Nov. | Dez.

tarnkappe MAGAZIN 05

Liebe Leserinnen und Leser,
ein frohes neues Jahr wünsche ich Euch beziehungsweise Ihnen, denn 2018 fängt ja mal so richtig „gut“ an. Vorsicht Ironie!

Den Nutzern sozialer Netzwerke fällt seit dem Jahreswechsel das Netzwerkdurchsetzungsgesetz von Heiko Maas so richtig auf die Füße. Und für den Justizminister könnte sich die Vorschrift in Anbetracht des lautstarken Protests zu einem waschechten Bumerang entwickeln. Dazu kommt: Mehrere rechtspopulistische Politiker loten derzeit mit Erfolg ihre Möglichkeiten aus, wie sie das NetzDG zum eigenen Vorteil missbrauchen können. Und auf der anderen Seite werden immer mehr Rufe von betroffenen Nutzern laut, deren Texte oder sogar Accounts ohne erkennbaren Grund gesperrt wurde. Für Facebook und Twitter ist es schlichtweg einfacher zu löschen und zu sperren, statt längere Zeit in eine intensive Prüfung der Inhalte zu stecken. Wir erinnern uns. Wer von den Betreibergesellschaften nicht pariert, muss von Seiten der deutschen Behörden mit empfindlichen Konsequenzen rechnen. Das Nachsehen hat die Netzgemeinde, also wir. Schon wurde von Merkels Sprecher bekannt gegeben, man werde das NetzDG einer genauen Prüfung unterziehen und will künftig für mehr Transparenz sorgen. Wie das im Detail geschehen soll, hat Regierungssprecher Steffen Seibert natürlich nicht bekannt gegeben. Wahrscheinlich weiß die Bundesregierung selbst noch gar nicht, wie sie mit dem Thema umgehen soll. Hauptsache es gibt erstmal eine Erklärung, die die aufgeheizten Gemüter beruhigt. Eine allgemeine Beruhigung würde sich auch Chiphersteller Intel wünschen, denn manche deren Manager haben sich vor Bekanntgabe der Lücke in ihren Chips in auffällig großer Zahl von ihren Aktien getrennt. \\ Sicherheitslücke: Supergau bei Prozessorherstellern

Lieber erstmal alles verkaufen, bevor der Kurs so richtig in den Keller fällt, lautete die Devise. Das Schlimme daran: Betroffen von der Lücke ist so gut wie jeder, auch die Besitzer von Smartphones. Noch warten wir auf finale Patches, zumal die Chiphersteller längst hätten reagieren können, wussten sie schon seit mehreren Monaten Bescheid. Das Dumme ist nur: Egal wie man es dreht oder wendet, die Geräte werden durch den Bugfix langsamer. Das ist ja genau das, was eigentlich niemand will. Und die NSA gab unlängst bekannt, sie hätten von dieser kritischen Sicherheitslücke vorab nichts gewusst. Das kann man glauben, aber das sollte man besser nicht. Wenn überhaupt jemand zeitnah über jegliche Lücken in Hard- oder Software informiert ist, dann der gigantisch anmutende militärische Geheimdienst NSA, dem wir in unserem Magazin ja auch schon ein eigenes Special gewidmet haben. https://tarnkappe.info/die-geschichte-der-nsa-keine-kontrolle-keine-konsequenzen/

Man sieht, der Kreis schließt sich. Eigentlich ist alles so wie immer. Oder besser gesagt: so schlimm wie eh und je. Was sich ändert, ist die Tatsache, dass wir zunehmend von moderner Technik umgeben werden. Diese soll unser Leben eigentlich bequemer und sicherer gestalten, aber de facto bringt sie uns auch zunehmend in Gefahr. Tatsächlich will Intel zunächst nur die Prozessoren der letzten fünf Jahre mit Patches versorgen. Was mit den älteren Prozessoren geschieht, ist noch unklar. Wie dem auch sei. Wir werden uns so oder so noch einige Tage gedulden müssen. Die endgültigen Patches werden irgendwann im Januar zu erwarten sein, hieß es. Wir bleiben bei dem Thema auf jeden Fall am Ball.

Wer sich über solche und ähnliche Themen austauschen möchte, sei hiermit erneut dazu eingeladen, unsere öffentliche Gruppe bei Telegram zu besuchen. https://t.me/tarnkappe_info/ Derzeit sind 345 Teilnehmer am Chat beteiligt. Die Redaktion ist natürlich nicht 24 Stunden pro Tag verfügbar, aber irgendwer wird sich gerne Euren bzw. Ihren offenen Fragen annehmen, sollten welche bestehen. Der Ton ist stets sehr freundlich und die Personen sind sehr hilfsbereit. Dumme Fragen gibt es nicht. Es gibt nur Menschen, die sich nicht trauen, ihre Fragen zu stellen. Doch auch das kriegen wir noch hin, versprochen.

Gruß aus der Provinz!

Das Team von Tarnkappe.info

SZENE

WUPPERTALER POLIZEI STOPPT HANDEL MIT RAUSCHMITTELN 9

DDL-WAREZ IM GESPRÄCH 9

USENET-BUSTS 14

STAY-DOWN-REGEL PROBLEMATISCH FÜR UPLOADED.NET 15

E-BOOK-PIRATERIE IM DEUTSCH- UND ENGLISCHSPRACHIGEN RAUM 16

E-BOOK-QUARTALSBERICHT 17

USENET-RAZZIEN 17

ERMITTLERN GELINGT SCHLAG GEGEN ANDROMEDA-BOTNETZ 19

EIN UPLOADER IM GESPRÄCH 20

Titelstory

Themenübersicht

Anonym

Themenübersicht

„NOW YOU KNOW. VIER JAHRE SNOWDEN“ 31

KINOX.TO: BETRÜGER VERSCHICKEN FAKE-ABMAHNUNGEN 31

GESICHTSERKENNUNG AM BAHNHOF SÜDKREUZ 32

THOMAS DE MAIZIÈRE: GESETZESÄNDERUNG FÜR LAUSCHANGRIFFE 33

AUSTRALIEN PLANT VERKAUF BIOMETRISCHER DATEN 34

TELEGRAM SPERRT PIRATEN-KANAL 35

SESSION-REPLAY 35

LAW

Themenübersicht

OBERSTER GERICHTSHOF BESTÄTIGT NETZSPERREN ZU TORRENT-LINKS 37

INTERNETPROVIDER ZUR SPEICHERUNG VON IP-ADRESSEN VERPFLICHTET 38

BEKLAGTE HAFTEN BEI ILLEGALEM FILESHARING 38

METADATEN-SPEICHERUNG FÜR BND KÜNFTIG TABU 39

BUNDESVERFASSUNGSGERICHT VERBIETET ÜBERZOGENE TELEFONGEBÜHREN 40

KEIN AUSSPIONIEREN VON FAMILIENMITGLIEDERN GEFORDERT 41

PAUSCHALE TÄTERSCHAFTSVERMUTUNG GENÜGT NICHT 41

Digital

Themenübersicht

DENUVO: NEUER KOPIERSCHUTZ NOCH UNGEKNACKT 42

SONY PS4: KERNEL GEKNACKT, JAILBREAK STEHT BEVOR 43

Security

Themenübersicht

SNOWDEN ENTWICKELT SICHERHEITS-APP FÜR ANDROID 44

HACKERGRUPPE ERBEUTET 10 MILLIONEN US-DOLLAR VON BANKEN 44

TASTATUR-APP STELLT DATEN VON 31 MILLIONEN NUTZERN INS NETZ 45

RUSSLAND STARTET AB AUGUST 2018 EIGENES DNS 46

WARNUNG VOR GEHACKTEN WEBSEITEN MITTELS BREACH ALERTS 47

WIE GOOGLE ANDROID-NUTZER TÄUSCHT UND AUSSPIONIERT 48

US-MILITÄR: WELTWEITE ÜBERWACHUNG SOZIALER NETZWERKE 49

BUNDESNETZAGENTUR UNTERSAGT DEN VERKAUF VON KINDERUHREN 49

TELEGRAM-GRUPPE DER TARNKAPPE BALD MIT 200 TEILNEHMERN 50

Darknet-Drogenhandel: Wuppertaler Polizei stoppt Handel mit Rauschmitteln in Millionenhöhe

Nach umfangreichen Ermittlungen gelang Staatsanwaltschaft und Polizei in Zusammenarbeit mit dem LKA NRW, dem Zoll und dem Sicherheitsdienst der Post in Wuppertal ein Schlag gegen die Drogenkriminalität. So soll ein 29-Jähriger Niederländer von Wuppertal aus weltweit Drogen verschickt haben. Die gelagerte Ware im Wert von drei Millionen Euro verkaufte er, den Ermittlern zufolge, im Darknet.

Polizei und Staatsanwaltschaft berichteten, dass sie bei einer Razzia am 13. November 2017 die Wohnungstüre des Verdächtigten eingetreten und ihn festgenommen hätte. Dem Niederländer wird vorgeworfen, von Wuppertal aus einen weltweiten Drogenhandel betrieben zu haben. Bei diesem Einsatz sind 200 Kilogramm Drogen im Wert von drei Millionen Euro beschlagnahmt worden. Der mutmaßliche Großdealer hatte eine breite Palette im Angebot, man fand sowohl Ecstasy, Cannabis-Schokotafeln, aber auch Kokain und Amphetamine. Zudem habe die Polizei Datenträger und Computer beschlagnahmt.

Den Verkauf der Rauschmittel habe der Mann in großem Stil über das Darknet abgewickelt, versandt hat er die Ware per Post unter Benutzung eines ganz gewöhnlichen Briefkastens. Abnehmer hatte er in aller Welt, die Drogenpakete gingen nach Thailand, in die USA und nach Australien, sowie flächendeckend nach Europa.

Vermutlich waren Frau und Kind des Mannes völlig ahnungslos. Sie wurden von der Razzia absolut überrascht. Für den Drogenvertrieb hatte der Mann noch eine zusätzliche, zweite Wohnung in Wuppertal angemietet. Nun hat ein Richter gegen ihn Untersuchungshaft angeordnet. Ihm droht eine Haftstrafe von bis zu 15 Jahren. Im Rahmen der Durchsuchungen konnten auch zahlreiche Daten der Käufer sichergestellt werden. Sie müssen nun ebenfalls mit Strafen rechnen. Die derzeitigen Ermittlungen, sowohl zur Herkunft der Drogen, als auch zu etwaigen Mittätern, dauern noch an.

Marc-Andre Opdam, Leiter der Ermittlungskommission würdigte den Erfolg mit den Worten: „Dieser Erfolg konnte nur durch die gute Zusammenarbeit mit dem LKA NRW, der Deutschen Post und den einzelnen Dienststellen der Polizei erreicht werden. Durch diese enge Zusammenarbeit gelingt es der Polizei immer mehr, die Besteller aus ihrer Anonymität zu holen“. „Das Darknet ist nicht sicher“, betonte auch Oberstaatsanwalt Wolf-Tilman Baumert, der die Ermittlungen als „Beispiel hervorragender Kriminalarbeit“ bezeichnete.

DDL-Warez im Gespräch

DDL-Warez ist einer der ältesten und bekanntesten Vertreter, wenn es darum geht, online illegale Downloads unter Zuhilfenahme von Sharehostern durchzuführen. Letzten Monat generierte die Seite nicht weniger als 41 Millionen Seitenzugriffe. Wahnsinn! Legal ist der Betrieb freilich nicht. Aufgrund der Popularität dürfe es zahlreiche Rechteinhaber ärgern, dass sie in den vergangenen 13 Jahren nichts dagegen ausrichten konnten.

Traditionell ist auf den Webwarez-Seiten im Herbst und Winter mehr los, als im Sommer. Wenn es, wie jetzt, draußen kalt und regnerisch ist, ziehen viele Anwender ihr heimisches Zuhause dem ungemütlichen Wetter vor. Natürlich ist auch DDL-Warez diesen Schwankungen unterworfen, ihre Zugriffszahlen sind dennoch gigantisch. Monatlich fast 7.5 Millionen Visits,

bei denen im Oktober 2017 durchschnittlich mehr als fünfeinhalb Seiten aufgerufen wurden (macht in der Summe 41,15 Mio. Seitenzugriffe), plus ein Besucher-Aufenthalt von mehr als fünf Minuten: Solche Zahlen würden gerne legale Anbieter, wie Online-Shops oder Streaming-Seiten vorweisen, viele tun es aber nicht. Auch solche nicht, die es wie DDL-Warez seit dem Jahr 2004 gibt. Wir machen im Rahmen des Gesprächs einen gemeinsamen Schwenk von der bewegten Vergangenheit der Seite, kommen zur Gegenwart und lassen die anonymen Betreiber abschließend einen Blick in die Zukunft werfen.

Vergangenes

DDL-Warez hatte immer wieder mit Hackerangriffen zu kämpfen. Im November 2015 hieß es dort, dass die Seite von Dritten mittels eines eingeschleusten Trojaners übernommen wurde. Was ist da im Detail passiert? Wem gehört die Seite denn nun? Den alten oder irgendwelchen neuen Besitzern? Und was ist mit DDL-Music?

DDL-Warez wird seit zwei Jahren wieder von den ursprünglichen Betreibern weitergeführt. Die haben das Projekt zu Rapidshare-Zeiten geleitet und mussten es dann aus Gründen verlassen, die hier nicht öffentlich genannt werden können. Ich bitte da um Verständnis. Wer damals schon dabei war, weiß die Hintergründe. Die 2015 abgeschaltete Seite war nie das offizielle Projekt und ist deshalb bei Null und mit neuer Domain gestartet. Letztendlich gibt es DDL-Warez (also das Original) schon seit 2004 und DDL-Music ist ein paar Jahre später dazugekommen.

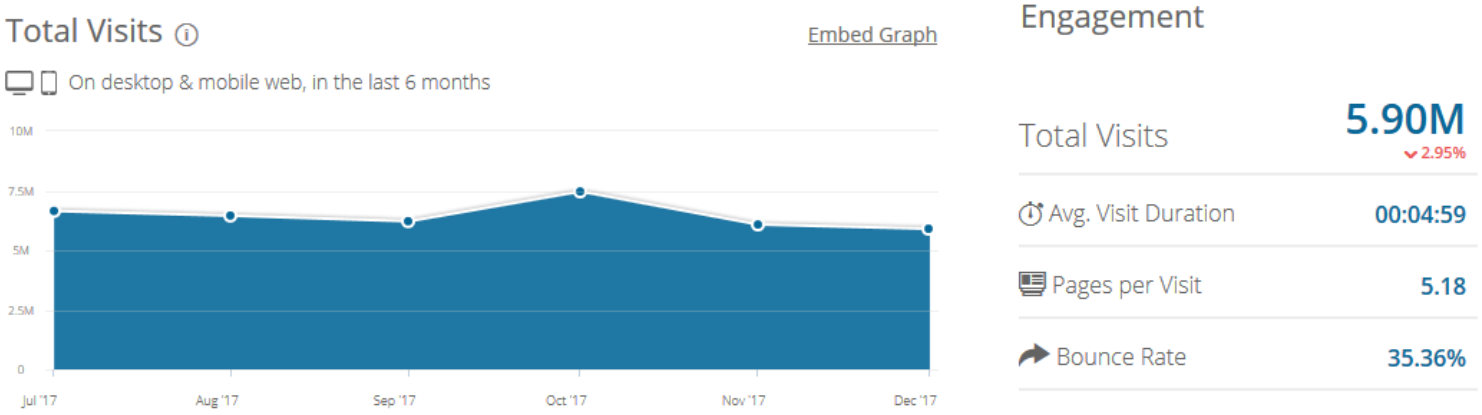
Wurdet ihr damals von besagten Seitenbetreibern erpresst oder warum kam die Story mit dem Hack, den viele bis heute nicht glauben?

Nein, es gab keine Erpressung oder sonstiges.

Gut, keine Informationen sind auch welche. Warum wurde denn im Jahr 2010 das hauseigene Forum unter ddl-board.to geschlossen? War dies für die Community nicht gleichbedeutend wie ein Schlag ins Gesicht? Oder war der Betrieb des Boards auf Dauer einfach mit zu viel Aufwand verbunden?

Ziel ist, Community-Funktionen direkt in DDL-Warez und DDL-Music einzubauen. Deshalb gibt es seit kurzem einen Kommentarbereich oder bei DDL-Music eine Bewertungsfunktion.

Habt ihr Kontakt zum alten (ehemaligen) Betreiber von DDL-Warez? Was macht er heutzutage? Er hatte nach dem Exit des Haupt-Administrators die Seite übernommen. Wie kam es zum plötzlichen Comeback damals? Ihm wurde seinerzeit vorgeworfen, er habe zu viel Werbung geschaltet. Habt ihr euch damals mal DDL ohne Ad Block angesehen?



Nein, es besteht kein Kontakt und alle früheren Kontaktversuche haben zu nichts geführt oder wurden ignoriert. Insgesamt gibt es im Vergleich wenig Werbung und weil ein eigener Linkcrypter direkt eingebaut ist, sehen die User insgesamt auch weniger Werbung als woanders. Dort werden User zum Teil über zwei bis drei andere Seiten geleitet, die nochmal eigene Werbung anzeigen, bis der User endlich den Download starten kann.

Oder fragen wir mal anders: Wie oft haben die Admins denn im Laufe der Jahre gewechselt?

So oft wie nötig, um den Usern jetzt das beste Download-Erlebnis zu bieten. Mit dem aktuellen Team können wir für hundertprozentige Sicherheit und User-Orientiertheit garantieren.

DDL-Warez stellt keinen Verlust für Rechteinhaber dar Man sieht, ein Marketing-Studium muss Euch niemand mehr

empfehlen. Besser hätte das ein Profi auch nicht schönreden ausdrücken können. Aber mal etwas anderes: Wie hat sich die Untergrund-Szene in den letzten Jahren gewandelt? Von außen hat man immer mehr den Eindruck, es geht nur noch ums liebe Geld.

Nach dem Aus von Rapidshare hat sich alles sehr verteilt. Auch viele kleinere Seiten haben in dem umkämpften Markt aufgegeben. DDL-Warez gibt es seit 2004. Uns geht es darum, Content anzubieten, den es auch ohne DDL-Warez online geben würde. Im Endeffekt ist das kein Verlust für Rechteinhaber, auch wenn es von Lobbygruppen und Medien anders dargestellt wird. Wir empfehlen unseren Usern klar, Filme und Software zu kaufen, wenn sie ihnen gut gefällt. Viele werden z.B. durch gute Filme zu Fans und wollen die Rechteinhaber dann auch unterstützen.

Fragen zum Betrieb

Na, ob die Labelbetreiber das auch so sehen!? Ihr habt sehr viele neue Uploads täglich. Wie viele Personen sind denn direkt und indirekt am Betrieb beteiligt?

Bei ddl-warez.to und ddl-music.to sind mehrere Uploader auf eigene Verantwortung am Werk, in zweistelliger Zahl. Die Mannschaft ist insgesamt sehr zuverlässig, so können den Usern rund um die Uhr neue Downloads unter ddl-warez.to/downloads/updates/ bereitgestellt werden. Neue Uploader werden dabei immer sehr sorgfältig ausgewählt. Oft fragen Groups auch direkt über das Kontaktformular nach Zugängen (auch Scene Groups).

Gibt es im Background eine Person, die das Vorhaben aktiv unterstützt ohne selbst in Erscheinung zu treten?

Unklar, was für ein Vorhaben hier gemeint ist. Im Hintergrund arbeiten natürlich viele Leute an dem Projekt, damit rund um die Uhr zuverlässig Downloads angeboten werden können. Der große Aufwand ist für den User erstmal nicht sichtbar. Wir haben kein Interesse, Daten von Usern zu speichern.

Ich sage ja, Marketing-Fachmann. Wie sichert ihr die Webseite ab? Seid ihr genau so gut abgesichert, wie andere Seiten?

Es besteht kein Interesse oder überhaupt die Möglichkeit, Daten von Usern zu speichern oder auszuwerten. Anders als bei Börsen, muss sich niemand für Downloads registrieren. Es gibt Ersatz-Server in verschiedenen Ländern, die in kurzer Zeit aktiviert werden können. Alle Server arbeiten mit verschlüsselten Daten.

Wie viel TB haben die ganzen Server, die im Einsatz sind?

Das wissen wir nicht, DDL-Warez speichert die Dateien ja nicht selber. Es werden nur die Links auf die Sharehoster angeboten. Mit allen Mirrors sind das bestimmt 800 Terabyte, weil vieles in HD oder 4K-Qualität verfügbar ist. Auch der Serien- und XXX-Bereich ist sehr gefragt. Sie machen mittlerweile den Großteil der TB-Zahlen aus.

Könnte so eine Panne, wie es bei Serienjunkes der Fall war bei DDL-Warez genauso passieren, oder habt ihr euch da was überlegt?

Die Links werden selber gespeichert. DDL-Warez braucht deshalb keine externen Linkcrypter. Gegen Datenverlust schützen generell natürlich regelmäßige Backups.

Downloads gesammelt durchführen: der Warezkorb

Wie kam es eigentlich zu der Idee mit dem Warezkorb?

Mit dem Warezkorb wollte sich DDL-Warez einfach von anderen Seiten abheben. Man kann damit Downloads bei DDL-Warez sammeln und dann mit einem Klick in einen Downloadmanager laden – ohne Umwege über Linkcrypter oder zwischengeschaltete Seiten. Vergleichen kann man das mit dem klassischen Warenkorb bei Alibaba oder Amazon. Ein ähnlich einfaches System wollte DDL-Warez auch für Downloads anbieten. Der Fakt, dass der Warezkorb mittlerweile auch von anderen Seiten “kopiert” wird, zeigt, dass User das so wollen.

Warum gibt es im Warezkorb das Limit von maximal 20 Downloads?

Das dient dem Schutz vor Massendownloads. 20 Downloads sind ein guter Kompromiss in Bezug auf die Benutzerfreundlichkeit und für die meisten ist das mehr als genug. Zum Beispiel wenn man eine Serie komplett downloaden möchte und diese in Einzel-Downloads (Episoden) verteilt ist.

Warum werden kritische Kommentare, z.B. wenn Cracks nicht

funktionieren, nicht zugelassen?

Grundsätzlich werden alle Kommentare freigegeben, die nicht beleidigend und kein Nonsens sind. Fragen zu nicht-funktionierenden Cracks werden automatisch an den Uploader gemeldet und wenn möglich, von ihm behoben. Die Erfahrung zeigt, dass 90% der Probleme auf falsche Bedienung zurück zu führen sind. Anleitungen für Cracks gibt es normalerweise bei DDL-Warez in der Beschreibung der Downloads.

mmer mehr Warez-Seiten bieten ihre Downloads verunreinigt oder sogar virenverseucht an. Woher soll man wissen, dass gerade DDL-Warez keinen unerwünschten Ballast mitbringt? Da es in der „Szene" nur noch um Geld geht, muss man sich fragen, woran man das überhaupt erkennen kann, ob die Downloads sauber sind.

Der Zusammenhang zwischen Geld und Viren erschließt sich bei dieser Frage nicht.

Wenn ich kurz unterbrechen darf: das ist schnell erklärt. Sobald ein Cybercrimineller eine bestimmte Summe pro verseuchten Computer (Victim) bezahlt, stehen nur noch monetäre Gesichtspunkt im Vordergrund. Die übernommenen Geräte können nach erfolgter Infektion für Bot-Netze, den Versand von Spam-Mails oder andere Zwecke missbraucht werden. Doch schließe erstmal deine Ausführungen ab…

Es gibt bei DDL-Warez zuverlässige Upper, die teilweise jahrelang dabei sind und vertrauenswürdig sind. Alle Downloads werden vorher auf Viren geprüft. Dass manche Keygens (von Antiviren-Programmen) als "unerwünscht" erkannt werden, liegt in der Natur der Sache und kann leider nicht geändert werden. Wirkliche Schadprogramme sind das nicht.

„Uploaded ist hohem rechtlichen Druck ausgesetzt"

Welche Erfahrungen haben die Macher in letzter Zeit mit dem Sharehoster Uploaded.net gemacht? Auf der Hauptseite wird derzeit explizit vor dem Abschluss neuer Premium-Accounts gewarnt. Wir haben ja auch schon über die Sperrung diverser Accounts von Uploadern berichtet, weil man ihnen wiederholte Urheberrechtsverletzungen vorwirft.

Die Berichterstattung von Tarnkappe.info können wir bestätigen. Uploaded ist hohem rechtlichen Druck ausgesetzt und ist wahrscheinlich gezwungen, so zu handeln. Für DDL-Warez entspricht das aber nicht mehr unseren Anforderungen an Zuverlässigkeit. Bei DDL-Warez sind aktuell alle Downloads mindestens auf Share-Online gehostet und das ist deshalb die beste Wahl für DDL-Warez User.

Wie kam es eigentlich zur engen Kooperation mit der deutschen NFO-Site Xrel?

Es gibt keine wirkliche Kooperation. xREL ist ohne Gegenleistung verlinkt. Es ist eine gute Informationsquelle für User, die mehr darüber wissen wollen, wie Releases zustande kommen.

Krypto-Mining

Wir wollen unsere User nicht mit so etwas belästigen

Was halten die Betreiber vom CoinHive Krypto-Mining? Ist dies eine gute Ergänzung oder sogar ein Ersatz für Werbung? Oder wäre ein Pay2Leech-Angebot wie bei Scenedownloads.pw eine Alternative, um die Seite zu monetarisieren?

DDL-Warez hat kein Krypto-Mining und will seine User nicht mit so etwas belästigen. Pay2Leech gibt es nicht und ist auch für normale User keine Alternative, weil da das Risiko einer strafrechtlichen Verfolgung und die Haftungsfrage ganz andere Dimensionen hat.

Wie schafft ihr es, so viele Downloads online zu halten? Ich habe es bei euch noch nie erlebt, dass eine Datei offline war.

Details können hier natürlich nicht verraten werden. Wir können mit Stolz sagen, dass es eine mittlere sechsstellige Zahl an verfügbaren Downloads online gibt und damit mehr, als viele andere Seiten zusammen. Der Preis dafür ist ein sehr hoher Aufwand, der erstmal für den Enduser nicht sichtbar ist, aber trotzdem im Hintergrund jeden Tag viele Leute beschäftigt.

Wie prüft Ihr, ob eure Links online sind? Selbst von Hand oder durch die User?

Weder noch. Das macht ein sehr, sehr fleißiger Bot, der rund um die Uhr arbeitet. ;)

Warum gibt es bei euch keine externen Linkcrypter? Oder anders gefragt: Warum habt ihr Euch den Linkcrypter selbst programmiert?

DDL-Warez möchte sich nicht von externen Cryptern abhängig machen und seinen Usern die Möglichkeit geben, direkt via Click'n'Load und ohne Umwege ihre Downloads zu starten.

Welches CMS verwendet ihr? Das verwendete CMS scheint ja auch eine Eigenproduktion zu sein.

Das ist eine Eigenproduktion. Nur so können Features, wie der Warezkorb, der Liveticker oder eine Vorschau von Videos angeboten werden.

Wie kann ich euch unterstützen, außer einen Premium Account zu kaufen?

Ganz klar: DDL-Warez an Freunde und Bekannte weiterempfehlen! Auch etwas zur Seite beitragen durch Kommentare schreiben (Feedback) ist seit kurzem möglich.

„Viele Angriffe kommen aus Osteuropa und Asien"

Habt ihr eine Ahnung, wieso unser Kommentator aus Bulgarien die Webseite nur noch über einen Proxy besuchen kann? Auch die Besucher aus den Niederlanden kommen nicht bei euch auf die Seite.

Bestimmte Länder, von denen erfahrungsgemäß ein gewisses Risiko ausgeht, müssen ausgeschlossen werden. Zum Beispiel kommen viele Angriffe aus Osteuropa und Asien. Diese Länder sind sind auch nicht die Zielgruppe.

Was verdient ihr eigentlich monatlich an dieser Webseite? Wofür werden die Einnahmen investiert?

Genaue Zahlen sind hier schwer bezifferbar und werden in der Regel auch überschätzt. Die Werbeeinnahmen fließen zurück an DDL-Warez: in den Betrieb der Server oder die Umsetzung neuer Features. Nur so kann den Usern von DDL-Warez langfristig etwas geboten werden. Viele unterschätzen dabei die Kosten, den Aufwand und das Risiko, das hinter einem Projekt wie DDL-Warez steckt. Die Uploader bei DDL-Warez handeln selbständig und auf eigene Verantwortung, deshalb können wir auch keine Angaben zu deren Einnahmen machen. Der Aufwand ist aber auch hier sehr, sehr groß.

Warum schaltet ihr Werbung von Vavoo? Bezahlen die so gut? Oder habt ihr etwas damit zu tun?

Es gibt fast täglich Anfragen von Leuten die Werbung schalten wollen. Vavoo ist ein normaler Partner, von dem wir uns trennen, wenn irgendwie das Gefühl entsteht, dass die Abrechnungen nicht sauber stattfinden…

Hat die Polizei je bei euch wegen Kinderpornografie angefragt?

Nein, das war nie ein Thema.

Zukunftsaussichten

Außer Spesen nichts gewesen? Haben neue LinkCrypter wie ToLink.to eine Chance, dauerhaft zu überleben? Das wissen wir nicht. Mit anderen Linkcryptern hat DDL-Warez nichts zu tun. Wir wünschen Tolink trotzdem viel Erfolg.

In den letzten Tagen wurden diverse Usenet-Foren hochgenommen. Habt ihr keine Angst vor einem Bust?

Ein gewisses Risiko gibt es immer, man muss vorsorgen. Wir leben nicht in Deutschland oder der EU und sind deswegen schon sehr gut geschützt. Auch die Server sind im Ausland.

Der Druck auf die Sharehoster-Szene hat zugenommen

Hat in den letzten Jahren der Druck auf die Webwarez-Szene per

Sharehoster tatsächlich zugenommen, wie die GVU behauptet? Auf jeden Fall. Die User von DDL-Warez.to sind davon aber gut geschützt weil sie sich nicht registrieren müssen. Bei Behördenanfragen könnten gar keine Daten zur Verfügung gestellt werden, weil nichts gespeichert wird. Es gab bisher auch keine Anfragen.

DDL-Warez bisher ohne Präsenz im Darknet

Gibt es eigentlich eine alternative Domain oder .onion-Adresse, falls mal wieder die Domain „abhanden" kommt?

Es gibt inoffizielle ddl-warez.to-Mirrors von Usern, die das als Hobby machen, aber keine offizielle .onion-Adresse. Den Vorschlag nehmen wir gerne auf.

Wie stellt ihr euch eure Zukunft vor? Wie wollt ihr euch am immer wachsenden Markt halten?

DDL-Warez.to will für seine User weiter an neuen Features arbeiten, täglich Updates bringen und als einziges Portal das Downloaden so einfach wie möglich machen. Viele User sind DDL-Warez schon lange treu, seit sie es entdeckt haben und bedanken sich regelmäßig für den Service. Das ist Motivation genug, weiter zu machen wie bisher.

Usenet-Busts: weiteres Forum zurück, erholt sich die Szene?

Usenet-Busts: Nach NFO-Underground ist ein weiteres Usenet-Forum aus der Versenkung aufgetaucht, dessen Administrator spontan ein paar unserer Fragen beantwortet hat. Manche Wettbewerber werden hingegen für immer offline bleiben. Schon jetzt ist klar: Die kürzlich durchgeführte Razzia wird die Szene nicht gänzlich zerstören, sie hat aber nachhaltige Spuren hinterlassen.

Der Betreiber von NFO-Underground war der Mutigste, sein Forum war schon letzte Woche wieder online. Für ein Statement war er hingegen nicht zu haben. Korrektur: NFO-Underground.XxX ist nur noch eine Board-Leiche ohne Inhalt.

Als nächstes tauchte das Forum HoU wieder aus der Versenkung auf. Wir wurden darum gebeten, den vollen Namen bzw. die URL nicht auszuschreiben, um GVU & Co. nicht mehr als nötig auf sie aufmerksam zu machen. Der Betreiber, der sich (wie die schwedische Release-Group) Fairlight nennt, erklärte uns heute, er habe seine Seite wieder angeschaltet, weil ihm „langweilig wurde". Außerdem habe er sich einen Server im Ausland besorgt, um sich besser gegen eine Aufdeckung oder Abschaltung der Behörden abzusichern.

Ob der bzw. die Verräter bei den Revos (Usenetrevolution.info) zwischenzeitlich ausfindig gemacht werden konnten, weiß er nicht. „Wir haben mit Usenetrevolution u.s.w. nichts zu tun und hatten auch keinen Kontakt zu denen." Die Generalstaatsanwaltschaft Dresden hatte in ihrer Pressemitteilung verlauten lassen, die beschlagnahmten Seiten hätten Einnahmen in Millionenhöhe generiert. Auf die Frage, für wie realistisch der Betreiber die Zahlen hält, antwortete er uns, dies könne „schon sein, wenn man so dreist vorgeht wie SSL News".

Es ist nur ein Hobby von uns
und wird es auch immer bleiben.

Der Administrator und sein Team von HoU distanzieren sich allerdings davon, ein Forum aus finanziellen Interessen zu betreiben. „Es ist nur ein Hobby von uns und wird es auch immer bleiben." Er hofft, dass die deutsche Usenet-Szene in ein paar Wochen wieder so sein wird, wie vor der Bust-Welle. Auf ein aktuelles Posting bei Reddit angesprochen, wo behauptet wird, HoU würde schon bald die Registrierung für neue Nutzer schließen, antwortete er: „Es gibt immer Idioten im Netz" Exakt durch ein solches Verhalten habe „das mit den TakeDowns doch angefangen". Er hält nichts davon, Aufmerksamkeit um jeden Preis zu erzeugen.

Useindex.net und Brothers of Usenet kommen definitiv nicht wieder!

B-DeadAngel, der in diesem Bereich des Webs sehr aktiv ist, wurde aufgrund unserer bisherigen Berichterstattung auf uns aufmerksam. Er teilte uns mit: "Rest in Peace Brothers of Use-

net nach nicht weniger als 9 Jahren (!) und good bye Useindex.net." Beide Seiten kommen sicherheitshalber „definitiv nicht mehr online", wie er uns schrieb. „Es gibt und gab definitiv eine Ratte (Verräter) bei den Revos. Man weiß leider bis heute nicht, wer das war." Sollten die Leser irgendwelche Fragen haben, sollen sie diese bei uns in den Kommentaren stellen. „Ich beantworte dann alles", bot er uns an. Natürlich ist B-DeadAngel nicht allwissend. Erst recht nicht, was das Vorgehen der Polizei und deren Abschaltungen der Server etc. betrifft. Beim Pressesprecher der Zentralstelle Cybercrime Sachsen (ZCS) anzurufen, wie es denn um die Verfolgung der Nutzer steht, wird ähnlich wenig bringen, wie unsere Anfrage bei der ZCB wegen LuL.to. Auch die Kollegen in Sachsen dürften mit der Auswertung der beschlagnahmten Computer geradezu in Arbeit schwimmen. Alleine die Zeit wird zeigen, hinter wem die Behörden im Detail her waren.

Fazit: Die Szene in diesem Bereich ist durch die Usenet-Busts ohne Zweifel stark angeschlagen. Sie ist aber offenbar nicht kaputt zu kriegen.

Schweiz: Stay-Down-Regel problematisch für Uploaded.net

Am Mittwoch präsentierte der Schweizer Bundesrat einen Gesetzesentwurf für deren Urhebergesetz. Die geplante Stay-Down-Regel soll dafür sorgen, dass illegale Inhalte bei Sharehostern nicht erneut hochgeladen werden dürfen. Auch dürfen Rechteinhaber künftig gegen Schweizer Uploader in P2P-Tauschbörsen vorgehen, wenn das Parlament den Entwurf verabschieden sollte.

Der Minimalkonsens, auf den sich vergangenen Mittwoch Vertreter der Kreaktiv-Wirtschaft, der Produzenten, Urheberrechtsnutzer und Konsumenten in der sogenannten Arbeitsgruppe Urheberrecht (Agur12) geeinigt haben, ist alles in allem keine gute Nachricht für Schweizer Filehoster.

Gegen Online-Piraterie, die von der Schweiz ausgeht, soll die geplante Stay-down-Regel vorgehen. Sie soll alle Schweizer Online-Speicherdienste dazu verpflichten, illegale Angebote nach Meldung nicht nur einmal von ihren Servern zu entfernen. Die Betreiber sollen dauerhaft dafür Sorge tragen, dass die urheberrechtlich geschützten Werke nicht erneut hochgeladen werden. Diese Verpflichtung nach Schweizer Recht gibt es bis dato noch nicht. Laut Medienberichten stand ein namentlich nicht genannter Filehoster im Fokus der Verhandlungen, gemeint ist natürlich Uploaded.net mit Sitz im Kanton Zug. Auf Seiten der Nutzer soll sich auch einiges ändern. So soll es künftig für die Rechteinhaber erlaubt sein, die IP-Adressen von Schweizer Tauschbörsenteilnehmern zu protokollieren, sofern sie an einem Upload beteiligt sind. Bislang macht es ein Urteil des Schweizer Bundesgerichts unmöglich, dass Rechteinhaber mit ermittelten IP-Adressen Anzeige bei den Strafverfolgungsbehörden erstatten dürfen. Der reine Download zu Privatzwecken bleibt hingegen straffrei. Dies gilt selbst dann, wenn die Quelle offensichtlich rechtswidrig ist. Legal bleibt auch der Besuch von offensichtlich rechtswidrigen Portalen wie KinoX.to und die Nutzung von Streaming-Hostern, um sich die TV-Serien und Kinofilme kostenlos anzusehen. Wer in der Schweiz künftig was darf, wird hier ausführlich erläutert.

Netzsperren nicht mehrheitsfähig

Auch hat sich die Arbeitsgruppe gegen die Einführung von Netzsperren ausgesprochen. Justizministerin Simonetta Sommaruga betonte am 22. November gegenüber der Presse, dies sei gegenwärtig nicht mehrheitsfähig. Noch wurde der Gesetzentwurf nicht vom Schweizer Parlament verabschiedet. Dafür muss der Kompromiss der Agur12 erst die Beratungen überstehen und eine Mehrheit finden. Wenn die Stay-down-Regel eingeführt wird, muss sich die Cyando AG (Betreibergesellschaft von Uploaded.net) auf noch mehr juristische Probleme als schon jetzt einstellen. Stellt sich die Frage, wie lange es noch dauert, bis das Unternehmen europäischen Boden verlässt oder sich auflöst, um sich der wachsenden Haftung zu entziehen. Offshore-Konkurrenten wie Share-Online.biz werden von der neuen Rechtsprechung nicht betroffen sein. Außer man kann ihnen eines schönen Tages nachweisen, wie das Geld von Belize zurück nach Deutschland, zu den wahren Hintermännern, geflossen ist.

Rezension: E-Book-Piraterie im deutsch- und englischsprachigen Raum

Sachbücher über E-Book-Piraterie sind die absolute Ausnahme. Von daher ist es wenig überraschend, dass Autorin Melina Tsiamos ihr Sachbuch beim weniger bekannten Wiener Verlag danzig & unfried veröffentlicht hat. Wir haben uns den Titel aus dem Jahr 2014 näher angeschaut. Lohnt sich der Kauf?

Der Börsenverein des Deutschen Buchhandels beobachtet die deutschen Verkaufszahlen für E-Books und bringt vierteljährlich einen neuen Quartalsbericht heraus. Das Ergebnis ihrer Beobachtungen ist immer wieder ernüchternd. Im Vergleich zum gedruckten Buch dümpelt der Markt für digitale Werke seit jeher vor sich hin. Obwohl beinahe jeder Deutsche ein tragbares Gerät in Form eines Smartphones mit sich herumträgt, mit dem man E-Books lesen könnte, will der Durchbruch einfach nicht gelingen.

Melina Tsiamos hat einige Faktoren für den fehlenden Erfolg von E-Books in ihrem Buch „E-Book-Piraterie im deutsch- und englischsprachigen Raum“ zusammengetragen. So mangelt es beispielsweise an der Verfügbarkeit digitaler Werke. Es wurden viele ältere Bücher nicht nachträglich als E-Book veröffentlicht, sie gibt es nur als gedrucktes Werk.

E-Books: der Preis ist heiß?

Zwar gibt es hierzulande ausreichend viele Online-Shops. Tsiamos beklagt allerdings deren mangelnde Usability. Wenn der Kaufvorgang zu kompliziert ist, springen viele potenzielle Konsumenten ab, statt diesen abzuschließen. Ein springender Punkt ist auch die Preisgestaltung. Während der Wettkampf der Anbieter in den USA den Preis gedrückt hat, wurde dieser hierzulande künstlich hoch gehalten. Für manche Verleger und Autoren mag dies von Vorteil sein, für die Käufer nicht.

Auch der Wegfall des Kostenapparates für Transport, Druck und Lagerung wirkt sich nicht sonderlich stark auf die Preisgestaltung für E-Books aus. Während beispielsweise das Paperback des Verkaufsschlagers „Darker“, der Fortsetzung von „Fifty Stades of Grey“, ab dem 8.12. für knapp 15 Euro angeboten wird, soll das E-Book fast 13 und das Hörbuch beinahe 16 Euro kosten. Und das ist keine Ausnahme, E-Books kosten im Schnitt drei Viertel des Preises der gedruckten Ware. Diese Preisgestaltung kann und will kaum jemand mitmachen.

Denn dazu kommen weitere Hürden, die die Verlage aufgestellt haben. Laut der Allgemeinen Geschäftsbedingungen der meisten Online-Shops dürfen E-Books weder gebraucht verkauft, kommerziell genutzt oder gefahrlos verliehen werden. Sollte meine Kopie, die für ein Familienmitglied oder Freund angefertigt wurde, bei einer P2P-Tauschbörse landen, kann ich aufgrund des digitalen Wasserzeichens für die illegale Verbreitung zivil- und strafrechtlich in Haftung genommen werden. Der Bundesverband der Verbraucherzentralen hat zwar versucht, juristisch gegen derartige Klauseln vorzugehen. Er ist dabei allerdings komplett gescheitert. Andere Online-Händler, wie Amazon, benutzen einen derart harten Kopierschutz, damit Laien überhaupt keine Chance haben, physisch an die gekaufte Datei zu gelangen. Zwar kaufe ich das Recht, auf einem der Kindle-Reader das Buch lesen zu dürfen. Viel mehr kann und darf ich aber als Käufer nicht tun. Leider schlägt sich das nicht mindernd auf den Verkaufspreis aus, wohl aber auf die Umsatzzahlen.

Und so warten die elektronischen Bücher in Deutschland noch immer auf ihren Durchbruch. An guten E-Book-Readern, Tablet-PCs oder Smartphones, mit denen die Werke komfortabel konsumiert werden könnten, mangelt es nicht. Doch die Hardware hat den Umsatz der E-Books nie wirklich ankurbeln können. Kein Wunder also, wenn Hersteller, wie Sony, ihre Sparte für E-Book-Reader schon wieder eingestellt haben. Die PRS-Modelle kann man zwar nach wie vor gebraucht kaufen, neue Reader von Sony wird es für den Heimgebrauch aber keine mehr geben. Und das, obwohl das japanische Unternehmen in Deutschland in Sachen E-Book-Reader eine Vorreiterrolle eingenommen hatte.

Guter Überblick fürs Geld

€ 27,90 für das Paperback sind absolut marktüblich, aber trotzdem eine Menge Geld für das vergleichsweise dünne Buch. Melina Tsiamos fasst dennoch auf 119 Seiten (die ganzen Anhänge abgerechnet) viel Wissenswertes zum Thema Buchpiraterie zusammen. Sie vergleicht die Urheberrechtsproblematik der Verlage häufig mit der der Musikwirtschaft und den Filmstu-

dios. Auch Vergleiche mit ausländischen Märkten, wo vieles anders läuft, fehlen nicht. Von daher erhält man für sein Geld einen guten Überblick. Melina Tsiamos hat im Vorfeld recht tief recherchiert, ihre Aussagen werden mit zahlreichen Verweisen zu weiterführender Literatur oder Links zu Artikeln belegt.

Fazit: Wer eine kritische und leicht verständliche Betrachtung sucht, wird hier gut bedient. Was fehlt, ist eine Analyse, wie die Angebote der Online-Piraten im Detail aufgestellt sind. In diesem Punkt unterscheidet Tsiamos lediglich zwischen P2P-Indexern und illegalen Anbietern, die ihre Besucher auf Sharehoster leiten, um dort den eigentlichen Download durchführen zu lassen. Da hätte man weit tiefer in die Materie eintauchen können und müssen. Wo bitte ist das Usenet, die Releaser-Szene, die ganzen Börsen, Schattenbiliotheken oder die LuLs, die das geistige Eigentum Dritter in bare Münze verwandelt haben!?

Eine Neuauflage dieses Sachbuches wäre sinnvoll, weil manche Fakten mittlerweile überholt sind. Doch wir dürfen nicht vergessen: E-Books fristen seit jeher ein Nischendasein. Somit ist fraglich, ob sich bei der wahrscheinlich eher geringen Nachfrage für den Verlag danzig & unfried die Überarbeitung der Inhalte und der Druck einer neuen Auflage rentieren würde. Es ist auf jeden Fall befriedigend zu sehen, dass man für den mangelnden Durchbruch der E-Books nicht alleine die bösen Piraten, sondern auch die Strategie der Verlage und ihres Dachverbandes verantwortlich macht. Wen wir neugierig machen konnten, weitere Infos zu diesem Buch sind hier verfügbar.

E-Book-Quartalsbericht: Schwacher Umsatz trotz steigendem Absatz

Erneut hat der Börsenvereins des Deutschen Buchhandels e.V. seinen E-Book-Quartalsbericht herausgegeben. Basierend auf Hochrechnungen der E-Book-Absätze und -Umsätze, die aus dem GfK Consumer Panel Media*Scope Buch stammen und an dem sich insgesamt 25.000 Personen beteiligen, werden nun die neuen Ergebnisse bekannt gegeben. Sie sind repräsentativ für die deutsche Wohnbevölkerung ab zehn Jahren, für insgesamt 67,8 Mio. Menschen. Die Erhebung des Börsenvereins in Kooperation mit GfK Entertainment zeigt die vierteljährlich die Entwicklung auf dem E-Book-Markt und beleuchtet sowohl die Perspektive der Kunden, als auch die des Handels und der Verlage.

Der Absatz von E-Books am Publikumsmarkt (ohne Schul- und Fachbücher) ist in den ersten drei Quartalen 2017 erneut angestiegen. So wurden insgesamt 20,5 Millionen E-Books gekauft,

was einen Anstieg von 1,7 Prozent zur Folge hat im Vergleich zum Vorjahreszeitraum. Der Umsatz sank im gleichen Zeitraum um 4,6 Prozent. Von 5,2 Prozent auf 5 Prozent zurück ging zugleich der Umsatzanteil von E-Books am Publikumsmarkt.

Als Grund für den schwachen Umsatz nennt der Börsenvereins des Deutschen Buchhandels e.V. eine Kombination aus sowohl geringerer Käuferanzahl, als auch dem Sinken der von ihnen bezahlten Preise pro gekauftem E-Book. So kauften nur noch 3,1 Millionen Menschen – und damit 7,9 Prozent weniger als im Vorjahreszeitraum – E-Books. Die Käufer bezahlten im Durchschnitt nur noch 6,29 Euro für ein E-Book, das bedeutet einen Rückgang von 6,1 Prozent im Vergleich zu den ersten drei Quartalen 2016.

Der steigende Absatz ist hauptsächlich zurückzuführen auf die gestiegene durchschnittliche Kaufintensität, das heißt, wer E-Books kauft, erwirbt mehr Bücher. So steigt die Kaufintensität in den ersten neun Monaten 2017 um 10,4 Prozent im Vergleich zu den ersten drei Quartalen 2016. In konkreten Zahlen ausgedrückt bedeutet das für das bisherige Jahr, dass durchschnittlich 6,7 E-Books auf den Readern der Käufer landen. Im Vergleichszeitraum waren es 6,1 E-Books.

Usenet-Razzien: Insider gibt Entwarnung für die Nutzer

Die Redaktion von Tarnkappe.info wurde kürzlich von einem Insider kontaktiert. Dieser möchte „einigen Quatsch“, den man derzeit in einschlägigen Foren lesen kann, richtigstellen. Mit Ausnahme von usenetrevolution.info seien vor der Durchsuchung die Daten aller Server „geschreddert“

worden, um den Ermittlern die Arbeit zu erschweren. Nach dem Bust von NFO-Underground.XxX, mit dem letzte Woche alles begann, war die Szene gewarnt und traf entsprechende Vorkehrungen. Nur im Fall von Usenetrevolution.info war man mit der nachhaltigen Löschung der Daten nicht schnell genug.

Die Echtheit unseres Kontaktes wurde uns von dritter Stelle bestätigt. Mit Ausnahme der Person können wir leider keine seiner Aussagen überprüfen, weswegen dieser Beitrag naturgemäß mit Vorsicht zu genießen ist. Für wie glaubhaft man das Ganze hält, muss jeder Leser für sich selbst entscheiden.

Usenet-Razzien: Entwarnung für die Nutzer

Alle Server wurden verschlüsselt betrieben. Die Beamten bekamen von den meisten Servern keine Logs, das einzige Problem war und ist der Server der Revos (also von Usenetrevolution.info). Dort begann die Löschung der Daten in etwa zeitgleich mit der Beschlagnahmung. Den Betreibern gelang es aber noch die Logs der letzte Tage aus der Datenbank und dem Server zu entfernen, dabei wurde die Verbindung gekappt. Bei Usenetrevoluion können somit maximal die Log-Dateien der letzten Stunde vorhanden sein. Dazu kommt, dass die Ermittler den Server bei ihrer Aktion abgeschaltet haben. Nachdem der Strom ausgeschaltet war, konnte man ohne gültiges Passwort wohl nicht mehr auf die verschlüsselten Festplatten zugreifen. Laut unserem Informanten war dies „das Beste“, was in dieser Situation geschehen konnte.

Von den Razzien waren auch mehrere Uploader betroffen. Die entscheidende Frage ist natürlich, was man bei ihnen zu Hause vorgefunden hat. Wir wissen von einem Fall, bei dem ein aktiver Uploader aus mangelnder Vorsicht keine seiner Festplatten verschlüsselt hat, das ist ja leider nicht unüblich im Graubereich. Dieser soll früher bei der auf Musik spezialisierten Seite CannaPower aktiv gewesen sein. Der Mann war nach Eintreffen der Beamten sofort vollumfänglich geständig. Betroffen war auch die Wohnung seines Verwandten, zu dem es einen direkten Durchgang gibt. Auch dort wurden Geräte beschlagnahmt. Der Durchsuchungsbeschluss lautete nur auf den Namen des Uploaders und nicht auf den seines Angehörigen. Von daher dürfte es rechtlich gesehen strittig sein, ob diese Beschlagnahmung rechtmäßig war. Einen Anwalt will sich der Beschuldigte nicht nehmen. Er habe ja bereits alles gestanden und müsse sich deswegen nicht mehr verteidigen lassen, rechtfertigt er sein unorthodoxes Vorgehen. Fest steht: Die Unterstützung eines Fachanwaltes auszuschlagen, ist so ziemlich das Dümmste, was man tun kann.

„Und es wird wahrscheinlich einen Maulwurf gegeben haben“

Der Betreiber von usenet-town.com und SSL News war ein Rene Ti*****n, der letzte Woche in Spanien verhaftet wurde. Seine Kundschaft wurde recht umfangreich zur Kasse gebeten: „Dort war es so, dass die User nur über SSL News an seinen Indexer kamen, der nochmals 99 Euro im Jahr gekostet hat.“ Usenet-Town soll ehedem für seine illegalen Geschäfte in Szene-Kreisen „bekannt gewesen sein“. Unser Mann mutmaßt, „Man griff vorher nur nicht zu, weil man jemanden bei den Revos eingeschleust hatte.“ speedUSE.NET hingegen war ein reiner Usenet-Provider, von dem es so viele wie Sand am Meer gibt.

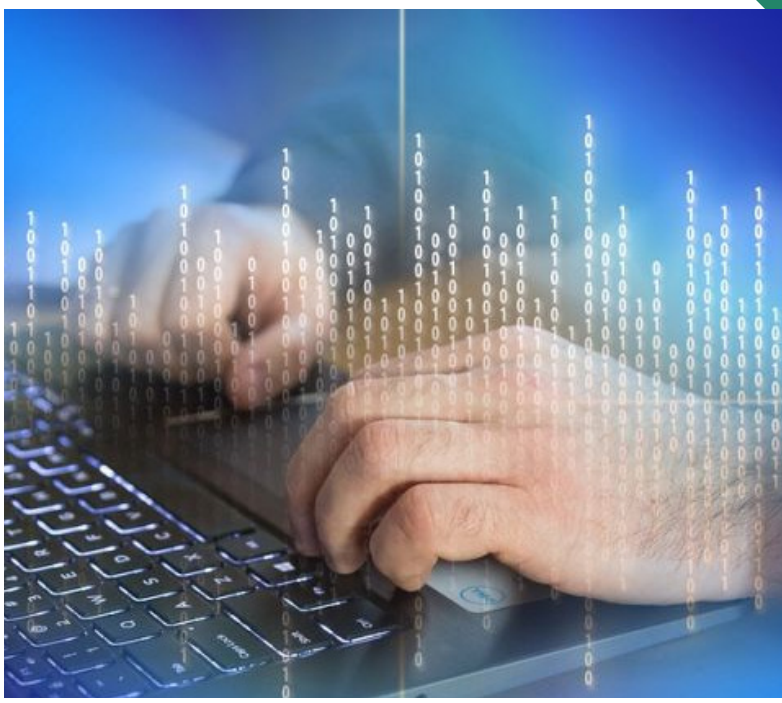
Nach Bekanntwerden der Durchsuchung beim Forum NFO-Underground.XxX, das aus unbekannten Gründen wieder online ist, waren die anderen Hintermänner der deutschsprachigen Usenet-Szene gewarnt. Unserem Informanten liegt es am Herzen, dass die Nutzer keine Angst bekommen, nur weil „irgendwelche Volltrottel bei myGully schreiben, sie hätten Besuch bekommen.“ Als die Polizisten bei den nächsten Servern ankamen, waren die Daten bereits vernichtet. Auch der Betreiber von speedUSE.NET war betroffen und dort fand man die Account-Daten der Server von Usenetrevolution. „Dumm gelaufen für Speeduse, zumal dieser Anbieter niemals Uploads mit eigener Werbung versehen hat, so wie SSL-News.” Speeduse habe nicht mal Upload-Accounts vertrieben, so wie andere Wettbewerber. Bei Speeduse.net konnte niemand Drittes aufgrund der Verschlüsselung der Transfers über Port 563 (SSL) sehen, was im Einzelnen übertragen wurde. Auch deswegen müsse man sich als Nutzer wenig Sorgen machen.

Komischerweise hat der Admin von NFO-Underground.XxX seine Pforten wieder geöffnet. Buddy war letzte Woche als erstes von der Bustwelle betroffen, von daher erscheint dieser Schritt sehr verwunderlich. Korrektur: NFO-Underground ist ohne Inhalt, weil dieser gelöscht wurde. Unser Kontakt hat übrigens nach seinen Vorkehrungen allen Beteiligten der Usenet-Szene empfohlen, vorerst die Pforten zu schließen. Und dies nicht nur um sich, sondern auch um die eigenen User zu schützen. Jetzt „heißt es Füße stillhalten und abwarten“. Ob eines der Foren wieder im Clearnet oder alternativ im Darknet online gehen wird, müsse laut unserem Insider „jeder für sich selbst entscheiden“.

Wenn die Mitarbeiter der Polizei etwas auswerten aus der Asservatenkammer, dann können es nur die Logs von Usenetrevolution (Revo) sein und nur von etwa der letzten Stunde. „Und wenn man die Kiste ausgeschaltet hat, dann war sowieso Essig (mit der Auswertung)“, schließt unser Informant seine Einschätzung ab.

Zudem haben wir gestern mit Benedikt Klas geklärt, dass der reine Besuch der Foren nicht illegal ist. Auch die NZB-Dateien herunterzuladen, ist an sich nicht strafbar. Auch nach dem Filmspeler-Urteil des EuGH „findet keine so weite Vorverlagerung der Strafbarkeit statt“, erklärte gestern Fachanwalt Klas die Sachlage. Selbst nachdem man sich im Forum für einen Download bedankt hat, steht nicht fest, dass es danach tatsächlich zu einem Download gekommen ist. Und nur der sei strafbar und eben diesen müsste die Polizei den verdächtigten Personen nachweisen. Ob dies im Zuge der Daten-Löschungen und des Eigentors der Ermittler (technisches K.O. durch Strom ausschalten) möglich war, bleibt unklar.

Was also droht den Nutzern der Usenet-Razzia, sollte man ihnen habhaft werden? Unser Telefon-Interview mit Fachanwalt Benedikt Klas klärt es auf.



Ermittlern gelingt Schlag gegen Andromeda-Botnetz

Am 29.11.2017 ist es Ermittlern aus neun Ländern gelungen, das global agierende Andromeda-Botnetz zu stoppen. Die Koordinierung der Maßnahmen erfolgte über eine zentrale Befehlsstelle bei Europol. In die Umsetzung aller genannten Maßnahmen waren insgesamt 27 Staaten eingebunden. Maßgeblich an der Aktion beteiligt waren Ermittler der Zentralen Kriminalinspektion Lüneburg unter Sachleitung der Staatsanwaltschaft Verden (Aller) sowie die US-Bundespolizei FBI, heißt es in einer Pressemitteilung.

Verteilt wurde die Schadsoftware mittels in E-Mails enthaltener Links. Durch das Anklicken des Links haben sich die Opfer ein infiziertes Microsoft Office-Dokument auf ihren Computer geladen. Außerdem konnte die Infizierung über Drive-by-Exploits erfolgen, die sich auf kompromittierten Werbebannern oder Websites, hauptsächlich solche mit zweifelhaftem Inhalt (Pornographie, illegale Verkäufe, Verstoß gegen Urheberrechte durch Videostreaming usw.), befinden. Einmal infiziert, späht der Schädling das Opfer-System aus und ist in der Lage, einen Banking-Trojaner nachzuladen, der auf die ausgespähten Daten der Opfer abgestimmt ist. Mittels dieser Schadsoftware gelang es den Tätern in den letzten Jahren, mehrere Millionen PC-Systeme zu infizieren. Hauptangriffsziele der Schadsoftware waren Nordamerika, Asien und in Europa im Schwerpunkt die Länder Rumänien, Italien, Deutschland und Polen.

Die Ermittlungen gegen das Botnetz wurden vor rund zwei Jahren gemeinsam mit Microsoft gestartet. Bereits durch das Aus-

schalten der internationalen Botnetzinfrastruktur “Avalanche” im vergangenen Jahr konnten neue Erkenntnisse gewonnen werden, die auch in diese Ermittlungsarbeiten mit eingeflossen sind. Die Polizeibeamten der ZKI Lüneburg unterstützten die US-amerikanischen Kollegen bei der Planung und Abschaltung des weiteren Botnetzes. Es wurde nicht nur das Botnetz selbst abgeschalten, sondern auch erste Festnahmen vollzogen. Die Aktion verlief unter dem Codenamen “Takedown 2”. Über 1,3 Millionen gekaperte Computer wurden befreit. Ein Tatverdächtiger wurde in Weißrussland festgenommen. Bei der Durchsuchung seiner Wohnung beschlagnahmten die Ermittler belastendes Material. Zudem konnten sieben Steuerserver in sechs verschiedenen Ländern beschlagnahmt und abgeschaltet werden. Darüber hinaus belegten die Ermittler über 1.500 Domains der Schadsoftware Andromeda mit einer sogenannten Sinkholing-Maßnahme. Allein dadurch wurden am vergangenen Mittwoch weltweit 1,35 Millionen IT-Systeme identifiziert, die mit der Andromeda Schadsoftware befallen waren.

Die Internetprovider informieren ihre Kunden, wenn deren Systeme infiziert sind. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) macht darauf aufmerksam, dass Nutzer auch nach der Zerschlagung des Andromeda-Botnetzes eine Infektionsmeldung von ihrem Internet-Provider ernst nehmen sollten und ihre Geräte prüfen. Auf seiner Internetseite informiert das BSI über Botnetze und gibt Betroffenen Tipps, wie sie ihre Computer sicher einrichten.

Auch ein Jahr nach Zerschlagung des Avalanche-Botnetzes beträgt die Zahl der Infektionsmeldungen in Deutschland immer noch ein gutes Drittel (39 Prozent) des Ursprungswertes. Das liege daran, dass Betroffene ihre Systeme trotz Benachrichtigung noch nicht bereinigt hätten. Zwar könnten betroffene Rechner sowohl bei Andromeda- als auch bei Avalanche-Infektionen durch BSI-Schutzmaßnahmen keinen Schaden mehr anrichten, wären aber weiter infiziert und somit anfällig für Missbrauch.

Geld sollte nicht die Hauptrolle spielen: ein Uploader im Gespräch

Heutzutage spielen die so genannten Uploader im Schattenbereich des Webs eine ungemein wichtige Rolle. Wenn es sie nicht gäbe, wären alle Warez-Seiten & -Foren leer, hätten die Sharehoster keine Kunden und diese nichts zu konsumieren. Wir haben uns mit

einem langjährigen Uploader der deutschsprachigen Szene getroffen, um mehr über sein illegales Handeln zu erfahren.

Tatort Berlin Hohenschönhausen

Wir treffen uns mit unserem anonymen Kontakt mitten in einer der typischen Hochhaussiedlungen Ost Berlins. Unser Treffpunkt liegt zwischen mehreren Seelenverkäufern, wie man die Wohnsilos auch nennen könnte, wo dazwischen große Wiesen angelegt wurden. Wahrscheinlich, um bei dem vielen Grau des Betons den Menschen noch ein wenig Grün zu spendieren. Im Erdgeschoss einiger Gebäude sind Handyläden, 1-Euro-Geschäfte und Discounter verschiedener Lebensmittelketten angesiedelt. Nur einen Steinwurf entfernt wurden zu DDR-Zeiten Staatsfeinde im eigenen Gebäudekomplex der Stasi verhört. Das ehemalige Gefängnis scheint unseren Mann aber nicht zu schockieren. Wir nehmen zum vereinbarten Zeitpunkt neben ihm auf der Parkbank Platz.

Sag mal, was machst Du eigentlich beruflich? Welche Hobbys hast Du neben der Szene?

Geht ja direkt los. Ganz schön private Frage, oder? Also beruflich bin ich in der Medienbranche tätig, ohne auf Details eingehen zu wollen. Und in meiner Freizeit mache ich eigentlich auch das, was Andere so machen ;) Serien gucken, mit Freunden etwas unternehmen etc. Alter und Wohnort bleiben aber privat.

„Alles ist auf Kommerz ausgerichtet“

Okay. Und was genau ist für dich die „Scene“?

Um es mal zu unterscheiden: die eigentliche Scene an sich gibt es so gut wie nicht mehr. Eigentlich ist es heute nur noch auf Kommerz ausgerichtet, seien es Tor-

rent-Seiten (Ausgenommen die privaten Tracker, da gibt es wirklich noch viele Leute, die es aus Liebe betreiben).

FTP-Dumps oder Warez-Seiten, überall geht es eigentlich nur noch ums Geld. Im Allgemeinen wird der Begriff Scene auch oft durcheinander gebracht mit dem Begriff Szene.

Um auf den Punkt zu kommen:
Die richtige Scene heißt für mich, die Releases zu erstellen oder Programme zu cracken, ohne kommerzielle Hintergründe. Und nicht, wenn diese Releases aus monetären Anreizen weiterverteilt werden.

Was ist Deine persönliche Motivation, dieser Tätigkeit nachzugehen? Wie lange machst Du das schon?

Meine Motivation ist eigentlich, Menschen, die kaum Geld haben, um sich andauernd neue Filme, Spiele, Musik, etc. kaufen zu können, oder Menschen, die keine Lust haben sinnlos Geld für ein Produkt auszugeben, was am Ende eine Menge Geld kostet und im Grunde totaler Müll ist, eine Möglichkeit zu geben, sich solchen Content zu beschaffen.

Menschen, die kaum Geld haben, werden sich den Content wahrscheinlich eh niemals kaufen. Aber ich denke, Menschen, die das Geld haben und denen das Produkt, was sie sich vorher illegal beschafft haben, und wenn ihnen am Ende der Content gefällt, diese werden sich den Content vielleicht später doch kaufen.

Viele denken ja bei den meisten Uploadern, das Geld wäre deren größte Motivation. Das trifft bei einigen bestimmt auch zu. Aber meine Motivation damit hauptsächlich Geld zu verdienen, ist es nicht.

Ich persönlich mache das aktiv seit 2006. Wobei ich vorher aber als Downloader schon seit dem Jahr 2002 aktiv war.

„Viele denken ja bei den meisten Uploadern, das Geld wäre deren größte Motivation. Das trifft bei einigen bestimmt auch zu."

Hast du eigene Seiten oder Foren? Bist du auf anderen Seiten als Moderator aktiv?

Eigene Seiten? Nein. Moderator bin ich auch nicht. Ich war es damals mal auf zwei großen Webseiten, die es mittlerweile nicht mehr gibt. Aktuell aber auf keiner, obwohl es Nachfragen gab. Damals ging es noch, aber heute wäre es mir viel zu zeitaufwendig.

Wie stehst Du zu Foren oder Streaming-Seiten? Welche davon nutzt Du, welche verabscheust Du?

Neutral, es ist halt ein Geben und Nehmen. Auf den deutschen Foren bzw. Webseiten stelle ich den Content, was DDL angeht, eigentlich überall bereit, wo es geht. Ansonsten sind Streams eigentlich das, was ich am meisten mache. Bis auf bs.to (Burning Series), was ich privat eigentlich am häufigsten eintrage. Und das tue ich überall da, wo es frei möglich ist.

Verabscheuen ist so eine Sache. Eigentlich hauptsächlich das Netzwerk um myGully/KinoX. Ich finde, die haben die deutsche Warez-Szene zu sehr im Griff und auch viele Mitbewerber mit Methoden wie DDoS, Erpressung etc. (movie2k.to) aus dem Weg gedrängt, die ich nicht gut finde.

Eigentlich sollte Platz für jeden da sein. Es kann nicht sein, dass einem einzelnen Netzwerk 70% der deutschen Warezseiten gehört.

Doch genauso ist es. Macht es Sinn, als Neuling noch mit dem Uploaden anzufangen? Oder ist der Markt zu überflutet? Welches Startkapital sollte man dafür in etwa mitbringen?

Sinn macht es eigentlich nur noch wenn man damit nicht hauptsächlich Geld verdienen will, weil es schon zu viele Uploader gibt, gegen die man sich erstmal beweisen muss.

Als Startkapital reichen eigentlich schon 20€ aus für einen billigen Server (Remote Desktop Protocoll = RDP) und einen (Virtual Private Network = VPN) -Anbieter. Um an Content zu gelangen, braucht es dann noch mehr.

Entweder man wählt die kostengünstige Variante und holt alles von privaten Torrent-Trackern. Oder man kauft sich den Premiumaccount (eines Sharehosters) und holt sich die Sachen von anderen Uploadern. Was allerdings zeitaufwendig ist und man am Ende nur vielleicht die Kosten herausbekommt, die man vorher investiert hat.

Wenn man es professionell machen und immer ganz vorne mit dabei sein will, benötigt man am Anfang Startkapital im mittleren 3-stelligen Bereich oder bei Tools, die man sich programmieren lässt, Geld im 4-stelligen Bereich. Und die Kosten muss man dann auch erstmal wieder einspielen. Und

wenn man Autotrader hat, braucht man auch die entsprechenden Server dazu, da reicht ein RDP für 10€ oder 20€ nicht aus.

Ob es Sinn macht, muss jeder für sich selber wissen.

Was macht die Content-Industrie eigentlich aus Deiner Sicht falsch? Wie bist du grundsätzlich gegenüber der Filmindustrie eingestellt?

Was sie falsch macht? Viel zu viel!

Fangen wir mal bei Musik an, da haben sie es zumindest gelernt. Dienste wie Spotify, iTunes, Deezer und wie sie alle heißen, haben dazu geführt, dass die meisten Leute von illegalen Angeboten zu legalen Angeboten gewechselt sind. Auch wenn diese Dienste die Künstler nicht gerecht bezahlen, so bringt es dennoch mehr ein, als wenn 100.000 Leute dein Album illegal downloaden.

Bei Filmen sind wir auch auf einem guten Weg, aber da kommt das große Problem. Anbieter haben ein Monopol, heißt die Lizenzen werden nur meist an Einen vergeben. Wenn ich wirklich viel sehen und abgedeckt sein will, gerade was auch gute TV-Serien oder neue Filme angeht, dann bräuchte man 3-4 Accounts bei unterschiedlichen Anbietern. Das wären schon mal monatliche Kosten von rund 40€.

Bei Exklusiv-Serien, die die Firmen selber produzieren, wie Netflix oder Amazon, da sehe ich es noch ein. Aber warum brauche ich für einen aktuellen Film einen Netflix-, Amazon- oder Maxdome- Account, nur weil es diesen Film nur dort geben würde. Das sehe ich nicht ein. Da greife ich als Konsument lieber zu illegalen Angeboten.

Dazu kommt noch, dass die Filmfirmen mit allen Mitteln Geld verdienen wollen, die es gibt. Nimmt man zum Beispiel 20 Jahre alte Filme. Diese sind zwar auf Amazon vorhanden. Aber ich soll für den Stream eines 20 Jahre alten Films für maximal 48 Stunden zwischen 3,99€ und 9,99€ bezahlen. Oder aber muss ihn gleich kaufen, weil das Streaming nicht mal freigeschaltet wurde!?? Das sehe ich bei aller Liebe nicht ein, und das werden die meisten Zuschauer auch nicht tun.

Ich finde, man sollte das Urheberrecht endlich lockern und Filme, die älter als 15 oder 20 Jahre sind, generell lizenzfrei machen. Aber das wollen die Content-Firmen ja nicht, weil sie damit immer noch gut Geld machen können.

Bezogen auf aktuelle Kinofilme würde es extrem viel bringen, diese nach zwei Wochen im Internet verfügbar zu machen. In den ersten zwei Wochen sind die Einspielergebnisse in den Kinos am höchsten. Danach sollte man den Film auch legal streamen können.

Aber nicht für 50€ pro Film. Aber ehe das die Filmindustrie endlich begreift, sind die Kinos ausgestorben.

Ich will jetzt hier auch keinen Monolog halten. Aber um das mal abzuschließen, nehmen wir die E-Books. Warum kosten die digital annähernd so viel, wie als Buchversion? Nach meiner Meinung sollten sich die Verlage endlich mal selbst die Frage stellen, warum illegale Downloads in dem Bereich so sehr boomen.

Das werden sie wohl nicht. Aber etwas anderes: Was denkst du über Vereine wie die GVU oder BREIN, die immer schärfere Gesetze gegen das Urheberrecht wollen und dafür klagen?

Also, die GVU finde ich einfach lächerlich. Dieser Verein hat tausende Mitglieder, die einen Haufen Geld dafür zahlen, dass man sie schützt und was passiert? Kaum etwas. Der größte ihrer Erfolge war Kino.to, aber die Seite würde heute noch stehen, wenn nicht jemand ausgepackt hätte. Und anscheinend nicht mal richtig, weil sonst wäre KinoX nicht so schnell entstanden. Und dort sind heute immer noch Mitglieder dabei aus dem Kino.to-Team, die damals nicht erwischt wurden. Und selbst KinoX bekommen sie nicht abgeschaltet, weil sie die Betreiber nicht packen können aufgrund ihrer schlampigen Ermittlungsarbeit. Sie können ihre Mitglieder kaum schützen.

BREIN hingegen sollte man aber schon ernster nehmen, denn sie fahren deutlich härtere Geschütze auf, verklagen auch die Rechenzentren, Domain Registrare etc. und bringen diese bis vor den EuGH und setzten dort auch Domainsperren, u.s.w. durch. Die könnten auch noch zur echten Gefahr werden in Sachen Internet-Zensur.

Die Content-Industrie kämpft lieber gegen kleine Anbieter, statt sich mit den Großen wie Google anzulegen.

Wie findest Du es, dass Sharehoster in die Haftung genommen werden, aber Firmen, wie Google mit YouTube, wo massenweise gegen das Urheberrecht verstoßen wird, nicht?

Ganz einfach, Google ist ein Konzern der Milliarden hat, um sich die besten Anwälte der Welt leisten zu können. Hinzu kommt, dass ein Verfahren gegen Google mit allen Revisionen Jahre andauern würde. Ein Sharehoster wird sich diesen Kampf nicht leisten können, also geht man zuerst auf die los. Die Chancen, dass sie vor Gericht verlieren und verboten werden, ist groß, weil so gut wie 90% der Inhalte auf One Click Hostern (OCHs) illegal sind, weil diese gegen das Urheberrecht verstoßen.

Selbst wenn man alle Videos auf YouTube nimmt, dürfte sich der illegale Content bei etwa 5-10% und maximal bei 20% bewegen. Für die Content-Firmen lohnt sich ein jahrelanger Rechtsstreit nicht, zumal Google gut mit denen zusammenarbeitet. Fast alle großen Content Firmen haben bei YouTube eigene Löschrechte.

Was aber ein Problem auf YouTube ist, sind die Live-Streams, wo 24/7 Serien nonstop gestreamt werden. Und wenn ein Account gebannt wird, geht sofort ein neuer online. Da könnte YouTube leicht gegenlenken mit strengeren Account-Anforderungen für Live-Streams (Mindestanzahl an Uploads, Abos etc.). Und das andere Problem von Google ist derzeit der Missbrauch von Google Drive etc. Da sollten sie auch eine Lösung finden, damit ein Missbrauch unterbunden wird. Aktuell gibt es zu viele Lücken dort.

Abzocke: Die Hoster bescheißen die Uploader mittlerweile sehr häufig

Bist Du der einzige Uploader nur einer Seite oder befüllst Du gleich mehrere Seiten?

Mehrere, mit einer alleine kann man die Ausgaben nicht decken. In Zeiten von 3dl und iLoad war es noch etwas anderes, da hat nur eine Seite gereicht.

Mit dem Programm Zoom kann eigentlich so gut wie jeder ein Uploader werden. Wie hast du es geschafft, Dich zu etablieren bzw. so weit zu kommen, wie du gekommen bist? Wo stehst Du heute? Gehörst Du zu einem der gut verdienenden Uploadern?

Zum einen, ich habe nicht mit Zoom angefangen, 2006, als ich aktiv mit dem Uploaden angefangen habe, gab es das noch nicht. Auch andere Tools wie z.B. IntelligeN gab es zur der Zeit wohl auch noch nicht. Das war reine Handarbeit. Aber da gab es noch nicht so viele Warezseiten, die mit Sharehostern zusammengearbeitet haben.

Heute ist es gut, dass es solche Tools gibt, sonst würde man es zeitlich kaum noch schaffen. Aber solche Tools haben auch dazu geführt, dass es jetzt so viele Uploader gibt, weil man kaum noch etwas machen muss. Diese Tools übernehmen zum Großteil das Crawlen und das Posten der neuen Einträge.

Sich etablieren? Damals war es leicht. Da warst du ständig in der Topliste ganz oben. Folglich haben die Leute immer deine Uploads gezogen. So ist es heute eigentlich auch noch. Wenn Du viele Beiträge hast und dafür sorgst, dass deine Uploads online bleiben und Du hilfst auch den Usern, so saugen diese auch eher bei Dir oder kaufen sich Premium-Zugänge über Deinen Account.

Gut verdienen? Die Zeiten sind vorbei, wo man mit vierstelligen Beträgen im Monat rausgeht.

Damals, so 2006/2007 zahlte beispielsweise Uploaded 20€ pro 1000 Downloads und 2€ pro vermitteltem Premiumaccount.

Trotzdem hat eine Seite gereicht, sofern man in der Topliste oben stand. Dann erhielt man als Umsatz vierstellige Beträge monatlich.

Und heute? Jetzt postet man auf 20 Seiten und kommt nicht annähernd an diesen Betrag heran, weil die Hoster mittlerweile auch viel bescheißen.

Außer man hat das Glück und verfügt über einen Account bei den großen Blogs.

Das klingt ja alles nicht so toll. Wie erlangt man als Uploader eigentlich eine große Reichweite? Ergo: Wie kann man sich aus der Masse hervorheben? Durch einschlägige Börsen, große Warez-Seiten, BB, IRC?

Qualität und Quantität. Und immer präsent sein. IRC spielt heutzutage kaum noch eine Rolle.

Ja, stimmt, der IRC ist ein Relikt aus der Vergangenheit. Was hältst Du von Sharehostern, wie Anonload, die nur im Darknet erreichbar sind?

Sieht aus wie jeder Filehoster mittlerweile. OCH-Hoster im Darknet gibt es ja schon, genauso wie Warezboards. Sind aber meistens nur .onion Adressen der Clearweb-Domains (also http://www. etc.).

Wofür gibst Du Deine Einnahmen aus? Und bitte keine Antwort à la das geht alles für die Server drauf. Wie viel kommt denn im Monat zusammen an Geld? (ohne Abzüge, mit Abzügen).

Tja, mittlerweile ist es aber genauso. Meine Server kosten ca. 100€ im Monat, dazu kommen 1 FTP mit 30€ dazu, 2 VPNs mit ca. 25€ Kosten zusammen, dazu die Mietkosten für mein Tool.

Round about sind es schon 200€ Ausgaben am Ende. Die müssen erstmal wieder reinkommen. Das ist derzeit noch machbar, obwohl Uploaded.net Accounts bannt und der Hoster keine Einnahmen mehr bringt.

Was genau am Ende an Einnahmen rauskommt, will ich nicht sagen, aber mehr als 1.000€ sind es nicht abzüglich der Serverkosten.

Das was am Ende rauskommt, wird 50/50 aufgeteilt. Die eine Hälfte wird auf ein BTC-Wallet (Bitcoin-Konto) eingezahlt. Und die andere Hälfte geht ins Real Life.

Warum wird auf Warez-Seiten und Foren (Boards) eigentlich so wenig Wert auf Verschlüsselung gelegt? Wenn überhaupt, sind es normalerweise nur der Seitenname oder der Name des Uploaders. Würde jeweils ein einmaliges Passwort nicht länger vor Abuse-Löschungen schützen?

Die neuen Boards/Blogs haben doch fast alle https://, bei den Alten ist es schwer wegen der Foren-Software. Zumal die Sicherheit auf Warez-Boards eher nicht auf Verschlüsselung liegen sollte, in Form einer SSL-Verschlüsselung, sondern darin, kaum etwas zu loggen, wie IP-Adressen und Co. Und der reine Besuch einer Warezseite und dort einen Account zu haben, das ist nicht illegal.

Ein einmaliges Passwort (für die hochgeladenen Archive) hilft nicht gegen ein Abuse. Die Bots der Abuse-Agenturen (Anti-Piracyfirmen) sind inzwischen so gut. Sie finden automatisch das Passwort im Posting.

„Die Angst erwischt zu werden lebt immer mit."

Hast Du keine Angst, erwischt zu werden?

Doch, die Angst lebt immer mit. Aber ich denke, ich sicher mich schon gut ab. Erwischt wird man hauptsächlich eigentlich immer bei den Geldwegen, da muss man aufpassen.

VPNs und Co. sind Standards.

Anders geht es wohl nicht. Was sind denn Deine drei wichtigsten Grundsätze in Bezug auf die Sicherheit?

Also, als als Erstes: Immer einen VPN-Anbieter verwenden, weil im Internet ist niemand anonym. Zweitens: Niemals private, persönliche Dinge (Alter, Wohnort, Stimme) über sich preisgeben, irgendwann wird es einem zum Verhängnis. Und Drittens: Im privaten Umfeld nicht erzählen, was du machst und auf keinem Fall mit dem Geld prahlen.

Wie wichtig ist Anonymität in diesem Bereich? Was nutzt Du sonst noch an Sicherheitsvorkehrungen?

Das ist wichtig. An Tools nutze ich eigentlich nur VPNs. Und das übliche: E-Mail-Adressen im Ausland auf eigene Domains, Domains auf falsche Daten u.s.w.

Welcher VPN eignet sich gut fürs Uploaden?

Perfect-Privacy, oVPN, nVpn, etc. Wichtig ist eigentlich nur, dass die Verbindung zum Server verschleiert wird. Und der Server anonym bezahlt wird ohne jeglichen Bezug zu persönlichen Daten.

Geldwäsche: „Man kann sich kein 80.000€ Auto vor die Tür stellen, wenn man nur 8,50€ die Stunde verdient."

Wie gehst Du bei den Auszahlungen mit dem Thema Geldwäsche um? Wie lässt Du das Geld auszahlen? Auf ein Bankkonto, per Bitcoins oder Gutscheine?

Damals gab es noch keine Bitcoins, meine ersten Auszahlungen sind damals auf PayPal-Konten geflossen. Als ich das erste Kapital angespart habe, habe ich mir ein Offshore-Konto erstellt, was heute noch aktiv ist.

Darüber laufen alle Einnahmen und Ausgaben. Dank Kreditkarte kann man auch überall auf der Welt das Geld abheben.

Mittlerweile lasse ich aber alles in Bitcoins auszahlen, damals waren es auch Gutscheine, aber die habe ich meistens an Exchanger verkauft.

Der größte Fehler ist es, die auf das eigene Amazon- oder sonstige Konten einzulösen, Wird ein Hoster hochgenommen und die Codes sind zurückverfolgbar, dann haben sie einen.

Ein anderer Punkt ist, wie man mit dem Geld umgeht. Damals, als ich vierstellige Beträge gemacht habe, war der größte Fehler, wenn man auf einmal eine sehr teure Uhr an seinem Handgelenk trägt. Dann kommen Nachfragen. Woher kommt das Geld, wenn man in der Lehre 300€ netto monatlich verdient. Da habe ich gelernt, lieber das Geld liegen zu lassen und langsam in den Kreislauf zu bringen.

Später mit den richtigen Kontakten kamen doch auch die richtigen Tipps. Wichtig ist es, mit dem Geld nicht zu prahlen. Zweitens man muss sich Wege suchen, wenn eine Steuerüberprüfung kommt und belegen, wie das eingenommene Guthaben zustande gekommen ist.

Außerdem: Man kann sich nicht ein 80.000€ Auto vor die Tür stellen, wenn man nur 8,50€ die Stunde verdient. Irgendwann steht vielleicht das Finanzamt vor Deiner Tür und fragt, woher Du das Geld hast. Wenn man die Einnahmen nicht belegen kann, werden die Sachen beschlagnahmt.

Wie genau jetzt die Geldwäsche abläuft, werde ich nicht erklären, aber es gibt Mittel und Wege.

Okay, mit solchen Interna habe ich auch nicht gerechnet. Wie viele TB an Daten hast Du zu Hause? Sind die Festplatten verschlüsselt?

Zuhause: zwei NAS mit insgesamt 9,8 TB von 16 TB.
Veschlüsselt ist alles.

Viel mehr pro Stunde als die meisten Uploader verdienen ja die Abuse-Agenturen wie fifthfreedom & Co. an Warez, und das unter dem Deckmantel des Urheberschutzes. Haben diese Unternehmen in Deinen Augen ihre Daseinsberechtigung? Wie schützt Du Dich als Uploader vor einem Abuse?

Diese Agenturen haben schon eine Daseinsberechtigung, schließlich müssen ja die Urheber auch geschützt werden. Aber teilweise nutzen diese auch illegale Methoden wie Botnetze etc. oder abusen Content, an dem sie keine Rechte besitzen. Vor einem Abuse (= Antrag auf Löschung von urheberrechtlich geschütztem Material) schützen kann man sich kaum, da die Bots von denen ziemlich gut sind. Da hilft nur eins gegen: Reuppen, reuppen und nochmals reuppen.

Also das Zeug immer wieder unter anderem Namen hochladen. Wurdest Du schon mal erwischt? Wie kam es dazu? Wie ging das Verfahren für Dich aus?

Ja, tatsächlich, damals im Zuge das FTP-Welt Busts.

Es gab eine Geldstrafe gegen Einstellung des Verfahrens. Ich glaube, das waren ein paar Tagessätze á 10€. Habe die Dokumente dazu nicht mehr. (Anmerkung der Redaktion: Damit stand unser Uploader alles andere als alleine da. 2005 wurden die ersten 15.000 Verfahren gegen die zahlende Kundschaft von ftp-welt.com eingeleitet, erst war von 45.000 Beschuldigten die Rede).

"Nach einem Bust hängen die Behörden wie eine Klette an Deinem Hals."

Würdest Du weiter machen, wenn man Dich erwischen würde?

Wenn ich heute erwischt werden würde, nein. Weil Du hast danach die Behörden wie eine Klette an Deinem Hals hängen.

Woher beziehst Du Deine Dateien? Auch von Affil FTP-Sites?

Gemischt, aber hauptsächlich geschlossene FTP-Server, aber weniger von den Release-Groups selber, weil man dort nur Access (= Zugriff) bekommt, wenn man selber dort Content liefert.

Der landet dann am Ende auf den Dumps, also wo so gut wie alles an Releases der Groups hinkommt. Von dort bekomme ich meinen Content her.

Wieviel Zeit verwendest Du am Tag für Deine Uploads und das Eintragen? Benutzt du Autotracker oder bevorzugst Du die Oldschool Handarbeit?

Täglich zwei Stunden, da das meiste mittlerweile Tools übernehmen. Nur Nachkontrolle wird gemacht und das nachgetragen, was die Tools nicht finden. Also ein Mix aus automatisch und Handarbeit.

Kaufst du auch Content, um ihn bereitzustellen?

Ja, wenn es den Content noch nicht gibt, wie bei alten Filmen.

Wo stehen Deine Upload Server? In welcher Größenordnung beläuft sich der Traffic?

Zwei Stück, einer in den Niederlanden und einer in Frankreich. Jeweils 1 gbit. Ca. 40-60 TB im Monat, dazu sagen aber Serverzentren kaum etwas.

Was wird denn generell am meisten geladen?

Pornos, danach Filme und Musik. Also wenn man neu anfangen will mit uploaden: Pornos gehen immer. The Internet is for porn ist kein Slogan.

Und was war die am häufigsten geladene Datei?

Gute Frage, damals auf 3dl oder iLoad haben sich die Downloads bei Top-Releases so um die 50.000 Downloads in der ersten Woche bewegt. Da war der Abuse aber auch noch nicht so extrem. Heute bei aktuellen Kinofilmen sind es bei mir so 1.000 Downloads am ersten Tag, wenn es in dieser Zeit nicht schon abused wurde. Meine meistgeladene Datei bei Share-Online, die noch online ist, steht bei 35.812 Downloads.

Das ist immer noch eine ganze Menge. Gibt es keine Probleme, wenn Account-Abuses hereinkommen und der Account beim Sharehoster dann gelöscht wird?

Bisher gab es keine, bis Uploaded kam. Und Rapidshare war damals schlimm, als sie mit Klagen überzogen wurden.

Aber ansonsten passiert kaum etwas. Das Schlimmste was passieren kann, das halt der Account gebannt wird und vielleicht dann noch Daten herausgegeben werden, was ich mir bei Uploaded mittlerweile gut vorstellen kann.

Notice & Take Down Verfahren: „ein Kampf zwischen Windrad und Vogel“

Ist die Abuse Rate groß bei Deinen Uploads? Und dann? Re-Upload oder nutzt Du einen anderen Sharehoster? Welche nutzt Du denn gerne? Und warum ausgerechnet diese?

Natürlich betrifft dies aktuelle Kinofilme, Filme von Constantin und Co., Serien von RTL und Pornos von allen großen Amilabels.

Musik wird sehr schnell (von den beauftragten Antipirateriefirmen per Notice and Take Down Verfahren) abused. Der Reupload folgt aber meist am selben Tag noch. Abusen und Reuppen ist wie ein Kampf zwischen Windrad und Vogel.

An welcher preDB hängst du?

IRC-Kanal vom FTP, preDB und xrel.

Wenn Du für Dritte arbeitest, musst Du einen Teil abdrücken, z.B. an den Seitenbetreiber?

Ich arbeite für niemanden und wenn eine Seite Geld will, ist sie nicht gut. Darauf würde ich mich auch nie einlassen.

Ausblick: Alles bewegt sich in Richtung Streams

In welche Richtung wird es in der Zukunft gehen, eher in Richtung Streams oder Downloads?

Ich glaube eher in Richtung Streams, da man diese sofort hat. Und wenn man in Zukunft auch noch Spiele oder Software streamen kann, werden Downloads kaum noch eine Rolle spielen.

Wird Kim Dotcom in die USA ausgeliefert? Welche Auswirkungen würde eine Verurteilung des Megaupload-Mitgründers haben?

Bisher wehrt er sich ja ganz gut. Ich denke, es wird nie eine Auslieferung geben. Wenn ja, eine Verurteilung würde kaum etwas ändern, die OCHs und Streamhoster stehen auch jetzt nach Jahren von Megaupload wie eine Festung. Nach dem Megaupload-Bust gab es zwar ein Massensterben von alten Größen wie Hotfile, Filesonic und Co., aber die OCHs blühen. Es gibt Tausende davon, wenn man nur mal auf wjunction.com schaut.

Wie siehst Du die Warez-Welt in fünf bis zehn Jahren?

Wenn es keine großen Busts (Razzien) gibt und keine Zensur, wird es so bleiben aber minimaler. Solange es keine legalen guten Angebote gibt in 5-10 Jahren, wird sich an der Verbreitung von Warez auch kaum etwas ändern.

Was glaubst Du, gibt es dann noch immer Streaming- oder Sharehoster?

Ja, bloß nicht in der Masse wie heute. Geld wird dort eine große Rolle spielen und die Möglichkeiten, Werbung zu schalten. Erst wenn man es schaffen würde, den One Click Hostern den Geldhahn komplett abzudrehen, nähern wir uns dem Ende.

Letzte Frage bevor die Sonne ganz weg ist und wir drohen uns zu erkälten: Wird dann das Internet komplett reguliert sein? Darf man dann überhaupt noch anonym surfen?

In den Ländern, wo ein Erdogan oder Putin regiert, wird die Zensur weiter stattfinden. Aber ich denke, in der EU wird es in nächsten 10-20 Jahren keine Regulierung geben. Und VPNs werden hier auch nicht verboten sein.

Ich hoffe es. Ich will kein Internet wie in China, der Türkei oder Russland.

Netzpolitischer Jahresrückblick 2017

Netzpolitischer Jahresrückblick 2017

Das Jahr 2017 brachte einige interessante neue Entwicklungen im Bereich der Netzpolitik. In der Summe war es wohl wieder einmal mehr Schatten als Licht, doch gab es auch einige erfreuliche Ereignisse zu verzeichnen. Einige Entwicklungen waren lang erwartet, andere kamen eher überraschend. Zeit, zurückzublicken auf ein ereignisreiches Jahr.

Chelsea Manning: frei, engagiert und laut

Das Jahr begann für die Bürgerrechts-Bewegung und die Unterstützer-Gemeindes von WikiLeaks sehr erfreulich. Als eine der letzten Amtshandlungen hatte der scheidende US-Präsident Barack Obama beschlossen, die Whistleblowerin Chelsea Manning frühzeitig aus dem Gefängnis zu entlassen. Statt den Rest ihrer 35-jährigen Haftstrafe zu verbüßen, kam die WikiLeaks-Informantin, die der Transparenz-Plattform zahlreiche Dokumente von US-Behörden zugespielt hatte, im April dieses Jahres frei.

Wenig überraschend angesichts ihrer vorherigen Versuche, schon aus dem Gefängnis medial die Stimme zu erheben, nutzte Manning die wiedergewonnene Freiheit, um öffentlich zu sprechen. Schon bald nach ihrer Entlassung wurde sie auf Twitter und Instagram aktiv. Auf diesen Plattformen gab sie Einblicke in ihre politischen Aktivitäten, aber auch in ihr Alltagsleben.

Manning setzte sich öffentlich für die Rechte der LGBTQ-Gemeinschaft und insbesondere für transsexuelle Menschen ein. Immer wieder forderte sie die Öffentlichkeit auf, die Rechte dieser Personen mehr zu achten und ihnen ein sicheres Umfeld zu bieten. Unter anderem nahm sie an mehreren „Gay Pride“-Veranstaltungen teil und postete immer wieder entsprechende Bilder und Slogans auf ihren Social-Media-Kanälen.

Daneben machte die Whistleblowerin aber auch deutlich, dass ihr Bürgerrechte und Transparenz nach wie vor am Herzen liegen. Sie betonte mehrfach die idealistischen Motive, die sie dazu gebracht hatten, als US-Soldatin Geheimdokumente an WikiLeaks weiterzugeben. Auch versuchte sie, einige Missverständnisse und Falschaussagen aufzuklären. So machte sie deutlich, dass sie von WikiLeaks keineswegs dazu aufgefordert wurde, Geheimdokumente zu beschaffen und weiterzugeben (https://www.washingtontimes.com/news/2017/jun/9/chelsea-manning-says-wikileaks-disclosures-werent-/). Entsprechende Aussagen waren von politischen Gegnern gestreut worden, um die Position WikiLeaks‘ als seriöse und schützenswerte journalistische Plattform zu untergraben. Auch betonte Manning, sie sei keineswegs eine Verräterin, sondern habe genau jene demokratischen Werte fördern und schützen wollen, die sie sich für ihr Land wünsche.

Donald Trump spaltet die (Online-)Welt

Kein Jahresrückblick wäre komplett ohne die Erwähnung des 45. US-Präsidenten Donald Trump (Republikaner), der Anfang des Jahres sein Amt antrat. Der Milliardär blieb seinem bereits aus dem Wahlkampf bekannten Stil treu – er beleidigte, rantete, provozierte und nahm es mit der Wahrheit nicht immer allzu genau. Schon zur Berühmtheit gebracht hat es Trumps Twitter-Account (https://twitter.com/@realdonaldtrump), wo der US-Präsident eine Menge umstrittener Aussagen traf, aber auch einige in Windeseile zu Memes mutierende Pannen erlitt (Covfefe, anyone?).

Bei allem Hang, sich über Trumps Exzentritäten und Missgeschicke lustig zu machen, hat seine Präsidentschaft natürlich auch eine ernste Seite. Minderheiten hatten es schwer in den USA und viele Menschen machen Trump für die Verschärfung gesellschaftlicher Dissenzen wie auch eine Verschlechterung der Diskussionskultur, offline wie auch im Internet, verantwortlich. Dass Trump es, anders als sämtliche Amtsvorgänger, mit der Transparenz weniger genau nahm und sich standhaft weigerte, seine Steuererklärung zu veröffentlichen, war da nur der Auftakt zu einem ereignisreichen Jahr.

Netzpolitisch trat Trump weniger auffällig in Erscheinung, sondern setzte lediglich die negative Tendenz fort, die in den USA schon seit Jahren zu verzeichnen ist. Die Netzneutra-

lität wurde unterminiert, die Überwachung der Telekommunikation weiter ausgebaut. Das ist (leider) eher Alltag.

Staatstrojaner auf dem Vormarsch

Nach wie vor aktuell blieb die Diskussion über den Einsatz sogenannter Staatstrojaner. Von Politik und Ermittlungsbehörden als unverzichtbares Werkzeug der Kriminalitätsbekämpfung angesehen, von Bürgerrechts-Aktivisten und IT-Sicherheits-Fachleuten gleichermaßen kritisiert, bleibt der Staatstrojaner umstritten.

Derzeit sieht es nicht so aus, als sei eine Einschränkung des behördlichen Trojaner-Einsatzes wahrscheinlich. Im Gegenteil wurde 2017 der Staatstrojaner-Einsatz sogar für Alltagskriminalität freigegeben. Das ist eine Abkehr von der zunächst vertretenen Linie, der Staatstrojaner sei lediglich für den Einsatz bei schweren Verbrechen und insbesondere Terrorismus vorgesehen. Allerdings ist eine derartige Ausweitung von Überwachungsmaßnahmen bereits des Öfteren vorgekommen.

Derweil waren die deutschen Behörden noch mit der Entwicklung eines eigenen Trojaners beschäftigt. Zugekaufte Versionen von Software-Unternehmen erwiesen sich mehrfach als mangelhaft und nicht verfassungskonform. Den Behörden wurde daher auferlegt, zukünftige Trojaner selbst zu programmieren. Das funktionierte jedoch zunächst mehr schlecht als recht. Nach einer ganzen Reihe von Misserfolgs-Meldungen und Verzögerungen hieß es gegen Jahresende jedoch, der Staatstrojaner „made by BKA“ sei beinahe fertig und solle noch 2017 zum Einsatz kommen. Ob diese Vorgabe tatsächlich eingehalten wurde, weiß die Öffentlichkeit bislang allerdings nicht.

NSAUA stellt die Ermittlungen ein

Der NSA-Untersuchungsausschuss war mit der Aufgabe betraut, Grundrechts-Verstöße und Kompetenzüberschreitungen der internationalen Geheimdienste und die Kooperation der deutschen Behörden insbesondere mit der NSA zu untersuchen. Im Laufe seiner mehrjährigen Arbeit förderte der Untersuchungsausschuss einige sehr interessante Informationen aus der Geheimdienstwelt zutage. An anderer Stelle blieb die Ausschuss-Arbeit jedoch notgedrungen an der Oberfläche und es ist davon auszugehen, dass einige interessante Geheimnisse im Verborgenen blieben (http://www.netzpiloten.de/nsa-untersuchungsausschuss-symbolpolitik/). Von Anfang an war klar, dass die Zuständigen befürchteten, es sich mit ihren amerikanischen Verbündeten zu verscherzen, und dem Ausschuss daher die Arbeit mit Samthandschuhen verordneten.

Im Herbst wurde die Arbeit des NSA-Untersuchungsausschusses offiziell beendet. Das wenig überraschende Fazit: zur Rechenschaft gezogen für die aufgedeckten Überwachungs-Aktivitäten wird wohl niemand. Die Begründung: in den meisten der Beweismittel, insbesondere den Snowden-Dokumenten, seien lediglich technische Möglichkeiten und grundsätzlich vorhandene Überwachungsprogramme dokumentiert. Konkrete Grundrechtsverstöße seien damit nicht nachweisbar. So bleibt ein gewisses Gefühl der Enttäuschung zurück.

Kontroverse ums Netzwerkdurchsetzungsgesetz

Viel diskutiert wurde im Jahr 2017 das Netzwerkdurchsetzungs-

gesetz. Dieses etwas sperrig bezeichnete Gesetz verpflichtet die Betreiber von Online-Diensten, strafbare Inhalte innerhalb einer Frist zu löschen. Anderenfalls drohen den Verantwortlichen empfindliche Bußgelder. So sollen insbesondere verhetzende Äußerungen und Hass-Postings eingedämmt werden.

Von Anfang an zog das Netzwerkdurchsetzungsgesetz viel Kritik auf sich. Zwar ist das Problem hasserfüllter oder auch manipulativer Online-Postings zweifellos real und in den letzten Jahren größer geworden. Das Netzwerkdurchsetzungsgesetz aber erschien vielen Menschen nicht als das geeignete Mittel zur Bekämpfung dieser Probleme. Kritiker befürchten vor allem, dass es zu einer sogenannten Überregulation kommt, also aus Angst vor Sanktionen auch rechtlich unproblematische (aber womöglich kontroverse oder unpopuläre) Inhalte gelöscht werden.

Trotz dieser Bedenken wurde das Netzwerkdurchsetzungsgesetz jedoch im Juli vom Bundestag beschlossen (https://tarnkappe.info/bundestag-beschliesst-netzwerkdurchsetzungsgesetz/). Am Jahresende trat es dann offiziell in Kraft (https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl117s3534.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s3534.pdf%27%5D__1510595767569). Gegnern des Netzwerkdurchsetzungsgesetzes bleibt also nur noch, auf eine Aufhebung oder zumindest eine Anpassung des Gesetzes hinzuarbeiten.

WannaCry sorgt für Diskussion über Umgang mit Software-Exploits

Auf den ersten Blick eher technisch, aber mit großen Auswirkungen auch für das Verhalten der Behörden, ist das Thema Exploits. Unter einem Exploit verstehen IT-Sicherheits-Fachleute eine dokumentierte Software-Schwachstelle nebst Quellcode zu deren Ausnutzung. Die begehrteste Form ist der sogenannte Zero-Day-Exploit: Eine Schwachstelle, die dem Hersteller der Software noch nicht bekannt ist und für die somit kein Patch existiert.

Schon seit längerem ist bekannt, dass einige Behörden solche Exploits in privaten Datenbanken sammeln. Das wurde von Sicherheits-Expertinnen und -Experten immer wieder kritisiert. Ihre Argumentation: jede Schwachstelle, die die Behörden entdecken, könnte ebenso auch von Kriminellen gefunden und zu destruktiven Zwecken ausgenutzt werden. Verantwortungsvoll wäre daher, den Herstellern derartige Sicherheitslücken umgehend zu melden (wie es viele Sicherheits-Fachleute im Rahmen der „Responsible Disclosure“ seit Jahren praktizieren). Die Behörden allerdings sammeln Exploits, um mit ihrer Hilfe politische Gegner angreifen oder Staatstrojaner auf der Software Verdächtiger platzieren zu können.

Mehrere spektakuläre Vorfälle bewiesen allerdings, dass die Warnungen der Skeptikerinnen und Skeptiker keineswegs reine Panikmache sind. Im Mai 2017 infizierte der Erpressungs-Trojaner WannaCry eine gigantische Anzahl von IT-Systemen in aller Welt. Darunter waren auch zu den kritischen Infrastrukturen zählende Rechner – öffentliche Transportmittel, mehrere Krankenhäuser und eine Reihe namhafter Unternehmen waren betroffen. Die bei WannaCry ausgenutzte Schwachstelle, so stellten Fachleute schnell fest, war der NSA schon seit Jahren bekannt, wurde von dieser aber mit Absicht geheim gehalten (http://www.netzpiloten.de/wannacry-exploit-policy-behoerden/). Um die Peinlichkeit noch zu vergrößern, stellte sich heraus, dass die Informationen über den genutzten Exploit von Angreifern aus einer NSA-eigenen Datenbank entwendet worden waren.

Nach WannaCry gab es noch einige kleinere, aber vom Prinzip her ähnlicher Vorfälle. Zwar verschwand das Thema des behördlichen Umgang mit Exploits bald wieder aus der Mainstream-Berichterstattung. Es ist aber davon auszugehen, dass es in der Fachwelt gerade heiß diskutiert wird.

Fazit

Wie schon in den letzten Jahren gab es ein wenig Licht, vor allem aber viel Schatten bei der Netzpolitik zu verzeichnen. Große Überraschungen blieben aus, aber an mehreren Stellen wurden die Rechte von Internet-Nutzerinnen und -Nutzern weiter eingeschränkt. Vor allem aber haben Aktivistinnen und Aktivisten eine Reihe von Herausforderungen und Aufgaben erhalten, denen sie sich im Kampf um ein freies Internet stellen müssen. Auch das Thema IT-Sicherheit bleibt auf der Agenda weit oben.

„Now You Know. Vier Jahre Snowden“ Hörbücher kostenlos verfügbar

Constanze Kurz und Frank Rieger haben etwa 50 ihrer Beiträge über Edward Snowden und die Massenüberwachung durch Geheimdienste ausgewählt, um sie nun als Hörbücher kostenlos zum Download anzubieten. Über 40 Sprecher haben sich freiwillig an der Aktion beteiligt.

Kurz notiert: Die beiden prominenten CCC-Mitglieder Constanze Kurz und Frank Rieger haben ihre 50 besten Veröffentlichungen aus diversen Zeitungen und Zeitschriften herausgesucht, um sie vorlesen zu lassen. Alle Beiträge sind seit ein paar Tagen einzeln, nach Jahreszahlen sortiert oder gesammelt, zum Download verfügbar.

Die Ankündigung der Autoren lautet wie folgt

„Seit dem Juni 2013, als die ersten Veröffentlichungen aus den Snowden-Unterlagen begannen, haben wir in Zeitungen, Zeitschriften und Büchern zahlreiche Texte zu diesem Themenkomplex geschrieben: in der FAZ und FAS, im SPIEGEL, in Buchbeiträgen. Davon haben wir etwa fünfzig ausgesucht, um den Rückblick auf viele Details und die jeweils aktuellen Reaktionen auf die zahlreichen enthüllten NSA– und GCHQ-Programme, die politischen Folgen und die Stimmung in der Öffentlichkeit zum Thema Massenüberwachung zu wagen.

Dank der Mitarbeit von vielen Freiwilligen, die uns im Tausch für ein „Arbeitsfrei“-Hardcover ihre Stimme geliehen haben, können wir nun akustisch zurückblicken auf mehr als vier Jahre Snowden-Veröffentlichungen.

Über vierzig freiwillige Sprecher haben sich beteiligt, die in jeweils ihrer eigenen Ausdrucksweise und Interpretation unsere Texte lesen. Zusammen ergeben die vielen Lesungen ein umfangreiches Hörbuch. Wir haben noch einen einleitenden Text aufgenommen und darin die vier Jahre Snowden-Veröffentlichungen aus unserer Sicht reflektiert und kommentiert.

Die eingesprochenen Texte können als vollständige Datei oder in Häppchen um die zwanzig Minuten heruntergeladen werden. Außerdem gibt es noch Jahresversionen, die zwischen einer Stunde und anderthalb lang sind. Die Gesamtdatei beginnt mit unserem Intro, gefolgt von den Texten vom Juni 2013 bis März 2017, sie umfasst fünfeinhalb Stunden.“

Hier geht es zum Download. Die vorgelesenen Artikel können wahlweise im Format MP3 oder OGG bezogen werden. Leider hat sich bisher noch niemand die Mühe gemacht, die Hörbücher via P2P anzubieten, das würde sich bei der Datenmenge durchaus anbieten.

Kinox.to: Betrüger verschicken Fake-Abmahnungen wegen illegalem Streaming

Die Verbraucherzentrale warnt derzeit vor massenhaft verschickten, falschen Abmahn-E-Mails. Eine angebliche Anwaltskanzlei fordert darin hohe Geldbeträge, die auf ein ausländisches Konto zu überweisen sind.

Konnten sich die Nutzer von illegalen Streaming-Seiten noch vor einem Urteil des Europäischen Gerichtshofes vom 26.04.2017 (Az.: C-527/15) in Sicherheit wiegen, hat sich dies nun geändert. Der EuGH kam zu dem Ergebnis, dass der Nutzer, der urheberrechtswidrige Inhalte streamt, sich nicht da-

rauf berufen kann, dass er damit eine vom Gesetz (Art. 5 der Infosoc-Richtlinie, in Deutschland umgesetzt in § 44a UrhG) privilegierte Zwischenspeicherung vornimmt. Der Nutzer, der urheberrechtswidrige Inhalte streamt, verletzt also selbst das Urheberrecht, jedenfalls dann, wenn er sich freiwillig und in Kenntnis der Sachlage Zugang zu einem kostenlosen und nicht zugelassenen Angebot geschützter Werke verschafft. Real sind Abmahnwellen allerdings unwahrscheinlich, da in den meisten Fällen bisher die IP-Adresse nicht gespeichert wird.

Gerade den Umstand, dass Streaming nun als Urheberrechtsverletzung gilt, machen sich vermehrt auch Betrüger zunutze. So landen seit kurzem gefälschte Anwaltsschreiben in zahlreichen E-Mail-Postfächern, die finanzielle Entschädigungen für Urheberrechtsverletzungen auf Kinox.to verlangen. Cyberkriminelle versuchen auf diese Weise mit authentisch wirkenden Abmahnungen Geld zu verdienen.

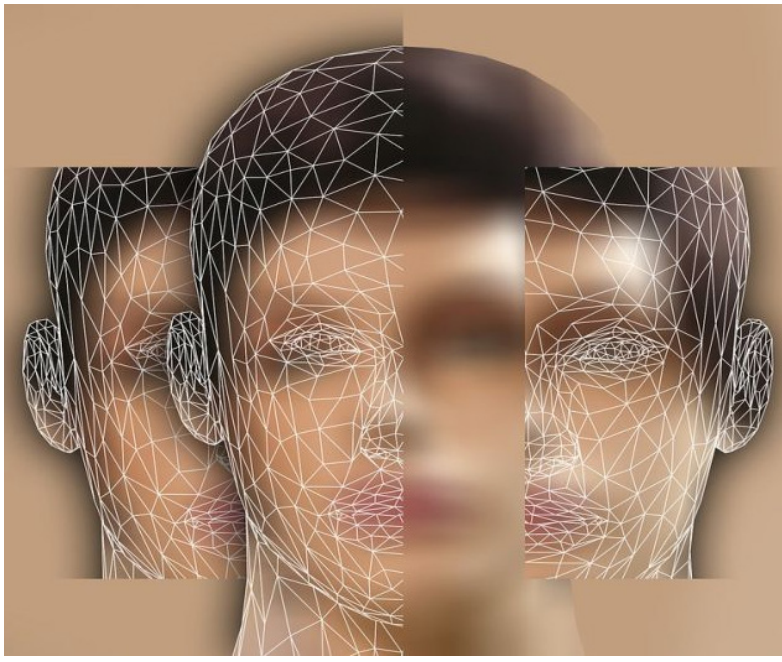
Die Verbraucherzentrale Niedersachsen warnt aktuell vor einer Serie von kostenpflichtigen Abmahnungen durch eine Berliner Kanzlei, wobei der Name der Kanzleiadresse des Rechtsanwaltes (RA) Hofmann missbräuchlich verwendet wird. In einer E-Mail werden für das angeblich illegale Ansehen von Filmen auf der Plattform Kinox.to rund 370 Euro Gebühren verlangt – zu zahlen auf ein Konto in Großbritannien. Die Kanzlei benennt in dieser Mail nicht, welche Filme oder Serien die Verbraucher geschaut haben sollen. Laut Verbraucherzentrale handelt es sich dabei um unberechtigte Abzocke.

Die Empfehlung der Verbraucherzentrale an die Betroffenen lautet: “Zahlen Sie nicht. Es handelt sich um Abzocke. Erstatten Sie Anzeige bei der Polizei.”

Gesichtserkennung am Bahnhof Südkreuz geht in die Verlängerung

Bundesinnenminister Thomas de Maizière (CDU) hat am Freitag (15.12.2017) bekannt gegeben, dass der Test zur umstrittene Gesichtserkennung am Bahnhof Südkreuz um weitere sechs Monate verlängert wird, wie Reuters berichtet. Eigentlich sollte das Pilotprojekt bereits im Januar enden.

Mit einer bisher positiven Bilanz wurde das Projekt der Gesichtserkennung am Bahnhof Südkreuz verlängert. So lobte Bundesinnenminister Thomas de Maizière die Zwischenergebnisse: „Bei



70 Prozent und mehr haben wir eine positive Erkennung der Gesuchten – das ist ein sehr guter Wert […] Das ist besser als ich erwartet habe und die meisten Kritiker auch”, sagte de Maiziere am Freitag bei einem Vor-Ort-Besuch. Nun solle der Test modifiziert und noch praxisnaher gestaltet werden, nämlich mit Vergleichsbildern schlechterer Qualität für den Abgleich mit der Datenbank. „Erst dann kann man wirklich präzise einschätzen, wie wirksam ein solches Fahndungsinstrument ist“, meinte de Maizière.

Seit dem 1. August 2017 sind mehrere Kameras in drei Bereichen des Umsteigebahnhofs Südkreuz – je eine an einem Ein- und Ausgang sowie an einer Rolltreppe im Einsatz – für Computerprogramme zur Gesichtserkennung. 300 Testpersonen beteiligen sich freiwillig an dem Projekt. Die Sicherheitsbehörden begründen ihr Vorhaben auch damit, dass mögliche Gefährder vor einem Anschlag erkannt werden könnten.

Datenschützer kritisieren hingegen eine solche Überwachung mit Argumenten, wie: durch diese Technik würden die Persönlichkeitsrechte von Menschen verletzt, der Überwachungsstaat weite sich aus. Der Deutsche Anwaltverein bemängelte am Freitag erneut das Fehlen einer Rechtsgrundlage. “Wenn massenhaft Gesichter von unbescholtenen Bürgerinnen und Bürgern an Bahnhöfen gescannt werden, dann greift der Staat schwerwiegend in Grundrechte ein”, kritisierte der Verein. Zum Start des Testlaufs hatte sich auch Deutschlands oberste Datenschützerin Andrea Voßhoff ablehnend geäußert: “Sollten derartige Systeme einmal in Echtbetrieb gehen, wäre dies ein erheblicher Grundrechtseingriff.”

Die Zwischenergebnisse versprechen nach Ansicht des Bundesinnenministers: „einen erheblichen Mehrwert für die Fahn-

dung nach Terroristen und Schwerverbrechern“. Im Polizeialltag seien die Fahndungsfotos aber in der Regel deutlich unschärfer als diese Porträts, gibt de Maizière zu bedenken. Deswegen werde nun in der zweiten Phase getestet, wie gut das automatisierte Verfahren mit qualitativ minderwertigen Fotos funktioniert. Wurden bisher die Gesichter der Bahnhofsbesucher, die sich zuvor für den Test angemeldet hatten, mit qualitativ hochwertigen Fotos der Testpersonen abgeglichen, so sollen in dem nun zusätzlichen halben Jahr ab Februar schlechtere Fotos als Grundlage des Abgleichs dienen.

De Maiziere erklärtes Ziel ist es, abhängig von den Ergebnissen beim Berliner Pilotprojekt, das System flächendeckend einzuführen: “mindestens im Bereich des Innenministeriums – also bei Bahnhöfen und Flughäfen.” Er sei aber zudem bereit, mit den Ländern über die Einführung im Personennahverkehr zu sprechen. Datenschutzrechtliche Bedenken sind nach seiner Überzeugung “ausgeräumt”. Verfassungsrechtliche Bedenken könne er sich schlecht vorstellen, wenn man nach Terroristen und Schwerverbrechern fahnde: “Die Bedenken würden dann höher, wenn man nach jedem Ladendieb fahndet.” Die Verhältnismäßigkeit müsse bei der Überwachung stets geprüft werden.

Thomas de Maizière: Gesetzesänderung für Lauschangriffe auf Autos, Computer und Smart-TVs

Wie das Redaktionsnetzwerk Deutschland (RND) berichtet, will der geschäftsführende Bundesinnenminister Thomas de Maizière (CDU) mit einer Gesetzesänderung die Industrie zum Öffnen digitaler Einfallstore von privaten Autos, Computern und Smart-TVs für das Ausspionieren im Rahmen der Strafverfolgung verpflichten. Das gehe aus einer Beschlussvorlage des Bundes zur Innenministerkonferenz in der kommenden Woche in Leipzig hervor. Der Antrag ist mit „Handlungsbedarf zur gesetzlichen Verpflichtung Dritter für Maßnahmen der verdeckten Informationserhebung nach §§ 100c und 100f StPO“ überschrieben.

Zur Innenministerkonferenz, die kommende Woche in Leipzig stattfindet, strebt der Bund eine weitreichende Gesetzesänderung an: Thomas de Maizière will insbesondere Konzernen und Produzenten von digitalen Sicherungssystemen eine Auskunfts- und Mitteilungsverpflichtung erteilen. So sollen deutsche Sicherheitsbehörden für eine gezielte Überwachung exklusive Zugriffsrechte auf private Tablets, Computer, Bord-Computer in Autos, Smart-TVs und alle anderen Geräte im „Internet der Dinge“ erhalten. De Maizière will auf diesem Weg den sogenannten Lauschangriff durch den „Einsatz technischer Mittel gegen Einzelne“ drastisch erweitern. Die geplante Gesetzesänderung soll “technikoffen” formuliert werden, “um eventuelle künftige Entwicklungen mit erfassen zu können”. Demnach wären Lauschangriffe demnächst überall dort möglich, wo Geräte mit dem Internet verbunden sind. Voraussetzung für diesen sogenannten Lauschangriff bliebe ein richterlicher Beschluss.

Den Anlass zu dieser Maßnahme geben Probleme bei der „verdeckten Überwindung von Sicherheitssystemen“. So falle es Ermittlern und Geheimdiensten zunehmend schwer, Abhörwanzen in Autos einzubauen und zu verstecken, weil die Sicherungssysteme so gut seien, heißt es aus Kreisen des Bundesinnenministeriums. Die modernen Schließanlagen von Fahrzeugen wären mittlerweile so schützend abgesichert, dass ihre Besitzer schon bei kleinsten Erschütterungen über Messenger-Dienste informiert würden. Laut Spiegel-Informationen seien seit vergangenem Jahr in 25 Fällen Überwachungsmaßnahmen daran gescheitert. De Maizière strebt mit der geplanten Gesetzesänderung an, diese automatischen Mitteilungen zu unterbinden. Zudem will er der Industrie vorschreiben, ihre Programmierprotokolle offenzulegen. Die Justizminister sollen eine entsprechende Rechtsänderung zeitnah prüfen.

Außerdem will de Maizière eine Ermächtigung für die Sicherheitsbehörden, im Krisenfall auch private Rechner herunterfahren zu können. So würde ein „Fachkonzept zum Takedown von Botnetzen“ vorsehen, Sicherheitsbehörden künftig zu gestatten, private Daten abzugreifen, um Endkunden rechtzeitig zu warnen, wenn Hackerangriffe vorliegen. Falls Online-Provider eine Zusammenarbeit ablehnen, sind weitreichende Strafen vorgesehen.

Die vorgesehenen Maßnahmen stoßen auf weitreichende Kritik: Uli Grötsch, SPD-Innenexperte und bayerischer Generalsekretär seiner Partei, verweist auf die wichtige Balance zwischen Freiheit und Sicherheit: “Mehr Eingriffe und Überwachung bedeutet nicht automatisch mehr Sicherheit.”

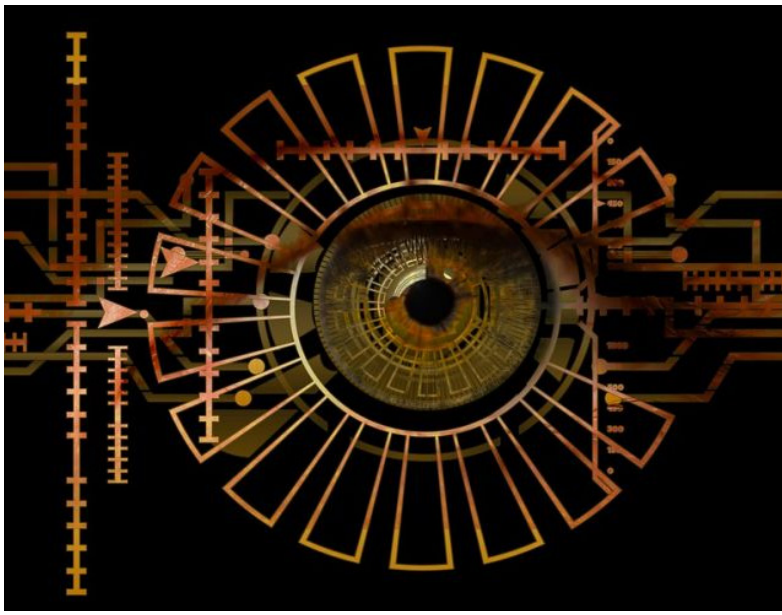
Konstantin von Notz, stellvertretender Fraktionsvorsitzender der Grünen im Bundestag, lehnt das Konzept ab mit den Worten: “Die Pläne des geschäftsführenden Innenministers lesen sich wie ein Orwellscher Albtraum. Bald werden alle Wohnungen der Bundesrepublik mit Geräten ausgestattet sein, die potenzielle Wanzen sind. Die physische Hürde eines großen Lauschangriffs fällt weg. Wir müssen uns gut überlegen, ob wir – mit zwei Diktaturen in der jüngeren Geschichte – in einem Land leben wollen, in dem es keine privaten Rückzugsorte mehr gibt und der Staat alles darf, was technisch möglich ist.”

Marc Fliehe vom Verband der Technischen Überwachungsvereine (VdTÜV), meint dazu, selbst wenn die “gezielte Schwächung der Sicherheitsarchitekturen” der Strafverfolgung dienen solle, spiele sie auch Hackern in die Hände. Ein potenzielles Angriffsziel könne nicht zwischen einem staatlichen oder einem kriminellen Akteur unterscheiden. “Solch tiefgreifenden Gesetzesänderungen brauchen aber gesellschaftliche Diskurse und eine Beteiligung von Unternehmen und Nichtregierungsorganisationen.”

Bernhard Rohleder, Hauptgeschäftsführer des Branchenverbands Bitkom äußert sich gegenüber dem Spiegel: “In Zukunft werden alle Geräte, Gebäude und im Übrigen auch fast alle Menschen mit dem Internet verbunden sein. Bei dem Vorstoß des Ministers gehe es also darum, “staatlichen Zugriff auf schlichtweg alles, jedes und jeden zu erhalten. Ein so weitreichender Eingriff dürfe “nicht handstreichartig” erfolgen, so Rohleder. “Wir brauchen eine schnelle, aber auch sorgfältige Abwägung darüber, wo wir die Privatsphäre im Zweifelsfall der allgemeinen Sicherheit opfern – und wo wir ganz bewusst allgemeine Sicherheitsrisiken eingehen, um die Privatsphäre Einzelner zu schützen.”

Für Frank Rieger, Sprecher des CCC, sind die Pläne ein „Frontalangriff auf die digitale und physische Sicherheit aller Bürger“. Der Zwang zu Software-Hintertüren bedeute, dass in Zukunft jedes Alltagsgerät ganz legal aus der Ferne zu einer Geheimdienst-Wanze gemacht werden könne: „Und ein Zugriff auf die IT eines modernen Autos bedeutet Gefahr für Leib und Leben: ein buchstäblicher Kill-Switch.“

Volker Tripp von der Digitalen Gesellschaft warnt, dass es bei Umsetzung des Vorhabens „keinerlei Privatsphäre, keinerlei Rückzugsraum und keinerlei Unbefangenheit“ mehr gebe. Die Pläne seien die „Antithese zu einem freiheitlichen und demokratischen Rechtsstaat“ und widerspreche diametral dem Menschenbild des Grundgesetzes. Den Akteuren im politischen Feld müsse spätestens jetzt klar sein, dass sie sich im Falle einer Koalition mit der CDU womöglich zum Steigbügelhalter bei der Einführung eines allumfassenden Überwachungsstaates machen würden.



Australien plant Verkauf biometrischer Daten

Die australische Regierung plant ein Pilotprojekt über den Verkauf biometrischer Daten an private Unternehmen. Gegen eine Gebühr erhalten diese Zugang zu einer vom Staat betriebenen Gesichtserkennungs-Datenbank, berichtet The Guardian.

Der australische Generalstaatsanwalt verhandelt derzeit mit Telekommunikationsunternehmen über die Nutzung der Daten auch im privaten Bereich. Dabei soll ein Service, der staatliche Face Verification Service (FVC), den derzeit das Justizministerium nutzt, künftig auch Privatunternehmen zur Verfügung gestellt werden. Geplant ist, dass authentifizierte Nutzer aufgrund ihnen vorliegender Bilder, wie Gesichter ihrer Kunden, über eine Schnittstelle nachfragen können, ob das Foto eine bereits vermutete Person zeigt. Die Bilder werden an ein sogenanntes „Biometric Interoperability Hub“ gesandt, dort werden sie mit Bildern aus der Regierungsdatenbank abgeglichen. Daraufhin bekommen die Firmen ein “Ja” oder “Nein” als Antwort. Ein direkter Zugriff auf die Daten bleibt den privaten Unternehmen jedoch verwehrt. Besonders starkes Interesse an einer Nutzung der Datenbank

zeigen bereits Finanzinstitute, aber ebenso sollen Banken an den biometrischen Daten australischer Bürger interessiert sein. Laut Informationen von Engadet, sollen 2018 erste Tests starten.

Vorgesehen ist die Verwendung der Daten zur Betrugsbekämpfung oder bei Identitätsdiebstahl. Private Unternehmen sollen die Daten jedoch nur mit entsprechender Zustimmung der betroffenen Personen nutzen dürfen und darüber hinaus nachweisen, dass sie nicht gegen australische Datenschutzgesetze verstoßen.

An einem ähnlichen staatlichen Projekt können Firmen bereits derzeit teilhaben, dem des seit 2014 von der australischen Regierung angebotenen Verifikationsdienstes für Dokumente (Document Verification Service, DVS). Dabei werden Daten auf Führerscheinen, Reisepässen, Visas oder Gesundheitskarten mit staatlichen Datenbanken abgeglichen. Allein im Jahr 2016 wurden auf diese Art mehr als 15,5 Millionen Transaktionen durchgeführt. Für die staatlichen Stellen bedeutete dies beträchtliche Mehreinnahmen, da die privaten Firmen für den Datenabgleich bezahlen müssen. Das geplante Projekt soll dabei ähnlich ablaufen, auch der FVS könnte dem Staat so zusätzliche Gelder einbringen. Derzeit ist bereits die Hälfte der australischen Bevölkerung in der biometrischen Datenbank erfasst, die Rate soll in den nächsten Jahren auf 85 Prozent steigen. Das Land setzt besonders bei der Passagierabfertigung an Flughäfen auf biometrische Systeme.

Kritik an diesem Pilotprojekt kommt vor allem von den Datenschützern. So meint Monique Mann von der australischen Privacy Foundation, wenn die Erbringung von Dienstleistungen, wie eine Kontoeröffnung, abhängig gemacht werden von einer freiwilligen Zustimmung, könne man kaum mehr von Freiwilligkeit sprechen. Ferner könne das Regierungsprogramm dazu führen, dass private Unternehmen ihre eigenen Gesichtserkennungs-Datenbanken aufbauen, denn sind die Daten einmal im Umlauf, wäre es schwierig zu ermitteln, mit wem sie geteilt und zu welchem Zweck sie genutzt wurden.

Telegram sperrt Piraten-Kanal

Roskomnadsor, der Föderale Dienst für die Aufsicht im Bereich der Kommunikation, Informationstechnologie und Massenkommunikation, bewilligt und beaufsichtigt Massenmedien und kann zudem auch Internet-Seiten in Russland blockieren lassen. Die Aufsichtsbehörde, mit Dienstsitz in Moskau, wurde im Jahr 2008 gegründet, im Oktober 2017 wurde durch

sie ein Dienst eingerichtet, der es Rechteinhabern ermöglicht, Copyrightverstöße im Netz zu melden mit dem Ziel, Maßnahmen zu ergreifen, um den Zugang zu illegalen Inhalten im Internet einzuschränken. Aufgrund dessen hat man den Messengerdienst dazu aufgefordert, entsprechende Inhalte vom Netz zu nehmen, berichtet die russische Nachrichtenagentur TASS.

Gegen das zur Verfügung stellen von urheberrechtlich geschütztem Content wird Telegram künftig demnach vorgehen. So hat: “Der Telegram-Messenger zum ersten Mal einen Kanal geblockt, der geschützte Audio-Inhalte unter Verletzung der Urheberrechte teilte. Wir werden uns im Kampf für einen legalen Inhalt zusammenschließen”, schrieb Roskomnadsor.

Bereits im Sommer stimmte Telegram-Gründer Pavel Durov zu, mit dem Dienst zu kooperieren auf eine Anfrage von Roskomnadzors Chef Alexander Scharow. Durov sicherte eine Zusammenarbeit unter dem sogenannten Anti-Terror-Paket (auch bekannt als Jarowaja-Gesetze) zu, allerdings werde man keinen Zugriff auf die Nachrichten-Inhalte der Nutzer gewähren.

Session-Replay: Beliebte Webseiten überwachen Tastatureingaben ihrer Nutzer

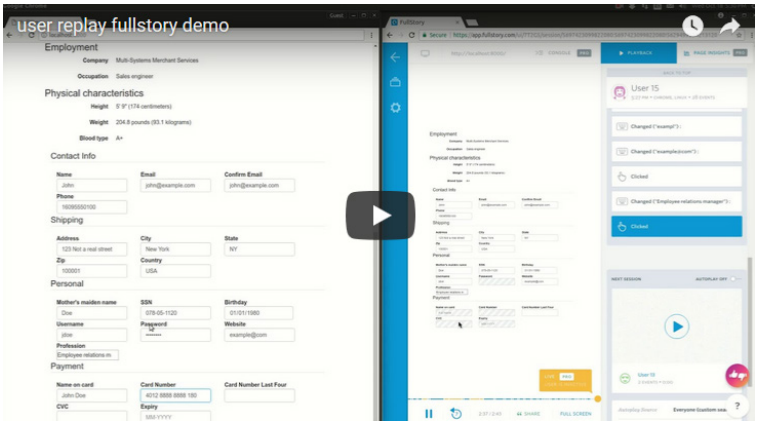
Forscher vom Centre for Information Technology Policy (CTIP) an der Princeton Universität haben im Rahmen einer aktuellen Studie herausgefunden, dass mindestens 482 der weltweit 50.000 beliebtesten Webseiten sogenannte “Session Replay”-Skripte verwenden, die sowohl dazu dienen, Mausbewegungen und Scrollverhalten der Nutzer aufzuzeichnen, als auch sämtliche Tastatureingaben auf der Webseite in Echtzeit zu erfassen, berichtet “Motherboard”.

Für ihre Studie hat sich ein Team von Sicherheitsexperten, Steve Englehardt, Gunes Acar und Arvind Narayanan, auf sieben der populärsten Session-Replay-Anbieter konzentriert, darunter FullStory, SessionCam, Clicktale, Smartlook, UserReplay, Hotjar und Russlands beliebteste Suchmaschine Yandex. Sie erstellten Testseiten und installierten Session-Replay-Skripte von sechs der sieben Unternehmen. Ihre Ergebnisse zeigten, dass mindestens eines dieser Skripte von 482 der weltweit 50.000 besten Websites gemäß Alexa-Ranking, verwendet wird.

Beunruhigend dabei ist, dass die Replay-Skripte gerade auch solche sensible Informationen, wie Kreditkarten-Daten, Passwörter oder Gesundheitsinformationen sammeln und an die Anbieter von „Session Replay"-Software übermitteln. Letztlich verhalten sich die Seiten wie ein Keylogger, der alle Eingaben des Nutzers speichert. Einige der Unternehmen, die diese Software anbieten, wie FullStory, entwerfen Verfolgungsskripte, die es den Websitebesitzern sogar erlauben, die erfassten Aufzeichnungen mit der tatsächlichen Identität eines Benutzers zu verknüpfen. Im Backend sehen Unternehmen, dass ein Benutzer mit einer ihm zugeordneten E-Mail oder einem bestimmten Namen verbunden ist. Es könnten sensible Daten sogar auch dann erfasst werden, wenn sie gar nicht abgeschickt wurden. Zudem werden diese Skripte üblicherweise von Drittanbietern geliefert, denen so auch direkter Zugriff auf die Daten ermöglicht wird. Die Forscher stellen die Rechtmäßigkeit der Datensammlung ohne Einwilligung der Nutzer in Frage.

Die Sicherheitsexperten veröffentlichten eine Liste von Websites, die Scripts von Anbietern der „Session Replay"-Software zum Einsatz bringen, jedoch weisen sie darauf hin, dass dies nicht notwendigerweise bedeutet, dass Daten von den aufgeführten Seiten auch real aufgezeichnet und an die Drittanbieter übermittelt werden, oftmals werden Session-Replay-Skripte einfach nur zu Analyse- und Debugging-Zwecken genutzt. Auch die einzelnen Möglichkeiten der Skripte weichen stark voneinander ab. Der russische Tech-Konzern und Suchmaschinenanbieter Yandex benutzt ein Skript, das von Haus aus wirklich alle eingegebenen Daten mitschneidet. Das besagte Skript befindet sich zudem auf vielen anderen Webseiten – womit die Informationen wieder zu Yandex gelangen. Allerdings, so betonen die Forscher, erfolgt die Datenübertragung zum Teil unverschlüsselt und eröffnet den Weg für Man-in-the-Middle-Angriffe.

Das Sicherheitsteam informiert, dass die von ihnen gefundene Anzahl der 482 Webseiten, auf denen Session Replay im Einsatz ist, das absolute Minimum an betroffenen Webseiten darstelle, da solche Skripte nicht immer einfach aufzuspüren sind. Eine Vielzahl von Seiten weist nach Angaben der Sicherheitsspezialisten Anzeichen für Session-Replay-Skripte auf, wobei zu den Betreibern auch viele namhafte Unternehmen gehören. Als Beispiele nannten sie die Websites von HP, Intel, Lenovo, Norton und Opera, des Pay-TV-Senders Sky, Samsung, Reuters, des britischen „Telegraph" sowie die von Russland aus betriebene Nachrichtenseite "Sputniknews". Ebenso soll bei dem russischen Facebook-Pendant VK.com Session-Replay zum Einsatz kommen. Zu den Websites gehören auch von deutschen Nutzern oftmals besuchte Webauftritte, wie die von Adobe, WordPress, Microsoft, Spotify, Skype, Evernote oder IBM.



Seit die Princeton-Forscher ihre Studie veröffentlicht haben, reagierten einige der solcherart kritisierten Seitenbetreiber bereits. Demnach hat der Bekleidungshersteller Bonobos ein Skript von seinen Seiten entfernt, das die vollständigen Kreditkartendaten der Nutzer erfasst und an den Skript-Anbieter FullStory wei-

tergegeben hatte. Die US-Drogeriekette Walgreens gab ebenso an, nun keine Daten mehr an den Session-Replay-Anbieter Full Story weiterzureichen, wie bisher üblich, die Details zu Medikamentenverschreibungen und Krankheiten der Kunden.

The Pirate Bay: Oberster Gerichtshof bestätigt Netzsperren zu Torrent-Links

In einem Urteil vom Oktober stellt der Oberste Gerichtshof (OGH) Österreichs fest, dass die Netzsperre gegen The Pirate Bay rechtens ist. Laut OGH ist bereits das "Bereitstellen und Betreiben einer BitTorrent-Plattform mit dem Zweck des Online-Filesharing" eine "öffentliche Wiedergabe" geschützter Inhalte. Der Fall wurde von einer Verwertungsgesellschaft eingereicht, die rund 3.000 Künstler vertritt, darunter die Beatles, Justin Bieber, Eric Clapton, Coldplay, David Guetta, Iggy Azalea, Michael Jackson, Lady Gaga, Metallica, George Michael, One Direction , Katy Perry und Queen berichtet torrentfreak.

Im Mittelpunkt des Verfahrens stand die Frage, ob "Urheberrechtsverletzungen im Internet mittels BitTorrent-Plattformen, auf denen selbst zwar keine urheberrechtlich geschützten Werke zum Abruf gespeichert sind, deren Dateien (Torrents) aber als Wegweiser dienen und es Nutzern ermöglichen, urheberrechtlich geschützte Werke auszutauschen und abzurufen, mit Sperrverfügungen gegen Zugangsvermittler (Access-Provider) betreffend derartige Webseiten unterbunden werden können." Unter Berufung auf die inzwischen vertrauten Fälle BREIN v Filmspeler und BREIN v Ziggo und XS4All, die beide Anfang dieses Jahres vom Europäischen Gerichtshof entschieden wurden, kam der Oberste Gerichtshof zu dem Schluss, dass dies der Fall sei.

Laut OGH steht der Beurteilung, dass The Pirate Bay "selbst kein urheberrechtlich geschütztes Material abrufbar gehalten oder übertragen" habe, nichts entgegen. Auch das Gegenargument, dass Anbieten von legalen Inhalten, die durch die Netzsperre ebenso unzugänglich gemacht würden, falle dabei nicht ins Gewicht, da laut OGH "auf anderen Seiten dieselben Inhalte ohne größeren Aufwand wieder hochgeladen werden könnten". Dass The Pirate Bay hauptsächlich geschützte Inhalte anbiete, ergäbe sich laut OGH schon aus dem "offensichtlich als Lockmittel eingesetzten Namen (‚Pirate Bay')".

Begründet wird das Urteil mit dem Argument, dass bereits das Anbieten eines Torrent-Verzeichnisses auf Online-Plattformen bereits eine öffentliche Wiedergabe sei. Bei urheberrechtlich geschützten Inhalten reicht damit das Verweisen auf Torrents bereits aus, um eine Netzsperre zu rechtfertigen. Demnach müssen die Provider Sperraufforderungen auch dann nachkommen, wenn eine Seite selber keine illegalen Inhalte, sondern nur Magnet-Links zu Torrents bereitstellt.

Während diese Entscheidung von der Musikindustrie begrüßt wurde, kam Kritik vom Dachverband der österreichischen Internet Provider (ISPA) und den Mobilfunkbetreibern. Diese haben sich mit dem Argument, dass The Pirate Bay und Co. eben keine Inhalte anböten und auch legale Daten verteilten, gewehrt gegen eine breite Auslegung des Anbietens geschützter Inhalte. Die ISPA befürchtet, der OHG könne mit diesem Urteil dafür sorgen, dass weitere mögliche Netzsperren auf entsprechende Onlineangebote folgen könnten. Sie weisen darauf hin, dass der OGH den "Kreis der potenziell zu sperrenden Webseiten" ausgedehnt habe, indem er auf "Suchmaschinen und Videoplattformen erweitert" wurde. Dies habe eine "enorme Sprengkraft in Bezug auf die Entwicklung des Internets". ISPA-Generalsekretär Maximilian Schubert kritisiert zudem: "Wir unterstützen keine illegalen Inhalte im Internet in irgendeiner Weise, halten es jedoch für äußerst fragwürdig, dass die Entscheidung darüber, was illegal ist und was nicht, an ISPs fällt, statt eines Gerichts. […] Illegale Inhalte sind dauerhaft durch Löschen aus dem Netzwerk zu entfernen. Alles andere ist ein Placebo mit extrem gefährlichen Nebenwirkungen, die sowohl von Anbietern als auch von Verbrauchern leicht umgangen werden können. Das Einzige, was bleibt, ist eine Sperrinfrastruktur, die für viele Zwecke missbraucht werden kann und leider vielerorts genutzt wird."

BGH-Urteil: Internetprovider zur Speicherung von IP-Adressen verpflichtet bei Urheberrechtsverletzungen

Der Bundesgerichtshof (BGH) hat mit einem Urteil vom 21.09.2017 (Az. I ZR 58/16) entschieden, dass der Internetprovider in Fällen offensichtlicher Rechtsverletzungen bis zum Abschluss des Gestattungsverfahrens verpflichtet ist, die Löschung der von ihm erhobenen Verkehrsdaten zu unterlassen, die die Auskunftserteilung gegenüber dem Rechtsinhaber ermöglichen, berichtet die Kanzlei Waldorf Frommer in einem Blogbeitrag.

Gegenstand des Rechtsstreits war die Frage, ob Provider Verbindungsdaten ihrer vergebenen IP-Adressen, die einem ihrer Kunden zuzuordnen sind, löschen und somit eine Auskunftserteilung vereiteln dürfen. Der BGH hat dies verneint und entschieden, es bestehe in Fällen offensichtlicher Rechtsverletzungen eine Pflicht zur Speicherung dieser Informationen.

Die Klägerin ist Tonträgerherstellerin und forderte die Beklagte, ein Telekommunikationsunternehmen, das seinen Kunden Zugang zum Internet vermittelt und dafür dynamische IP-Adressen vergibt, auf, noch während die Täter online waren, Verbindungsdaten zu 21 IP-Adressen mit den dazu gehörigen Verbindungszeitpunkten vorerst nicht zu löschen, bis ein Gericht über die Zulässigkeit der Verwendung der Verkehrsdaten entschieden habe. Die Klägerin wies darauf hin, dass diese Kunden der Beklagten unter den genannten IP-Adressen mittels einer File-Sharing-Software im Internet Musikaufnahmen zum Herunterladen bereitstellen würden, an denen der Klägerin ausschließliche Verwertungsrechte zustünden.

Bei Urheberrechtsverletzungen im Internet ist dem Verletzten häufig nur die IP-Adresse des Täters bekannt. Diese werden vom Provider vergeben, aber nur einige Provider speichern auch nach Ende der jeweiligen Verbindung für einige Tage die Verbindungsdaten, die eine Verknüpfung der IP-Adresse zum betroffenen Kunden ermöglichen. Andere Provider lehnen eine derartige Speicherung ab, wie auch im vorliegenden Fall, sie löschen diese Daten sofort nach dem Beenden der Verbindung. Somit war es bisher unmöglich gegenüber solchen Providern Auskunftsansprüche geltend zu machen.

Diese Sachlage hat sich mit dem nun vorliegenden BGH-Urteil geändert: Der BGH hat entschieden, dass „der an der Verletzung des Urheberrechts […] nicht beteiligte Dritte in Fällen offensichtlicher Rechtsverletzungen […] , nicht nur zur Auskunftserteilung verpflichtet, sondern auch zum Unterlassen der Löschung von bei ihm vorhandenen Daten, die die Auskunftserteilung erst ermöglichen“, ist, weil sich der zu beurteilende Speicheranspruch hier auf Fälle offensichtlicher Rechtsverletzungen bezieht, die Auskunftserteilung stehe zudem unter einem Richtervorbehalt. Weder datenschutzrechtliche Bedenken, noch die Aufhebung der Richtlinie über die Vorratsdatenspeicherung, noch verfassungsrechtliche Bedenken stünden dem entgegen. Es könne nicht dem Belieben des Providers überlassen werden: „in Kenntnis einer möglichen Rechtsverletzung die Auskunftserteilung unmöglich zu machen und damit den Anspruch des Rechtsinhabers gegen den Verletzer zu vereiteln.“

Amtsgericht Bochum: Beklagte haftet trotz möglichem Fremdverschulden bei illegalem Filesharing

Wie die Kanzlei Waldorf Frommer in einem Blogbeitrag mitteilt, verurteilte das Amtsgericht Bochum in einem Urteil vom 22.08.2017, Az. 65 C 354/16, eine Anschlussinhaberin wegen illegalem Filesharing trotz Zugriffsmöglichkeiten weiterer Personen auf diesen Internetanschluss zur Zahlung von Schadensersatz.

In dem Verfahren ging es um illegales zur Verfügung stellen von urheberrechtlich geschützten Filmaufnahmen mittels einer Tauschbörse. Die Klägerin konnte vorgerichtlich keine Ansprüche durchsetzen, so erhob sie Klage. Sie hat ermittelt, dass über drei unterschiedliche IP-Adressen der streitgegenständliche Film in einer Tauschbörse zum Download angeboten wurde. Alle drei Adressen waren nach Auskunft

des Providers dem Anschluss der Beklagten zugeordnet.

Angesichts der ermittelten Mehrfachverletzung reicht das einfache Bestreiten der zutreffenden Ermittlung nicht aus. Diese Tatsache spricht grundsätzlich zu Lasten des Anschlussinhabers. Die tatsächliche Vermutung ist allerdings dann nicht begründet, wenn zum Zeitpunkt der Rechtsverletzung auch andere Personen diesen Anschluss nutzen konnten. Dann allerdings trifft den Inhaber dieses Internetanschlusses eine sekundäre Darlegungslast.

Demnach hatte die Beklagte vor Gericht bestritten, die Tat begangen zu haben. Sie verwies darauf, dass noch andere sich zu ihrem Anschluss Zugriff verschaffen konnten. Im weiteren Verlauf des Rechtsstreits ergänzte sie, dass auch ihr Lebensgefährte oder ihr 13-Jähriger Sohn Zugriff auf den Internetanschluss gehabt hätten und die Rechtsverletzung begangen haben konnten.

Diese Argumente waren für das Gericht allerdings nicht ausreichend, sie genügten im Rahmen der sekundären Darlegungslast in keiner Weise. Das Vorbringen der Beklagten wäre zudem widersprüchlich hinsichtlich der möglichen Täterschaft der Familienmitglieder der Beklagten: Eine Täterschaft des Lebensgefährten hatte die Beklagte in der Klageerwiderung zunächst ausgeschlossen. Erst im Laufe des Rechtsstreits und nach Hinweis des Gerichts, dass eine Täterschaft unbekannter Dritter höchst unwahrscheinlich sei, hat die Beklagte es für möglich gehalten, dass ihr Lebensgefähne die Dateien heruntergeladen und angeboten habe. Konkrete Tatsachen sind insoweit jedoch nicht vorgetragen worden. Auch hat die Beklagte nicht erwähnt, ob sie bei ihrem Lebensgefährten konkret nachgefragt hätte und welche Auskunft sie darauf erhielt. Damit begründet der Vortrag der Beklagten letztlich nur die theoretische Zugriffsmöglichkeit ihres Sohnes und ihres Lebensgefährten, ohne dass Tatsachen vorgetragen werden, aus denen ernsthaft auf eine Täterschaft der beiden Personen geschlossen werden konnte.

Hauptsächlich der von der Beklagten pauschal vorgetragene unberechtigte Fremdzugriff führe nicht dazu, dass das Gericht eine Haftung der Beklagten ablehnen würde: “Anhaltspunkte dafür, dass Dritte sich unberechtigt Zugang zum ordnungsgemäß abgesicherten W-LAN-Netz der Beklagten verschafft oder dass Dritte die IP-Adresse der Beklagten „gekapert“ haben könnten, sind nicht vorgetragen. Die rein pauschale Möglichkeit entkräftet die bestehende Vermutung nicht.“

Das Amtsgericht verurteilte die Beklagte daher vollumfänglich zur Zahlung von Schadensersatz, zum Ersatz der außergerichtlichen Rechtsanwaltskosten sowie zur Übernahme der gesamten Kosten des Rechtsstreits. Gegen das Urteil hat die Beklagte Berufung zum Landgericht Bochum eingelegt.

Bundesverwaltungsgericht Leipzig: Metadaten-Speicherung für BND künftig tabu

Laut einem Urteil (Az. BVerwG 6 A 6.16 und BVerwG 6 A 7.16) des Bundesverwaltungsgerichts Leipzig vom Mittwoch (13.12.2017) darf der Bundesnachrichtendienst (BND) wegen mangelnder Rechtsgrundlage keine Metadaten aus Telefongesprächen der Journalistenorganisation Reporter ohne Grenzen (ROG) speichern. Das Urteil könnte zudem auch über den Gerichtsfall hinaus Bedeutung haben.

Der Bundesnachrichtendienst (BND) betreibt eine Datenbank mit dem Namen “VerAS”, was soviel heißt wie “Verkehrsanalysesystem”. Die Datenbank hat insgesamt fünf

Ebenen, Terrorverdächtige werden in die "erste Ebene" aufgenommen. Ferner werden Personen in weiteren Ebenen erfasst, die mit den Verdächtigen Kontakt hatten – per Telefon, E-Mail oder auf anderen "leitungsgebunden" Wegen. Damit betreibt der BND eine eigene Vorratsdatenspeicherung.

Nun hat die Journalistenorganisation Reporter ohne Grenzen (ROG), vertreten durch den Anwalt Niko Härting, mit dem Vorwurf, Kommunikation mit ausländischen Partnern und Journalisten widerrechtlich zu erfassen, im Juni 2015 gegen die strategische Fernmeldeaufklärung des BND geklagt, die dem Geheimdienst u.a. die Durchsuchung von Internet-Traffic nach bestimmten Stichworten sowie die Überwachung von leitungsgebundenem Fernmeldeverkehr erlaubt. Vor einem Jahr war die Klage bezüglich eines Ausspähens des E-Mail-Verkehrs gescheitert. Offen war dabei noch die Frage geblieben, ob der BND anonymisierte Metadaten im Verkehrsanalysesystem (VerAS) speichern darf.

Die Antwort darauf gab mit dem aktuellen Urteil das Bundesverwaltungsgericht Leipzig. Demnach greifen die Erhebung, Speicherung und Nutzung von Telefonie-Metadaten "ungeachtet der vor der Speicherung durch den BND vorgenommenen Anonymisierung in das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG ein. Daher sind diese Eingriffe nur zulässig, wenn die Erhebung der Daten und ihre weitere Verwendung auf eine gesetzliche Grundlage gestützt werden kann. An einer solchen gesetzlichen Regelung fehlt es gegenwärtig." Das Gericht verfügte nun, dass die Klage nur in Bezug auf die Telefonie-Metadaten zulässig sei, nicht aber hinsichtlich der Metadaten aus Internet- und E-Mail-Verkehren. Die vorgenommene Anonymisierung sei nicht mit der verfassungsrechtlich gebotenen Löschung gleichzusetzen, da VerAS zwar gespeicherte Telefonnummern und die Identifikationsnummer auf der SIM-Karte zur Anonymisierung unkenntlich machen könne, das sich aber nur auf die von VerAS selbst erstellte Netzwerk-Datenbank beziehe. Der BND könne die deutschen Inhaber der Nummern jederzeit wieder identifizieren.

Für Reporter ohne Grenzen bedeutet das ein "wegweisendes Urteil" gegen den BND. "Das Urteil zeigt, dass es sich lohnt, wenn sich Menschenrechtsorganisationen über Gerichte gegen die massenhafte Speicherung von Daten durch den BND zu Wehr setzen. Durch das Urteil könnten nun auch andere Personen und Organisationen mit demselben Anliegen an den BND herantreten," sagte ROG-Geschäftsführer Christian Mihr.

Auch Grünen-Netzpolitiker Konstantin von Notz begrüßte das Urteil mit den Worten: "Heute ist ein guter Tag für unsere Grundrechte. […] Das Urteil zur Speicherung anonymisierter Verbindungsdaten in der BND-Datei „VerAS" wird absehbar weitreichende Auswirkungen auch auf andere Datensammlungen haben. Es stellt die technische Aufklärung der Nachrichtendienste und die Anlasslosigkeit der Maßnahmen insgesamt in Frage."

Bundesverfassungsgericht verbietet überzogene Telefongebühren in Haftanstalten

Wie Strafrechtler Udo Vetter berichtet, verbietet das Bundesverfassungsgericht (BVerfG) „Mondpreise" für Telefonate hinter Gittern. Ein Inhaftierter aus Schleswig-Holstein wehrte sich vor Gericht erfolgreich gegen doppelt so hohe Telefonpreise wie draußen. Der Beschluss wurde heute unter dem Aktenzeichen 2 BvR 222/16 veröffentlicht.

Haftanstalten in ganz Deutschland dürfen den Gefangenen keine überzogenen Preise mehr für Telefonate berechnen. Auch nicht in dem Fall, dass dafür externe Anbieter in Anspruch genommen werden. Zwar habe man im Gefängnis keinen Anspruch auf Gratisgespräche – auch nicht ins Festnetz. Aber die Kosten für die Telefonate müssen in etwa denen außerhalb der Gefängnismauern entsprechen, so das BVerfG.

Der Kläger hatte vor Gericht bemängelt, dass er plötzlich das Doppelte bezahlen sollte, weil die Haftanstalt einen langfristigen Vertrag mit einem privaten Exklusivanbieter abgeschlossen hatte. Die Richter kamen zu dem Urteil, Aufschläge seien nur zulässig, sofern sie sich aus speziellen „verteuernden Bedingungen und Erfordernissen" des Strafvollzugs ergeben. Dies resultiere aus der Fürsorgepflicht der Haftanstalt für das Vermögen der Gefangenen, dem Resozialisierungsgebot und aus dem Grundsatz der Verhältnismäßigkeit.

Vor allem die Verhältnismäßigkeit war unter diesen Bedingungen nicht mehr gegeben. Die Haftanstalt versuchte sich vor Gericht damit herauszureden, man habe sich vertraglich 15 Jahre an einen Anbieter gebunden und besitze keinen Einfluss auf die Preisgestaltung des Unternehmens. Die Beauftragung von Fremdfirmen rechtfertigt allerdings laut Richterspruch nicht die Abkopplung von den marktüblichen Preisen. „Wenn die Haftanstalt ungünstige und nicht zeitgemäße Verträge abschließe, sei das ihr Problem und dürfe das nicht auf den Gefangenen abgewälzt werden“, berichtet Vetter in seinem Blogpost.

Die heute veröffentlichte Entscheidung ist deutschlandweit von großer Bedeutung. Häufig müssen Gefangene selbst für Telefonate ins deutsche Festnetz Sätze bezahlen, die man „draußen höchstens bei Telefonaten (zum Mond oder) nach Übersee kennt“.

Filesharing: Wegen familienfreundlicher Ausrichtung kein Ausspionieren von Familienmitgliedern gefordert

Das Amtsgericht (AG) Charlottenburg hat in einem Verfahren (Urteil vom 14.11.2017, Az. 203 C 255/17) zugunsten eines wegen Filesharing Beklagten geurteilt. Gemäß diesem familienfreundlichen Urteil genügte der Familienvater seinen Nachforschungspflichten auch ohne die mitunter hohen Anforderungen an die sekundäre Darlegungslast bereits durch bloßes Befragen der gleichfalls für die Tat infrage kommenden Familienmitglieder. Somit wurde eine Klage der Münchner Anwaltskanzlei Waldorf Frommer abgewiesen. Für die Anwaltskanzlei Wilde Beuger Solmecke, die die Verteidigung übernommen hatte, bedeutet das Urteil eine weitere Übereinstimmung mit der Rechtssprechung des Bundesgerichtshofes (BGH), berichtet Rechtsanwalt Solmecke auf seiner Blogseite.

Die Klägerin, die Universum Film GmbH aus München, mit dem Urheberrecht an “The Call – Leg nicht auf”, stellte fest, dass dieser Film auf einer Tauschbörse mit der IP-Adresse des beklagten Familienvaters zum Download angeboten wurde. Daraufhin verlangte sie eine Erstattung der Abmahnkosten sowie Schadenersatz für das widerrechtlich öffentliche Zugänglichmachen des Films vom Internetanschluss des Beklagten. Waldorf Frommer verlangte diesbezüglich einerseits 1.000 Euro Schadensersatz wegen der angeblich vom Beklagten begangenen Urheberrechtsverletzung und andererseits Abmahnkosten in Höhe von insgesamt 215 Euro.

Der Beklagte gab an, die Rechtsverletzung selbst nicht begangen zu haben. Jedoch hätten sowohl seine Frau, als auch sein volljähriger Sohn, seine volljährige Tochter und seine Schwägerin noch Zugang zum Zeitpunkt der Urheberrechtsverletzung zu besagtem Internetanschluss. Sie alle verfügten über gute Computerkenntnisse und nutzten den Anschluss unter anderem zum Konsum von Filmen, Serien, Musik sowie für soziale Netzwerke. Der Familienvater befragte alle diese Personen, die jedoch angaben, auch sie seien nicht für die Tat verantwortlich.

Das Gericht urteilte in diesem Fall so, dass der Beklage durch seine Angaben die sekundäre Darlegungslast vollumfänglich erfüllt hat. Trotz der Aussage blieben diese Personen mögliche Täter der Urheberrechtsverletzung und die Vermutungswirkung ist mit dem Vortrag entkräftet. Weiterer Nachforschungspflichten sind dem Beklagten nicht zuzumuten. Das Gericht stellt fest, dass das ungestörte eheliche und familiäre Zusammenleben durch Art. 7 und Art. 6 Abs. 1 der EU-Grundrechtecharta vor derartigen Beeinträchtigungen geschützt werden. Es obliegt somit dem Familienvater weder, die Nutzung des Anschlusses zu dokumentieren, noch wäre er zur Untersuchung der Rechner im Hinblick auf Filesharing-Software verpflichtet.

Da eine Störerhaftung hinsichtlich der Abmahnkosten Prüfpflichten voraussetzt, kommt diese in dem vorliegenden Fall ebensowenig zur Anwendung, denn bei volljährigen Familienangehörigen ist das normalerweise nicht der Fall. Der Familievater braucht seine Angehörigen weder zu belehren noch zu überwachen.

Somit wurde die Klage abgewiesen, die Klägerin hat die Kosten des Rechtsstreites zu tragen.

Gemäß einer Aussage von Rechtsanwalt Solmecke sollen sich: *“Vor allem Familien von Abmahnkanzleien nicht einschüchtern lassen. Diese stellen häufig Anforderungen an Nachforschungen, denen der BGH in jüngster Zeit eine Absage erteilt hat.”*

Amtsgericht München: Pauschale Täterschaftsvermutung genügt nicht für sekundäre Darlegungslast

Das Amtsgericht München hat in einem Urteil vom 06.10.2017, Az. 264 C 4216/17, entschieden, dass eine Anschlussinhaberin wegen illegalem Files-

haring zu Schadensersatz verurteilt wird. Hierbei reiche ein "Pauschaler Fingerzeig auf dritte Personen nicht zur Erschütterung der Täterschaftsvermutung" aus, berichtet die Kanzlei Waldorf Frommer in einem Blogbeitrag.

In dem Verfahren ging es um illegales zur Verfügung stellen von urheberrechtlich geschützten Filmaufnahmen mittels einer Tauschbörse, wobei der Beklagten nachgewiesen wurde, dass über ihren Internetanschluss der besagte Film zum Download auf einer Tauschbörse angeboten wurde, obwohl die Beklagte hierzu nicht berechtigt war. Allein die Klägerin hatte die uneingeschränkten Rechte an dem Film.

Zunächst mal trägt die Klägerin die Darlegungs-und Beweislast für die Voraussetzungen des Anspruchs. Daher muss sie auch nachweisen, dass die Beklagte für die behauptete Urheberrechtsverletzung verantwortlich ist. Allerdings spricht eine tatsächliche Vermutung für die Täterschaft des Anspruchsinhabers, wenn keine andere Person diesen Internetanschluss benutzen konnte. Diese Vermutung wird dann widerlegt, wenn der Internetanschluss zum Verletzungszeitpunkt auch von anderen Personen benutzt werden konnte. In diesen Fällen trifft den Anschlussinhaber eine sekundäre Darlegungslast.

So gab die Beklagte an, dass auch ihr ehemaliger Ehemann als Täter in Frage kommen könnte, er habe dies ihr gegenüber nach Erhalt der Abmahnung sogar zugegeben. Sie selbst habe zum Tatzeitpunkt bereits geschlafen und scheide so als Täterin aus. Im Laufe des Verfahrens als Zeuge vernommen, gab der Ex-Partner jedoch an, weder die Tag begangen, noch es eingestanden zu haben. In Anbetracht dieser Aussage, änderte die Beklagte ihre Aussage und behauptet nun, dass auch die beiden Kinder des Zeugen die Rechtsverletzung begangen haben könnten.

Für das Amtsgericht München kam diese Änderung allerdings sowohl verspätet, zudem sah es sie auch als zu pauschal an. Während der Zeuge, also der ehemalige Ehemann der Beklagten, glaubhaft bekundet hat, dass er die Rechtsverletzung nicht begangen habe, fehle es in Bezug auf die Kinder des Zeugen hingegen an einem detaillierten Sachvortrag: „Die Beklagte hat nicht dargelegt, dass die Kinder zum Tatzeitpunkt tatsächlich Zugriff auf den PC hatten, auch fehlt der Vortrag zum konkreten Nutzungsverhalten der Kinder zum Tatzeitpunkt oder zu sonstigen Hinweisen der Kinder. Insoweit ist das Vorbringen der Beklagten zudem widersprüchlich, da sie zunächst ausschließlich den Zeugen […] als Rechtsverletzer benannt hat."

In der Folge verurteilte das Gericht die Beklagte vollumfänglich zu Schadensersatz nebst Zinsen an die Klägerin. Außerdem hat sie die Kosten des Rechtsstreites zu tragen.

Denuvo: Neuer Kopierschutz noch ungeknackt

Wer sich auf den NFO- oder ftp-Sites umschaut, wird schnell bemerken, dass bislang keines der Windows-Games mit der neuen Anti-Tamper-Version von Denuvo geknackt wurde. Das gilt nicht nur für Assassin's Creed Origins, wo zudem noch VMProtect als zusätzlicher Schutz eingebaut wurde, sondern bei allen genannten Spielen von EA, Ubisoft, SEGA und Warner Bros.

Keiner der Programmierer von CODEX, Steampunks oder Conspiracy war bislang dazu in der Lage, eines der seit November veröffentlichten PC-Games zu knacken, welches mit der aktuellen Anti-Tamper-Variante ausgestattet wur-

de. Dazu gehört beispielsweise Star Wars Battlefront 2, Sonic Forces, Injustice 2, Football Manager 2018, Need for Speed Payback und last, but not least Assassin's Creed Origins. Bei Assassin's Creed Origins kommt noch zusätzlich VMProtect als Zusatz-DRM zum Einsatz, was bei einigen PCs zu erheblichen Geschwindigkeitseinbußen geführt hat.

Die letzten Denuvo-Versionen wurden jeweils innerhalb weniger Stunden oder Tage geknackt, wie wir bereits berichtet haben. Für die Spielepublisher bzw. Hersteller ist es wichtig, dass neue Titel mehrere Monate exklusiv als käufliche Versionen erhältlich sind, bevor die entsprechenden Schwarzkopien im Internet erscheinen. Die hohen Produktionskosten können nur wieder eingespielt werden, wenn es genügend besonders neugierige oder ungeduldige Gamer gibt, die bereit sind, die Spiele nach der Veröffentlichung zum vollen Kaufpreis zu erwerben.

Im Anbetracht der jetzigen Lage kann der österreichische Hersteller Denuvo natürlich darauf hoffen, dass einige Publisher zu ihrem kostenpflichtigen Kopierschutz zurückkehren werden. Und dies obwohl die Warner Bros. Spiele Batman: Arkham Knight, Middle-Earth: Shadow of War und Mad Max anfangs Probleme mit der Verbindung mit den Denuvo-Servern hatten und deswegen nicht benutzt werden konnten. Die Situation hat sich mittlerweile geklärt, die Games laufen trotz des Online-Zwangs wieder einwandfrei, wie John Papadopoulos vom Blog Dark Side of Gaming (DSOG) berichtet. Einige Gamer laufen wegen der Probleme noch immer Sturm und behaupten im Kommentarbereich von DSOG, der Kopierschutz habe sie vor allem erfolgreich davor bewahrt, die PC-Spiele mit dem neuen Kopierschutz und den entsprechenden Anlaufschwierigkeiten zu kaufen.

Sony PS4: Kernel geknackt, Jailbreak steht bevor

Der PS4 Entwickler Specter hat heute auf Github den Quellcode zum Knacken des PS4 Kernels 4.05 veröffentlicht. Den Kopierschutz kann man mit dem Kernel Exploit namens namedobj noch nicht umgehen, das ist aber nur noch eine Frage der Zeit.

Im Oktober machten sich die Gamer letztmalig Hoffnungen auf einen kostenlosen Spielgenuss, weil die stark veraltete Firmware 1.76 aus dem Jahr 2014 per Jailbreak geknackt werden konnte. Die Freude war nicht von langer Dauer, alle neueren Geräte bzw. Firmware-Versionen weisen die ausgenutzte Schwachstelle nicht mehr auf und sind deswegen sicher.

Mit dem neuen Kernel Exploit namedobj kann man einen eigenen Loader ausführen, der Kopierschutz von Sony wird damit aber noch nicht umgangen, das will Specter selbst auch nicht anbieten. Autoren des Exploits waren ursprünglich die Mitglieder von fail0verflow. Sie haben bereits im Oktober eine Linux -Distribution auf einer Playstation 4 ausgeführt. Für das Ausführen eigener Programme (Homebrew) oder kommerzieller Spiele, ist dieser Code mit Webkit-Unterstützung aber noch nicht geeignet.

namedobj soll immerhin dazu in der Lage sein, Modifikationen auf Kernel-Ebene vorzunehmen und das Gerät komplett für die verschiedensten Zwecke zu knacken. Wer die PS4 dazu in die Lage versetzen will, darauf schwarzkopierte Spiele auszuführen, soll den Entwickler für weitere Details kontaktieren. Das Thema ist ihm selbst offensichtlich zu heiß.

Trotzdem darf man davon ausgehen, dass sich schon bald die ersten Teams daran setzen werden, Sonys Spielkonsole aufgrund dieser Sicherheitslücke in einen regelrechten Alptraum für alle Softwarepublisher und Spielehersteller zu verwandeln. Wir bleiben auf jeden Fall am Ball und werden über weitere Fortschritte berichten.

> Hope everyone had a Merry Christmas! Here's the 4.05 kernel exploit, fully implemented. Enjoy! Write-up coming soon! https://t.co/MQR0lzCu9Y
>
> — Specter (@SpecterDev) 27. Dezember 2017

Haven: Snowden entwickelt Sicherheits-App für Android-Smartphones

Die Sicherheits-App Haven verwandelt Android-Smartphones in Überwachungsgeräte. Die App soll so jede Art von Spionageversuche in persönlichen Räumlichkeiten aufdecken. Die von Edward Snowden als Präsident vertretene Freedom of the Press Foundation hat aktuell eine erste Beta-Version des Open-Source-Sicherheitssystems veröffentlicht. Haven verwendet u.a. Handy-Sensoren, die Änderungen in Klang, Licht und Bewegung überwachen, um private Räume zu beaufsichtigen und zu schützen, berichtet Wired.

Haven wurde für Android-Smartphones entwickelt, die App nutzt die Kameras, Mikrofone, Lichtsensoren und Beschleunigungssensoren des Handys, um auf Bewegungen, Geräusche oder Abweichungen zu reagieren. Die App ist dazu gedacht, zu überwachende Räumlichkeiten so abzusichern, dass ein Eindringen von außen nicht unbemerkt bleibt. Sie kann Fotos und Audiodateien von Personen aufnehmen, die den Raum betreten, während der Nutzer der App unterwegs ist. Töne, ein Einschalten der Beleuchtung, Foto-Blitze und Bewegungen werden durch die App automatisch erfasst und in Log-Dateien gespeichert. Alarmmeldungen werden zusammen mit Bildern und Soundclips sofort an mobile Geräte des Users weitergeleitet. Die Haven App wird dann Ende-zu-Ende-verschlüsselte Benachrichtigungen per Signal an das User-Handy senden und er kann die Aktivitäten über einen Tor Onion-Dienst remote überwachen. Wichtig ist, dass sich Haven nicht auf die Cloud verlässt und keine Daten überträgt, auf die Dritte zugreifen können

Edward Snowden vergleicht die App mit einem virtuellen Wachhund, den man zurücklässt und der alle Ereignisse vor Ort aufzeichnet. Die Idee dahinter ist, dass man mit der App bestimmten Orten bezüglich der Privatsphäre vertrauen kann. Allerdings erkennt Sownden an, dass Haven einen Eindringling nicht aufhalten kann, der darauf aus ist, die Privatsphäre zu verletzen. Allerdings hätte man nun aber die Möglichkeit, deren Anwesenheit aufzuspüren und aufzuzeichnen. So kann man einerseits die Eindringlinge dazu bringen, über die Folgen einer Dokumentation dieses Eindringens nachzudenken und andererseits den Opfern ein wichtiges Werkzeug geben, das sie vorher nicht hatten: “Wenn die Geheimpolizei Menschen verschwinden lässt, verändert Haven die Risikoabschätzung, die Sie durchlaufen müssen”, sagt Snowden. “Sie müssen sich nun sorgen, dass jedes mögliche Handy ein Zeuge sein könnte.”

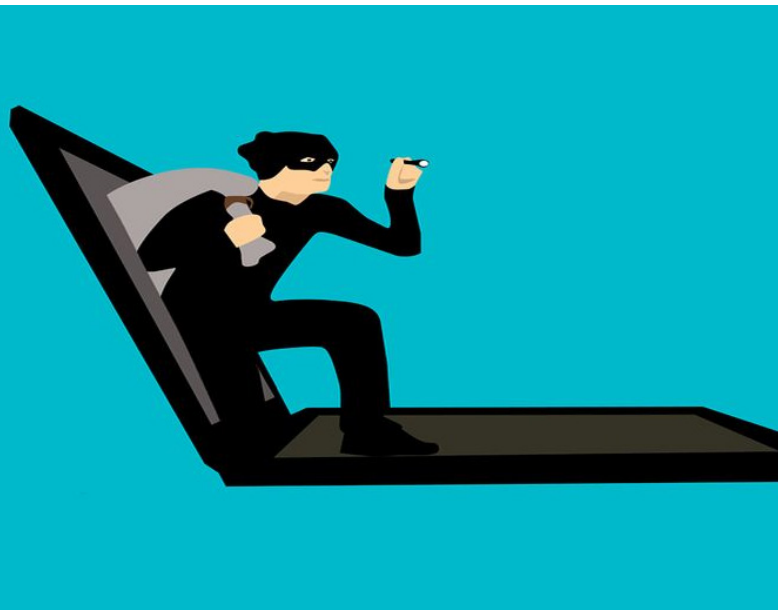
Snowden ist seit Anfang 2016 Präsident der Freedom of the Press Foundation und arbeitet dort seither mit einem kleinen Team aus Programmierern und IT-Experten an einer Reihe von Sicherheitstools. Die Haven-App wurde in Zusammenarbeit mit dem “Guardian Project” umgesetzt, das bereits besonders sichere Open-Source-Software entwickelt hat. Dazu gehören solche Apps, wie Orbot, eine Android-Version des Proxy-Dienstes Tors, der Browser Orfox, die sichere Chatsoftware Chatsecure, die automatisch Gesichter verpixelnde Obscuracam oder Pixelknot, das geheimen Botschaften in Bildern verstecken kann. Das Entwicklerteam hat Haven besonders für investigative Journalisten und Menschenrechtsverteidiger entworfen, um eine neue Art von Immunität zu schaffen. Durch eine Kombination der Sensoren, wie sie in jedem Smartphone zu finden sind, mit den weltweit sichersten Kommunikationstechnologien, wie Signal und Tor, soll Haven verhindern, dass solche Menschen zum Schweigen gebracht werden.

Die App kann man von hier herunterladen!

MoneyTaker: Hackergruppe erbeutet 10 Millionen US-Dollar von Banken

Eine Hackergruppe namens MoneyTaker soll bereits seit dem Jahr 2016 Banken in England, Russland und den USA bisher unbemerkt um Geld erleichtert haben. Sicherheitsforscher von Group-IB haben 21 erfolgreiche Angriffe aufgedeckt, wobei die Hacker zehn Millionen US-Dollar erbeutet haben sollen. Sowohl Europol als auch Interpol ermitteln aktuell in der Sache.

Gemäß einem Bericht der Sicherheitsforscher von Group-IP nutzte MoneyTaker für ihre Angriffe verschiedenen Tools, um sich damit höhere Rechte in IT-Systemen zu verschaffen. So ge-



lang es den Hackern, Geldkarten zu ordern, das Abhebelimit zu entfernen, um Geld am Automaten abzubuchen. Auch der Banking-Trojaner Kronos soll dabei zum Einsatz gekommen sein.

Mit weiteren Tools sollen Zahlungen gefälscht und Spuren verwischt worden sein. Um von Anti-Virensoftware unentdeckt zu bleiben, nutzten die MoneyTaker-Hacker gezielt Powershell- und VBS-Skripte. Um unentdeckt zu bleiben, setzten die Hacker unter anderem dateilose Malware ein, die nach dem Neustart eines infizierten Computers verschwindet. Dadurch sollen sie zudem an solche Informationen gelangt sein, die weitere Angriffe ermöglichten, wie auf das SWIFT-Netzwerk, über das Interbankengeschäfte abgewickelt werden.

Auf Command-and-Control-Servern (C&C) hat MoneyTaker die legitime Pentesting-Software Metasploit zum Aufspüren von Schlupflöchern eingesetzt. Den Traffic der C&C-Server haben die Angreifer vor Sicherheitsforschern verschlüsselt hinter TLS-Zertifikaten versteckt. Die gefälschten Zertifikate sollen legitime Namen, wie Bank of America oder Microsoft, tragen.

Ai.Type: Tastatur-App stellt Daten von 31 Millionen Nutzern ins Netz

Sicherheitsforscher vom Kromtech Security Center via MacKeeper Security haben bei der weltweit beliebten Tastatur-App Ai.Type für iOS und Android eines Startup-Unternehmens aus Tel Aviv ein massives Datenleck aufgedeckt. Eine 577 GByte umfassende MongoDB lag aufgrund eines Konfigurationsfehlers ungesichert im Netz und gab so sensible Daten von 31.293.959 Nutzern preis. Betroffen sind vor allem die Informationen von Personen, welche das Programm auf einem Android-Smartphone verwendet haben, berichtet ZDnet unter Bezugnahme auf die Sicherheitsforscher von Kromtech. Im App Store beschreiben die Ai.Type-Entwickler ihre App als die „intelligenteste Zusatz-Tastatur für iPhone und iPad“. Die App ist weit verbreitet – Google Play weist rund 40 Millionen Downloads auf, sie wertet die Tastatureingaben aus und würde sich, nach eigenen Angaben, dadurch auf den persönlichen Schreibstil ihrer Nutzer einstellen. Bereits nach der Installation wird man darauf hingewiesen, dass alle mit der Tastatur eingegebenen Texte, einschließlich persönlicher Daten, wie Postanschrift, Passwörter und Kreditkartennummern, gesammelt und übertragen werden. So haben die App-Entwickler die erforderliche Zustimmung zum Anlass genommen, um all diese eingegebenen sensiblen Daten der User auszuspähen. Doch damit nicht genug: die erbeuteten Daten waren offenbar nicht einmal richtig geschützt, die Sicherheitsforscher haben sie auf einem Server ohne Passwortschutz im Internet gefunden.

Zu den aufgezeichneten Nutzerdaten, gehörten den Kromtech-Forschern zufolge, Namen, Telefonnummern, E-Mail-Adressen, Adressdaten, der genaue Standort eines Nutzers, einschließlich seiner Stadt und seines Landes. Aber auch die IMSI- und die IMEI-Nummer, Angaben zum Modell, zur Bildschirmauflösung, zur Spracheinstellung, zum Betriebssystem, IP-Adressen, Anbieterinformationen, der Name genutzter WLAN-Verbindungen, Links zu Social-Media-Profilen und Angaben aus den Sozialen Medien, wie Geburtsdatum oder Profilfotos, wurden gespeichert. Offenbar sind teilweise sogar die Adressbücher der Nutzer ausgelesen worden. Die Datenbank enthält zudem Statistiken, wie viele Nachrichten Nutzer pro Tag geschrieben haben und wie viele Wörter sie dabei durchschnittlich

verwendeten, ferner Informationen über die populärsten Suchbegriffe für verschiedene Regionen. Von dem Datenleck sind sogar Personen betroffen, die die App gar nicht heruntergeladen haben: “Wir haben auch mehrere Tabellen gefunden mit Kontaktdaten, die von Nutzertelefonen hochgeladen wurden”, informiert ZDNet. In einer Tabelle fanden sich 10,7 Millionen E-Mail Adressen, in einer anderen 374,6 Millionen Telefonnummern.

Die Sicherheitsforscher bezeichnen die von der App gesammelten Informationen als eine “schockierende Menge”. Insgesamt seien 577 GB an Daten ins Netz gelangt. Durch das Sicherheitsleck seien alle Einträge “für jeden mit einer Internet-Verbindung” frei zugänglich gewesen, sowohl zum Herunterladen, als auch zum Löschen.

AI.type-Mitgründer Eitan Fitusi habe seine Nachlässigkeit inzwischen zugegeben. Laut ZDNet sollen die Informationen auf dem AI.type-Server aber mittlerweile abgesichert sein, sodass keine weiteren Inhalte ins Netz gelangen dürften. Gegenüber der BBC meinte Fitusi, die Darstellungen wären übertrieben, denn bei der nicht passwortgeschützten Datenbank habe es sich um eine “sekundäre Datenbank” gehandelt, die nicht so viele Informationen beinhalte, wie von Kromtech behauptet. So seien keine Geräteinformationen erfasst oder genaue Standortdaten gespeichert worden. Die App habe lediglich erfasst, welche Werbeanzeigen die Nutzer klickten. In der App-Beschreibung von “Ai.Type” heißt es: “Ihr Datenschutz ist uns wichtig. Wir geben nie Ihre Daten frei oder erfassen Ihre Passwörter. Texte bleiben verschlüsselt und privat.”

Kromtech-Sicherheitsforscher Bob Diachenko hält Bedenken vor dem Einsatz kostenloser Apps, die vollen Zugriff auf Geräte verlangen, für angebracht: “Wieder einmal stellt sich die Frage, ob es das wirklich wert ist, wenn Konsumenten ihre Daten im Austausch zu kostenlosen oder vergünstigten Produkten preisgeben”, heißt es im Blog der Forscher.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnte über Twitter vor der Keyboard-App AI.type. Das Amt rät dazu, bei allen über ein Smartphone mit AI Type genutzten Diensten die Passwörter zu ändern, weil diese ebenfalls durch den Leak kompromittiert sein könnten. User sollten laut BSI den Nutzen solcher Apps abwägen. Kostenlose Dienste wie AI.type würden meistens mit den Daten ihrer Nutzer bezahlt, deshalb sollten derartige Anwendungen mit besonderer Vorsicht betrachtet werden.

Russland startet ab August 2018 eigenes DNS mit den BRICS-Staaten

Die BRICS-Staaten Brasilien, Russland, Indien, China und Südafrika wollen ab August 2018 eine eigene Internet-Infrastruktur aufbauen, meldet die Nachrichtenagentur RT (Russia Today). Hierzu wird ein alternatives DNS (Domain Name System) aufgebaut, das euphemistisch als “Backup-System” bezeichnet wird und unabhängig vom bisherigen weltweiten DNS arbeitet, welches die ICANN-Organisation verwaltet. Die ICANN koordiniert weltweit die Vergabe von Domain-Namen und Adressen im Internet. Bei den Domain-Namen handelt es sich um die www-Namen der Webseiten, während die Adressen deren IP-Nummern sind, unter denen sie im Internet angemeldet sind.

Webseiten können nur über ihre IP-Nummern aufgerufen werden. Daher ist das DNS nötig, um Browsern und anderen Programme die IP-Nummern von Webseiten mitzuteilen. Vergleichbar ist das DNS mit einem Telefonbuch, in dem zu jedem Namen die Rufnummer steht, über die der Teilnehmer erreichbar ist.

Tippt man in den Browser den Namen einer Webseite ein (auch Weblink oder URL genannt), dann fragt der Browser zuerst beim DNS nach der IP-Adresse des Domain-Names der Webseite an, z.B: tarnkappe.info. Anschließend wird die zurückgelieferte IP-Nummer vom Browser aufgerufen. Dadurch landet man beim Server, auf dem die Webseite gespeichert ist. Dem Server wird bei diesem Schritt der vollständige Weblink übergeben, wodurch dieser den Inhalt der Webseite an den Browser sendet, der ihn dann angezeigt. Wer die Macht über das DNS hat, kontrolliert das Internet

Den BRICS-Staaten geht es bei ihrem Vorstoß allein um die Kontrolle des Internets, wobei Kontrolle bedeutet, dass Be-

nutzer bestimmte Seiten nicht finden sollen. Entfernt man die Einträge unliebsamer Webseiten aus dem DNS, kann der Browser sie nicht mehr anzeigen. Besonders China ist Vorreiter bei dieser Art der Zensur, da es zahlreiche dunkle Flecken in der chinesischen Geschichte und Politik gibt, die man der eigenen Bevölkerung unbedingt vorenthalten möchte.

Andere Staaten wie etwa Russland unterdrücken massiv politisch unbequeme Meinungen. Auch hierbei ist die Kontrolle des DNS hilfreich. Es kann sogar genutzt werden, um gefälschte Webseiten anzuzeigen, indem man die Browser auf präparierte Server leitet, statt die echte IP-Nummer auszuliefern.

Auch manche deutsche Politiker haben sich in der Vergangenheit in einer Zensur des Internets versucht, wie etwa Frau von der Leyen mit ihrem Zugangserschwerungsgesetz. Das ist allerdings am allgemeinen Widerstand der Bevölkerung und durch ein Urteil des Verfassungsgerichts gescheitert. Auch viele Verfechter eines restriktiven Urheberrechts rufen gerne nach "Websperren", was nur ein weiterer Name für Zensur am DNS ist. Ganz abgesehen von rechten, linken und korrupten Politikern, die gerne am DNS schrauben würden, wie jetzt die chinesische Diktatur, der lupenreine Demokrat Putin und seine willfährigen Mitstreiter.

Echte Demokratien müssen unliebsame Webseiten aushalten und rechtlich problematische Webseiten auf andere Weise angehen. Zensur ist kein legitimes Mittel der Rechtspflege und in der EU funktioniert das auch ganz gut ohne. Ein zensiertes DNS lässt sich auch leicht umgehen, indem alternative DNS-Server verwendet werden oder man gibt direkt die IP-Adresse der Webseite direkt ein oder benutzt ein lokales DNS auf dem eigenen Computer in der hosts-Datei.

Wer DNS wirkungsvoll kontrollieren will, ist in einem weiteren Schritt gezwungen alle Außenverbindungen abzuschneiden, da sonst immer ein Weg zu "verbotenen" Inhalten gefunden werden kann. Letztlich endet man bei einer Mauer um die eigene Bevölkerung, die sich nicht anders in Schach halten lässt.

Wohin das führt, kennen wir schon…

Firefox-Browser: Warnung vor gehackten Webseiten mittels Breach Alerts

Laut Firefox-Entwickler Nihanth Subramanya soll ein neues Feature künftig für mehr Sicherheit beim Surfen sorgen:

„Breach Alerts" wird Nutzer warnen, wenn sie eine Seite aufrufen, die Opfer von Hackerangriffen wurde. Subramanya gibt bekannt, dass das neue Feature zu einem zentralen Bestandteil der regulären Browser-Ausgabe wird. Der konkrete Zeitpunkt, wann das Tool einsatzbereit ist, steht derzeit jedoch noch nicht fest.

Hat noch vor kurzem Firefox seinen Quantum Browser veröffentlicht, so wird schon bald der nun wesentliche schnellere Firefox mit einer neuen Sicherheitsfunktion ausgestattet sein: Der Code im Repository "Breach Alerts" vergleicht von Nutzern aufgerufene Webseiten mit einer öffentlich verfügbaren Liste des unabhängigen Passwort-Prüfdienstes Have I Been Pwned. Falls die Seite dort aufgelistet ist, erscheint ein Warnhinweis. Zudem sollen Nutzern weiterführende Informationen über das Datenleck sowie Ratschläge zum weiteren Vorgehen erhalten. Für zusätzliche Sicherheit wird eine E-Mail-Benachrichtigung sorgen, die Firefox-Nutzer darüber informiert, ob bei genutzten Diensten ein neues Datenleck aufgetreten ist.

Die Webseite "Have I been pawned" schafft mehr Transparenz in Sicherheitsfragen. Nutzer können hier erfahren, ob sie mit ihrer E-Mail-Adresse bei einem Dienst angemeldet sind, der in der Vergangenheit gehackt wurde, vorausausgesetzt, der Angriff wurde bereits bekannt. Nun will Mozilla diese Datenbank auch in seinen neuen Firefox-Browser integrieren. Auf der Github-Seite des Firefox-Entwicklers Nihanth Subramanya findet sich bereits eine sehr frühe Version der geplanten Browser-Erweiterung. „Have I Been Pwned"-Betreiber Troy Hunt bestätigte die Zusammenarbeit mit dem Firefox-Entwickler Mozilla auf Twitter und zeigte sich erfreut über die positive Resonanz auf das kommende Feature.

Wie Google Android-Nutzer täuscht und ausspioniert

Fehler kommen in allen Softwareprodukten vor. Meist führen sie zu Fehlfunktionen oder Sicherheitsproblemen bei den Nutzern. Ein ganz anderes Kaliber ist es jedoch, wenn der größte Hersteller von Mobilfunksoftware beschließt, den Kunden heimlich ein Softwareupdate zu installieren, dass gegen deren ausdrücklichen Willen den Standort ermittelt und an die Firma überträgt.

Google ist Hersteller des Android-Betriebssystems mit einem Marktanteil von 87,7 %, das auf weit über einer Milliarde Geräten läuft. Dieser hohe Anteil zeigt die Beliebtheit der Geräte, die sehr viele praktische Eigenschaften in sich vereinen, aber auch sehr viel über die Kunden verraten.

Viele Android-Nutzer haben die Lokalisierung ihres Standortes ausgestellt

Zum Schutz der Privatsphäre bieten alle Smartphones in den Einstellungen die Option an, ihre Standortdaten nicht weiterzugeben. Und viele verwenden diese Einstellung auch, um nicht alle Details über sich zu verraten. Die Problematik von Bewegungsprofilen ist inzwischen allgemein bekannt und wird öffentlich seit über 6 Jahren diskutiert.

Einer Firma wie Google ist das natürlich auch nicht entgangen. Umso mehr verwundet es, wie man bei der Firmenleitung auf die Idee kommen kann, allen Kunden ein automatisches Update zu installieren, dass die ausdrückliche Vorgabe der Privatsphäre ausschaltet und eine Spionagesoftware installiert.

Die amerikanisch News-Seite Quartz fand heraus, dass Google seit Januar 2017 auf allen Android-Geräten ein Update installiert hat, dass genau diese Einstellung der Privatsphäre außer Kraft setzt und heimlich die Standortdaten an die Firma sendet. Technische Einzelheiten hierzu findet man bei Golem.de oder heise online.

Die Dreistigkeit geht so weit, dass auch ohne Benutzung irgendwelcher Apps und selbst bei Geräten, in denen sich keine SIM-Karte befindet, die Standortdaten gesendet werden. Und falls das Internet per WLAN ganz abgeschaltet ist, werden die Daten einfach zwischengespeichert und erst dann gesendet, wenn sich das Gerät wieder mit dem Netz verbindet, wie Quartz herausfand.

Google versucht sich herauszuwinden

Google wurde daraufhin zur Rede gestellt und gibt an, dass diese Aktion nur zum “Wohl des Kunden” durchgeführt wurde, um die so genannte Push-Benachrichtigung bei Chat- und Mail-Diensten zu verbessern. Niemals würden diese Daten weitergegeben oder gespeichert… Wer’s glauben mag, kann das tun.

Allerdings ist das ungefragte Installieren einer Spionagesoftware eine arglistige Täuschung des Kunden, wenn nicht sogar ein Straftatbestand – und seien die angeführten Gründe noch so ehrenhaft. Außerdem ist die Behauptung, Push-Benachrichtigungen mit Standortdaten verbessern zu wollen, eine glatte Lüge.

Eine Push-Nachricht wird an die IP-Adresse des Smartphones gesendet, um den Benutzer umgehend über eine neue Nachricht zu informieren. Die IP-Adresse gibt bereits eine ungefähre Information über den Standort des Gerätes und ist hierbei der einzige Weg, den Besitzer zu benachrichtigen. Google liegt mit der IP-Adresse daher bereits der ungefähre Standort vor. Selbst eine exakte Lokalisierung des Standortes lässt keinen anderen Weg zu, als dem Smartphone über diese eine IP eine Nachricht zu senden. Auch mit Kenntnis genauer Standortdaten lässt sich hier gar nichts “optimieren“. Es ist in etwa das gleiche, als bespitzelte man eine Person und behauptet, das würde dazu dienen, um Telefonate zu verbessern.

Google gelobt Besserung – mal wieder

Bis Dezember will Google die Software von den Geräten wieder entfernen. So lange dauert es, bis automatisch überall neue Updates installiert sind. Bis dahin sollte man sein Android-Smartphone ausschalten oder zu Hause lassen, wenn man seine Privatsphäre schützen will.

Google ist bereits in zahlreichen Ländern wegen immer wieder vorkommender Verstöße gegen Datenschutz und sogar Behinde-

rung der Justiz verurteilt worden. Daher ist die Wahrscheinlichkeit groß, dass der weltgrößte Spion und Datenhehler auch diesmal wieder rückfällig wird. Wer seinem Smartphone unbekümmert sein Privatleben anvertraut, bezahlt dafür mit seinen Daten.

US-Militär: Weltweite Überwachung sozialer Netzwerke

Der Sicherheitsforscher von UpGuard, Chris Vickery, ist auf einen riesigen Daten-Container des US-Militärs gestoßen. Gespeichert wurden darin Überwachungsdaten von Social-Media-Nutzern weltweit, die zudem in Amazons Cloud-Speicherdienst S3 öffentlich zugänglich waren für jedermann.

Bei einem Routinescan der Amazon-Cloud entdeckte der Security-Experte Chris Vickery cloudbasierte Speicherserver des US-Verteidigungsministeriums, bestückt mit mehreren TByte Rohdaten aus sozialen Netzwerken von Nutzern aus der ganzen Welt. Es handelt sich um drei riesige Datencontainer, die unter den Namen “Centcom-Backup”, “Centcom-Archive” und “Pacom-Archive” geführt wurden, wobei Centcom für die militärische Leitung der US-Streitkräfte Cental Command und Pacom für Pacific Command steht, also den Teil der Streitkräfte, der sich auf China, Asien und Australien konzentriert.

Zu Testzwecken lud Vickery eine Datenprobe von 400 Gigabyte herunter. In ihr enthalten waren rund 1,8 Milliarden Social-Media-Beiträge aus den vergangenen acht Jahren. Dem Forscher zufolge sind mindestens 1,8 Milliarden Posts, wie öffentliche Internetbeiträge, Kommentare, Beiträge in Webforen und ähnliches von Facebook, Twitter, YouTube und anderen sozialen Netzwerken gesammelt worden, die nach Sichtung vor allem aus Asien und den USA stammten.

Laut Vickery wäre es anhand der Datenstruktur und Verschlagwortung offensichtlich, dass die Daten zur Terrorabwehr gesammelt wurden. Zudem hat UpGuard ermittelt, dass die Datenpakete eine Firma namens VendorX analysiert hat. Informationen zufoge arbeitet die Firma an einem Projekt namens Outpost. Dieses Programm wäre als mehrsprachige Plattform dazu geeignet, Kampagnen zu starten, um die Meinung von Jugendlichen in instabilen Regionen der Welt zu beeinflussen. Weitere Hinweise fanden sich zu “Coral”, womit das Data-Mining-Programm Coral Reef gemeint sein könnte. Mit Coral Reef ist es Analysten möglich, in kürzester Zeit große Datenbestände zu durchleuchten, um Verbindungen und Kontaktnetzwerke aufzuzeigen.

Vickery wies das US-Militär auf die fehlerhafte Serverkonfiguration der S3-Server hin. Die bedankten sich und passten daraufhin die Sicherheitsmaßnahmen so an, dass Unbefugten künftig kein Zugriff darauf mehr möglich ist. Vickery war erstaunt darüber, wie fahrlässig mit solchen hochsensiblen Daten umgegangen wurde und welche Folgen an Datenmissbrauch sich theoretisch daraus ableiten ließen, auch wenn in diesem Fall keinen solchen Schäden bekannt geworden sind.

Smartwatch: Bundesnetzagentur untersagt den Verkauf von Kinderuhren mit Abhörfunktion

Wie die Bundesnetzagentur (BNetzA) in einer Pressemitteilung am 17.11.2017 informiert, verbietet sie den Verkauf und Besitz von Kinderuhren mit Abhörfunktion. Käufer einer solchen Smartwatch sollten sie laut der Behörde vernichten, denn der Besitz eines entsprechenden Gerätes ist strafbar. Gegen mehrere Angebote im Internet ist die Regulierungsbehörde bereits vorgegangen.

Hintergrund dieser Maßnahme ist die Tatsache, dass die Geräte zum unerlaubten Abhören der Umgebung des Trägers verwendet werden können und das völlig unbemerkt, weder das Kind noch sein Umfeld würde die Abhöraktion bemerken, denn verschiedene Smartwatches für Kinder verfügen über eine SIM-Karte und eine eingeschränkte Telefoniefunktion, die über eine App eingerichtet und auch aus der Ferne gesteuert werden kann, eine

sogenannte Babyphone- oder Monitorfunktion. Dabei lasse sich per App bestimmen, dass die Uhr unbemerkt vom Träger eine beliebige Telefonnummer anrufe, um so das Abhören der Gespräche des Uhrenträgers und dessen Umgebung ermöglichen.

Jochen Homann, Präsident der Bundesnetzagentur, erklärt dazu: „Über eine App können Eltern solche Kinderuhren nutzen, um unbemerkt die Umgebung des Kindes abzuhören“. Die Uhren seien somit als „unerlaubte Sendeanlage“ anzusehen. „Nach unseren Ermittlungen werden die Uhren von Eltern zum Beispiel auch zum Abhören von Lehrern im Unterricht genutzt.“ So gehe es darum, das “Umfeld von Kindern zu schützen”. Solche Abhöraktionen sind in Deutschland verboten.

Laut Netzagentur gibt es auf dem deutschen Markt zahlreiche Anbieter von Smartwatches für Kinder mit einer Abhörfunktion. Zielgruppe sind vor allem Kinder im Alter von fünf bis zwölf Jahren. Haben Eltern eine solche Uhr einmal gekauft, wird ihnen von der Bundesnetzagentur geraten, die Uhren eigenständig unschädlich zu machen und einen Vernichtungsnachweise, wie beispielsweise das Bestätigungsschreiben einer Abfallwirtschaftsstation, bei der die vernichtete Uhr abgegeben wurde, aufzubewahren. Aber auch Schulen sollten verstärkt auf Uhren mit Abhörfunktion bei Schülern achten, denn der Besitz einer solchen Uhr ist laut der Behörde in Deutschland strafbar. Aus den gleichen Gründen hatte die Behörde Anfang des Jahres die Kinderpuppe “Cayla” aus dem Verkehr gezogen. Sie war ebenso in der Lage, unbemerkt Gespräche des Kindes und seiner Umgebung aufzunehmen und weiterzuleiten, die Puppe verfügte über ein Mikrofon und eine Funkverbindung.

Telegram-Gruppe der Tarnkappe bald mit 200 Teilnehmern

Anfang Oktober eröffneten wir unseren öffentlichen Treffpunkt beim Messaging Dienst Telegram, seitdem ist die Anzahl der Nutzer stetig nach oben gegangen. Tagsüber diskutieren im Durchschnitt rund fünf Personen miteinander, angemeldet sind dort momentan fast 200 Nutzer. Leider lesen viele einfach nur still mit, statt sich einzubringen.

Natürlich würde es viele andere Möglichkeiten geben, sich inhaltlich zu beteiligen oder uns Feedback zu geben. Aber über den direkten Austausch im Chat geht einfach nichts drüber. Zwar könnte man untereinander und mit uns per Facebook, Google Plus, Twitter oder in den Kommentaren in Kontakt treten. Doch das hindert zahlreiche Personen nicht daran, tagtäglich bei uns in der Telegram-Gruppe reinzuschauen.

Zugegeben: Es sind irgendwie zumeist die gleichen Gesichter, die man dort sehen bzw. lesen kann. Es geht oft um technische Fragen wie VPN-Anbieter, die Absicherung von Servern, gute Linux-Distributionen oder aber, warum Sharehoster X schon seit einigen Tagen nicht mehr als Geschwindigkeit Y beim Download zulässt. Der Austausch beginnt wochentags schon am frühen Morgen und endet oft erst tief in der Nacht. Der Tonfall ist zumeist sehr freundlich, nicht nur Kati Müller ist beim Beantworten der gestellten Fragen überaus hilfsbereit. Übrigens kam Kati über den Chat bei Telegram auf uns zu und fragte, ob sie nicht für uns schreiben könne.

Du hast davon bisher noch gar nichts mitbekommen und hast jetzt Lust bekommen, mitzumachen? Kein Problem! Installiere Dir einfach den kostenlosen Messenger Telegram, die es für beinahe jedes Betriebssystem gibt und mach mit! Einfach auf die unten stehende Grafik klicken, der Link führt Dich nach erfolgter Installation von Telegram automatisch in unsere Gruppe.

Jede und jeder unabhängig von Alter, Rasse, Geschlecht, Religionszugehörigkeit, politischer Einstellung oder OS ist dort willkommen, solange er die Meinung Dritter akzeptiert und nicht den normalen Ablauf stört. Anfragen nach Schwarzkopien bitten wir woanders zu stellen, wir sind keine Warez-Börse und wollen auch keine werden. Dafür gibt es im Netz mehr als genug andere Orte und Möglichkeiten, sich diesbezüglich zu erkundigen.

Und denkt bitte daran: Sicher verschlüsselt ist die Kommu-

nikation bei Telegram nur in einem sogenannten geheimen Chat. Dieser startet erst, sobald beide Kommunikationspartner online sind. Alles was ihr in einem normalen Chat oder in einer Gruppe schreibt, wird auf den Servern von Telegram gespeichert und nicht Ende-zu-Ende-verschlüsselt. Und nur bei der Methode haben lediglich die beiden Chat-Partner die Schlüssel, um die übertragenden Daten zu entschlüsseln.

P.S.: Wir sind nicht 24 Stunden am Tag verfügbar. Bitte nicht wundern oder sauer sein, sollte mal niemand vom Team online sein. Die meisten eurer Fragen können die anderen Nutzer genauso gut beantworten.

Unter dem Radar: Der satirische Monatsrückblick (November/2017)

Über den November wissen viele Menschen nur schlechtes zu sagen. Kalt, dunkel und nass sorgt er bei der Mehrheit eher für düstere Stimmung. Da ist es gut, dass auf unsere Prominenten und Einflussreichen wieder einmal Verlass war. Heldenhaft sprangen sie in die Bresche, um mit großem Einsatz für Kopfschütteln und ungläubiges Lachen zu sorgen und so die aufkommende Novemberdepression zu vertreiben. Wir teilen dieses Wundermittel für die Stimmung im neuen satirischen Monatsrückblick.

Es war einmal im Neuland

Die nun beginnende Weihnachtszeit ist eine Zeit, in der häufig die Nostalgie und die Sehnsucht nach einfacheren, vermeintlich besseren Zeiten herrschen. Das haben anscheinend auch einige Regierende vorweg genommen. Überfordert mit der freien Wissensgesellschaft des 21. Jahrhunderts sehnen sie sich nach Zeiten, in denen weltweite Kommunikation, breite Verfügbarkeit von Wissen und freier Austausch von Informationen noch reines Wunschdenken waren. Glücklicherweise gibt es Möglichkeiten, diesen Zustand auch heutzutage noch passabel zu simulieren. Eines der besten Mittel dazu: Netzsperren. Da ist es kein Wunder, dass sich dieses probate Mittel gelebter Traditionspflege in den letzten Jahren steigender Beliebtheit erfreut. Es geht einfach nur um ein wohliges Gefühl mitten im kalten Winter, ein Stück Heimat im unwirtlichen Neuland.

US Army is Coming to Town

Ebenfalls schon weihnachtlich geht es beim US-Militär zu. Das nämlich nimmt sich gerne ein Beispiel am Weihnachtsmann: es weiß dank Überwachung sozialer Netzwerke, wann wir schlafen, wann wir wach sind und wahrscheinlich auch, ob wir schön brav waren… Nun ja, letzteres ist fraglich, da die wenigsten Leute in den sozialen Medien ehrlich sind. Da stellen sich viele, deren Leben eigentlich alles andere als vorbildlich verläuft, gerne so dar, als hätten sie alles im Griff. Im Gegenzug gibt es bestimmt auch so manchen braven Langweiler, der auf Facebook und Instagram den Harten mimt, als verdiene er vom Nikolaus mindestens drei Ruten. Das dürfte für Chaos bei der Geschenkeverteilung sorgen. Wahrscheinlich werden die USA alsbald wieder zu ihrem gewohnten System übergehen: böse sind die, die entweder einen muslimisch klingenden Namen haben oder von irgendwem verdächtigt werden, Kommunisten zu sein. Das ist zwar auch nicht fairer, aber wenigstens weniger verwirrend. Ho ho ho!

Two Girls, one Selfie

Kurioses gegen saisonal düstere Stimmung bietet ein neues Pilotprojekt des Sozialen Netzwerks Facebook. Dieses testet eine neuartige Methode, um Bots von menschlichen Nutzern zu unterscheiden. Statt wie bisher langweilige Mathe-Aufgaben zu lösen oder vollkommen verzerrte Texte entziffern zu müssen (letzteres ist immerhin lebensnah, berücksichtigt man die typische Handschrift junger Digital Natives), sollen Nutzer, die verdächtigt werden, Bots zu sein, künftig aufgefordert werden, ein Selfie hochzuladen.

Was könnte schiefgehen? Nun, nimmt man das typisch chaotische Verhalten von Internetnutzern zum Anlass, eine ganze Menge. Meine Vermutung ist, dass bei zehn Selfies min-

destens vier männliche Geschlechtsteile, ein Bild von Donald Trump und eine Toilette dabei sein werden, nebst einiger kreativerer Dinge, für die meine Fantasie selbst nach annähernd zwei Jahrzehnten Internet noch zu unschuldig ist.

Auf ins Winterwunderland

Wie ihr seht, gibt es auch in der dunklen Jahreszeit keinerlei Grund zur Verzweiflung. Rettung für die Stimmung naht, sei es in Form von Geschichts-Reenactment im Neuland oder von Santa Clause und seinen fleißigen Helferlein. Da fällt der Übergang in die nun folgende, hektische Weihnachtszeit doch gleich leichter.

In diesem Sinne: macht es gut, verirrt euch nicht im Neuland und lasst euch vor allem nicht mit Wham! beschallen.

Unter dem Radar: Der satirische Monatsrückblick (Dezember/2017)

Der Dezember – ein Monat voller Harmonie und Besinnlichkeit, so dachten wir zumindest. Was wir allerdings stattdessen zu sehen bekamen, war eher ein so kapitaler Verkehrsunfall, als habe der Weihnachtsmann die Steuerung seines Schlittens an ein betrunkenes Rentier delegiert. Lest die Details des Unfallhergangs in unserem Monatsrückblick. Türchen-Thomas und der Fernseher des Grauens

Wo wir gerade beim Schlitten sind – diesen würde unser Bundesinnenminister, Thomas de Maizière, nur zu gerne überwachen. Geschieht dem Weihnachtsmann nur recht, er weiß schließlich auch immer, was wir gerade tun und ob wir schön artig sind. Neben Santas heißem Gefährt möchte der Innenminister auch Autos, Computer, Smart-TVs und alle möglichen anderen, an das "Internet der Dinge" angeschlossenen Geräte überwachen. Sie alle sollen demnächst Software-Hintertüren für Staatstrojaner eingebaut bekommen. Anscheinend hat Herrn de Maizière das Türchen-Öffnen an seinem Adventskalender so gut gefallen, dass er unbedingt das ganze Jahr damit weiter machen möchte, und sei es bei der Firmware von Nachbars neuem 50-Zoll-TV.

Die Idee ist typisch brillant. Ein für die öffentliche Sicherheit, sagen wir, nicht ganz unwichtiges Gerät wie ein Auto, auf dem eine dilettantische, lückenhafte Schadsoftware made by German Staats-supercyberbeauftragte, installiert wird – was könnte schiefgehen? Wenn sich diese Pläne durchsetzen, haben zumindest Europas Online-Kriminelle demnächst eine üppige Bescherung.

Die Gefahr lauert in der Packstation

Ebenfalls ein großes Thema rund um Weihnachten 2017: der Versandhandel. Wer sich nicht darauf verlassen will, dass der Weihnachtsmann – oder dessen Rentier – den Weg zu seinen Lieben findet, bestellt die Geschenke gerne online. Klingt harmlos, oder? Ist es aber nicht, wenn man wiederum Herrn de Maizière glaubt. Der Gute fühlt sich offenbar nicht nur von Autos und Fernsehern bedroht, sondern ganz besonders von Menschen, die Pakete aus DHL-Packstationen holen. Der Abwechslung halber sollen diese Packstationen aber keine Software-Backdoors bekommen, sondern flächendeckend videoüberwacht werden.

Was der Minister dabei zu sehen glaubt, bleibt wohl sein Geheimnis. Den in Schlangenlinien anfliegenden, rotnasigen Rudolph, der sich die Beschaffung der Geschenke erleichtert? Gelangweilte sexy Hausfrauen in knapper Unterwäsche? Böse Kommunisten bei der Umverteilung von… irgendwas? Extremistische Cybers? Notfalls egal, Hauptsache Videoüberwachung, ist wohl die typische Logik von Herrn de Maizière und seiner Partei…

Selbst ist der Weihnachtsmann

Enttäuscht von den Weihnachtsgeschenken? Wieder nur einen hässlichen Schlafanzug von Tante Frieda bekommen? Da hilft nur eins – sich demnächst die passenden Geschenke selbst machen. Das dachte sich wohl auch eine US-amerikanische Hackergruppe und bescherte sich kurzerhand mit 10 Millionen US-Dollar aus dem Fundus diverser Banken selbst. Das sah bestimmt beeindruckend unter dem Weihnachtsbaum aus. Bonuspunkte gibt es für den kreativen Namen "Money-Taker". Nach dieser Logik heißt unsere Bahn-Gesellschaft zukünftig "LateComer" und die nächste politische Partei, die in

Deutschland gegründet wird, bestimmt “LyingPowerTaker” – was in seiner Ehrlichkeit fast schon wieder sympathisch wäre. Über die Wählbarkeit besagter Partei ließe sich vermutlich eher streiten, aber in Zeiten von UKIP und Donald Trump ist diese Maßeinheit sowieso eine sehr subjektive…

Guten Rutsch – möglichst unfallfrei

Wie ihr seht, gab es im Dezember durchaus noch anderes zu tun, als Geschenke zu kaufen (mit oder ohne Packstation), über Weihnachtsmärkte zu bummeln oder zuhause mit Tee und Plätzchen vor dem Kamin zu sitzen. Auch die Beobachtung des alltäglichen Wahnsinns dort draußen, von Verkehrsunfall-Rudi bis Paranoia-Thomas, vermochte zu erheitern und die langen, dunklen Abende zu verkürzen. Es bleibt zu hoffen, dass ihr weder von einem verirrten Schlitten angefahren noch beim Paket-Abholen festgenommen wurdet und sich auch die Geschenke durchweg erfreulich gestalteten. Ansonsten wisst ihr ja im nächsten Jahr, was zu tun ist.

Ich wünsche allen Leserinnen und Lesern bei dieser Gelegenheit einen guten Rutsch. Kommt gesund und fröhlich, möglichst auch ohne unerfreuliche Begegnungen mit Rentieren und Cybers, ins neue Jahr. Wir lesen uns dann 2018 in alter Frische wieder. Ich bin sicher, dass uns die Themen für den satirischen Monatsrückblick nicht ausgehen werden.

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

05

digital
publishing
momentum