Schieb Report

Ausgabe 2021.21

Mobilfunk-Provider führen Eco-Rating für Smartphones ein

Smartphones sind schick und leisrungsfähig - aber auch eine erhebliche Belastung für die Unwelt. Deshalb führen europäische Mobilfunk-Anbieter ein Öko-Rating für Smartphones ein - damit Kunden auf einen Blick sehen, wie nachhaltig bestimmte Modelle sind.

Bessere Kamera, schnellerer Prozessor, mehr Funktionen - und bitte möglichst schick und dünn: Bislang haben Smartphone-Käufer vor allem auf solche Aspekte geachtet, wenn sie sich ein neues Gerät angeschafft haben. Nur "stylische" Geräte mit möglichst viel (neuem) technischen Schnickschnack hatten lange Zeit eine Chance, möglichst viele Kunden zu begeistern.

Neue Hardware belastet immer die Umwelt

Doch das ändert sich allmählich. Zwar nicht unbedingt rasend schnell, doch es hat sich herumgesprochen: Die Nutzung digitaler Medien verursacht einen hohen CO2-Ausstoß, vor allem das Streaming. Aber auch die Geräte selbst werden alles andere als umweltschonend hergestellt - und entsorgt. Das alles kostet Ressourcen und belastet die Umwelt - und sorgt zunehmend für einen gewissen Scham-Faktor beim Hardwarekauf.

Immer mehr Kunden achten auf Nachhaltigkeit. Die Art der Herstellung wird langsam zu einem Verkaufsargument. Das haben auch die Mobilfunk-Provider erkannt. Die europäischen Mobilfunk-Anbieter haben jetzt ein gemeinsam betriebenes "Eco Rating" angekündigt: Schon bald wollen die Provider alle Smartphones nach diversen Öko-Gesichtspunkten vermessen und Punkte vergeben.

Wie nachhaltig ist die Herstellung, wie langlebig ist das Gerät, wie gut lässt sich das Gerät reparieren - und wie umweltschonend (oder eben nicht) wird es hergestellt. Für alles gibt es Punkte - bis zu 100 Punkte sind möglich.

Nicht alle Handy-Hersteller mit von der Partie

Die Idee ist grundsätzlich gut. Aber noch wollen nicht alle Handy-Hersteller mitmachen. Ausgerechnet Apple, Sony und Google sind noch nicht mit an Bord. Eine Kooperation ist erforderlich, da die Hersteller Auskunft geben müssen, etwa über die genauen Herstellungsbedingungen - oder wo die verwendeten Ressourcen herkommen.

Erstaunlicherweise macht auch Fairphone nicht mit - dabei bauen die Niederländer die mit Abstand nachhaltigsten und umweltfreundlichsten Smartphones. Fairphone gefällt das Bewertungssystem nicht. Es würden nicht alle relevanten Aspekte bei der Bewertung berücksichtigt.

Der große Wurf ist das geplante "Eco Rating" also noch nicht, aber eindeutig ein Schritt in die richtige Richtung: Hin zu mehr Sensibilität beim Einkauf von Hardware.

Ein Schritt in Richtung "Klima Awareness"

Allerdings könnten und sollten die Mobilfunk-Anbieter nicht nur auf die Hardware schauen, sondern auch auf ihre eigene Öko-Bilanz. Wer weiß: Möglicherweise soll die Bewertung der Hardware nur von der Tatsache ablenken, dass auch Mobilfunk alles andere als klimafreundlich ist. Denn die Mobilfunk-Anbieter verbrauchen enorme Mengen Energie für ihre Netzwerke und Rechenzentren.

Auch hier müssen wir unbedingt genauer hinschauen: Wie ökologisch werden Rechenzentren betrieben? Auch hier wäre ein Öko-Siegel denkbar - ja, sogar dringend erforderlich. Damit die Verbraucher entscheiden können, in welchem Netzwerk sie unterwegs sein wollen.

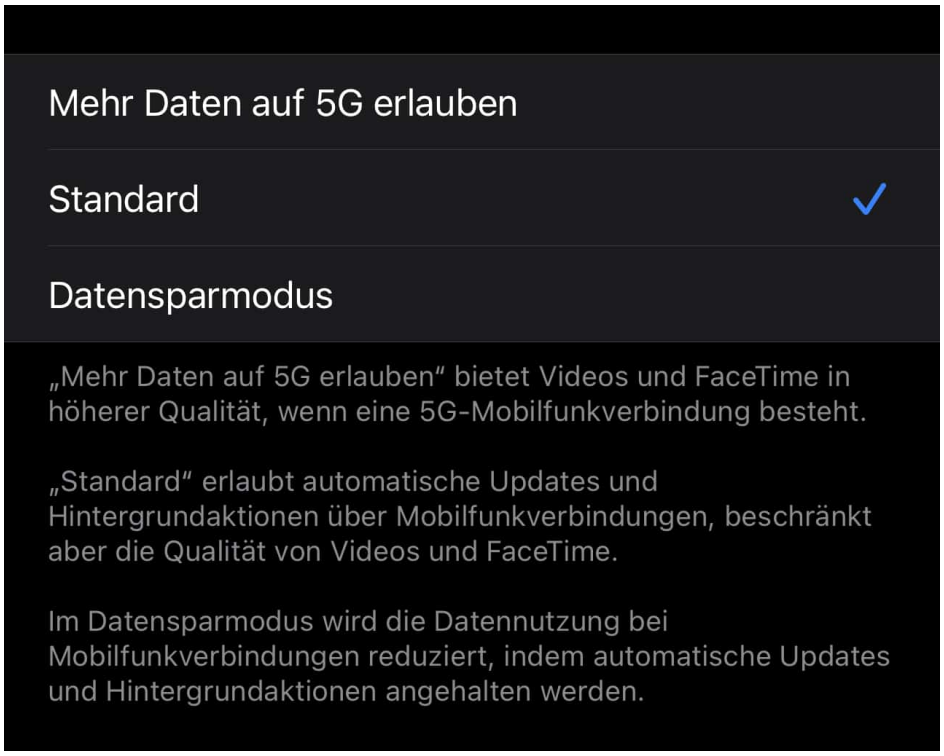
Wir stehen eben erst am Anfang.

Auch beim Handy-Kauf spielt Klimaschutz eine Rolle

Daten sparen bei 5G-Verbindungen unter iOS

Die neuen iPhones haben endlich auch die Unterstützung für das schnelle 5G-Netz integriert. Damit kann sich - entsprechende Netzversorgung vorausgesetzt - deutlich höhere Datendurchsätze und damit schnellerer Up- und Download möglich. Manche Netzanbieter trennen die Inklusiv-Volumen nach LTE und 5G, in sofern kann es Sinn machen, 5G nur auf relevante Datenübertragungen zu beschränken. Das erlaubt iOS mit Bordmitteln.

Um den Verbrauch von 5G-Daten zu beeinflussen, tippen Sie auf **Mobilfunk**, dann auf den Eintrag für die SIM-Karte, für die Sie diese Einstellung machen wollen. Dann tippen Sie auf **Datenmodus**. Im Normalfall steht die Einstellung auf **Standard** und Datenübertragungen werden über 5G geleitet, Videoübertragungen bleiben aber in normaler Qualität.



Mehr Daten auf 5G erlauben erlaubt zusätzlich bei FaceTime und Videostreams eine höhere Qualität, wenn Sie im 5G-Netz online sind. Damit steigt natürlich auch das benötigte Datenvolumen.

Gegenteilig wirkt Datensparmodus: Aktivieren Sie diesen, dann werden Updates und andere Hintergrund-Datenübertragungen verschoben, bis Sie wieder im WLAN sind und diese nicht über das Inklusivvolumen gehen.

Wenn Influencer für Geld Biontech verleumden

Eine PR-Agentur aus London spricht gezielt Influencer an - und bietet ihnen Geld an, wenn sie vor dem Impfstoff Biontech warnen. Einige haben das gemacht. Nach Recherchen scheinen russische Quellen dahinter stecken.

Mirko Drotschmann ist nicht nur Videoblogger und mit seinem Youtube-Kanal Wissen2Go für „funk“ der ÖRR sehr beliebt, sondern auch Influencer. Allerdings kein typischer. Er hinterfragt Dinge – und macht für Geld eben längst nicht alles. Vor einigen Tagen hat Mirko ein unmoralisches Angebot bekommen: Er sollte im Auftrag einer Agentur den Impfstoff von Biontech schlecht machen. Dafür wurde ihm Geld geboten.

Influencer erreichen oft Hunderttausende, manchmal Millionen Menschen – und sind deshalb begehrte Multiplikatoren. Es ist nicht ungewöhnlich, dass sich PR-Agenturen bei Influencern melden und sie bitten, für Geld für Produkte zu werben. Ungewöhnlich ist allerdings, dass Influencer für Geld gezielt Desinformationen verbreiten sollen.

Aber genau das ist passiert: Eine PR-Agentur aus London, sie heißt „Fazze“, hat in den vergangenen Tagen diverse Influencer aus drei Kontinenten angesprochen – und ihnen Geld angeboten, wenn sie auf ihren Kanälen – etwa auf Youtube oder

Instagram – gezielt Falschinformationen über den Impfstoff Biontech verbreiten.

Sie sollten behaupten, dass in ihrem Land eine große Zahl von Menschen an den Folgen einer Impfung mit Biontech gestorben seien – und dass sie sehr besorgt über diese Entwicklung seien. Also eine bezahlte Anti-Kampagne, die ganz bewusst für Unruhe und Verunsicherung sorgen soll.

Zwei Influencer haben falsch berichtet

Mindestens zwei Influencer haben zugegriffen. Ein brasilianischer Influencer mit drei Millionen Abonnenten und ein indischer Influencer mit 500.000 Abonnenten haben berichtet.

Sie haben Tabellen mit Todeszahlen gezeigt. Angeblich seien deutlich häufiger Menschen nach einer Impfung mit Biontech gestorben als bei AstraZeneca. Zahlen, die offensichtlich die PR-Agentur aus London bereitgestellt hat. Die Influencer haben ein Passwort für einen geschützten Bereich auf der Webseite

der Agentur erhalten, in dem Falschinformationen und Anweisungen für die Desinformation bereitgestellt worden.

Agentur hat russische Kundschaft

Ein starkes Stück.

Netzpolitik.org und das ARD-Magazin „Kontraste“ haben recherchiert. Es handelt sich offensichtlich um eine Scheinfirma, denn einen echten Firmensitz in Londo hat die Agentur nicht. Wie es aussieht, hat die Scheinfirma vor allem russische Kunden – und auch der Geschäftsführer scheint in Russland zu sitzen.

Keine Überraschung. Denn schon im April sind auf Twitter-Konten gezielt Bedenken gegen Biontech gestreut worden – damit der russische Impfstoff „Sputnik“ besser da steht. Es ist schwierig zu sagen, ob der Kreml dahinter steckt.

Aber russische Quellen stecken offensichtlich eindeutig dahinter. Wir müssen also feststellen: Es braucht nicht Facebook oder bezahlte Anzeigen in Sozialen Netzwerken, um gezielte Desinformation und Kampagnen zu verbreiten. Mittlerweile werden auch andere Tricks angewendet.

Influencer bewerben Crème mit Asbest

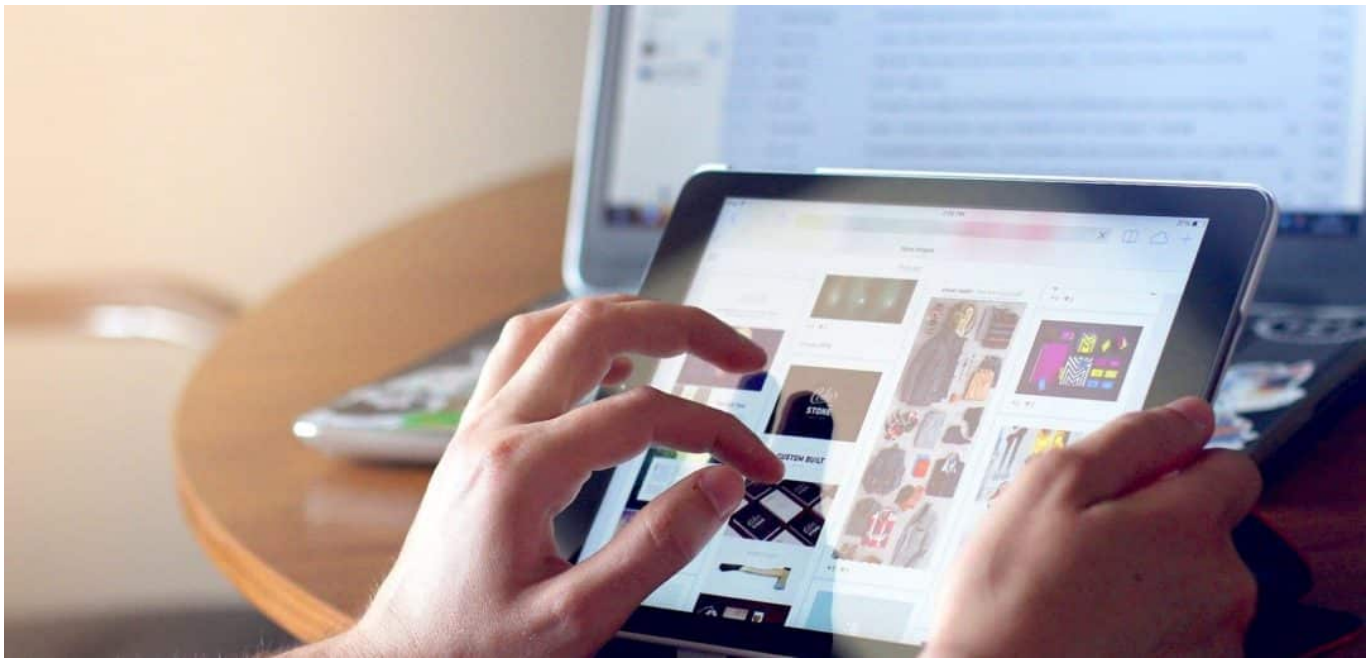
Influencer sind ja schwieriger zu kontrollieren als Werbeanzeigen auf Sozialen Netzwerken. Wie sehr kann man sich denn auf Influencer verlassen, dass sie Fakten-Checks machen und keinen Unsinn verbreiten?

Leider gar nicht. Ein Youtuber hat gerade einen sehr umfangreichen und aufwändigen Test gemacht: Er hat ein Pseudo-Produkt hergestellt, eine angebliche Gesichts-Crème – und die verschiedenen Influencerinnen angeboten. Er hat Geld angeboten, wenn sie die vollkommen wirkungslose Creme jubelnd vorstellen.

In Wahrheit Gleit-Crème. Auf dem Etikett standen die Inhaltsstoffe, darunter auch „Asbest“, „Uran“ und „Pipi-Kaka-Seed-Oil“. Das hat einige Influencerinnen aber nicht davon abgehalten, die Crème zu bejubeln. Was zeigt: Einige Influencerinnen und Influencer tun für Geld wirklich alles.

Es ist dringend nötig, hier was an den Regeln zu ändern. Influencer sollten ab einer bestimmten Zahl von Abonnenten auch in die Pflicht genommen werden. Sie müssen zB haften, dann würden sie einen solchen Unsinn nicht mehr verbreiten.

Digitalisierung - wer ist da nochmal zuständig, Frau Bär?



Wir steuern auf die Bundestagswahl zu - und alle Parteien erwecken den Eindruck, sich für Digitalisierung einsetzen zu wollen. Aber wie genau? Was soll passieren? Und vor allem: Warum ist es nicht längst geschehen? Laut einer aktuellen Studie sind die Deutschen "Online-Muffel". Wie sollte es auch anders sein, wenn es an der Infrastruktur mangelt?

Manche Erkenntnis ist so quälend offensichtlich, dass einen nur noch ein humorvoller Umgang damit rettet. Anders lässt es sich nicht erklären, dass wir Deutschen über Funklöcher, Papierformulare in Behörden und völlig unzureichenden Glasfaser-Ausbau nur noch ironische Bemerkungen machen: Weil wir es nicht anders kennen und - schlimmer noch! - gar nichts anderes mehr erwarten.

McKinsey: Deutsche sind "Online-Muffel"

Als wäre das noch nicht demütigend genug, präsentieren die Unternehmensberater von McKinsey eine aktuelle Studie. Auch sie belegt mal wieder, wie desaströs es in Deutschland um die Digitalisierung bestellt ist. Allerdings überschreibt McKinsey seine Studie "Deutsche Verbraucher bleiben Europa Online-Muffel".

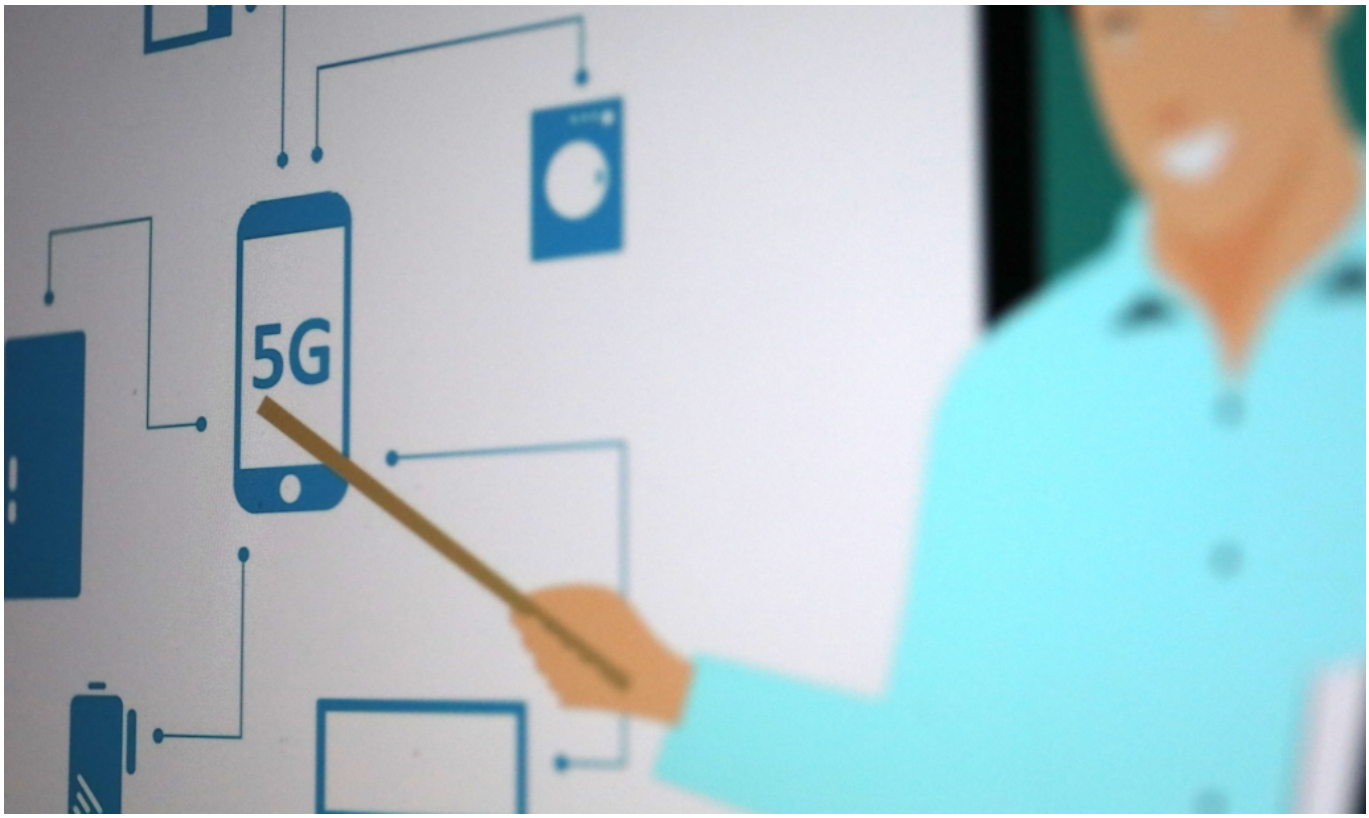
Als wären die Verbraucher schuld. Zwar finden sich auch in der Studie Hinweise, dass unzureichende Angebote und schlecht gemachte Benutzeroberflächen von behördlichen Angeboten die Menschen verunsichern. Doch den Verbrauchern gewissermaßen die Schuld in die Schuhe zu schieben, ist schon ein starkes Stück.

Was macht eigentlich die Staatssekretärin?

Auch seien "Datenschutzbedenken so groß wie in keinem anderen Land Europas", so die Studie. Zweifellos richtig, aber sicher nicht der Grund für die eigentlichen Probleme. Die da wären: schlechte Infrastruktur, unzureichend Glasfaser, zu wenig Sachkompetenz und Gestaltungswillen in den Ministerien.

Wozu haben wir eigentlich eine Staatssekretärin für Digitalisierung im Bundeskanzleramt? Dorothee Bär (CSU) leitet zwar kein Ministerium und hat zweifellos auch nur eingeschränkte Mittel zur Verfügung. Aber wie wunderbar wäre es gewesen, hätte die Zuständige in gut drei Jahren Amtszeit mal konkrete Konzepte und Visionen entwickelt, wie sich Deutschland digitalisieren ließe? Umsetzbare Konzepte, die in den passenden Ministerien dann umgesetzt werden - oder wenigstens mal diskutiert.

Aber nichts ist passiert.



Keine Konzepte, keine Visionen

Digitalisierung der Behörden, des Gesundheitswesens, der Forschung und Bildung, Ausbau der Netze (mobil wie Glasfaser) - es gibt so viele drängende Themen. Aber sie sind alle liegen geblieben. Nichts ist vorangekommen.

"Dorothee Bär ist das fröhliche Gesicht der digitalen Misere in Deutschland", schreibt der "Spiegel" - und hat völlig recht damit. Zwar wäre es ein Fehler, den Eindruck erwecken zu wollen, Dorothee Bär hätte die alleinige Verantwortung. Aber sie gehört der Bundesregierung an und ist Mitglied der größten Fraktion im Bundestag. Was würde sie unternehmen, würde sie einem Digitalministerium vorstehen, sollte das jemals kommen? Es ist ihr nicht gelungen, dafür eine Phantasie zu entwickeln.

Dorothee Bär über Klarnamenpflicht

Vermeiden von Virenbefall

Das klingt so toll: Sie haben eine Antivirussoftware installiert, dann kann Ihnen ja nichts mehr passieren. Oder? Diese Aussage ist ähnlich wahr wie „Ich schnalle mich an, dann kann ich ja einen Auffahrunfall riskieren!“. Besser ist es, wenn Sie sich schon im Vorhinein schützen, damit Viren gar nicht erst auf Ihren PC kommen. Wir zeigen Ihnen, wie Sie mit wenig Aufwand mehr Sicherheit bekommen.

Eine der Haupteinfallsquelle von Malware auf PC und Smartphone sind Apps, die Sie selber installieren. Nachdem Sie sie heruntergeladen haben, oder nachdem Sie einen Anhang in einer E-Mail geöffnet haben. Dabei muss es sich nicht mal um ein Programm handeln, auch andere Anhänge können Viren mitbringen oder nachladen. Achten Sie auf Folgendes:

Ist die Quelle sicher?

Die Verlockungen sind groß: Da gibt es den neuesten Kinofilm oder die angesagte

Serie kostenlos zum Download, per Mail bekommen Sie ein Dokument mit vermeintlich anstößigem Inhalt, das Sie unbedingt öffnen sollen und vieles mehr. Viele dieser Angebote bringen das Risiko von Malware mit.

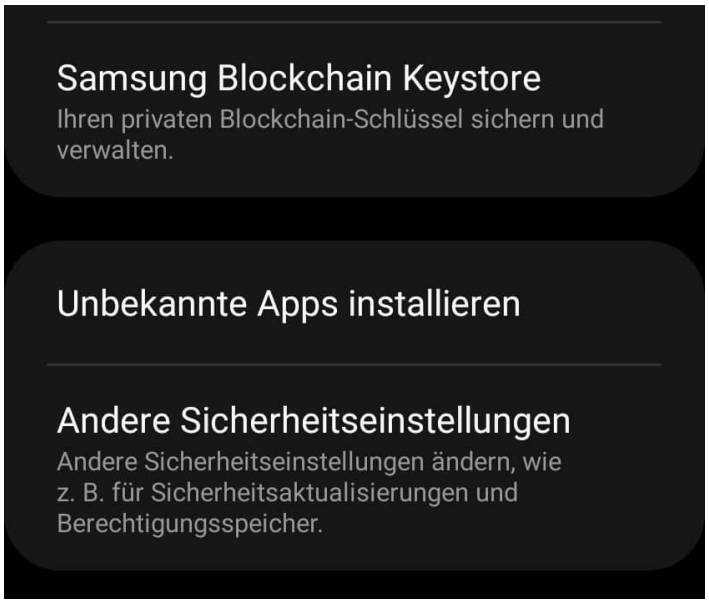
Achten Sie darauf, ob die Quelle vertrauenswürdig ist. Bei Downloads im Internet ist es wie im Versandhandel: Ist etwas viel günstiger als überall sonst oder gar kostenlos, dann verbirgt sich hinter dem Angebot oft eine böse Absicht. Schickt Ihnen ein Absender, den Sie nicht kennen plötzlich irgendwelche Dateien, dann widerstehen Sie der Neugier und öffnen diese einfach nicht!

Der Download aus App Stores

Windows, Mac, iOS, Android: Für die meisten Betriebssysteme gibt es eigene Software-Stores. Diese sind für den Download deutlich sicherer als irgendwelche Webseiten im Internet. Auch hier gilt wieder: Bietet man Ihnen sonst kostenpflichtige Software kostenfrei an, dann ist mit diesem Angebot oft etwas faul.

Besonders bei Android-Geräten sollten Sie vorsichtig sein: Es gibt den einen oder anderen vermeintlichen Softwareanbieter, der Ihnen die Android-Apps als APKs, zum Download anbietet. Normalerweise läuft der Download zwischen dem Android Play Store und Ihrem Gerät, ohne, dass Sie die Dateien in die Hand bekommen. Diese APKs sind oft nicht signiert und unterliegen keiner Prüfung durch Google oder eine andere Instanz. Solche Dateien sollten Sie nur in absoluten Ausnahmefällen verwenden. Dann, wenn Sie den Entwickler kenne und der Ihnen beispielsweise zur Fehlereingrenzung eine solche Datei zur Verfügung stellt.

Prüfen Sie, ob auf Ihrem Android-Smartphone **Einstellungen** > **Biometrische Daten und Sicherheit** > **Unbekannte Herkunft** aktiviert ist (die Option kann von Gerät zu Gerät und Android-Version zu Android-Version anders heißen). Diesen Schalter sollten Sie grundsätzlich deaktiviert lassen und nur dann aktivieren, wenn es wie oben beschrieben im Ausnahmefall nötig sein sollte.



Jailbreaks und Custom ROMs

Unter iOS und iPadOS haben Sie schon per se mehr Sicherheit, denn Apple hat das System sehr stark gekapselt. Damit kommen (Schad-) Apps gar nicht an die Systemdaten und können kaum Schaden anrichten. Hinzu kommt, dass jede App, die im Apple AppStore verfügbar ist, einem umfangreichen Test unterzogen wird, bevor sie zum Download verfügbar gemacht wird.

Auch hier gilt allerdings: Keine Regel ohne Ausnahme. Der so genannte Jailbreak (die Befreiung des Telefons aus dem von Apple verordneten Gefängnis) wird von Händlern angeboten. Im Internet finden sich dazu sogar einige Anleitungen, wie Sie diesen selber durchführen können. Auch wenn Sie plötzlich auf alle Dateien zugreifen können, andere Programme nutzen können und vieles mehr: Lassen Sie es. Das Risiko, dass die Aufhebung des Schutzes vor Schädlingen zu einer Infektion führt, ist höher als dieser Nutzen. Dasselbe gilt übrigens auch die die so genannten Custom ROMs bei Android!

Was tun bei Ransomware-Befall?

Fast noch schlimmer als ein normaler Virenbefall ist die Infektion Ihres Rechners mit einer Ransomware (einem Verschlüsselungstrojaner). Das ist eine Schadsoftware, die Dateien auf Ihrem PC verschlüsselt und diese nur gegen Zahlung einer teils heftigen Gebühr wieder entschlüsselt. Zumindest ist das das Versprechen, was die Ransomware Ihnen in der Meldung auf Ihrem Bildschirm anzeigt. Wir zeigen Ihnen, was Sie in einem solchen Fall machen sollten!

Zuerst die gute Nachricht: Die meisten Antivirenprogramme haben auch einen Schutz gegen Ransomware integriert. Die Wahrscheinlichkeit einer Infektion ist also begrenzt. Wenn Sie aber trotzdem in die Situation kommen, dass Ihre Dateien gekapert wurden, dann prüfen Sie die folgenden Dinge:

Identifikation der Ransomware

Programmierer eines Virus oder einer Ransomware sind meist mitteilsam: Sie wollen Ihnen zeigen, wie gut sie sind. Natürlich nicht so, dass Sie die Person

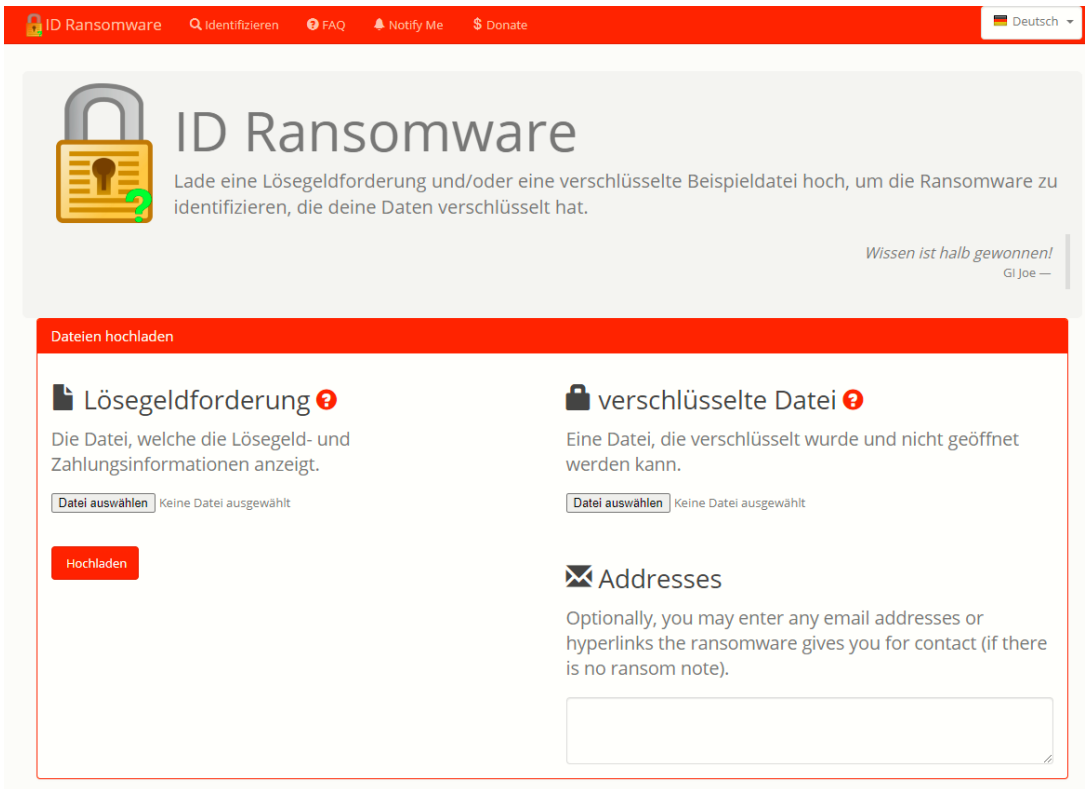
dahinter identifizieren können, aber eines können Sie immer machen: Die Infotexte mit der Suchmaschine Ihrer Wahl finden.

Das geht in den allermeisten Fällen, weil der Natur der Erpressung nach der Browser benötigt wird, damit Sie die Überweisung in Bitcoins ausführen können. Wenn Sie die Ransomware identifizieren konnten, dann finden Sie darin meist eine wichtige Entscheidung: Fahren Sie den Rechner herunter oder lassen sie ihn laufen.

Bei einem Teil der Ransomwares findet die Verschlüsselung erst nach einem Neustart des Rechners statt. Bei anderen sollten Sie den Rechner schnellstmöglich herunterfahren.

Beheben der Schäden

Um weitere Hilfe zu bekommen, können Sie auch einen Screenshot der Lösegeldforderung oder eine bereits verschlüsselte Datei bei dem kostenlosen Dienst ID Ransomware hochladen und bekommen Informationen über die Malware inklusive der ersten Tipps, was Sie als nächstes machen sollten.



Auch die Seite NoMoreRansom.com ist eine gute Anlaufstelle. Sie bietet Ihnen für

immer mehr Ransomwares Entschlüsselungssoftware an, die Ihre Dateien entschlüsselt und wieder zugänglich macht.

Das alleine ist allerdings nur ein Teil der Gegenmaßnahmen. Dieser nützt Ihnen nur kurzfristig, wenn Sie die Ransomware selber nicht loswerden. Das kann durch Ihre Antivirensoftware geschehen, die Ransomware als Virus erkennen sollte. Wenn Sie sich jetzt die Frage stellen, warum diese nicht schon die Infektion verhindert hat: Das kann viele Gründe haben, beispielsweise die Tatsache, dass auch Computerviren schnell mutieren und es immer eine Zeit dauert, bis die Virendefinitionen angepasst sind.

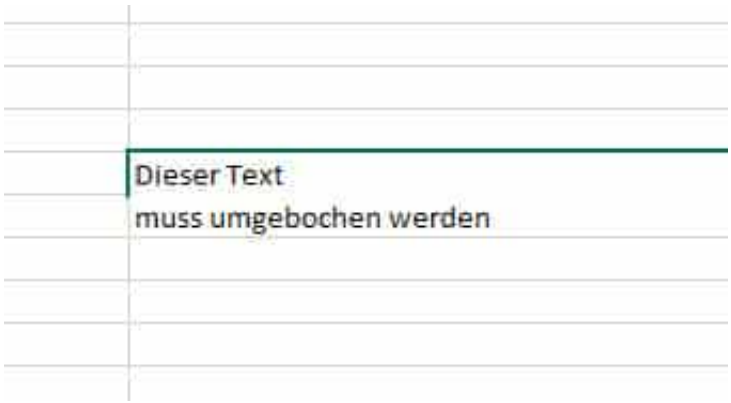
Um sicher zu gehen, installieren Sie Windows/macOS komplett neu! Das Einspielen eines Backups über eine Systemwiederherstellung (Windows) oder Time Machine (macOS) macht nur Sinn, wenn Sie sicher sind, dass zu dem Zeitpunkt die Infektion noch nicht erfolgt war.

Zeilenumbrüche in Excel festlegen

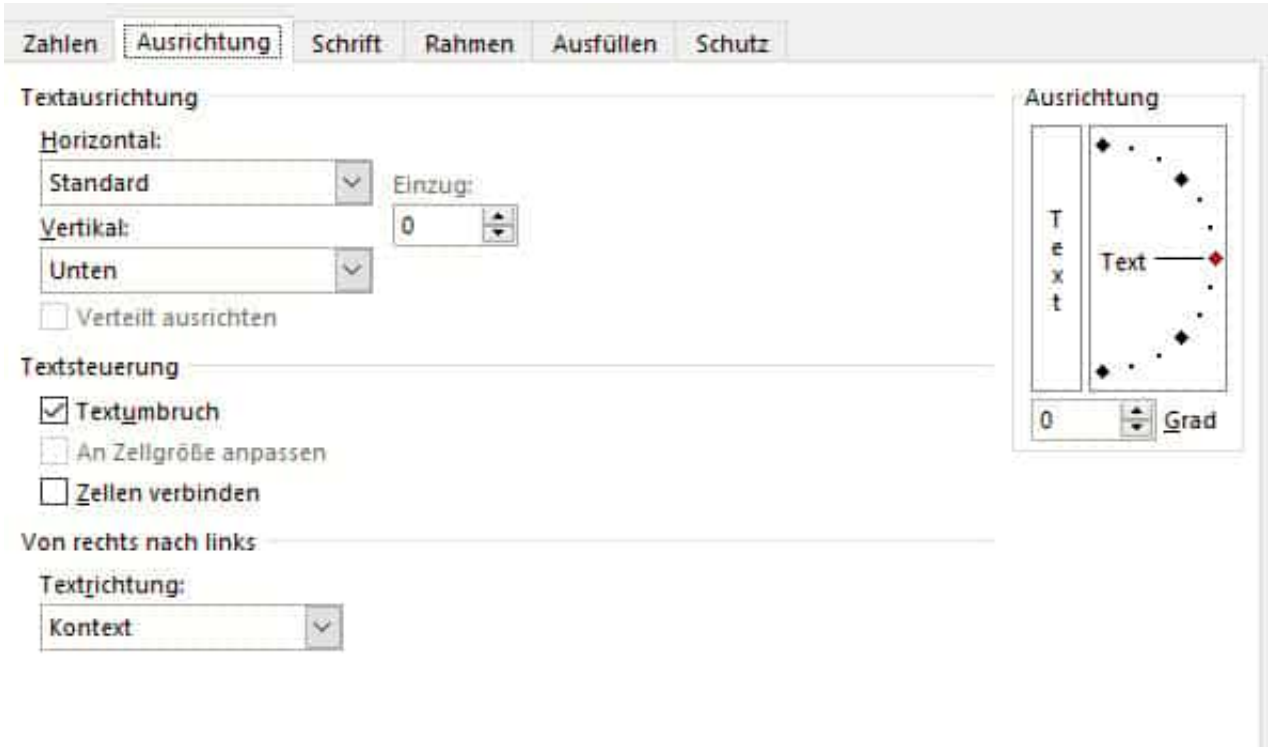
Excel ist als Tabellenkalkulation mit einem festen Anwendungszweck Teil der Office-Familie. Das bedeutet aber nicht, dass Sie nicht auch andere Elemente als reines Zahlenwerk in Excel pflegen können. Besonders bei Textfelder, die sowohl als Beschriftungen als auch als Kommentare dienen können, stellen Sie die Umbrüche das ein oder andere Mal vor Herausforderungen. Hier können wir helfen!

Im Normalfall schreibt Excel den Text immer weiter in die Zelle, auch wenn die Zellbreite lange überschritten ist. Das sieht weder schön aus, noch ist es effektiv: Ist die angrenzende Zelle ebenfalls gefüllt, dann gehen Ihnen Inhalte verloren. Die Lösung: Der Zeilenumbruch. Während dieser bei Word automatisch stattfindet, müssen Sie ihn in Excel manuell anwählen. Dazu haben Sie zwei Möglichkeiten:

Wenn Sie in einer Zelle einen Zeilenumbruch erreichen wollen, dann drücken Sie an der entsprechenden Stelle im Text gleichzeitig die Tasten **Alt** + **Eingabe**, Excel schreibt dann in der selben Zelle in einer weiteren Zeile weiter.



Wenn Sie Zellen nachträglich umbrechen wollen, dann markieren Sie zuerst die betreffenden Zellen. Klicken Sie dann mit der rechten Maustaste in die Markierung, dann auf **Zellen formatieren**. Wählen Sie die Registerkarte **Ausrichtung** und aktivieren Sie darin **Textumbruch**.



Optimal mit Tabs arbeiten in Microsoft Edge

Tabs sind das Haupt-Sortierkriterium für das Surfen im Internet. Jede Internetseite kommt in eine eigene Registerkarte. Dazwischen können Sie hin- und herspringen und so schnell zwischen den aktuell offenen Seiten wechseln. Je mehr Tabs es aber werden, desto unübersichtlicher wird die Navigation. Das können Sie in Microsoft Edge direkt mit Bordmitteln optimieren!

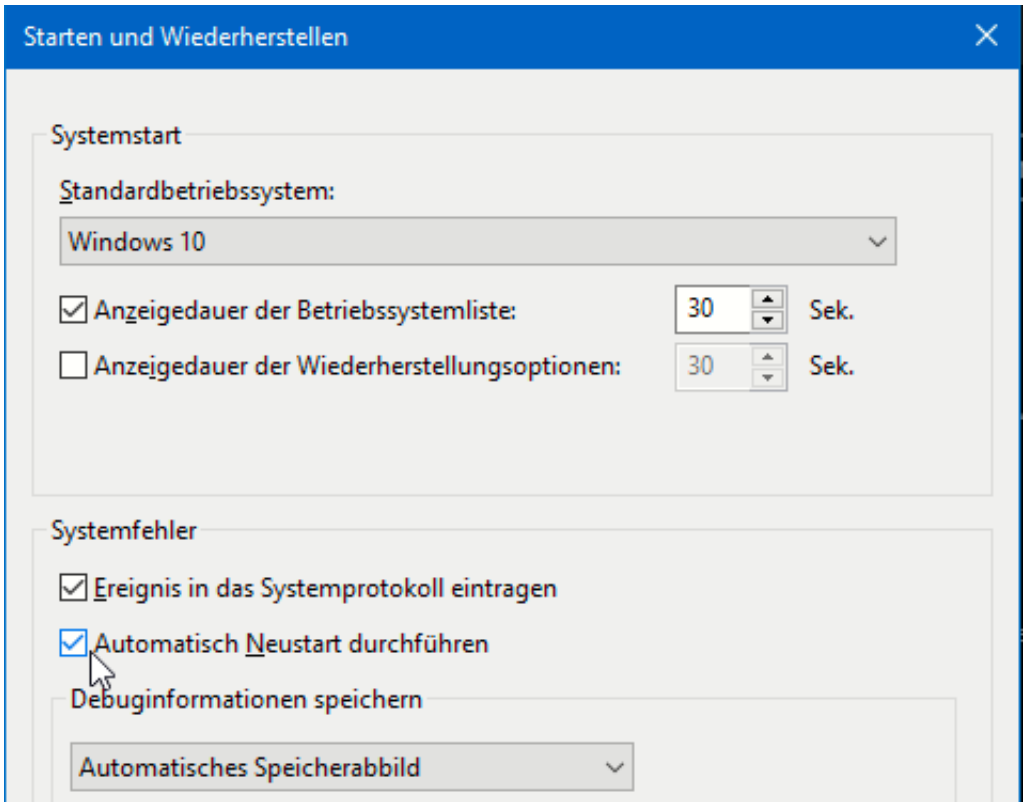
Oft ist das Problem, dass neue Tabs immer neben dem aktuellen erzeugt werden. Im Zweifel also mitten in der Vielzahl der offenen Seiten und später nur mit Aufwand wiederzufinden. Unter dem Menüpunkt **Tabs** in Microsoft Edge können Sie durch einen Klick auf Tab anheften die aktuelle Registerkarte fest ganz links neben den normalen Tabs als Symbol anheften.

Der Vorteil: Die angehefteten Tabs haben keinen Schließen-Button, der schnell mal versehentlich gedrückt ist und damit das Tab unwiderbringlich zu macht. Erst, wenn Sie mit der rechten Maustaste auf den Tab klicken und dann entweder **Tab lösen** und dann das **X** oder **Tab schließen** anklicken, können Sie es loswerden. Innerhalb der angehefteten Tabs können Sie dir Anordnung durch Anklicken und halten des Tabs verändern.

Neustart bei einem Systemfehler/Bluescreen unterbinden

Windows läuft stabil. Zumindest meistens. Wenn allerdings etwas Unvorhergesehenes passiert, dann quittiert das Betriebssystem das oft mit einem Bluescreen, einem blauen Fehlerbildschirm, der eine Vielzahl an Informationen enthält. Dummerweise haben Sie im Standard nicht wirklich die Zeit, diese Informationen aufzuschreiben: Ihr OC startet neu, und schon sind diese Informationen verschollen. Das können Sie ändern!

Der Schalter für den Neustart nach einem Bluescreen versteckt sich tief in den Systemeinstellungen. Geben Sie in das Suchfeld von Windows Systemeinstellungen ein und klicken Sie auf **Erweiterte Systemeinstellungen anzeigen**.



Klicken Sie jetzt in der Registerkarte **Erweitert** im Abschnitt **Starten und Wiederherstellen** auf **Einstellungen**. Im Bereich, der die Überschrift **Systemfehler** (das sind die Verursacher des Bluescreens) trägt, entfernen Sie den Haken neben **Automatisch Neustart durchführen**.

Tritt ein solcher Fehler auf, dann bleibt Windows auf dem Fehlerbildschirm stehen und wartet auf Ihre Reaktion. Machen Sie ein Foto von den angezeigten Werte, diese können Sie später mit der Suchmaschine Ihrer Wahl zur Fehlersuche verwenden!