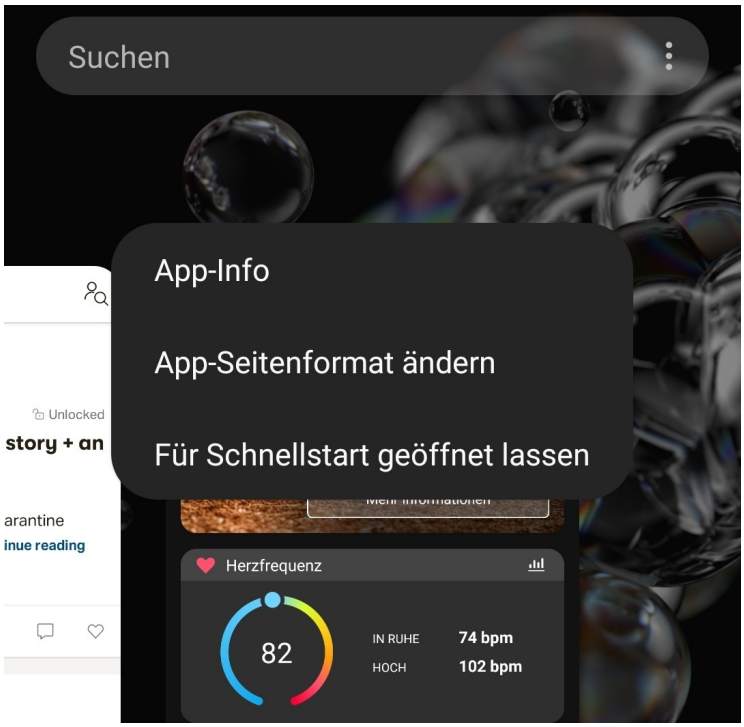
Schieb Report

Ausgabe 2022.11

Apps beim der Samsung S22-Serie im Vordergrund halten

Smartphones sind vor allem von der Kapazität ihres Akkus abhängig. Ist der leer und keine Steckdose und kein Ladegerät in der Nähe, dann ist die Nutzung schnell am Ende. Da ist es nur logisch, wenn die Stromspareinstellungen so konfiguriert sind, dass der Akku möglichst lange hält. Das allerdings kann böse Nebeneffekte haben!

Android schaut sich den Akkuverbrauch und die Nutzung von Apps an, um Bösewichter zu identifizieren. Und wenn eine App nicht benötigt wird, dann wird sie einfach geschlossen. Ohne Rücksicht auf Verluste. Eine App, die nicht läuft, kann aber auch keine neuen Nachrichten empfangen und benachrichtigen. Dumm, wenn Sie beispielsweise auf eine wichtige WhatsApp warten!



Zusätzlich zum Stromsparmodus für Apps können Sie explizit Apps auswählen, die auf jeden Fall weiterlaufen sollen, quasi für das automatische Beenden gesperrt sind. Diese Funktion ist bei der neuen S22-Serie von Samsung anders implementiert als sie es vorher war.

Gehen Sie über ein Wischen vom linken unteren Bildschirmrand nach oben in die Übersicht der laufenden Programme. Tippen Sie mit dem Finger in den Kreis, der das Symbol der App ist, dann auf **Für Schnellstart geöffnet lassen**.

Aktualisierung eines NAS durchführen

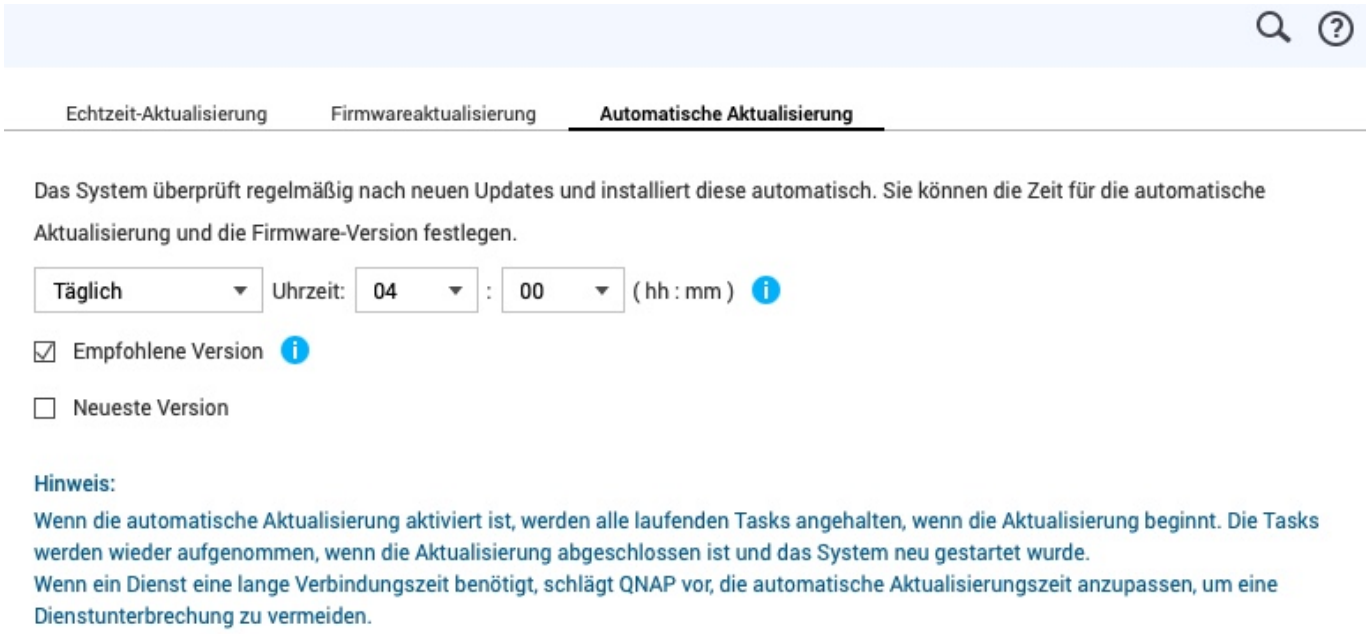
Manchmal könnte man meinen, alle Geräte wollen Updates. Auch die, von denen man es auf den ersten Blick nicht erwartet wie beispielsweise Netzwerkfestplatten (NAS). Das ist gut so: Auch die sind Gegenstand von Angriffen aus dem Internet!

Netzwerkfestplatten (NAS, Network Attached Storage) sollen eigentlich nur Daten zentral im eigenen Netzwerk speichern. Wie so oft bei technischen Geräten geht der Anwendungsbereich aber viel weiter: Sie fungieren als FTP-Server, als virtueller PC und vieles mehr. Das bringt mit sich, dass sie aus dem Internet erreichbar sind. Diese Erreichbarkeit hat einen Haken.

Erreichbarkeit ist auch Angreifbarkeit

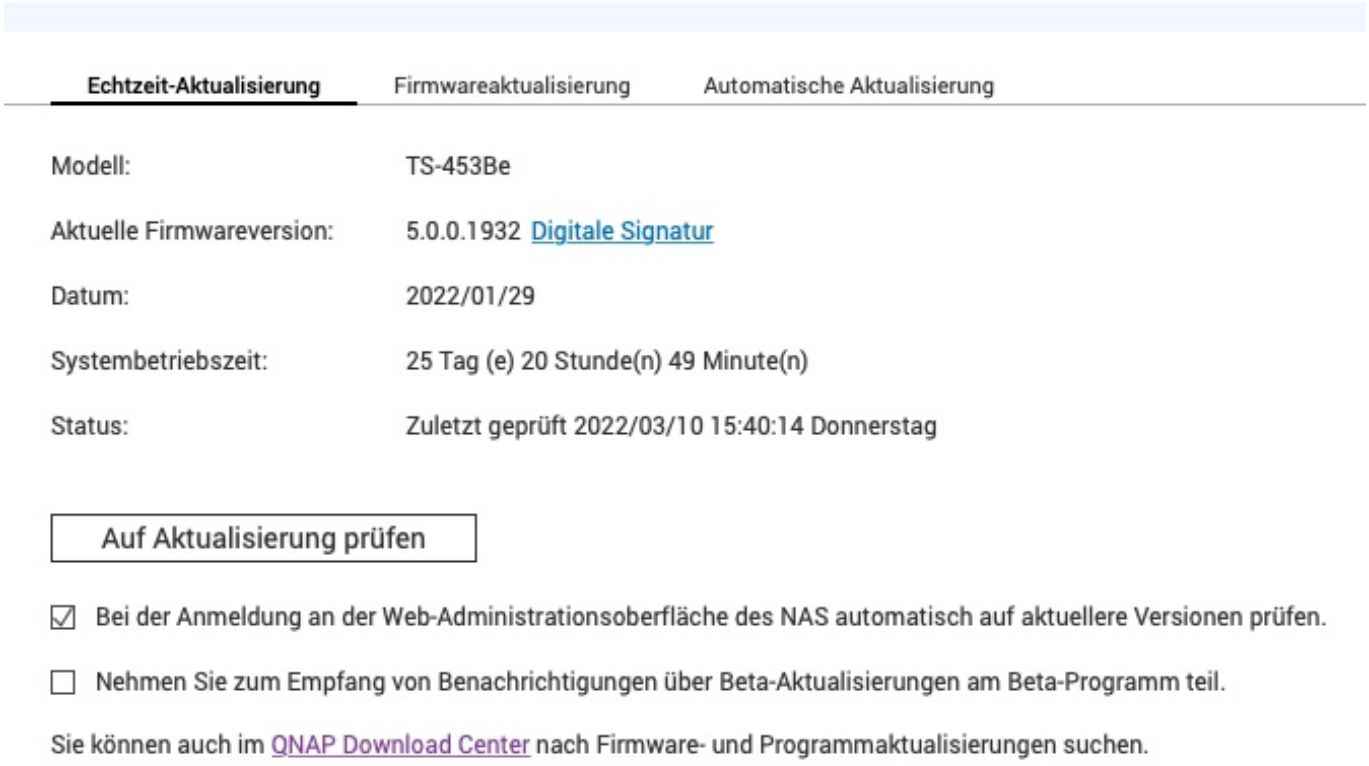
Jedes Gerät, das aus dem Internet erreichbar ist, kann angegriffen werden. Dabei ist Datenverlust nur die eine Seite des potenziellen Schadens: Die meisten Netzwerkfestplatten haben ein Betriebssystem, das zwar spezifisch für das Gerät ist, nichts desto trotz aber auch Sicherheitslücken aufweist und mit Viren

verseucht werden kann. Die QSnatch-Malware ist ein gutes Beispiel dafür. Ist das NAS erst einmal gekapert, dann kann es in Botnetzen eingesetzt werden, die Daten verschlüsselt und dann gegen Lösegeld erst wieder freigegeben werden und vieles mehr.



Aktualisierung ist wichtig

Jeder Hersteller von NAS-Systemen hegt und pflegt seine Geräte und bietet regelmässige Updates an. Sobald diese installiert sind, sind die bekannten Sicherheitslücken deaktiviert und der unberechtigte Zugang von Außen wird für Angreifer schwerer. Es empfiehlt sich, die automatische Aktualisierung zu aktivieren. Das geht in den Einstellungen der Administrationsoberfläche unter **Firmwareupdate**. Dann lädt das NAS nach regelmässiger Prüfung die neue Firmware herunter und installiert sie, ohne, dass Ihr Euch darum kümmern müsst.


Echtzeit-Aktualisierung
Firmwareaktualisierung
Automatische Aktualisierung
Modell:
TS-453Be
Aktuelle Firmwareversion:
5.0.0.1932 Digitale Signatur
Datum:
2022/01/29
Systembetriebszeit:
25 Tag (e) 20 Stunde(n) 49 Minute(n)
Status:
Zuletzt geprüft 2022/03/10 15:40:14 Donnerstag
Auf Aktualisierung prüfen
Bei der Anmeldung an der Web-Administrationsoberfläche des NAS automatisch auf aktuellere Versionen prüfen.
Nehmen Sie zum Empfang von Benachrichtigungen über Beta-Aktualisierungen am Beta-Programm teil.
Sie können auch im QNAP Download Center nach Firmware- und Programmaktualisierungen suchen.

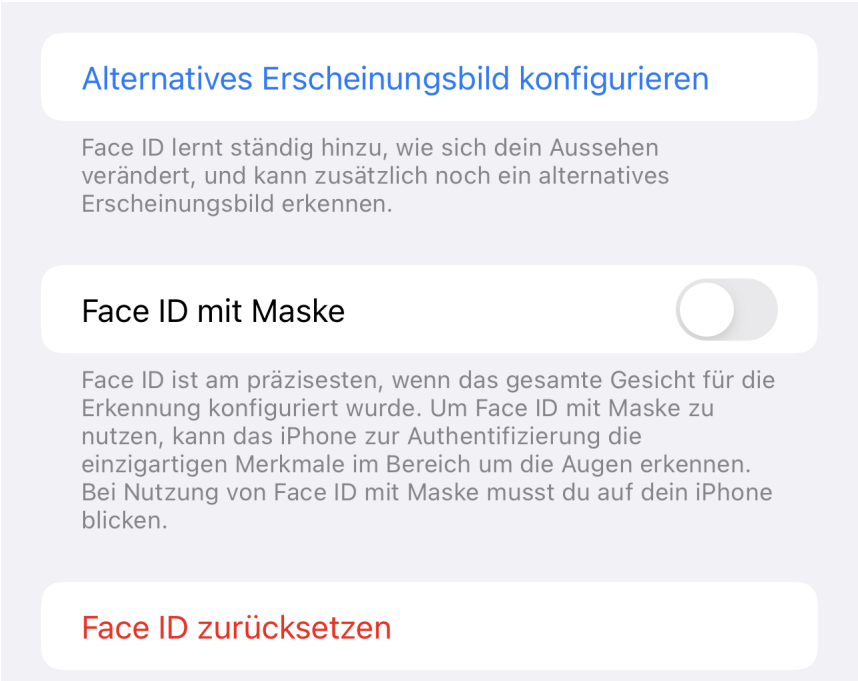
iOS 15.4: Face ID mit der Maske bedienen

Zwei Jahre Corona, zwei Jahre Masken. Ein Graus auch für die Gesichtserkennung eines iPhones, sind doch charakteristische Merkmale des Gesichts verdeckt. Mit dem Update auf iOS 15.4 lässt sich das umgehen!

Face ID hat immer noch einen großen Vorteil zu den Gesichtserkennungen der Konkurrenz: Durch die verwendete Technik lässt sich Face ID nur mit extrem hohen Aufwand täuschen, vor allem reicht ein Foto dafür nicht aus. Um diesen Standard auch unter Aussparung des von der Maske verdeckten Bereiches beizubehalten, waren umfangreiche Anpassungen an der Software nötig.

Funktion erst ab iPhone 12

Nach dem Update auf iOS 15.4 bietet das iPhone (aber der Version 12) die Konfiguration von **Face ID mit einer Maske** automatisch an. Um die Konfiguration später manuell zu starten, dann findet sich die Option unter **Einstellungen** > **Face ID** & **Code** und kann durch Einschalten von **Face ID mit Maske** aktiviert werden.



Konfiguration ohne Maske

Bei der Konfiguration muss der Benutzer keine Maske tragen: iOS nimmt mit und ohne Brille jeweils die Gesichtsdaten neu auf und konzentriert sich dabei vor allem auf die Augenpartie. In einem zweiten Schritt sollte dann jede Brille, die in Verwendung ist, einmal separat konfiguriert werden.

Nach diesem einmaligen Vorgang erkennt das iPhone den Benutzer auch, wenn ein Teil des Gesichtes verdeckt ist. Eine deutliche Erleichterung, wenn das Gerät während des Tragens einer Maske verwendet werden soll!

iOS 15.4: Corona-Impfpass jetzt auch bequem in der Wallet

Das neue iOS15.4 für iPhone und iPad bringt eine Menge interessanter Neuerungen. Eine ist besonders praktisch: Wer mag, kann seine Impfzertifikate jetzt in der Wallet speichern - und hat sie so schnell zur Hand.

Klar, das Impfzertifikat ist auch in der Covpass Pass und/oder in der Corona Warn App schnell hervorgeholt. Aber die Wallet in iOS lässt sich noch eine Spur schneller aktivieren. Eine Funktion, die ich mir sogar schon früher gewünscht hätte - als wir die Zertifikate noch viel häufiger vorzeigen mussten als heute.

Neue Funktion ab iOS 15.4

Um die neue Funktion nutzen zu können, müsst Ihr das neue IOS15.4 (oder neuer) laden und installieren. Aber Version 15.4 ist es möglich, die Impfzertifikate (EU Covid Pass).

Der Corona-Impfpass lässt sich über die Apple-Health-App einscannen und taucht dann auch automatisch in der Wallet auf. iPhone oder iPad präsentieren in der Health-App das Zertifikat unter „Immunisierungen“. In der Wallet taucht das Zertifikat in knallrot als "Impfkarte" auf. Es ist wirklich nicht zu übersehen.

Und so geht Ihr vor...

Es ist ganz einfach, den QR-Code des Impfzertifikats zu scannen, den ihr im Zusammenhang mit eurer Impfung gegen COVID-19 erhalten habt. Der QR Code wird so zu den überprüfbaren Gesundheitsdaten zur Health-App/Apple Wallet hinzugefügt.

1. Als Erstes öffnet Ihr bitte im Home-Bildschirm, Kontrollzentrum oder Sperrbildschirm auf dem iPhone oder iPod touch wie gewohnt die Kamera-App (Ihr müsste also nicht etwa in die **Health**-App gehen).
2. Wählt die rückseitige Kamera aus.
3. Haltet das Gerät so, dass der QR-Code im Sucher in der Kamera-App angezeigt wird. Das Gerät erkennt automatisch den QR-Code und zeigt in Gelb direkt nebem dem QR-Code den Hinweis "Covid-19-Zertifikat" an. Eine Mitteilung der Health-App.
4. Tippt auf die Mitteilung der Health-App (Scan-Icon rechts unten).
5. Danach tippt Ihr auf "Zu Wallet und Health hinzufügen", um den verifizierbaren Impfeintrag zur Health-App und zur Wallet-App hinzuzufügen.
6. Abschließend tippt Ihr noch auf "Fertig" - das Zeritifkat ist in der Wallet gespeichert.

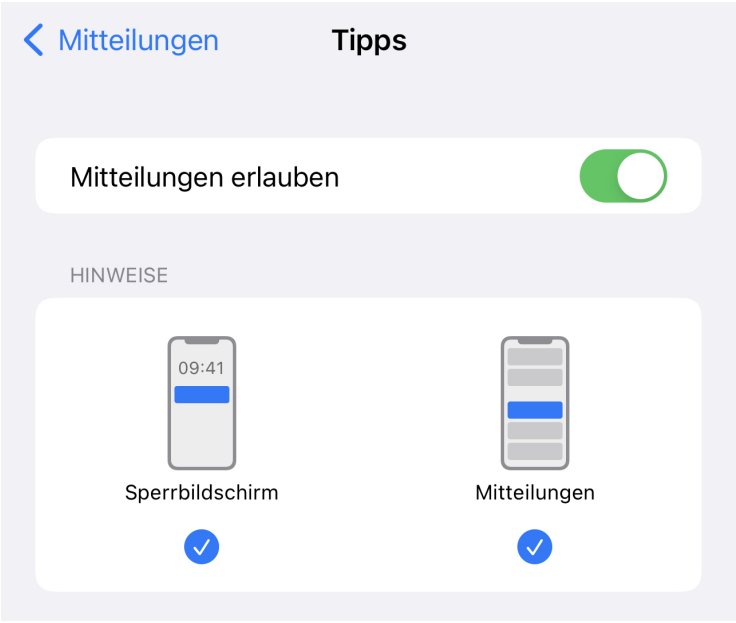
Nutzen der Tipps-Funktion unter iOS

Jedes Update von iOS bringt mehr Funktionen. Wir tun unser Möglichstes, um Euch up to date zu halten. IOS selbst bietet hier aber auch eine Info-Funktion!

Viele der vorinstallierten Apps von iOS sind schnell in einen Ordner sortiert und nie wieder betrachtet. Das ist verständlich, jeder Anwender hat sich im Laufe seiner Zeit mit einem Smartphone seine Lieblings-Apps für alle Anwendungsbereiche gesucht und verwendet eher die als die Apple-Standard-

Apps. Dabei gehen leider Apps wie die Tipps-App unter, die durchaus ihr Alleinstellungsmerkmal haben und hilfreich sind.

Startet die Tipps-App aus dem Home Screen, dann zeigt diese die neuesten Tipps rund um iOS an. Die sind nach Themenbereichen geordnet, ein Tippen auf eine Kategorie öffnet die darin befindlichen Tipps. Noch besser ist es, Euch immer mal wieder mit neuen Tipps überraschen zu lassen. Dazu muss die Tipps-App die Berechtigung zum Versenden von Nachrichten haben:



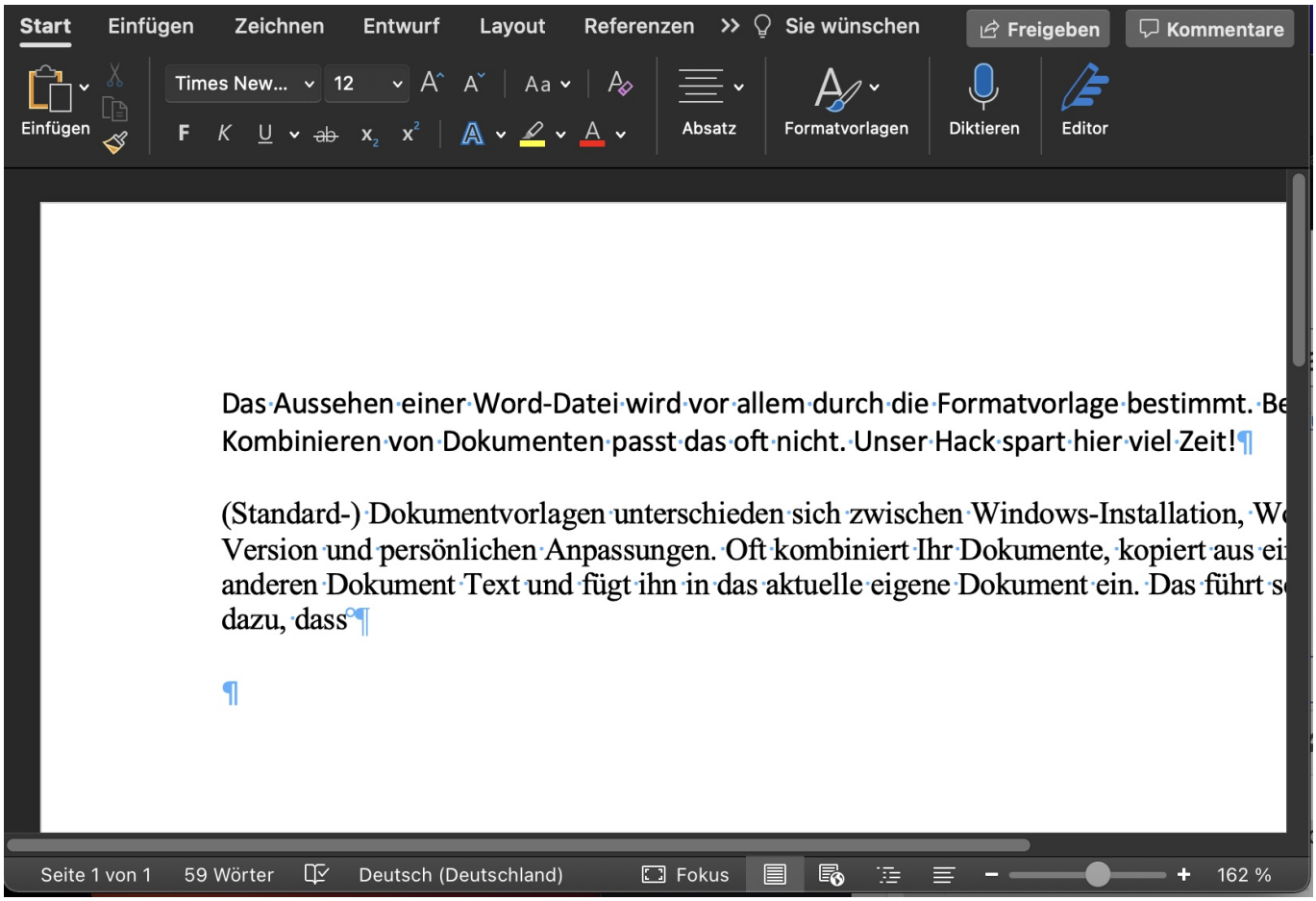
In den iOS-Einstellungen muss unter **Mitteilungen** unten in der Liste die Tipps-App angetippt werden. Im folgenden Bildschirm lassen sich dann die Mitteilungen aktivieren. Dazu müsst Ihr den Schalter neben **Mitteilungen erlauben** aktivieren, dann könnt Ihr unter **Hinweise** festlegen, welche Art von Meldungen Ihr sehen wollt. Idealerweise aktiviert nur Sperrbildschirm, denn da sind die Meldungen weniger störend als während der Arbeit und lassen sich einfach ignorieren, wenn das nötig sein sollte.

Übertragen von Formatvorlagen in Word

Das Aussehen einer Word-Datei wird vor allem durch die Formatvorlage bestimmt. Beim Kombinieren von Dokumenten passt das oft nicht. Unser Hack spart hier viel Zeit!

(Standard-) Dokumentvorlagen unterschieden sich zwischen Windows-Installation, Word-Version und persönlichen Anpassungen. Oft kombiniert Ihr Dokumente, kopiert aus einem anderen Dokument Text und fügt ihn in das aktuelle eigene Dokument ein. Das führt schnell dazu, dass der Text gestückelt aussieht. Das manuell nachzupflegen, ist ein riesiger und unnötiger Aufwand.

Word speichert die aktuell verwendete Formatvorlage in der Datei. Führend ist also immer die Datei, die gerade auf dem Rechner geöffnet ist und in die Text aus einer anderen Datei hineinkopiert wird. Word nimmt das Format der kopierten Bereiche mit hinüber in das neue Dokument.


Start
Einfügen
Zeichnen
Entwurf
Layout
Referenzen
Sie wünschen
Freigeben
Kommentare
Times New...
12
Einfügen
Absatz
Formatvorlagen
Diktieren
Editor
Das Aussehen einer Word-Datei wird vor allem durch die Formatvorlage bestimmt. Be
Kombinieren von Dokumenten passt das oft nicht. Unser Hack spart hier viel Zeit!
(Standard-) Dokumentvorlagen unterschieden sich zwischen Windows-Installation, W
Version und persönlichen Anpassungen. Oft kombiniert Ihr Dokumente, kopiert aus ei
anderen Dokument Text und fügt ihn in das aktuelle eigene Dokument ein. Das führt s
dazu, dass
Seite 1 von 1
59 Wörter
Deutsch (Deutschland)
Fokus
162 %

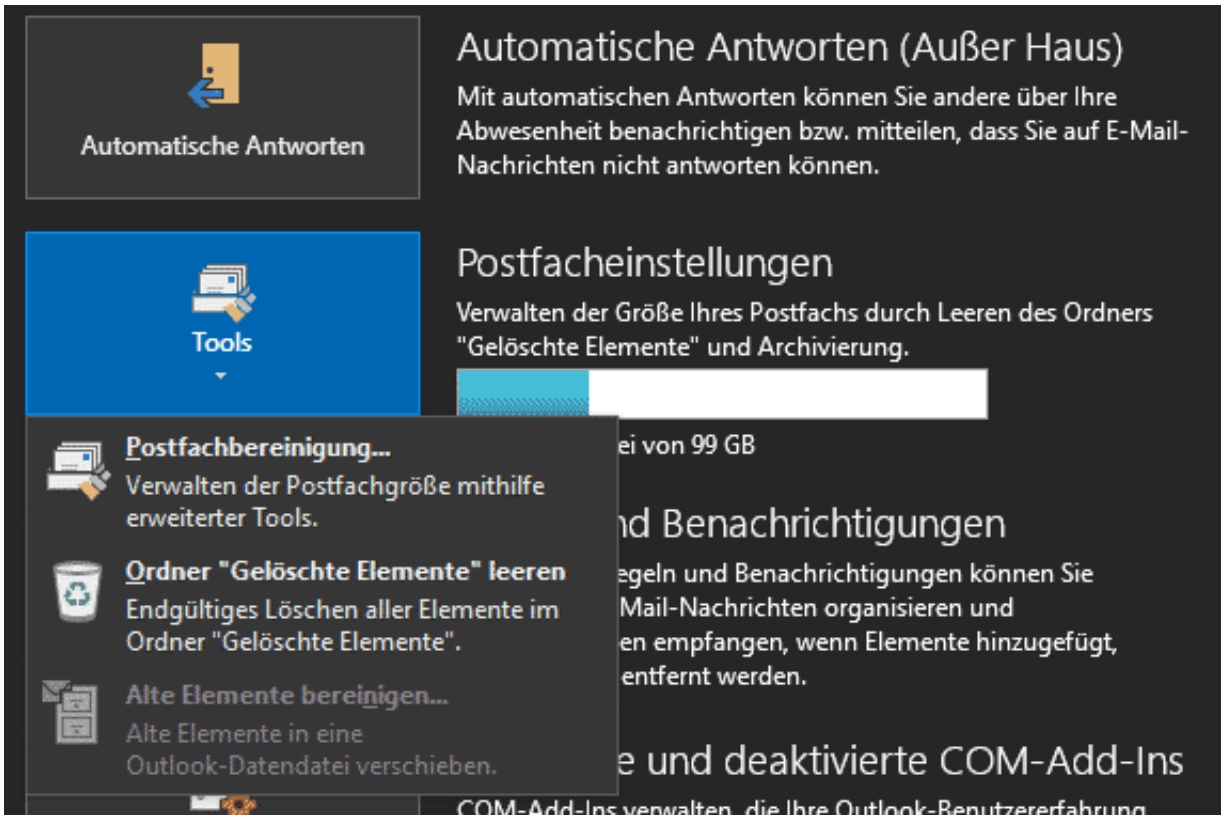
Um nun die Textbereiche automatisch in das richtige Format zu bringen, hilft eine Tastenkombination, die Word im Standard mit an Bord hat: Markiert den Bereich, der umformatiert werden soll, mit der Tastatur oder der Maus. Drückt dann auf der Tastatur gleichzeitig die Tasten **Alt** + **Shift** + **N**. Word wendet die aktuelle Formatvorlage des Dokuments auf den markierten Bereich an.

Statt den Text zu markieren, könnt Ihr auch absatzweise vorgehen: Stellt den Cursor in einen Absatz, dann drückt wieder die Tasten **Alt** + **Shift** + **N**. Word wendet die Formatvorlage nun auf den aktuellen Absatz an.

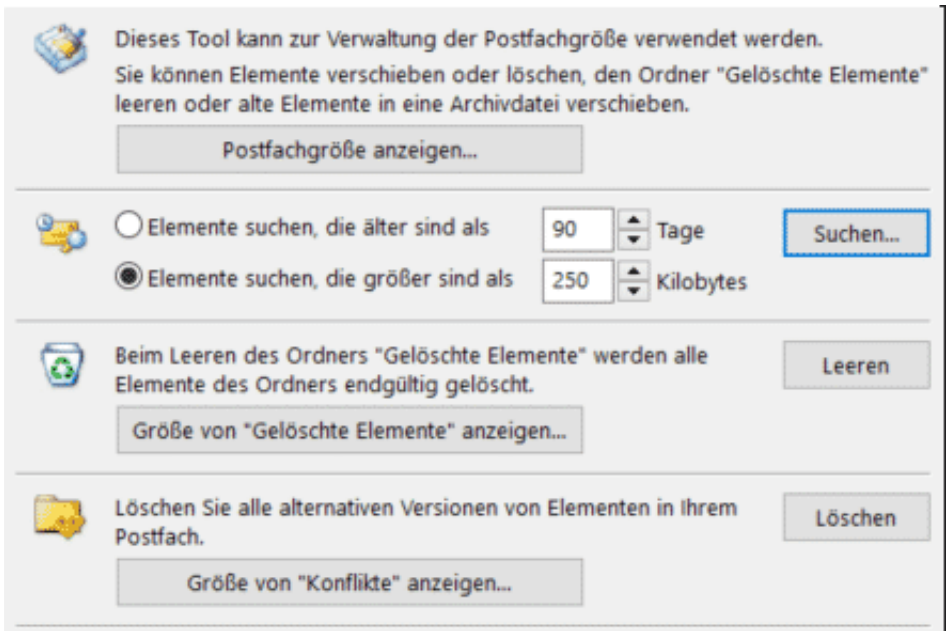
Platz frei im Outlook-Postfach!

Immer mehr Mails, immer mehr belegter Speicher: Outlook nimmt schnell viel Speicher weg, hat aber auch einige Funktionen integriert, die dem entgegenwirken können.

Die Verwaltungsfunktionen für Outlook-Postfächer finden sich unter **Datei** > **Tools**. Ist nicht genug freier Speicherplatz in den Postfächern vorhanden, dann klickt erst einmal auf **Ordner "Gelöschte Elemente" leeren**. Damit löscht Outlook endgültig die E-Mails, die sowieso schon gelöscht waren, aber für den Notfall noch aufgehoben sind. Damit ist natürlich die Möglichkeit, im Notfall eine gelöschte E-Mail wiederherzustellen, nicht mehr vorhanden.



Feiner lässt sich die Bereinigung durch einen Klick auf **Postfachbereinigung...** einrichten. Eine Verringerung der **Postfachgröße** schafft mehr Platz, auch eine Verschiebung von E-Mails in den Archiv-Ordner lässt sich konfigurieren. Die Archivdateien halten die älteren E-Mails noch vor, nehmen aber deutlich weniger Platz weg.

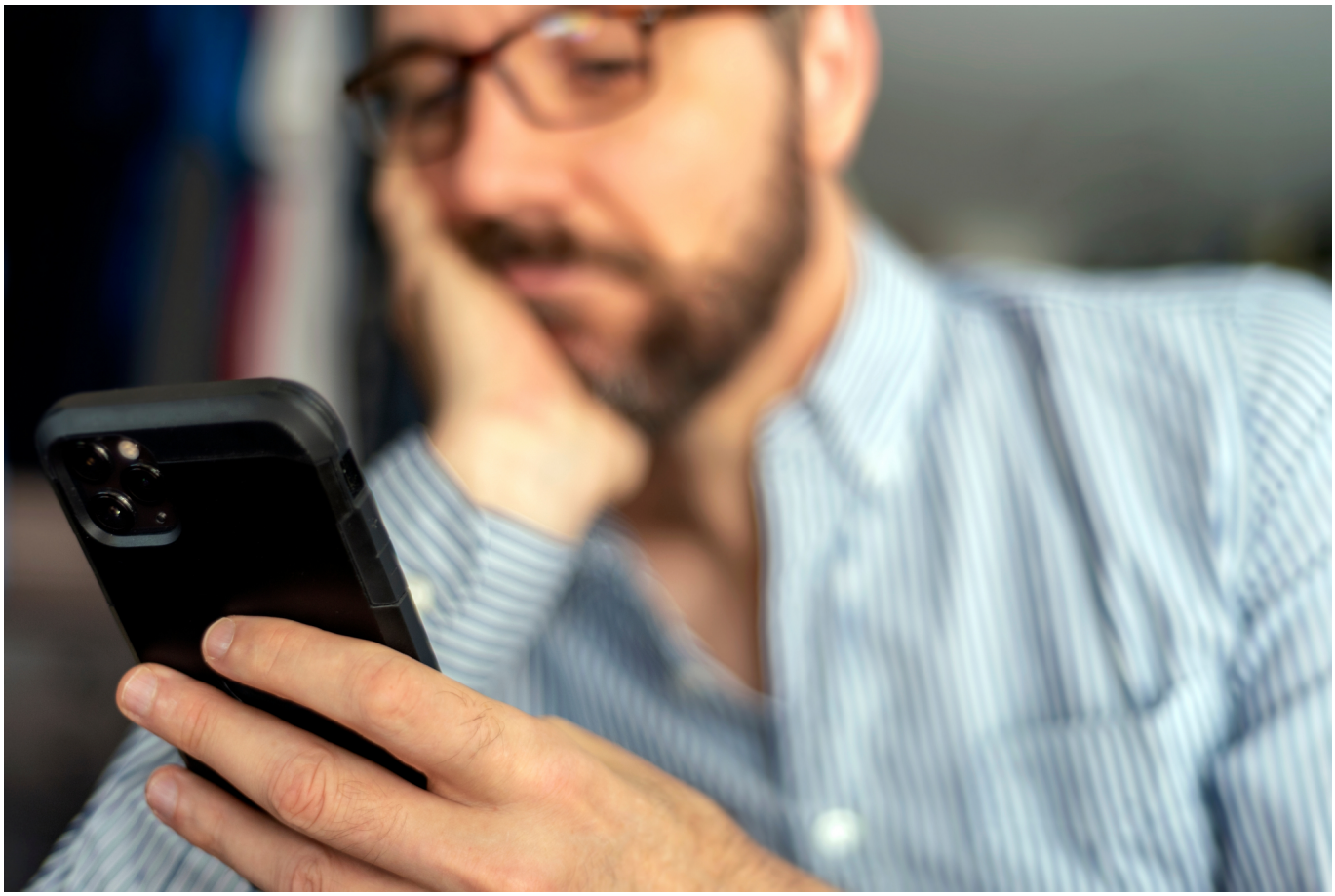


Oft sind für die Überfüllung Ihres Postfaches einige wenige E-Mails verantwortlich,

die große Anhänge haben. Diese lassen sich anzeigen, wenn Ihr unter **Elemente suchen, die größer sind als** die minimale Größe einstellt und auf **Suchen** klickt. Eine weitere Alternative ist die Suche nach **älteren Elementen**, hier kann das Alter nach Tagen vorgegeben werden.

Die gefundenen Elemente können dann markieren und gelöscht werden und machen eine Menge an Platz in Outlook frei.

Doomscrolling: Krieg überall - auch auch im Hochformat



Zwei Jahre Corona, jetzt Krieg in der Ukraine: Die Medien sind voll mit schlechten Nachrichten, Hiobsbotschaften und schlimmen Bildern. Das bringt einen Begriff an die Oberfläche, den viele noch nicht kannten: „Doomscrolling“. Was verbirgt sich dahinter?

Der Krieg in der Ukraine ist derzeit in den Medien allgegenwärtig. Denn die Bedrohung durch Russland und das, was da in der Ukraine vor sich geht, will eingeordnet und verstanden werden. Praktisch kein Tag vergeht ohne „Brennpunkt“ oder Extras. Aber auch die Sozialen Medien sind voll mit dem Thema.

So voll, dass manche Menschen sich schon überfordert fühlen. Denn es macht natürlich was mit einem, wenn man praktisch rund um die Uhr mit den unterschiedlichsten Aspekten des Kriegs konfrontiert wird. Auch auf dem Handy.

Der Begriff "Doomscrolling"

Der Begriff „Doomscrolling“ bezeichnet den "exzessiven Konsum negativer Nachrichten im und aus dem Internet".

„Doom“ bedeutet im Englischen ja: Ein drohendes schwerwiegendes Problem, das unvermeidbar ist. Ein Gefühl von Gefahr, schwerwiegender Gefahr, Düsternis oder Verzweiflung. Der Tod, das Schicksal oder das Ende. Es gibt populäre Computerspiele, die so heißen.

Und genau das ist damit auch gemeint: Ich schaue in mein Handy und kann quasi unentwegt scrollen und scrollen – und es kommen immer mehr schlimme Nachrichten, Bilder und Erkenntnisse. Das Display ist voll damit. Und wie das mit dem Smartphone so ist: Die Algorithmen der Social Media wählen aus, was am meisten Aufmerksamkeit bekommt – und alles andere wird ausgeblendet.

Und so sehen wir reguläre Nachrichten, aber auch auf Facebook, Youtube, Twitter und sogar TikTik sehr viel über den Ukraine-Kriegt – und auch jede Menge schlimmer Bilder. Und als wäre das noch nicht schlimm und tragisch genug, sind auch noch jede Menge Fake-News darunter, die auch nicht gerade „Aufheller“ sind. Ein solches **Doomscrolling**, also der gesteigerte Konsum von vornehmlich negativen Schlagzeilen kann gesundheitsschädliche psychologische Folgen haben.

Gesundheitliche Folgen

Und genau das kann gesundheitliche Folgen haben. Und selbst die Jüngeren bleiben nicht verschont, da auch auf TikTok der Krieg eine Rolle spielt.

Auch auf TikTok wählen Algorithmen aus, was die User zu sehen bekommen – viel stärker als auf Instagram. Und so kommt es, dass auch TikTok-Nutzer Bilder aus dem Krieg zu sehen bekommen – zwischen all den üblichen Tanz- und Spaß-Videos, die da so üblich sind. Ein Panzer, der durch eine Wohnsiedlung rollt. Ein Soldat, der eine ukrainische Flagge hisst.

Menschen, die in einen oder aus einem Bunker laufen. Politiker in Soldaten-Kluft. Selbst ein Kind oder Jugendlicher nicht genau weiß, worum es hier geht, sind die Bilder doch eindeutig. Krieg. Konflikt. Leid. Kinder, denen es nicht gut geht.

TikTok bringt die Bilder in die Köpfe der Kinder und Jugendlichen. Und sie müssen diese Bilder nicht abonnieren oder gezielt suchen, sie poppen so auf den Displays auf. Aus diesem Grund ist es aktuell wichtiger denn je, dass Eltern genau kontrollieren, was ihre Kinder am Handy machen – und mit ihnen sprechen.

Jetzt werden viele sagen: Moment! Das ist erstaunlich, dass so viele Bilder aus der Ukraine zu sehen sind. Ich kann mich erinnern, dass die teilweise auch sehr brutalen Demonstrationen in Hongkong auf TikTok kaum zu sehen waren...

Ja, das fällt mir auch auf. Es verstärkt den Verdacht, dass die chinesische Regierung hier Einfluss genommen hat: Die Proteste in Hongkong sollte keiner sehen. Deswegen haben die Algorithmen sie ignoriert, muss man annehmen. Der Krieg in der Ukraine jedenfalls ist auf Instagram mehr als nur präsent.

Ukraine-Konflikt in Podcasts

Bilder ist eine Sache, Worte eine andere. Offensichtlich gibt es auch einige Podcasts, die sich mit dem Ukraine-Konflikt beschäftigen.

„Generäle auf allen Kanälen“, hat ein Kollege geschrieben. In Talkshows sowieso. Aber auch viele Podcasts beschäftigen sich mit dem Thema. Eine Art „Krisen-Podcast“, könnte man sagen. Mit Christian Drostens „Corona Virus Update“ vom NDR wurde ein Podcast geschaffen, der äußerst erfolgreich war und ist – in einer Krise entstanden.

Und fast hat man den Eindruck, da wollten viele nacheifern. Es sind einige neue Podcasts rund um den Krieg in der Ukraine entstanden. Der NDR ist mit zwei Podcasts dabei: „Krieg in Europa: Das Update zur Lage“ liefert zwei Mal(!) täglich Updates zum Konflikt. Außerdem gibt es den Podcast „Streitkräfte und Strategien“, den es schon länger gibt, ebenfalls täglich derzeit.

Der MDR hat einen Podcast „Was tun, Herr General?“ und den ARD-Podcast „Alles ist anders: Krieg in Europa“, der sich vor allem an ein jüngeres Publikum richtet. Aber auch Spiegel und viele andere haben Podcasts am Start. Einige gab es vorher schon, andere wurden neu erfunden. Auch in der Podcast-Welt ist Teil des Doomscrollings. Immerhin ist es bei Podcasts so, dass man sich gezielt aussucht, was man sich anhört.

Fake-News eindämmen

On top haben wir noch das Problem, dass auch Fake-News in den Sozialen Medien kursieren. Fotos, die alt sind, aber dem aktuellen Konflikt zugeordnet werden oder komplett gefälschte Fotos und Videos. Was tun?

Das ist ein wachsendes Problem. Ich kann nur empfehlen: Nicht alles glauben. Und schon gar nicht Teil des Problems sein und alles gleich in der eigenen Community teilen. Im Zweifel ist es hilfreich, bei mimikama.at mal nachzuschauen. Denn hier sind Fakten-Checker am Werk, die im Augenblick eine ganze Menge viral gehender Nachrichten und Fotos analysieren und den Wahrheitsgehalt einordnen. Das ist eine sehr wichtige Arbeit – auch und vor allem, damit man nicht auch noch unter den Fake-News leidet.

BSI und Kaspersky: Offener Brief von Eugene Kaspersky

Das BSI warnt aktuell vor der Verwendung von Schutz-Software von Kaspersky. Eine Warnung, die ich aufgrund der politischen Lage nachvollziehen kann und sogar richtig finde. Nun wendet sich Eugene Kaspersky mit einem offenen Brief an die Öffentlichkeit.

Niemand verbietet den Einsatz von Kasperskys Software in Deutschland. Das BSI hat eine Risikobewertung vorgenommen und warnt davor, dass das russische Regime Unternehmen mit Firmensitz in Russland - und das ist bei Kaspersky der Fall - zweifellos zwingen kann, Dinge zu tun, die uns hier schaden.

Um sich selbst ein Bild zu machen, ob man den Einsatz von Kaspersky als Risiko einstuft oder nicht, veröffentliche ich hier gerne den offenen Brief von Eugene Kaspersky. Ich möchte bewusst an dieser Stelle keine weitere Kommentierung vorsehen, da es sich eben um einen offenen Brief handelt. Ich werde das an anderer Stelle bewerten.

"Kollateralschaden – für die Cybersicherheit"

In den letzten drei Wochen hat der Krieg in der Ukraine die Welt, wie wir sie kannten, dramatisch verändert. Familien, Beziehungen und Partnerschaften wurden in der Ukraine, in Russland, in Europa und in der ganzen Welt auf dramatische Weise erschüttert. Die Lawine dieser tragischen Ereignisse hat uns alle erfasst.

Auch mein Unternehmen, das weltweit größte private Cybersicherheitsunternehmen, das mit Stolz meinen Namen trägt, ist davon betroffen. In dieser Woche hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Warnung vor Kaspersky-Produkten herausgegeben, in der auf potenzielle Risiken der Nutzung von Kaspersky-Produkten und -Lösungen hingewiesen wird.

Ohne auf Details einzugehen kann ich sagen, dass diese Behauptungen reine Spekulationen sind, die durch keine objektiven Beweise oder technischen Details gestützt werden. Der Grund dafür ist einfach. In der fünfundzwanzigjährigen Geschichte Kasperskys gab es nie einen Beweis für einen Missbrauch unserer Software zu schädlichen Zwecken. Und das trotz unzähliger Versuche, einen Beweis dafür zu finden.

Ohne Beweise kann ich nur zu dem Schluss kommen, dass die Entscheidung des BSI allein aus politischen Gründen getroffen wurde. Ich empfinde es als traurig, ja ironisch, dass die Organisation, die sich für Objektivität, Transparenz und technische Kompetenz einsetzt – im Übrigen dieselben Werte, die Kaspersky seit Jahren ebenso wie das BSI und andere europäischen Regulierungsbehörden und Branchenverbände unterstützt –, sich buchstäblich über Nacht dazu entschlossen hat oder gezwungen wurde, diese Prinzipien aufzugeben.

Kaspersky, langjähriger vertrauensvoller Partner und Unterstützer des BSI und der deutschen Cybersicherheitsindustrie, hatte lediglich wenige Stunden Zeit, um sich zu diesen falschen und unbegründeten Anschuldigungen zu äußern. Dies ist keine Einladung zum Dialog – es ist eine Beleidigung.

Trotz vieler Angebote seitens Kaspersky, unseren Quellcode, unsere Updates, unsere Architektur und unsere Prozesse in den Transparenzzentren Kasperskys in Europa eingehend zu prüfen, hat das BSI dies bisher nie getan. Die Warnung lässt praktischerweise die Tatsache außer Acht, dass Kaspersky seit Jahren Pionierarbeit für mehr Transparenz leistet, indem es im Rahmen seiner Globalen

Transparenzinitiative Bedrohungsdaten seiner europäischen Kunden in die Schweiz verlagert hat.

Bei allem Respekt, ich betrachte die Entscheidung des BSI als einen ungerechtfertigten Angriff auf mein Unternehmen und insbesondere auf die Kaspersky-Mitarbeiter in Deutschland und Europa. Vor allem aber ist dies auch ein Angriff auf die große Zahl der Verbraucher in Deutschland, die Kaspersky – in den letzten zwei Wochen als bestes Sicherheitsangebot ausgezeichnet (AV-TEST) – ihr Vertrauen schenken.

Es ist auch ein Angriff auf die Arbeitsplätze tausender deutscher IT-Sicherheitsexperten, auf Strafverfolgungsbeamte, die wir für die Bekämpfung fortschrittlichster Cyberkriminalität trainiert haben, auf deutsche Informatikstudenten, denen wir bei ihrer Ausbildung geholfen haben, auf unsere Partner in Forschungsprojekten in den kritischsten Bereichen der Cybersicherheit und auf zehntausende deutsche und europäische Unternehmen aller Größenordnungen, die wir vor dem gesamten Spektrum von Cyberangriffen geschützt haben.

Der Schaden für unsere Reputation und unser Geschäft, der durch die Warnung des BSI entstanden ist, ist bereits erheblich. Mich beschäftigt eine Frage: Was ist der Zweck? Kaspersky nicht in Deutschland zu haben, wird Deutschland oder Europa nicht sicherer machen. Ganz im Gegenteil. Die BSI-Entscheidung bedeutet, dass deutschen Nutzern empfohlen wird, das einzige Antivirenprogramm zu deinstallieren, das laut dem unabhängigen deutschen IT-Sicherheitsinstitut AV-Test, den besten Schutz vor Ransomware garantiert.

Sie bedeutet, dass die führenden deutschen Industrieunternehmen keine Informationen mehr über kritische Schwachstellen in ihrer Software und Hardware von Kaspersky ICS-CERT erhalten werden – einer Organisation, die von eben diesen Herstellern für ihre verantwortungsvolle Aufklärungsarbeit gelobt wird. Sie bedeutet, dass deutsche Automobilkonzerne nicht über die Fehler informiert werden, die es einem Angreifer ermöglichen könnten, das gesamte Bordcomputersystem zu übernehmen und dessen Logik zu verändern. Sie bedeutet einen riesigen blinden Fleck auf der Angriffsfläche für europäische Incident Response-Experten und SOC-Betreiber, die nicht mehr in der Lage sein werden, Bedrohungsdaten aus der ganzen Welt – und insbesondere aus Russland – zu empfangen.

Meine Botschaft an das BSI, das leider den Kontakt zu meinem Team in Deutschland seit kurzer Zeit zu meiden scheint, ist einfach: Wir halten diese Entscheidung für ungerecht und grundfalsch. Nichtsdestotrotz sind wir nach wie vor offen dafür, alle Bedenken, die das BSI hat, auf objektive, technische und ehrliche Weise auszuräumen.

Wir sind den europäischen Regulierungsbehörden und Branchenexperten dankbar, die einen ausgewogeneren Ansatz gewählt haben, indem sie eine zusätzliche technische Analyse und Prüfung von Sicherheitslösungen und der IT-Lieferkette gefordert haben, und ich verpflichte mich, dass Kaspersky während dieses Prozesses alle erforderlichen Informationen zur Verfügung stellen und gerne kooperieren wird. Unseren deutschen und europäischen Kunden möchte ich sagen: Wir sind sehr dankbar, dass Sie sich für Kaspersky entschieden haben, und dass wir weiterhin das tun werden, was wir am besten können – Sie vor allen Cyberbedrohungen zu schützen, ganz gleich, woher sie kommen, und dabei unsere Technologie und unsere Tätigkeit völlig transparent zu machen.

Der Krieg in der Ukraine kann nur auf diplomatischem Wege beendet werden, und wir alle hoffen auf die Einstellung der Kampfhandlungen und eine Fortsetzung des Dialogs. Dieser Krieg ist eine Tragödie, die bereits Leid über unschuldige Menschen gebracht hat und sich auf unsere hypervernetzte Welt auswirkt. Die globale Cybersicherheitsindustrie, die auf der Grundlage von Vertrauen und Zusammenarbeit zum Schutz der digitalen Verbindungen zwischen uns allen aufgebaut wurde, könnte einen kollateralen Schaden erleiden – und damit alle weniger sicher machen.

Eugene Kaspersky

Double Standards: Zweierlei Maß bei Telegram und Co?

Mal werden Sperrungen eingefordert, mal sind sie "Zensur". Wir erleben viele solcher Double Standards. Telegram zum Beispiel stand in Deutschland kurz vor einem Verbot. Doch jetzt hilft Telegram im Krieg gegen Russland - und die Kritik verstummt.

Der Krieg in der Ukraine, er wird auch medial ausgetragen – wie wohl jeder Krieg der Neuzeit. Aber beim Krieg in der Ukraine ist das besonders deutlich zu spüren. Auch die Sozialen Netzwerke spielen eine große Rolle. Die EU sanktioniert russische Sender wie Russia Today oder Sputnik – und auch Facebook sperrt die Sender. Daraufhin sperrt Russland Facebook im Land. Oder der Messenger Telegram: Er war der deutschen Politik lange ein Dorn im Auge.

Im Ukraine-Konflikt spielt er aber eine große Rolle.

Die Rolle von Telegram

Der Messenger Telegram wurde bei uns in Deutschland eher kritisch gesehen. Doch jetzt finden es alle toll, dass die Ukraine darüber ihre Kräfte mobilisiert. Was

ist da los?

Aufgrund der Radikalisierung von Corona-Leugnern und Impfgegnern auf Telegram und wegen der Verbreitung von Falschinformationen stand Telegram hier in Deutschland gewissermaßen kurz vor dem Aus**:** Selbst Verbote wurden in der politischen Führungsriege erwogen und angedroht.

Davon ist aktuell nichts mehr zu hören. Denn im Ukraine-Krieg spielt Telegram eine nicht unwesentliche Rolle. Der ukrainische Vizepräsident und Minister für Digitalisierung Fedorov hat auf Telegram einen Kanal eingerichtet, über den Cyberangriffe auf russische Ziele koordiniert werden Federov hat eine IT-Armee ausgerufen – und die wird eben über Telegram organisiert.

Rund 300.000 Mitglieder hat die Gruppe. Das eine zu begrüßen und das andere einschränken zu wollen, ist etwas, was man wohl als „Double Standard“ bezeichnen muss. Es gelten nicht immer dieselben.

Die Rolle von Facebook

„Double Standards“ gibt es recht häufig. Auch Sperrungen bei Facebook werden von der Öffentlichkeit sehr unterschiedlich bewertet. Wenn hierzulande russische Propagandasender wie RT oder Sputnil gesperrt werden, gibt's Applaus - sperrt Russland Inhalte, die dem Regime nicht passen, ist es inakzeptable Zensur.

Nehmen wir das Beispiel Facebook. Auch hier gibt es ein Hin und Her. Facebook hatte die Angebote von Russia Today und Sputnik entfernt, weil die russischen Propagandasender von der EU sanktioniert wurden. Daraufhin hat der Kreml Facebook in Russland geblockt.

Jetzt berichten Nachrichtenagenturen, die Facebook-Führung habe ihre Mitarbeiter ausdrücklich angewiesen, bei bestimmten Äußerungen quasi ein Auge zuzudrücken. In vielen osteuropäischen Ländern ist es demnach erlaubt, auf Facebook „Tod den Invasoren“ zu sagen und zu posten.

Dasselbe gilt für andere gewalttätige Äußerungen, die normalerweise eindeutig gegen die Nutzungsregeln widersprechen. Auch Putin darf man den Tod an den Hals wünschen, ebenso dem belarussischen Präsidenten Lukaschenko. Auch wenn man das selbst vielleicht denkt, ist es doch etwas anderes, wenn man es

öffentlich äußert. Bei Todesdrohungen gegen deutsche Politiker sehen wir das völlig anders. Ein Double Standard.

Wo fängt Zensur an?

Es ist ja immer die Frage: Wo fängt Zensur an, wo hört das Recht auf freie Meinungsäußerung auf. Besonders in den Soziale Netzwerken ein Problem. Und gerade kursieren dort ja sehr viel Falschinformationen, Fake News zum Krieg. Stellst du da auch fest, dass die Plattformen ungleich damit umgehen, je nachdem, von welcher Seite das kommt.

Es gibt ein Video auf Youtube, ein Deep Fake Video – es steht auch dabei. Es kann also niemand überrascht sein. Man sieht eine Filmszene aus dem Quentin Tarentino Film „Inglorious Bastards“. Hier schlägt ein jüdischer Soldat einem deutschen Soldaten den Schädel ein. Im Deep Fake ist der knieende Soldat Vladimir Putin.

Erschlagen wird er von Ukraines Präsident Selenskyi. Was stimmig ist – auch Selenskyi ist ja Jude. Die Detailtreue dieses Deep Fakes ist enorm. Putin trägt ein KGB-Logo auf seiner Weste. Und rechts am Rand sitzt Joe Biden und sieht zu. Die Gesichter sind technisch ausgesprochen gut. Aber die gesamte Szene ist

äußerst brutal – und kann mit Fug und Recht wohl als Aufruf zur Gewalt und zum Mord verstanden werden.

Aber Youtube löscht das Video nicht. Hätten die Russen ein solches DeepFake Video ins Netz gestellt, wären die Rufe unüberhörbar laut: „Löscht das Video!“. Double Standards. Ich habe übrigens in meiner Netz-Community das mal thematisiert. Fast alle waren der Ansicht: Das müsste eigentlich gelöscht werden.

Wie umgehen mit "Double Standards"?

Ich finde, diese Beispiele machen sehr deutlich, dass wir sehr häufig solche Double Standards haben. Wenn Werkzeuge einen Dienst erfüllen, den wir gut finden, ist alles in Ordnung. Passt es uns politisch nicht, gehört es verboten. Es bleibt aber dasselbe Werkzeug. Bei Telegram erleben wir das ja gerade. Standards müssten weitgehend immer gelten.

Ein Video, das zur Gewalt aufruft, ruft zur Gewalt auf – und hat auf einem öffentlichen Portal meiner Ansicht nach nichts zu suchen. Ganz zu schweigen davon, dass Tarantinos Film erst ab 16 Jahren freigegeben ist, die Szene aber jeder sehen kann. Es ist auch schwierig, Russland mangelnde Pressefreit zu attestieren – was zweifellos zutreffend ist –, aber gleichzeitig Sender wie Russia Today verbieten. Das hat zumindest ein Geschmäckle.

BSI warnt vor Schutz-Software von Kaspersky: Das ist jetzt zu tun

Das BSI warnt offiziell vor dem Einsatz der Schutz-Software des russischen Herstellers Kaspersky. Ein ungewöhnlicher Vorgang. Viele fragen sich: Was soll ich jetzt tun?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht nach §7 BSI-Gesetz eine offizielle Warnung "vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky" aus. Das BSI begründet diesen Schritt mit dem in diesem Zusammenhang notwendigen Vertrauen in "die Zuverlässigkeit" sowie die "authentische Handlungsfähigkeit" eines Herstellers von Antiviren-Software.

Missbrauch nicht völlig auszuschließen

Genau das sei angesichts des kriegerischen Konflikts nicht mehr gegeben, erklärt die Behörde. Gemeint ist damit, dass aus technischer Sicher nicht auszuschließen

ist, dass der russische Präsident Putin die Software für seine Zwecke nutzt. So wäre es durchaus denkbar und technisch möglich, über die Software PCs oder Mobilgeräte fernzusteuern, Gespräche zu belauschen oder ganze Systeme lahmzulegen.

Das BSI schreibt wörtlich:

> *"Ein russischer IT-Hersteller kann selbst offensive Operationen durchführen, gegen seinen Willen gezwungen werden, Zielsysteme anzugreifen, oder selbst als Opfer einer Cyber-Operation ohne seine Kenntnis ausspioniert oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht werden."*
> *BSI, 16.03.2022*

Wichtig zu wissen: Schutz-Software wie die von Kaspersky greift sehr tief ins Betriebssystem ein – anders ließen sich die gestellten Aufgaben einer solchen Software nicht erledigen. Benutzer geben der Software weitreichende Rechte. Normalerweise eine sinnvolle Sache, doch in der aktuellen Situation nach Ansicht der Sicherheitsexperten aus Bonn ein erhebliches Risiko.

BSI empfiehlt Deinstallation

Die Schutz-Software ist vor allem bei privaten Nutzern sehr beliebt – und in kleineren Unternehmen im Einsatz. Aufgrund des hohen Bedienkomforts ist es möglich, PCs, Rechner oder Mobilgeräte vor möglichen Angriffen zu schützen – oder auch Hackangriffe zu erkennen und zu melden. Die Sorge der Experten ist, dass diese Funktionen abgeschaltet und ins Gegenteil verkehrt werden könnten.

Das BSI empfiehlt deshalb, Apps und Anwendungen des Unternehmens Kaspersky möglichst zeitnah zu deaktivieren und zu deinstallieren. Kaspersky stellt zu diesem Zweck sogar eine eigene Funktion bereit.

Bei Bedarf sollten Produkte anderer Hersteller zum Einsatz kommen. Auf Windows-Rechnern reicht es nach Ansicht des auf IT-Sicherheit spezialisierten Experten Klaus Rodewig am meisten Sinn, den serienmäßig mitgelieferten „Windows-Defender“ zu aktiveren. Wichtig ist aber vor allem – und das auf allen Geräten! – regelmäßig bereitgestellte Updates zu installieren. Und das möglichst

zeitnah. Auf diese Weise lassen sich viele Hackangriffe verhindern.

Hersteller Kaspersky widerspricht den Bedenken

Der Hersteller Kaspersky widerspricht in einer ersten Stellungnahme den Bedenken und spricht von einer „politischen Entscheidung“. Das Unternehmen Kaspersky sei „ein internationales, unabhängiges Privatunternehmen ohne jegliche Verbindungen zu Regierungen, einschließlich der russischen. Wir haben niemals irgendeiner Regierung bei Cyberspionage geholfen und werden dies nie tun, erklärte das Unternehmen gegenüber dem Fachverlag Heise.

Die Absichten des Unternehmens sind vermutlich ehrenwert. Problematisch ist aber: Kaspersky hat seinen Firmensitz in Moskau und könnte sich damit möglichen Anordnung der Putin-Regierung unmöglich widersetzen. Und genau das ist der Grund für die dringende Warnung des BSI.

Was jetzt zu tun ist

Die BSI-Empfehlung zum Umstieg auf alternative Software sollte man im Augenblick ernst nehmen.

Auch ich setze Software von Kaspersky auf einigen Geräten ein. Ich misstraue jetzt nun nicht den Mitarbeitern bei dem agilen Unternehmen, unterschätze allerdings auch nicht, was die russische Regierung möglicherweise bereit ist zu tun.

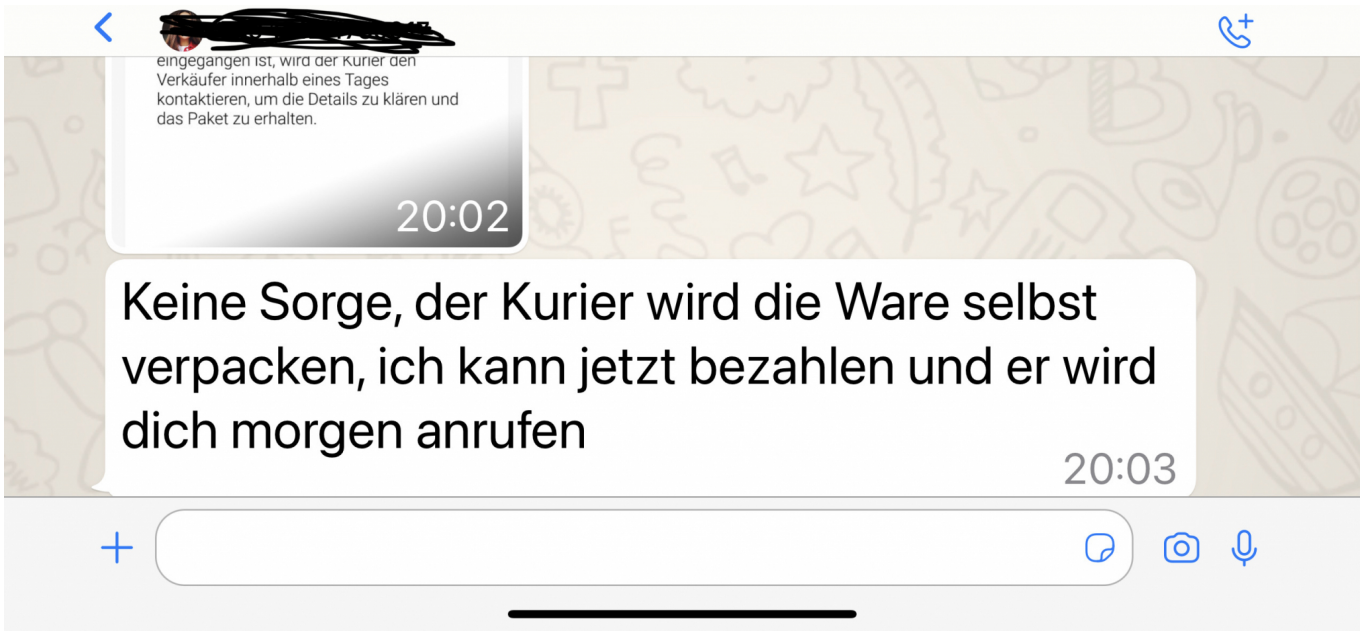
Es ist recht einfach, Kasperskys Antiviren-Software zu deaktivieren. Dazu genügt es in der Regel, die App oder die Anwendung zu deinstallieren. Auf Windows-Rechnern sollte anschließend der serienmäßig mitgelieferte **Windows Defender** aktiviert werden und so zum Einsatz kommen. Der bietet einen ausreichend guten Schutz vor VIren und Würmern.

Sollte es beim Entfernen der Software zu Problemen kommen, lohnt es sich, das von Kaspersky selbst bereit gestellte Entfernungsprogramm kavremove zu nutzen. Laut Hersteller bietet KavRemove eine "vollständige De-Installation von Kaspersky-Programmen". Glauben wir das mal. ;-)

Vorsicht bei Speditionsversand und ebay Kleinanzeigen

Es klingt so gut: Kaum ist das alte Fahrrad zum Verkauf online, da meldet sich ein Interessent: Sofortige Zahlung, Abholung per Spedition bietet er an. Vorsicht: Meist ist das ein Betrugsversuch!

eBay selbst hat lange auf ein eigenes Zahlungssystem umgestellt. Die Käufer zahlen an eBay, eBay leitet die Zahlung an den Verkäufer weiter. Das mag auf der einen Seite an einem gewissen Kontrollzwang von eBay selbst liegen, schützt aber auch Käufer und Verkäufer gleichermaßen. eBay steht als Zwischenstation auch für die Echtheit der Zahlungsvorgänge ein.

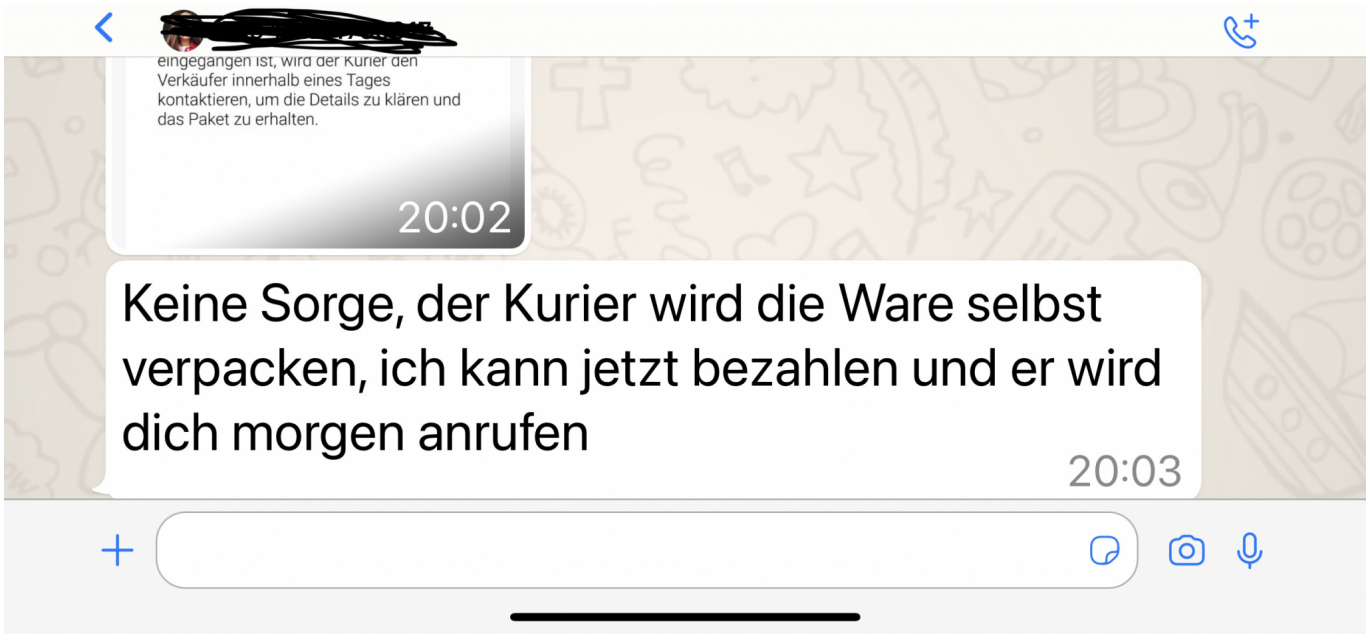


Anders sieht es bei eBay Kleinanzeigen aus: Käufer und Verkäufer kommunizieren direkt miteinander, unkontrolliert und offen für Betrugsmaschen. So sind Account-Übernahmen nicht selten, und auch der Zahlungsvorgang wird angegriffen.

Käufer - in den meisten bekannten Fällen vom Profilbild her junge, gut aussehende Frauen - melden sich per WhatsApp und bieten an, die sperrige Ware sofort zu bezahlen und dann von einer Spedition abholen zu lassen. Weil sie weiter weg wohnen, keine Transportmöglichkeit haben. Danach gibt es verschiedene Vorgehensmodelle:

Ihr sollt die IBAN schicken, damit die Überweisung erfolgen kann. Kurze Zeit später kommt dann eine Bestätigung "Deiner Bank", dass der Betrag eingegangen sei. Diese Bestätigung ist gefaked, aus der IBAN lässt sich ja die Bank auslesen und einfach eine vermeintlich echte E-Mail fälschen. Die so erbeuteten IBANs werden verkauft oder missbräuchlich genutzt, die Ware schnell von einer vermeintlichen Spedition abgeholt. Eine weitere Vorgehensweise: Die Bestätigung enthält einen so hohen Betrag, der Käufer bittet um Rücküberweisung der Differenz.

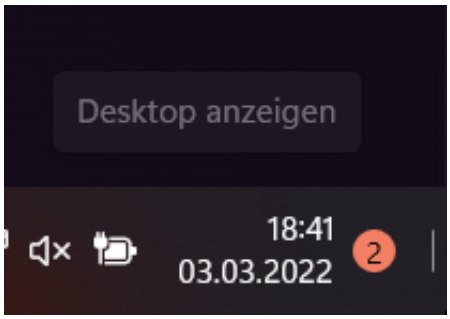
Befolgt immer die einfache Regel: Erst das Geld (in der Hand oder selbst überprüft auf dem Konto), dann die Ware!


eingegangen ist, wird der Kurier den
Verkäufer innerhalb eines Tages
kontaktieren, um die Details zu klären und
das Paket zu erhalten.
20:02
Keine Sorge, der Kurier wird die Ware selbst verpacken, ich kann jetzt bezahlen und er wird dich morgen anrufen
20:03

Alle Wege führen zum Desktop

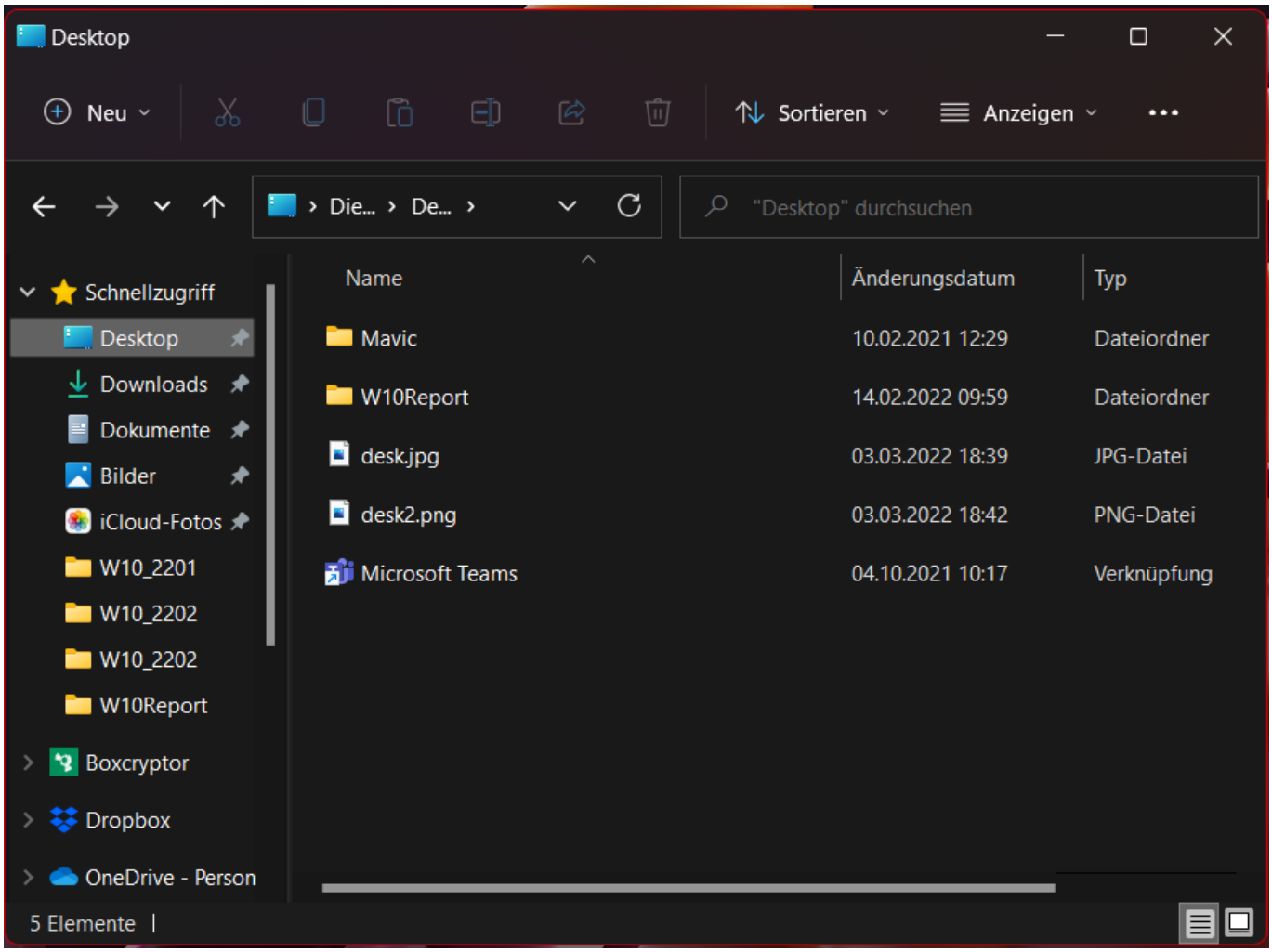
Der Desktop: Sammelbecken für Programme, Dateien und Verknüpfungen. Richtig eingesetzt ist dieser virtuelle Schreibtisch eine Riesenhilfe!

Windows und das echte Leben sind oft sehr ähnlich: Der eine Anwender ist Ordnungsfanatiker und hat alles peinlich aufgeräumt, der andere ist Jäger und Sammler und hat seine eigene, für andere Benutzer chaotische "Ordnung". Windows lässt beides zu! Am schnellsten erreicht Ihr den Desktop über eine Tastenkombination: Durch Drücken von **Windows** + **D** minimiert Windows alle Fenster und zeigt nur noch den Desktop an.



Wenig bekannt ist der Ecken-Trick: Mit dem Mauszeiger in der unteren, rechten Ecke des Bildschirms einmal geklickt reagiert Windows genauso: Alle Fenster werden minimiert und nur noch der Desktop angezeigt.

Zu guter Letzt ist der Desktop nichts anderes als ein Speicherort für verschiedene Dateien, der sich auch im Windows Explorer anzeigen lässt: Zum einen findet Ihr ihn unter den Schnellzugriffen ganz oben im Ordnerbaum. Ist diese Verknüpfung nicht vorhanden, dann führt der Weg ein wenig tiefer in die Verzeichnisstruktur.



Der Desktop ist immer an den Benutzer geknüpft. Folglich liegt der zugehörige Ordner auch im Verzeichnis **C:\Benutzer\\Desktop**. Egal, wie Ihr dorthin gelangt: Ihr könnt alle Elemente frei bewegen, Löschen oder auch neue hinzufügen, ganz so, wie Ihr es braucht.

Übrigens: Ihr könnt Eure Desktop-Symbole auch speichern, um sie später wiederherstellen zu können. Nicht mit Bordmitteln, aber mit einer kleinen, feinen

App.