber, dass die Polizei ihr keinerlei angemessenen Schutz geboten hat. Obwohl sie sich immer wieder an die Polizei gewandt hat. Aber ohne nennenswerte Reaktion. So, als ob Straftaten im Internet eine Naturgewalt wären, die man einfach hinnehmen müsste. Oder nicht ernst zu nehmen braucht.

Wir wissen alle, dass das völlig falsch ist. Eine fatale Fehleinschätzung.

Verbale Gewalt ist auch Gewalt

Es gibt leider unzählige Fälle: Politiker, Menschen, die sich öffentlich exponieren – viele erleben andauernd unerträgliche Shit Storms und rohe verbale Gewalt. Auch Bedrohungen. Doch Polizei und Staatsanwaltschaft unternehmen nur selten etwas dagegen.

Bei körperlicher Gewalt heißt es gerne: „Gewalt geht gar nicht!“ Bei verbaler Gewalt hingegen wird gerne weggeschaut. Nicht nur im Netz, wo gerne alles, auch Pöbeleien und sogar Bedrohungen als Meinungsfreiheit verstanden werden wollen.

Nein, nach meiner Beobachtung handelt es sich hier um ein ganz generelles Problem. Erniedrigungen jeder Art, auch und besonders in der Öffentlichkeit, Hohn, Spott, Häme – sie werden schon lange durch diverse abscheuliche Fernsehsendungen bei RTL und Co. hoffähig gemacht. Im Netz gibt es dann kein Halten mehr. Jeder versucht den anderen an Boshaftigkeit und Aggression zu übertrumpfen.

Das Netz ist Teil des Problems

Natürlich: Das Netz fördert Hemmungslosigkeit. Das wissen wir längst. Im Schatten der Anonymität trauen sich viele deutlich mehr, als sie sich im „echten Leben“ erlauben würden. Die Opfer sind weit weg, irgendwie virtuell. Doch das Leid, das Hass, Hetze, Häme und Bedrohungen erzeugt, das Leid ist echt.

Jetzt allein die Plattformen verantwortlich zu machen – wie so gerne und so häufig –, wäre völlig zu kurz gegriffen. Natürlich: Facebook, Twitter, Instagram, Telegram und Co. sind ganz klar ein Teil des Problems und nicht ein Teil der Lösung. Weil sie Hemmungslosigkeit fördern und immer noch viel zu wenig tun, um etwas gegen Hass, Hetze und Bedrohungen zu unternehmen.

Doch die Wahrheit ist: Lösen können die Plattformen das Problem auch nicht.

Versagen des Staates

Das ist Aufgabe des Staates – und der Gesellschaft. Der Staat muss härter durchgreifen: Erst wenn klar ist, dass Straftaten blitzschnell verfolgt werden und Konsequenzen haben, wird es auf den Plattformen im Internet vielleicht ein bisschen friedlicher. Dafür muss aber investiert werden: Polizei und vor allem auch Justiz müssen befähigt werden, ihre Aufgaben schnell und konsequent nachzukommen. Es muss personell und technisch aufgerüstet werden. Dazu aber braucht es den entschlossenen Willen.

Doch den sehe ich nicht, allen Sonntagsreden zum Trotz. Niemand will etwas verändern.

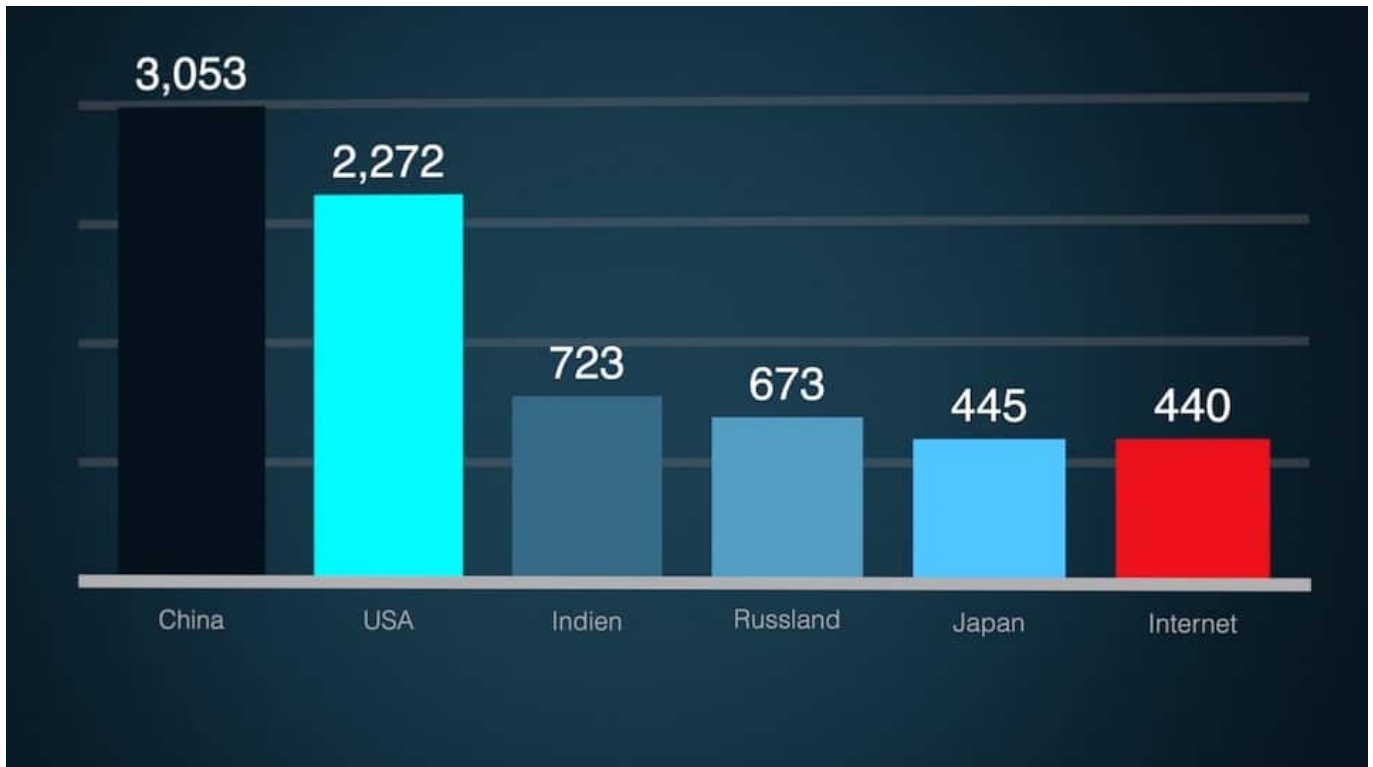
Aber auch die Gesellschaft braucht dringend ein Update. So lange es kein „Wir“ mehr gibt, ein Interesse an der Gemeinschaft, sondern immer nur Gruppenbildung – nach Geschlecht, Herkunft, Ideologie, Hobbys, Ernährungsweise..., und alle anderen „die anderen“ sind, die bekämpft und nicht verstanden werden wollen –, so lange ist keine Lösung in Sicht.

Wir brauchen mehr "Wir"

Ja, das Internet befördert das Problem zweifellos. Leider. Weil jeder jederzeit folgenlos alles raushauen kann. Und das im Blitztempo. Aber auch, weil Erregung und Aufregung das neue Nachdenken ist. Facebook, TikTok, Twitter und all die anderen reiben sich die Hände. Sie verdienen daran, dass sich die User im Netz bekriegen.

Das muss sich dringend ändern. Wir alle müssen uns dringend ändern. Mehr zuhören. Mehr Respekt haben. Mehr Verständnis aufbringen. Ja, sich bitte gerne auch mal selbst in Frage stellen. Muss ja nicht öffentlich in Social Media sein. Aber warum eigentlich nicht?

Energie sparen: Auch ans Netz denken!



Das Internet verbraucht mehr Energie als ganz Indien: Jede einzelne Aktivität im Netz hat einen Anteil daran. Durch bewusste Nutzung von Cloud, Apps und Netz lässt sich durchaus Energie einsparen – und der CO2-Ausstoß verringern.

Noch vor wenigen Monaten macht Verkehrsminister Volker Wissing in einem Tweet darauf aufmerksam, dass jedes gepostete Foto von einer Mahlzeit Energie. Der Minister wurde für seine Bemerkung mit Hämme überschüttet. Aber in der Sache hatte er Recht: Alles, was wir im Netz tun, ist mit teilweise erheblichem Energieaufwand verbunden.

Was Wissing nicht gesagt hat: Auch Scrollen im News-Feed von Instagram oder TikTok kostet Energie. Sogar mehr als das Posten eines Fotos.

TikTok verbraucht mehr Energie als Instagram

Eine Minute durch den [TikTok-Newsfeed](#) zu scrollen, verursacht laut einer Studie

des Analyse-Unternehmens Greenspector drei Mal mehr CO₂-Ausstoß als das Scrollen bei Facebook. Beim Business-Netzwerk LinkedIn ist es noch mal deutlich weniger. Was damit zu tun hat, dass dort weniger Videos gepostet werden, die automatisch loslaufen.

TikTok ist damit bei den Social Media Netzwerken in punkto Energie-Verbrauch der Spitzenreiter.

Aber alles verbraucht Energie. Das Internet ist (fast) immer da. Wenn nicht, liegt es nicht am Internet selbst, sondern an der mangelnden Versorgung vor Ort. Doch um rund um die Uhr Internet anbieten zu können, sind enormen Kraftanstrengungen erforderlich – und damit einhergehend eine Menge Energieverbrauch. Wäre das Internet ein Land, es verbrauchte mehr Energie als ganz Indien.

Mindestens 6% des weltweiten Stromverbrauchs

Der Weltklimarat IPCC warnt in seinem jüngsten Bericht erstmals vor dem „steigenden Energiebedarf von Rechenzentren und IT-Systemen“: Mittlerweile sind Nutzung und Betrieb des Internet inzwischen für sechs bis zwölf Prozent des gesamten globalen Stromverbrauchs verantwortlich. Bis zum Jahr 2030 – so die Befürchtung – könnten es 50% des globalen Stromverbrauchs sein.

Ergo: Wer Energie sparen will, kann hier unmöglich wegschauen.

Wer weiß schon, wie viel Energie nötig ist, um eine [Anfrage bei Google zu beantworten](#)?

Ganz präzise lässt sich das nicht sagen – aber annäherungsweise. Und es ist ganz sicher mehr, als die meisten vermuten: Laut Berechnungen verbraucht eine einzelne Anfrage bei Google rund 0,003 Wattstunden. Schon 1.000 Suchanfragen lassen eine 30-Watt-Glühbirne für eine Stunde leuchten. Angesichts von acht Milliarden Suchanfragen allein auf Google pro Tag kommt da einiges an Energieaufwand zusammen.

Jede einzelne Suchanfrage kostet Energie

Keineswegs nur in den Rechenzentren von Google, sondern auch in den vielen

anderen Rechenzentren von Netzbetreibern, Providern und Mobilfunkanbietern. Denn damit unsere PCs, Notebooks und Mobilgeräte online gehen können, ist im Hintergrund eine Menge Aufwand erforderlich. Aufwand, den wir nicht sehen – und über den sich die meisten auch keine Gedanken machen.

„Jede einzelne eingesparte Suchanfrage bei der Suchmaschine unseres Vertrauens entlastet das Netz – und spart Energie ein. Denn Rechenzentren benötigen viel Strom, vor allem für die Kühlung der Rechner und Server. Bei sinkender Netznutzung ist weniger Kühlung nötig – und die Stromnetze sind entlastet. Denn noch beziehen nur wenige Rechenzentren ihre Energie aus eigenen Energiequellen (etwa Google oder Apple in Kalifornien).

Energie sparen: So geht's

Damit lässt sich ohne Übertreibung sagen: Alles, was nicht online erledigt wird, spart Energie ein. Deswegen hier ein paar Tipps, wie sich global Energie einsparen lässt – vor allem bei den Cloud-Diensten.

Weniger Suchanfragen: Anstatt eine Webadresse zu googeln, lieber die Internetadresse direkt eingeben. Wer Webseiten regelmäßig besucht, legt dafür am besten Favoriten an – das erspart Suchanfragen. Bei 1.000 eingesparten Suchanfragen kann eine 30-Watt-Birne eine Stunde leuchten.

Videos abschalten im Team Call: Eine Studie aus dem Jahr 2021 belegt: Wer in einem Team Call die Videos abschaltet, reduziert seinen CO₂-Fußabdruck um 96%.

Geringere Auflösung beim Streaming: Filme und Serien zu streamen ist besonders energieaufwändig. Laut US-Studien verursacht eine Stunde Streaming so viel CO₂ wie eine Fahrtstrecke von 1,8 Kilometern in einem durchschnittlichen PKW. Wer anstatt in 4K-Qualität „nur“ in HD-Qualität streamt, spart 86% Energie.

E-Mails löschen: Wer seine nicht mehr benötigten E-Mails löscht, macht Platz frei in seinem Cloud-Speicher. Wenn das alle machen, kommen gigantische Speichermengen zusammen, die freigegeben werden – und das erspart den Einsatz von vielen Servern und damit Energie.

Videos nicht automatisch abspielen: Ob auf Youtube, im Browser oder auf Facebook oder Instagram: Überall werden Videos automatisch abgespielt

(„Autoplay“). Das lässt sich durch entsprechende Einstellungen bei Facebook, Youtube oder im Browser (für Videos auf Webseiten) abstellen. Denn werden Videos nicht automatisch abgespielt, lässt sich eine Menge Energie einsparen. Bei Bedarf kann man die Videos manuell starten.

Download statt Streamen: Wer sich unterwegs Filme, Serien oder Videos anschauen will, sollte sie zu Hause im WLAN downloaden, anstatt sie unterwegs zu streamen. Denn ein Download im WLAN braucht nur einen Bruchteil des Energieaufwandes. Das Mobilfunknetz verbraucht deutlich mehr Energie – und erzeugt einen größeren CO2-Footprint.

Zukunft von Metaverse: Ist das eine gute Idee und was sind die Risiken?



Eindeutige Metaverse-Analyse: Welche Chancen bietet es? Wird diese Zukunft rosig sein? Welche Risiken bestehen? Was also ist das Meta-Universum heute?

Die Metawelt wird wahrscheinlich eine der wichtigsten Technologien der nahen Zukunft sein.

Warum das Meta-Universum so wichtig ist, dass sogar [Mark Zuckerberg den Namen seines Unternehmens ändert, was in Zukunft von dem Metaversum zu erwarten ist](#) und welche Risiken es außerdem in diesem Überblick über Kryptowährungen. Die Nachricht ist keine Finanzempfehlung.

Was ist ein Meta-Universum?

Der Begriff „Meta-Universum“ wurde erstmals 1992 von dem amerikanischen Science-Fiction-Autor Neal Stephenson in seinem Science-Fiction-Roman *Avalanche* geprägt. Das Konzept der virtuellen Realität, die das reale Leben

vollständig ersetzt, wurde jedoch schon früher entwickelt. Zum Beispiel in der berühmten Serie Blade Runner.

Eine der vielleicht eindrucksvollsten Demonstrationen des Meta-Universums ist der Film The Matrix aus dem Jahr 2000. In weniger als 30 Jahren war die Menschheit in der Lage, sich von der Fantasie zu lösen und in die Tat umzusetzen. Was also ist die Metawelt heute?

Eine Metawelt ist eine virtuelle Welt, die eine nahezu identische Projektion der realen Welt darstellen soll.

Es handelt sich um einen Raum, in dem Menschen [mit Hilfe von Technologien](#) wie VR-Brillen, Handschuhen mit Sensoren usw. all die Handlungen ausführen können, die sie auch im echten Leben in Germany ausführen. Das Endziel der Metawelt als Produkt ist es, die Welt mit allen Sinnen und Prozessen neu zu erschaffen.

Mark Zuckerberg und seine Metawelt

Mark Zuckerbergs Unternehmen Meta geht einen ähnlichen Weg. Im Juli 2021 kündigte Mark Zuckerberg offiziell an, dass Facebook innerhalb von 5 Jahren zu einem Meta-Universum werden wird. Das Unternehmen plant die Entwicklung mehrerer Produkte in diese Richtung. Bislang sind zwei bekannt:

- Horizon;
- Rival Peak.

Horizon ist Facebook in einer virtuellen Welt, die im Moment nur mit der Oculus Quest 2 VR-Brille funktioniert. In diesem Raum können sich die Nutzer in der Welt bewegen, mit ihren Freunden kommunizieren, Sendungen ansehen, Spiele spielen und sogar kochen. Die App ist kostenlos, aber man kann nur mit einer Oculus-Brille einsteigen. Rival Peak ist eher eine Reality-Show, in der KI-gesteuerte virtuelle Helden Aktionen ausführen, die ihnen von den Zuschauern der Show in Echtzeit vorgeschlagen werden.

Was kommt als Nächstes?

Im Moment erleben wir die Anfänge einer größeren virtuellen Welt. Im Moment ist vor allem eines interessant: Wer wird als erster die beste Version herstellen und die Mehrheit des Marktes erobern können. Dazu muss man das technische Problem lösen, die VR-Technologie so einfach wie möglich zu gestalten.

Es ist unwahrscheinlich, dass die Menschen massenhaft Spezialbrillen kaufen werden, nur um der bestehenden Produkte willen. Die chinesischen Entwickler von Baidu, die ihre eigene Xi Rang Metawelt angekündigt haben, sind klug genug, dies zu tun.

Sie erfordert keine VR-Brille, sondern kann einfach über ein Smartphone oder einen Computer genutzt werden. Die Benutzererfahrung ohne VR wird wahrscheinlich schlechter sein. Aber es wird mehr Menschen in die neue Technologie locken. Und zunehmend interessieren sich die Verbraucher für Kryptowährung kaufen von neuen Gadgets.

Zusammenfassend lässt sich sagen, dass die Metawelt [eine der wichtigsten Technologien](#) der nahen Zukunft sein könnte. Im Grunde genommen schafft die Menschheit eine neue Welt. Das Wichtigste ist, dass sie sich nicht in eine Anti-Utopie verwandelt.

Blockchain und Kryptowährungen

Dank der Blockchain ist es der Menschheit erstmals möglich, Kryptowährung tauschen zu können - in einem dezentralen und sicheren System. Sie ist auch die schnellstmögliche. Blockchain ist ein äußerst wichtiger Teil der Welt des Meta-Universums.

Diese Technologie könnte man als den „Wirtschaftsmotor“ der Zukunft bezeichnen. Die Blockchain wird die Daten und das Geld eines jeden Nutzers mit seinem digitalen Konto verknüpfen und es ihm ermöglichen, die von ihm gekauften Produkte im gesamten Meta-Universum zu nutzen. Dieser Prozess ist bereits jetzt auf dem NFT-Markt und dem digitalen Bekleidungsmarkt zu beobachten.

Alle Güter aus der virtuellen Welt, seien es Skins für einen Charakter, digitale Trainer für ein Instagram-Foto oder andere Dinge, werden in einer Kryptowährung verankert. Im Asset selbst ist die Frage noch offen: Welche digitale Währung wird in der Metawelt verwendet werden? Eine Monopolisierung ist wahrscheinlich nicht

zu erwarten.

Sicherheitswarnungen bei eBay Kleinanzeigen



[eBay Kleinanzeigen](#) erfreut sich immer größerer Beliebtheit. Was aber, wenn plötzlich eine Sicherheitswarnung in den Posteingang flattert? Reagieren solltet Ihr in jedem Fall!

Lange Zeit war eBay Kleinanzeigen der kleine, schnuddelige Bruder der großen [eBay-Seite](#) für den lokalen Einkauf vor Ort. Steigende Gebühren bei eBay für Verkäufer und auf der einen und die Möglichkeit des Versands über Kleinanzeigen auf der anderen Seite haben das geändert. Viele Anwender empfinden den Umgang und die Abwicklung hier deutlich angenehmer. Was aber zu beachten ist: Es findet auch [viel Betrug über die Plattform statt!](#) Übernommene Accounts, Zahlungsaufforderungen ohne Absicherung und mehr sind nicht selten.

Da sorgt eine Sicherheitswarnung per e-Mail schnell für Unruhe. Damit teilt eBay Kleinanzeigen Euch mit, dass eine Anmeldung an Euren Account erkannt wurde, die nicht dem üblichen Muster entspricht.

Hallo,

jemand hat sich mit einem neuen Gerät in deinem Konto

Wann: Dienstag, 21. Juni 2022 um 13:52 Uhr, MESZ

Wo: Nähe Frankfurt am Main, Deutschland

Gerät/Browser: Windows, Edge 102

Falls du dich nicht mit diesem Gerät eingeloggt hast, änc

[Neues Passwort vergeben](#)

Dein Team von eBay Kleinanzeigen

Ignoriert diese e-Mail nicht, sondern schaut genau in den Inhalt.

- Habt Ihr Euch gar nicht zum angegebenen Zeitpunkt angemeldet? Dann solltet Ihr umgehend Euer Kennwort ändern, denn diese e-Mail kommt immer nur nach einer erfolgreichen Anmeldung, Benutzername und Kennwort waren bei der Anmeldung korrekt.
- Habt Ihr Euch zu dem Zeitpunkt angemeldet, aber der Ort scheint falsch? Der Ort der Anmeldung wird automatisch aus der IP-Adresse bestimmt. Die kann durchaus eine gewisse geographische Streuung haben. Seiten wie dein-ip-check.de zeigen Euch an, welcher Ort für Euch gerade erkannt wird. Wenn das mit der Angabe der e-Mail übereinstimmt, ist alles gut. Wenn nicht: Ändert vorsichtshalber das Kennwort.

Aktivierung von Bitlocker



Sicherheitsmaßnahmen wie Passwörter sind wichtig, reichen aber nicht aus: Gerade bei mobilen Geräten solltet Ihr auch die Festplatte verschlüsseln!

Das [beste Passwort](#) nützt nichts, wenn der PC oder das Notebook gestohlen werden und die Festplatte ausgebaut und in einen anderen PC eingebaut wird. Windows lässt sich damit nicht starten (das durch das Passwort geschützt), die Daten kann der Dieb aber schon lesen und verwerten.

Die Lösung ist, die Festplatte direkt zu verschlüsseln. Wer den Schlüssel nicht hat, kann nur Datenbrei sehen, nicht aber Eure Daten. Wenn Ihr eine [Datensicherung](#) gemacht habt, dann kann Euch damit der Verlust des Rechners zumindest aus Sicherheitserwägungen kalt lassen.

Die Aktivierung und Deaktivierung von Bitlocker für Festplatten findet sich im Windows Explorer:

- Klickt mit der rechten Maustaste auf die Festplatte, die verschlüsselt werden soll (meistens also C:) und dann auf **Bitlocker Aktivieren** (bzw. **Bitlocker Verwalten**).

Betriebssystemlaufwerk

Local Disk (C:) BitLocker aktiviert



-  Schutz anhalten
-  Wiederherstellungsschlüssel sichern
-  BitLocker deaktivieren

Festplattenlaufwerke

Volume (E:) BitLocker aktiviert

Wechseldatenträger - BitLocker To Go

D: BitLocker deaktiviert

- Folgt nun den Anweisungen auf dem Bildschirm, um Bitlocker zu aktivieren.
- Im normalen Betrieb werdet Ihr hier keine Unterschiede erkennen, die Festplatte ist nicht spürbar langsamer und Ihr müsst auch beim Systemstart kein zusätzliches Kennwort eingeben. Letzteres übernimmt hier das [TPM-Modul](#) im Hintergrund.

Das TPM-Modul ist allerdings an den PC gekoppelt. Wenn Ihr den wechseln wollt, aber die Festplatte mitnehmen wollt oder müsst, dann könnt Ihr das trotzdem machen. Windows hinterlegt in Eurem Microsoft-Konto die Wiederherstellungsschlüssel, mit denen Ihr die Daten wieder entschlüsseln könnt. Wie Ihr darauf zugreifen könnt, lest Ihr [hier](#).

Wenn der Desktop nicht aktuell ist

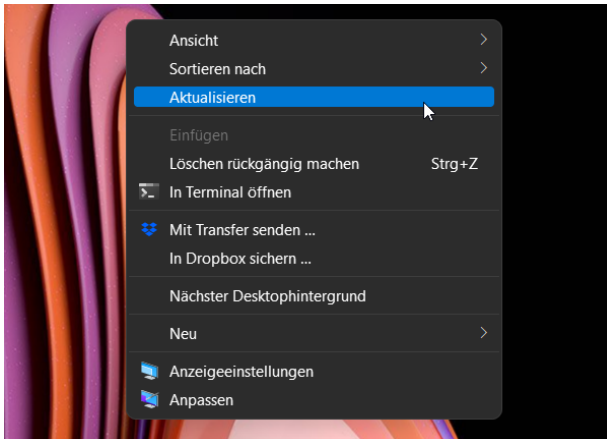


Wenn Ihr Dateien auf dem [Desktop](#) speichert und die dort nicht auftauchen, macht sich schnell Panik breit. Wir zeigen Euch, wie Ihr die vermeidet!

Euer virtueller Schreibtisch in Windows ist je nach Anwender entweder eine Sammlung der wichtigsten Verknüpfungen und Dokumente oder nahezu leer. Wenn Ihr zu der ersten Kategorie von Benutzern gehört, dann verlasst Ihr Euch darauf, dass die Dateien auch verfügbar sind. Im Gegensatz zu normalen Speicherorten wird der Desktop eher visuell (über die Desktopansicht von Windows) als als Speicherort über den Explorer genutzt. Das bringt einige Herausforderungen mit sich:

- Dateien und Verknüpfungen werden oft automatisch mitten auf dem Desktop abgelegt und werden von Fenstern verdeckt.
- Der Desktop aktualisiert sich nicht automatisch.

- Je nach Cloud-Anbindung gibt es mehrere Desktops.



Wenn Ihr eine [Datei](#), die auf dem Desktop liegen sollte, nicht findet, dann versucht Folgendes:

- Minimiert alle Fenster und schaut nach, ob die Datei irgendwo auf dem Desktop liegt. Alternativ öffnet den Explorer und klickt im Verzeichnisbaum **Desktop** an und schaut im Detailfenster nach der Datei.
- Auf dem Desktop selbst klickt mit der rechten Maustaste auf einen freien Bereich und dann im Menü auf **Aktualisieren**.
- Schaut im Windows Explorer, ob es unter OneDrive (oder einem anderen Cloud-Service) einen weiteren Desktop-Ordner gibt. Wenn ja, dann schaut auch auf diesem nach!