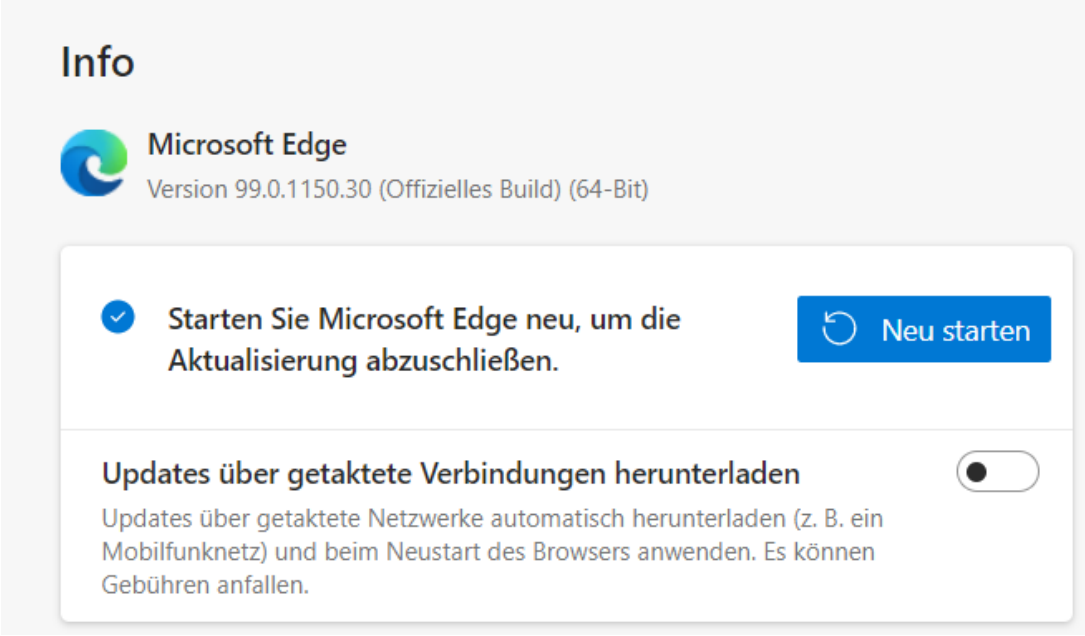
Schieb Report

Ausgabe 2022.12

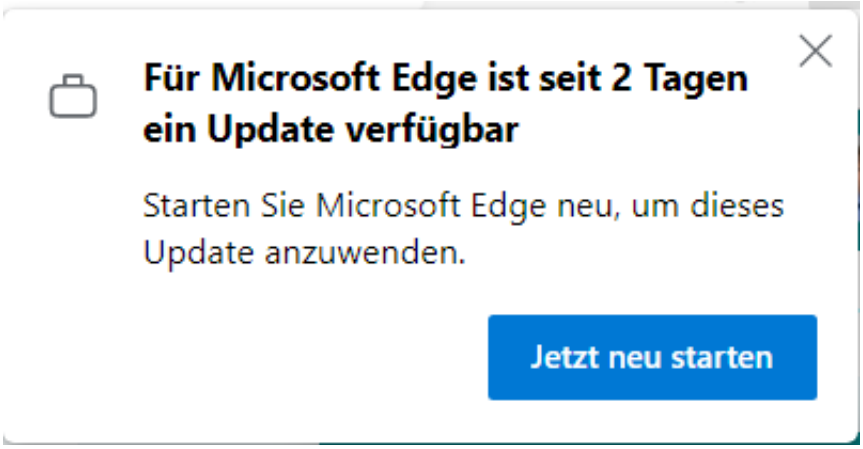
Updaten von Microsoft Edge

Updates sind wichtig. Lange hat Windows diese auch für eigene Apps wie den Browser zentral durchgeführt. Seit Microsoft Edge ist das anders, hier müsst Ihr selbst handeln!

Die Idee war gut: Windows Updates sind ein Automatismus, der auf jedem Windows-Rechner eingespielt ist: Windows sucht nach den Updates, informiert den Benutzer und installiert sie. Kaum ein manueller Eingriff, kaum Zeitverzögerung zwischen Verfügbarkeit und Installation. Die zunehmenden Angriffe aus dem Internet aber haben hier eine Anpassung des Prozesses bewirkt: Sicherheitslücken im Browser werden rasend schnell ausgenutzt, jeder Anwender ist potenziell betroffen. Auf der anderen Seite lässt sich der Browsers eigenständige App schneller aktualisieren. Die Konsequenz: Edge hat einen eigenen Update-Mechanismus. Den könnt - und solltet - Ihr beeinflussen!

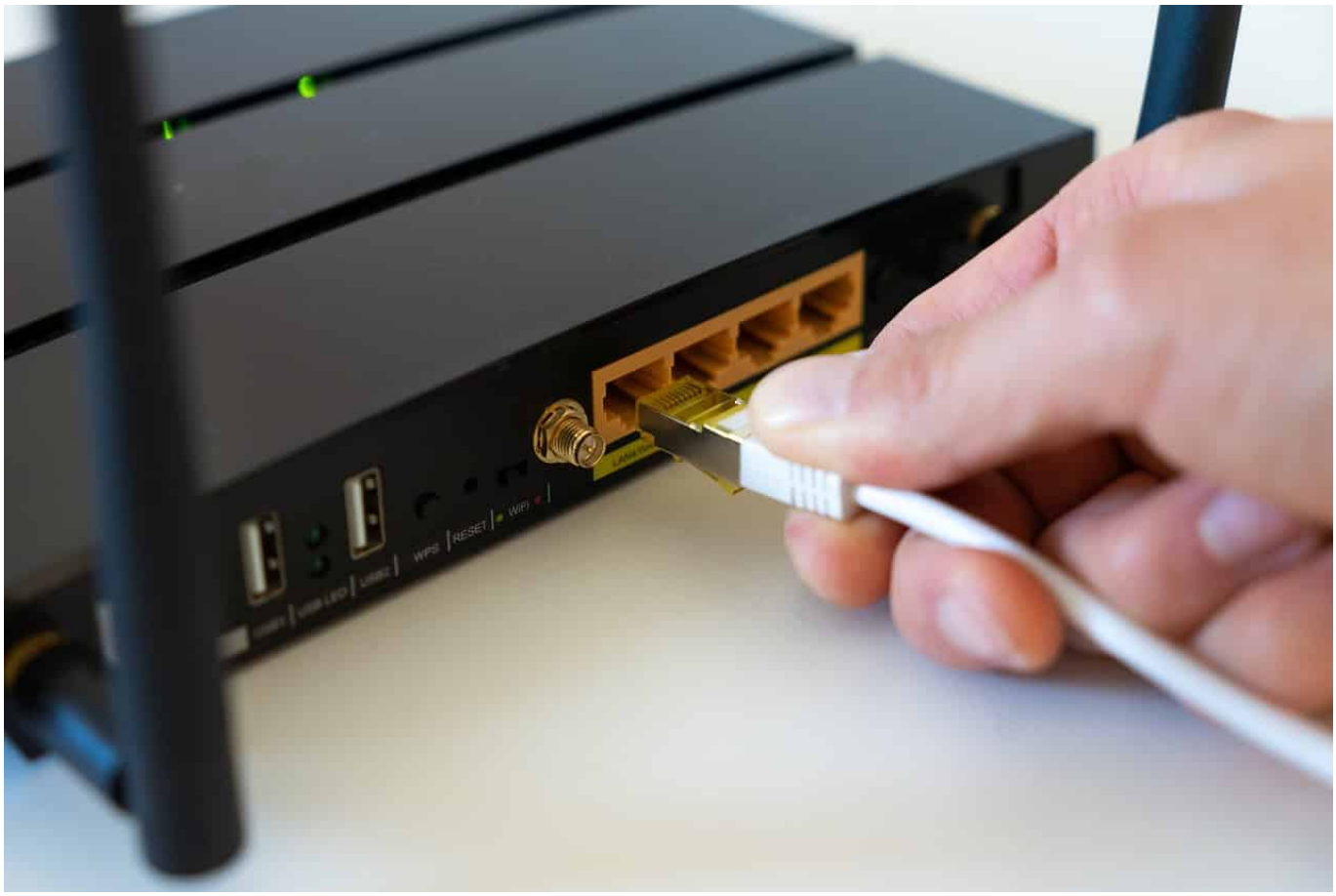


Im drei-Punkte-Menü von Edge unter **Einstellungen** > **Infos zu Microsoft Edge** > **Info** findet Ihr den aktuellen Stand der Version von Edge. Edge sucht automatisch nach Updates, wenn Ihr den Bildschirm öffnet. Wird ein Update gefunden, dann zeigt Edge es an und es kann über einen Klick auf **Jetzt neu starten** installiert werden.



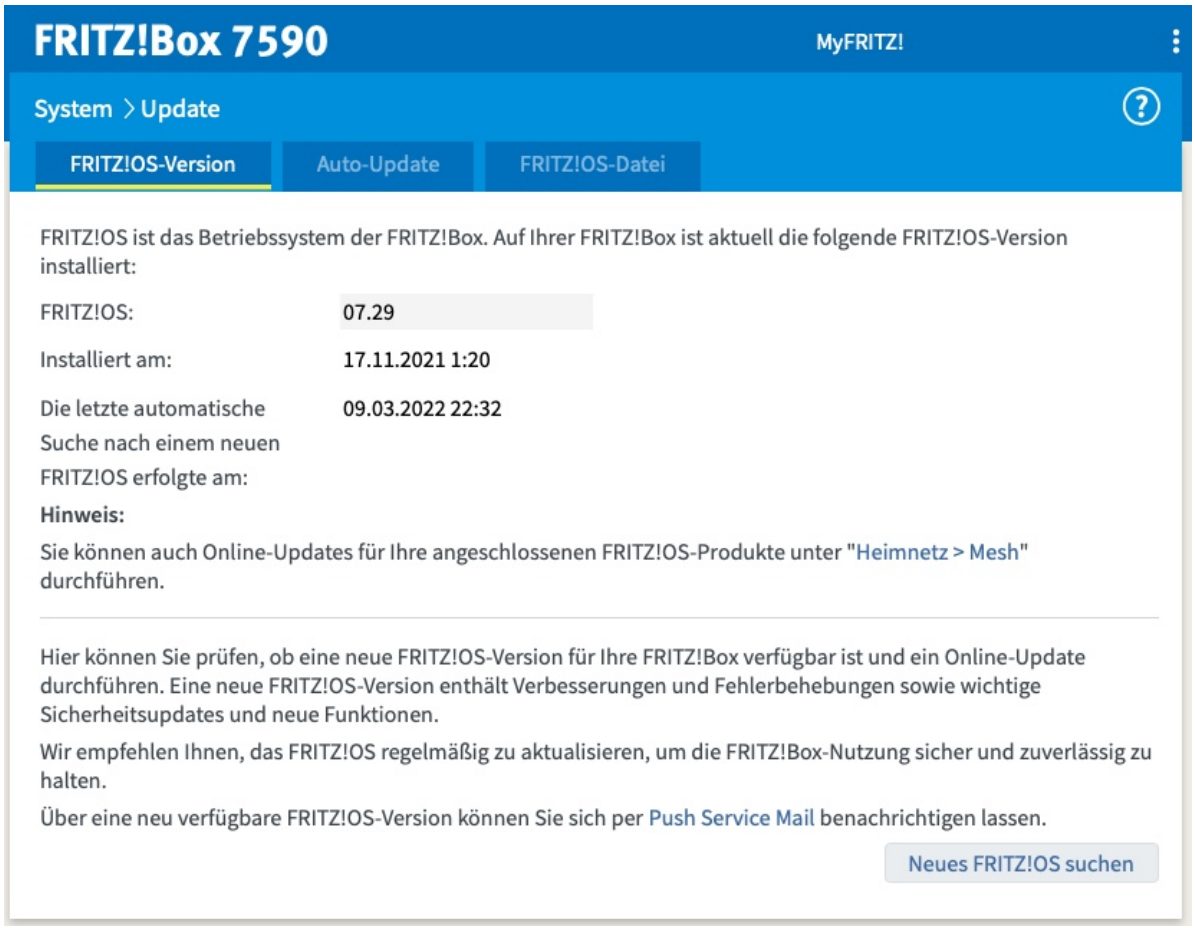
Das Programm sucht selber in regelmäßigen Abständen nach Updates. Wird eines gefunden, dann zeigt Edge eine Meldung und einen Infotext in den Einstellungen an. Reagiert darauf und wendet das Update durch einen Klick auf **Jetzt neu starten** an. Je schneller ein Update installiert wird, desto sicherer surft Ihr im Internet!

Updaten der Router-Firmware



Der DSL-Router ist nicht nur der Weg ins Internet, sondern auch der Weg aus dem Internet ins eigene Netzwerk. Jede Aktualisierung erhöht sich Sicherheit und ist schnell durchgeführt!

In den meisten Haushalten ist der Router die zentrale Netzwerk-Komponente. Er stellt das WLAN bereit, verteilt die IP-Adressen an alle Geräte, die sich mit ihm verbinden und sortiert die Datenpakete zwischen Sendern und Empfängern.



Der Weg ins Innere des Netzwerks

Zusätzlich schafft er oft auch einen Weg vom Internet ins eigene Netzwerk über Dynamische DNS-Dienste. Da liegt es nahe, dass Router für Cyberkriminelle ein lohnendes Angriffsziel sind: Jede Schwachstelle wird ausgenutzt. Die Hersteller dagegen beheben diese Schwachstellen so schnell es geht und rollen Updates aus. Die müssen allerdings auc installiert werden!

Am Besten: Automatische Aktualisierung

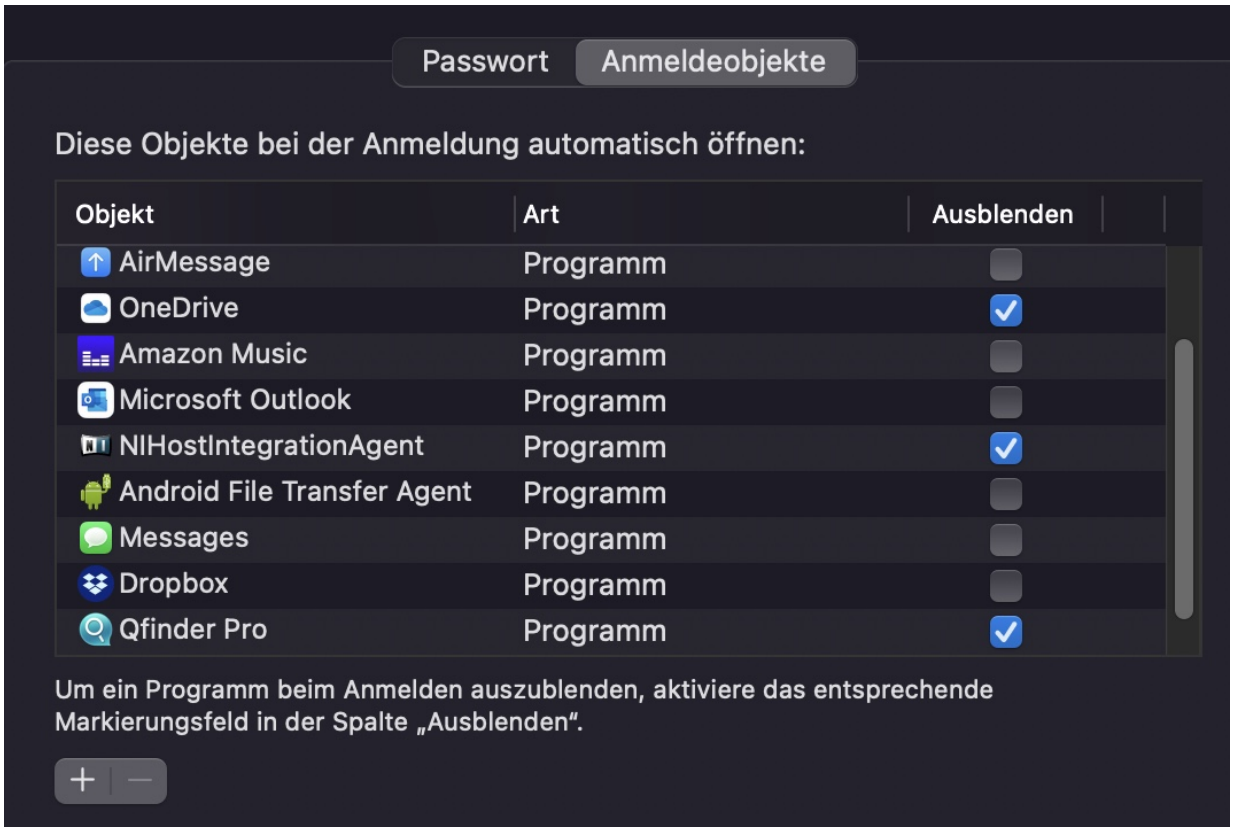
Bei den meisten Routern lässt sich das in den Systemeinstellungen aktivieren. Dazu meldet Euch an der Adminoberfläche des Routers an imd klickt im Menü auf **System**. Darunter findet sich meist ein Menüpunkt **Aktualisierung** oder **Update**. Hier lassen sich neben den Statusinformationen über die aktuelle Softwareversion des Routers und der neuesten verfügbaren auch festlegen, dass der Router Updates automatisch suchen und installieren soll.

Manchmal funktioniert das nicht und der Router verweigert die Suche mit einer abstrusen Fehlermeldung wie "Update nicht möglich, überprüfen Sie die Internetverbindung!". In einem solchen Fall könnt Ihr die Firmwaredatei vom Hersteller herunterladen (bei der AVM Fritz!Box zum Beispiel hier) und manuell installieren.

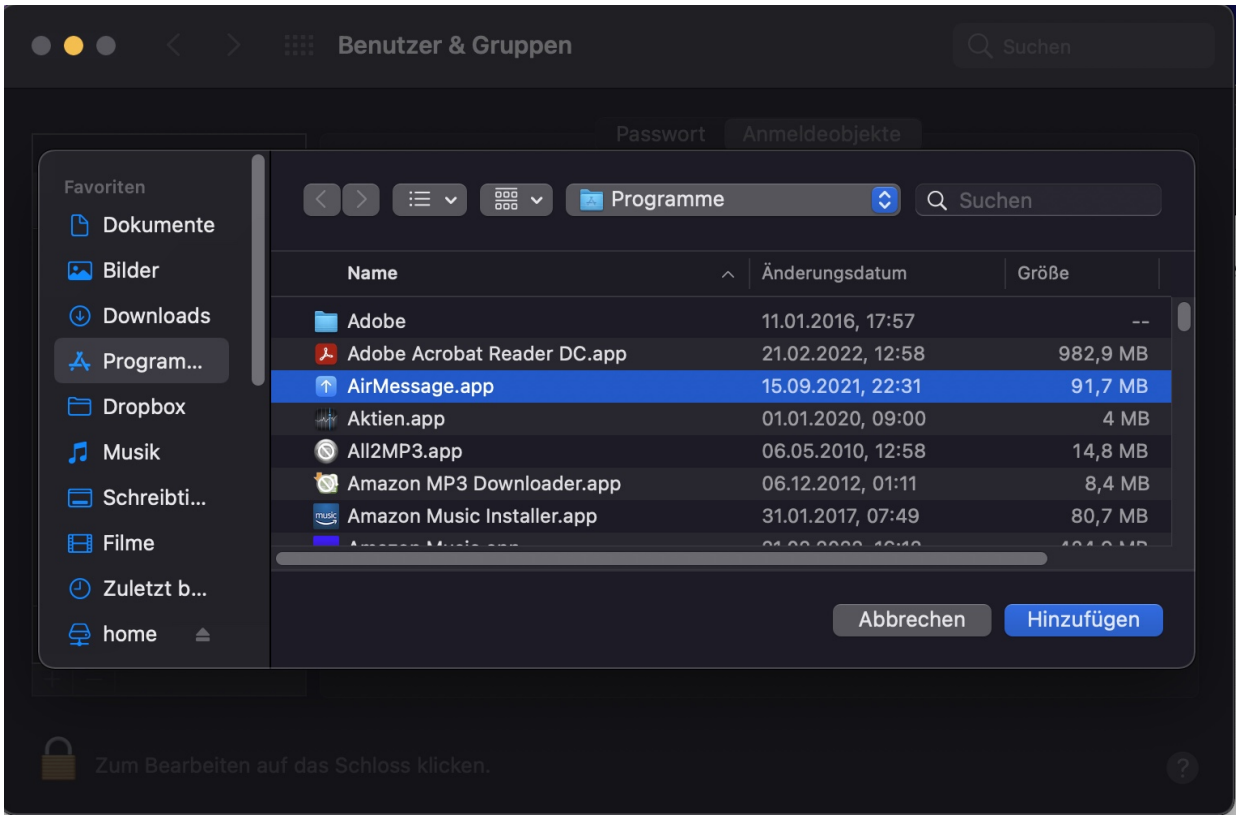
Autostart bei Mac und Windows bearbeiten

Der automatische Start von Programmen beim Hochfahren spart manuellen Aufwand und bereitet den Mac auf die Arbeit vor. Auf diesen Prozess könnt Ihr Einfluss nehmen und festlegen, welche Programme und Apps automatisch gestartet werden sollen.

MacOS unterscheidet sich an einigen Stellen von Windows, auch wenn Windows 11 hier den Abstand verringert hat. Das beinhaltet, dass einige Funktionen deutlich versteckter zur Verfügung gestellt werden, als man es erwarten würde. Das Autostart findet sich in Windows im Task Manager, dort lassen sich die Programme aktivieren und deaktivieren. Bei macOS müsst Ihr die Einstellungen öffnen und dann auf **Benutzer & Gruppen** klicken.



In dem sich öffnenden Einstellungsbildschirm muss auf **Anmeldeobjekte** geklickt werden. MacOS zeigt in einer Liste alle Objekte (sprich: Programme und Apps) an, die beim Start und der darauf folgenden Anmeldung des Benutzers geöffnet werden sollen. Die Autostart-Objekte sind also immer abhängig vom Benutzer.

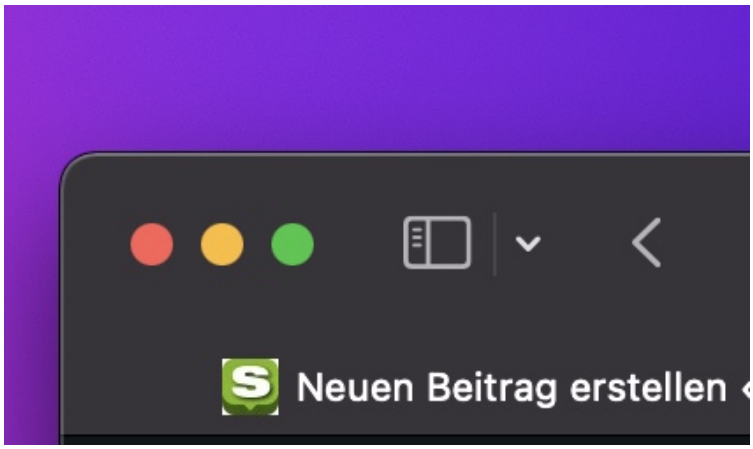


Um ein Objekt aus dem Autostart zu entfernen, klicken Sie den Eintrag an und dann auf das **Minus-Zeichen** unter der Liste. Um ein Objekt hinzuzufügen, klicken Sie auf das **Plus-Zeichen** unter der Liste und wählen Sie dann das Programm aus. Ein Klick auf **Hinzufügen** fügt dann das entsprechende Programm zum Autostart des Benutzers hinzu. Setzt einen Haken neben **Ausblenden**, damit das Programm stumm startet, ohne, dass der Benutzer etwas davon sieht.

Intelligentes Maximieren von Fenstern bei macOS

Fenster enthalten Programme und deren Daten, den Kern Ihrer Arbeit. Wichtig, dass die Daten so gut wie möglich dargestellt werden. Bei macOS gibt es einen tollen Hack, der den benötigten Platz eines Fensters optimiert.

Im Standard sieht der Benutzer nur zwei Möglichkeiten zur Größenanpassung von Fenstern: Entweder werden diese minimiert oder maximiert, alternativ können sie durch Ziehen der Fensterränder manuell die Größe bestimmen. Alle diese Lösungen haben eines gemeinsam: Sie nehmen nur befingt auf die Fensterinhalte Rücksicht. Ein maximiertes Fenster ist in den meisten Fällen für die Inhalte zu groß, ein manuell skaliertes nutzt oft weniger Platz, als sinnvoll wäre.



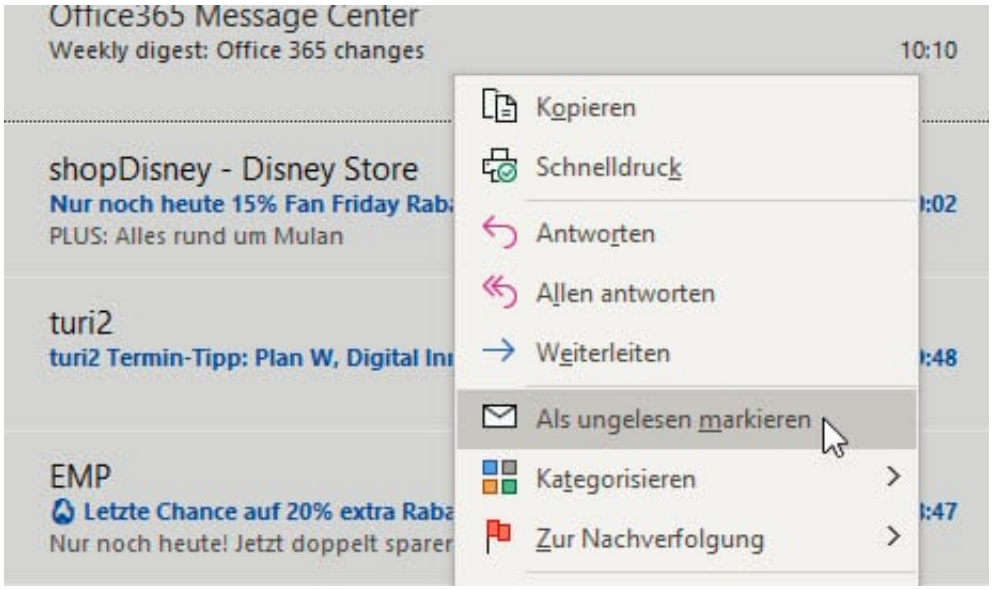
MacOS hat einen versteckten Automatismus, mit dem Ihr ein Fenster in die optimale Größe bringen könnt. Dazu klickt mit der Maus auf den grünen Button oben links. Dabei drückt allerdings parallel zur linken Maustaste die **ALT-Taste**. Mac OS analysiert jetzt den Platzbedarf des Fensters. Bei fixen Bereichen werden diese so groß dargestellt, wie sie es anfordern. Bei Fenstern mit variablen Eingabefeldern versucht macOS eine Anpassung auf Grund von Erfahrungswerten. Hat der Benutzer den Eingabebereich breiter gewählt als macOS es empfehlen würde, dann wird die Breite beibehalten. Nach dem Motto: "Der Benutzer wird wissen, was er tut". Eine manuelle Anpassung ist natürlich weiterhin möglich.

Lesemarkierungen bei E-Mails entfernen

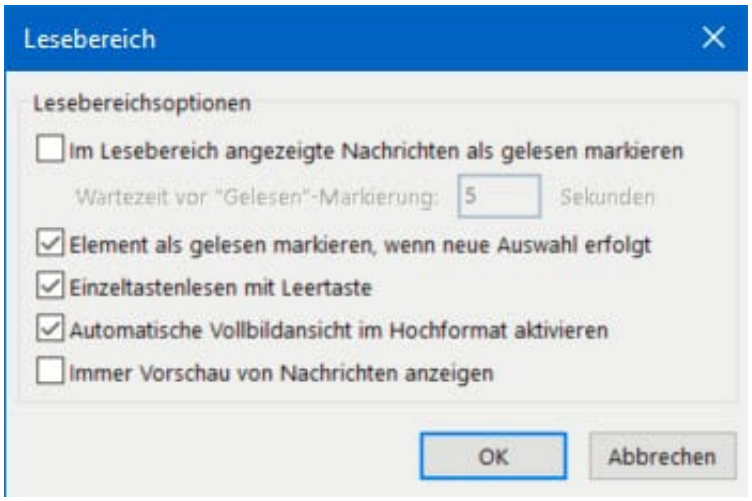
Mehrere Personen, ein E-Mails-Postfach. Wer muss welche E-Mail bearbeiten? Einmal angeklickt wird eine E-Mail als gelesen markiert, auch wenn Ihr sie gar nicht öffnen wolltet. Das lässt sich besser organiseren!

Ob es nun eine Stellvertretung eines Kollegen in der Firma ist, die Betreuung eines Funktionspostfachs mit mehreren Personen einfach nur ein gemeinsam benutzter Rechner: Ihr müsst sicherstellen, dass jeder die Mails bekommt, die er benötigt. Outlook ist auf einzelne Benutzer ausgelegt, lässt sich aber davon überzeugen, auch mit mehreren Anwendern in einem Postfach zu arbeiten.

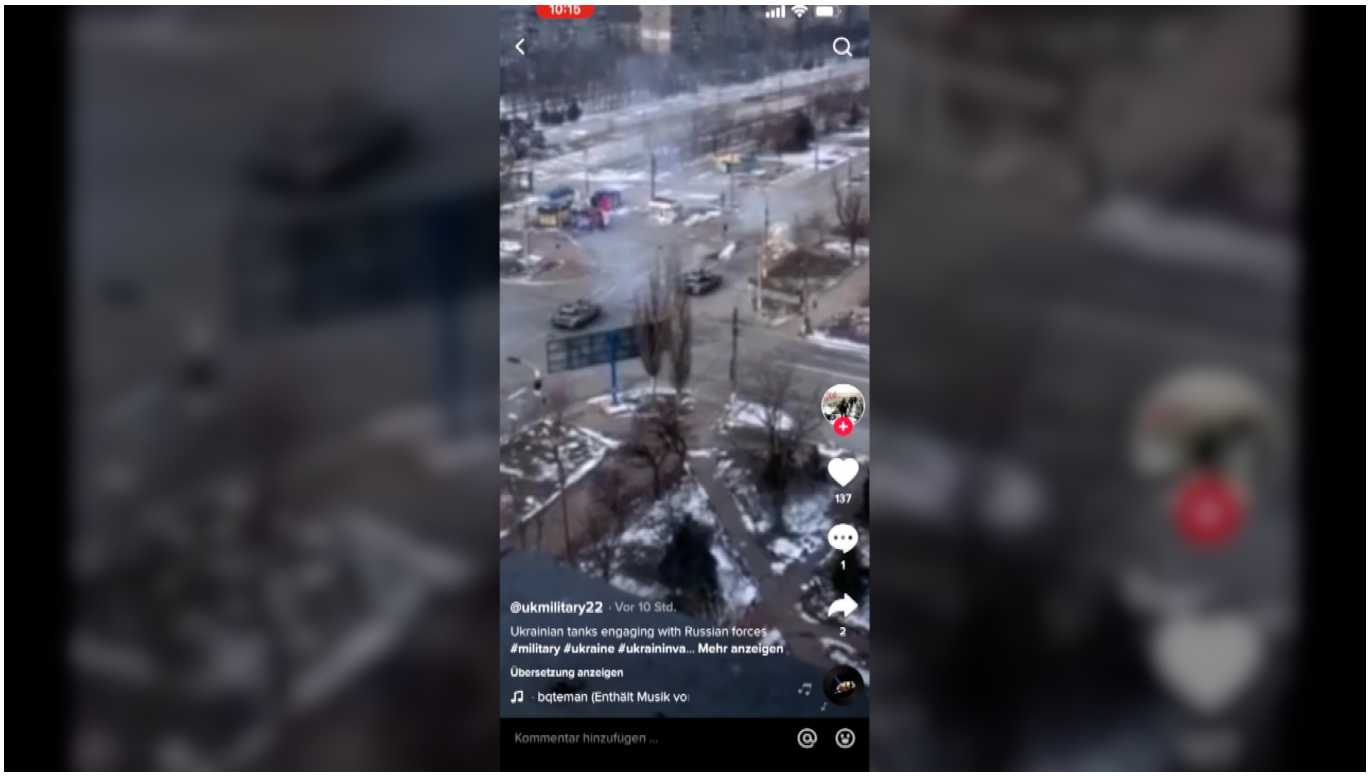
Generell gilt: Die Mails, die ungeöffnet sind, sind noch unbearbeitet. Leider ist im Standard eingestellt, dass Mails nach dem Öffnen automatisch als gelesen markiert werden. Hier kann manuell nachgebessert werden: Klickt eine E-Mail an, die als gelesen markiert ist, dann klickt mit der rechten Maustaste darauf und dann auf **Als ungelesen markieren**. Alle markierten E-Mails werden nun wieder so dargestellt, als wären sie noch nie geöffnet werden.



Um das Problem an der Wurzel zu packen, schaltet einfach die automatische Markierung der E-Mails aus. In Outlook klickt dazu auf **Datei** > **Optionen** > **Erweitert**. Klickt dann auf die Schaltfläche **Lesebereich**. Hier finden sich eine Vielzahl von Optionen, wann und wie E-Mails als gelesen markiert werden. Probiert die für Euch passenden einfach aus!



Über WarTok und Warfluencer



Die Sozialen Medien sind in diesem Ukraine-Krieg ein Phänomen: Sie erlauben den Ukrainern mit der Welt zu kommunizieren. Das macht die Kriegsereignisse greifbarer - und schneller verfügbar.

Der Krieg in der Ukraine – er spielt auch in den Sozialen Netzwerken eine große Rolle. Darüber haben wir hier verschiedentlich schon gesprochen. Heute wollen wir aber mal etwas genauer hinschauen, welche Rolle genau zum Beispiel TikTok, Instagram und andere Dienste spielen können. Ausnahmsweise sind es mal eher positive, erfreuliche Nachrichten. Die Netzwerke übernehmen eine wertvolle Aufgabe: Sie informieren die Welt, was in der Ukraine los ist. Einige Menschen machen das besonders intensiv – sie werden sogar als „WarFluencer“ bezeichnet.

Soziale Medien sehr wertvoll

Die Plattformen fungieren in diesem Krieg wie ein Bindeglied zwischen den Menschen in der Ukraine – und dem Rest der westlich geprägten Welt. In Russland sind die meisten Sozialen Medien ja aktuell verboten und/oder abgeschaltet. Soldaten und Menschen in der Ukraine nutzen Instagram, Tiktok, Twitter und Co., um mit uns zu kommunizieren. Sie zeigen den Kriegsalltag.

Richten Appelle an die Menschen. Das ist umso wichtiger, weil normale Berichterstattung von Zeitungen und Sendern im Krieg ja meist nicht möglich sind.

So viele Eindrucke aus einem Krieg hat die Welt wohl noch nie bekommen – und das fast live, und nicht erst Wochen oder Monate später. Spätestens seit dem Vietnam-Krieg wissen wir, welche Macht Bilder aus einem Krieg haben können. Soldaten der Ukraine zeigen, wie sie kämpfen. Teilweise auch, um Propaganda zu verbreiten: Seht her, wir haben hier ein russisches Flugzeug abgeschossen.

Aber vor allem menschliche Szenen. Auch Soldaten haben Momente, in denen sie rumalbern. Müde sind. Mit Tieren kuscheln. Noch eindrucksvoller ist das, was die Menschen aus der Ukraine posten – vor allem auf TikTok. Es gibt aktuell derart viele Inhalte über den Krieg in der Ukraine auf TikTok, dass TikTok schon WarTok genannt wird.

Aus TikTok wird WarTok

TikTok hat seinen Schwerpunkt verändert. Überraschend, weil TikTok ja eigentlich als reine Spaß-Plattform wahrgenommen wird, völlig unpolitisch.

Das Spektrum ist wirklich groß: Berichte vom Gefecht, aber auch Eindrücke aus dem Kriegsalltag. Ein schönes Beispiel ist Alina Volik. Eine junge Ukrainerin, kein TikTok-Star, die auf ihrem Kanal normalerweise ihren Alltag zeigt – und Eindrücke aus dem Urlaub. Doch seit Kriegsbeginn zeigt sie dort den Alltag in der Ukraine: Wach werden mit Sirenengeheul, ab in den Keller, und wieder herauf.

Den Notfall-Rucksack packen und bestücken. Einkaufen, wenn die Regale voll sind. Das macht sie überaus charmant. „Dieses Treppenhaus ist meine Gym“, schreibt sie – und erklärt, dass sie mehrmals am Tag rauf und runter läuft. TikTok sei ihr Entertainment-Programm. Und Zelenskyi ihr Therapeut. Einzelne Videos von Alina wurden schon weit über eine Million Mal angeschaut. Eine ganz normale junge Frau, die äußerst menschlich berichtet – und so Nähe schafft. Weil es kein Draufschauen ist, keine Propaganda, keine schlimmen Gefechtsszenen.

Wie "Warfluencer" die Wahrnehmung prägen

Aber es sind keineswegs nur Menschen vor Ort, die in den Sozialen Medien Inhalte posten. Auch auf dem Instagram-Kanal von David Beckham gab es Bilder aus der Ukraine zu sehen.

Beckham ist auch Botschafter der Unicef – setzt sich also für Kinder ein. In dieser Funktion hat der prominente Fußballer seinen Instagram-Account für einen Tag einer ukrainischen Ärztin überlassen, die Chefin der Geburtsklinik von Charkiw ist. Das ist wirklich ein interessanter Move: Die Ärztin aus der Ukraine durfte einen Tag lang auf dem Insta-Kanal von Beckham das sagen und zeigen, was sie für wichtig hält. Darüber sollte man nicht schmunzeln, denn Beckham hat 70 Millionen Follower auf Instagram.

Welche Fernsehsendung könnte das von sich sagen? Die Ärztin konnte also unmittelbar 70 Millionen Menschen in der ganzen Welt erreichen – und mehr, denn natürlich wurden die Posts der Ärztin auf Beckhams Kanals auch weitergereicht. Die Reichweite war also noch entschieden größer. Die Ärztin hat ihre Chance auf jeden Fall genutzt und auf dem Kanal von Beckham über ihren Kriegsalltag berichtet – und vor allem auch über die Not, die an der Klinik herrscht. Auf diese Weise wird blitzschnell Nähe hergestellt, da wo man es überhaupt nicht erwarten würde.

Wie "Warfluencer" die Wahrnehmung prägen

Es geistert schon der Begriff „WarFluencer“ herum, den der Spiegel-Kolumnist Sascha Lobo jetzt geprägt hat.

Stellt sich die Frage: Kann jeder zum WarFluencer werden - und/oder ab wann ist man einer?

Das ist eigentlich ein passender Begriff. Denn in der Tat sehen wir gerade ein interessantes Phänomen: Putin versucht mit aller Macht, die Kontrolle und Deutungshoheit über den Krieg zu behalten. Das gelingt ihm aber nur, indem die Meinungsfreiheit beschnitten und Medien verboten oder gesperrt werden. Die Ukrainer hingegen nutzen die Sozialen Medien, die Stärken der Sozialen Medien, und informieren die Welt, kommunizieren mit der Welt.

Das muss man im Einzelfall sicher auch kritisch hinterfragen, aber auf jeden Fall verändert die Bilderflut aus der Ukraine die Wahrnehmung, wie die Krieg verläuft,

welches Leid er anrichtet. Die Inhalte fließen ja natürlich auch in die regulären Medien ein. Und damit: Ja, Personen wie Alina sind WarFluencer – im besten Sinn. Aber mehr als das: Anders als viele Influencer, die sich regelrecht prostituieren und für Geld alles machen, bekommen diese WarFluencer ja kein Geld. Sie machen es, weil sie es wollen oder können.

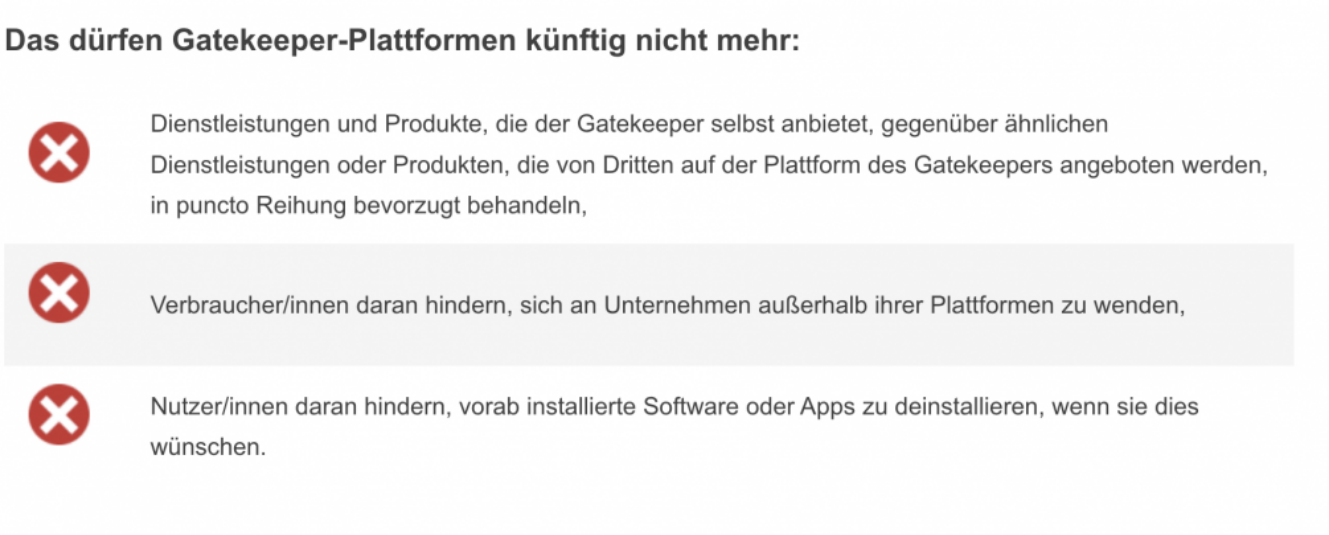
Und natürlich hat auch eine Aktion wie die von David Beckham einen enormen Einfluss – weil Bilder aus der Ukraine auch in den Timelines von Beckham-Fans auftauchen, die sich womöglich sonst nicht für das Thema interessieren. Auch ihn könnte man also als WarFluencer bezeichnen. Es ist eindeutig so, dass Zeitungen, Radio und Fernsehen nicht mehr die einzigen Medien sind, in denen man sich über den Krieg informieren kann.

Digital Markets Act: Deutlich mehr Regeln für Tech-Konzerne

Apple, Google, Microsoft und andere Tech-Giganten müssen sich auf neue Gesetze in der EU vorbereiten: Kommission, Rat und Parlament haben den „Digital Markets Act“ auf den Weg gebracht. Für Verbraucher bedeutet das im Wesentlichen mehr Wahlfreiheit und Auswahl.

Schon seit einigen Jahren bereiten EU-Kommission und EU-Parlament zwei Regelpakete vor, die vor allem die großen Tech-Konzerne einhegen sollen: Im „**Digital Services Act**“ (DSA) geht es vor allem um die großen Plattformen, im „**Digital Markets Act**“ (DMA) um einen fairen Wettbewerb im Netz. Letzterer ist jetzt von der EU beschlossen worden – und soll „eine neue Ära der Tech-Regulierung einläuten“, wie es im EU-Parlament heißt.

Das ist wahrscheinlich ein wenig übertrieben, aber eins steht fest: Tech-Konzerne wie Google, Microsoft, Facebook, Apple und andere müssen sich künftig an deutlich strengere Regeln halten. Verstoßen sie dagegen, drohen harte Strafen und Sanktionen.



Gatekeeper: Google, Microsoft, Apple, Facebook

Gemeint und vom neuen Gesetz betroffen sind nur die größten Spieler am Markt, sogenannte „Gatekeeper“, die Dienste wie Betriebssysteme, Internet-Browser, Messenger oder soziale Medien anbieten und mindestens 45 Millionen Nutzer pro Monat haben. Das Gesetzpaket richtet sich also konkret an die Großen der Branche.

Es geht darum, mehr und vor allem fairen Wettbewerb zu ermöglichen – und auf diese Weise den Verbraucherschutz zu stärken. Große Tech-Konzerne versuchen in der Regel, die Konkurrenz kleinzuhalten. So wurde zum Beispiele Google vorgeworfen und auch nachgewiesen, in seinem mobilen Betriebssystem Android die eigenen Anwendungen zu bevorzugen – und den eigenen Browser Chrome zu promoten. Apps und Angebote kleiner Konkurrenten hatte so keine Chance.

So etwas soll in Zukunft verhindert werden: Große Tech-Konzerne sind angehalten, sich für den Wettbewerb zu öffnen. Nutzer sollen vorinstallierte Apps häufiger löschen können (etwa Google Maps oder den jeweiligen Standard-Browser von Apple, Microsoft oder Google).

Mehr Verbraucherschutz und Wahlfreiheit

Darüber hinaus sollen Verbraucher einen Dienst auch nutzen können, ohne gleich ein ganzes Paket aller Angebote eines Gatekeepers hinweg zustimmen zu müssen. Nutzer sollen nicht mehr allen AGBs und der freien Verwendung ihrer Daten zustimmen müssen, nur um einen Messenger oder einen anderen Dienst verwenden zu können. Jeder einzelne Dienst soll künftig separat für sich stehen – damit Verbraucher frei wählen können.

Beschlossen ist auch eine „Interoperabilität“ von Messengern. Etwas, das viele Netzaktivisten und Verbraucherschützer schon lange fordern. Interoperabilität bedeutet konkret: Whatsapp, iMessage und der Facebook Messenger müssen sich künftig für konkurrierenden Anwendungen wie Signal oder Threema öffnen. Es soll möglich sein, aus jeder Messenger-App heraus Nutzer in jedem anderen Messenger anzuschreiben und Nachrichten auszutauschen.

Interoperabilität bei Messengern kommt

Das soll verhindern, dass jeder einen Messenger wie WhatsApp nutzten muss, bloß weil alle schon da sind (sogenannter Netzwerk-Effekt). Stattdessen sollen Nutzer künftig eine wirklich freie Wahl haben. Mit iMessage eine Nachricht an WhatsApp schicken: Kein Problem. Erst später sollen dann auch plattformübergreifende Gruppen-Chats möglich werden.

Aber auch Apple wird das neue Gesetz zu spüren bekommen. Der Konzern hat das Gesetz bereits kritisiert: Es drohten Datenschutz- und Sicherheitslücken. Denn der DMA verpflichtet Apple zur Öffnung seines Betriebssystems für alternative App-Stores und Zahlungsanbieter.

Auch Apple-Nutzer haben künftig mehr Auswahl

Derzeit müssen Kunden Apples Infrastruktur nutzen, um Apps zu laden. Anders als bei Android ist es unmöglich, Apps aus anderen Quellen als den App-Store von Apple zu laden. Das soll sich ändern – bedeutet aber in der Tat auch mehr Sicherheitsrisiken für die Anwender. Darüber hinaus sollen auch alternative Bezahlsysteme zugelassen werden. Für Apple eine bedrohliche Situation, da der Konzern 30% Provision an allen Einnahmen verdient.

Für Verbraucher bedeutet das aber auf jeden Fall: mehr Auswahl. Allerdings werden dadurch auch die hohen Sicherheitsstandards von Apple aufgeweicht - was Apple auch erwähnt und kritisiert.

Verbesserter Datenschutz

Auch in punkto Datenschutz bewegt der DMA etwas: Tech-Konzernen wie Meta und Google soll es künftig sein verboten sein, Daten aus unterschiedlichen Quellen zu verbinden, sofern Nutzer nicht ihre ausdrückliche Zustimmung erteilt haben. Das betrifft vor allem Facebook: Die Daten aus Instagram, Facebook, WhatsApp und Facebook Messenger dürfen nicht mehr automatisch miteinander verbunden werden. Zumindest muss Facebook die Möglichkeit bieten, das so zu handhaben – freiwillig zustimmen geht immer noch.

Es bleibt abzuwarten, wie die einzelnen Regeln alle konkret umgesetzt werden. Doch die Verbraucherrechte sind auf jeden Fall gestärkt.

Fake-Videos erkennen: Auf Details achten

Derzeit kursieren viele Fake-Videos, die gezielte Desinformationen rund um den Ukraine-Konflikt beinhalten. Urheber sind häufig russische Trollfabriken, die das öffentliche Meinungsbild mit gezielten Desinformationen manipulieren wollen. Der Unterschied zwischen Fake-Videos und Deep-Fakes – und wie sich solche Fälschungen erkennen lassen.

Videos verbreiten sich auf Facebook, Youtube, Instagram und TikTok sehr schnell. Was Emotionen schürt, das wird von den Algorithmen ungeachtet von Inhalt oder Wahrheitsgehalt besonders häufig angezeigt – und damit rasant verbreitet.

Genau mit diesem Mechanismus spielen Personen und Gruppen, die Fake-Videos produzieren.

Oft reicht es schon, ein paar vorhandene Bilder neu zusammenzuschneiden, mit Off-Texten zu versehen (gesprochener Text), mit Soundeffekten zu garnieren und/oder mit Untertiteln auszustatten, um einen völlig falschen Eindruck zu vermitteln. Natürlich kommen auch gezielt gedrehte Szenen zum Einsatz. Da beim Posten keine Prüfung auf Wahrheit oder Echtheit erfolgt, ist es leicht, auf

den Plattformen Fake-Videos jeder Art zu verbreiten.

Information als Waffe

Stichwort: „Information als Waffe“. Es ist hinlänglich bekannt, dass der Kreml sogenannte „Trollfabriken“ finanziert, die nur das eine Ziel haben: Sie sollen gezielt Desinformation verbreiten. In Wort, Bild und in Form von Videos – und das auf allen gängigen Plattformen wie Youtube, Facebook, Twitter, Instagram und Co. Die Mitarbeiter dieser Trollfabriken verbreiten rund um die Uhr Unwahrheiten – um so die öffentliche Meinung zu verändern und zu prägen.

Das aktuell aufgetauchte Video, in dem behauptet wird, eine Gruppe Ukrainer hätte einen 16-Jährigen in Euskirchen zu Tode geprügelt, ist ein typisches Beispiel. Ein solches Ereignis ist absolut denkbar und möglich – und wird deswegen von vielen Menschen ungeachtet der Richtigkeit empört geteilt. Auf diese Weise entsteht ein unaufhaltsamer Schneeballeffekt. Bis klar ist, dass es sich um ein Fake-Video handelt bewusste mit Falschbehauptungen, ist der Schaden längst angerichtet.

Fake-Videos erkennen: Für Laien schwierig

Solche Fake-Videos als solche zu erkennen und zu enttarnen, ist für Laien nicht besonders leicht. Am besten ist, im Zweifel bei Fakten-Checkern wie Mimikama nachzuschauen, ob dort unabhängige Journalisten solche oft viral gehenden Bilder oder Videos bereits auf ihren Wahrheitsgehalt untersucht haben. Wichtig ist aber auf jeden Fall, solche Inhalte nicht ungeprüft weiterzureichen. Liken oder Teilen führt nur dazu, selbst zum Schneeballeffekt beizutragen.

Noch heikler sind sogenannte Deep Fakes. Das sind Videos, die mit Hilfe von Künstlicher Intelligenz (KI) erzeugt wurden. Dabei werden Gesichter ausgetauscht oder Personen ganz andere Worte in den Mund gelegt. Was vor wenigen Jahren noch Forschungsprojekte waren, ist heute in der Popkultur angekommen. Mit Apps wie Reface oder Wombo kann jeder mit seinem Smartphone sein eigenes Gesicht in ein Video oder die Szene eines Kinofilms montieren. Hier sorgt das für Spaß – in vielen anderen Situationen kann es aber enormen Schaden verursachen.

Deep Fakes: Mit Hilfe von KI erzeugte Fakes

Profis können technisch noch sehr viel überzeugendere Aufnahmen erstellen. Und so kursieren bereits Deep-Fake-Videos von Putin und Selenskyi im Netz, in denen die Politiker jeweils ihre Kapitulation bekanntgeben. Es ist damit zu rechnen, dass noch mehr solcher Deep-Fake-Videos im Ukraine-Konflikt auftauchen – um die Öffentlichkeit zu täuschen und die Meinung zu manipulieren.

Bei technisch gut gemachten Deep-Fakes ist es nicht einfach, sie als Laie als solche zu erkennen. Es gibt manchmal Hinweise, vor allem an den Kanten des Gesichts: Wenn die Übergänge zum Hintergrund oder zur Bekleidung nicht stimmen, Schatten fehlen oder etwas unsauber erscheint, können das Hinweise auf eine Fälschung sein. Letztendlich feststellen können das aber nur Profis, die forensische Untersuchungen des Videomaterials vornehmen.

Deshalb: Selbst wenn in einem Video prominente Personen etwas behaupten, sollte dem nicht einfach geglaubt werden. Es ist zweifellos besser, eine Begutachtung von Fakten-Checkern und/oder seriösen Medien abzuwarten.

Auch wenn das im Eifer des Gefechts manchmal eine kleine Herausforderung bedeutet: Nicht alles, was echt aussieht und empört, gleich mit der Community teilen.

Hidden Tracks aus MP3-Dateien extrahieren

Früher Bonus, heute fast Standard: Hidden Tracks - Musikstücke, die sich hinter einer langen Pause auf der CD oder LP verbergen. Nach der ersten Überraschung wollt Ihr die Pause nicht mehr abwarten müssen? Kein Problem!

Im Normalfall habt Ihr die Musik dann in Form einer MP3- oder FLAC-Datei zur Verfügung. Ist das nicht der Fall, dann bietet sich ein Programm wie XLD an, um die CD in Dateien umzuwandeln. Zur Bearbeitung ladet Euch das kostenlose Tool Audacity herunter. Nach dem Laden der Musikdatei lässt sich schnell identifizieren, wo die Stille nach dem letzten "echten" Musikstück und wo der Hidden Track sind.

Nun gilt es, den Hidden Track zu markieren. Das funktioniert in Audacity genauso wie bei Word oder anderen Programmen: Mauszeiger auf den linken Rand, linke Maustaste gedrückt halten und Maus ans Ende des rechten Randes ziehen.

Das Entfernen des Rests der Musik - anders betrachtet das Zuschneiden auf den Hidden Track versteckt sich tief in den Menüs von Audacity: Unter **Bearbeiten** > **Spezial Entfernen** > **Audio Zuschneiden** wird alles Audio außer dem Hidden Track gelöscht.

Mit aktivierter Markierung klickt jetzt auf **Datei** > **Exportieren** > **Ausgewähltes Audio exportieren**. Nach der Eingabe des sprechenden Dateinamens und des Speicherortes exportiert Audacity den Hidden Track als separate Datei auf die Festplatte.

Stichwort: Was ist eine Trollfabrik?

Derzeit sind sie wieder häufiger zu hören: Begriffe wie "Troll", "Trollfabrik", "Trollarmee" oder "Putin-Bots." Hier mal eine (kompakte) Erklärung, was sich hinter den Begriffen eigentlich verbirgt.

Ein **Troll** ist ein unberechenbares Fabelwesen in der nordischen Mythologie, dem man lieber nicht begegnen möchte. Der Begriff selbst ist schon sehr alt. Es gab ihn schon im Mittelhochdeutschen.

Heute bezeichnet „Troll“ eine echte Person, die in der Netz-Kommunikation durch Provokation, Störung, Beleidigungen und schiere Häufigkeit der Kommunikation auffällt. Trolle rüpeln sich durchs Netz: Sie melden sich überall zu Wort, meist mit wenig hilfreichen Kommentaren – und weil sie das sehr aktiv tun, erschweren sie jede angenehme oder sinnvolle Kommunikation.

Es gibt sehr viele Trolle, sie können auf Twitter Hashtags kapern, Diskussionen erschweren, auf Facebook blöde Fragen stellen. Es ist so ziemlich jede Art von Störung denkbar. Trolle agieren unter ihrem echten Namen, im Namen anderer, unter Pseudonym oder auch anonym.

Trollarmee und Trollfabrikl

Der Troll gehört schon immer zum Internet. Er ist ein lästiges, aber bisweilen auch unterhaltsames Phänomen.

Doch es gibt auch staatlich kontrollierte Trolle, die gezielt Propaganda verbreiten. Es sind so viele, dass von einer **Trollfabrik** oder **Trollarmee** die Rede ist. Weil ein regelrechtes Heer von Trollen – bezahlt vom Kreml – in westlichen Netzwerken und Plattformen unterwegs sind, um überall Desinformation zu platzieren und so die öffentliche Meinung zu manipulieren.

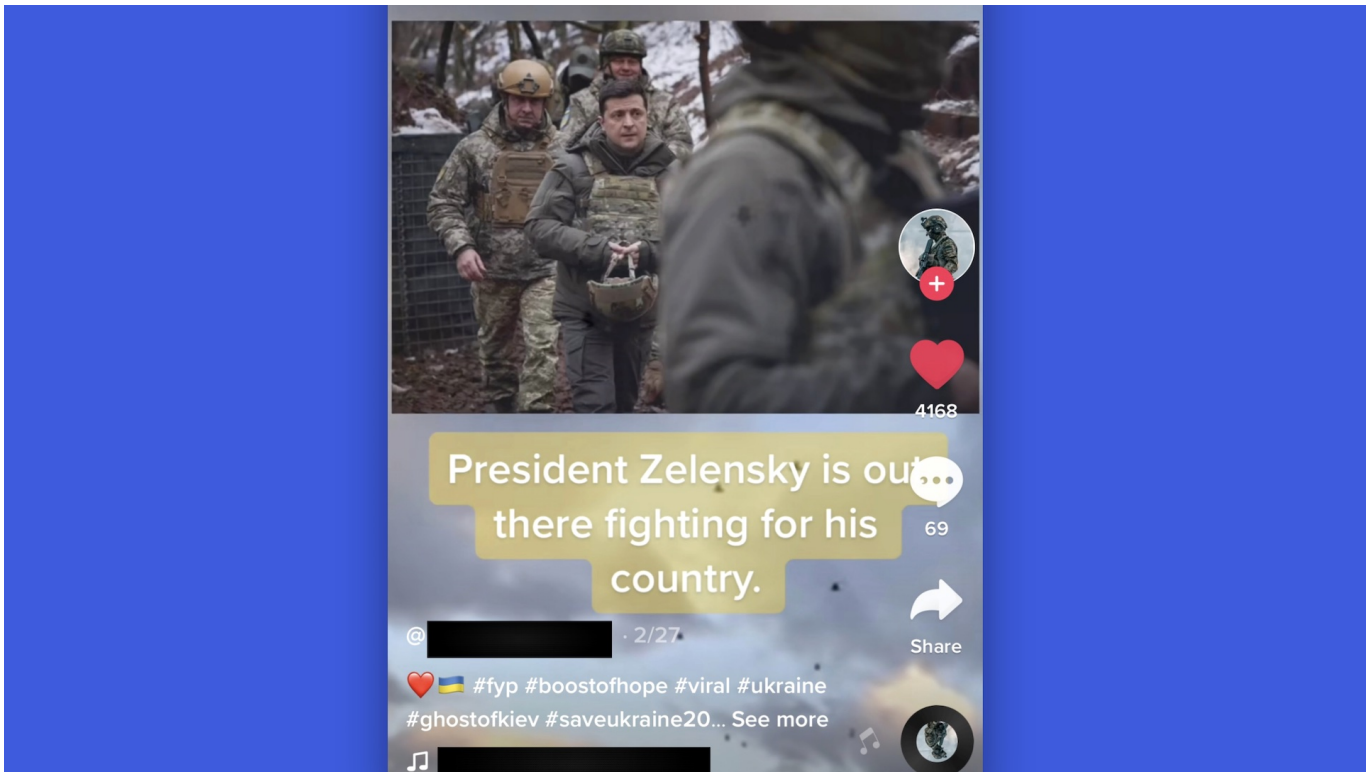
Mit Falschbehauptungen, Fake-News und Deep-Fakes, die praktisch überall platziert werden.

Das machen nicht nur echte Menschen, sondern auch Computerprogramme – die, entsprechend programmiert –, das Netz durchforsten und überall dort, wo bestimmte Schlagwörter vorkommen, automatisiert ihre Propaganda platzieren.

Solche Systeme werden auch **Putin-Bots** genannt.

https://soundcloud.com/user-999041145/stichwort-trollarmee?utm_source=clipboard&utm_medium=text&utm_campaign=social_sharing

TikTok ist zum WarTok geworden



Eigentlich ist TikTok eine reine Spaß-Plattform: Hier stehen Entertainment und Tanzeinlagen im Vordergrund. Doch seit dem Krieg in der Ukraine bietet die Video-App auch viele Inhalte über den Krieg an, seriöse wie unseriöse.

TikTok hat über eine Milliarde regelmäßig aktive Nutzer weltweit und ist damit zweifellos neben Facebook und Instagram eine der führenden Plattformen. Auf TikTok posten vor allem junge Menschen Videos – und schauen sie sich die anderer User an. Normalerweise stehen Spaß, Sport, Unterhaltung und Albernheiten im Vordergrund.

TikTok zeigt Kriegsalltag in der Ukraine

Doch das hat sich seit dem Krieg in der Ukraine geändert. Der kriegerische Konflikt ist Thema auf der Plattform. Es gibt jede Menge Bilder aus erster Hand zu sehen – gedreht von Menschen in der Ukraine, auch von Soldaten. Auf diese Weise wollen die Ukrainer mit der Welt sprechen.

Ein prominentes Beispiel ist Alina Volik. Die 18-Jährige aus Saporischschja ist nur eine von vielen Menschen aus der Ukraine, die regelmäßig auf TikTok Videos

posten. Vor dem Krieg hatte sie 22.000 Follower – heute sind es 78.000. Alina zeigt den Menschen auf TikTok, wie sich ihr Alltag verändert hat: Notfall-Rucksack packen, bei Alarm aufstehen und unter Sirenengeheul in den Keller flüchten.

Einblicke in das Leben von Alina

„Das ist meine Gym“, schreibt Alina – und zeigt das Treppenhaus, das zum Keller führt. Sie zeigt leere Einkaufsregale, zerstörte Straßen und Häuser, berichtet, wie sie schläft und wie es sich anfühlt, in ständiger Angst zu leben. Äußerst realistische Einblicke in ihr Leben, ohne Dramaturgie – und deshalb so ergreifend.

Alina ist längst nicht die einzige, die offen und ehrlich gezeigt, wie Krieg in der Ukraine aussieht – und wie das Leben im Krieg. Sie teilt ihre Eindrücke, lässt die Welt teilhaben, sie ist dabei weder aggressiv noch anklagend. Es gibt aber auch Soldaten, die ihren Kriegseinsatz zeigen. Sogar Soldaten, die Tanzeinlagen präsentieren – ganz wie auf TikTok üblich. Das sind dann schon eher makabre Eindrücke.

TikTok ist derzeit ein WarTok

Die Videos werden nicht nur auf TikTok gepostet, sondern auch angeschaut. 200.000 Menschen zum Beispiel haben das Kurzvideo „Good Morning Sound in Ukraine“ gesehen – es zeigt, wie Alina durch Sirenengeheul wach wird. Die ungewohnte Popularität solcher Videos auf TikTok haben der Plattform den Namen „**WarTok**“ eingebracht.

Die Popularität des Themas auf TikTok ist allerdings auch ein Problem: TikTok wird auch mit Desinformationen geflutet. Videos und angebliche „Informationen“, die in der Regel aus Russland kommen (aber keineswegs nur) und die öffentliche Meinung bewusst manipulieren sollen. Die Fakten-Checker von NewsGuard (eine private Initiative) oder Mimikama ermitteln regelmäßig Falschinformationen, die viral gehen – auch auf TikTok.

Desinformationen aus russischer und ukrainischer Quelle

Das Besondere an TikTok ist laut NewsGuard aber: TikTok zeigt neuen Nutzern innerhalb von Minuten Desinformation über den Krieg an – selbst wenn sie gar nicht nach Inhalten mit Bezug zur Ukraine suchen. Bedeutet: Die Algorithmen

präsentieren auch Menschen Videos mit Desinformationen aus der Ukraine, die gar nicht ausdrücklich danach suchen oder sich andere Videos zu diesem Kontext angesehen haben.

Um das zu untersuchen, erstellte ein Team von sechs Analysten von NewsGuard im März 2022 neue Konten auf TikTok und führten zwei Experimente durch. Hier wurde eine ganz gewöhnliche der App simuliert. Im ersten Experiment wurden die Analysten angewiesen, 45 Minuten lang durch den personalisierten “For You”-Feed von TikTok zu scrollen und alle Videos mit Bezug zum Russland-Ukraine-Konflikt in voller Länge anzuschauen, aber keinen Konten zu folgen oder eigene Suchen durchzuführen.

TikTok zeigt schon nach 40 Minuten Kriegsinhalte

Bereits innerhalb von 40 Minuten nach Anmeldung auf TikTok wurden allen NewsGuard-Analysten falsche oder irreführende Inhalte über den Krieg in der Ukraine angezeigt. Darunter waren sowohl pro-russische als auch pro-ukrainische Unwahrheiten.

Die Experten von NewsGuard kommen zu dem Schluss: TikTok unternehme zu wenig gegen gezielte Desinformation und nehme bewusst in Kauf, dass User auf der Plattform völlig ungewollt Kriegsinhalte zu sehen bekommen.

Angesichts der Tatsache, dass TikTok vor allem durch sehr junge Menschen genutzt wird, ein besorgniserregender Sachverhalt. Eltern und Pädagogen sollten das wissen und mit ihren Kindern darüber sprechen – und den TikTok-Konsum sorgfältig überwachen.

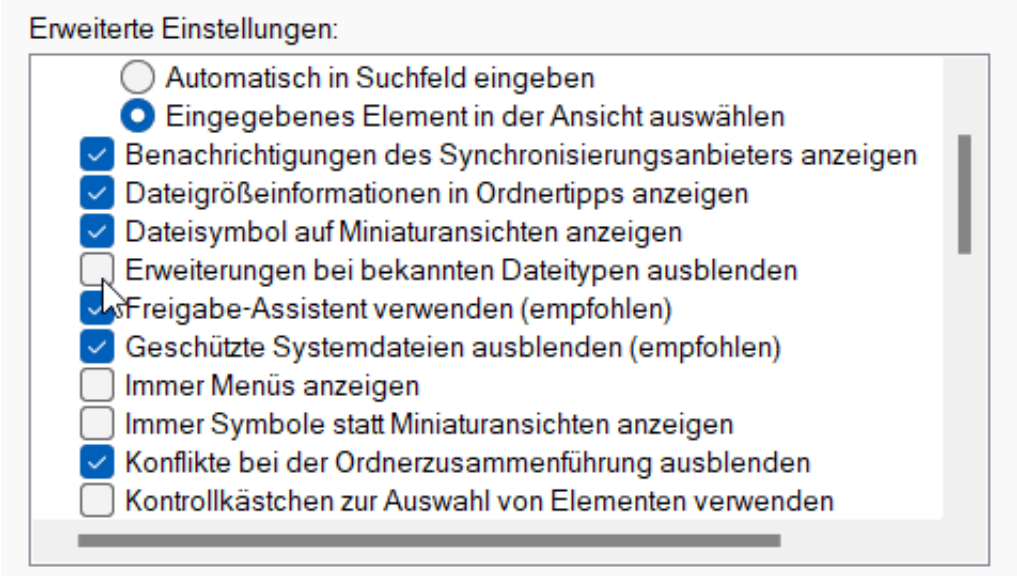
Dateinamenerweiterungen in Windows anzeigen

Manchmal ist es wichtig, den Typ einer Datei erkennen zu können. Der wird im Standard bei Windows nicht angezeigt. Mit einem kleinen Hack lässt sich das korrigieren.

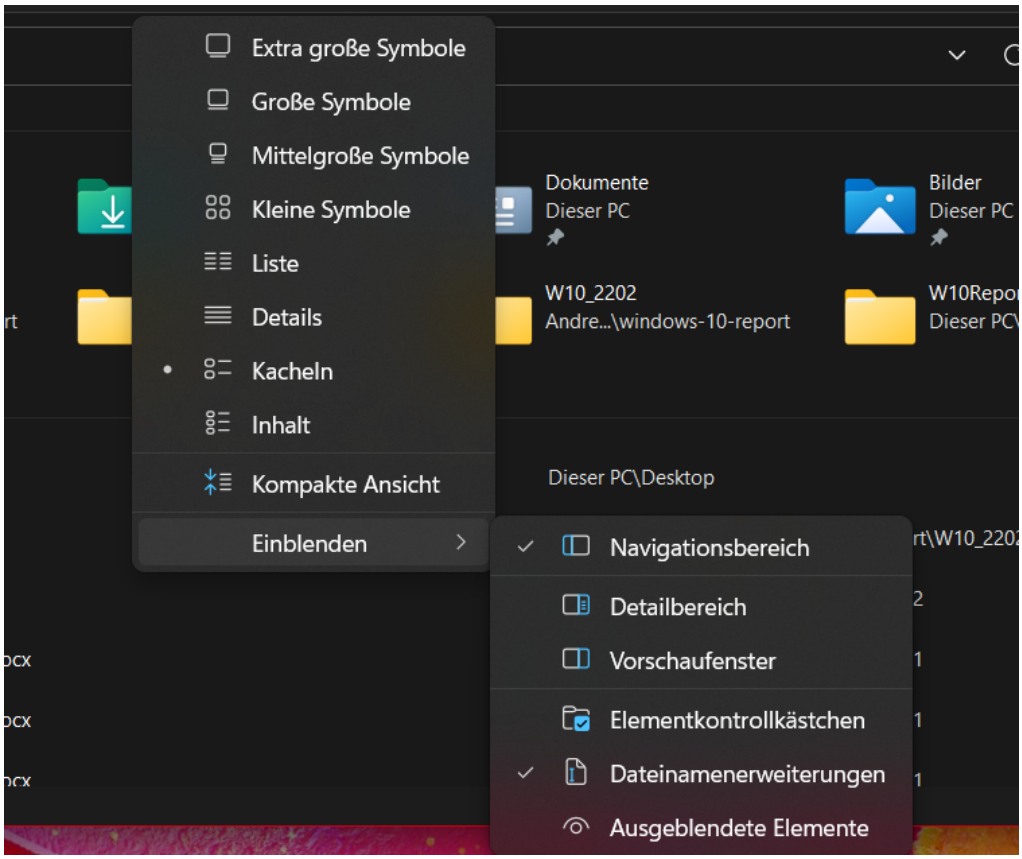
Die Dateinamen von Windows haben zwei Teile, die von einem Dezimalpunkt voneinander getrennt werden. Der erste Teil dient der reinen Identifikation der Datei, sollte möglichst sinnvoll gewählt werden. Am Ende ist es Windows egal, ob dieser aus einer wilden Ziffern- und Zahlenkombination besteht oder aus lesbarem Text. Hauptsache, der Eigentümer der Datei kann sie zuordnen.

Der zweite Teil des Namens gibt den Typ der Datei an, der vor allem für die Zuordnung des Programmes, dass die Datei öffnet, zuständig ist. Diese Zuordnung lässt sich über diesen Hack verändern.

Im Standard blendet Windows die Erweiterung aus, lässt es aber zu, dass der Benutzer diese anzeigen lässt. Dazu kann in jeder Windows-Version in den Ansichtsoptionen unter **Ansicht** > **Erweiterungen bei bekannten Dateitypen ausblenden** der Haken entfernt werden,



In Windows 11 ist es noch einfacher: Klickt im Explorer auf **Anzeigen** > **Einblenden** > **Dateinamenerweiterungen** und setzt den Haken, um die Erweterungen einzuschalten bzw. entfernt den Halen, um sie nicht anzeigen zu lassen.



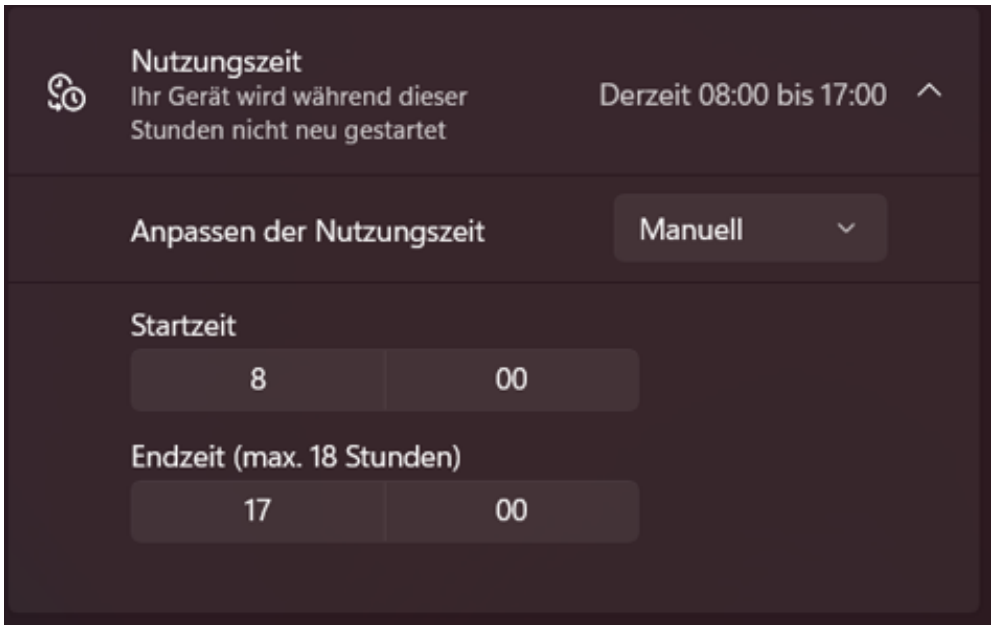
Wichtig: Die Dateinamen-Erweiterungen dürfen nicht manuell verändert werden - beziehungsweise nur dann, wenn es unbedingt nötig ist. Eine XLS-Datei, die plötzlich in DOC umbenannt wird, würde Windows mit Word öffnen. Mit dem Ergebnis, dass sie nicht oder falsch angezeigt würde.

Automatische Updates von Windows

Das Betriebssystem ist der erste und wichtigste Punkt, über den Angreifer versuchen, ins System zu kommen. Gleichzeitig bietet das Betriebssystem viele übergreifende Funktionen, die das verhindern sollen. Ein immer aktuell gehaltenes Betriebssystem ist schon einmal ein guter Basisschutz.

Manuelle Prozesse sind meist nicht optimal. Sie verlassen sich auf die schwächste Komponente an unseren Rechnern: Den Menschen. Das hat auch Microsoft nach vielen Jahren erkannt und mit Windows 10 Updates quasi verpflichtend gemacht. Wo Ihr bei früheren Windows-Versionen noch dauerhaft manuell nach Updates suchen (lassen) konntet, machen Windows 10 und 11 das zwingend automatisch.

- Liegt ein Update vor, dann erscheint in der Taskleiste ein Symbol mit zwei runden Pfeilen und einem Punkt daran.
- Ein Klick darauf öffnet das Update-Menü. Dieses kann auch durch **Einstellungen** > **Windows Update** manuell aufgerufen werden.
- Wenn ein Update einen Neustart erfordert, dann führt Windows die Installation außerhalb der festgelegten Nutzungszeit statt (dazu gleich mehr).
- Ein Klick auf **Jetzt neu starten** stößt die Installation des Updates direkt an. Vorsicht dabei: Vorher solltet Ihr alle Daten speichern und Programme beenden. Das stellt sicher, dass im unwahrscheinlichen Fall keine Daten verloren gehen.
- Die Installation kann mehrere Neustarts mit sich bringen, abhängig von der Komplexität des Updates.
- Nach Abschluss könnt Ihr Windows wieder normal nutzen.



Planen des Neustarts

Der optimale Zeitpunkt für ein Update ist für jeden Anwender anders. Meist aber gibt es regelmäßig Phasen, zu denen Ihr den Rechner nicht benutzt. Diese könnt Ihr individuell festlegen:

- Klickt auf **Einstellungen** > **Windows Update** > **Erweiterte Optionen** > **Nutzungszeit**.
- Im Standard legt Windows die Nutzungszeit anhand Eurer tatsächlichen Nutzung automatisch fest: Wenn Ihr zwischen 08:00 und 17:00 meist am Rechner sitzt, dann wird dieser Wert angenommen.
- Klickt auf die Schaltfläche **Automatisch** und wählt im sich öffnenden Menü **Manuell**
- Legt die **Startzeit** und die **Endzeit** manuell fest. Die außerhalb dieser Angaben liegenden Zeiten verwendet Windows als mögliche Update-Zeiten.