Schieb Report

Ausgabe 2019.27

Studie: Was Google mit journalistischem Content verdient

Eine aktuelle Studie belegt: Google verdient nur extrem wenig an journalistischen Inhalten. Denn lediglich 0,25% der bezahlten Keywords/Suchbegriffe haben eine journalistische Relevanz.

Als vor einigen Wochen so leidenschaftlich über die EU-Urheberrechtsreform diskutiert wurde, ging es vor allem um die befürchteten Upload-Filter. Dabei hat die EU-Reform noch etwas Anderes gebracht: das Leistungsschutzrecht für ganz Europa. Google und andere Suchmaschinen sollen dafür bezahlen, wenn sie in Suchergebnissen Überschriften oder kurze Teaser präsentieren.

Auch dieses Leistungsschutzrecht ist äußerst umstritten. Unser Netzdenker Jörg Schieb ist nun auf eine interessante Studie gestoßen, die in diesem Zusammenhang eine Rolle spielt. Die Studie räumt auf mit der ständig wiederholten Behauptung, Google würde mit journalistischen Inhalten viel Geld verdienen.

Was soll das Leistungsschutztrecht?

Das Leistungsschutzrecht soll das geistige Eigentum von Autoren und Verlagen besser schützen. Das Argument: Suchmaschinen wie Google würden Unsummen damit verdienen, dass sie verlegerische Inhalte im Netz indexieren und in Suchergebnissen präsentieren, also nutzen – ohne die Verlage an den Einnahmen zu beteiligen.

In der Tat erscheinen bei einer Suche bei Google natürlich auch aktuelle Artikel. Das Leistungsschutzrecht schränkt das ein: Suchmaschinen dürfen nur noch einzelne Wörter präsentieren, anderenfalls müssen sie eine Abgabe zahlen. In Spanien und Deutschland gibt es das Leistungsschutzrecht schon – allerdings ohne dass Geld an die Verlage gezahlt wird. Wegen Sondervereinbarungen.

Wie viel verdienen Suchmaschinen an journalistischen Inhalten?

Konkret kann das nur Google beantworten. Aber Unsummen dürften es eher nicht sein. Denn Google News – der Suchbereich von Google, in dem man ausschließlich redaktionelle Texte präsentiert bekommt –, gibt es gar keine Werbung. Hier sucht man werbefrei – also ohne Umsatz. In der regulären Suche gibt es Werbung – aber eben nicht nur redaktionelle Inhalte.

Das Bonner Unternehmen Sistrix ist spezialisiert darauf, genau zu untersuchen, was im Web los ist: Welche Webseiten laufen gut, nach welchen Begriffen wird gesucht, was klicken die Leute an, wie wertvoll sind einzelne "Keywords" in den Suchmaschinen? So etwas weiß Sistrix besser als nahezu jedes andere Unternehmen in der Welt.

Die Firma bietet Werkzeuge für SEO an (Search Engine Optimization = Suchmaschinenoptimierung). Da ist es extrem wichtig, so etwas zu wissen. Sistrix hat konkret untersucht, welche Relevanz journalistische Inhalte eigentlichim Netz haben: Wie oft wird

danach gesucht, wie oft tauchen journalistische Inhalte in Suchergebnissen auf – und was kann Google damit verdienen.

Die Rolle journalistischer Inhalte

Knapp 8% aller Suchtreffer bei Google verweisen auf journalistische Domains – also auf die Angebote von Zeitungen, Sendern, Magazinen, Blogs. Das ist gar nicht wenig. Doch lediglich 4,6% der eingetippten Suchbegriffe sind journalistisch geprägt. Das ist schon wenig. Nur jede 25. Anfrage bei Google hat also im weitesten Sinne etwas mit Inhalten zu tun, mit denen sich Redaktionen und journalistische Inhalte beschäftigen.

Doch nun kommt der wirklich erstaunliche Information: Nur 0,25% aller Suchbegriff sind kommerziell relevant. Bedeutet: Nur bei einer von 400 Anfragen kann Google bezahlte Anzeigen präsentieren. Auf Keywords/Schlüselwörter mit redaktioneller Relevanz wird nicht geboten. Anzeigenkunden bezahlen dafür nicht.

Aber wenn ich "Angela Merkel" eingebe oder "EU-Ratspräsident", dann bekomme ich doch Tausende von Artikel gezeigt.

Keine Frage: Das ist so. Aber: Man wird dort keine bezahlten Anzeigen finden. Denn wer will darauf bieten? Was will man verkaufen, wenn man nach "Angela Merkel" sucht? Es gibt ja nicht mal ein Buch von ihr... Die Suchseite ist komplett werbefrei. Man müsste schon "Angela Merkel T-Shirt" eingeben, wenn man ein Fan-T-Shirt haben will – dann erscheinen Anzeigen von T-Shirt-Shops. Aber nicht wegen des Schlüsselworts "Merkel", sondern wegen "T-Shirt".

Was bedeutet das nun für das Leistungsschutzrecht?

Das bedeutet: Die Verlage überschätzen in diesem Punkt ihre Bedeutung hemmungslos. Google verdient viel Geld, aber ganz sicher nicht wegen redaktioneller Inhalte. Google könnte auf diese 0,25% Umsatz mühelos verzichten.

Wenn man bei Google einen Hebel umlegt und alle journalistischen Inhalte bei Google verschwinden, kostet das Google praktisch Null Umsatz. Die redaktionellen Webseiten hingegen würden deutlich weniger Besucher bekommen. Das macht eindrucksvoll deutlich, was für ein Popanz da aufgebaut wurde. Das Leistungsschutzrecht ist überflüssig wie ein Kropf und vollkommen sinnlos.

Leistungsschutzrecht: Google kann auch ohne Verlage

Die Studie eines auf Suchmaschinenoptimierung (SEO) spezialisierten Unternehmens aus Bonn fördert erstaunliche Ergebnisse zutage: Nur für einen verschwindend geringen Teil an Keywords, die mit journalistischem Content zusammenhängen, wird Geld bezahlt. Bedeutet: Google könnte mühelos auf die Indexierung von redaktionellen Inhalten verzichten.

Die äußerst umstrittene EU-Urheberrechtsreform hat uns nicht nur das Risiko für die Einführung von Upload-Filtern gebracht, sondern auch das Leistungsschutzrecht (LSR) für ganz Europa - obwohl ähnliche Vorschriften in Deutschland und Spanien effektlos sind, jedenfalls den Verlagen keinen Umsatz gebracht haben.

Der Wunsch der LSR-Lobby: Suchmaschinen wie Google sollen dafür bezahlen, wenn sie Headlines und Kurz-Teaser (Snippets) in den Suchergebnissen präsentieren. Dieser eher absurde Gedanke wurde vom EU-Parlament bekanntlich vor kurzem auf den Weg gebracht. Das Argument, dass Google mit den Inhalten der Verlage Geld verdiene, gebetsmühlenartig wiederholt.

Journalistische Inhalte spielen fast keine Rolle

Doch wie relevant sind journalistische Inhalte überhaupt für Google? Wenn die Menschen wahnsinnig häufig nach journalistischen Inhalten suchen, dann profitiert Google natürlich davon,

wenn viele Treffer zu Angeboten von Verlagen führen. Weil sie dann die Suchmaschine öfter nutzen und weil sie auf Anzeigen klicken (nicht auf Google News, da gibt es keine Anzeigen).

Doch ob hier überhaupt relevante Umsätze entstehen, ist schwierig zu sagen - denn eigentlich kann nur Google wissen, nach welchen Begriffen gesucht wird, welche angeklickt werden, was die User so beschäftigt und welche Umsätze daraus entstehen.

Eine Ausnahme bildet der auf Suchmaschinenoptimierung spezialisierte Anbieter Sistrix aus Bonn. Sixtrix beobachtet ganz genau, welche Suchbegriffe eingetippt werden, welche Keywords (Schlüsselwörter) zum Einsatz kommen, wie populär Webseiten sind, wie oft Menschen dort landen - und besonders wichtig: Was ein Anzeigenkunde zahlen muss, um bei einem Suchbegriff in der Trefferliste aufzutauchen. Nur damit verdient Google Geld.

Die unabhängigen Experten von Sistrix haben herausgefunden: Journalistische Inhalte sind für Google in der Regel irrelevant. Demnach verweisen 7,89 Prozent aller Suchtreffer auf journalistische Domains, 4,65 Prozent der Suchbegriffe sind journalistisch - aber nur 0,25 Prozent der kommerziellen Suchbegriffe sind journalistisch geprägt.

Google könnte auf Inhalte komplett verzichten

Das bedeutet: Nur bei einer von 400 Suchanfragen geht es um journalistischen Content - wo dann eine bezahlte Anzeige auftauchen könnte.

Würde Google einen Hebel umlegen und alle journalistischen Inhalte aus seinem Such-Index verbergen, würde dem Unternehmen praktisch kein Umsatz verloren gehen. 99,75 Prozent der bezahlten Keywords (also bezahlten Anzeigen) haben nichts mit journalistischen Inhalten zu tun.

Der Wirbel, der um das Leistungsschutzrecht gemacht wurde, und der Ärger, der dadurch entsteht, sind durch rein gar nichts zu rechtfertigen. Jeder Verlag, überhaupt jeder Anbieter im Web ist froh über "Traffic" von den Suchmaschinen. Den gibt es kostenlos. Und Google kann sehr gut ohne diese Angebote leben.

Das Leistungsschutzrecht: völlig überflüssig.

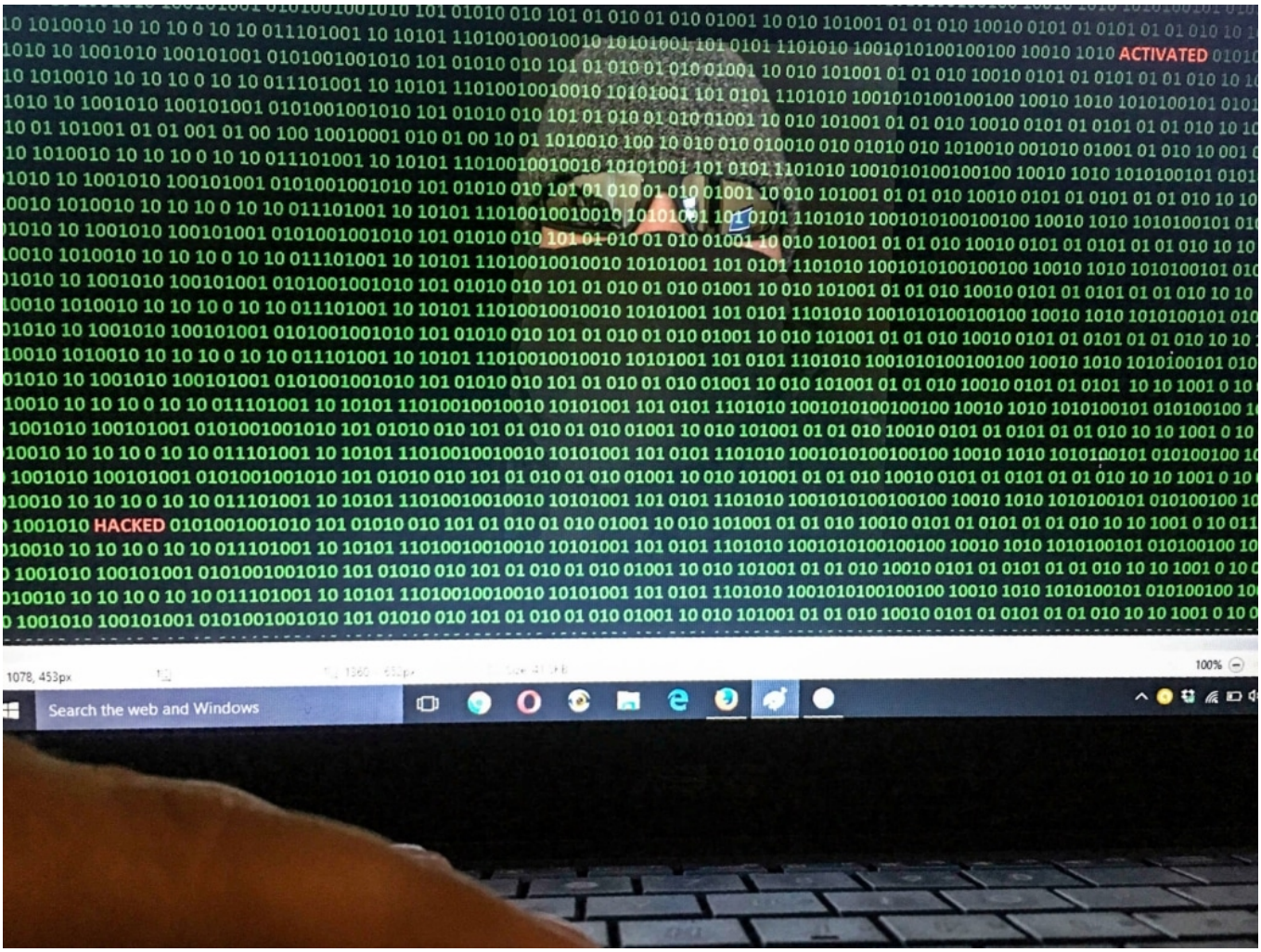
https://vimeo.com/326744808

Der Einsatz von Ethical Hackers

Unternehmen stehen ständig vor der Herausforderung, mit der wachsenden Bedrohungslandschaft Schritt zu halten. Eine Möglichkeit, um Sicherheitslücken in Systemen frühzeitig zu identifizieren, ist der Einsatz sogenannter **Ethical Hackers**.

Zu ihren Aufgabengebieten gehören etwa Penetrationstests von Netzwerken, Rechnern, webbasierten Anwendungen und anderen Systemen, um potenzielle Bedrohungen aufzudecken. Oft handelt es sich bei diesen Mitarbeitern um Hacker, die ihre Fähigkeiten in der Vergangenheit für illegale Aktivitäten wie etwa Einbruch in Unternehmenssysteme und -netzwerke genutzt haben.

Geläuterte Cyberkriminelle bieten damit einen umfangreichen Erfahrungsschatz sowie neue Denkansätze und können Lösungen vorschlagen, die nicht gleich auf der Hand liegen.



Bug-Bounty-Programme: Kopfgeldjagd auf Softwarefehler

Ein gutes Beispiel für das Einsatzspektrum von ethischen Hackern sind sogenannte Bug-

Bounty-Programme. Mit diesen setzen Unternehmen quasi ein Kopfgeld auf Schwachstellen aus. Damit bieten sie Hackern finanzielle Anreize, um Fehler in einem bereitgestellten Softwareprodukt zu identifizieren und zu melden. Unternehmen können dadurch zeitnah reagieren und Schwachstellen beheben, bevor sie öffentlich bekannt werden.

Die Sicherheitslücken Meltdown und Spectre sind gute Beispiele für Schwachstellen, die in einer großen Anzahl von Systemen gefunden und rechtzeitig gepatcht wurden, bevor sie umfangreich missbraucht werden konnten. Hätten böswillige Angreifer diese Lücken entdeckt, wären die Auswirkungen sehr weitreichend gewesen.

Mögliche Probleme beim Einsatz von Ethical Hackers

Wenn Unternehmen zulassen, dass Hacker versuchen, in ihre Systeme einzudringen, birgt das natürlich auch Risiken. Denn im Erfolgsfall muss darauf vertraut werden, dass der Hacker unternehmensloyal handelt. Ein probates Mittel dafür sind deshalb Bug-Bounty-Programme, da sie den Aufwand des Hackers von vornherein monetarisieren. Sobald eine Schwachstelle gefunden und bestätigt wurde, wird der Hacker für seinen Aufwand bezahlt. So gibt es nur einen begrenzten Anreiz, Daten zu stehlen oder den Exploit weiterzuverkaufen.

Wichtig ist: Die Geschäftsbeziehung zwischen Bug-Bounty-Plattform und Hacker basiert auf gegenseitigem Vertrauen und Respekt. Es gibt Fälle, bei denen sich Hacker nicht an die Regeln und Einschränkungen des Bug-Bounty-Programms gehalten haben. Dies kann rechtliche Konsequenzen durch das Unternehmen nach sich ziehen.

Ebenso sind einige Unternehmen und Bug-Bounty-Plattformen bekannt dafür, Hacker nicht zu bezahlen, obwohl die gemeldete Schwachstelle bestätigt wurde. Solch ein Verhalten schädigt das Vertrauen der Ethical-Hacker-Community enorm und kann sogar dazu führen, dass das Unternehmen und die Plattform auf eine Liste mit Zielen für böswillige Angriffe gesetzt werden.

programmer hacker working on front of his laptop writing code in the middle of night .[/caption]

Bedenken beim Einsatz ehemalig krimineller Hacker

Es gibt potenziell immer Personen, die Hacking nur wegen des Nervenkitzels betreiben. Deren Fähigkeiten können jedoch durch legale, herausfordernde Aufgaben positiv umgeleitet werden. Natürlich mag die Frage aufkommen, wie man sich sicher sein kann, dass ein ehemaliger Krimineller nicht wieder straffällig wird, doch dies ist kein spezifisches Problem der Cyber-Branche.

Wichtig ist, ein Umfeld zu schaffen, bei dem technische Herausforderung, Lern- und Weiterbildungsmöglichkeiten sowie entsprechende Vergütung gut ausgelotet sind. Überwiegen diese Vorteile, lohnt sich das Risiko einer Straftat nicht.

Auch ist es wichtig, dass die Gesetzeslage mit der Technologieentwicklung Schritt hält, damit strafrechtliche Konsequenzen gut bekannt sind und genügend Abschreckung bieten. Cyber-Straftaten werden oft immer noch nachgiebiger geahndet als andere Delikte mit vergleichbarem finanziellem Schaden. Ein Grund, weshalb organisierte Banden immer mehr in die Online-Welt abwandern.

Von Kontrolle zu Freiheit: Zusammenarbeit von Unternehmen und Hackern

Es sollten auf beiden Seiten sehr klare Vereinbarungen getroffen werden, die die Möglichkeit bieten, gegenseitiges Vertrauen aufzubauen. Beispielsweise können Unternehmen zu Beginn Zeit und Ort für die Nutzung internetfähiger Geräte begrenzen, um eine bestimmte Aufgabe zu erfüllen.

Ethische Hacker sollten Vorgaben und Abmachungen klar einhalten. Gleiches gilt für das Unternehmen. Werden Vereinbarung durch das Unternehmen nicht erfüllt, ist dies genauso schädlich für die Beziehung. Hat sich das gegenseitige Vertrauen schließlich bestätigt, sollten ehemalig straffällig gewordene Hacker wie jeder andere Mitarbeiter behandelt werden und die Verantwortung und Rolle erhalten, die ihnen gebührt. Dauerhafte Stigmatisierung erhöht erwiesenermaßen die Wahrscheinlichkeit einer Rückfälligkeit. Der Glaube an eine Rehabilitation ist ein wichtiger Bestandteil für ihr Gelingen.

[caption id="attachment_763758" align="alignnone" width="1030"]

Cosmotech Podcast Folge 5: Die Volksparteien und dieses Internet

In der neusten Ausgabe unseres Cosmotech-Podcast gehen wir der Frage auf den Grund, wieso die Volksparteien so große Schwierigkeiten im (richtigen) Umgang mit dem Internet haben. Vor allem die CDU tut sich schwer. Bei der Recherche haben wir gerausgefunden: Es sind womöglich die Strukturen, die eine große Rolle spielen. Wer Digitalisierung ernst nimmt, muss wohl hier ansetzen. Hört unsere neue Folge.

"Hey Rezo, Du alter Zerstörer" - mit diesen Worten hat CDU-Youngster Philipp Amthor seine bebilderte Antwort auf Rezos mittlerweile berühmtes YouTube-Video begonnen. Gar nicht schlecht! Immerhin hat sich Amthor die Mühe gemacht, auf Rezos provokantes Video zu antworten. Doch die CDU-Führung hat das Video eingesackt - kaum jemand kennt die Antwort von Amthor. Schade eigentlich - aber nur ein weiteres Indiz für die Hilflosigkeit, mit der die CDU auf den zunehmenden Druck aus dem Netz umgeht.

Digitalisierung im Schneckentempo

Ein Plot wie aus "House of Cards" oder "Designated Survivor": Ein simpler YouTuber greift die etablierte Politik an - und die Parteichefin gerät außer sich, droht mit Einschränkungen der Meinungsfreiheit und schüttet so noch Öl ins Feuer. Aber nicht nur die Chefin patzt - praktisch die ganze Partei ist paralysiert. Nicht nur die CDU, auch die SPD und die FDP wissen mit dem "Phänomen" nicht umzugehen.

Dennis Horn und ich haben uns gefragt: Wieso sind unsere Volksparteien in Sachen

Digitalisierung so schlecht aufgestellt? Wieso können sie nicht kommunizieren? Wieso geht es bei der Digitalisierung nur im Schneckentempo voran? Darum haben wir in unserer neuesten Ausgabe des Cosmotech Podcast mit cnetz-Sprecher Thomas Jarzombek gesprochen. Er klingt im Gespräch manchmal verzweifelt, aber trotzdem tapfer - und sagt den bemerkenswerten Satz:

> Jemand, der Digitalisierung nicht versteht, der darf künftig auch nicht mehr Bundesminister werden.

Die neuste Ausgabe des CosmoTech Podcast - jetzt anhören und abonnieren!

Ohne Digitalkompetenz kein/e Minister/in

Das ist ein Satz, schneidend wie ein Schwert. Denn im Grunde genommen bedeutet das die sofortige und fristlose Kündigung für praktisch das komplette Kabinett. Sieht man mal von Dorothee Bär oder Lars Klingbeil ab, die durchaus ein gewisses Verständnis für Digitalisierung haben - aber keine Ministerposten -, sind alle anderen Kabinettsmitglieder mehr oder weniger ahnungslos. Kanzlerin inklusive.

ARD-Korrespondentin Kristin Becker hat eine These, wieso es die Digitalisierung in der Politik so schwer hat: Möglicherweise könnten die verkrusteten Strukturen schuld sein, die es seit Jahrzehnten gibt - und nicht gerne geändert werden. Streng hierarchisch organisiert und zudem, regionalisiert: Ortsverbände. Landesverbände. Bundesverbände. Eine barrierearme Kommunikation ist gar nicht vorgesehen - eine mit dem "Volk" schon mal gar nicht. Erst recht nicht direkt.

Aber es ändert sich was. Thomas Jarzombek ist nicht der einzige, der entschlossen zu sein scheint, einen anderen Weg einzuschlagen. In dieser Hinsicht war das Rezo-Video sogar eine Hilfe. Selbst Uneinsichtige sehen ein, dass sich "was ändern muss". Was auch immer das bedeutet.

Mehr dazu gibt es in der aktuellen Ausgabe von unserem Podcast.

Polizei zerschlägt Drogen-Shop

Ecstasy, Amphetamin und Heroin – nur einige der illegalen Drogen, die im Onlineshop „Chemical Revolution“ zu kaufen waren. Die Polizei hat lange ermittelt – und ist nun gegen die Hintermänner vorgegangen. Elf Tatverdächtige wurden festgenommen. Der Onlineshop wurde abgeschaltet. Wie aber kann so etwas funktionieren: Ein Onlineshop für Drogen und wie kann die Polizei die Täter ermitteln.

Viele stellen sich die Frage: Wie haben die das gemacht, dass sie Drogen im Internet zum Verkauf anbieten und so lange nicht entdeckt wurden?

Was man wissen muss: Es gab offensichtlich einen ganz gewöhnlichen Onlineshop namens „Chemical Revolution“, im regulären Internet. Hier alles zu tarnen, so dass man nicht so leicht entdeckt wird, ist schwierig.

Darüber hinaus wurden die Waren aber auch und vor allem im Darknet verkauft, und zwar über den Darknet-Marktplatz „Wallstreet Market“. Hier sind Anbieter und Kunden grundsätzlich anonym unterwegs. Da ist es für die Polizei schwierig, die Betreiber zu vermitteln.

Verkaufen im Darknet

Vom Darknet sagt man ja häufig: Hier finden vor allem illegale Geschäfte statt. Wieso ist das dort so einfach – und wieso unternimmt der Staat nichts dagegen?

Zunächst einmal: Im Darknet gibt es keineswegs nur illegale Angebote. Es gibt auch nützliche Dienste. Journalisten in aller Welt zB kommunizieren über das Darknet, weil sie hier verschlüsselt und anonym Daten austauschen können – auch mit Informanten.

Das Darknet ist kein komplett eigenes Netz, sondern funktioniert über das Internet. Allerdings werden hier alle Daten und Informationen verschleiert: Nie kommuniziert ein Nutzer mit einem Server direkt, sondern immer über Umwege. Das macht es unmöglich, das Darknet abzuschalten – und es macht es sehr schwer, Akteure im Darknet auszukundschaften. Dann wird auch noch mit Bitcoin bezahlt, ebenfalls ein anonymes Zahlmittel.

Mehr oder weniger ja. Ins Darknet selbst gelangt man mit dem Tor-Browser – und für einzelne Bereiche braucht man dann allerdings oft eine Art Zugangspasswort. Man muss die Adresse kennen und braucht einen „Bürgen“.

Bitcoin ermöglicht anonyme Bezahlung

Bitcoin ist eine Kryptowährung und wird gerne zum Bezahlen von illegalen Geschäften genutzt. Wieso eigentlich?

Weil Bitcoin so anonym wird Bargeld ist – man braucht kein Konto, es gibt keine relevanten Datenspuren. Und man kann schnell auch große Beträge übermitteln, ohne einen Dienstleister zwischenschalten zu müssen, ohne Spuren, ohne Gebühren.

Ideal also, um krumme Geschäfte abzuwickeln. Es heißt zwar immer, dass bei Bitcoin keine Daten anfallen, das stimmt so allerdings nicht. Wer an wen bezahlt, das lässt sich rekonstruieren, ist aber extrem aufwändig – und setzt auch voraus, dass man ohnehin schon eine Menge weiss.

Wenn das alles so schwierig ist, wie hat die Polizei dann hier einen Fahndungserfolg erzielen können?

Genaue Angaben macht die Polizei natürlich nicht, sie will ja nicht ihre Taktiken verraten. Es wird aber gute alte Polizeiarbeit gewesen sein: Eine Person ist durch andere Geschäfte auffällig geworden, dann sind die Beamten der Spur gefolgt und haben die Onlineshop – auch die im Darknet – entdeckt. Auf diese Weise sind dann in wochenlanger Ermittlungsarbeit die Täter ermittelt worden.

#facebookdown: Kein Vorbote der Uploadfilter

Facebook, Instagram und WhatsApp down - für mehrere Stunden. Die Aufregung bei den Usern zeigt nicht nur, wie bedenklich abhängig viele sind. Auch die vermuteten Ursachen sind interessant: Es könnte ein Vorbote der Upload-Filter sein, hieß es unter anderem. Was unmöglich stimmen kann.

Es kommt immer öfter vor, dass es im Netzwerk von Facebook zu Problemen kommt. Dann herrscht bei vielen Usern Alarmstufe Rot: #facebookdown. Tatsächlich konnten viele User stundenlang in WhatsApp keine Sprachnachrichten austauschen. Fotos sind nur verschwommen erschienen.

Und auch die Instagram-Timeline zeigte häufig nur leere graue Kästen anstatt die eigentlichen Bilder – was uns aber immerhin vor den Werbebotschaften vieler Influencer verschont hat. Auch in Facebook selbst kam es mitunter zu Schwierigkeiten bei der Bilddarstellung.

[caption id="attachment_759895" align="alignnone" width="500"]


geralt / Pixabay[/caption]

Zentralisierung der Netzwerke ein Problem

Die meisten Nutzer denken in einer solchen Situation: Mit meinem Netz stimmt was nicht. Mein Smartphone spinnt. An eine Störung bei Facebook denken erst mal nur wenige – als wäre das Netzwerk eine Selbstverständlichkeit. Ein naives Urvertrauen. Doch solche Situationen zeigen noch etwas anderes: Die Abhängigkeit erschreckend vieler Menschen von diesen Netzwerken. Wer unruhig wird, nur weil ein soziales Netzwerk mal hakt, ist definitiv abhängig. Das mag man belächeln, ist aber ein ernsthaftes Problem.

Und eine weitere Problematik wird deutlich: Da Facebook wächst und wächst und offensichtlich die technische Infrastruktur für alle Netzwerke zusammenlegt, fallen bei Störungen auch alle Systeme wie Dominosteine um – und dann aus. Diese Mega-Konzerne und Mega-Netzwerke machen uns erkennbar verwundbar. Das wird bei Facebook deutlich – gilt aber auch für andere

Mega-Netzwerke, die für uns Nutzer häufig unsichtbar bleiben.

Keine Vorboten von Uploadfiltern

Allerdings ist es im Zuge der Ausfälle auch zu interessanten Mutmaßungen gekommen: Die Störungen seien womöglich ein Vorbote der Uploadfilter, die kommen sollen. Denn da, wo sonst die Fotos erscheinen - ob bei Facebook, im Facebook Messenger oder bei WhatsApp -, sind teilweise nur graue Rahmen mit einer Bildbeschreibung aufgetaucht.

Hintergrund ist aber: Facebook analysiert hochgeladene Fotos schon lange per KI. Die Software ermittelt grob, was im Bild zu sehen ist und fügt das in die Bildbeschreibung ein. Auf diese Weise lassen sich die Aufnahmen leichter kategorisieren und durchsuchen. Und: Menschen mit Sehbehinderung können sich die Beschreibung vorlesen lassen und erfahren so, was im Bild zu sehen ist.

Eine Vorbereitung auf Upload-Filter, zwei Jahre, bevor das tatsächlich nötig wird – nein, niemals. Das halte ich für ausgeschlossen.

https://vimeo.com/346069886

Störungen bei WhatsApp, Instagram und Facebook

Es gibt mal wieder Störungen im Facebook-Netzwerk: User können nicht auf Sprachnachrichten zugreifen - und es erscheinen häufig keine Bilder. Auf Twitter kursieren Verdächtigungen: Upload-Filter seien schuld, die gerade eingerichtet würden.

Auf der Onlinekarte von allestörungen.de ist es deutlich zu sehen: Über 15.000 Meldungen von Störungen in kürzester Zeit. Wer sich die Karte anschaut, sieht, dass vor allem Deutschland und Benelux betroffen ist. Aber auch vereinzelt in Spanien, in Südamerika und in Teilen von Asien werden Störungen gemeldet.

Bei WhatsApp lassen sich keine Sprachnachrichten senden und empfangen. Fotos und Videos funktionieren nicht - und im Foto-Stream von Instagram erscheinen keine Bilder. Vereinzelt gibt es auch Störungen in Facebook. Was aber funktioniert, sind Texte.

Das deutet auf Schwierigkeiten in der Server-Infrastruktur hin. Denn audiovisuelle Medien werden offensichtlich anders gespeichert und gemanagt als Texte. Das ist durchaus üblich. Hier scheint eine Störung vorzuliegen, die derart gravierend ist, dass mal eben die halbe Welt darunter "leidet".

Einige User spekulieren, es könnte sich um die Einführung des Upload-Filters handeln - der zu Fehlfunktionen führt. Als Beleg werden Screenshots präsentiert, die anstelle der Bilder kurze

Beschreibungen wie "Baum mit Sonnenuntergang" zeigen. Aber das ist ein normaler Vorgang: Facebook scannt alle Fotos auf Inhalte und "beschreibt" sie in der Beschreibung. Das soll Menschen mit Sehbehinderungen helfen: Ihnen werden die Beschreibungen vorgelesen.

Facebook und sein Oversight Board: Fragen und Antworten

Immer wieder kursieren Fotos, Videos und Nachrichten in den Sozialen Netzwerken, die gefälscht, bedenklich oder sogar kriminell sind. Facebook reagiert in der Regel eher zurückhaltend, lässt ein gefälschtes Video lieber etwas länger online als es zu stoppen. Und dann wiederum werden Posts gelöscht, die eigentlich in Ordnung sind. Es gibt ständig Ärger. Deshalb will Facebook eine Art „Schiedsgericht“ auf den Weg bringen, das in schwierigen Situationen entscheiden soll.

Was genau plant Facebook da?

Mark Zuckerberg hat ein Gremium angekündigt, das intern „Oversight Board“ genannt wird. Die Aufgabe: In schwierigen oder strittigen Situationen zu entscheiden, was gelöscht werden soll und was nicht. Sobald das Gremium eingerichtet ist, soll grundsätzlich jeder User die Möglichkeit haben, sich an das Gremium zu wenden, wenn es zu Schwierigkeiten kommt.

Etwa, wenn ein Post nicht gelöscht wird – oder wenn ein Post gelöscht wird, man selbst betroffen ist und das nicht in Ordnung findet. Es kommt manchmal ja auch zu Kontosperrungen, auch dafür ist das Gremium zuständig. Die Entscheidungen des Gremiums sind für Facebook bindend. Übrigens soll auch Facebook selbst sich an das Gremium wenden können, etwa, wenn Kritik von außen laut wird, die Facebook für unbegründet hält.

Wie setzt sich das Gremium zusammen?

Das Gremium soll hochklassig besetzt werden. Zunächst mit 40 Personen aus aller Welt und

aus unterschiedlichen Fachgebieten, etwa Menschenrecht, Journalismus, Peivatsphäre oder Recht. Eine Amtszeit dauert drei Jahre – und kann maximal ein Mal verlängert werden.

Facebook bezahlt die Leute, kann sie aber nicht vor die Tür setzen – nur bei extremem Regelverstoß. Verlässt ein Mitglied das Gremium, kann es selbst einen Nachfolger bestimmen. Auch Facebook kann neue Mitglieder vorschlagen, diese müssen aber vom Gremium genehmigt werden. Es sind also schon Vorkehrungen getroffen, dass Facebook sich keine Runde treuer Fans zusammenstellen kann.

Sind die Entscheidungen bindend?

Jede Entscheidung des Gremiums soll für Facebook bindend sein. Wie bei einem „Obersten Gerichtshof“. Außerdem sollen die Entscheidungen öffentlich gemacht, also dokumentiert werden. Allerdings ohne die Betroffenen Parteien konkret zu nennen, wo das möglich ist. Darüber hinaus erarbeitet das Gremium auch Empfehlungen für Facebook, etwa, was die Allgemeinen Geschäftsbedingungen oder die Praktiken betrifft. Diese sollen für Facebook aber nicht bindend sein.

Eine gute Idee?

Es soll noch in diesem Jahr los geht. Grundsätzlich finde ich es richtig, dass Facebook einen

Weg wählt, der weniger bequem ist als der bisherige, nämlich selbst die Regeln festzulegen und sie auch selbst zu interpretieren und durchzuführen. Von Machtteilung kann hier keine Rede sein.

Wünschenswert wäre, dass die Entscheidungen des Gremiums in jedem Fall bindend wären, auch wenn das Gremium die Nutzungsbedingungen ändern will – denn anders als die Firmenleitung hat das Gremium nicht den Profit im Focus. Nicht zuletzt muss man sagen: Es bleibt eine Lösung, die von der Rechtsstaatlichkeit entkoppelt ist. Das ist bedenklich.

Facebook und sein "Oversight Board": Kein schlechter Ansatz

Nach welchen Regeln soll Facebook Inhalte blockieren und löschen? Manchmal wird zu wenig gelöscht, manchmal zu viel. Einfach ist die Aufgabe ganz sicher nicht - was daran liegt, dass Facebook Plattform und Mediunm zugleich ist. Jetzt will Facebook ein "Oversight Board" rinführen. Eine Art Entscheidungsgremium für Zweifelsfälle - reicht das?
Man kann Facebook überflüssig finden, genial, banal, schädlich - aber eins steht fest: Einfach ist es nicht, Facebook zu sein. Vor allem wenn es darum geht, schädliche von nützlichen, echte von falschen oder legitime von illegalen Inhalten zu unterscheiden. Denn überall in der Welt herrschen andere Regeln und Gesetze. Jeder kann alles unkontrolliert und anonym hochladen.

Ganz zu schweigen, dass sich nur schwer klären lässt, was eine Lüge ist - oder ob ein Foto oder Video manipuliert wurde.

Facebook ist ein Medium

Doch auch wenn es schwierig ist: Das entlässt Facebook nicht aus der Verantwortung - was Mark Zuckerberg am liebsten hätte. Immer wieder betont er, dass Facebook kein Medium sei. Was Unsinn ist: Natürlich ist Facebook - auch! - ein Medium. Laut Definition ist ein Medium "eine Einrichtung, organisatorischer und technischer Apparat für die Vermittlung von Meinungen, Informationen, Kulturgütern". Das trifft auf Facebook ohne Abstriche zu.

Aber Facebook drückt sich - immer wieder. Vor einigen Tagen kursierte ein manipuliertes Video der US-Demokratin Nancy Pelosi im Netz. Das boshafte Video erweckt den Eindruck, die

Sprecherin des Repräsentantenhauses wäre high oder betrunken. Eindeutig mit dem Ziel in Umlauf gebracht, der Politikerin zu schaden. Youtube hat das Video schnell wieder aus dem Netz genommen - Facebook nicht. Erst sehr spät wurde das Video als bedenklich markiert. Aber gelöscht wurde es nicht.

Das "Oberste Gericht" für die Facebook-Welt

So etwas macht Facebook immer wieder - nur nach den eigenen Regeln spielen. Deshalb hat das Unternehmen jetzt ein "Oversight Board" eingerichtet. Eine Art "Oberstes Gericht" für das Facebook-Imperium. Die Moderatoren haben etwas gelöscht, was sie nicht löschen sollen? Oder fragwürdige Inhalte wurden nicht schnell genug oder gar nicht gelöscht? Künftig können Betroffene da das Oversight Board ansprechen.

40 Spezialisten aus der ganzen Welten - keine mit Facebook-Vergangenheit und keine Politiker - werden anfangs in diesem Gremium sitzen. In Vollzeit. Mit eigenen Mitarbeitern. Das Gremium soll bindende Entscheidungen fällen können. Wünschenswert wäre, dass dieses Gremium auch die Nutzungsbedingungen von Facebook abändern könnte - aber das ist noch umstritten. Leider. Die Mitglieder des Gremiums sollen maximal unabhängig sein.

Insgesamt erst mal eine gute Entwicklung. So ein Gremium wird nicht alle Probleme lösen können, aber doch mehr Bewegung in die Sache bringen. Allerdings entlastet das die Politik nicht: Auch die befindet sich bekanntlich im Tiefschlaf, wenn es um Digitalsierung geht (wie in

unserem Podcast diskutiert) und sollte eigene Regeln entwickeln, um zu regulieren. Das darf nicht an ein Oversight Board delegiert werden.

https://vimeo.com/280822037

Facebook blockiert nicht mal Holocoust-Leugner

Neue Ransomware installiert sich ohne Zutun

Forscher von Kaspersky haben eine neue Verschlüsselungs-Ransomware namens "Sodin" entdeckt, die eine kürzlich entdeckte Zero-Day-Windows-Sicherheitslücke ausnutzt, um erhöhte Berechtigungen in einem infizierten System zu erlangen. Des Weiteren nutzt sie die Architektur der Central Processing Unit (CPU), um eine Erkennung zu vermeiden, und benötigt keine Nutzerinteraktion zur Infizierung.

Ransomware, die Geräte oder Daten verschlüsselt oder sperrt und Lösegeld verlangt, ist eine ständige Cyberbedrohung für Privatanwender und Unternehmen. Die meisten Sicherheitslösungen erkennen bekannte Versionen und etablierte Angriffsmethoden. Die Sodin-Ransomware ist allerdings anspruchsvoller und nutzt eine kürzlich entdeckte Zero-Day-Sicherheitslücke in Windows (CVE-2018-8453) aus, um seine Rechte auf dem betroffenen System auszuweiten.

Die Malware scheint Teil eines RaaS-Programms (Ransomware-as-a-Service) zu sein. Die Hintermänner, die den Schädling in Umlauf bringen, können dabei frei entscheiden, wie der Verschlüsseler in Umlauf gebracht werden soll. Es gibt Anzeichen dafür, dass die Malware über ein Partnerprogramm verbreitet wird.

So haben die Malware-Entwickler eine Lücke in der Funktionalität hinterlassen, die es ihnen ermöglicht, Dateien zu entschlüsseln, ohne dass ihre Partner es wissen: eine Art Hauptschlüssel, der nicht den Schlüssel des Partners beziehungsweise Verteilers zur Entschlüsselung benötigt. Damit können die Entwickler Opferdaten entschlüsseln sowie die Verteilung der Ransomware kontrollieren, indem beispielsweise bestimmte Distributoren aus dem Partnerprogramm ausgeschlossen werden und die Malware unbrauchbar gemacht wird.

„Ransomware ist eine sehr beliebte Art von Malware, aber es kommt nicht oft vor, dass wir eine so ausgefeilte und hochentwickelte Version sehen“, erklärt Fedor Sinitsyn, Sicherheitsforscher bei Kaspersky. „Die Verwendung der CPU-Architektur, um unter dem Radar zu fliegen, ist für Verschlüsseler keine gängige Praxis. Wir erwarten einen Anstieg der Angriffe durch Sodin, da die Menge an Ressourcen, die zum Erstellen solcher Malware erforderlich sind, erheblich ist. Diejenigen, die in die Entwicklung der Malware investiert haben, erwarten auf jeden Fall, dass sie sich bezahlt machen.“

Sodin hatte bisher vor allem Opfer im asiatischen Raum im Visier: 17,6 Prozent der Angriffe wurden in Taiwan, 9,8 Prozent in Hongkong und 8,8 Prozent in der Republik Korea entdeckt. Es wurden jedoch auch Angriffe in Europa – darunter auch Deutschland und Italien -, Nordamerika und Lateinamerika beobachtet. Die Ransomware-Notiz, die auf infizierten PCs hinterlassen wird, verlangt von jedem Opfer Bitcoin im Wert von 2.500 US-Dollar für die Entschlüsselung.

Komplexe und hochentwickelte Ransomware

Ransomware erfordert normalerweise eine Form der Interaktion des Nutzers wie das Öffnen eines Anhangs in einer Mail oder das Anklicken eines schädlichen Link. Bei Sodin ist dies anders: Die Angreifer suchten sich anfällige Server und sendeten einen Befehl zum Herunterladen einer schädlichen Datei namens **radm.exe**, wodurch die Ransomware lokal gespeichert und ausgeführt wurde.

Sodin nutzt zudem die sogenannte „Heaven's Gate"-Technik, wodurch die Ransomware schwer zu erkennen ist. Mit dieser Technik kann ein schädliches Programm 64-Bit-Code aus einem laufenden 32-Bit-Prozess ausführen, was keine alltägliche Praxis ist und bei Ransomware nicht häufig vorkommt.

Die Forscher glauben, dass diese in Sodin aus zwei Hauptgründen verwendet wird:

- Um die Analyse des Schadcodes zu erschweren. Der Grund: Nicht alle Debugger (Software zur Code-Analyse) unterstützen diese Technik und können sie daher nicht erkennen;
- Um der Erkennung durch installierte Sicherheitslösungen zu entgehen. Die Technik wird verwendet, um die emulationsbasierte Erkennung zu umgehen. Hierbei handelt es sich um eine Methode zum Aufdecken zuvor unbekannter Bedrohungen, bei der Code in einer virtuellen Umgebung gestartet wird, die einem realen Computer ähnelt. So soll verdächtiges Verhalten einer Software aufgedeckt werden.

Kaspersky-Sicherheitstipps für Unternehmen

- Die verwendete Software sollte regelmäßig aktualisiert werden. Sicherheitsprodukte mit Funktionen zur Schwachstellenanalyse und zum Patch-Management können dazu beitragen, diese Prozesse zu automatisieren.
- Die Verwendung einer zuverlässigen Sicherheitslösung wie Kaspersky Endpoint Security for Business [3], die über verhaltensbasierte Erkennungsfunktionen verfügt, schützt vor bekannten und unbekannten Bedrohungen einschließlich Exploits.

[1] https://securelist.com/sodin-ransomware/91473/
[2]
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8453
[3]
https://www.kaspersky.de/small-to-medium-business-security/endpoint-select

Nützliche Links:
- Kaspersky-Analyse: https://securelist.com/sodin-ransomware/91473/
- Kaspersky Endpoint Security for Business:
https://www.kaspersky.de/small-to-medium-business-security/endpoint-select

E-Mails ganz einfach verschlüsseln

In der Welt der Messenger ist das Verschlüsseln von Nachrichten heute selbstverständlich - sogar Ende zu Ende. Auch Webseiten werden heute in aller Regel verschlüsselt übertragen (https://). Nur bei der E-Mail leisten wir uns den Luxus, auf Verschlüsselung weitgehend zu verzichten. Dabei wäre sie hier dringend nötig. Doch es gibt jetzt eine Lösung, die das Verschlüsseln von E-Mails einfacher macht.

Zweifellos würden mehr Menschen ihre E-Mails verschlüsseln, wenn es nur einfacher wäre. Doch gerade bei der E-Mails ist es zumindest mit etwas Aufwand verbunden: Man muss spezielle Extra-Software einrichten, Zertifikate austauschen und einiges mehr. Sender **und** Empfänger müssen auf den verschlüsselten Nachrichten, sonst klappt es nicht.

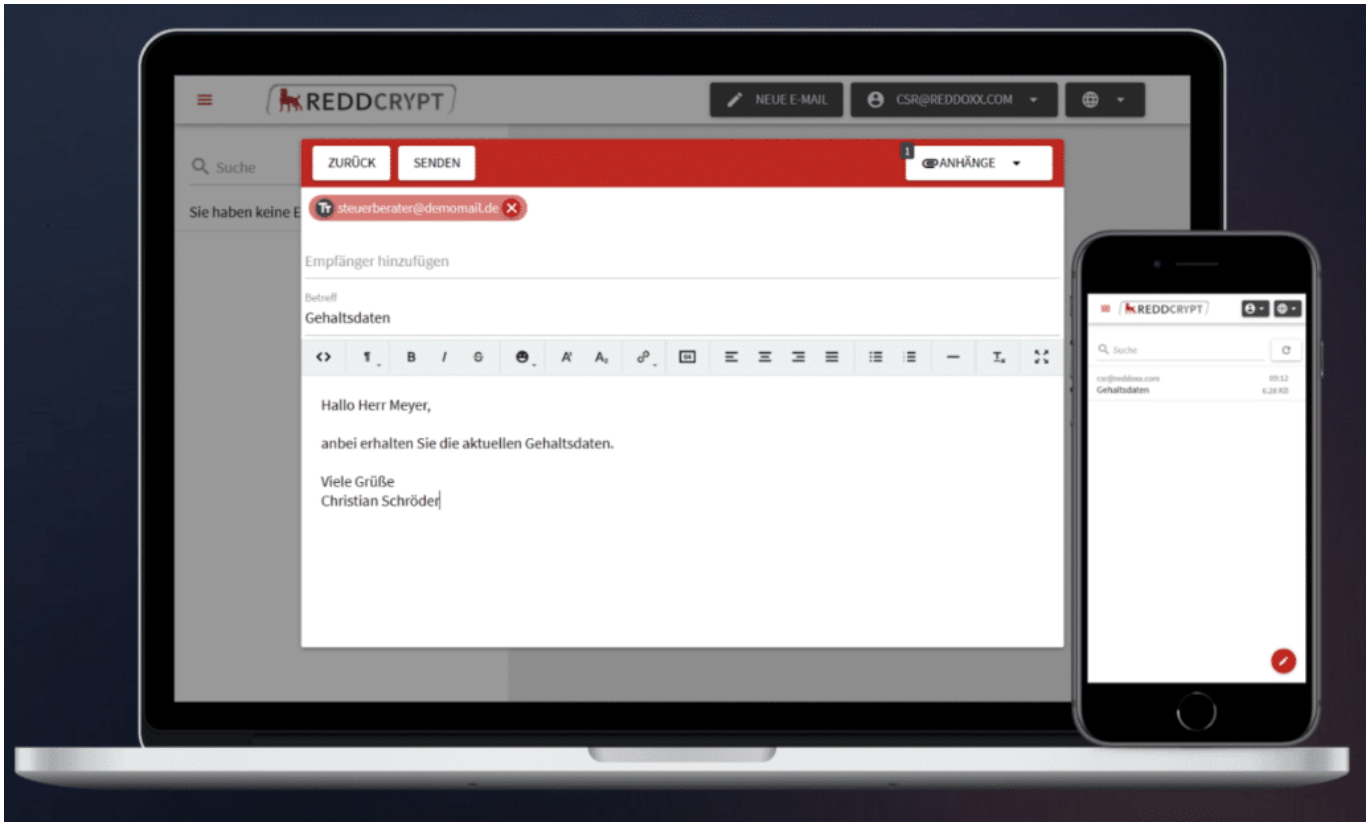
Die Lösung des deutschen Softwarehaus reddcrypt macht die Sache deutlich einfacher.

Data security and computer server network safety with a protection symbol of a lock with a keyhole[/caption]

Automatische Verschlüsselung

Bei der Registrierung per E-Mail-Adresse und Passwort generiert die Software automatisch ein OpenPGP-Schlüsselpaar (öffentlicher und privater Schlüssel), ohne dass der Anwender dabei eingreifen müsste. Das ist wichtig, damit Nachrichten verschlüsselt und entschlüsselt werden können.

Vor dem Versand einer Mail verschlüsselt das System nun Nachricht und Anhänge. Nutzt der Empfänger ebenfalls Reddcrypt, ist alles komplett automatisch erledigt. Es findet automatisch der öffentliche Schlüssel Verwendung – ein Austausch der Schlüssel im Vorfeld ist also nicht erforderlich.



Zertifikat für den Empfänger generieren

Sollte der Mail-Partner nicht bei Reddcrypt registriert sein - was die Regel sein dürfte -, erzeugt der Absender einfach einen individuellen Passphrase (Geheimcode) und übermittelt diesen an den Empfänger, etwa per SMS oder telefonisch, um sicher zu sehen. Das ist aber nur einmal nötig! Auf diese Weise entsteht im Hintergrund unbemerkt das Zertifkat für den Partner. Dieser Prozess ist nur einmal erforderlich.

Bis Ende des Jahres (31.12.2019) soll Reddcrypt inklusive aller Apps kostenfrei nutzbar sein. Die Web-App bleibt dauerhaft gratis verwendbar. Wer nur gelegentlich verschlüsselt kommunizieren muss, hat so eine bequeme Lösung. Für die Nutzung zusätzlicher Features wie Smartphone-Apps, Outlook-Plug-in oder Windows App sollen ab 2020 monatlich 2,00 Euro zzgl. MwSt. je E-Mail-Adresse für "Reddcrypt Professional" fällig werden.

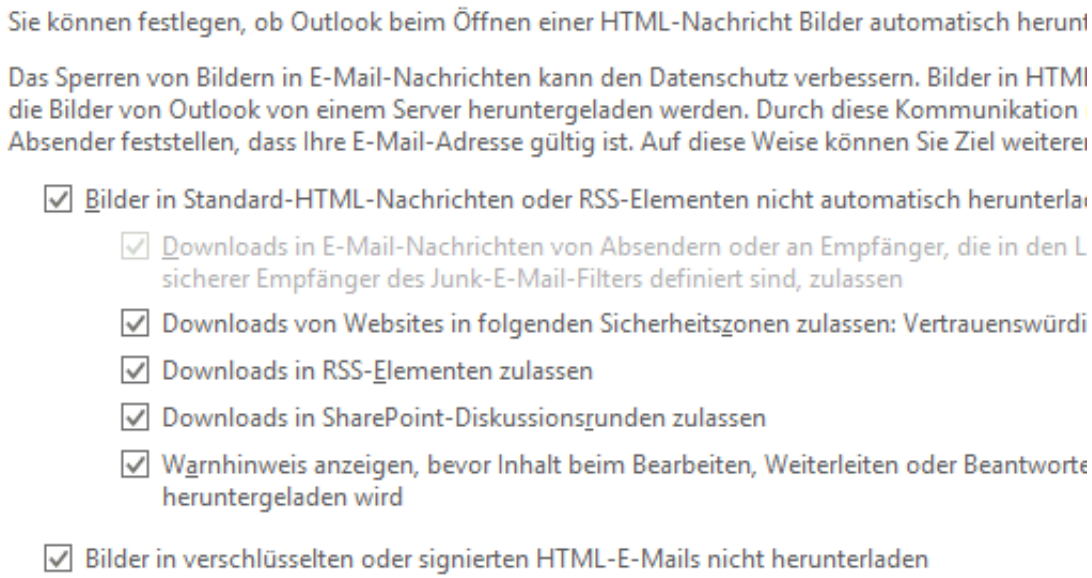
Weitere Informationen finden sich unter www.reddcrypt.com.

Kein automatisches Laden von Bildern in Outlook

Eine E-Mail besteht nicht nur aus Text. Ganz im Gegenteil: Mit Bildern können Sie viel mehr aussagen. Und so enthalten auch die meisten eingehenden E-Mails viele Bilder. Um die Mails dann so lesen zu können, wie Sie gedacht sind, können Sie den automatischen Download der Bilder aktivieren. Das sollten Sie sich allerdings zweimal überlegen!

Es gibt zwei Arten von E-Mails: Die einen enthalten die Bilder direkt. Auch wenn Outlook sie noch nicht anzeigt, sind Sie auf dem E-Mail-Server vorhanden, werden aber nicht dargestellt. Das macht Sinn, wenn Sie nur eingeschränktes Datenvolumen oder eine schlechte Internetverbindung zur Verfügung haben.

Die zweite Kategorie ist fieser: Die Bilder sind nur als Link hinterlegt. Aktivieren Sie den Download der Bilder darin, dann werden diese vom Server des Absenders nachgeladen. Oder aber von einem Server, den der Absender hinterlegt hat. Ein gängiges Mittel, um Traffic zu erzeugen und Webseiten besser in den Suchergebnissen zu platzieren. Oder Schadsoftware nachzuladen. Es macht also Sinn, die Bilder nur auf manuelle Anforderung - wenn Sie den Absender kennen und ihm vertrauen - herunterzuladen.

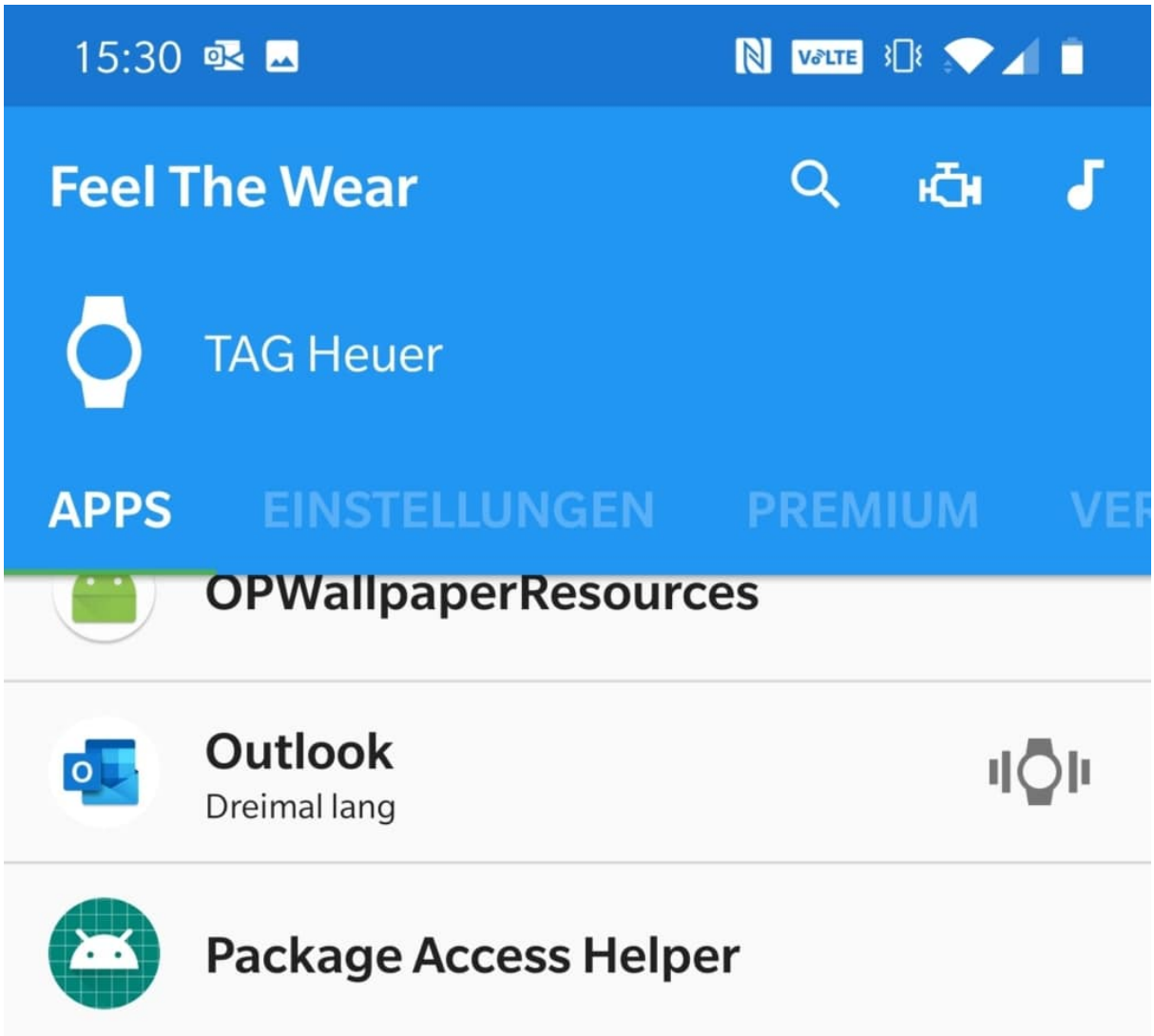


Klicken Sie dazu in Outlook auf **Datei** > **Optionen** > **Trust Center** > **Einstellungen für das Trust Center** und aktivieren Sie **Bilder in Standard-HTML-Nachrichten oder RSS-Elementen nicht automatisch herunterladen**. In einer solchen E-Mail finden Sie in der Kopfzeile einen Hinweis, dass die Bilder nicht heruntergeladen wurden. Das können Sie dann mit einem Klick nachholen.

Stärkere Vibration bei Smartwatches: Feel The Wear

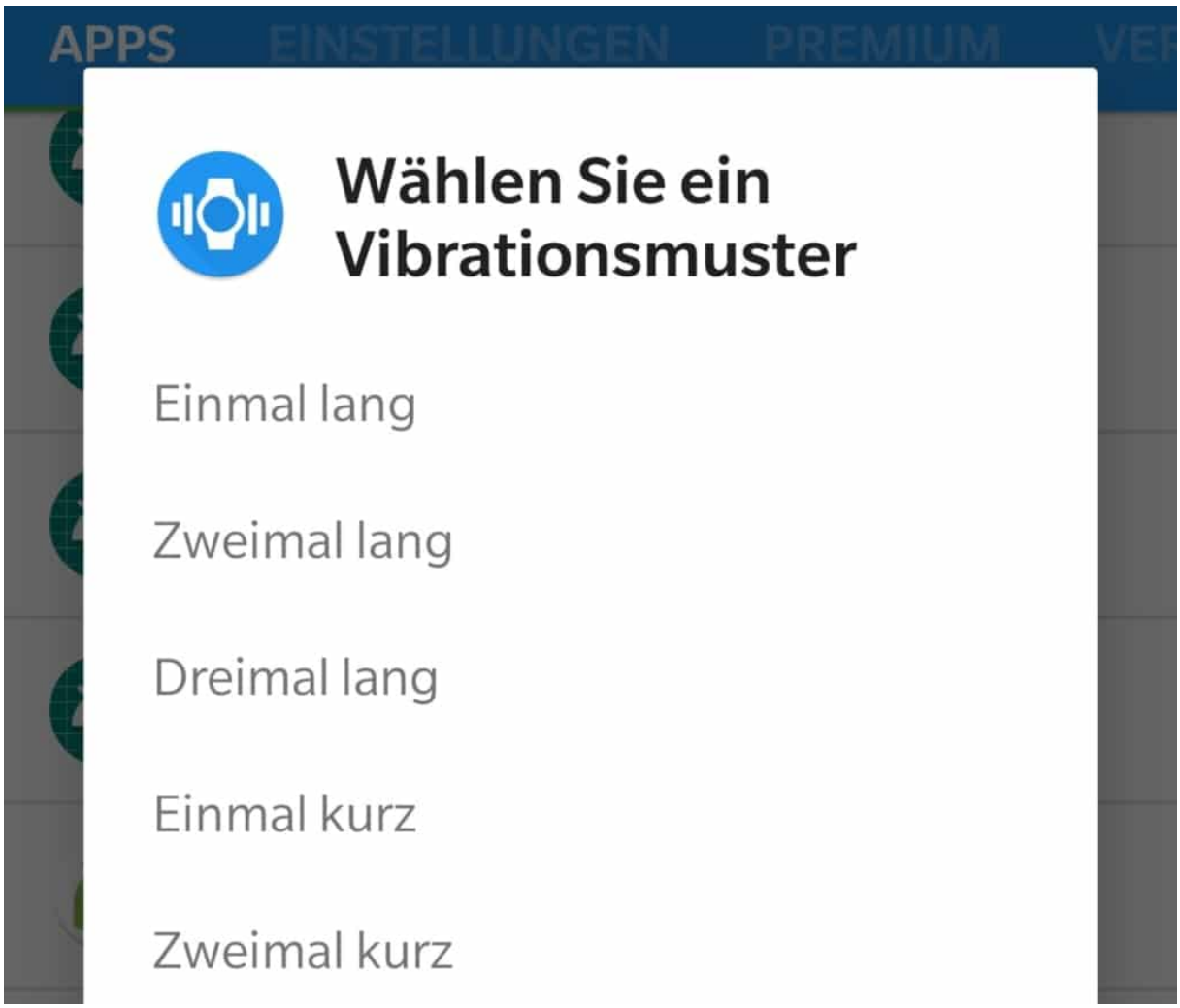
Smartwatches sind der zweite Bildschirm, den Sie an Ihrem Handy nicht haben. Der spart Ihnen, Ihr Telefon dauernd aus der Hosentasche zu holen, um nach neuen Benachrichtigungen zu sehen. Die Uhr vibriert, Sie wissen, dass Sie eine neue Nachricht haben und mit einem kurzen Blick sind Sie informiert. Je nach verwendeter Hardware ist die Vibration allerdings nicht so stark, daß sie in jeder Situation bemerkbar ist. Abhilfe schafft hier die kostenlose App Feel The Wear bei Android Wear-Smartwatches.

Der Vibrationsmotor der Smartwatch ist nichts, was Sie beeinflussen können. Wohl aber die Auffälligkeit der Vibration. Eine Standardvibration mit einem kurzen Signal merken Sie nicht. Mehrere Vibrationen hintereinander, vielleicht auch noch mit unterschiedlichen Längen schon eher. Und genau hier setzt die App an.



Für jede App, die auf Ihrem Smartphone installiert ist (inklusive der System-Apps, die Sie normalerweise gar nicht sehen) steht zur Auswahl. Wählen Sie eine App aus, dann können Sie

das Vibrationsmuster auswählen. In der kostenlosen Version der App sind die Muster vorgegeben. Die Vibrationen sind dann entweder nur lang oder nur kurz.



In der Kaufversion (die Sie ab EUR 2,29 bekommen) können Sie dann eigene Muster festlegen. Beispielsweise das klassische SOS-Signal, wenn ein Anruf eingeht. Der Vorteil: Zum einen erkennen Sie auf Wunsch sogar einzelne Apps, zum anderen verpassen Sie keine Benachrichtigung mehr, auch wenn der Vibrationsmotor Ihrer Smartwatch schwach ist.

Akkutausch als Selbstbausatz für ältere iPhones

Alles hat ein Ende. Auch der Akku eines Smartphones. So sehr die Technik in den vergangenen Jahren vorangeschritten ist: Der Akku ist immer noch die Achillesferse eines mobilen Gerätes. So sehr, dass Apple zeitweise sogar eine Bremse in iOS eingebaut hatte. Je schwächer der Zustand des Akkus, desto langsamer wurden die iPhones gemacht. Das sollte vermeiden, dass die Geräte bei prozessorhungrigen Anwendungen einfach abschalteten. Der Tausch eines Akkus ist aber mitnichten eine Aufgabe, die nur eine Werkstatt machen kann: Die wenigen Handgriffe können Sie auch selbst ausführen.

Wenn der Akku stirbt, dann ist das noch kein Grund, das gesamte Gerät zu entsorgen. Die meisten Komponenten (wie Prozessor, Speicher, Display, Funksender etc.) unterliegen weit weniger einem Verschleiß und sind meist noch in Ordnung. Der Tausch des Akkus über einen Händler oder eine Vertragswerkstatt ist meist nicht wirtschaftlich: Kostenpauschalen im dreistelligen Bereich sind keine Seltenheit. Die Abwägung, ob eine Reparatur sich noch lohnt, schlägt da eher negativ aus.

Prinzipiell ist die Reparatur in eigener Hand möglich, wenn man weiss wie und das entsprechende Werkzeug hat. Dieses Paket (natürlich inklusive des Akkus) gibt es zum Beispiel mit den Hagnaven-Akkus. Diese bestehen (neben einer Apple-würdigen Verpackung) aus dem Akku selbst, der Anleitung und dem gerätespezifischen Werkzeug, das zum Öffnen des Telefons nötig ist.

Braucht der Akkutausch Mut? Sicherlich. Auf der anderen Seite: mit einem nicht mehr leistungsfähigen Akku macht der Betrieb des Smartphones auch keinen Sinn. Ist der Akkutausch schwierig? Nicht wirklich. Wenn Sie einen Schraubenzieher in der Hand halten und benutzen können, dann sind Sie hier nicht überfordert. Und das für einen Preis von - abhängig vom Modell des Smartphones - unter EUR 30,- ist das Risiko überschaubar und der "Gewinn" im Vergleich zur Werkstatt immens.

Die richtige Pflege eines Tablets

Vor vielen Jahren gab es mal ein Buch namens "Pflege und Aufzucht eines Pocket PCs". Die Idee dahinter: Alle Tipps zusammenzufassen, die einen Pocket PC möglichst effektiv und langanhaltend einsetzbar machen. Pocket PCs sind Geschichte, der Ansatz aber nicht. Wenn Sie ein mobiles Gerät einsetzen, dann können Sie mit wenigen Schritten dazu beitragen, dass es verlässlich und lange seinen Dienst verrichtet.

Der Akku

Auch wenn Akkus seit längerem keinen spürbaren Memory-Effekt mehr haben, Pflege tut trotzdem Not. Entladen Sie Ihr Gerät einmal im Monat so weit es geht bevor Sie es wieder laden. Das hält die Akkuzellen frisch, hält aber auch die Ladeanzeige aktuell. Die regelmäßige Entladung eines Akkus führt zur Neukalibrierung der Akkustandsanzeige und macht diese genauer.

Das Display

Ein Touchscreen ist seiner Natur nach empfindlich (im Sinne der Erkennung von Berührungen). Fingerabdrücke sehen Sie schnell und anhalten. Darum reinigen Sie es in regelmäßigen Abständen. Verwenden Sie dazu keine scharfen Reinigungsmittel. Am besten verwenden Sie dazu ein Mikrofasertuch, das leicht feucht ist, oder ein anderes fusselfreies Tuch mit Brillenreiniger. Glasreiniger ist definitiv das falsche Mittel und fügt dem Glas eher Schaden zu!

Umgang mit Netzteil und Kabeln

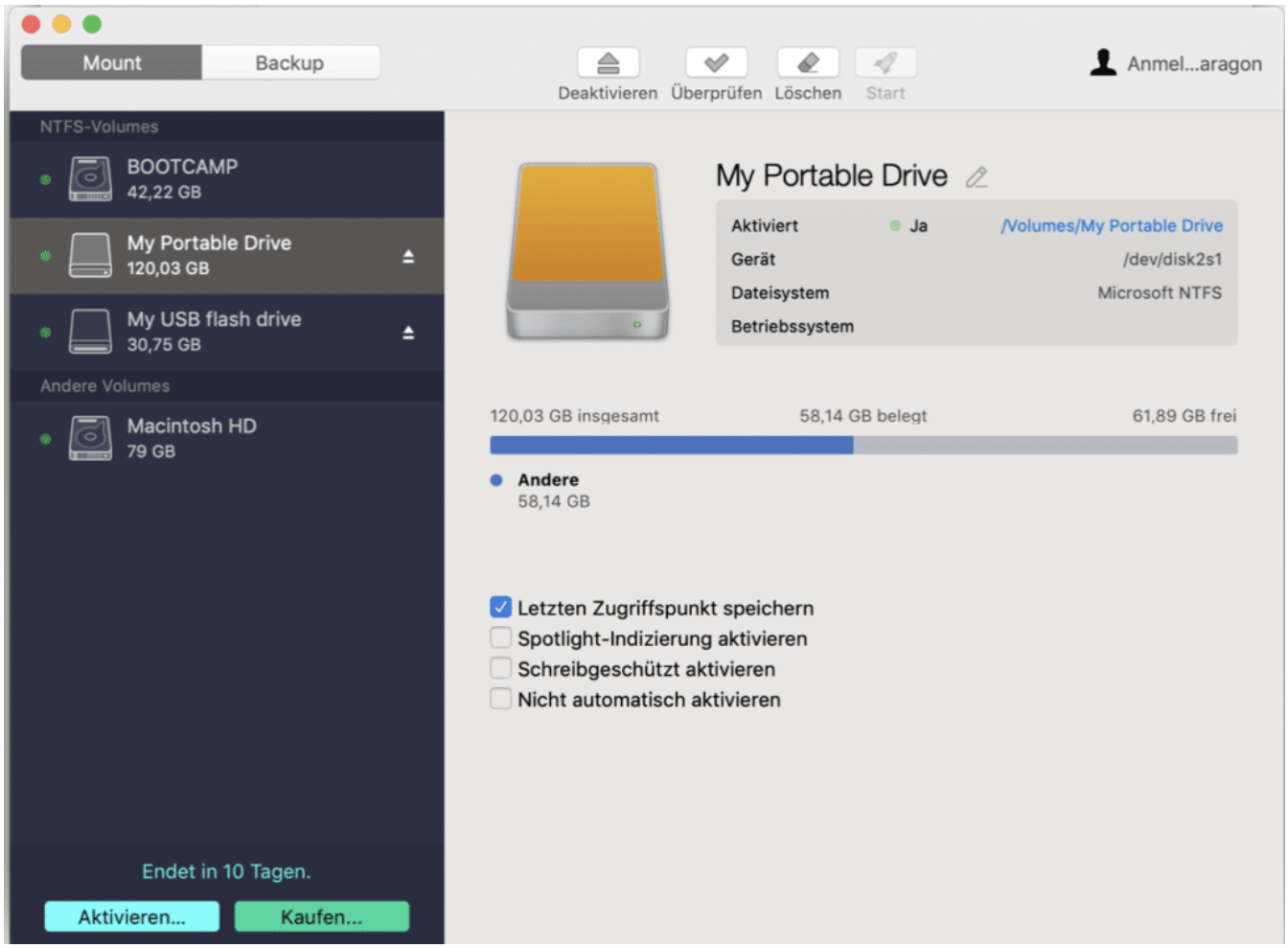
Die meisten defekte sind nicht in er Basiseinheit eines Notebooks oder Tablets, sondern im Netzteil. Intuitiv wickeln viele Anwender die Kabel so eng wie möglich um sdas Netzteil. Das bringt keine zusätzliche Sicherheit, belastet aber Kabel, Lötstellen und Stecker. Das provoziert schnell einen Kabelbruch, der dann zu Funktionsstörungen führt.

NTFS-Festplatten am Mac beschreiben

Die Welten von Apples macOS und Microsofts Windows sind über die Jahre immer weiter zusammengerückt. Nicht wenige Anwender benutzen beide Systeme parallel. Ob nun für unterschiedliche Anwendungen oder einfach nur so: Viele Arbeiten können Sie nahtlos zwischen den beiden Systemen austauschen. Wäre da nicht die Verwirrung der Laufwerksformate: Besonders NTFS, das unter Windows vor allem wegen der möglichen großen Dateien, macht auf Macs Probleme. Die sind aber schnell gelöst.

NTFS-Laufwerke sind unter Windows weit verbreitet, weil das Format im Gegensatz zu FAT nahezu beliebig große Dateien verwalten kann. Wenn Sie beispielsweise eine Festplatte mit Videos haben, dann ist die Wahrscheinlichkeit hoch, dass diese auf NTFS formatiert ist. Lesen können Sie diese dann auf einem Mac, aber leider nicht beschreiben. Und damit auch keine Dateien löschen oder umbenennen, geschweige denn neue hinzufügen.

Die Lösung kommt von Paragon, die mit NTFS for Mac eine Software entwickelt haben, die den Vollzugriff auf NTFS-Laufwerke erlaubt. Sie installiert sich als Systemerweiterung und ist weitestgehend unsichtbar für den Anwender. Schließen Sie eine NTFS-Festplatte, SSD oder einen USB-Stick an den Mac an, dann ist der Lese- und Schreibzugriff ohne weitere Handgriffe möglich.



Nebenbei erlaubt das Programm auch noch, die Festplatte Ihres Macs auf eine externe Festplatte zu sichern, ohne dabei Time Machine oder andere macOS-Mechanismen zu nutzen.

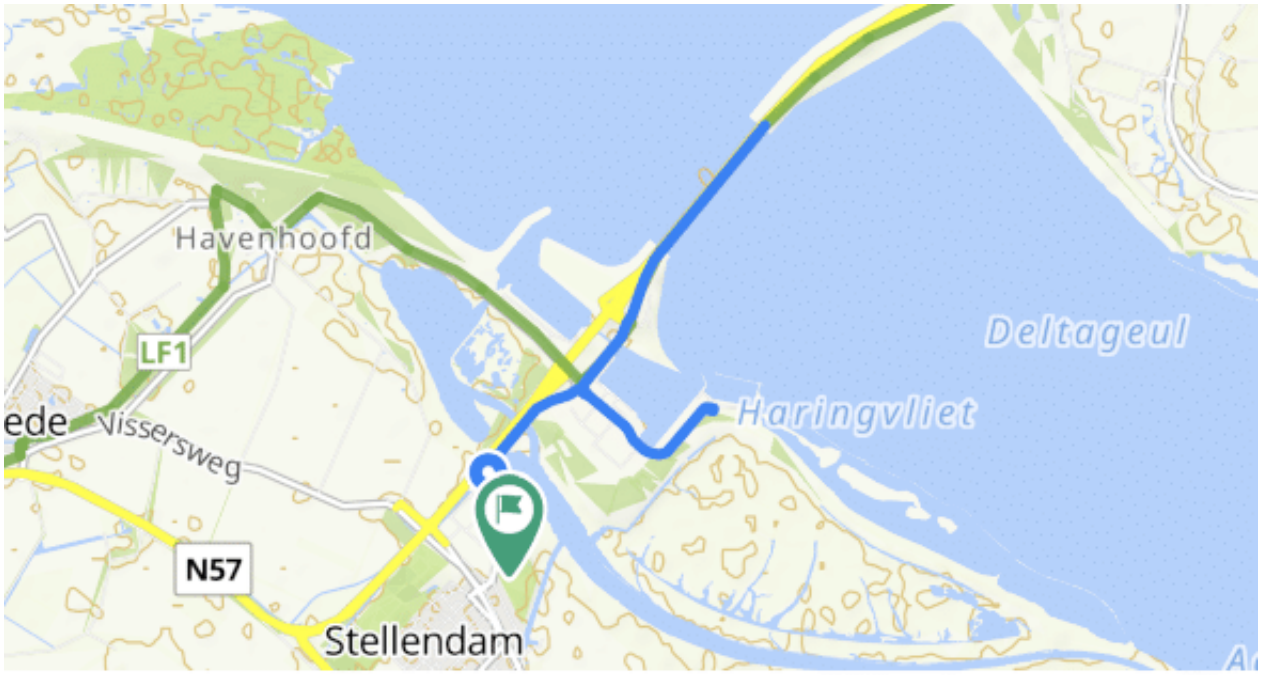
Testen können Sie NTFS for Mac kostenlos für 10 Tage, danach muss eine Version erworben werden.

Fahrradtouren auf iOS und Android: BikeMap

Der Sommer ist da, und damit die Zeit der Fahrradtouren. Wo für die Navigation mit dem Auto eine Vielzahl von Apps existieren, ist der Markt der Fahradnavis überschaubar. Nun ist die Wahl der Strecken immer abhängig vom Fortbewegungsmittel: Mit dem Fahrrad wollen Sie möglichst verkehrsarme und schöne Straßen in Anspruch nehmen. Eine tolle App ist das in der einfachen Version kostenlose BikeMap, das für Android und iOS im jeweiligen Store verfügbar ist.

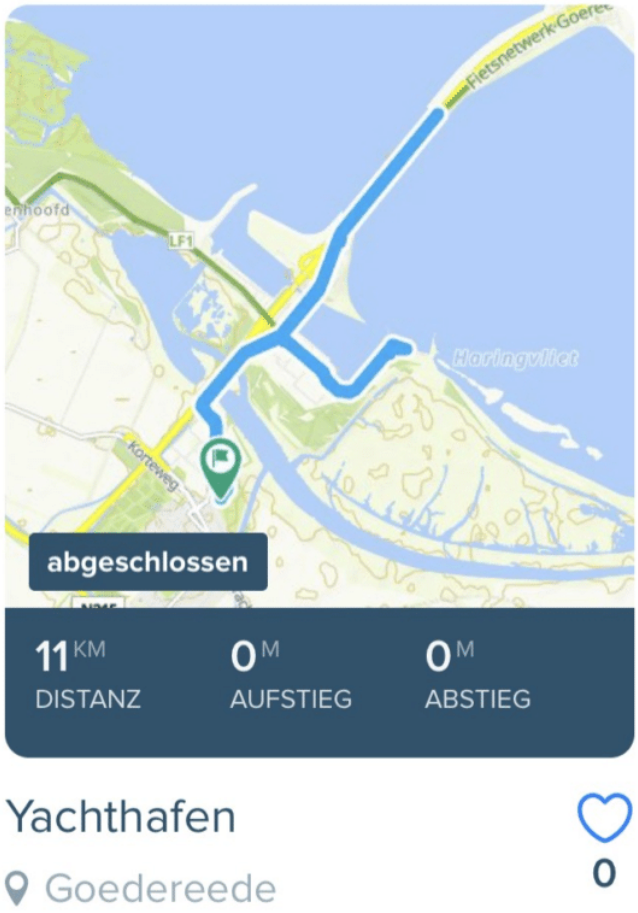
Aktuell funktioniert BikeMap am besten in der Kombination der App auf dem Smartphone und der Webseite von BikeMap. Nachdem Sie einmal ein kostenfreies Konto angelegt haben, können Sie alle Routen, die Sie aufgezeichnet haben, auf der Webseite verwalten. Das Löschen beispielsweise geht nur auf der Seite, nicht aber in der App.

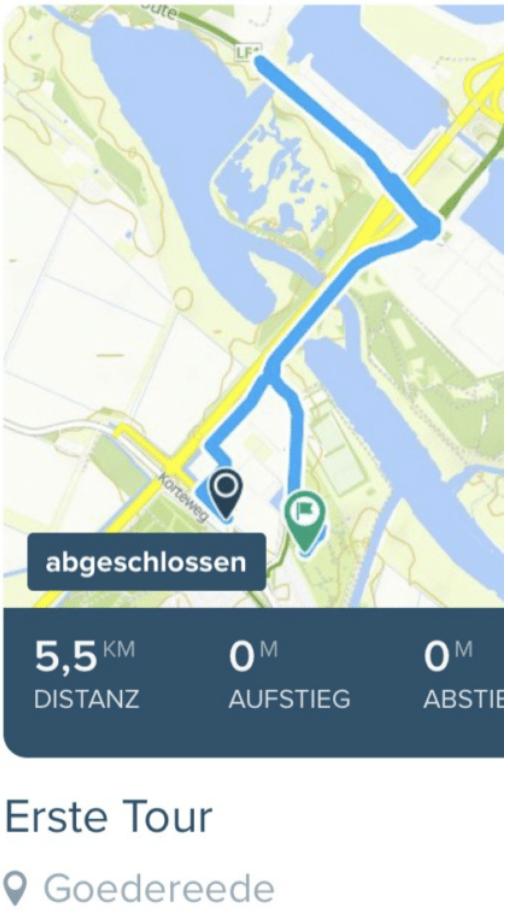
Geben Sie ein Ziel auf dem Smartphone ein. Dann können Sie entscheiden, ob die Karte heruntergeladen werden oder online navigiert werden soll. Ersteres hat den Vorteil, dass Sie damit Datenvolumen unterwegs sparen. Zum Beispiel, wenn Sie die Tour in der Reichweite eines WLANs planen!



Während der Navigation (und auch während des freien Fahrens) können Sie die Route aufzeichnen lassen. Später können Sie dann noch einmal ansehen, wo Sie hergefahren sind. Wenn Sie mögen, dann können Sie die Route auch als Navigationsziel verwenden und mit Sprachanweisungen nachfahren.

Über die Webseite können Sie weitere Routen beziehen, die andere Biker als schön klassifiziert haben, und Ihre eigenen Routen für andere zur Verfügung stellen.



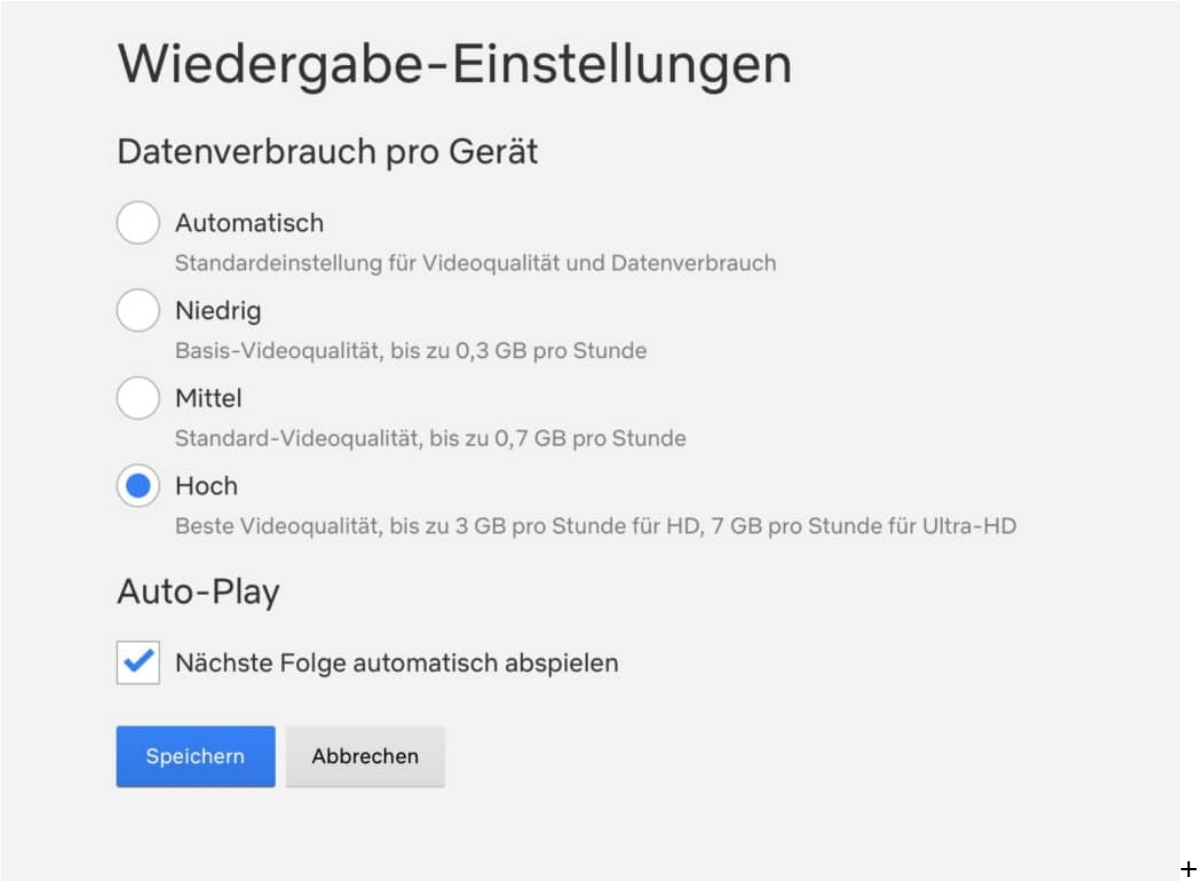


Wiedergabequalität und Datenverbrauch von Netflix einstellen

Netflix ist einer der beliebtesten Streaming-Dienste für Filme und Serien. Nicht nur auf Smart TVs oder Konsolen, sondern auch auf mobilen Geräten wie Tablets und Smartphones. Geräten also, die unterwegs genutzt werden und so das Streamen über den Datentarif des Telefons durchführen. Das kostet schnell das Inklusivvolumen. Wussten Sie, dass Sie die volle Kontrolle darüber haben?

Im Idealfall bietet Ihnen Ihr Netzbetreiber einen Streaming-Pass (wie StreamOn der Telekom oder der Gigapass von vodafone) an. Damit können Sie bestimmte Musik- und Videodienste nutzen, ohne dass der verursachte Datenverbrauch vom Inklusivvolumen abgezogen wird.

Bei Netflix haben Sie noch eine andere Möglichkeit: Sie können die Qualität der Übertragung manuell festlegen, statt die Standardeinstellung Automatisch zu verwenden. Bei dieser gibt Netflix im Web wie auch in den Apps das Video immer mit der höchsten Qualität wieder, die ihr Abo und die Datenverbindung zulassen. Bis zu 7GB pro Stunde im UltraHD-Modus.



Melden Sie sich auf der Netflix-Seite an und Klicken Sie auf Ihr Profilbild, dann auf **Konto**. Ganz unten auf der Seite klicken Sie dann auf **Wiedergabe-Einstellungen**. Hier können Sie nun den Datenverbrauch für Ihre Geräte auswählen.

Je geringer die Qualität ist, desto weniger Daten werden verbraucht und um so weniger wird das mobile Datenvolumen belastet. Allerdings sollten Sie die Einstellung wieder zurücknehmen, wenn Sie zuhause schauen: Auf einem UHD-Fernseher in Niedriger Qualität zu schauen, macht wenig Spaß!

Google Camera beim OnePlus 7 Pro und anderen installieren

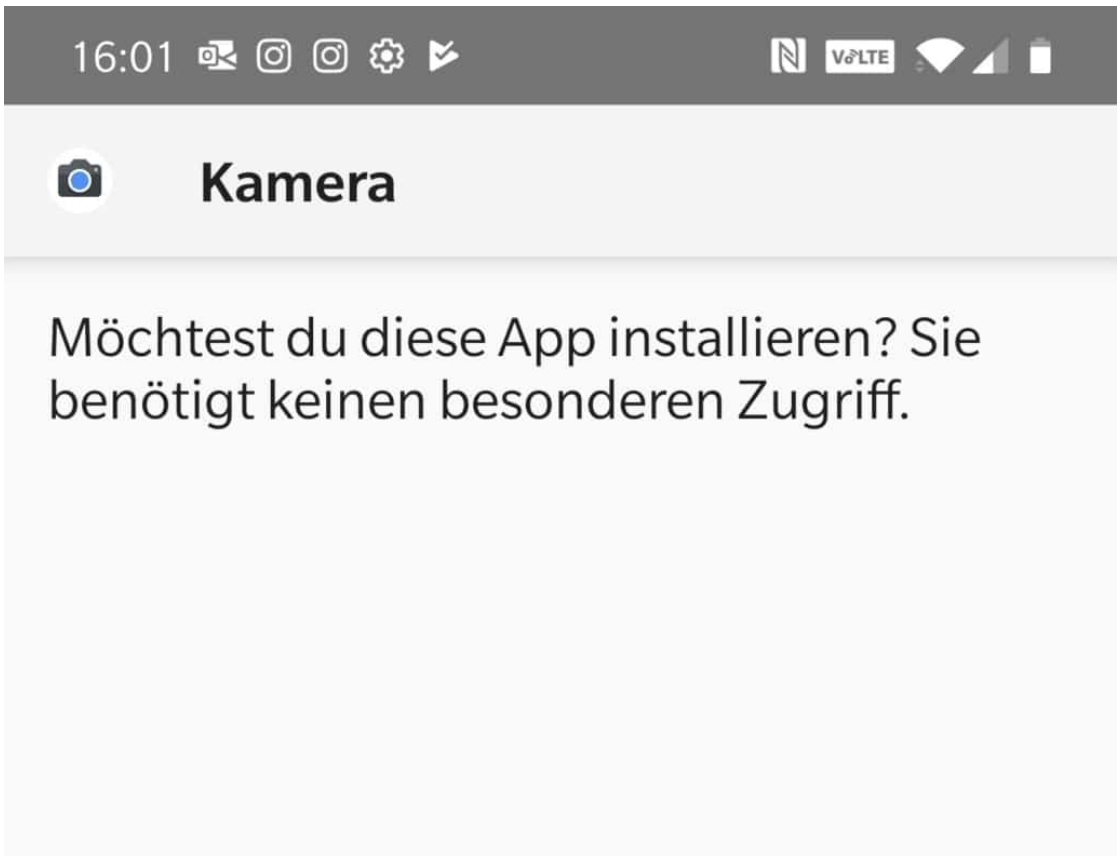
Das OnePlus 7 Pro ist eines der von den Kritikern am meisten gelobten neuen Smartphones. Nachdem das Gerät das erste große Firmware-Update bekommen hat, liegt es im DxO Kameratest nur ganz knapp hinter einem der Platzhirschen, dem Huawei P30 Pro. Allerdings bemängeln viele Anwender, dass die Kamerasoftware deutlich schlechtere Bilder produziert, als es nötig wäre. Referenz ist hier die Google Camera-App, wie sie beispielsweise das Pixel verwendet. Installieren Sie die doch einfach!

Natürlich gekommen Sie die App nicht frei im PlayStore, aber dafür gibt es ja die Community. Hier finden Sie die immer aktuelle Version der angepassten GCam-App von Arnova8G2. Laden Sie die App und die Config-Datei herunter.

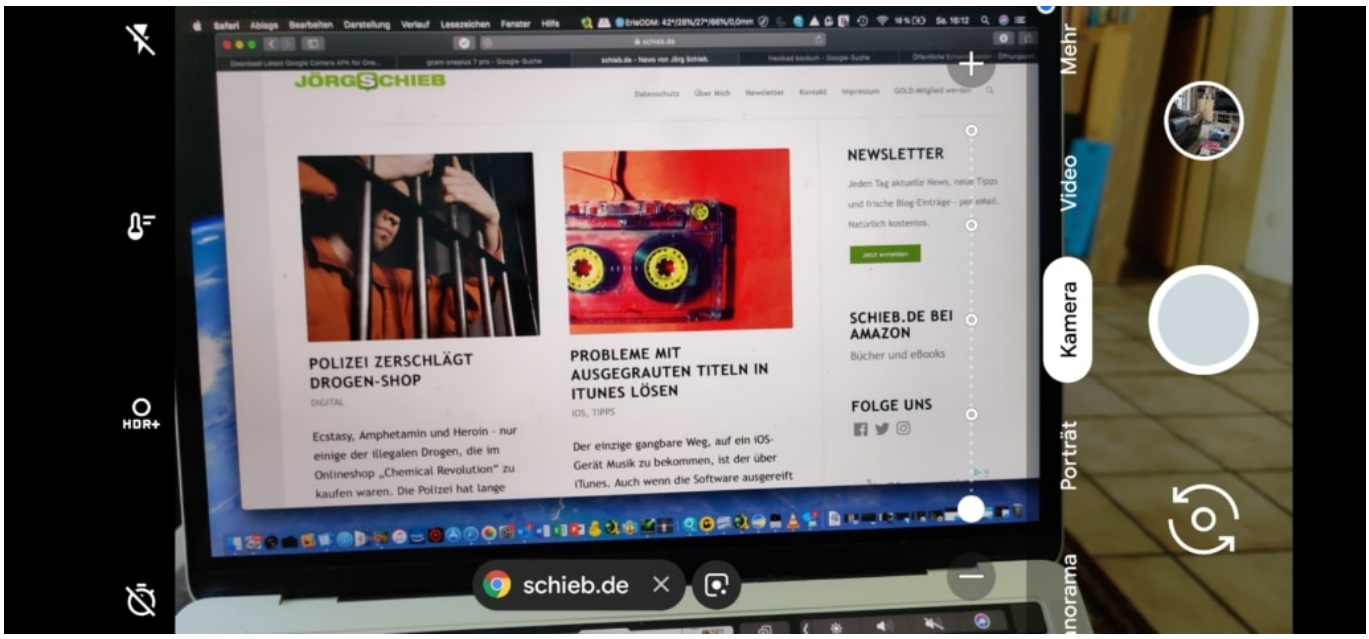
Schließen Sie dann Ihr Smartphone an den PC oder Mac an und legen Sie im internen Speicher einen Ordner **GCam** an. Dort Kopieren Sie die APK-Datei hinein. Legen Sie dann einen Order Configs in diesem Verzeichnis an, und kopieren Sie die Config-Datei hinein.

Starten Sie nun eine Explorer-App auf dem Smartphone (OnePlus liefert gleich eine im OnePlus-

App-Ordner mit) und starten Sie die GCam-App. Die Sicherheitsnachfrage können Sie ruhig bestätigen.



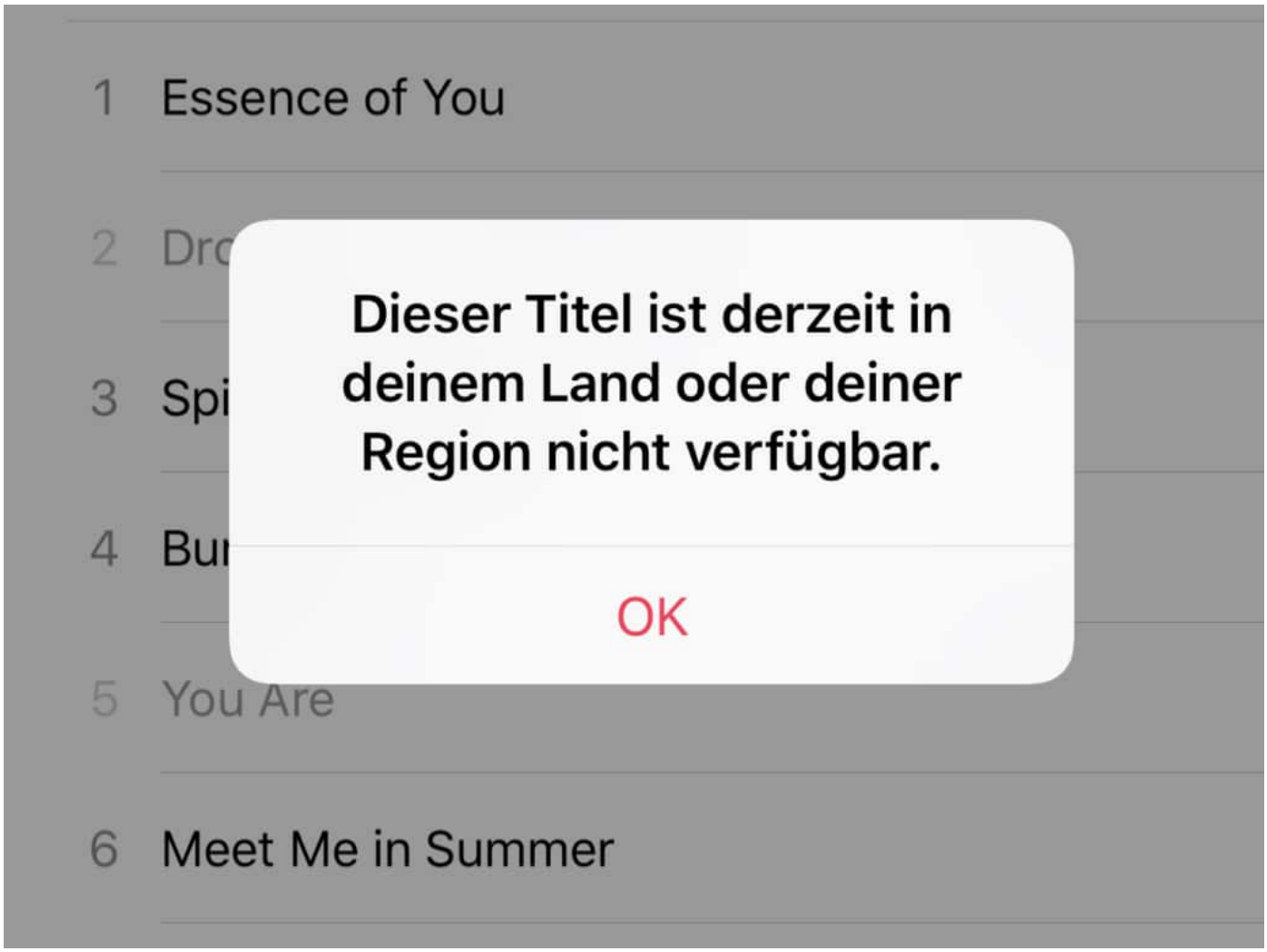
Danach haben Sie ein zusätzliches Kamera-Symbol im App Drawer und können damit die Google Camera App starten. Vergleichen Sie einfach die Ergebnisse dieser App mit der der im Standard installierten Kamera-App und freuen Sie sich über die Unterschiede.



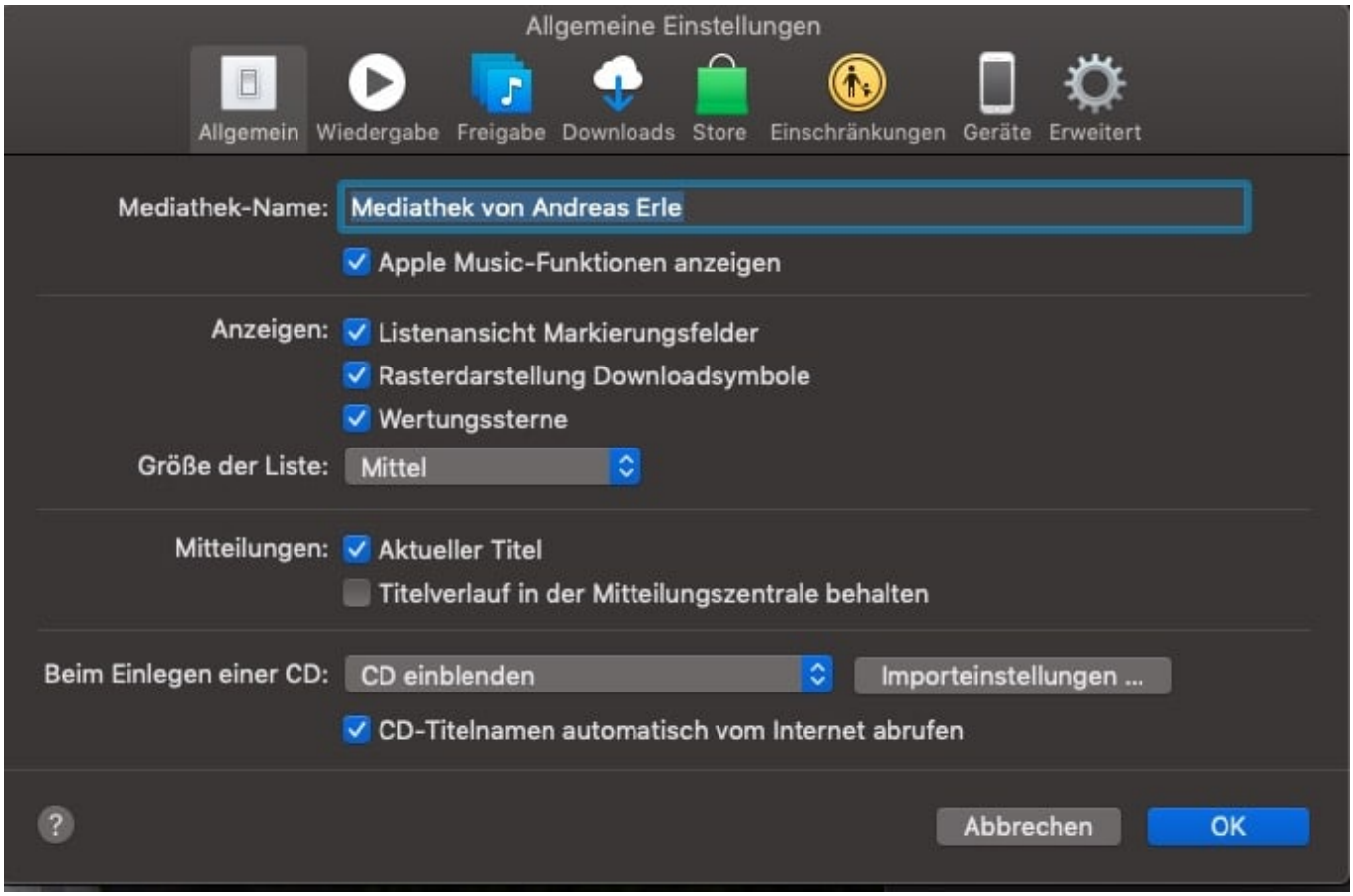
Probleme mit ausgegrauten Titeln in iTunes lösen

Der einzige gangbare Weg, auf ein iOS-Gerät Musik zu bekommen, ist der über iTunes. Auch wenn die Software ausgereift ist und von Apple selbst kommt, hat sie manchmal so ihre Tücken. Eine davon ist die Fehlermeldung "Dieser Titel ist derzeit in deinem Land oder Deiner Region nicht verfügbar." Die betroffenen Titel sind ausgegraut und nicht abspielbar. Ärgerlich, aber nicht unlösbar!

Wenn es sich hier um gekaufte Musik aus dem iTunes Store handelt, dann kann es tatsächlich sein, dass das Album/Stück nicht mehr verfügbar ist, weil es aus dem Store entfernt wurde oder mit einer Apple ID gekauft wurde, die in einem anderen Land als dem aktuell eingestellten registriert ist. Das hat natürlich keine Wirkung, wenn Sie die Musik von einer CD gerippt und dann in iTunes importiert haben.



Oft allerdings ist die Ursache einfach: Die Stücke wurden nicht vollständig synchronisiert. Entweder, weil das iPhone/iPad zu früh vom PC oder Mac getrennt wurde, oder, weil die Quelldateien während des Imports in iTunes gelöscht oder verschoben wurden.



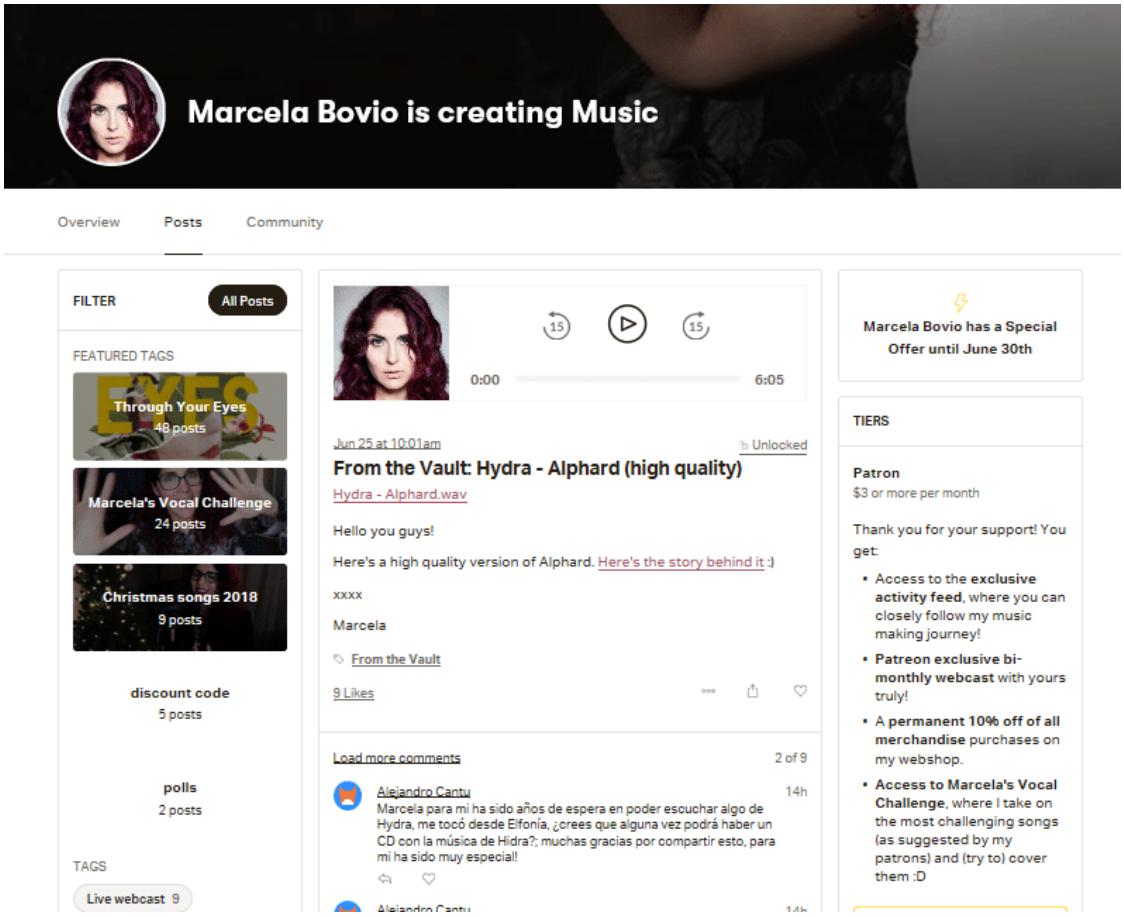
1. Synchronisieren Sie das betroffene Geräte einfach einmal neu und achten Sie darauf, dass die Synchronisation ohne Fehler zu Ende läuft.
2. Hilft das nicht, dann löschen Sie die Musik aus iTunes und fügen Sie sie über die MP3-Dateien erneut hinzu und führen die Synchronisation dann erneut durch.

Crowdfunding mal anders: Patreon

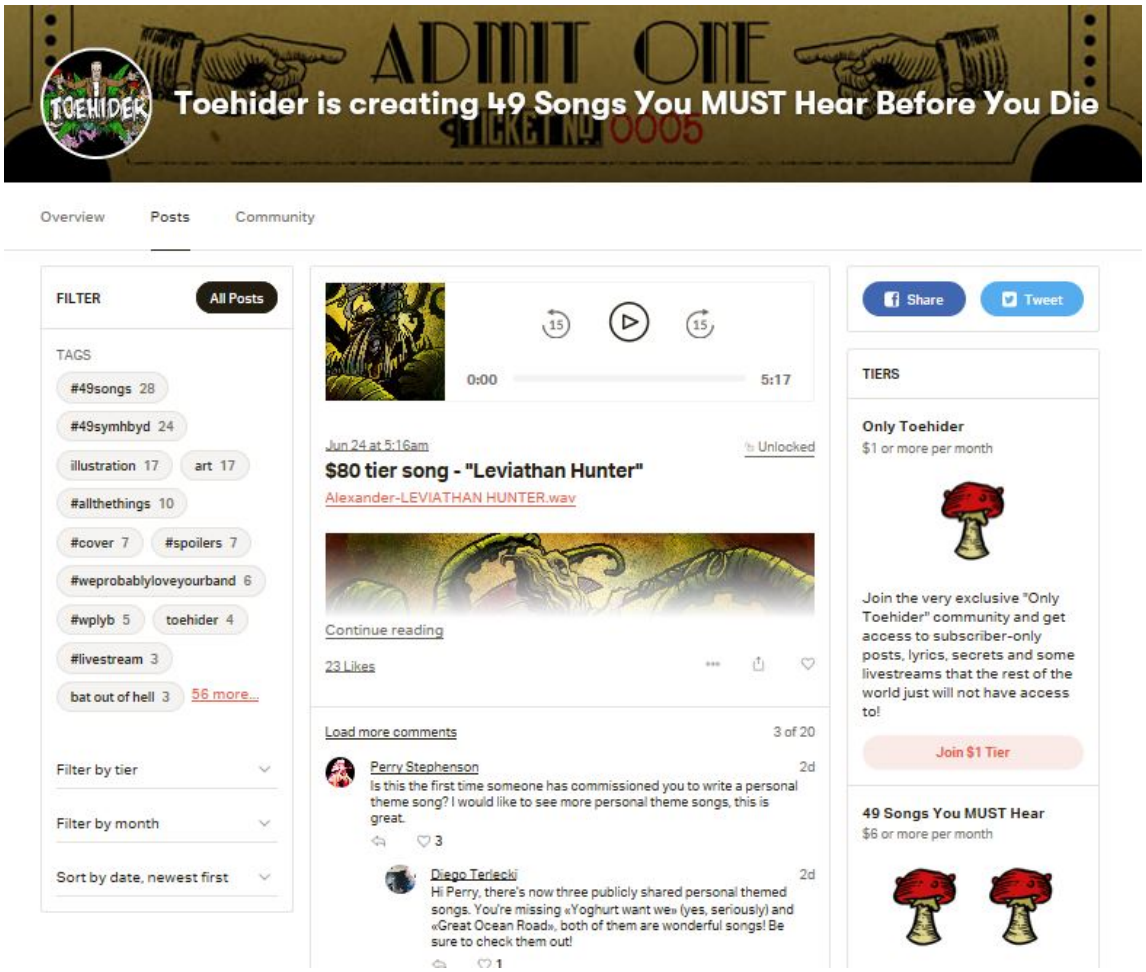
Die Musikindustrie ist schwieriges Terrain: Als unbekannter Künstler sind die Chancen sehr überschaubar, Aufmerksamkeit zu bekommen. Auch etablierte Künstler kämpfen in Zeiten des Streamings um Aufmerksamkeit und zahlendes Publikum. In Zeiten sinkender Umsätze sind die Plattenlabels zudem wenig investitionsfreudig. Viele vielversprechende Alben lassen sich so gar nicht erst realisieren. Einmal mehr ist die Lösung die Vorfinanzierung durch die potentiellen Hörer. Patreon ist das Gegenstück zu Kickstarter für Musik und auf jeden Fall einen Klick wert!

Im Gegensatz zu den klassischen Crowdfunding-Portalen wie Kickstarter und Indiegogo ist das Risiko deutlich geringer: Das Produkt ist nicht abhängig von Fertigungsstraßen in Fernost und von technischen Innovationen, die sich noch beweisen müssen. Natürlich kann es immer passieren, dass eine Band sich trennt und ein Album nicht produziert wird. Das ist aber eher selten.

Der Name der Seite kommt vom im Mittelalter gebräuchlichen Begriff der Patronage, also die gezielte und regelmäßige Förderung von Künstlern. Die kann auf verschiedene Weisen umgesetzt werden. Die klassische Förderung eines Albums, wie die mexikanisch-niederländische Sängerin Marcela Bovio es beispielsweise gemacht hat. Je nach Förderbetrag gibt es "nur" einen Download des Albums, die CD, ein Paket mit T-Shirt bis hin zu persönlichen Skype-Sessions und persönlichem Song. Und nach dem Album ist vor dem Album...



Andere Interpreten wie der australische Multiinstrumentalist Mike "Toehider" Mills schaffen sich eine finanzielle Grundlage, weiterhin Musik als Vollzeitjob machen zu können. Dafür gibt es Live-Streams, Cover-Versionen, komplett neue Lieder, Q&A-Sessions und dann und wann eine physische CD.



Zusammengefasst: Durch die direkte Unterstützung von Künstlern können Sie ganz nah am Schaffensprozess von Musik teilnehmen.