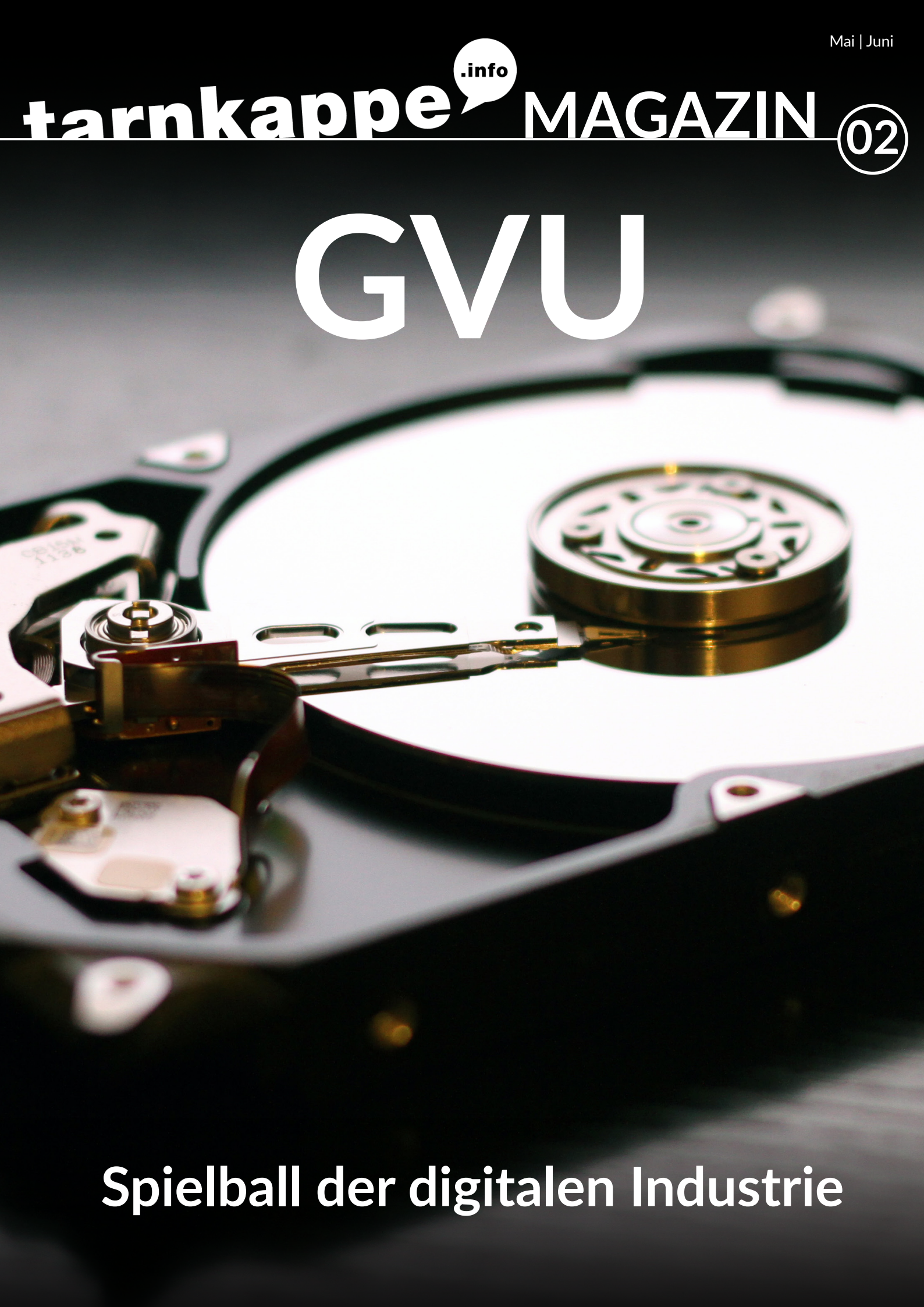
Mai | Juni

tarnkappe.info MAGAZIN 02

GVU



Spielball der digitalen Industrie

Liebe Leserinnen und Leser,

die Redaktion erreichte eine Anfrage eines wirklich verzweifelten Mannes. Der frühere Kunde des illegalen Download-Portals Lesen & Lauschen, aktiv unter der Internet-Adresse LuL.to, kann nach eigenen Angaben seit dem 21. Juni nachts kein Auge mehr zumachen. Er ist etwa sechzig Jahre alt und wohnt jenseits der Weißwurstgrenze. Wie er erzählt, kam er im Laufe vieler Monate gar nicht auf die Idee, die Bezahl-Webseite auf ihre Legalität zu überprüfen. Die Seite für preiswerte E-Books und Hörbücher sah in seinen Augen so professionell aus, das konnte doch eigentlich nur ein reguläres Angebot sein, dachte er. Auf den enormen Preisunterschied zu anderen Webseiten angesprochen, wusste er keine Erklärung, warum ihn das nicht stutzig machte. Auch die Endung der Internet-Adresse, also die Domain in Tonga, rüttelte ihn nicht wach. Umso wacher wurde er allerdings, als er plötzlich statt der Startseite von LuL den Warnhinweis der Polizei sah und Sekunden später auf diversen News-Portalen nachlesen musste, auf was er sich da eingelassen hat. [**1**]

Der ältere Herr aus Süddeutschland hat schon mehrfach ernsthaft in Erwägung gezogen, sich in Anbetracht der möglichen Konsequenzen „vor einen Zug“ zu werfen. Er kam auf uns, weil wir über die möglichen straf- und zivilrechtlichen Konsequenzen der Nutzung von LuL ausführlich berichtet haben. [**2**]

Klar ist einerseits, dass noch gar nicht entschieden ist, ob überhaupt gegen die Käufer der illegal beschafften Ware ermittelt wird. Polizeien und Staatsanwaltschaften haben sich in solchen Fällen bislang stets auf die Betreiber gestürzt, weil sie finanziell von ihrem Projekt profitiert haben. Ob die Verlage ihre eigenen Leser abmahnen oder die Staatsanwälte strafrechtlich gegen eben diese vorgehen wollen, bleibt also in Ruhe abzuwarten. Aber genau das ist es ja, was den ehemaligen LuL-Kunden so schwer fällt. In Anbetracht der Aussicht auf empfindliche Strafen oder hochpreisige Kostennoten von Abmahn-Anwälten ist es beinahe unmöglich, ruhig zu bleiben. Das zeigen unter anderem auch sehr deutlich die vielen Kommentare aufgeschreckter LuL-Konsumenten hier und anderswo. Andererseits hätte sich der Betroffene ausführlicher informieren müssen, von wem er denn da jetzt ganz genau die digitalen Bücher erwirbt. Es existierte dort naturgemäß kein regelkonformes Impressum samt ladungsfähiger Adresse der Macher. Und es gab auch Hinweise innerhalb der Webseite, dass es die LuL-Betreiber mit der Gesetzgebung nicht so ganz so genau nehmen. Wir halten fest: Phlegmatismus und Ahnungslosigkeit schützen vor Strafe nicht. Sollte es tatsächlich zu einem Gerichtsverfahren kommen, dann werden sich die Käufer kaum damit herausreden können, dass sie halt nicht so genau geprüft haben, wo der ganze heiße Scheiß zum Schleuderpreis herkam. Der fassungslose Rentner wird sicher kein Einzelfall sein. Und dennoch wird die Mehrzahl der LuL-User genau gewusst haben, was sie dort taten. Offenbar fühlten sie sich ähnlich sicher, wie die drei Betreiber, die wahrscheinlich noch immer in Untersuchungshaft sitzen. Festzuhalten ist ferner, dass das Geschäftsmodell von LuL verachtenswert ist. Den Hintermännern ging es nicht darum, ihren Besuchern etwas Gutes zu tun. [**3**]

Hierbei stand einzig die Gewinnmaximierung, respektive die persönliche Bereicherung der Kriminellen, im Vordergrund. Natürlich kann man versuchen, das wegzudiskutieren oder die Handlungen der Verhafteten irgendwie zu verharmlosen. Doch selbst die völlig überzogenen Preise für E-Books, die die Verlage mit oder ohne LuL nicht modifizieren werden, ändern nichts an der Faktenlage.

Die GVU als Spielball der digitalen Industrie? Gegen die Buchpiraten ist es den meisten Verlagen auch gar nicht wert, vorzugehen. Eine Möglichkeit wäre es, ein bezahltes Mitglied der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU) zu werden, die dann stellvertretend für sie alle Ermittlungen übernimmt. Doch dies ist vielen Chefetagen entweder zu teuer oder viel zu unwichtig, weil auch im letzten Quartal im Durchschnitt nur etwas über 5 Prozent aller verkauften Werke digitaler Natur waren. [4]

E-Books sind in Deutschland trotz der vielen Smartphones, die hierzulande genutzt werden, eine Nische geblieben. Vor dem Hintergrund erscheint der durch Online-Piraterie erzeugte Schaden wohl eher überschaubar. Beliebt bei den Verlagen oder nicht, wir werfen in dieser Ausgabe einen ausführlichen Blick auf die Helfershelfer der Rechteinhaber, also auf die GVU. Wie funktioniert dieser Verein, der alles andere als gemeinnützig ist und dessen Sitz absichtlich vor einigen Jahren vom schönen Hamburg in die Bundeshauptstadt Berlin verlegt wurde? Mit welchen Mitteln wird versucht, die Piraten zu bekämpfen? Heißt konkret sie zu identifizieren, damit man gegen sie vorgehen kann. Und warum wäre es für die GVU katastrophal, wenn der Verein eines schönen Tages seine Mission zu einhundert Prozent erfüllen würde?

Ihr Lars Sobiraj
Ihre Redaktion von Tarnkappe.info

SZENE

Themenübersicht

ZZB00T: POLIZEI FASST MUTMASSLICHEN CYBER-ERPRESSER

Am Dienstag, den 23.05.2017 gelang es dem Fachkommissariat für Computerkriminalität der Bielefelder Kriminalpolizei in Zusammenarbeit mit der Schwerpunktabteilung für Wirtschaftskriminalität der Staatsanwaltschaft Bielefeld, den bundesweit tätigen DDoS-Erpresser namens „ZZB00t“ festzunehmen. Der 24-jährige Fachinformatiker forderte laut Polizeibericht Lösegeld von namhaften deutschen Firmen.

Nach Angaben des Link11 Security Operations Centers (LSOC) startete der 24-jährige Fachinformatiker aus Voerde am Niederrhein seit dem 22. April diesen Jahres wiederholt DDoS-Angriffe gegen Webseiten. Die meisten seiner Opfer hatten ihren Sitz in Deutschland. Auf der Suche nach Schwächen in der IT-Infrastruktur hat er unter dem Pseudonym ZZb00t bereits erfolgreich E-Commerce-Shops, Logistikunternehmen und Telekommunikationsanbieter angegriffen. Er soll über ein Bot-Netzwerk die Webseiten namhafter deutscher Firmen mit DDoS-Attacken lahmgelegt haben, um ein Lösegeld in Bitcoin zu erpressen. Demnach wollte er die Angriffe beenden, sobald die Unternehmen bereit waren, auf seine Lösegeldforderungen einzugehen.

Auch über Twitter kommentierte der 24-Jährige seine DDoS-Aktivitäten. Dort gab er bekannt, dass er zuvor als IT-Sicherheitsberater gearbeitet hat. Er benutzte die Tweets als Plattform zur Veröffentlichung seiner Angriffe. Zudem verspottete er seine Opfer: „Habe ich erwähnt, dass ich während eines Angriffs Hardstyle höre?“

Beamte eines Spezialeinsatzkommandos nahmen den Täter am Dienstag (23.05.2017), noch vor seinem Rechner sitzend, fest. Kriminalbeamte führten ihn dem Haftrichter vor, der ihn wegen Verdacht auf Erpressung in Untersuchungshaft schickte. Die Ermittlungen dauern an. Es gibt zunächst keine näheren Angaben zur Höhe der Beute. Ferner ist nichts darüber bekannt, wie die Ermittler dem Mann auf die Schliche gekommen sind. Es habe aber eine Reihe von Anzeigen gegeben.

Obwohl viele der betroffenen Unternehmen einen DDoS-Schutz gekauft hatten, waren sie gegen diese Angriffe wehrlos. Die Link11 Security Operations Centers (LSOC) hat die Angriffe des Cyberkriminellen und die fehlerhafte Verteidigung der Anti-DDoS-Dienstleister analysiert.

Auch wir von Tarnkappe.info waren in der Vergangenheit bereits mehrfach massiven DDoS-Angriffen ausgesetzt, was unseren Webserver häufiger zum Stillstand brachte. Seit dem Einsatz von Google Project Shield, gehören Angriffe dieser Art nunmehr der Vergangenheit an.

GOOGLE DRIVE: IMMER ÄRGER MIT PIRATEN

Googles Cloud-Speicher Drive wird zunehmend für illegale Zwecke missbraucht. Wie TorrentFreak berichtet, bedienen sich aktuell häufiger Piratenseiten mit ihren illegalen Streaming-Angeboten urheberrechtlich geschützter Filme und Serien dieses von Google bereitgestellten Dienstes.

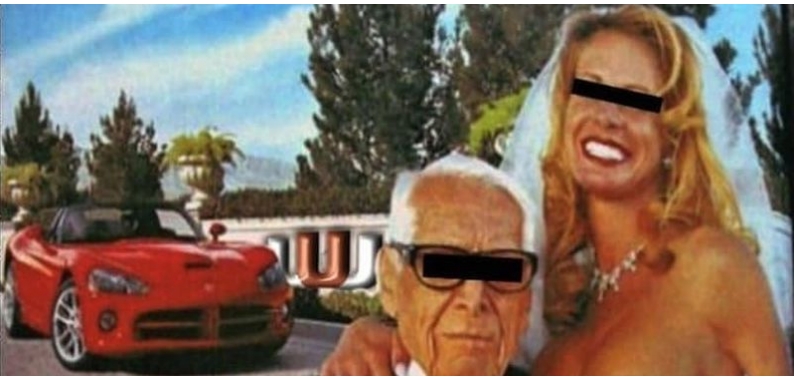
Googles Werbeslogan für den Cloud-Speicher Drive: „Alle Ihre Dateien – immer und überall einsatzbereit“ verspricht den Kunden Datenzugriff zu jeder Zeit und von jedem beliebigen Gerät, egal ob Smartphone, Tablet oder Computer. Diese einmal dort gespeicherten Daten sind für alle berechtigten Nutzer erreichbar und lassen sich zudem auch von Usern, denen man Zugriff darauf gewährt, abrufen.

Entsprechend nutzen gegenwärtig ebenso illegale Streaming-Dienste die bereitgestellten Leistungen Google Drives zu ihrem Vorteil. Die Piraten-Website-Betreiber haben offenbar einen Weg gefunden, um Videos direkt aus Google Drive und verschiedenen anderen Quellen zu streamen. Mit einem Trick umgehen sie bisher erfolgreich die Filter Googles, die eigentlich urheberrechtlich geschütztes Material er-

kennen sollten. So können sie oft eine Vielzahl an Features gleich mit anbieten, über die andere Plattformen nicht verfügen, wie optionale Untertitel oder Chromecast-Unterstützung.

Natürlich bleiben diese Aktivitäten den Rechteinhabern nicht verborgen. Laut dem Transparenzbericht wurden Google beispielsweise für die Domain Googlevideo.com bis zum Ende des vergangenen Jahres rund 13.000 dieser URLs gemeldet, im Jahr 2017 erhöhte sich die Zahl bisher sogar auf mehr als 265.000 Löschanfragen. Dabei handelt es sich lediglich um Anfragen, bestimmte URLs aus der Suche zu entfernen. Allein der massive Anstieg zeigt deutlich, dass dies ein ernstzunehmendes Problem für die Rechteinhaber ist. Es ist unklar, wieso es Google nicht gelingt, solche Inhalte frühzeitig zu erkennen und illegale Streamer von seinen Diensten auszusperren.

Der Konzern gab dazu bislang keine Stellungnahme ab. Laut TorrentFreak wurden aber in den vergangenen Tagen „hunderte oder gar tausende“ Google-Drive-Konten wegen angeblicher Verstöße gesperrt, besonders solche Business-Accounts, die offenbar rechtswidrig über eBay gehandelt worden und über unbegrenzten Speicherplatz verfügen. Viele der Konten sind auch mit Streaming-Hosts verknüpft. So könnte es sein, dass dies der erste Schritt von Google ist, um die Situation besser in den Griff zu bekommen.



STATEMENT VON DER AUTORIN MARINELLA CHARLOTTE VAN TEN HAARLEN

Auf meine Anfrage hin hat sich die Autorin Marinella Charlotte van ten Haarlen bereit erklärt, sich bei uns exclusiv zu dem Bust von LuL.to zu äußern. Sie war ja bekanntermaßen die Autorin, die mit einer Anzeige gegen die Betreiber und der gleichzeitigen Aussetzung eines Kopfgeldes erste Schritte gegen LuL.to unternahm und damit im Namen aller Autoren agierte.

Völlig anders als Romanautor Richard, dem es ausschließlich nur um seine entgangenen Gewinne geht und für den alle Downloader schwarze Schafe sind, die nun für ihre Vergehen büßen müssen, hat sie ihr erklärtes Ziel – LuL.to für immer vom Netz zu nehmen – erreicht. Alles weitere liegt nun „in den Händen der Ermittlungsbehörden“, schreibt sie.

An dieser Stelle veröffentlichen wir ihr vollständiges Statement.

Sehr geehrte Antonia,

danke für die Anfrage.

Vorab: Einen besonderen Dank möchte ich der GVU aussprechen. Die beiden Herren, die gemeint sind, wissen schon warum. Insbesondere auch H. und A. für ihre moralische und menschliche Unterstützung in der Zeit. Mein Beitrag an der Ergreifung von Lul.to ist eher klein.

Danke auch an die Beamten des LKA Sachsen und herzlichen Dank auch an die Generalstaatsanwaltschaft Bamberg, die Lul.to zur Strecke brachte.

Danke auch für Ihr Kompliment, Antonia. Zumindest verstanden Sie meinen damaligen „Aufschrei“. Lars sah die Klickraten steigend!

Ideale

Ich bin für alle Autoren eingetreten, weil sich niemand traute. Ich schreibe Bücher, weil ich meine Ideale leben will, nicht nur darüber schreiben will.

Autoren haben das Recht auf gerechte Entlohnung – nicht ein selbst ernannter Pirat legt die Preise fest, sondern die Autoren, die Verlage.

Ich würde Lul.to gerne im Supermarkt sehen, wenn die Piraten sich nur Rotkäppchen-Sekt leisten können, aber dann Veuve Cliquot klauen gehen. Bei der dritten Flasche würden sie auch im Knast sitzen.

Ich bin ein Querkopf

Gleich, für wen, auch für die, die „Alle meine Entchen“ neu verfassen, für alle, bin ich eingetreten. Ich würde es wieder tun, wieder für alle. Das bedeutet für mich, meine Ideale zu leben. Scheißegal, was die Welt über mich denkt. Mein Gewissen interessiert mich.

Ich bin von dem Bodensatz der Trolle für meine Zivilcourage verleumdet, bedroht und öffentlich diskreditiert worden. Gegen zwei dieser Personen (Trolle) habe ich Strafanzeige gestellt, sonst habe ich die besten Morddrohungen und Gewalt (Vergewaltigungs)-fantasien, Erpressungsversuche, Beleidigungen, üble Nachrede gesammelt. Zumal ich als eine Person geschildert wurde, mit der ich nichts zu tun habe. Es wurde eine passende Geschichte erfunden, um mich für die Rechtfertigungsorgie der Lysander- Jünger griffiger zu machen. Da müssen sich einige User fragen lassen, ob das Verhalten nicht schon Beihilfe war.

Das sollen das Gericht/ die Staatsanwaltschaft entscheiden.

Ich gebe diese außergewöhnliche Sammlung gerne dem Richter in der Verhandlung gegen Lul.to. Er kann in seinem Geschäftsbereich damit sehr viel mehr anfangen. Das erstreckt sich natürlich auch auf die Kommentatoren unter dem nunmehr angefragten Beitrag. Ich sammle gerne weiter, auch wegen meiner „Hommage an Lul.to“, die ich in Form eines Artikels online setzen werde. Screenshots inklusive.

Die Äußerungen von Lul.to, aus 2015, kann man als öffentlichen Aufruf zu Straftaten gegen mich verstehen, was dann auch, zu meinem tiefsten Bedauern, eintrat. Zum Teil waren die Drohungen in §130 StGB (Volksverhetzung) zu suchen. Mehr Niveau hatten die Schreiberlinge nicht.

Quintessenz

Zitieren Sie mal, das, was Sie mir schrieben, das haben die Leute, User und ein Teil der Schriftsteller, noch nicht begriffen:

Zitat: „Vor einiger Zeit haben sie in ihren ausführlichen Kommentaren bei uns die Erstellung einer Strafanzeige gegen lul.to angekündigt und zudem eine Belohnung auf die Betreiber von lul.to ausgesetzt.“

Schließlich wurden ihr Einsatz und Engagement doch von Erfolg gekrönt, da die Täter nun gefasst sind. Sicher ist es nicht zuletzt ihrem beherzten Eingreifen zu verdanken, dass die Autoren nun künftig von weiteren Raubkopien in einem solch großen Maßstab verschont werden, denn LuL.to war der wohl einzige Einkäufer von Neuerscheinungen. Es ist folglich davon auszugehen, dass alle anderen Boards sich in der Scene nur bei ihnen bedient haben.“

Ja, ich habe Lul.to wegen zahlreicher Delikte angezeigt. Ich bin als konsequent bekannt. Was ich öffentlich ankündige, betreibe ich auch.

Bis zur Lächerlichkeit versegelt

Was ich nicht ertragen kann, ist Feigheit in allen Formen. Lysander hat mit extremer Brutalität gegen Kritiker gearbeitet. Lysander ist und war schrecklich feige und gleichermaßen gierig.

Lysander wollte, wie in guten Tagen auf Tortola, ein Kopfgeld auf sich vereinen. Dem Wunsch bin ich nachgekommen. Er fing an, Fehler zu machen, das freute mich. Das war genau der Punkt, den ich erreichen wollte. Mit Kopfgeld a la Joost van Dyk hat er nicht gerechnet. Mit allem, nur nicht damit. Er musste immer Verräter in seinen eigenen Reihen fürchten. Letztendlich waren damals schon Verräter am Werk, Lul.to hatte sich verselbstständigt. Ein Pirat beschiss den anderen. Das war der Untergang der modernen „Holzbeine“.

In seiner unendlichen Arroganz und Selbstüberschätzung segelte Lysander über seinen Horizont hinaus. Vielleicht war die Erde für ihn doch eine Scheibe.

Ich wurde nach der Aufstachelung durch Lysander und den Trollen, zahlreichen weiteren Straftaten ausgesetzt, die Gegenstand einer polizeilichen, respektive staatsanwaltschaftlichen Ermittlung sind. Ich habe Vertrauen in die Fähigkeiten derer, die den Staat Bundesrepublik Deutschland vertreten.

Ich stelle fest, die Person auf dem Bild, das den Hund und mich zeigen soll, war ich nicht, gab letztendlich aber für die folgenden Ereignisse einen wichtigen Aufschluss: Lul.to hat sich bis zur Lächerlichkeit versegelt.

Der Rechtsstaat in der Bundesrepublik ist nun an der Aufarbeitung des „Gesamtwerkes Lul.to“ gefordert.

Dabei interessiert es mich auch nicht, ob der Bodensatz der Gesellschaft, meine Bücher „scheiße“ findet. Sollen sie doch. Die geistige Armut, einen mutmaßlichen 129er StGB öffentlich zu verteidigen, muss man erst einmal haben. Solche Leser sind nicht nötig. Ein feiges Versteckspielen hinter Kommentaren, die den Schreiber der Intelligenz schon beim

Verfassen dieser berauben, ist der Ausdruck dessen, was die notorischen Schnorrer und Lysanders Mitstreiter vermögen. Lul.to war ein Parasit der übelsten Sorte.

Useless

Antonia, ich kann nicht sagen, ob die User vor Strafverfahren zittern. Ehrlich, mir ist es egal. Die User können zittern wie Espenlaub oder sich der Downloads erfreuen, solange sie das noch können.

Es liegt in den Händen der Ermittlungsbehörden.

Lysander hatte weniger Glaubwürdigkeit als Kapitän Blaubär. Jeder, der mit ihm segelte, muss sich fragen, warum „er nun an den Füßen zuerst aufgehängt wird“. Ich denke da zurück an „rechtliche Grauzone“ etc. Jedem Vorschüler war klar, dass Lysander und seine Mannschaft, Kriminelle waren, die nur an ihren eigenen Vorteil dachten.

Wobei, wir dürfen nicht vergessen, die Unschuldsvermutung gilt auch für Lysander und seine verquere Weltansicht vom parasitären Dasein eines modernen Psychopathen.

Lysander und seine mutmaßlichen Mittäter sollen jegliche Vorteile des modernen Rechtsstaates genießen, den sie so sehr durch ihr Tun ablehnen.

Das wünsche ich ihm von ganzem Herzen.

Lysander, der wahrscheinlich noch unter den Lebenden weilen wird, und seine Gruppe von romantischen Nachruf-Legasthenikern sollen sich erklären.

Ich kann mich einer zusätzlichen Schadenfreude nicht erwehren. Das ist menschlich. Fast prophetisch gab Lysander damals seine Stellungnahme gegenüber Tarnkappe ab. In die Glaskugel geschaut – er wird darben. Shame.

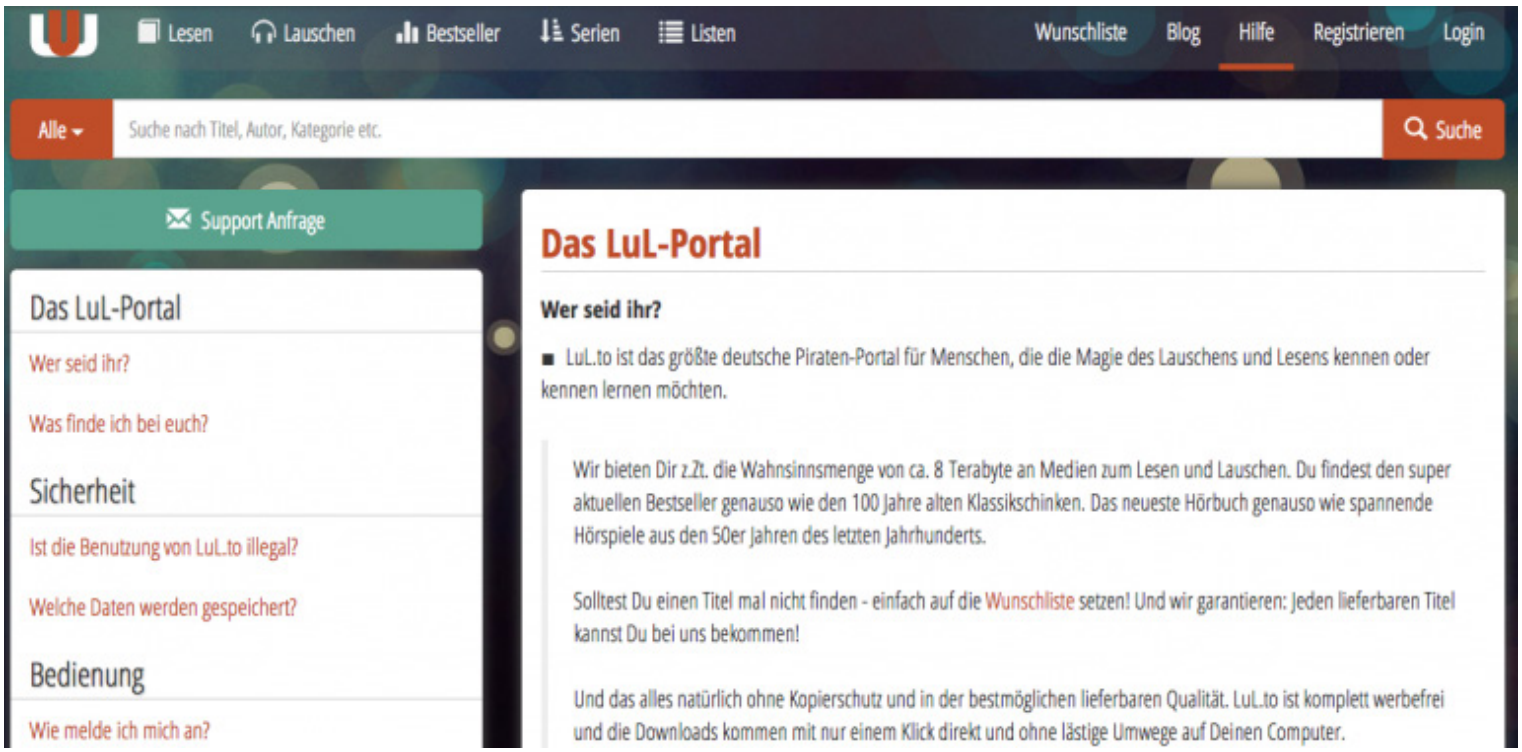
Das geht mir runter wie Öl: „So ein Mist, jetzt bin ich aufgeflogen. Vorbei all die Vergnügen, die ich mir durch das Abzocken von ahnungslosen E-Book-Downloadern leisten konnte. Ab morgen muss ich darben, weil uns eine frustrierte Indie-Autorin gnadenlos verfolgt und zur Strecke gebracht hat. (Ja, da guckst Du!!!) Reuemütig werde ich ihr all meine Bankschließfächer öffnen und ihr helfen, mein mühsam ergaunertes Geld wegzuschaffen. (Das macht schon die Polizei) Wie man oben auf dem Bild sehen kann, bin ich ja nicht mehr der Jüngste. Ich werde nun die letzten Tage meines Lebens in bitterer Armut fristen und für absehbare Zeit im Knast.

AUFWACHEN! “Das ist alles nur ein Traum!“

Lysander aufwachen – ich reiche Dir, wie versprochen, die Taschentücher! Sein nachfolgendes Blah- Blah von: „Das neue Besitzen heißt Teilen!“ -war die Rechtfertigung für seine Gier.

Motorrad, aha- schade, dass es keine Pferde waren.

Leider haben die User der kriminellen Plattform nicht verstanden, dass die persönliche Gier einiger Piraten sie gleich



mit -kriminalisierte. Ja, jetzt, wo der Kahn sinkt, verlassen die letzten Leichtmatrosen das Deck. Wasser hat keine Balken.

Vor Gericht und auf hoher See ist man in Gottes Hand.

Ich kann nicht beurteilen, ob die Generalstaatsanwaltschaft nun Verfahren gegen User einleitet. Das steht mir auch nicht zu. Wenn im Zuge der Ermittlungen User erkannt werden und eine Möglichkeit besteht, diese in Haftung zu nehmen, so soll dies geschehen.

Ich bin in diesem Punkt tiefenentspannt.

Bei Lul.to wird nichts zu holen sein. Nie wieder wird bei einem der Beteiligten irgendetwas zu holen sein. Da stehen Forderungen ins Haus, die die Vorstellung eines Otto-Normal-Verbrauchers sicherlich übersteigen.

Ob die GStA sich auf einen Kuhhandel einlässt, vermag ich nicht zu beurteilen. Es steht mir auch nicht zu, weder zu kommentieren noch zu fordern. Da müssen Sie die Juristen fragen. Oder den GStA.

Wenn ich die BILD Zeitung irgendwo sehe, dann ist sie meistens Tage alt. Ich lese weder die BILD Zeitung noch weiß ich, was die Redakteure recherchiert haben- die Zahl der User erscheint mir zu niedrig. Ich habe den Artikel nur zufällig gefunden und verlinkt. Die Userzahl lässt sich anhand der beschlagnahmten Beute der Piraten schon hochrechnen und die Piraten haben sicher nicht schlecht gelebt.

Lehren aus Lul.to

Natürlich habe ich auch Lehren aus Lul.to gezogen. Ich habe die ISBN Nummern für ungültig erklären lassen, die Bücher vom Markt genommen. Nicht alle, etwa 85 % der Ausgaben. Das ist ein beträchtlicher Schaden. Es steht mir zu, zu entscheiden, was ich als Abwehrmaßnahme entscheide und wen ich später dafür in die Haftung nehme, soweit das den rechtlichen Rahmenbedingungen entspricht.

Was andere Verlage, Schriftsteller, machen, kann und will ich nicht beurteilen.

Ich werde nicht mehr über Portale arbeiten, sondern nur noch Direktverkauf betreiben.

Ich habe die Preise soweit gesenkt, dass es keinen Spaß mehr macht, bei Piraten einzukaufen.

Jeder ahnt, wie ich mit Piraten und Entourage umgehe.

Wir haben jedes Buch mit einem individuellen, nicht veränderlichen Merkmal versehen – das macht Arbeit, ist aber der richtige Weg, um nachzuvollziehen, wo Piraten ihre Ware herbekommen.

Sicher, ich werde Lysander neue Erstausgaben in den Knast senden, damit ihm die Zeit nicht so lang wird.

In diesem Sinn
Beste Grüße!

Marinella

Wir, das Team von Tarnkappe.info, danken Marinella Charlotte van ten Haarlen für das abgegebene Statement und wünschen Ihr Erfolg beim Veröffentlichen ihrer Werke.


Sicherheit

Ist die Benutzung von LuL.to illegal?

- Die Registrierung bei LuL ist vollkommen legal.

  Das Herunterladen allerdings erfolgt in einer rechtlichen Grauzone. Nach laufender Rechtsprechung kann unter bestimmten Umständen ein Download eine Ordnungswidrigkeit darstellen (so wie bei roter Ampel die Straße zu überqueren).

ILLEGALE PLATTFORM GERMANYHUSICAYSX.ONION GEBUSTET?

Versucht man die Seite germanyhusicaysx.onion im Tornetzwerk zu erreichen, ist dies bereits mindestens seit dem 09.06.2017 nicht mehr möglich. Das Einzige, das man jetzt dort noch zu sehen bekommt, ist ein BKA Banner. Demnach wurde die Plattform und der kriminelle Inhalt durch das BKA im Auftrag der Generalstaatsanwaltschaft Frankfurt am Main beschlagnahmt.

Laut Alexa Traffic Rank war germanyhusicaysx.onion.to auf Platz 55.044 und 0,00167% Internet-Nutzer besuchten diese Seite. Mit 8.350 täglichen Besuchern erzielten sie 19.539 (2.34 pro Besucher) Seitenaufrufe pro Tag. Folglich handelte es sich dabei um ein relativ großes, deutschsprachiges Forum.

Gerüchten zufolge könnte diese Schließung noch eine Reihe von Hausdurchsuchungen nach sich ziehen, falls die Nutzerdaten unverschlüsselt vorlagen, war es doch ein Marktplatz für den Verkauf illegaler Waren aller Art.

Natürlich ist bisher alles reine Spekulation. Tatsächlich könnte es auch sein, dass ein Hackangriff auf die Plattform erfolgte oder es wäre zudem denkbar, der Betreiber selbst hat die Seite vom Netz genommen. Momentan sind wir auf der Suche nach weiteren Fakten, die Licht in diese Angelegenheit bringen könnten.

Nach Angaben des Bundeskriminalamtes (BKA) vom Montag haben Beamte des BKA mit Unterstützung von Spezialkräften der Bundespolizei am Abend des 8. Juni 2017 in Karlsruhe einen 30-jährigen Beschuldigten aus Karlsruhe festgenommen und dessen Wohnung durchsucht. Das Forum „Deutschland im DeepWeb“ (DiDW), das unter der Adresse germanyhusicaysx.onion im Tornetzwerk zu erreichen war, ist vom Netz genommen.

Der Beschuldigte, der im Forum unter dem Namen „luckyspax“ oder „Lucky“ auftrat, steht im Verdacht, seit März 2013 als alleiniger Administrator die große, deutschsprachige Darknet-Plattform „Deutschland im DeepWeb“ (DiDW) betrieben zu haben. Die als Forum aufgebaute Plattform, auf der nach Polizeibericht zuletzt über 20.000 Mitglieder registriert waren, verfügte unter anderem über eine Marktplatz-Sektion, über die zahlreiche illegale Handelsgeschäfte getätigt wurden. Insbesondere war es ein Umschlagplatz für illegale Drogen- und Waffenverkäufe. Darüber hinaus konnten über die Plattform auch Falschgeld, gefälschte Personalausweise, ausgespähte Kreditkartendaten und Kundenkonten auf Internethandelsplattformen sowie gefälschte Bankkonten erlangt werden. Auch die Anbahnung des Erwerbs der bei dem Amoklauf in München am 22. Juli 2016 eingesetzten Waffe erfolgte über diese Plattform.

Der Festnahme am Donnerstagabend gingen laut BKA monatelange verdeckte Ermittlungen voraus. Bei einer Wohnungsdurchsuchung stellten Einsatzkräfte zahlreiche Beweismittel, insbesondere Computer, Datenträger und geringe Mengen Betäubungsmittel sicher. Auch der Server wurde beschlagnahmt, das Forum abgeschaltet.

Der Haftrichter am Amtsgericht Karlsruhe hat am Freitag einen bereits erlassenen Haftbefehl des Amtsgerichts Gießen wegen des Verdachts der Beihilfe zum unerlaubten Handel mit Waffen und Betäubungsmitteln verkündet. Der Beschuldigte befindet sich seitdem in Untersuchungshaft.

Das nun geschlossene DiDW war primär zum Meinungsaustausch gedacht. Es gab jedoch auch zahreiche Händler, die ihre Ware in Threads angeboten und verkauft haben.

FÄLSCHERWERKSTATT HQCNS.COM NACH DREIVIERTELJAHR NOCH IMMER ONLINE

Zwei Männer im Alter von 23 und 24 Jahren aus dem niedersächsischen Lingen befinden sich seit August 2016 wegen des Verdachts auf gewerbsmäßige und bandenmäßig begangene Geldfälschung zuzüglich zur Beihilfe zum Handel mit Betäubungsmitteln in Untersuchungshaft. Über ihren High Quality Counterfeit Notes Store (HQCNS) wurden nachweislich mehr als 7.200 gefälschte Geldscheine veräußert. Kurios: Die zugehörige Webseite hqns.com ist rund neun Monate nach der Verhaftung der beiden Verdächtigen noch immer online.

Bei Lingen nahe der niederländischen Grenze haben zwei Männer binnen eines Jahres nach Angaben der Staatsan-

waltschaft mehr als 7.200 gefälschte 50-Euro-Scheine hergestellt. Sie veräußerten die Ware ganz ohne .onion-Adresse über ihren High Quality Counterfeit Notes Store (HQNS.com) an deutsche und ausländische Kunden. Im August 2016 war damit Schluss, die Schwerpunktstaatsanwaltschaft zur Bekämpfung der Informations- und Kommunikationskriminalität Osnabrück wurde aktiv. Seitdem befinden sich die Verdächtigen in Untersuchungshaft. Im Januar dieses Jahres wurde vor dem Landgericht Osnabrück Anklage erhoben.

Was bleibt, ist der Webshop (konkret: ein WordPress Blog auf Basis von WooCommerce), der dem geneigten Publikum bis heute unter der URL https://hqcns.com gefälschte 50-Euro-Scheine in verschiedener Qualität und somit in unterschiedlichen Preiskategorien anbietet. Die Wahl der Ware ist kein Zufall. Unter den Blüten ist der Fünfziger am beliebtesten. Typ 5 der „falschen Fuffziger“, also die nachgemachten Geldscheine mit der höchsten Qualität, werden dort pro Stück für 16,50 Euro angeboten. Wer große Mengen abnahm, konnte von der Rechnungssumme noch etwas Rabatt abziehen.

„Die Blüten sind so gut, ich bearbeite die nicht mal.“

Ein Kommentator, oder einer der beiden Macher des Shops, der den Kommentar gefaked (= nachgemacht) hat, schrieb als Rezension, dies wären die besten nachgemachten Scheine, die man online kaufen könne. „Die Blüten sind so gut, ich bearbeite die nicht mal.“ Der Käufer ließ sie lediglich ein wenig in seinem Geldbeutel liegen, damit die Scheine nicht mehr so neu und unverbraucht aussehen würden. Er hätte mit diesem Produkt bisher keine Probleme gehabt, schrieb der unbekannte Käufer. Der Slogan der Fälscherwerkstatt lautet höchst passend „Take me to paradise“. Im Eingangsbereich des Shops ist bis heute ein bei shutterstock geklautes Foto von zwei Geschäftsleuten aus Plastik zu bewundern. Zu ihren Füßen, wie sollte es anders sein: Geldscheine. Mit dem Tor-Browser musste und muss man bis heute nicht nach den Blüten suchen, der Shop wurde im Clearnet (offenen Internet) errichtet und soll von Suchmaschinen wie Bing, DuckDuckGo und Google indiziert werden.

hqcns.com: keine Bustmeldung im Untergrund

Merkwürdig ist allerdings, dass nirgendwo im Graubereich nähere Informationen über die Festnahmen durchgesickert sind. Selbst auf Fraudsters, Crimenet & Co. findet man keine näheren Angaben über die Hintergründe der Beschuldigten oder über mögliche Durchsuchungen bei Käufern, was der logische nächste Schritt der Ermittler wäre. Die Angelegenheit wurde im Internet mit Ausnahme weniger Lokalzeitungen kaum behandelt. Es fragt sich nur, warum. Auf Fraudsters findet man lediglich das Ergebnis verschiedener Testkäufe von HQCNS-Blüten, die übrigens weniger positiv wie die oben genannte ausfiel. Dass die Hintermänner erwischt wurden (= busted), wird dort und anderswo im Graubereich nirgendwo erwähnt. Und das, obwohl sich derartige Gerüchte in Untergrund-Foren normalerweise wie im Lauffeuer verbreiten.

Können die Behörden den Online-Shop nicht abschalten?

Ein Dreivierteljahr nach der Festnahme der beiden Lingener ist der Webshop noch immer verfügbar, als wenn nichts wäre. Nach erfolgter Registrierung (klappt allerdings nicht mit allen Browsern!) erfolgt aber über mehrere Wochen hinweg keine Antwort auf Support-Anfragen. Da die ehemaligen Fälscher nicht mehr frei über ihren Aufenthaltsort verfügen können, wie es im Fachjargon so schön heißt, ist dies wenig überraschend. Allem Anschein nach ist der Shop seit dem Bust nicht mehr aktiv.

Den Behörden ist das Abschalten von HQCNS.com allerdings auch noch nicht gelungen. Ende 2016 standen die Server in Hongkong beim Hosting-Anbieter tnet.hk. Seit dem Wechsel zu Cloudflare ist es ungleich schwieriger geworden, den tatsächlichen Aufenthaltsort der zugehörigen Webserver zu ermitteln. Die Domain der alternativen URL HQCNS.BIZ wurde übrigens auch in China registriert. Doch wer diese Internet-Adresse aufruft, wird automatisch zur im Web bekannten Online-Fälscherwerkstatt weitergeleitet. Weiter als bis zu Cloudflare ist die Staatsanwaltschaft offenbar auch nicht vorgedrungen, wie es scheint. Trotzdem ist es merkwürdig, dass ein derart großer Anlaufpunkt für Fälschungen noch immer aktiv ist.

Weitere Informationen sind momentan leider nicht verfügbar. Wer etwas zu unseren Recherchen beitragen kann, den bitten wir, seine Erkenntnisse hier in den Kommentaren zu hinterlassen.

DER WEG IN DIE CYBERKRIMINALITÄT: WAS IST DIE MOTIVATION DAHINTER?

In einem aktuellen Bericht stellt die britische National Crime Agency (NCA) fest, dass viele junge Leute nicht unbedingt durch finanzielle Anreize motiviert werden, den Weg zur Cyberkriminalität einzuschlagen. Die tatsächlichen Motivatoren sind Anerkennung unter Gleichaltrigen, Beliebtheit in angemeldeten Foren, Selbstbestätigung oder das Erleben eines Erfolgsgefühls.

Die Veröffentlichung beruht auf Gesprächen mit Straftätern. Es wurde erforscht, warum Jugendliche Gefallen an Internetkriminalität finden und sich dort einbringen. Man erkennt gleich mehrere Gründe, die dann in der Summe dazu führen. Zum einen ist es das Gefühl, eine Herausforderung erfolgreich bewältigt zu haben und das sich Beweisen innerhalb einer Gruppe, wobei der finanzielle Gewinn nicht unbedingt eine Priorität für junge Straftäter ist. Einer der Probanden meinte: „…es machte mich beliebt, ich genoss das Gefühl…“ Ein 18-Jähriger, der wegen des unrechtmäßigen Zugangs zu einer US-Regierungs-Website verhaftet wurde, führte an: „Ich habe es getan, um die Leute in der Hackergemeinschaft zu beeindrucken und um ihnen zu zeigen, dass ich die Fähigkeiten hatte, es durchzuziehen […] ich wollte mich beweisen.“

Ein weiterer, zweiter entscheidender Faktor dafür, dass Jugendliche gerade diesen Weg wählen, ist das Gefühl, kein Verbrechen im „traditionellen Sinne“ begangen zu haben und zudem die Hoffnung dabei zu hegen, dass man nicht für die Durchführung eines Cyber-Angriffs verhaftet werden wird. Viele der cyber-kriminell aktiven, britischen Jugendlichen würden sich nicht in „traditionelle“ Verbrechen“ verwickeln lassen, da ist sich die NCA sicher.

Als dritter Grund wird angegeben, dass die Barriere für den Einstieg in die Internetkriminalität aktuell niedriger wäre, als jemals zuvor. So stehen bereits eine Vielzahl von Hacker-Tools für geringes Entgelt zur direkten Verfügung eines jeden daran Interessierten mit passenden Video-Instruktionen oder zweckdienlichen Schritt-für-Schritt-Tutorials als Anleitung zum Handeln. Folglich ist es genau diese Leichtigkeit, mit der Angriffe und bösartige Aktivitäten initiiert werden können und die Jugendliche dazu verleiten, diese Tools auch ausprobieren zu wollen, wobei es alle nur denkbaren Arten davon online gibt, die weder teuer sind noch schwer zu bedienen. Im vorliegenden Bericht heißt es: „Schon ein wenig Geschick genügt, um cyber-kriminelle Aktivitäten zu starten. Mit keinem oder wenig Startkapital beziehen Anfänger Tools wie Remote Access Trojaner (RAT) und beginnen Gesetze zu brechen. Ist das Gesetz erst einmal gebrochen, sinkt die Hemmschwelle für nachfolgende Übertretungen.“ Der Einstieg ins kriminelle Milieu beginnt für viele Straftäter mit der Teilnahme auf Gaming-Cheat-Webseiten und „Modding-Foren“ (Spiele-Modifikations-Foren), der dann in der Folge zu kriminellen Hacker-Foren führt. Dort werden die entsprechend relevanten Themen offen diskutiert.

Das Durchschnittsalter derjenigen, die Cybercrime-Delikte begehen, ist wesentlich jünger als bei Tätern anderer Verbrechensarten. Im Jahr 2015 lag das Durchschnittsalter bei Cybercrime-Tätern bei gerade mal 17 Jahren, im Vergleich dazu: Täter im Drogenmilieu sind im Durchschnitt 37 Jahre alt, Täter in Sachen Wirtschaftskriminalität 39 Jahre.

national crime agency NCADie National Crime Agency nimmt an, dass Jugendliche unter Aufsicht eines Mentors von dem Einstieg in die Cybercrime-Szene abgebracht werden können: „Ex-Täter, die ihre Cyber-Aktivitäten einstellten und sich einer Ausbildung oder Karriere in der IT widmeten, haben diesen Wandel einem positiven Mentor zu verdanken.“ Auf diese Weise soll die Kluft zwischen ihnen und den Behörden geschlossen werden. Der Bericht zeigt deshalb auch mögliche Alternativen für Jugendliche auf, wie Jobperspektiven, um die vorhandenen Fähigkeiten positiv einzusetzen. Mentoren sollen potenzielle Straftäter in Richtung einer zukünftigen Karriere lenken, wie der Cyber-Sicherheit, der Gaming-Industrie oder in Codierung und Programmierung. Richard Jones, Leiter des Prevent-Teams der National Cyber-Crime Unit, ist der Überzeugung, dass eine solche Perspektive ihnen immer noch das Gefühl vermitteln wird, dass sie doch suchten, nämlich das der Selbstverwirklichung und des Respekts.

Als besonders bedenklich stufte man im Bericht ein: „Was bei uns schlussendlich Besorgnis erregt hat, ist die Tatsache, wie leicht Jugendliche in die Welt des Cybercrime gelangen können und wie sorglos sie selbst darüber denken.

Dazu gehört auch, dass die jungen Menschen das Gefühl der Chancenlosigkeit haben und ohne Vorbild zu sein scheinen."

Das Ziel dieser Studie ist es gewesen, die Wegweiser zu verstehen, die in die Cyberkriminalität geführt haben und gleichzeitig die effektivsten Interventionspunkte zu finden, um die Jugendlichen auf einen positiveren Weg zu lenken.

CYBERCRIME CONFERENCE C3: CYBERCOPS SOLLEN BALD GEGEN CYBER-KRIMINALITÄT VORGEHEN

Die Bilanz der aktuellen Cybercrime Conference C3 in Berlin ist alarmierend. Demnach stellt Cybercrime eine wachsende Bedrohung dar. Im Vergleich zum Vorjahr stieg die Anzahl dieser Fälle im Jahr 2016 um 80 Prozent.

Die Cybercrime Conference C3 am 3. und 4. Mai 2017 in Berlin sollte Akteure aus diesen Bereichen zusammenbringen, Informationen zu aktuellen Trends und Strategien vermitteln sowie einen intensiven Meinungs- und Erfahrungsaustausch ermöglichen. So bestand der Teilnehmerkreis nicht nur aus Vertreterinnen und Vertretern von polizeilichen Cybercrime-Dienststellen und Staatsanwaltschaften mit der Schwerpunktzuständigkeit Cybercrime, sondern umfasste auch die Führungsebene ausgewählter Wirtschaftsunternehmen. Die Konferenz wurde erstmals gemeinsam mit den Vereinen Digital Society Institute (DSI) und dem German Competence Centre against Cyber Crime veranstaltet. Ein wesentlicher Aspekt der Diskussionen waren dabei Strategien gegen die digitale Kriminalität.

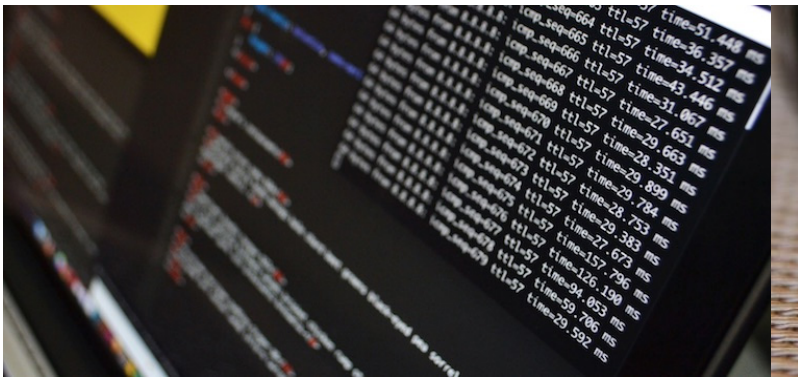
So hat die Digitalisierung in Politik, Wirtschaft und Gesellschaft auch Auswirkungen auf die Kriminalitätslage. Es sind steigende Schäden durch immer neue Angriffsformen und die Professionalisierung der Täter, neue Tatgelegenheiten in Zukunftsfeldern wie Internet of Things und Industrie 4.0 sowie Bedrohungspotentiale durch Cyberangriffe auf Unternehmen und kritische Infrastrukturen zu verzeichnen. Das erfodere eine ständige Weiterentwicklung von Präventions- und Bekämpfungsstrategien, sowohl von der Wirtschaft, als auch der Wissenschaft und gleichermaßen von den Strafverfolgungsbehörden.

BKA-Präsident Holger Münch gab am Mittwoch auf dieser Fachtagung die neuen Zahlen bekannt: So hat die Polizei nach Angaben des Bundeskriminalamts 2016 in Deutschland rund 83.000 Fälle von Cybercrime erfasst. Dabei sei ein Schaden von über 51 Millionen Euro entstanden. „Polizeiliche Statistiken und Lagebilder spiegeln aber nur einen kleinen Teil der Realität wider.", gab Münch dabei zu bedenken. Auch Sandro Gaycken, Direktor des Digital Society Institute verwies auf das große Dunkelfeld. Der tatsächliche Schaden sei deshalb schwer zu schätzen. Deutschland wäre als Industrieland jedoch mehr als viele andere Länder betroffen. Cyberkriminelle hätten sich in den vergangenen Jahren professionalisiert und oft eine klassische Entwicklung „von der Garage zum Großkonzern" durchlaufen, daneben gebe es auch „gute" Mittelständler, führte er weiter aus. Markus Koths, Leiter der Gruppe Cybercrime beim BKA, gab bekannt, dass viele klassische Deliktfelder, wie der Handel mit Drogen oder Waffen, längst ins Internet abgewandert seien. Die Kriminalität habe sich zu einem hoch organisierten und arbeitsteiligen Dienstleistungsgewerbe entwickelt, wobei allein für Privatpersonen in Deutschland 2015 nach Schätzungen des Deutschen Instituts für Wirtschaftsforschung DIW ein Schaden von 3,4 Milliarden Euro entstanden sei.

Münch erklärte, heute würden so viele Daten produziert wie in der gesamten Menschheitsgeschichte zuvor. Straftätern böten sich durch die Digitalisierung immer neue Angriffspunkte. Kriminalität werde digitaler, vernetzter, internationaler. Sie operierten innovativ und anpassungsfähig und bedienten sich neuster Technologien. Ermittler und Analysten bräuchten neben internationalen und interkulturellen auch digitale Kompetenzen: „Dem müssen wir bei der Fortentwicklung unseres Berufsbildes hin zu einem Cybercop Rechnung tragen." Münch empfielt daher „Streifen im digitalen Raum", etwa in sozialen Netzwerken.

Sandro Gaycken weist auf die noch vorhandenen Defizite zur Bekämpfung der Cyberkriminalität hin: In der Bundesrepublik gäbe es nur 360 Cyberexperten, die häufig von großen Unternehmen engagiert würden, weil sie in der freien Wirtschaft mehr verdienen könnten. Im internationalen Vergleich hinge Deutschland noch ein paar Jahre hinterher, „aber dass ist keine Schande – das ist überall so", meint Gaycken.

So gehe es dabei zudem um eine beschleunigte Anpassungsfähigkeit, um mit den Veränderungen Schritt zu halten. „Wir dürfen den Tätern nicht zu Fuß hinterherlaufen." Und die Ermittlungsbehörden müssten der hochvernetzten Cyber-Kriminalität ebenfalls ein leistungsfähiges Netzwerk gegenüber stellen. Netzwerkarbeit sei ein wichtiger Bestandteil erfolgreicher Polizeiarbeit. Die diesjährige Konferenz des BKA in Berlin sei dafür ein weiterer Schritt in die richtige Richtung.



Emily Haber, Staatssekretärin im Bundesinnenministerium, verwies darauf, dass vor allem in der aktuellen Entwicklung der „Industrie 4.0" Cyberkriminalität ein immer ernstzunehmenderes Thema darstelle, denn jeder, der einen Computer benutze, wäre ein potenzielles Opfer. Sie fügte hinzu, dass „die Komplexität und Kreativität der kriminellen Machenschaften atemberaubend ist". Präventionsmaßnahmen bedürften eines enormen Know-Hows.

Kritik gibt es an der Kriminalstatistik, die im April von der Polizei veröffentlichte wurde: So beziehen sich die veröffentlichten Zahlen lediglich auf Fälle, die von den Opfern angezeigt wurden – 90 Prozent blieben unentdeckt. Daraus ergibt sich eine immense Dunkelziffer: das Deutsche Institut für Wirtschaftsforschung (DIW) schätzt, dass es 2015 rund 15 Millionen Fälle von Cyberkriminalität gab. Matthias Spielkamp, Leiter des Informationsportals „Mobil sicher" meinte, die Zahlen in der Statistik seien unplausibel. So wäre die polizeiliche Kriminalstatistik zur Cyberkriminalität ein großes Stochern im Nebel: „Wie soll beispielsweise die Telekom angeben, wie groß der Schaden war, nachdem ihre Server lahmgelegt worden sind? Die Daten sind alle ziemlich vage".

PREMIUMFILLER: VERKÄUFER ILLEGALER WAREN RECHNET MIT DER SZENE AB

Der Verkäufer PremiumFiller hat seine Aktivitäten komplett eingestellt. In seinem Abschiedsbrief rechnet er mit der Untergrund-Szene im Allgemeinen und dem Forum Crimenetwork (CNW) im Speziellen ab. Die meisten Verkäufer würden nur das schnelle Geld auf Kosten Dritter machen wollen, statt sich langfristig einen guten Namen aufzubauen. Ziel der Abzocker seien vor allem Anfänger, weil man sie sehr leicht in die Falle locken könne.

Der Vendor (Verkäufer in Untergrund-Foren) PremiumFiller hat kürzlich mit einem lauten Knall die Szene verlassen. Er wirft den Machern von Crimenetwork.biz (CNW) vor, die Daten aller Besucher aufzuzeichnen und kritische Beiträge zu zensieren. Außerdem wird dem CNW-Admin Zeroday vorgeworfen, er sei mit insgesamt drei Accounts aufgetreten und habe per Jabber Schindluder mit seinen virtuellen Persönlichkeiten getrieben. Diesbezüglich wurden auch selbst erstellte „Beweisvideos" in Umlauf gebracht.

Der Hauptvorwurf von PremiumFiller ist und bleibt aber, dass die meisten Anbieter illegaler Dienstleistungen oder Waren stets nur versuchen, auf Kosten Dritter das schnelle Geld machen zu wollen. Die meisten Vendoren hätten es nur auf die Anfänger abgesehen, um sie um ihr Geld zu bringen. So auch beim Crimenetwork, wo den Betreibern schon häufiger öffentlich vorgeworfen wurde, sie hätten Betrüger wissentlich und aktiv bei ihrem Tun unterstützt. Im konkreten Fall ging es um einen Exit-Ripp. (Erklärung: Dabei täuscht ein Händler vor, er wurde von der Polizei hochgenommen oder habe aus anderen Gründen die Szene verlassen. Er nimmt dabei das Geld seiner Kunden mit.)

„Threads werden geschlossen (…) das Thema totgeschwiegen", kritisiert ein Nutzer die Admins bei Crimenetwork.biz. Die Verkäufer hätten dabei durchaus die Möglichkeit, richtig viel Geld zu verdienen, glaubt PremiumFiller. Allerdings benötigte man dafür gute Partner, Fleiß, Ausdauer und es dauere eben lange, bis man sich eine gute Reputation als Anbieter aufgebaut habe. Darauf wollen viel betrügerische Verkäufer nicht hinarbeiten, heißt es im Abschiedsbrief.

cnw crimenetworkDen Machern vom Crimenetwork wirft der Aussteiger zudem vor, den Wettbewerber Underground.to mit ständigen DDoS-Angriffen aus der Bahn werfen zu wollen. Der illegale Online-Marktplatz Underground.to wird derzeit nur unzureichend durch Cloudflare geschützt und ist somit ein leichtes Ziel für jegliche Angriffe von Bot-Netzwerken.

Anmerkung: Bei den Verbalattacken und Vorwürfen des Aussteigers gegen das CNW muss man mitbedenken, dass dieser vormals einer der Moderatoren von Untergrund.to war und somit nicht neutral über das Geschehen berichten kann.

ÄTHIOPIEN: PRIVATKOPIEN PER USB-STICK AUS DEM AUTOMATEN

Wer in Äthiopien den neuesten Blockbuster oder einfach nur eine Dokumentation anschauen möchte, der kann an Automaten Filme auswählen und diese dann auf USB-Stick gegen einen kleinen Obolus speichern, so berichtet das Nachrichtenportal „TorrentFreak“ unter Berufung auf einen Informanten.

Die Ära der CDs, DVDs und Blu-Ray Discs neigt sich bereits ihrem Ende zu. Die Zukunft liegt jetzt in neuen Speichermedien, wie dem USB-Stick, der überzeugt durch seine geringe Größe und vielseitige Verwendbarkeit. Da lag es wohl nahe, eine neue Geschäftsidee damit auszuprobieren, die zwar bei uns strafrechtliche Konsequenzen nach sich ziehen würde, wohl aber seit einiger Zeit zum äthiopischen Alltag zu gehören scheint.

So sind nun gelbe Shopping Mall Touchscreen Kiosks, die Geldautomaten äußerlich ähneln sollen, namens SwiftMedia mit Display und USB-Anschluss in den äthiopischen Einkaufszentren präsent. Deren Angebotspalette umfasst ein riesiges Archiv von Filmen und reicht von den neuesten Kinofilmen über Dokumentationen bis hin zu Filmklassikern. Auch die Preise sind durchaus kundenfreundlich. So kann man die Filme bereits für günstige 25, 50 und 100 Birr ($ 1, $ 2 und $ 3) erwerben. Spielfilme bekommt man sogar schon für 3 bis 5 birr (13 bis 22 Cent), je nach Release-Datum.

Betrieben und gewartet werden die Swift Media-Automaten von einem Unternehmen namens Escape Computing, wobei sich die Wartung nicht nur auf die Prüfung technischer Funktionen bezieht, sondern gleichzeitig auch das ständige, aktuelle Bereitstellen neuer, raubkopierter Inhalte umfasst. Das geht aus einer Jobbeschreibung der Firma aus dem Vorjahr hervor, worin man nach einem IT-Spezialisten suchte, der auch ein guter „Filmverkäufer“ sein sollte.

swift media Escape ComputingMittlerweile ist das Telekommunikationsnetz in Äthiopien schon gut ausgebaut. In allen regionalen Zentren gibt es öffentliche Telefone, oft auch Internetcafés und Telefon-Shops. Internetverbindungen allerdings sind oftmals sehr langsam, so dass eine Nutzung kaum oder nur mit sehr viel Geduld möglich ist. Unter diesen denkbar ungünstigen Voraussetzungen, kann man kaum davon ausgehen, dass Filme über das Internet bezogen werden können und deshalb stellen derartige Film-Automaten dort ein einträgliches Geschäft dar und werden ganz sicher oft genutzt. Die Möglichkeit, den USB-Stick im nächsten Einkaufszentrum per Automat mit dem Film seiner Wahl zu befüllen, kommt daher jedem Filmfreund sicher sehr gelegen.

Der Informant von Torrentfreak wollte anfangs gar nicht glauben, dass diese Automaten Raubkopien ausgeben. Zunächst ging er davon aus, dass nur alte Filme verkauft werden. Doch wurde er eines Besseren belehrt, als er sich das Angebot genauer betrachtete, denn er fand dort auch die neuesten Blockbuster vor. Da erst wurde ihm bewusst, dass Urheberrechtsverletzungen in diesem Land wohl nicht so ernst genommen werden, wie in anderen Ländern und wirklich Raubkopien in großem Umfang zum freien Verkauf angeboten werden.

NETFLIX: HACKER ERPRESSEN STREAMING-DIENST

Die Hacker-Gruppe „Thedarkoverlords“ hat zehn neue Folgen der fünften Staffel von „Orange is the new Black“ veröffentlicht. Vorher haben sie versucht, Netflix mit den gestohlenen Episoden zu erpressen, jedoch der Streaming-Dienst habe die Geldforderung offenbar ignoriert, berichtet „New York Times“.

Netflix hatte in diesem Jahr angekündigt, dass die 5. Staffel der beliebten Serie von „Orange Is the New Black“ am 9. Juni erscheinen würde. Nun ist jedoch die Staffel bereits fast komplett erhältlich auf einschlägigen Torrent-Seiten, wie The Pirate Bay, bereits Wochen vor ihrem offiziellen Juni-Release-Datum, da Netflix offenbar der an sie gerichteten, erpres-

serischen Zahlungsaufforderung nicht nachkam. Die erste Episode wurde bereits am Freitag auf einer File-Sharing-Website veröffentlicht, die mit einem Twitter-Link der Hacker versehen war, der zu der Drohung geführt haben soll: “Lasst uns nun konkreter werden, Netflix.”, woraufhin auch die anderen Folgen am Samstag öffentlich illegal verfügbar waren.

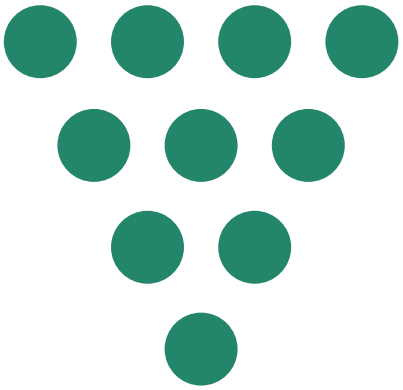
Als verantwortlich, sowohl für das Einstellen der Links auf den illegalen Downloadportalen, als auch für die Erpressung von Netflix, bekannte sich die Hacker-Gruppe „Thedarkoverlords“. Die Hacker veröffentlichten auf der Plattform „Pastebin“, auf der man anonym Texte hochladen kann, eine Art Bekennerschreiben: „Wir sind es wieder“, heißt es darin. „Habt ihr uns vermisst?“ Und an die Adresse von Netflix: „Es hätte nicht so kommen müssen, Netflix. Ihr verliert jetzt viel mehr, als ihr uns hättet zahlen müssen.“ Zudem drohten die Verfasser anderen Produzenten: Man sei im Besitz von unveröffentlichtem Material von National Geographic, Fox, ABC und IFC. „Ihr habt noch Zeit, um euch zu retten.“ Gleichzeitig drohten „Thedarkoverlords“ auf einem eigenen Twitter-Account den anderen großen TV-Anbietern: „Wer ist der nächste auf der Liste?“ […] „Oh, was für ein Spaß wir alle haben werden. Wir machen keine Spielchen mehr.“ Nach Angaben der „New York Times“ weigern sich die bedrohten TV-Stationen, zu der Drohung öffentlich Stellung zu beziehen.

Gemäß Netflix haben sich die Hacker bei einem kleinen Unternehmen in Los Angeles, den Larson Studios, einer in Hollywood ansässigen Post-Production-Firma, die offensichtlich nicht ausreichend gegen Hacker-Angriffe geschützt war, Zugang zu den Folgen verschafft. Der Streamingdienst hatte das Material zur Nachbearbeitung an die Firma Larsen Studios geschickt, die laut Netflix von etlichen großen Fernsehstudios benutzt wird. Die Folgen sind also möglicherweise nicht gänzlich fertiggestellt, sollen aber eine hohe Bild- und Tonqualität haben. Die Staffel Fünf der Serie hat insgesamt 13 Episoden. Es fehlen in dem Leak die Episoden 11 bis 13, weil diese das Studio zum Zeitpunkt des Hacks noch nicht von Netfix erhalten hatte.

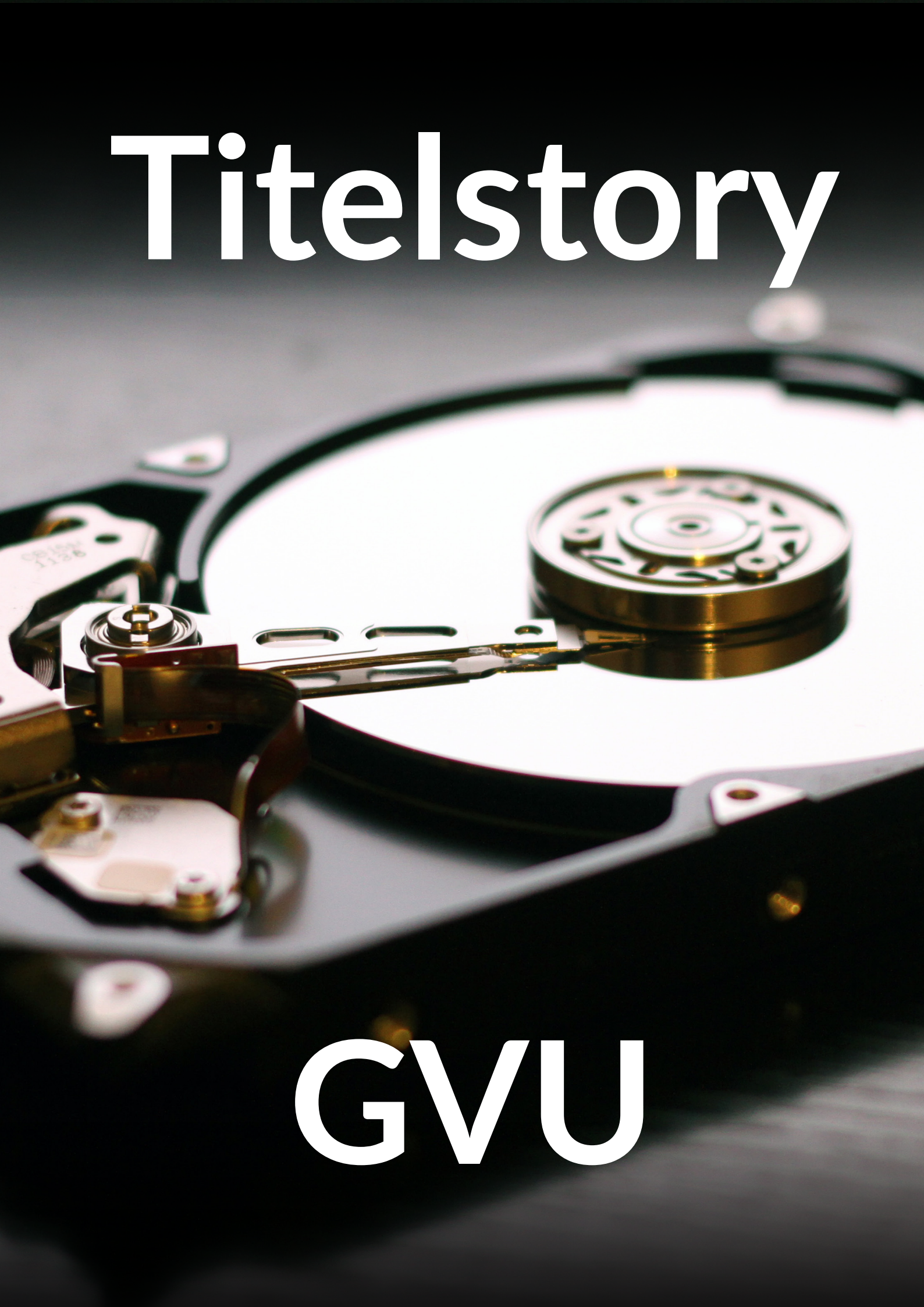
Von der Serie hat Netflix sich erhofft, seine Abonenntenzahl weiter steigern zu können. Zudem ist „Orange is the new Black“ ein Quotenhit und spielt viel Geld ein in die Kassen des Unternehmens. Netflix selbst reagierte bereits mit einer Stellungnahme auf den Fall: „Wir wissen von der Situation. Sie hat sich aus einem Sicherheitseinbruch bei einer Nachproduktionsfirma ergeben, der sich etliche größere Fernsehstudios bedienen. Die zuständigen Strafverfolgungsbehörden sind eingeschaltet.“ Es ist also sehr wahrscheinlich, dass die Hacker auch über Material von anderen Serien-Produktionen verfügen. Das FBI habe schon im Januar davon erfahren, Netflix aber erst vor einem Monat informiert, sie ermitteln bereits in diesem Fall.

Die Hacker-Gruppe „Thedarkoverlords“ wird nach Informationen der „New York Times“ mit weiteren Internet-Verbrechen der jüngsten Vergangenheit in Verbindung gebracht. So sollen die Hacker auch hinter einer Attacke aus dem Sommer 2016 stehen. Damals waren mindestens drei große Krankenversicherungsunternehmen in den USA gehackt worden. Danach sollen die Täter versucht haben, die Daten im Netz zu verkaufen. Zudem stecken die Hacker, dem Bericht zufolge, auch hinter einem Angriff auf eine kleine Wohltätigkeitsorganisation für Krebskranke. Bei dem Angriff wurden im Januar sämtliche Server des Unternehmens leergeräumt. Die Täter verlangten 43.000 US-Dollar für die Rückgabe der Daten. Das Unternehmen zahlte nicht. Nun sind die Datendiebe bei Netfix erneut mit einem Erpressungsversuch gescheitert.

Es könnte sich statt einer Hacker-Gruppe auch um einen Einzeltäter handeln. Das genau festzustellen, war uns leider nicht möglich. Die Medien berichten jeweils verschieden darüber. Einerseits heißt es bei Twitter „thedarkoverlord“, also Einzahl, dann wieder schreiben sie: „We are releasing the remainder of OITNB Season 5“, was auf eine Gruppe hindeutet. Es ist also bisher fraglich.



Titelstory



GVU

GVU
SPIELBALL DER DIGITALEN INDUSTRIE

Die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU) wurde schon vor einiger Zeit, am 27. Februar 1985, gegründet. Der heutige Geschäftsführer Jan Scharringhausen erklärte im Jahr 2008:

„In den ersten Jahren der GVU war die Szene vom Geschäft mit illegal hergestellten Kinofilmvideos und im Wesentlichen von Tätern aus dem in Westdeutschland ansässigen Rotlichtmilieu geprägt. […] Das Ankommen der Digitalisierung in der breiten Bevölkerung in den 1990er Jahren machte aus einem relevanten ein existenzielles Problem. Jetzt konnte praktisch jeder problemlos das Urheberrecht verletzen."

Damit hat Scharringhausen nicht Unrecht, denn die technische Entwicklung inklusive der Erfindung der MP3 und der flächendeckenden Versorgung mit DSL führte dazu, dass neben den zahlenden Mitgliedern aus der Filmbranche Ende der 90er Jahre einzelne Spiele-Publisher dazugestoßen sind. Wir haben es hier mit einigen wichtigen Vertretern der Unterhaltungs-Industrie zu tun. So etwa Sony Pictures, 20th Century Fox, Paramount Pictures, Warner Bros. und Walt Disney Studios. Aus der Spieleindustrie stammen populäre Firmen wie Activision, Konami, Microsoft, Koch Media oder Ubisoft. Seit einigen Jahren gehören auch Verlage und einige Branchenverbände dazu. Daneben werden im Jahresbericht 2011 technische Dienstleister wie arvato, Cinram, OpSec, Rovi und viele mehr als GVU-Mitglieder ausgewiesen.

Spannend wird es zum Beispiel auf den Kongressen der GVU, wenn leitende Mitarbeiter unterschiedlicher Verbände auf Diskussionspanels völlig gegensätzliche Meinungen vertreten. ***[i]*** Naturgemäß verlangen die Teilnehmer aus den Reihen der Filmindustrie ein mehr an Kontrolle und Zensur des Internets, die Sprecher der Telekommunikationsverbände pochen auf das genaue Gegenteil. Jede zusätzliche Netzsperre oder anlasslose Speicherung von IP-Adressen auf Vorrat würde die Internet-Anbieter bares Geld kosten. Als Außenstehender sollte man folglich nicht davon ausgehen, dass alle Mitglieder an einem Strang ziehen. Ähnlich wie beim Bundesverband Musikindustrie (BVMI) ist oftmals das genaue Gegenteil der Fall. ***[i]*** Bedenken muss man dabei auch, dass die Unternehmen gleicher Branche in direkter Konkurrenz zueinander stehen.

GVU Zentrale in Berlin

Ein rechtlich interessantes Konstrukt

Da es sich bei der GVU um einen wirtschaftlichen, also nicht gemeinnützigen Verein (e.V.) handelt, ist diese Organisation wie ein Unternehmen anzusehen. Genauso wurde es auch strukturiert. Das heißt im Klartext: Es gibt einen Geschäftsführer nebst einem Vorstandsvorsitzenden und mehrere Vorstandsmitglieder, die sich aus den verschiedenen Branchen rekrutieren. Neue Mitglieder können nur mit Zustimmung des Vorstands oder einer Mehrheit der Mitgliederversammlung aufgenommen werden. Die Abkürzung e.V. beinhaltet zwar eine sehr positive Außenwirkung. Was viele nicht wissen: e.V. bedeutet nur, dass eine Eintragung im Vereinsregister vorgenommen wurde. Karitative Zwecke sind damit nicht automatisch verbunden, auch wenn auf der Webseite der GVU kein entsprechender Hinweis zu finden war.

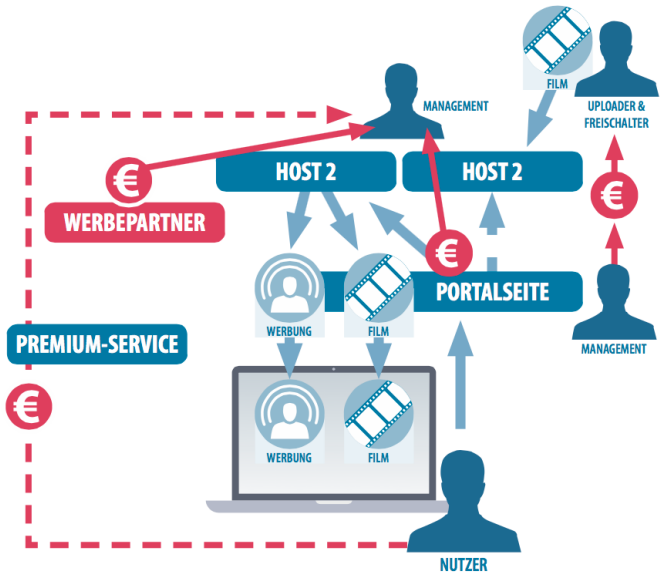
GVU: Drei Strategien, ein Ziel. Strafverfolgung!

Für die Strafverfolgung ***[i]*** stehen der GVU eigene Ermittler zur Verfügung. Einer der hauptamtlichen Mitarbeiter war in der Redaktion von Tarnkappe.info 2013 zu Besuch und hat früher bei der Polizei seinen Dienst versehen. Zu den GVU-Kongressen werden stets Staatsanwälte und Mitarbeiter der verschiedensten Landeskriminalämter eingeladen, die sich in nicht öffentlichen Sitzungen besprechen und dort versuchen, ihre Tätigkeit zu koordinieren.

Die GVU-Strategie richtet sich dabei in erster Linie gegen die Quellen der Warez, also gegen die Vollzieher der Beschaffungskriminalität und gegen jegliche Verteiler, die damit Geld verdienen. Soweit möglich, versucht man in erster Instanz gezielt gegen Personen vorzugehen, die in der Releaser-Szene tätig sind. Also die Cracker (Programmierer) und ihre Groups, die den Kopierschutz von Spielen oder Programmen entfernen. Illegale Veröffentlichungen, bei denen kein Kopierschutz entfernt werden muss, sind in der Releaser-Szene verpönt, weil dafür kein technisches Wissen vonnöten ist. Deswegen sind E-Books oder Cam-Rips (von der Leinwand abgefilmte Mitschnitte aktueller Kinofilme) auch auf zahlreichen ftp-Servern verboten. Von den ftp-Sites, die über eine extrem schnelle Internet-Anbindung verfügen, wandern die Werke binnen kürzester Zeit zu den Usenet-Providern, P2P-Indexseiten, Sharehostern, Warez-Foren und zu allen anderen illegalen Quellen, die es im Internet gibt. Trocknet man die Quelle der Warez aus, hätten die Verbreiter kein Material mehr und könnten mit dem geistigen Eigentum Dritter kein Geld mehr verdienen, lautet der Leitgedanke der GVU. Daneben geht es neben den Warez (Kopien) auch um Produktfälschungen (z.B. von Game-Controllern) und um andere Imitate, die bei e-Bay, Online-Shops oder auf Flohmärkten zum Verkauf angeboten werden.

Mitarbeiter der GVU sind bei Bedarf auch bei einzelnen Hausdurchsuchungen anwesend, um die Polizei zu unterstützen. Denkbar wäre auch eine aktive Unterstützung der Auswertung von beschlagnahmten Computern, externen Speichermedien wie Festplatten etc. Je nach Bedarf und Kooperationswillen der ermittelnden Behörden, findet ein Gedankenaustausch statt, man hält sich gegenseitig auf dem Laufenden. Bisher ist es nur in Einzelfällen gelungen, deutsche Cam-Ripper (Abfilmer von Neuerscheinungen im Kino) zu überführen. Früher dagegen war man häufiger mit Erfolg auf diversen Flohmärkten unterwegs, um Verkäufer von Schwarzkopien auszumachen und zu überführen. Während die Mitglieder der Release-Szene, die Wasserzeichen aus den abgefilmten Neuerscheinungen unkenntlich machen, um zu verschleiern, wo die Aufnahmen stattfanden, schwer aufzufinden sind, können Verkäufer von nachgemachten Audio-CDs, DVDs oder anderen imitierten Speicher-Medien sehr viel leichter dingfest gemacht werden. Man muss lediglich die Stände eines Flohmarktes systematisch abklappern und einen Testkauf durchführen. Danach macht die Polizei ihren Job, indem sie den Stand auflöst, alle Imitate beschlagnahmt und die Identität der Verdächtigen festhält. ***[i]***

Wie alle anderen Anti-Piracy-Organisationen ist die GVU auf die Mithilfe aus der Branche und auf Denunzianten aus den Reihen des digitalen Untergrunds angewiesen. Dabei verhält man sich aber weitaus weniger krass, als beispielsweise die Business Software Alliance (BSA), die gekündigte Mitarbeiter in Werbe-Anzeigen geradezu ermuntert, ihre früheren Chefs wegen nicht gekaufter Microsoft-Lizenzen anzuzeigen. ***[i]***



GVU: Parasitäre Geschäftsmodelle statt „Piraterie“

Doch seien wir realistisch: Wenn sich illegale Wettbewerber gegenseitig aus dem Markt drängen wollen, ist es Gang und Gäbe, der GVU einen anonymen Tipp ***[i]*** zu geben, damit der Konkurrent schon bald vom Netz genommen wird. Oder aber man droht dem Kontrahenten damit, seine Realdaten preiszugeben, sofern man die Seite nicht selbst offline schaltet. Das ist alles schon passiert.

Da heutzutage mittels Cloudflare & Co. sehr viele Daten-Transfers verschleiert und das Webhosting plus Domain anonymisiert werden, sind die Ermittler darauf angewiesen, der Spur des Geldes zu folgen. Die meisten Anbieter deutschsprachiger Portale halten sich wahrscheinlich noch immer in ihrer Heimat auf. Wenn für Banner-Werbung, der Vermittlung von Abos, Abzocke oder das Einschleusen von Schadsoftware Geld fließt, wollen die Betreiber trotz ihrer Briefkastenfirma irgendwann wieder hierzulande an ihre Einnahmen gelangen. Dann wird es für GVU & Co. spannend zu sehen, über welche Zahlungsdienstleister die Gelder der Kunden zunächst zur Briefkastenfirma und dann später zurück zu einem deutschen Konto gelangt sind. Auch gilt es zu bedenken, dass zwar das Webhosting (also die Speicherung aller Daten einer Webseite) in Deutschland für illegale Anbieter sehr gefährlich ist. Dafür sind die deutschen Webhoster im Vergleich preiswert und bieten eine schnelle Anbindung ans Internet an.

Man sollte besser nicht glauben, dass alle Streaming-Portale ihre Daten in Osteuropa oder weiter abseits vorhalten. Vor allem die kleineren Seiten greifen gerne auf Webhoster aus dem deutschen Raum zurück und versuchen die Fahnder mit Reverse-Proxys (technischen Umleitungen der Datenströme) in die Irre zu führen.

Beratung

Ein weiteres Standbein der GVU ist die Beratung. Diese richtet sich an Rechteinhaber, Behörden und Entscheider (Geschäftsführer, Vorstandsvorsitzende etc.). Dazu gehört eine hauseigene Rechtsberatung, die selbstredend nur den Unternehmen zur Verfügung steht, die sich zuvor für die kostenpflichtige GVU-Mitgliedschaft entschieden haben. ***[i]***

Öffentlichkeitsarbeit

Im Sommer 2009 wurde der Sitz von Hamburg nach Berlin verlegt. ***[i]*** Einer der Gründe war offenkundig, dass man aufgrund der Entfernung von der Hansestadt aus keine effektive Lobbyarbeit durchführen konnte. Seit bald acht Jahren versucht die GVU nun schon Einfluss auf die wechselnde Bundesregierung in Berlin auszuüben, bislang mit eher mäßigem Erfolg.

Warum? Das Thema Urheberrecht hat bei vielen Politikern schlichtweg keine allzu große Priorität. Dies liegt in der Natur der Sache. Gemacht wird von Politikern zumeist das, was einem bei der nächsten Wahl mehr Stimmen bringt. Die Bedürfnisse einzelner Branchen oder ihrer Interessenverbände sorgen hingegen für keine stabilen Mehrheitsverhältnisse der eigenen Partei. Außerdem ist die Angelegenheit höchst kompliziert, weil sich das Internet nicht für Ländergrenzen interessiert. Dafür sind die Gesetze eines Staates nur innerhalb eines gewissen Gebietes gültig.

Wenn überhaupt wäre eine effektive Eindämmung der Urheberrechtsproblematik nur auf internationaler Basis möglich. Ob jeder Staat bei den zu erwartenden Einnahmen ihrer IT-Firmen ein größeres Interesse daran hat, ihr eigenes Geschäftsmodell zu zerstören, sei mal dahingestellt.

Ein paar Hoch- und Tiefpunkte der GVU

Operation Boxenstopp

An diese Aktion erinnert sich bei dieser Antipiracy-Organisation niemand gerne. Zwar sollte es im Februar 2006 eine Großrazzia im Kampf gegen deutsche Releaser-Crews und deren ftp-Sites werden. Am Ende war die GVU plötzlich einer der beschuldigten Parteien. Es kam sogar zu einer Hausdurchsuchung der Geschäftsräume des Vereins. Offenbar hatte einer der GVU-Mitarbeiter undercover mehr mit dem Betrieb oder der Finanzierung mindestens eines ftp-Servers zu tun, als man anfangs zugeben wollte. Eine Stellungnahme, ob die GVU als Zeuge oder Beschuldigter geführt wurde, gab die Staatsanwaltschaft Hamburg damals gegenüber der Redaktion der c't nicht ab ***[i]*** – ein peinliches Thema

Fachgespräch

Erinnert werden sollte an dieser Stelle auch an ein Experiment, das wirklich gut ausgegangen ist. Nicht nur mit dem ach so bösen Raubkopierer-Portal gulli.com war man bereit zu plaudern. Christine Ehlers, die ehemalige Pressesprecherin, und GVU-Jurist Jan Scharringhausen waren sogar bereit, mit den gulli:Usern selbst im Forum zu diskutieren. Dort findet man auch diverse interessante Aussagen zur Geschichte und selbst gestellten Aufgabe der GVU. ***[i1] [i2] [i3]***

Over and out: kino.to

Ein Highlight der GVU ist ohne Frage die Razzia gegen das frühere Streaming-Portal Kino.to. Wie der ehemalige Geschäftsführer Matthias Leonardy in einem Interview bekannt gab, kam der entscheidende Tipp aus dem direkten Umfeld des Betreibers Dirk B. Den beiden Denunzianten, die sich mit den Einnahmen aus Kino.to nicht zufrieden geben wollten, sagte man für ihre sachdienlichen Hinweise einen dicken Batzen Geld nebst der Strafmilderung zu. ***[i]***

Warnhinweis auf kino.to

Ausblick:

Halten wir fest. Das Internet unterliegt einem unfassbar schnellen Wandel. Was heute hipp ist, kann in sechs Monaten schon

vergessen sein. Auch die Hardware-Hersteller der Entertainment-Industrie müssen sich bei ihrer Entwicklung neuer Geräte stets den Bedürfnissen der Konsumenten anpassen. Nur die Unternehmen, die eigene Inhalte (Content) produzieren, sind und bleiben sehr langsam bei der Anpassung ihrer Geschäftsmodelle. So weigern sich die Filmstudios bis heute, etwas an der Verwertungskette zu ändern. Immer wieder werden neue Verträge aufgesetzt, die den Kinos für eine gewisse Zeit eine exklusive Aufführung zusichert. Nach Ablauf der Frist werden die Streifen per DVD und Blu-ray vertrieben, in der Zwischenzeit sind sie schon längst als Cam-Rip illegal erhältlich. Monate später beginnen endlich die Verhandlungen über die Ausstrahlung per Fernsehsender und das Internet.

Doch würde man sich flexibel zeigen und die Blockbuster gegen Bezahlung ins Internet streamen, dann könnte ganz schnell Schluss mit dem Kampf gegen die Windmühlen sein. Für Don Quichote (die GVU) könnte dies eines schönen Tages bedeuten, dass sie mangels Piraten nicht mehr zu tun haben. Doch ob dies je geschehen wird?

TECH DAYS

TECH DAYS 2017: WIR WAREN VOR ORT

Während die hochstehende Sommersonne Münchens Pflastersteine aufheizte, wurden in den gut klimatisierten Räumlichkeiten des Werkviertels die Tech Days 2017 ausgetragen. Ein kühler Kopf war auch nötig, denn Namhafte Unternehmen wie Giesecke & Devrient, Secunet, Fujitsu oder Infineon hielten Vorträge zu dem hochkomplexen und teilweise sehr theoretischen Thema „Post-Quantum-Encryption“. Aber auch eine Handvoll Startups präsentierten innovative Lösungen sowie Konzepte für eine sichere, digitale Welt.

Für thematische Abwechslung sorgte auf der Show-Bühne die Künstlerin YPL mit ihrer musikalisch untermalten Life-Performance „distorted vanity“ sowie Marco di Filippo, der am praktischen Beispiel „Social Engineering“ erläuterte. Das Highlight war aber ohne Frage die bereits erwähnte Vortragsreihe zur Post-Quantum-Security. Wo stehen wir heute? Was wissen wir über Quanten-Computer und wie können wir unsere Daten vor Fremdzugriff durch Konzerne und Regierungsorganisationen schützen? Um es vorwegzunehmen – einige der Antworten könnten Sie verunsichern.

Ungewissheit

Konkrete und vor allem verlässliche Details zum aktuellen Stand von Quanten-Computern sind Mangelware. Wie viele Qubits sind derzeit möglich? Die Angaben reichen von 17 echten Quantenbits bei IBM bis hin zu 2048 Qubits bei D-Wave, die jedoch „nur“ auf Basis von Quanteneffekten arbeiten und damit nicht dem Prinzip eines Quantencomputers entsprechen. Letzteres könnte in einigen Jahren eine Alternative zum klassischen Server darstellen und völlig neue Dienste ermöglichen. Alle Redner waren sich jedoch auch einig, dass die öffentlich vorgestellten Quantencomputer nicht den aktuellen Status repräsentieren. Selbst große Konzerne wie Google und IBM haben nur begrenzte Kapazitäten zur Verfügung. Sei es das Budget, die Ausstattung der Forschungseinrichtungen oder die wissenschaftlichen Mitarbeiter. Die Quantencomputer, an denen Regierungen in aller Welt arbeiten, sind weiter fortgeschritten und werden bereits sowohl im geschlossenen, als auch offenen Betrieb getestet.

Insbesondere das Brechen von Verschlüsselungen ist für Regierungen interessant und wichtig, um an sensible sowie vertrauliche Informationen heranzukommen. Da Speicherplatz heutzutage kaum noch etwas wert ist, können die über Jahre gesammelten Daten in ein umfangreiches Archiv abgelegt und nun dank Quantentechnologie verarbeitet werden. Vor allem ältere Daten, die meistens nur unzureichend geschützt waren, sind

betroffen. Mit der Zeit und steigender Leistung der Quantencomputer, nimmt das Risiko jedoch auch für sichere Verschlüsselungsmethoden zu. Eine Empfehlung auszusprechen, welche Verschlüsselung die derzeit beste Wahl ist, fällt aber allen Experten schwer. Eine Kombination aus RSA (über 2048 Bits) und Whirlpool stehen jedoch ganz weit oben auf der Präferenzliste.

Verschlüsselt jetzt. Sofort!

So tief die Angst vor Quantencomputern auch sitzen mag, komplett auf Verschlüsselung von Daten zu verzichten ist der falscheste Weg, den man gehen kann. Zum einen wird der Zugriff auf wichtige Informationen mit aktuellen, binären Computern erschwert. Zum anderen sind auch Quantencomputer keine Wundermaschinen und benötigen Zeit, um eine Verschlüsselung zu knacken. Präventiv muss eine Verschlüsselung also sowohl für lokale als auch online „in der Cloud“ gespeicherte Daten zwingend verwendet werden. Alte Daten, die auf eine schwache oder mittlerweile obsolete Verschlüsselung setzen, sind in Zero-Trust-Zonen neu zu verschlüsseln.

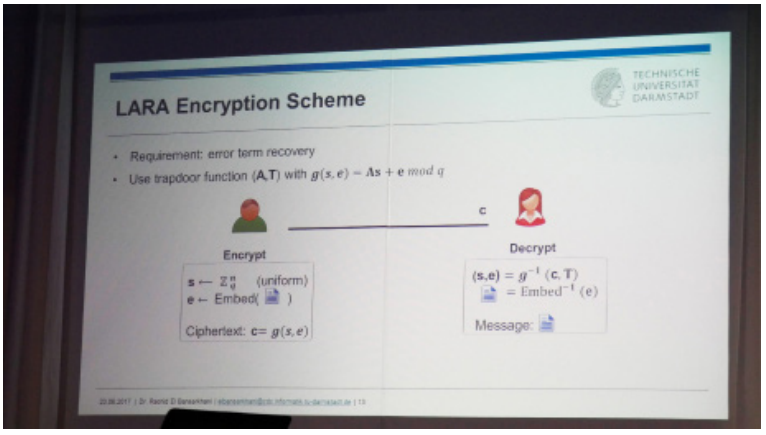
Neben Staatsbediensteten sind in unserer Zeit Journalisten einem Risiko ausgesetzt. Zwar gibt es noch immer solche, die behaupten nichts zu verbergen zu haben, doch der Trend entwickelt sich hin zu (abhör-)sicherer Kommunikation. „Ein Dank sollte nicht nur den schlauen Köpfen gelten, die hochkomplexe Verschlüsselungsverfahren ausarbeiten, sondern auch all denen ausgesprochen werden, die auf Verschlüsselung gänzlich verzichten. Jegliche Daten im Internet von sich preisgeben und Dienste wie Dropbox und Google Drive nutzen. Sie sind die Bauernopfer, die für ein Grundrauschen sorgen und die Maschinen (Anm.d.R sowie besagte Archive) mit (hoffentlich irrelevanten) Informationen füllen. So schnell Quantencomputer bei der Auswertung auch sein mögen, der Tag hat stets 24 Stunden und der menschliche (Fehler-)Faktor bei der Sortierung und Aufbereitung von Daten, sollte nicht unterschätzt werden“, so der Kommentar eines Teilnehmers in der QA-Runde.

Die technische Hürde für den Einstieg in die Verschlüsselung ist mittlerweile so gering, dass es keine sinnvollen Argumente gegen den zusätzlichen Schutz der Daten gibt. Selbst auf mobilen Geräten ist die Verschlüsselung durch die Bemühungen von Apple und Google salonfähig geworden. Staaten, wie Deutschland mit dem Bundestrojaner, bemühen sich zunehmend auf die sensiblen und privaten Daten zuzugreifen. Ein Quantencomputer würde dieses Vorhaben mit hoher Wahrscheinlich beschleunigen, doch in erster Linie nur wenn ein physikalischer Zugriff vorhanden ist. Wesentlich mehr gefährdet sind IoT-Geräte, die entweder unverschlüsselt kommunizieren. Oder eine sehr schwache Verschlüsselung aufweisen. Vor allem die Auswertung dieser Daten kann mit der Rechenleistung eines Quantencomputers effizient durchgeführt werden. Die Redner waren sich einig: Eine frühe Implementierung starker Sicherheitsmechanismen ist für die „Internet of Evering Ära“ enorm wichtig.

Mit Fehlern verschlüsseln

Dass Fehler nicht immer schlecht sind, zeigt der Vortrag zum „Learning with Errors“ von Dr. Rachid El Bansarkhani. Eine Post-Quantum-Kryptographie kann mit LWE, zumindest in der Theorie, umgesetzt werden. Für eine praktische Überprüfung fehlt der Zugang zu einem Quantencomputer – doch schon in der Vergangenheit haben Konzepte auf dem Papier auch in der Praxis funktioniert. Die Experten sprechen LWE das höchste Potential zu. Der Erfinder hinter LWE ist Oded Regev, der das Verfahren erstmals 2005 vorstellte.

LWE ist ein mathematisches Problem, das dem Lösen von Gleichungssystemen sehr ähnlich ist. Beim Learning-with-Errors-Problem wird jedoch ein oder mehrere zusätzliche Vektoren eingebaut, so dass der gewöhnliche Gaußschen Algorithmus nicht greift. Auf Basis dieses Problems wird ein Schlüsselaustausch realisiert, wobei als Voraussetzung knapp 245 KBytes an Daten zu übertragen sind. Eine Reduktion der Datenmenge wird durch den Einsatz von nicht zufälligen Zah-



len im Gleichungssystem erreicht. Die Einträge des Gleichungssystems werden zyklisch rotiert, so dass das System mit einer Datenmenge von ca. 4 KBytes auskommt. Dadurch erinnert es an einen klassischen Diffie-Hellmann-Schlüsselaustausch.

Viel Theorie und Prävention

Die Tech Days 2017 haben den Status Quo aufgezeigt und erneut an die Wichtigkeit und Bedeutung sicherer Verschlüsselungsverfahren erinnert. Zwar ist noch Vieles „nur“ Theorie und bis eine praktische Anwendung möglich ist, werden noch einige Jahre vergehen. Ein präventiver und aktiver Einsatz starker Verschlüsselungsverfahren ist heutzutage Pflicht. Zumindest für alle, die etwas zu verbergen haben.

Interaktive 360° Fotos

Anonym

Themenübersicht

WIRE SPEICHERT KONTAKTDATEN UNVERSCHLÜSSELT: ANONYMITÄT VS. BENUTZERFREUNDLICHKEIT

Es mag verrückt klingen, aber genauso ist es: Der Krypto-Messenger Wire setzt für seine Kommunikation auf eine State-of-the-Art-Verschlüsselung. Gleichzeitig werden alle Kontakte in der eigenen Datenbank unverschlüsselt gespeichert, wie der Sicherheitsforscher Thomas H. Ptácek herausgefunden hat. Kein Verfallsdatum: Die Daten werden erst von den Wire-Servern entfernt, sofern man seinen eigenen Account löschen lässt.

Thomas H. Ptácek schrieb die Betreiber des Messengers Wire vor einigen Tagen per Twitter an, weil ihm auffiel, dass die Software mit den Kontaktdaten nicht ganz so umgeht, wie er sich das vorgestellt hat.

Ihm wurde geantwortet, dieses Vorgehen biete den Nutzern bei der Anwendung des Messengers auf verschiedenen Geräten eine bessere User Experience an. Man könne so die Konversation mit vergleichsweise wenig Aufwand bei Verwendung eines neuen Geräts synchronisieren. Es könnte aber sein, dass sich dies bei einem der nächsten Updates ändern wird.

Das englischsprachige News-Portal Motherboard aka Vice brachte die Story nur einen Tag nach Ptáceks Tweet. Dort wird auch erwähnt, die Speicherung aller Kontakte ohne jegliche Verschlüsselung könnte zwar für die Nutzer ein erhebliches Problem darstellen, muss es aber nicht unbedingt. Dies sei stets von der Fragestellung abhängig, wie sicher bzw. anonym der Nutzer mithilfe von Wire kommunizieren will. Der CEO und Mitbegründer Alan Duric bestätigte gegenüber Motherboard, dass die Liste aller Personen, mit denen man je kommuniziert hat, erst dann gelöscht wird, sobald man seinen Wire-Account löschen lässt. Erst dann werden alle gespeicherten Verbindungen, E-Mail-Adressen, Telefonnummern bzw. Usernamen von den Wire-Servern entfernt. Duric führte weiter aus, dem Unternehmen ginge es darum, alternative Wege zu erforschen, wie die Kommunikation bei gleichzeitiger Anwendung der unterschiedlichsten Geräte realisiert werden kann.

Wir haben Wire um eine Stellungnahme gebeten. Man wies uns wenige Tage später auf einen neuen Beitrag bei medium.com hin. Dort heißt es, man habe bei der Entwicklung der Software alle Optionen abgewogen. Im O.-Ton wird ausgeführt:

After weighing the options, we settled on having the list of connections and conversations on our servers. This has several benefits:

- Full multi-device support. Wire does not rely on your phone as the main device. You can just as easily register on desktop or with your tablet and log in later on the phone.
- Synced chats. Sign in on a 2nd device and your friends and list of chats are already there. Chat history is not available on new devices, but from that moment onwards everything is nicely in sync.
- Group conversation experience. Group members can add and remove other participants, delete unintended messages from everyone's devices, and access the group from up to 8 devices.
- Better spam control. The concept of connections means that you have control over who can send you messages or call you. There's no room for large scale spam, phishing links, or malware "campaigns".
- Improved security. When you start using Wire on a 2nd device, Wire knowing your email address allows us to show you both an alert in the app, but also to email you about the login. This ensures you'll know if someone has compromised your account and to take appropriate actions.

Wire: Anonymität kontra Benutzerfreundlichkeit

Meinung: Die oben aufgezählten Vorteile lassen sich nicht von der Hand weisen. Ich persönlich finde aber, wenn der Anbieter eines Krypto-Messengers, der alles können soll, jede Menge Daten unverschlüsselt vorhält, dann hätte man dies den Nutzern schon im Vorfeld mitteilen müssen. Jeder, der auf seine Anonymität achtet, sollte dies schon vor dem ersten Chat wissen. Wenn die Kontaktdaten mit so einfachen Mitteln einsehbar sind, kann IMHO auch die sichere Abwandlung des Axolotl-Protokolls von Moxie Marlinspike nichts an der mangelnden Anonymität der Wire-User ändern.

GOOGLE: KONZERN TRACKT OFFLINE-EINKÄUFE

Google hat am Dienstag auf einer Konferenz in San Francisco für seine Werbekunden ein Tool vorgestellt, das ermitteln kann, wie viel Geld Kunden in physischen Geschäften ausgeben, nachdem sie auf Online-Werbung geklickt haben. Wenn das Programm funktioniert, könnte es helfen, Händler zu überzeugen, ihre digitalen Marketing-Budgets zu steigern, berichtet die „Los Angeles Times".

Um zu beweisen, dass die Google-Online-Werbung kausal mit dem Kauf einer Ware in einem bestimmten Geschäft verbunden ist, kombiniert Google das Online-Verhalten und die Käufe in Geschäften mit der Auswertung der Bewegungsprofile, mit denen der Konzern schon länger erfasst, in welche Geschäfte Nutzer gehen, u.a. um ihnen Werbung auf die Smartphones aufzuspielen. Zur Verfolgung des Kaufverhaltens seiner Nutzer über die verschiedenen Kanäle hinweg, setzt Google sowohl Datenanalyse-Modelle, als auch maschinelles Lernen ein.

Die Idee dahinter ist, die Kunden so zu beobachten, dass man sehen kann, welche Google-Online-Ads sie anklicken und demnach Interesse für bestimmte Produkte zeigen, um dieses Interesse mit Kreditkarten-Käufen in Geschäften zu verbinden. Das wäre dann ein Hinweis darauf, dass Online-Werbung genauso Geschäften hilft, ihre Waren an die Kunden zu bringen, auch wenn der eigentliche Kauf erst Tage später stattfindet. Dazu gleicht dann Google die Klicks auf Online-Werbung von eingeloggten Google-Nutzern mit Daten zu Käufen per Kredit- und Bankkarten im Handel ab.

So gab Google an, in den USA über Partner Zugang zu 70 Prozent aller Kredit- und Bankkarten-Transaktionen zu haben. Wenn also in der Folge einem Anwender auf seinem Smartphone mehrfach von Googles Werbeprogramm Anzeigen für ein bestimmtes Produkt gezeigt werden und dieser dann mit seinem Android-Mobiltelefon in einem Geschäft eben dieses Produkt kauft, kann man davon ausgehen, dass die Google-Werbung erfolgreich war.

Der Vorteil für Google wäre, dass sich auch Kaufentscheidungen nachverfolgen lassen, bei denen zwischen Anzeigeneinblendung und Transaktion etwas Zeit vergeht. Es ist also nicht nötig, dass der Kunde direkt nach dem Ansehen des Banners einen entsprechenden Kauf tätigt. Die so gewonnenen Daten ergänzen die digitalen Dossiers, die Google für Benutzer seiner Suchmaschine und anderer Dienste zu-

sammengestellt hat, darunter Gmail, YouTube und Android.

Auf Basis der gesammelten Daten könne zwar nicht erhoben werden, was konkret gekauft wurde oder wie viel bestimmte Personen ausgegeben haben, aber es erlaubt Rückschlüsse über die Wirkung von Online-Werbung, meint Sridhar Ramaswamy, Google's Senior Vice President für Werbung und Commerce. Persönliche Informationen seien bei den Einkäufen im Offline-Handel von Google nicht einsehbar, umgekehrt könnten auch Partnerunternehmen nicht auf die von Google gesammelten Daten zugreifen, versichert Ramaswamy. Man werte nur Google-Ads nach den Profilen der Werbekunden aus, wozu man Algorithmen verwende, die Datenschutz gewährleisten (double-blind encryption). Für die wurden Patente angemeldet, sie sind kein Geschäftsgeheimnis.

Die Arten von Daten, die Google sammelt, könnten jedoch ein einladendes Ziel für Hacker werden, sagte Miro Copic, Marketingprofessor an der San Diego State University. Er sprach weiterhin von einer „massiven Implikationen für die Privatsphäre" und warnte vor den Folgen solcher Datensammlungen. Selbst wenn Google gute Absichten verfolge, könnten die Daten dennoch künftig missbraucht werden.

Fazit

Mit Google-Ads setzte Google letztes Jahr ca. 80 Milliarden US-Dollar um. Allerdings sollten dem Gewinn nach oben keine Grenzen gesetzt werden, daher dehnt der Konzern nun seine Kundenüberwachung in den USA auch auf Offline-Käufe aus. Sie wollen auf diese Weise Werbekunden demonstrieren, dass Online-Werbung auch dann ihr Geld wert ist, wenn die User zwar auf die Werbung klicken, aber zeitnahe online nichts kaufen.

SPOTIFY: BIN ICH AUCH VOM HACK BETROFFEN?

Eine unbekannte Hackergruppe namens „The Leak Boat“ hat in der Nacht zum Dienstag via Twitter Zugangsdaten tausender Nutzerkonten von Spotify veröffentlicht. Nach Angaben der Hacker sind etwa 9.000 real existierende Spotify-Konten betroffen.

Der beliebte Musikstreaming-Dienst Spotify ist einem Hacker-Angriff zum Opfer gefallen. Auf der Website Ghostbin wurden Passwörter und Nutzernamen aus aller Welt von der bisher noch unbekannten Hacker-Gruppe „The Leak Boat“ veröffentlicht. Mittels der bereitgestellten Logins könnte man sich theoretisch ohne Probleme anmelden und würde damit zum jeweiligen Nutzerprofil gelangen. Somit wären Kontakte, E-Mail und Adressdaten für jedermann beliebig erreichbar.

Bei weltweit insgesamt mehr als 100 Millionen Spotify-Kunden (davon 50 Millionen Abonnenten) ist ein eher kleiner Nutzerkreis von dem Hack betroffen. In einer öffentlich gemachten Account-Liste sind die Zugangsdaten von 6.410 Spotify-Kunden aufgeführt, darunter befinden sich genauso deutsche Konten. Ob man selbst auch zu den Opfern gehört, ist schnell herausgefunden. Man braucht nur den auf Twitter veröffentlichten Links nach ghostbin.com zu folgen und diese Listen auf die eigenen Daten hin zu überprüfen. Allerdings sollte man, auch wenn man nicht betroffen ist, unbedingt das Spotify-Passwort ändern.

> Here's a few #Spotify Prems, get em' more they're changed!https://t.co/LTlzTQOeMh#Lulzocalypse#SecTeamSix@IntelGroupHax@Requpwns
>
> — The Leak Boat (@SecTeamSix_) 24. Mai 2017

„The Leak Boat“ haben bereits nachgelegt und noch weitere Enthüllungen via Twitter veröffentlicht. Unter den neuen Informationen ist die eingescannte Signatur des kürzlich entlassenen FBI-Direktors James Comey zu finden, private Nacktfotos der US-Schauspielerin Kristanna Loken und einige Zugangsdaten zur Online-Spieleseite wizard101.com. Die Hacker kommentieren diesen Tweed selbst wie folgt: „Nicht viel, aber Kinder werden sich darüber freuen“. Weitere Enthüllungen sollen folgen.

Wie die Hacker an die Zugangsdaten gelangten und ob es sich um einen aktuellen Datenstand handelt, ist augenblicklich nicht bekannt. Spotify hat sich bislang nicht öffentlich zum Vorfall geäußert, weder im offiziellen Presse-Kanal noch auf Twitter.

BUNDESTAG: ONLINE-ZUGRIFF AUF PASSFOTOS GENEHMIGT

Der Bundestag hat am Donnerstag (18.05.2017) mit der Mehrheit der großen Koalition gegen die Stimmen von Linken und Grünen eine Änderung des Personalausweisgesetzes beschlossen. Datenschützer sind beunruhigt.

So sollen künftig Personalausweise standardmäßig mit einer einsatzbereiten Onlinefunktion (eID) ausgegeben werden. Zudem wird mit dem Gesetz auch das Zugriffsrecht der Sicherheitsbehörden auf die Ausweisbilder stark erweitert. Automatisierten Zugriff rund um die Uhr auf die biometrischen Lichtbilder aus Personalausweis und Pass bei den Meldeämtern haben demnach Polizei, Geheimdienste, Steuer- und Zollfahnder sowie Ordnungsbehörden.

Bisher war der Online-Zugriff in Eigenregie auf Passfotos den Geheimdiensten gar nicht gestattet, den Ermittlungs- und Ordnungsbehörden sowie Steuer- und Zollfahndern nur unter engen Einschränkungen, nämlich wenn die Ausweis- beziehungsweise Passbehörde nicht erreichbar war oder bei Gefahr im Verzug, also wenn Abwarten den Ermittlungszweck gefährdet hätte. Diese Schranken fallen nun. Der Kreis der Abrufberechtigten wurde um die Verfassungsschutzämter, den Bundesnachrichtendienst (BND) sowie den Militärischen Abschirmdienst erweitert.

Bereits in dem seit November 2010 eingeführten Personalausweis ist ein elektronischer Identitätsnachweis integriert. Damit lassen sich beispielsweise Behördengänge online erledigen. Allerdings haben nach den Angaben vom Bundesinnenministerium von insgesamt 45 Millionen Bürgern, an die die Ausgabe des Ausweises erfolgte, nur schätzungsweise ein Drittel der Ausweisinhaber die Onlinefunktion tatsächlich aktiviert und nur 15 Prozent davon, also etwa 2,5 Millionen Bürger, haben die Funktion überhaupt schon einmal genutzt. Die Regierung

will das jedoch ändern und sie nun verpflichtend aktivieren.

Die große Koalition begründet diese Änderung des Personalausweisgesetzes damit, dass eine Identitätsüberprüfung von Personen durch die Sicherheitsbehörden auf Lichtbilderbasis „zeitkritisch und zugleich auch aus Gründen der Gefahrenabwehr rund um die Uhr“ nötig sei. Ziel wäre es dabei, die Zahl der ins Vertrauen zu ziehenden Personen „auf das unbedingt notwendige Maß zu beschränken“. Auch reduziere sich für die Meldeämter der Verwaltungsaufwand. Dem Datenschutz werde Rechnung getragen.

Kritik kommt vom Grünen-Abgeordneten Konstantin von Notz: „Die bürgerrechtliche Krone im zynischen Sinne setzt die Große Koalition dem ganzen aber nun erst auf: Es ist die im Gesetz sorgfältig auf den hinteren Seiten versteckte Einführung des – nach dem Änderungsantrag völlig – voraussetzungslosen Pass- bzw. Personalausweisfotoabgleichs durch alle bundesdeutschen Geheimdienstes im automatisierten Verfahren. Das ist nichts anderes als der offene Einstieg in eine bundesweite biometrische Bilddatenbank aller Bundesbürger. Und dies vor dem Hintergrund der Tatsache, dass man derzeit am Bahnhof Südkreuz in Berlin die intelligente Videoüberwachung mit Gesichtserkennung an öffentlichen Plätzen testen.“

Die Bundes-Datenschutzbeauftragte Andrea Voßhoff (CDU) sagt: „Der nahezu voraussetzungslosen Abruf des Lichtbildes wird aus datenschutzrechtlicher Sicht abgelehnt.“

Ihr Vorgänger, Peter Schaar, ehemaliger Bundesdatenschutzbeauftragter kritisiert das Vorhaben ebenso. Er ist der Meinung, in dem Gesetz stecke eine „datenschutzrechtliche Ungeheuerlichkeit“. Vorgesehen ist darin auch, dass die Sicherheitsbehörden von Bund und Ländern in Zukunft das biometrische Lichtbild im Ausweis „zur Erfüllung ihrer Aufgaben im automatisierten Verfahren“ abrufen dürfen. Schaar befürchtet eine Massenüberwachung. Er sprach von einem „Big-Brother-Gesetz“. Die bisherigen Auflagen habe der Gesetzgeber eingeführt, um eine „Massenüberwachung“ anhand der Gesichtsfotos zu verhindern. Jetzt sei damit zu rechnen, „dass die umfassenden Abrufmöglichkeiten längerfristig dazu verwendet werden, im Rahmen der ‚intelligenten Videoüberwachung‘ alle Menschen zu identifizieren“, die sich im öffentlichen Raum aufhielten.

Auch FDP-Vize Wolfgang Kubicki hat Bedenken. Dem RedaktionsNetzwerk Deutschland sagte er: „Da das automatisierte Verfahren standardmäßig erfolgen soll, wird hier faktisch eine biometrische Datenbank aller Bürger geschaffen. Zusammen mit der geplanten Ausweitung der Videoüberwachung sind wir dann gefährlich nah am Überwachungsstaat“.

Constanze Kurz, Sprecherin des CCC, nannte in einer Stellungnahme den elektronischen Personalausweis ein „totes Pferd“, das nun wiederbelebt werden soll: eID werde deshalb nicht genutzt, weil die Bürger kein Interesse an dem System hätten oder ihm nicht vertrauten. Und nicht, weil sie nicht wüssten, wie sie die Funktion aktivieren können. „Dieses fehlende Vertrauen lässt sich auch durch eine zwangsweise Aktivierung nicht zurückgewinnen.“

BAUSBACK FORDERT RECHTSSICHERHEIT IM KAMPF GEGEN DARKNET-GESCHÄFTE

Bayerns Justizminister Winfried Bausback möchte zum einen Stalking-Opfer besser schützen und zum anderen brauche es mehr Rechtssicherheit bei Postsendungen nach Darknet-Geschäften, sagte er der Deutschen Presse-Agentur in München.

Bei der am 21.06.2017 beginnenden Justizministerkonferenz in Rheinland-Pfalz will sich der CSU-Politiker dafür einsetzen, dass auch Stalkern elektronische Fußfesseln angelegt werden dürfen. Zudem setzt er sich für mehr Rechtssicherheit bei Postsendungen nach Darknet-Geschäften ein.

Seit dem Jahr 2013, dem Ende des originalen Silk Road, gab es einen regelrechten Boom an illegalen Online-Marktplät-

zen, die nur über das Tornetzwerk zu erreichen sind. Verschiedene Drogen und verschreibungspflichtige Medikamente sind dort genauso im Angebot, wie Falschgeld, Waffen und Tutorials für Cyberkriminalität. Im Darknet können sich Internetnutzer fast komplett anonym bewegen. Auch der Amokläufer von München hatte seine Waffe im Darknet geordert.

Die Rechtslage in Bezug auf das Auskunftsverlangen nach Auslieferung von im Darknet besteller Ware ist aktuell unklar. So können Ermittler nach geltendem Recht von Postdienstleistern Auskunft über Name und Anschrift des Absenders und des Adressaten nur solange verlangen, wie die Postsendung unterwegs ist, erklärte Bausback. Ist die Sendung jedoch erst einmal ausgeliefert, beurteilten Gerichte die Frage unterschiedlich, ob die Ermittlungsbehörden eine entsprechende Auskunft erhalten können. Diese Rechtsunsicherheit müsse schleunigst beseitigt werden, fordert der Minister: „Denn eines ist klar: Gerade am Übergang von der virtuellen zur realen Welt ergeben sich vielversprechende, ja leider allzu oft die einzigen Ansätze, um Tatverdächtige zu identifizieren und dingfest machen zu können.“[…] „Bei aller Anonymität der digitalen Welt, die die Ermittlungen regelmäßig sehr schwierig macht – die Ware muss analog und real versandt werden. Und bei diesem Übergang der virtuellen zur realen Welt müssen unsere Ermittler auf gesicherter rechtlicher Grundlage den Fuß in die Türe bekommen, indem sie auch nachträglich Auskünfte über Absender und Empfänger von Postsendungen erhalten.“

Zum Thema Stalker meint Bausback, dass Täter sich mit einer elektronischen Fußfessel nicht mehr unbemerkt dem Opfer annähern könnten „Und: Sie erhöht das Entdeckungsrisiko und die Hemmschwelle für die Täter, mit den Opfern weiter ihr perfides Katz-und-Maus-Spiel zu spielen.“ Auf verurteilte Stalker, von denen weiterhin Gefahr ausgeht, müsse der Rechtsstaat ein besonderes Auge haben. Die Fußfessel sei zwar kein Allheilmittel. Dennoch: „Wenn das Opfer weiß, der Stalker trägt eine elektronische Fußfessel, kann dies dem Opfer zumindest ein gewisses Sicherheitsgefühl geben. So wird es ihm regelmäßig leichter fallen, sein Leben normal weiterzuführen.“

BERLINER BAHNHOF SÜDKREUZ: POLIZEI SUCHT TESTPERSONEN FÜR GESICHTSERKENNUNG PER VIDEO

Ein sechsmonatiges Projekt zur Erprobung von intelligenter Videotechnik startet zum 1. August 2017. Dafür werden bis

zu 275 Freiwillige gesucht, die bei dem Testlauf mitmachen wollen, vorzugsweise Personen, die den Bahnhof häufiger nutzen, etwa als Pendler und die zudem die markierte Testzone in der Westhalle des Bahnhofes durchqueren. Seit Montag wirbt die Bundespolizei an dem Bahnhof für eine Beteiligung.

Zum geplanten Probelauf am 01.08.2017 zur Gesichtserkennung per Videotechnik am Berliner Bahnhof Südkreuz sucht die Bundespolizei Testpersonen. Beteiligt am Probelauf sind sowohl das Bundesinnenministerium, als auch die Deutsche Bahn und das Bundeskriminalamt. Den Polizeibehörden geht es darum, die technischen Möglichkeiten unter realen Bedingungen auszuloten.

Gemäß den Plänen von Bundespolizei und Deutscher Bahn soll der Berliner Bahnhof Südkreuz zu einem Modell-Projekt für die Verwendung expandierender Überwachungstechnik werden. Hier kommen künftig nicht nur die ohnehin immer häufiger zu findenden Überwachungskameras zum Einsatz, sondern diese werden zusätzlich noch mit einer Software zur Gesichtserkennung gekoppelt. So lässt sich im Grunde jederzeit nachvollziehen, wer den Bahnhof wann und wie oft nutzt.

Von den Testpersonen werden verschiedene Lichtbilder angefertigt, die in einer Testdatenbank abgelegt und für ein Jahr gespeichert werden. Zudem werden die Lichtbilder auch für ein Fake-Verbrecherprofil benötigt, die in der Datenbank „gesuchter Personen“ gespeichert werden, damit die Kameras aufgrund des Abgleichs gegenbenenfalls Alarm anzeigen können. Die Probanden bekommen für dieses Projekt einen RFID-Transponder-Chip in Form einer Kreditkarte, den sie an einem Schlüsselbund oder ähnlichem bei sich tragen müssen für eine Gegenkontrolle. So soll festgestellt werden, ob das System die Person tatsächlich immer erkennt, wenn sie einen markierten Bereich im Bahnhof betritt. Dieser Bereich ist mit RFID-Baken „abgezäunt“. Die Freiwilligen mit den RFID-Transpondern sollen so auf jeden Fall erkannt werden, sobald sie die Fläche betreten. Diese Daten bilden die Referenzmenge zu den Erkennungsraten der automatischen Gesichtserkennung, sodass die

Quote der „False Positives“ und „False Negatives“ bestimmt werden kann. Überschreiten beide einen Grenzwert, ist die Gesichtserkennung gescheitert: Entweder gibt es dann zu viele Fehlalarme oder zu viele „Gesuchte“ werden nicht erkannt.

Ferner wird, unabhängig von diesem Feldtest, ein weiterer Test durchgeführt, auch mit Videokameras, doch mit anderer Software. Dabei sollen die Systeme potenziell gefährliche Gegenstände erkennen, wie Koffer, die auf den Bahnsteig gestellt und verlassen wurden, stürzende Personen oder die Aktionen von Graffitti-Sprayern. Auch die Mustererkennung von Taschendieben, die in meistens in Gruppen auftreten, wird dazugehören.

Beide Tests sollen letzlich als Vorstufen dazu dienen, den gesamten Berliner Bahn-Nahverkehr umfassend mit dem getesteten Videoüberwachungssystem auszurüsten. Geplant ist es, dass bereits Ende 2017 alle Berliner S-Bahnhöfe mit Videokameras ausgestattet sind. Eine zentrale Leitstelle der Bahn und der Bundespolizei hat dann Zugriff darauf. Derzeit werden nur alle „Wechselbahnhöfe“ durchgängig überwacht mit einem Einsatz von ca. 1000 Kameras, 80 davon am Bahnhof Südkreuz.

Wer sich freiwillig als Testperson meldet und im gesamten Testzeitraum mindestens an 25 unterschiedlichen Tagen durch die gekennzeichnete Zone läuft, soll einen Amazon-Gutschein im Wert von 25 Euro erhalten. Wer an über 30 Tagen und am häufigsten von allen Testpersonen erfasst wird, soll einen der Hauptpreise erhalten, wie eine Apple Watch Series 2, eine Fitbit Surge oder eine GoPro Hero Session. Reisende, die nicht überwacht werden wollen, empfiehlt die Bundespolizei, die „Ausweichmöglichkeiten“ zu nutzen.

In einer FAQ der Bundespolizei heißt es zuversichtlich: „Mit dieser Technik könnte es gelingen, Straftaten und Gefahrensituationen vorab zu erkennen. Mögliche Gefährder könnten vor einem geplanten Anschlag festgestellt und dieser verhindert werden.“

Aus Sicht der Bundesbeauftragen für Datenschutz, Andrea Voßhoff, sei das Projekt „für sich genommen noch nicht als schwerwiegender Eingriff zu sehen”. Das ändere allerdings nichts an „grundsätzlichen Bedenken” gegen diese Technologie. „Sollten derartige Systeme später einmal in den Echtbetrieb gehen, wäre dies ein erheblicher Grundrechtseingriff.” Auch Berlins Datenschutzbeauftragte Maja Smoltczyk hatte die Technik zur Gesichtserkennung zuvor als problematisch kritisiert. Sie könne „die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören“, gibt sie zu bedenken. Ebenso tadelt der innenpolitische Sprecher der Grünen im Abgeordnetenhaus, Benedikt Lux, das Vorhaben:„Wir auf dem Weg in ein absolutes Überwachungsszenario“, meint er.

UMFRAGE: DEUTSCHE SIND GEGEN OFFLINE-TRACKING IM SUPERMARKT

Was in Online-Shops bereits zum Alltag gehört, soll nun auch im Einzelhandel Einzug halten – Kundentracking. Die Idee, das Kaufverhalten der Kunden zu analysieren, weckt inzwischen genauso Begehrlichkeiten bei Inhabern von herkömmlichen Ladengeschäften. Passende Technologien stehen bereits dafür bereit. Die EU will das erlauben jedoch die Mehrheit der Deutschen ist laut einer aktuellen Umfrage dagegen.

Die Einzelhandelskette der Metro Group, Real, hat als Vorreiter für den Einzelhandel die Gesichtsanalyse an der Supermarkt-Kasse schon mal ausgetestet, um zielgerichtete Werbung noch besser an den Kunden zu bringen. Andere Handelsketten werden sicher auch schon bald diese Möglichkeit für sich entdecken und entsprechend nachziehen. So möchten Shop-Betreiber z.B. das Alter und das Geschlecht der Kunden wissen, welche Inhalte sie sich dort wie lange ansehen, welche Artikel sie kaufen usw., ganz nach dem Motto, mehr Daten – mehr Informationen – größere Gewinne. Tracking-Tools, die diese Informationen sammeln, sind vorhanden und lassen sich nach Maßgabe von § 15 Abs. 3 Telemediengesetz auch datenschutzkonform nutzen.

Die Gesichtsanalyse ist nur eine von zahlreichen gangbaren Varianten. Mit Offline-Tracking sind aber auch die Möglichkeiten gemeint, Verbraucher in der Offline-Welt über ihr Smartphone zu identifizieren. Smartphones senden eindeutig wiedererkennbare Signale und Identifikationsnummern – etwa um Internet-, WLAN- oder Bluetooth-Verbindungen zu ermöglichen. Vor diesem Hintergrund erfassen WiFi-Hotspots von allen Smartphones in Reichweite die sog. MAC-Adresse und

die Signalstärke. Einzige Voraussetzung hierfür ist eine aktive Wifi-Schnittstelle am Endgerät. Die MAC-Adresse ist eine unveränderbare Ziffernfolge, durch die der Hotspot das Endgerät eindeutig erkennen kann. Anhand der Signalstärke lässt sich bestimmen, wie weit Hotspot und Endgerät voneinander entfernt sind. Beim WLAN-Tracking wird die Verkaufsfläche mit einer Vielzahl von Hotspots ausgestattet. Auf diese Weise lassen sich Kunden, die ein netzwerkfähiges Smartphone bei sich tragen, zuverlässig orten und ihre Bewegung über die Verkaufsfläche nachvollziehen und deren Aufenthaltsdauer in Geschäften bestimmen oder Kunden wiedererkennen, wenn sie zum wiederholten Mal am Schaufenster stehen bleiben – und ganz ohne das der Kunde davon etwas mitbekommt. Zudem enthalten viele Apps Werbemodule, die verschiedene Informationen erfassen und übermitteln, die auf den Mobiltelefonen der Nutzer gespeichert sind. Auch darunter könnten Identifikationsnummern fallen, die eindeutig einem bestimmten Gerät zugeordnet werden und mit anderen Informationen verknüpft werden können.

Aus einer aktuellen, repräsentativen Umfrage von forsa im Auftrag des Bundesverbands der Verbraucherzentralen (vzbv) geht hervor, dass die Verbraucher die Hoheit über ihre Bewegungsdaten wollen. Für den Verbraucherzentrale Bundesverband befragte forsa 1002 repräsentativ ausgewählte Bürger ab 18 Jahren zwischen dem 24. und 26. April 2017.

Im Ergebnis dieser Umfrage will die Mehrheit, nämlich 54 Prozent der Deutschen, dass die Nutzung der Bewegungsdaten ihrer Handys generell verboten wird. 34 Prozent halten demnach eine solche Auswertung unter gewissen Bedingungen für akzeptabel, nur neun Prozent finden das sogenannte Offline-Tracking generell akzeptabel.

Klaus Müller, Vorstand des Verbraucherzentrale Bundesverbands (vzbv), wertet das Ergebnis wie folgt aus: „Verbraucherinnen und Verbraucher in Deutschland sehen das Offline-Tracking sehr kritisch. Die Bundesregierung sollte sich im Europäischen Rat dafür einsetzen, dass die Interessen der Verbraucher berücksichtigt werden. Der aktuelle Entwurf der ePrivacy-Verordnung schützt Verbraucher in diesem Punkt unzureichend“. Er zeigt sich mit dem derzeitigen Entwurf für die neue E-Privacy-Verordnung der EU demnach unzufrieden. So befürchten die Verbraucherschützer: „Das könnte in Zukunft zum Alltag gehören, denn die geplante EU-Verordnung setzt dieser Praxis keine Grenzen“.

Auszusetzen an dem aktuellen Entwurf der EU-Kommission wäre, dass für das Offline-Tracking keinerlei Widerspruchsmöglichkeiten vorgesehen sind. So sollen Verbraucher lediglich Hinweise erhalten, wenn sie einen derart überwachten Bereich betreten. Fraglich jedoch ist, wie die Hinweise gestaltet werden müssten, damit Verbraucher sie auch wahrnehmen und verstehen können. „Die vorgeschlagenen Regelungen sind absolut inakzeptabel. Verbraucher, die nicht überwacht werden wollen, hätten nur die Möglichkeit, den Flugmodus anzuschalten. Da macht ein Mobiltelefon kaum noch Sinn. Die EU muss Regeln treffen, damit Verbraucher selbst entscheiden können, ob ihre Daten erhoben werden dürfen“, so Müller.

Fazit

Wenngleich die E-Privacy-Verordnung der EU eigentlich die Kommunikationsdaten der Bürger besser schützen sollte, sieht sie doch auch Einschränkungen beim Zugriff auf Online-Daten vor, erlaubt sie in der Offline-Welt jedoch das Tracking…und das ganz ohne größere Einschränkungen.

Genau das wird von den Verbraucherschützern kritisiert, denn nach dem aktuellen Entwurf zur ePrivacy-Verordnung wären Verbraucher beim Offline-Tracking nicht ausreichend geschützt. Der vzbv fordert deshalb, dass Kunden, bevor die Märkte deren Smartphones anzapfen dürfen, erst eine ausdrückliche Einwilligung aussprechen. Mit dieser Meinung sehen sie sich durch die Umfrage bestätigt. Die E-Privacy-Verordnung soll ab Mai 2018 in Kraft treten.

THOMAS DE MAIZIÈRE FORDERT AUSWEITUNG DER ÜBERWACHUNG

Innenminister Thomas de Maizière (CDU) will die staatlichen Befugnisse im Kampf gegen den Terrorismus weiter ausweiten. Im „Tagesspiegel am Sonntag“ forderte er für die Sicherheitsbehörden vollen Zugriff auf die Kommunikation in verschlüsselten Messenger-Diensten, wie WhatsApp. Zudem solle eine erweiterte Videoüberwachung zum Einsatz kommen.

Mehr Überwachungsmöglichkeiten sollen den Sicherheitsbehörden sowohl im Kampf gegen den Terrorismus, aber auch, um Gefährder und Straftäter zu fassen, künftig zur Verfügung stehen:

Ermittler sollen Zugriffsmöglichkeiten auf verschlüsselte Messenger-Dienste, wie WhatsApp erhalten Ausweitung der Videoüberwachung mit Gesichtserkennung Online-Durchsuchung und Quellen-Telekommunikationsüberwachung (TKÜ) kommen zum Einsatz

Galten Messenger, wie WhatsApp, bis vor kurzem noch als relativ sicher, da sie eine sogenannte Ende-zu-Ende-Verschlüsselung bieten, fordert Bundesinnenminister Thomas de Maizière (CDU) nun in einem Interview mit dem Berliner „Tagesspiegel„ dass Sicherheitsbehörden auch auf die verschlüsselte Kommunikation über Messenger-Dienste wie WhatsApp zugreifen dürfen: „Wir wollen, dass Messenger-Dienste eine Ende-zu-Ende-Verschlüsselung haben, damit die Kommunikation unbescholtener Bürger ungestört und sicher ist. Trotzdem brauchen Sicherheitsbehörden, wie bei einer SMS auch, unter bestimmten Voraussetzungen Zugriffsmöglichkeiten“, gibt er an.

Dazu könnten Online-Durchsuchung und Quellen-Telekommunikationsüberwachung (TKÜ) als wirksame Instrumente genutzt werden. Bei der Quellen-TKÜ können die Behörden mit einer Software die laufende Kommunikation eines Verdächtigen bereits auf einem Gerät mitlesen, bevor sie verschlüsselt wird.

Einsatzbereich von Videoüberwachung mit Gesichtserkennung wäre über Bahnhöfe hinaus auszuweiten

Im Kampf gegen den Terror will de Maiziere noch zusätzliche Überwachungsmöglichkeiten schaffen. So sollten die Sicherheitsbehörden außerdem Software zur Gesichtserkennung nutzen können. Zwar habe man derzeit an Bahnhöfen die Videoüberwachung. Man verfüge aber nicht über die Möglichkeit, das Bild etwa eines flüchtigen Terroristen in die Software einzuspielen, so dass ein Alarm ausgelöst werde, wenn er irgendwo an einem Bahnhof auftauche, nannte de Maizière als Beispiel.

Thomas de Maizière kündigte an, im Sommer werde es am Berliner Bahnhof Südkreuz einen Probebetrieb mit Freiwilligen geben. Der Minister hält es demnach auch für möglich, den Einsatzbereich über Bahnhöfe hinaus auszuweiten: „Wenn die Software wirklich zuverlässig funktioniert, sollte sie bei schweren Verbrechen auch an anderen Stellen zum Einsatz kommen können, an denen öffentliche Videokameras eingesetzt werden“. Die Grundrechtseinschränkung sei dabei gering, da Unbeteiligte nicht erfasst würden, meint de Maizière.

Beide Instrumente sollen in den kommenden Sitzungswochen in der Strafprozessordnung geregelt werden. Der Maßstab müsse sein, was die Polizei im analogen Bereich darf, „das muss sie auch im Digitalen rechtlich dürfen und technisch können“, fordert de Maizière.

Die Vorschläge des Innenministers dürften auf erhebliche Kritik stoßen. Die rot-rot-grüne Koalition in Berlin sperrte sich im Januar nach dem Anschlag auf den Breitscheidplatz gegen eine groß angelegte Videoüberwachung.

USA-EINREISE: INTERNETAKTIVITÄT WIRD PRÄZISE ABGEFRAGT

Welche E-Mail-Adresse ist in Verwendung, wie heißen die Social Media Accounts, wo arbeiten Sie und mit wem sind Sie verwandt? All das sind Fragen, die wohl niemand gerne beantworten möchte. Doch wer künftig in die USA einreisen will und als „verdächtig“ gilt, muss diese Informationen preisgeben.

„Was, Sie wollen uns Ihren Facebook-Account nicht geben? Dann dürfen Sie nicht einreisen!“ So oder so ähnlich dürfte wohl künftig die Devise bei der Grenzkontrolle lauten. Die US-Regierung hat verschärfte Einreisebestimmungen eingeführt, die es in sich haben. Gilt man als „verdächtig“, ist man gezwungen, persönliche Daten, auch über Social-Media-Accounts, anzugeben – ansonsten wird einem die Einreise verweigert. Zu den Fragen gehört etwa, welchen Namen man in den letzten fünf Jahren bei sozialen Netzwerken verwendet hat sowie die dazugehörige E-Mail-Adresse.

Befragungen zu Reisen, Familienmitgliedern und dem Arbeitsleben

Des Weiteren muss der Antragsteller eines Visums private Details über die familiäre Situation angeben: Daten über Geschwister, Ehegatten und Kinder sind Pflicht. Außerdem interessiert sich das US-Außenministerium für die Arbeitgeber der letzten 15 Jahre, Wohnorte der vergangenen 15 Jahre – sowie für die in den vergangenen 15 Jahren bereisten Ländern. Das Formular ist ein Zusatz zu den bestehenden Visa-Antragsformularen. Laut der Behörde müssen es nur die Personen ausfüllen, deren Identität bestätigt werden muss oder wenn eine gründlichere Untersuchung aufgrund der nationalen Sicherheit nötig sei. So werden bislang etwa 0,5% der Antragsteller aufgefordert, das Einreiseformular auszufüllen. Das wären dann immerhin 65.000 Ausländer.

Teil von Präsident Trumps Verschärfungen

Das Programm ist Teil der Verschärfung der Einreisebestimmungen von US-Präsident Donald Trump (Republikaner). Zuletzt ist das Einreiseverbot für Bürger einiger muslimischer Staaten in die Kritik geraten. Das radikale Einreiseverbot wurde letztlich von US-Gerichten gestoppt. Auch eine mäßigere Variante ist vor Gericht gescheitert. Die US-Regierung will an den Bestimmungen festhalten. Präsident Trump will bis vor den Obersten Gerichtshof ziehen.

GNUPG STARTET NEUE SPENDENKAMPAGNE

Am gestrigen Dienstag wurde eine neue Spendenkampagne zur Förderung des Kryptographiesystems GNU Privacy Guard (GnuPG) gestartet. Ziel ist es, die Fortsetzung des Projekts dauerhaft zu sichern. In zahlreichen Videos erläutern Journalisten und Bürgerrechtler, warum die Verschlüsselung von Informationen für sie so wichtig ist.

Vertreter von Bürgerrechtsbewegungen & NGOs, Journalisten, Unternehmen, Aktivisten, Anwälte und viele mehr verlassen sich auf GnuPG, um damit ihre Kommunikation zu schützen. Die kostenlose als auch quelloffene Software schützt neben E-Mails auch Dateien und Programme vor staatlichem und kriminellem Abhören auf Windows, Mac OS und Linux. Außerdem benutzen mehr als zwei Drittel aller Internetserver GnuPG, um die Updates ihrer Systemsoftware abzusichern.

Wer sich unseren historischen Abriss der NSA durchgelesen hat, der weiß, wie lange die staatliche Datenschnüffelei schon mittels moderner Technik betrieben wird. Spätestens seit den Enthüllungen von Edward Snowden müsste der breiten Masse klar sein, wie hilflos wir der staatlichen Spionage ausgeliefert sind. Snowden war es auch, der seine Kommunikation mit Journalisten damit verschlüsselt hat, um dem langen Arm der Geheimdienste zu entkommen.

Ohne von jeglichen kommerziellen Interessen abhängig zu sein, ist GnuPG nach eigener Aussage eines der wenigen Werkzeuge, das echten Schutz bieten kann. Viele Einrichtungen bevorzugen GnuPG, da es einen offenen Standard verwendet und so sicherstellt, dass Daten auch in vielen Jahren noch entschlüsselt werden können.

Das aus 6 Personen bestehende Entwicklerteam von GnuPG finanziert sich momentan aus der Spendenkampagne von Anfang 2015, zuzüglich zu regelmäßigen Spenden der Linux Foundation, Facebooks, des Zahlungsdienstleisters Stripe sowie einigen bezahlten Entwicklungsaufträgen. Um eine langfristige Stabilität zu erreichen, konzentriert sich die gestern gestartete Kampagne auf das Werben für Daueraufträge, anstatt wie bisher auf Einmalspenden zu setzen. GnuPG-Erfinder und Projektleiter Werner Koch kommentiert die neue Kampagne mit den Worten:

„Wir möchten diese Arbeit auf Dauer fortsetzen. Jedoch wollen wir dabei in erster Linie der Allgemeinheit verpflichtet sein. Deshalb soll der Großteil unserer Finanzierung durch Einzelspender gedeckt werden und nicht von Konzernen."

Um die Rolle von GnuPG zum Schutz von Daten hervorzuheben, wurden 26 Organisationen aus aller Welt vor der Kamera zum Thema GnuPG befragt. Diese Berichte von Aktivistengruppen, Zeitungen, Anwaltskanzleien und Firmen werden in täglich wechselnden Videos auf der Kampagnenseite veröffentlicht.

Hintergrund: Seit dem Jahr 1997 ermöglicht das Kryptographiesystem GnuPG Privatleuten und Firmen ihre Daten und Kommunikation zu verschlüsseln und digital zu signieren. Hierzu wird der wohlbekannte und (nach eigenen Angaben) hoch kompatible OpenPGP Standard benutzt. Die Software basiert auf modernsten kryptographischen Verfahren (= Verschlüsselungs-Verfah-

ren) und verfügt über ein vielseitiges System zur Verwaltung der Schlüssel. GnuPG dient dabei als kryptographischer Unterbau für eine Vielzahl von Programmen, wie Thunderbird mit Enigmail, Gpg4win für Windows, und den GPGTools für Mac OS X. Die meisten Betriebssysteme nutzen GnuPG, um den Einbau von Hintertüren durch Systemupdates einen Riegel vorzuschieben. GnuPG is kostenlos erhältlich und wird immer mit vollständigem Quelltext geliefert; hierdurch ist eine Überprüfung der Software jederzeit möglich, genügend technisches Wissen vorausgesetzt. Hinter dem Projekt steht die Firma g10 Code GmbH, die in der Nähe von Düsseldorf beheimatet ist. Die bezahlten Entwickler sind dort fest angestellt. Die Firma investiert alle Gewinne wieder in die Entwicklung von GnuPG und dazugehöriger freier Software. Der Softwareentwickler Koch ist auch einer der Mitgründer der Free Software Foundation Europe (FSFE).

In einem Interview sagte mir Koch im Jahr 2007, dass es nach allen zur Verfügung stehenden Erkenntnissen nicht möglich sei, die Verschlüsselung dieser Software zu überwinden, sofern der vom Nutzer festgelegte Schlüssel lang genug ist. „ Der technische Fortschritt wird dies wahrscheinlich irgendwann ermöglichen aber wir können dies durch Vergrößern der Schlüssellänge einfach verhindern. Auch ist der Aufwand, der dann für einen Schlüssel getrieben werden müsste, immens hoch und deswegen niemals kosteneffektiv (Selbst Geheimdienste und Großkonzerne haben begrenzte Ressourcen).

Andererseits ist das Ziel ja nicht, einen Algorithmus, bzw. den Schlüssel zu knacken, sondern an die Informationen zu gelangen. Da gibt es nun wesentlich kostengünstigere Methoden. Will man heimlich an die Inhalte kommen, so verwanzt man einfach den Rechner des Senders oder Empfängers (Stichwort: Bundestrojaner) und protokolliert z. B. einfach den noch nicht verschlüsselten oder bereits wieder entschlüsselten Text. Muss es nicht heimlich geschehen, so wird in vielen Ländern und auch bei Wirtschaftsspionage zur altbewährten Rubber-Hose Kryptoanalyse (im Klartext: Folter) gegriffen. Jeder Gangsterfilm gibt hinreichend Einblick, wie man mit körperlicher Gewalt an Informationen kommen kann. Gegen Abhören auf der Leitung oder des Funkverkehrs ist die heutige Verschlüsselungstechnik schon sehr, sehr sicher – sofern es sich um ein anerkanntes Verfahren wie OpenPGP oder S/MIME handelt.“

P.S.: Ich habe Werner Koch geraten, für diese Spendenkampagne Banner zu erstellen, die wir nach Fertigstellung gerne kostenlos bei uns auf Tarnkappe.info einbinden werden. Wir würden uns freuen, wenn diesem Beispiel möglichst viele weitere Blogs und kommerzielle Webseiten folgen werden.

P.S.S.: Sehr gut gefallen hat mir auch das Koch-Interview von Kai Schlieter von der taz.

ALTERSGRENZE SOLL FALLEN: ÜBERWACHUNG VON KINDERN NOTWENDIG

Bayerns Innenminister Joachim Herrmann (CSU) sprach sich gegen eine Altersgrenze für Überwachungen aus, denn der Verfassungsschutz müsse im Terrorfall auch Minderjährige beobachten dürfen, sagte er den Zeitungen der Funke Mediengruppe.

Mit der Begründung, auch Minderjährige hätten schon Straftaten begangen, rät der CSU-Spitzenkandidat für die Bundestagswahl „dringend“ dazu, bundesweit die Altersgrenze für die Überwachung durch den Verfassungsschutz in ganz Deutschland fallen zu lassen. Insbesondere sollten Minderjährige im islamistischen Umfeld beobachten werden. „Minderjährige haben schon schwere Gewalttaten begangen. Da muss der Staat konsequent handeln“, ergänzte er.

Bereits seit einem Jahr dürfen terrorverdächtige Jugendliche von den deutschen Sicherheitsbehörden überwacht werden. Im vergangenen Jahr hatte der Bundestag ein entsprechendes Anti-Terror-Paket beschlossen, in dem die Altersgrenze für die Überwachung mutmaßlich islamistischer Jugendlicher auf 14 Jahre gesenkt wurde. Daten von Jugendlichen dürfen demnach gespeichert werden, wenn „tatsächliche Anhaltspunkte“ bestehen, dass der Minderjährige einen Anschlag plant, begeht oder begangen hat. Die Große Koalition reagierte damit auch auf den Fall einer mutmaßlichen 15-jährigen Islamistin, die im Februar 2016 einen Polizisten am Hauptbahnhof Hannover mit einem Messer schwer verletzt hatte.

Nun fordert Bayerns Innenminister Herrmann, die Altersgren-

ze von 14 Jahren generell bundesweit aufzuheben und verweist dabei auf eine entsprechende Regelung in Bayern. Bayern habe die Altersgrenze für die Überwachung bereits abgeschafft. Im Normalfall beobachte der bayerische Verfassungsschutz keine Kinder, sagte er. „Aber wenn es einen konkreten Hinweis gibt, dass im Umfeld einer islamistischen Gruppe ein Zwölfjähriger unterwegs ist, müssen wir den auch beobachten können".

REAL: GESICHTSANALYSE AN DER SUPERMARKT-KASSE

Die Real-Supermärkte erproben im Kassenbereich ihrer Geschäfte eine besondere Form der Videoüberwachung. Kunden werden dort gezielt bei der Betrachtung von Werbung durch ein Videosystem erfasst und analysiert. Datenschützer sind beunruhigt, berichtet Spiegel Online.

Die Supermarktkette Real setzt seit Herbst 2016 in 40 von 285 Filialen Videokameras ein. Kunden werden im Kassenbereich gescannt, um gezielte Werbung zu schalten. Die Kamera erfasst dabei alle Blickkontakte des Kunden mit dem Werbebildschirm. Ein Algorithmus analysiert dann, welches Geschlecht der Kunde hat und wie alt er ist und speichert diese Informationen ab. Die Kamera speichert zudem die Dauer der Betrachtung.

Diese Daten werden nun weitergegeben an die Echion AG mit Sitz in Augsburg. Bereits seit 20 Jahren unterbreitet das Unternehmen perfekte Angebote für große Werbekunden. Ihr Spezialgebiet liegt auf sogenannten Instore-Medienlösungen. Ziel ist es dabei, dass Kunden eines Geschäfts beim Einkauf möglichst angenehme Erfahrungen machen. So sorgt Echion beispielsweise dafür, dass an der Fleischtheke die richtige Musik läuft oder am Gemüsestand der passende Duft versprüht wird. Auch bei Real will die Augsburger Firma auf diese Weise die Qualität der ausgestrahlten Werbefilme zielgruppenorientiert anpassen.

Michael Kimmich, Gründer und Geschäftsführer von Echion behauptet gegenüber Wired: „Wir wurden schon öfter gefragt, ob wir Fotos der Kunden zeigen könnten, aber genau das geht eben nicht". Die Kameras dienten nur einer Live-Erfassung von anonymen Metadaten, Bilder verschicke sie keine. „Natürlich kann man Bilder theoretisch für Programmierzwecke im Labor auslesen, aber mal ehrlich: Der einzelne Kunde ist uns wirklich egal".

Das Echion-System beruhe auf drei Säulen

Zuerst soll die Reichweite der Werbung bestimmt und ausgewertet werden, so wäre im Supermarkt der „nachgewiesene Blick" vergleichbar mit dem Klick im Internet auf eine Onlineanzeige Zum Einsatz käme nun das Targeting: das gezielte Ausspielen der Werbung für die passende Zielgruppe (Musterbeispiel bei Echion: „AutoBild-Werbung für eine Gruppe mittelalter Männer, Kosmetikartikel für jungen Frauen.") Zuletzt werden Details festgelegt (Optimierung der Werbeart): Welche Art von Spot generiert die meiste Aufmerksamkeit? Wie lang muss er sein? Welche Inhalte und Farbgebung muss er haben? Auf die Frage, ob die Kunden mitbekommen, dass sie aufgenommen werden, meint ein Sprecher von Real: „Eine Information für unsere Kunden erfolgt über eine gut sichtbare Hinweisbeschilderung ‚Dieser Markt wird videoüberwacht'." Ferner ist Real der Meinung, es gebe keine datenschutzrechtlichen Probleme: „Die Bilder sind nur für jeweils 150 Millisekunden im Speicher, sie werden nicht weiter gespeichert". Die Erkennung der Personen erfolge komplett anonym, das System erkennt lediglich einen Mann von rund 45 Jahren. „Das System weiß jedoch zu keinem Zeitpunkt, wer diese Person ist. […] „Es werden lediglich Metadaten zum eigentlichen Bild übertragen. Das Recht am eigenen Bild wird daher nicht berührt"

Die Aufsichtsbehörden im Datenschutz sehen diesen Ablauf dagegen kritisch. Der Hamburger Datenschutzbeauftragte Johannes Caspar gibt gegenüber der „Lebensmittelzeitung" zu bedenken: „In dem Moment, in dem Bilder von Personen durch Kameras erhoben werden, ist das nicht mehr anonym." Folglich müssten die Händler ihre Kunden über die genaue Videoüberwachung informieren.

Mit dem Artikel: „Gesichtserkennung: was Real macht – und was nicht" hat Real bereits auf die Kritik reagiert. Ob Real die eingesetzte Software auch in den anderen 285 Filialen einsetzen will, ist bislang noch unbekannt. Das Programm namens Adpack sei jedenfalls datenschutzrechtlich geprüft und auf

die Videoüberwachung werde zudem hingewiesen. Mit der gleichen Software testet die Deutsche Post in einigen Filialen in München eine Gesichtserkennung zum gleichen Zweck: um passendere Werbung an den Schaltern auszuspielen.

FACEBOOK: WERDEN EMOTIONEN DER NUTZER FÜR ZIELGERICHTETE WERBUNG VERWENDET?

Laut einem gestern veröffentlichten Bericht der Tageszeitung The Australian, würde Facebook Jugendlichen genau dann zielgerichtete Werbeanzeigen präsentieren, wenn diese sich in einer, für Teenager typischen, labilen Situation befinden. In Australien soll Facebook Algorithmen genutzt haben, um diese Gefühlslagen zu erkennen und entsprechend werbewirksam umzusetzen.

Der Bericht, der auf einem 23-seitigen vertraulichen internen Facebook-Dokument (Confidential: Internal Only) basiert, behauptete, dass durch die Überwachung von Beiträgen, Posts, Bildern, Interaktionen und Internet-Aktivitäten in Echtzeit, Facebook-Algorithmen „Momente identifizieren können, wenn junge Menschen einen Vertrauensschub brauchen“. Werbetreibende könnten diese schwachen Momente gezielt für sich nutzen, heißt es laut Australien in dem Dokument.

Facebook sammelte in diesem Schriftstück psychologische Einblicke von 6.4 Millionen Schülern und Studenten in Australien und Neuseeland. Die Autoren des Berichts sind zwei australische Facebook-Manager. Screenshots, die das Dokument zeigen, veröffentlichte The Australian nicht.

Laut dem Dokument könne Facebook anhand des Nutzungsverhaltens genau feststellen, wann junge Leute sich „gestresst“, „besiegt“, „überwältigt“, „ängstlich“, „nervös“, „dumm“, „nutzlos“ fühlen oder einen „Misserfolg“ feststellen. Das Unternehmen ermöglicht es Werbetreibenden, Benutzer auf der Grundlage ihrer algorithmischen Auswertung, passgenau auf deren Wohlbefinden zu zielen.

Wenn also die eingesetzten Algorithmen zur Zielgruppen-Analyse anhand Auswertungen der aktuellen Nutzungsweise und der geposteten Inhalte zu der Ansicht kommen, dass ein Jugendlicher gerade mit starken Selbstwert-Problemen zu kämpfen hat, blenden sie genau in diesem Moment Werbung für bestimmte Status-Produkte ein, die das Versprechen einer Status-Aufwertung in sich tragen. In dem Dokument ist auch zu lesen, dass die jungen Nutzer zum Ende der Woche stärker ihre Gefühle reflektieren; das Wochenende werde vor allem dazu genutzt, Erfolge zu teilen.

Kritiker in Australien bewerten die Analyse als ethisch äußerst fragwürdig. Solche Gemütslagen auszunutzen, um Produkte zu verkaufen, führte natürlich zu einer regelrechten Empörung. Entsprechend zügig hat die kalifornische Konzernzentrale von Facebook auch ein Dementi veröffentlicht. Auf Nachfrage des Australian entschuldigte sich Facebook zunächst und kündigte eine Untersuchung an. In einem Statement heißt es, der Artikel des Australian sei irreführend: „Facebook bietet keine Tools an, um Nutzer basierend auf ihrem emotionalen Zustand anzusprechen“. Die Analyse sollte Vermarktern lediglich zeigen, wie sich die Nutzer auf Facebook „ausdrücken“. Die Informationen seien nie dazu gedacht gewesen, Werbeanzeigen zu personalisieren.

Allerdings wurde eingeräumt, dass entsprechende Analysen durchaus zu Forschungszwecken durchgeführt wurden. Hierbei habe man mit anonymisierten Daten gearbeitet. Das Ziel hierbei sei es gewesen, Werbetreibende zu einem besseren Verständnis der Nutzer zu verhelfen. Konkrete Beispiele, die daraus resultierten und auch in der Broschüre auftauchten, seien aber komplett fiktiv gewesen.

LAW

Themenübersicht

WHATSAPP: CSU FORDERT ZUGRIFF AUF KOMMUNIKATION

Die CSU will in einer neuen Bundesregierung den Zugriff der Polizei auf WhatsApp-Kommunikation gesetzlich ermöglichen, das gab Joachim Herrmann, Bayerns Innenminister, der „Rheinischen Post“ (Samstagausgabe) bekannt. Als Grund führt er den Terroranschlag in Ansbach im vergangenen Juli an, der über WhatsApp koordiniert wurde.

Mit den Worten: „Wir wissen, dass die Terroristen WhatsApp nutzen, deshalb müssen wir die gesetzliche Kontrollmöglichkeit nach der Wahl sofort angehen“, verlieh der CSU-Spitzenkandidat Joachim Herrmann gegenüber der in Düsseldorf erscheinenden „Rheinischen Post“ seiner Forderung Ausdruck. Indem er auf den Terroranschlag von Ansbach verwies, bei dem der Täter bis zum Schluss Anweisungen aus dem Nahen Osten über den Kommunikationsdienst erhalten habe, zeigte er seine Unzufriedenheit, dass bisher in dieser Hinsicht noch nichts geschehen wäre: „Seit einem Jahr mahnen wir das bei der SPD an, geschehen ist nichts“, kritisierte Herrmann.

Der Sprengstoffanschlag von Ansbach am 24. Juli 2016 war ein islamistischer Terroranschlag in der Altstadt von Ansbach. Dort zündete der 27-jährige syrische Flüchtling Mohammed Daleel vor einem Weinlokal eine Rucksackbombe. 15 Menschen wurden dabei verletzt, 4 davon schwer, keiner lebensgefährlich und er kam selbst dabei ums Leben. Der Attentäter lebte seit zwei Jahren in Deutschland und hatte Verbindungen zur Terrormiliz „Islamischer Staat“ (IS). Wie Ermittlungen später ergaben, stand der Täter zu diesem Zeitpunkt und im weiteren Verlauf in regem Chatkontakt mit einer Person aus dem Nahen Osten und hat bis zum Schluss Anweisungen über WhatsApp erhalten.

Der bayerische Innenminister Joachim Herrmann äußerte nach dem Auftauchen des Bekennervideos: „Es [sei] unzweifelhaft, dass es sich bei dem Anschlag um einen Terroranschlag mit islamistischem Hintergrund und islamistischer Überzeugung des Täters handelt“. Die Vermummung im Bekennervideo und dass Daleel weiteres Material zum Bombenbau besaß, sind – neben den Inhalten des Chats – Indizien, dass er weitere Anschläge verüben sollte. Die Behörden gehen davon aus, dass sein Tod ein Unfall durch vorzeitige Explosion des Sprengsatzes war.

Im Hinblick auf mögliche weitere geplante Terroranschläge mahnte Herrmann zugleich mehr Vereinbarungen nach dem Muster des EU-Türkei-Abkommens an, um Mittelmeerflüchtlinge zurück nach Afrika bringen zu können. „Es kann nicht sein, dass jeder Afrikaner, der mit einem Gummiboot in See sticht, automatisch in der Europäischen Union aufgenommen wird“, konstatiert der Innenminister.

Nachrichten, Fotos, Anrufe und Videos, die über WhatsApp verschickt werden, sind deutlich besser geschützt, seit der Messenger mit rund einer Milliarde Nutzern, eine sogenannte Ende-zu-Ende-Verschlüsselung für alle Betriebssysteme eingeführt hat. Das bedeutet, dass die Inhalte in der App nur für beteiligte Nutzer sichtbar sind. Die Codes können auch die Ermittlungsbehörden in der Regel nicht knacken. Das deutsche Recht macht einen Unterschied zwischen „Telekommunikationsdiensten“ und „Telemediendiensten“. Zu den Telekommunikationsdiensten gehören Anrufe, SMS und IP-Adressen: Hier müssen die Anbieter zehn Wochen lang speichern, wer mit wem wann telefoniert oder gesimst hat. Auf Anordnung eines Richters müssen diese Daten dann den Behörden übergeben werden. WhatsApp, Skype oder die sozialen Medien zählen dagegen zu den Telemediendiensten – hier müssen die Anbieter für die Behörden keine Verbindungsdaten auf Vorrat speichern. Die CSU fordert deshalb, dass Telekommunikationsdienste und Telemediendienste gleichgestellt werden.

UNTER KRITIK: GEPLANTES GESETZ ÜBER DAS URHEBERRECHT IN DER WISSENSGESELLSCHAFT (URHWISSG)

Am Montag (29.05.2017) findet eine öffentliche Anhörung zum Entwurf des Urheberrechts-Wissensgesellschafts-Gesetzes (UrhWissG) vor dem Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags statt. Bundesjustizminister Heiko Maas (SPD) will mit dem Gesetz die Nutzung digitaler Semesterapparate mit dem Urheberrechts-Wissensgesellschafts-Gesetz an Universitäten vereinfachen.

Jedoch wollen sowohl die Verlage als auch die Union verhindern, dass Dozierende lizenzfrei Teile von Büchern Studenten zur Verfügung stellen können. Aber auch der Börsenverein des Deutschen Buchhandels warnt, das Gesetz würde den freien Markt für Bildungs- und Wissenschaftsmedien außer Kraft setzen.

Das geplante Urheberrechts-Wissensgesellschafts-Gesetz sieht vor, dass künftig Lehrende den StudentInnen bis zu 15 Prozent eines Buches online zur Verfügung stellen dürfen – auch ohne Genehmigung von Verlagen und AutorInnen. Derzeit müssen RechteinhaberInnen gemäß Urheberrecht jeder Verwendung ihrer Werke ausdrücklich zustimmen, allerdings kann der Gesetzgeber auch Ausnahmefälle, wie eine Kopie für private Zwecke, zulassen – die sogenannten „Schranken" des Urheberrechts. Das regelt der Wissenschaftsparagraf 52a: Danach dürfen „kleine Teile" eines Werks für einen „abgegrenzten Kreis von Unterrichtsteilnehmern" online zugänglich gemacht werden. Nach Präzisierung des Bundesgerichtshofs im Jahre 2013 in einem Grundsatzurteil stand dann fest: Als „kleine Teile" können maximal 12 Prozent eines Werks lizenzfrei genutzt werden.

Justizminister Maas legte im Februar 2017 einen Referentenentwurf für das UrhWissG vor. Darin hieß es, es sollten bis zu 25 Prozent eines Buches ohne Lizenz in elektronische Semesterapparate eingestellt werden dürfen. Im Gegenzug müssen Unis – wie bisher – eine Vergütung an die Verwertungsgesellschaft (VG) Wort zahlen, die diese dann an die RechteinhaberInnen verteilt. Da die Hochschulen aber nur eine jährliche Pauschalgebühr zahlen und keine Informationen zu den genutzten Büchern weitergeben müssen, kann die VG WORT den eingehenden Betrag nur „mit der Gießkanne" unter sämtlichen bei ihr gemeldeten wissenschaftlichen Urhebern aufteilen. Für die Verfasser des Lehrbuchs ergibt sich bestenfalls eine Ausschüttung von wenigen Cent. Die Höhe der Vergütung regelt der Gesetzentwurf nicht, branchenüblich wären zur Zeit aber 0,8 Cent pro Seite und StudentIn. Der Verlag erhält für die Nutzung seines Lehrbuchs kein Geld, da seine angemessenen Lizenzangebote von der Hochschule nicht vorrangig berücksichtigt werden müssen und er an den Ausschüttungen der Verwertungsgesellschaft (VG) Wort aufgrund eines Urteils des Bundesgerichtshofs nicht beteiligt wird.

Der Referentenentwurf wurde im April 2017 von der Bundesregierung gebilligt, allerdings mit der Einschränkung, dass nur 15 Prozent eines Buches lizenzfrei genutzt werden können. Derzeit ist es so, wenn der Verlag ein angemessenes Angebot macht, muss die Uni einen Vertrag mit

dem Verlag schließen und kann das Werk dann infolge dessen nicht mehr lizenzfrei nutzen. Das grundlegend Neue ist nun, dass der lizenzfreie Basiszugang auch dann gelten soll, wenn der Verlag ein „angemessenes" Lizenzangebot macht.

Genau hierin sieht die CDU/CSU-Fraktion Ansatz für Kritik. So meint der CDU-Abgeordnete Stefan Heck: Maas' Vorschlag sei eine „Absage an die freie Marktwirtschaft" und könnte Verlagen und AutorInnen wirtschaftlich ruinieren. SPD-Abgeordneter Christian Flisek hält dagen: Wenn es weiter einen Vorrang der Lizenzangebote gebe, dann bleibe die Rechtsunsicherheit bestehen, „weil niemand weiß, was denn ein ‚angemessenes' Angebot ist". Auch Minister Maas verteidigt sein Konzept mit den Worten: „Diese lebensfremde Regelung schaffen wir ab."

In einer Stellungnahme gibt Verlegerin Barbara Budrich zu bedenken, dass die Verlage bei Abschaffung des bestehenden und funktionierenden Lizenzvorrangs enormen Schaden nehmen würden: „Für meinen Verlag heißt dies konkret, dass nicht nur die bestehenden Angebote weniger genutzt werden. Es bedeutet auch, dass wir weniger gedruckte Bücher und Zeitschriften verkaufen werden. Und es bedeutet, dass es für unsere beträchtlichen privatwirtschaftlichen Investitionen keine Sicherheit bei den Rahmenbedingungen gib." Auch hieße das, die Verlage müssen auf ein Subventionsgeschäft umbauen, da die Bücher nicht mehr im gleichen Umfang Erlöse erzielen würden.

Alexander Skipis, Hauptgeschäftsführer des Börsenvereins, gab in einer Pressemitteilung bekannt: „Wenn das Gesetz wie geplant verabschiedet wird, erhalten Verlage und Autoren keine nennenswerten Erlöse mehr für die Nutzung ihrer Werke in Forschung, Unterricht und Lehre. Das wäre ein kapitaler Fehler: Unsere Wissensgesellschaft braucht keine Lehrbücher zum Nulltarif, sondern einen freien Markt für hochwertige Medien. Nur Lizenzeinnahmen gewährleisten eine faire, angemessene Vergütung für Autoren und Verlage und damit private Investitionen in ein breitgefächertes und hochwertiges Angebot an wissenschaftlicher Literatur." Durch das Gesetz werde die

Qualität von Bildung und damit die Basis des Bildungs- und Wissenschaftsstandorts Deutschland Schaden nehmen, so Skipis: „Verlagen werden die Mittel fehlen, in neue Publikationen und attraktive Modelle für die Zugänglichmachung von Werken zu investieren. Autoren haben keinen Anreiz mehr, ihr Wissen für den Nachwuchs aufzubereiten und Lehrbücher zu verfassen. Gut funktionierende privatwirtschaftlich finanzierte Publikationsstrukturen werden zerstört, sodass am Ende der Staat die Veröffentlichung wissenschaftlicher Werke organisieren und mit Steuergeld bezahlen muss. Das kann niemand wollen."

Das Kernproblem des Gesetzentwurfs bestünde aus Sicht der Verlage in dem Wegfall der Lizenzierungsmöglichkeit: Dafür, dass Schüler, Studierende, Lehrende und Forschende große Teile von Lehrbüchern oder ganze Zeitschriftenartikel kostenlos vervielfältigen, herunterladen und ausdrucken können, sollen Bibliotheken und Bildungseinrichtungen keine Lizenzverträge mehr mit Verlagen abschließen müssen. Stattdessen würden Verlage und Autoren nur noch eine minimale Pauschalvergütung erhalten.

Für dieses Problem hätte der Börsenverein eine praktikable Lösung im Angebot: „Verlage unterbreiten Bibliotheken und Universitäten Lizenzangebote für die Nutzung ihrer Werke. Für einen bestimmten Preis pro Seite und Nutzer können Bildungseinrichtungen und Bibliotheken dann Auszüge aus Lehrbüchern, Zeitschriften und anderen Medien digital beziehen und Studierenden, Lehrenden und Forschenden zur Verfügung stellen."

Das Justizministerium hingegen glaubt nicht, dass durch das Gesetz die Existenz der Wissenschaftsverlage bedroht wäre. Sie sind davon überzeugt, eine einfache und rechtssichere Regelung werde vielmehr die Einnahmen, die über die VG Wort verteilt werden, deutlich erhöhen. Doch selbst wenn damit ein Rückgang verkaufter Bücher und Lizenzen kompensiert werden könnte, wird das die Verlage kaum besänftigen, denn nach aktueller BGH-Rechtsprechung stehen die VG-Wort-Einnahmen ausschließlich den AutorInnen der Bücher zu. Diesen steht es jedoch frei, etwas an ihre Verlage abzugeben.

Das Gesetz soll von der Bundesregierung noch in dieser Wahlperiode beschlossen werden, im März 2018 soll das Gesetz dann in Kraft treten. Nächster wichtiger Termin ist die öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz am 29.05.2017.

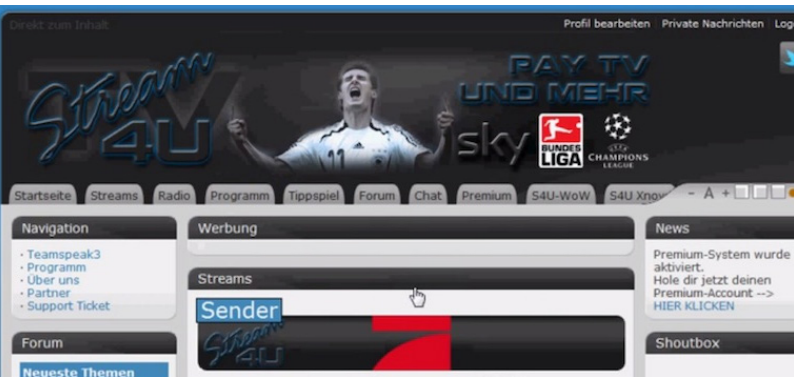
GROSSBRITANNIEN: MEHRJÄHRIGE GEFÄNGNISSTRAFEN WEGEN PRIVATKOPIERTER DVDS

In Großbritannien wurde am 16.05.2017 eine Gruppe von Raubkopierern wegen dem Verkauf raubkopierter DVDs, Verwendung gefälschter Identitäten und Geldwäsche zu mehrjährigen Haftstrafen verurteilt, berichtet die Antipiraterie-Organisation FACT (Federation Against Copyright Theft).

Selbst im Streaming-Zeitalter wird offenbar noch Geld mit dem Verkauf von DVDs verdient. So führten 4 Männer in Großbritannien ein einträgliches Geschäft mit raubkopierten Filmen. Über einen Zeitraum von zweieinhalb Jahren verkauften sie über 31.000 DVDs im Werte von mehr als 500.000 Pfund (etwa 580.000 Euro).

Entsprechende Hausdurchsuchungen führten zur Beschlagnahme von insgesamt ca. 11.000 Pfund an Bargeld, Geschenkkarten im Wert von 1.250 Pfund, 600 gefälschten DVD-Titeln, mehreren Hundert leerer DVDs, einem Laserdrucker, Computer, Laptops, Tabletts und Mobiltelefonen. Drei von den Tätern bekamen Haftstrafen nicht unter 40 Monaten.

Kieron Sharp, CEO von FACT gab bekannt: „Das war kein Ein-Mann-Betrieb, dies war gut organisierte Kriminalität. Die raubkopierten DVDs standen den echten Produkten in nichts nach. Auch die Kunden hatten bei diesem Geschäft den Eindruck, sie hätten echte Produkte gekauft und glaubten nicht, dass sie Raubkopien erworben hätten.[…] Viele Leute denken, dass Piraterie ein relativ harmloses Verbrechen sei ohne Opfer, aber kriminelle Operationen wie diese, haben verheerende Auswirkungen auf die kreative Branche und die Menschen, die dort tätig sind."



STREAM4U.TV: 18.000 EURO SCHADENERSATZ FÜR BETREIBER UND DIENSTLEISTER

Das Landgericht Hamburg (Az.: 310 O 221/14) verurteilte die Betreiber der Live-Streaming-Plattform Stream4u.tv und dessen technischen Dienstleister zu jeweils 18.000 Euro Schadenersatz. Der Dienstleister besorgte die Hardware zur Entschlüsselung und Verbreitung des illegalen Sky-Signals.

Wie der Pay-TV-Sender Sky heute in seiner Pressemitteilung mitteilt, sei es somit erstmals zu einer zivilrechtlichen Verurteilung (Schadensersatz) wegen illegalen Sky-Streamings im Rahmen einer Gesamtschuld gekommen. Gesamtschuld bedeutet: Sowohl der Betreiber als auch der technische Dienstleister müssen beide ihren Schadenersatz in gleicher Höhe leisten. Dies wurde Tarnkappe.info vorhin von Sky-Sprecher Stefan Bortenschlager telefonisch bestätigt. Das LG Hamburg begründete das Urteil damit, dem Zulieferer der Hardware zur Entschlüsselung des Sky-Signals musste klar sein, dass ihre Hardware zu missbräuchlichen Zwecken eingesetzt wurde.

Abschreckung an erster Stelle?

Für Sky steht offenbar die abschreckende Wirkung im Vordergrund, denn mit diesem Urteil setzt sich jeder technische Dienstleister, der über die illegale Nutzung seiner Dienste von Sky informiert wird, einem erheblichen Haftungsrisiko aus, wenn er nicht unverzüglich reagiert und seine Leistung einstellt. Thomas Stahn, Director Anti-Piracy & Technology bei Sky Deutschland kommentiert das Urteil: „Die Verurteilung ist eine Warnung für alle Beteiligten an der illegalen Verbreitung von Sky Inhalten. Im Gegensatz zum Strafrecht haftet jeder Gehilfe auch alleine für den vollen Schaden des Verletzten – unabhängig davon, ob er von dem illegalen Geschäft profitiert hat oder nicht."

Verhandlung teilweise in Abwesenheit der Gegenseite

Laut telefonischer Auskunft des Sky-Sprechers gegenüber Tarnkappe.info wurden mehrere Termine angesetzt, bei denen teilweise entweder die Vertreter des Ex-Betreibers von Strea-m4u.tv oder des technischen Dienstleisters nicht vor Gericht erschienen sind. Wir warten noch auf eine E-Mail von Herrn Bortenschlager, die diesbezüglich mehr Details enthalten soll. Update: Es handelt sich um eine Stufenklage, bei der der Dienstleister vor Gericht erschienen ist, der Betreiber nicht.

Hintergrund: Deutsche Fußball Liga (DFL) und Sky Deutschland hatten im November 2016 gemeinsam erklärt, dass sie sich von der illegalen Konkurrenz im Web bedroht sehen. Hauseigene Sky-Ermittler konnten auf Basis ihrer Recherchen die Hauptverdächtigen eindeutig identifizieren. Daraufhin fanden Ende 2013 Durchsuchungen und Beschlagnahmungen im hessischen Pfungstadt und in Sulzbach (Saarland) statt. Im November 2016 wurden in der Folge zwei Angeklagte strafrechtlich verurteilt. Einer der beiden Personen wurde zu einer Haftstrafe auf Bewährung verurteilt.

DATENSCHUTZBEHÖRDE CNIL: FACEBOOK BEKOMMT HÖCHSTSTRAFE WEGEN USER-TRACKING

Die Pariser Datenschutzbehörde CNIL hat gegen Facebook wegen unrechtmäßigen Webtrackings und illegaler Profilbildung eine Strafe in Höhe von 150.000 Euro verhängt. Der Vorwurf gegen das US-Unternehmen lautet, dass dem Nutzer keine Möglichlkeit eingeräumt wird, der „massiven Kombination" ihrer Daten zu Werbezwecken zu widersprechen.

Der Umgang Facebooks mit Userdaten ist in vielen Fällen nicht mit europäischem Recht zu vereinbaren. Den Umstand hat nun auch die Französische Datenschutzbehörde CNIL dem Unternehmen vorgeworfen. Als abzustellende Mängel wurden von der Datenschutzbehörde aufgeführt:

- dass Facebook auch Daten von unbeteiligten Bürgern sammelt und nutzt, die keine User des sozialen Netzwerks sind,
- dass Facebook seine aktiven Nutzer nicht ausreichend

über die Verwendung persönlicher Angaben wie ihrer religiösen, politischen und sexuellen Orientierung informiert,
- in den Nutzereinstellungen fehlen Widerspruchsmöglichkeiten gegen die Verwendung der dort hinterlegten persönlichen Daten.

Dabei wurde nicht nur das alleinige Sammeln von Daten kritisiert, sondern in erster Linie deren umfangreiche Kombination, um immer genauere Zielgruppenangaben für Werbeschaltungen zu erhalten. Die Anwender hätten hier letztlich weder eine Übersicht oder gar Kontrolle darüber, welche Informationen über sie gespeichert werden, noch könnten sie sich auch nur im Ansatz gegen das Tracking wehren.

Ebenso ist die Tatsache, dass das Sammeln von Daten keineswegs nur auf Facebooknutzer beschränkt bleibt, die sich ja letztlich bewusst bei dem Social Network angemeldet und damit die Arbeitsweise des Unternehmens mehr oder weniger akzeptiert haben, kritikwürdig. So werden zudem völlig unbeteiligte Nutzer in die umfangreiche Datensammlung gleich mit integriert, nämlich immer dann, wenn auf externen Seiten Like-Buttons direkt eingebunden sind und Facebook somit tracken kann, wie sich auch unangemeldete User durchs Web bewegen.

CNIL hatte Facebook Anfang 2016 öffentlich aufgefordert, die in dem Land geltende Datenschutzbestimmungen umzusetzen und Details zu gesammelten Daten und ihrer Verknüpfung offenzulegen. Das Unternehmen habe aber keine zufriedenstellenden Antworten gegeben. Die Strafe resultiert hauptsächlich daraus, dass das soziale Netzwerk nach ersten Ergebnissen der Untersuchung keine Anstrengungen unternahm, die bemängelten Probleme abzustellen. Was nun für Facebook bei einem weltweiten Umsatz von mehr als 25 Milliarden Dollar und 10 Milliarden Dollar Gewinn im Jahr 2016 eher nicht als empfindliche Sanktion wahrgenommen wird, bedeutet jedoch für CNIL, ihre Möglichkeiten hier bereits bis zum Maximum ausgeschöpft zu haben. 150.000 Euro ist die höchstmögliche Strafe, die die Behörde derzeit überhaupt verhängen kann.

Das Unternehmen hat nun vier Monate Zeit, beim Staatsrat, dem obersten französischen Verwaltungsgericht, Widerspruch gegen den Beschluss einzulegen. Parallel laufen auch in verschiedenen anderen europäischen Ländern entsprechende Verfahren.

Gleichfalls aktuell wurde bekannt, dass die EU-Kommission in ihrem Verfahren gegen Facebook zu dem Schluss kam, dass der Konzern bei der Übernahme von WhatsApp 2014 falsche Angaben gemacht hat. Die damalige Behauptung, es sei nicht möglich, einen automatischen Abgleich zwischen den Benutzerkonten und den gespeicherten Nutzerdaten beider Unternehmen einzurichten, habe sich zwei Jahre später als falsch erwiesen.

Die EU-Kartellkommissarin Margrethe Vestager teilte mit, dass ihre Behörde für deren Arbeit bei Fusionen akkurate Angaben von Firmen benötigt: „Der heutige Beschluss ist eine deutliche Botschaft an Unternehmen, dass sie die EU-Fusionskontrollvorschriften einhalten müssen, darunter auch die Verpflichtung, sachlich richtige Angaben zu machen. Aus diesem Grunde sieht er eine angemessene und abschreckende Geldbuße gegen Facebook vor."

Daher wurde Facebook für seine falschen Angaben bezüglich der späteren Datenweitergabe nun hart bestraft. Facebook spricht zwar von einem unbeabsichtigten Fehler, muss aber 110 Millionen Euro Strafe zahlen, berichtet The Guardian. Die Höhe der Zahlung soll eine Signalwirkung für künftige kartellrechtlich relevante Firmenfusionen haben. Die 2014 erteilte Genehmigung zur Fusion der beiden US-Internetunternehmen wird dennoch beibehalten. Facebook scheint die Strafe auch zu akzeptieren: „Die heutige Ankündigung bringt die Sache zum Abschluss", lässt sich ein Sprecher zitieren.

JULIAN ASSANGE: SCHWEDEN STELLT VERFAHREN EIN

Die schwedische Staatsanwaltschaft hat das Verfahren gegen den WikiLeaks-Chefredakteur Julian Assange eingestellt. Die Einstellung erfolgte aus formalen Gründen. Entwarnung für Assange bedeuten diese Nachrichten allerdings nicht – vorerst wird er wohl trotzdem weiter in der ecuadorianischen Botschaft in London ausharren müssen.

Staatsanwaltschaft stellt Verfahren ein

Die schwedische Staatsanwaltschaft hat das Verfahren ge-

gen Julian Assange eingestellt. Dem 45-jährigen Transparenz-Aktivisten wird vorgeworfen, mit einer Unterstützerin im Jahr 2010 nicht einvernehmliche Sexualpraktiken durchgeführt zu haben. Assange bestreitet die Vorwürfe und bezeichnete das Verfahren immer wieder als politisch motiviert.

Nun hat die schwedische Staatsanwaltschaft – nach zähem Ringen um eine Vernehmung Assanges – das Verfahren eingestellt. Grund dafür sei allerdings keine erwiesene Unschuld Assanges, sondern lediglich die mangelnde Aussicht, das Verfahren zu einem erfolgreichen Ende zu führen, betonte Staatsanwältin Marianne Ny. Nach Ansicht der Staatsanwaltschaft seien alle Möglichkeiten, das Verfahren erfolgreich zu beenden, ausgeschöpft. Deswegen sei es „nicht länger angemessen, den Haftbefehl gegen Julian Assange in dessen Abwesenheit aufrechtzuerhalten und an dem europaweiten Haftbefehl festzuhalten," so Ny. Ob Assange schuldig sei oder nicht, sei nach wie vor ungeklärt.

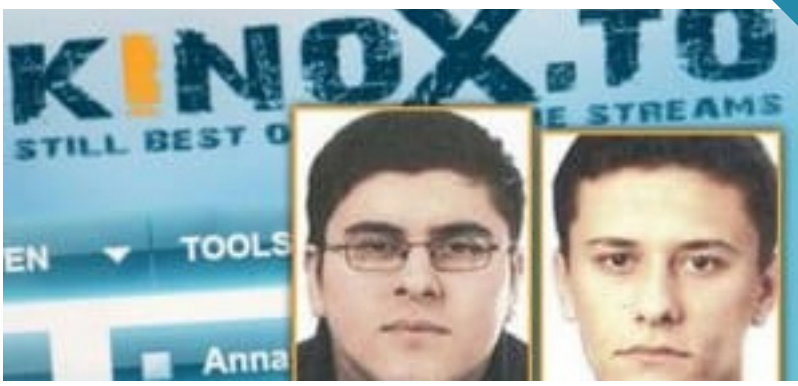
Keine Entwarnung für Julian Assange

Für Julian Assange ist es allerdings noch zu früh, um aufzuatmen – und um die Botschaft, in der er seit 2012 ausharrt, zu verlassen. Die britischen Behörden kündigten nämlich an, ihn trotz der Entscheidung Schwedens nach wie vor verhaften zu wollen. Zur Begründung nannten sie einen versäumten Gerichtstermin.

Eine Verhaftung durch die britischen Behörden wird Assange nicht riskieren wollen. Er befürchtet nämlich eine Auslieferung an die USA – sein Hauptgrund dafür, sich dem Verfahren in Schweden nicht zu stellen. Ob die USA einen Auslieferungsantrag an England gestellt haben, ist unbekannt. Klar ist allerdings, dass in den USA seit der Wahl Donald Trumps zum Präsidenten verstärkt über eine Anklage gegen WikiLeaks diskutiert wird. Unter anderem wird derzeit geprüft, ob WikiLeaks sich der Spionage schuldig gemacht hat.

KINOX.TO WEITER ONLINE: POLIZEI MACHTLOS

Die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU) schätzt den Schaden, der der Filmindustrie durch illegales Streaming jährlich allein in Deutschland entsteht, auf ca. 300 bis 400 Millionen Euro. Auch auf dem Portal kinox.to sind solche Angebote zu finden. Als Nutzer bekommt man dort illegal sowohl TV- als auch Kinoproduktionen online zu sehen, wobei das Urheberrecht verletzt wird. Natürlich ist diese Seite ein Dorn im Auge der Filmindustrie, jedoch alle Versuche von Polizei und Staatsanwaltschaft, das Portal vom Netz zu bekommen, scheiterten bisher.



Trotz intensiver Bemühungen der IT-Spezialisten wäre es nicht gelungen, die Zugangscodes und Passwörter zur Seite „Kinox.to" zu ermitteln. Oberstaatsanwalt Wolfgang Klein, Pressesprecher der Generalstaatsanwaltschaft Dresden, erklärte gegenüber sputniknews: „Wir haben bislang die Zugangscodes nicht knacken können". Als wenig hilfreich erwiesen sich dabei auch die Aussagen der bereits gefassten und verurteilten Mitbetreiber in diesem Fall.

Laut GVU machte der 29-jährige Avit O. weder zu seinen mutmaßlichen Komplizen noch zu den ausstehenden Passwörtern im Prozess irgendwelche Angaben. Stattdessen sagte er aus, eine namentlich nicht benannte Person soll die Kontrolle über die Seite übernommen haben. O. habe mit dieser Person irgendwann gebrochen, erwähnte aber während der Verhandlungen auch hier keine weiteren Details. Ähnlich hat auch Dirk B. reagiert, als er als Zeuge vorgeladen wurde, er wollte gegen den Anonymen genauso wenig aussagen. Es liegt die Vermutung nahe, dass beide Personen von dieser Person bedroht werden könnten.

KinoX.to: ohne die Selimis keine Passwörter

Im Rahmen einer Verhandlung gab der Verteidiger, Prof. Wilhelm, zu bedenken, dass Staatsanwaltschaft und Polizei in Fällen dieser Art oft „keine Ahnung" hätten, worum es technisch gehe. Die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU) verhalte sich wie „ein Trojaner in der Justiz" und beeinflusse die Arbeit der Staatsanwaltschaft. In einer Pressemitteilung der GVU heißt es, dies sei ein „Erheiterung auslösender Vorwurf" gewesen. Der Industrieverband feiert die Verurteilung als Erfolg, da Streamingseiten schwer beizukommen wäre.

Fest steht, Avit O. soll Kinox.to nicht allein betrieben haben. Noch immer sucht die Generalstaatsanwaltschaft in Dresden nach zwei Brüdern, Kastriot und Kreshnik Selimi, aus Lübeck. Laut Landeskriminalamt Sachsen stehen die Brüder im dringenden Tatverdacht, als Gründer und Rädelsführer einer kri-

minellen Vereinigung im Zusammenhang mit dem Betreiben des Raubkopienportals kinox.to, spätestens seit dem 21. Juni 2011 und ihrer Filehoster freakshare.com und bitshare.com bereits seit spätestens 2009, Straftaten, wie Räuberische Erpressung, Nötigung, Brandstiftung, Urheberrechtsverletzung und Steuerhinterziehung, begangen zu haben. Bisher fehle zu dem 26-Jährigen und dem 22-Jährigen jede Spur. Seit 2014 werden die beiden als ehemalige Köpfe des Betreibernetzwerks von „Kinox.to“ durch einen internationalen Haftbefehl gesucht. Sowohl deutsche Behörden als auch Europol fahnden nach den Brüdern. Oberstaatsanwalt Wolfgang Klein teilte mit, dass es aktuell noch keinerlei Spur von den beiden Verdächtigen gebe, aber die Staatsanwaltschaft ermittle in alle Richtungen: „Wir sind nach wie vor auf der Suche nach den beiden Hauptbeschuldigten, die Fahndung läuft weltweit. Wir haben bislang keine heiße Spur. Aber als Strafverfolger muss man einen langen Atem haben. Wir sind zuversichtlich, dass wir die zwei Personen irgendwann festnehmen können.“

Brute-Force-Angriff fällt aus

Nun gab Pressesprecher Klein gegenüber sputniknews Details zu den aktuellen Ermittlungen in diesem Fall bekannt. Demnach könne die Staatsanwaltschaft die fehlenden Passwörter zum Abschalten der Seite Kinox.to nur über die beiden zur Fahndung ausgeschriebenen, flüchtigen Haupttatverdächtigen, die Brüder Kastriot und Kreshnik Selimi, finden: „Die Zugangscodes und Passwörter liegen offensichtlich ausschließlich bei den beiden flüchtigen Hauptbeschuldigten. Laut unseren Ermittlungen verfügen keine anderen Personen über diese Codes. Aus IT-Sicht ist zu sagen: Passwörter und Codes für die Streaming-Seite sind mit legalen Mitteln nicht zu knacken. IT-Experten, mit denen die Generalstaatsanwaltschaft zusammenarbeitet, sind natürlich beschränkt auf legale Mittel. Wir kommen daher nicht weiter, ohne dass wir die Codes von den beiden Beschuldigten erlangen.“ Zudem sollen die Selimi-Brüder auch andere, gleichfalls illegale Streaming-Plattformen mitbetreiben, wie „movie4k.to“ oder „shared.sx“: „Wir gehen nach derzeitigem Erkenntnisstand davon aus, dass die beiden Selimi-Brüder auch für diese illegalen Portale verantwortlich sind. Es wird auch hier ermittelt.“ Käme die Justiz an das Brüderpaar heran, hätte sie Zugriff auf die Passwörter, um auch diese Internet-Portale offline zu nehmen. „Das Streaming ist und bleibt nicht zulässig. Wir als Generalstaatsanwaltschaft Dresden haben uns auf den Kampf gegen die Hinterleute dieser Streaming-Portale fokussiert. Wir sind mit unseren Bemühungen dran, die Drahtzieher aus dem Verkehr zu ziehen.“, so gab Klein bekannt und hofft nun auf baldige Fahndungserfolge.

IN PLANUNG: EINSATZ VON STAATSTROJANERN AUCH BEI „ALLTAGSKRIMINALITÄT“

Auf Grundlage einer von netzpolitik.org veröffentlichten „Formulierungshilfe“ des Bundesjustizministeriums, will die Große Koalition die rechtlichen Voraussetzungen für einen umfangreichen Einsatz von Überwachungsprogrammen auf Endgeräten von Verdächtigen schaffen. Die Anwendung solcher Programme soll dabei auf insgesamt 38 Straftatbestände ausgeweitet werden.

Die gesetzliche Legitimation, um auch bei Alltagskriminalität künftig Rechner und Smartphones infiltrieren zu dürfen, soll über einen Änderungsantrag der bereits seit Jahren laufenden Reform des Strafprozessrechts geschaffen – und noch vor der Bundestagswahl beschlossen werden. Die Strafrechtsreform soll ergänzt werden, um mit Hilfe von gehackten Smartphones oder Computern eine verschlüsselte Kommunikation überwachen (Quellen-TKÜ) oder Dateien auslesen zu können (Online-Durchsuchung).

Der Einsatz von Staatstrojanern kommt in 2 verschiedenen Bereichen zur Anwendung, einmal bei der Online-Durchsuchung. Hier dringen die Ermittler komplett in die Systeme zur Durchsuchung ein. Diese Form der Beschaffung von Beweismaterial ist bisher laut Bundesverfassungsgericht nur in Ausnahmefällen bei schwersten Delikten genehmigungsfähig. Dazu zählen Gefährdungen von Menschenleben, ihrer Gesundheit und elementarsten Lebensgrundlagen.

Zum anderen gibt es die so genannte Quellen-Telekommunikaionsüberwachung (Quellen-TKÜ). Hier wird die Kommunikation zwischen den Beteiligten überwacht und aufgezeichnet. Diese ergibt sich aus technischen Gründen: Die Kommunikation könnte nach dem geltenden Recht zwar im öffentlichen Telekommunikationsnetz ausgeleitet werden, würde den Ermittlungsbehörden dann aber nur in verschlüsselter Form vorliegen. Die Entschlüsselung jedoch ist entweder extrem zeitaufwändig oder sogar gänzlich ausgeschlossen. Auch dieser Einsatz war auf bestimmte schwere Taten beschränkt, und kam nur dann zur Anwendung, wenn: „ein konkreter Tatverdacht und eine hinreichend sichere Tatsachenbasis auf die Annahme einer Straftat von erheblicher Bedeutung“ schließen ließ, heißt es im Urteil des Ersten Senats des BVerfG vom 12. März 2003, 1 BvR 330/96, Rn. 77.

Der Einsatzbereich von Staatstrojanern würde sich nach dem neuesten Gesetzentwurf, der von der CDU/SPD-Regierung in den Bundestag eingebracht wird, jedoch stark erweitern, wie Netzpolitik.org berichtet. Das ermöglicht der Polizei nun bald, Staatstrojaner zusätzlich bei strafrechtlich relevanten Delikten anwenden zu können. Künftig würden Ermittlungsbehörden also nicht nur in solchen Fällen, wie Gefahrenabwehr von internationalem Terrorismus, sondern bereits auch bei „gewöhnlicher“ Kriminalität, wie Drogen- oder Betrugsdelikten, Staatstrojaner zum Einsatz bringen dürfen.

Demnach soll die Quellen-TKÜ zukünftig bei allen 38 Straftatbeständen eingesetzt werden können, bei denen Ermittlungsbehörden bisher eine normale Telekommunikationsüberwachung durchführen konnten. Allein im Jahr 2015 wurde die „normale Telekommunikationsüberwachung“, bei der Computer oder Smartphones nicht „gehackt“, sondern man nur den Datenverkehr oder Telefongespräche angezapfte, immerhin schon 32.668 mal angeordnet – davon in knapp der Hälfte der Fälle wegen Drogendelikten. Die Vermutung liegt nahe, dass nach einem Inkrafttreten des neuen Gesetzes, vor allem die Rechner und Smartphones von Dealern mit Staatstrojanern verwanzt werden.

Deutlich ausgeweitet werden soll aber auch die Online-Durchsuchung. So soll sie für 27 Straftatbestände angewandt werden. Das geht in einigen Fällen klar über die „Gefährdungen von Menschenleben, ihrer Gesundheit und elementarsten Lebensgrundlagen“ hinaus, die das Bundesverfassungsgericht als Grenze definierte.

Sowohl Experten als auch die Opposition sehen das Vorhaben sehr kritisch: „Dieser Gesetzesvorschlag ist eine krasse Provokation in Richtung Karlsruhe“, meint Ulf Buermeyer, Richter am Landgericht Berlin und Vorsitzender der Gesellschaft für Freiheitsrechte gegenüber netzpolitik.org.

Dadurch, dass auf einen eigenen Gesetzesentwurf verzichtet wird und die Quellen-Telekommunikationsüberwachung mit in die Reform des Strafprozessrechts aufgenommen wird, die aktuell kurz vor ihrer Verabschiedung im Bundestag steht, verkürzt sich das parlamentarische Verfahren. Unter anderem

entfällt dadurch die erste Lesung des Entwurfs im Bundestag. Aber auch, um eine große öffentliche Debatte zu vermeiden, wird die neue Regelung einfach mittels Verfahrenstrick in einem bereits existierenden Gesetzesprozesses versteckt.

Tobias Singelnstein, Inhaber des Lehrstuhls für Kriminologie an der Juristischen Fakultät der Ruhr-Universität Bochum, kommentiert dieses Prozedere gegenüber netzpolitik.org: „Es ist ein starkes Stück, dass diese extrem umstrittene Maßnahme nun plötzlich mittels eines Änderungsantrages zu einem laufenden Gesetzgebungsverfahren binnen Wochen durchgepaukt werden soll. Ein solcher Schweinsgalopp durch die Hintertür hat mit demokratischer Debattenkultur nichts zu tun."

Linus Neumann, Experte für IT-Sicherheit und einer der Sprecher des Chaos Computer Club, kommentiert gegenüber netzpolitik.org: „Aus der Asche der Wannacry-Attacken steigt noch Rauch auf. Die Schwachstelle, die die Angreifer zur Infektion ausnutzten, stammt aus dem Giftschrank der NSA. Über fünf Jahre hat die NSA diese Lücke geheim gehalten und so die ganze Welt dem Risiko ausgesetzt. Diese absolute Verantwortungslosigkeit scheint die große Koalition zu beeindrucken. Sie will nun den gleichen Weg gehen, statt endlich für die innere Sicherheit, und damit auch die unserer IT-Systeme, einzustehen."

Auch Harald Petzold von der Linksfraktion lehnt das „Hacking-Programm" ab. Habe der Staat die Tür in IT-Systeme geöffnet, könnten „auch ganz andere Akteure hindurchgehen".

DARKMON: NAMHAFTER E-BOOK-PIRAT ERMITTLERN INS NETZ GEGANGEN

Der Firma Counterfights Anti-Piracy in Jena ist es gelungen, im Kampf gegen E-Book-Piraten und deren illegales Einstellen der Werke auf einschlägigen Buchportalen, erneut einen Erfolg zu verbuchen. Dieses Mal ist ihnen der namhafte E-Book-Pirat – Darkmon – ins Netz gegangen. So wurden bereits vor einigen Monaten polizeiliche Maßnahmen gegen den in Karlsruhe wohnhaften Uploader Darkmon umgesetzt, bestätigte die Staatsanwaltschaft Karlsruhe. Für die erfolgreichen Vorermittlungen sorgte das einschlägig bekannte Unternehmen CounterFights Anti-Piracy. Diese führten schließlich zur Ergreifung des Verdächtigten. In Vertretung von 35 betroffenen Verlagen und Autoren, stellte CounterFights Anti-Piracy daraufhin Strafanzeige. Der Beschuldigte mittleren Alters hätte laut Pressemitteilung die rechtswidrigen Handlungen bereits eingeräumt.

Der unter dem Pseudonym „Darkmon" agierende E-Bookpirat war in der E-Bookszene kein unbeschriebenes Blatt. Über Jahre hinweg bot er auf den einschlägigen E-Bookportalen, wie mygully.com., in ca. 12.000 gestarteten Forumeinträgen u.a. auch aktuelle Neuerscheinungen illegaler E-Bookkopien an. Darin stellte er Downloadlinks zu belletristischen E-Book Titeln zur Verfügung über Sharehoster, wie z.B. Uploaded.net.

Nach vorsichtiger Schätzung der Anti-Piracyfirma hätte Darkmon mittels der Downloadvergütungen und Provisionen über die Sharehoster mehrere Hunderttausende Euro umgesetzt. Laut Einzeluntersuchungen von CounterFights Anti-Piracy soll der legale Umsatz der Rechteinhaber an genau den Tagen der illegalen Einstellung der E-Books von Darkmon in Foren um etwa 30 Prozent gegenüber den vorigen Tagen zurückgegangen sein. Der Umsatzverlust lag teilweise über 50 Prozent, wenn „Darkmon" die E-Book Kopien nach einer von CounterFights Anti-Piracy veranlassten Löschung der Download-Links erneut zur Verfügung stellte.

„Bei Darkmon handelte es sich um einen Haupttäter der E-Book Piraterie, welcher jeden Tag eine höhere Anzahl von E-Books wiederholt illegal zur Verfügung stellte und nach unserer Einschätzung daran kräftig verdiente", so kommentiert Andreas Kaspar, Inhaber des in Jena ansässigen Ermittlungsunternehmens den Vorfall. „Nicht jeder Täter in diesen Piraterieportalen verbreitet die illegalen E-Book Kopien vorwiegend, um damit Geld zu erwirtschaften. Dennoch entstehen den Autoren und

Verlagen erhebliche Umsatzverluste. Es sollte jedem Vollzeit- und jedem Freitzeituploader in diesen Piraterieportalen inzwischen klar sein, dass er das Ziel von Ermittlungen sein kann."

Hintergrund: Der verdeckte Ermittler der Firma Counterfights Anti-Piracy, Andreas Kaspar, hatte bereits im Jahr 2014 in dem Fall „Spiegelbest" einen Fahndungserfolg zu verzeichnen. Auf seine Tätigkeit ist es zurückzuführen, dass am 09.12.2014 deutschlandweit eine E-Book-Razzia durchgeführt wurde. Zu diesem Zweck infiltrierte er unter dem Decknamen Rivalon das Buchportal ebookspender.me, indem er sich mit seinen Programmierfähigkeiten als technischer Support anpries und so den Behörden den Zugang zu den Servern ermöglichte, wie der Spiegel berichtete.

Auch bei Lars klingelte es an diesem Tag an der Wohnungstür – und das war allein der Tatsache geschuldet, weil er Spiegelbest auf der Tarnkappe bei sich schreiben ließ. Allerdings den namhaftesten Buchpiraten – Spiegelbest – hat er bis heute nicht erwischt. Dieser wird wohl als bestgetarntes Phantom in die Chronik der Geschichte der E-Bookpiraterie eingehen.

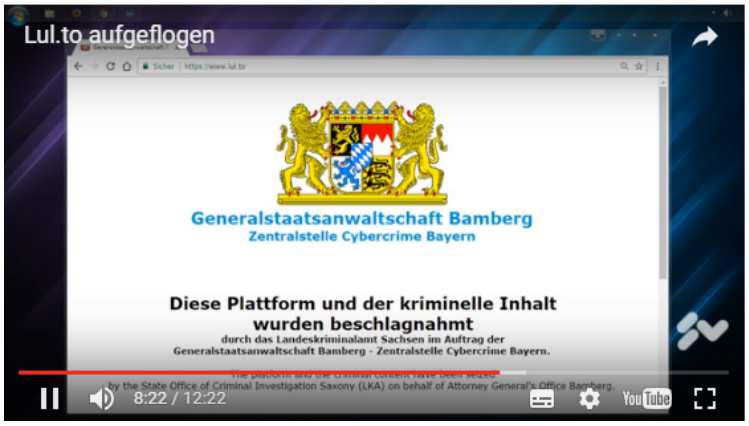
Wie Kaspar dieses Mal bei seinen Ermittlungen vorging, ist noch unbekannt. Fest steht nur, Darkmon hat einen Fehler gemacht, der ihm schließlich zum Verhängnis wurde. Viele Varianten wären da möglich, von daher gibt es allerlei Raum für Spekulationen. Ob er vielleicht einmal sein VPN vergessen hat einzuschalten oder es ausgefallen ist und er so nur für wenige Augenblicke bei einem E-Mailkonto eingeloggt war, dass ihm zugeordnet werden konnte, oder er hat, wie auch Spiegelbest, der falschen Person zu viel Vertrauen entgegengebracht. Denkbar wäre weiterhin ein Honeypot. Man kann ebenso nicht gänzlich ausschließen, dass sein VPN-Anbieter ihn verraten hat. Genaueres wissen wir zu diesem Zeitpunkt noch nicht, hören uns aber weiter um. Wer nähere Informationen dazu hat, kann sich gerne bei uns melden oder hier einen Kommentar hinterlassen, danke!

NACH DER RAZZIA: WAS DROHT DEN NUTZERN VON LUL.TO?

LUL.to: Seit der Razzia am 21. Juni 2017, bei der neben den früheren Betreibern auch Uploader betroffen sind, wird überall im Netz darüber spekuliert, welche zivil- und strafrechtlichen Konsequenzen auf die Nutzer dieses illegalen Portals zukommen könnten. Für unseren Hintergrundbericht haben wir uns bei allen relevanten Stellen erkundigt

Generalstaatsanwaltschaft Bamberg
Zentralstelle Cybercrime Bayern

Neben den anonymen Kommentatoren, die sich hier bei Tarnkappe.info als wütende Autoren ausgeben, wird den Kunden von Lesen & Lauschen (kurz LUL.to) auf verschiedenen Blogs und Webseiten systematisch Angst eingejagt. Grundlage der Panikmache ist ein Bericht von BILD Dresden, wonach „LKA-Hacker" jetzt angeblich damit beschäftigt seien, die rund 40.000 User von LUL.to zu „jagen". Im Artikel selbst drückt sich der Redakteur allerdings weitaus vorsichtiger aus. Für die zahlende Kundschaft „könnte" es jetzt eng werden, heißt es dort. Wer die Formulierung überprüft, wird feststellen, dass sie letzten Endes gar nichts Konkretes aussagt. Es könnte heute auch Hunde und Katzen regnen, wenn nicht gar E-Book-Reader. Dazu kommt: Ob den angemeldeten Nutzern oder zumindest den Power-Downloadern Abmahnungen, also zivilrechtliche Konsequenzen, oder sogar Strafbefehle drohen, wird von Bild.de nicht ausgeführt. Aber genau das interessiert natürlich unsere Leser, weil nicht wenige davon betroffen wären. Wir haben uns bei zahlreichen relevanten Stellen telefonisch erkundigt.



Ein Medien- und Strafrechtler, der wegen seiner direkten Verbindung zu diesem Fall nicht namentlich genannt werden kann, erläuterte, dass es strafrechtlich gesehen zwei Möglichkeiten gebe, sofern tatsächlich gegen die LUL.to-User ermittelt werden sollte. Abhängig von der Menge der nachweislich bezogenen Werke droht den aktiven Nutzern eine Geldauflage gemessen an der Anzahl der Downloads. Die Verfahren gegen Gelegenheits-Nutzer werden nach § 153 (StPO) (Absehen von der Verfolgung bei Geringfügigkeit) eingestellt. Das heißt, ent-

weder man zahlt an eine karitative Vereinigung eine festgelegte Strafe, oder aber der Staatsanwalt sieht wegen der Geringfügigkeit von einer Verfolgung komplett ab. Ab welcher Menge die LUL-Nutzer verfolgt werden könnten, liegt im Ermessensspielraum des zuständigen Staatsanwalts. Wer auf den Vorschlag der Staatsanwaltschaft nicht eingeht, müsste folglich mit einem gerichtlichen Verfahren rechnen. Doch dazu später mehr.

LKA Sachsen: Strafrechtliche Konsequenzen weder bestätigt noch dementiert!

Bei unserer Anfrage bei der Pressestelle des LKA Sachsen erläuterte uns Oberstaatsanwalt Matthias Huber, dass er derzeit weder bestätigen oder dementieren könne, ob strafrechtliche Schritte gegen die Nutzer von LUL.to geplant seien. Wir haben unsere E-Mail-Adressen ausgetauscht und vereinbart, das Gespräch in vier Wochen zu wiederholen. Dann könne er mir wahrscheinlich mehr Informationen geben, ob ein derartiges Vorgehen geplant sei. Strafrechtler Udo Vetter erläuterte mir, dieses Vorgehen der Pressestelle sei normal und nachvollziehbar. Die müssen sich auch erstmal ein genaues Bild von der Sache machen, bevor sie überhaupt einen Kommentar abgeben können. Jetzt stellt sich natürlich die Frage, auf Basis welcher Informationen die BILD-Zeitung berichtet haben will!?

Rechtsanwalt Tobias Röttger: Abmahnungen möglich, alles weitere in Ruhe abwarten!

Medienanwalt Tobias Röttger, LL.M., hält es für theoretisch möglich, dass die Konsumenten dieses offensichtlich rechtswidrigen Portals Abmahnungen erhalten werden. Dabei müsse man aber bedenken, dass es im Gegensatz zu den P2P-Abmahnungen keinen Upload gab, von daher sei der Streitwert sehr viel geringer. Die Kosten setzen sich dabei stets zusammen aus dem Wert der bezogenen Werke, dem Schadenersatz und den Kosten für die Ermittlung des jeweiligen Downloaders. Die Kanzlei Waldorf Frommer vertritt mehrere große Verlage und gab im Rahmen ihrer Pressemitteilung bekannt, dass man das umfangreiche Ermittlungsverfahren „begleitet“ habe. Wir haben am heutigen Donnerstag telefonisch und per E-Mail um ein Statement des Namensgebers Björn Frommer gebeten und warten derzeit auf eine Antwort. Wir reichen die Antwort unverzüglich nach. Update: E-Mail von 11.58 Uhr von Herrn Frommer: „Sie werden sicher verstehen, dass ich Ihnen in einem laufenden Strafverfahren weder Fragen beantworten noch Auskunft geben kann.“ Ja, natürlich ist diese Aussage nachvollziehbar.

Strafrechtlich gesehen erinnert der Fall laut Röttger an Ebay-Händler, die dort immer wieder illegale Lizenzen für Microsoft-Produkte anbieten und dabei erwischt werden, was auch für die Käufer knifflig werden kann. Röttger erinnert dabei allerdings daran, dass er selbst kein Strafrechtler sei, weswegen wir auch Udo Vetter um eine zusätzliche Einschätzung gebeten haben. Laut Röttger verstoßen die Downloader bei LUL.to gegen § 106 UrhG. Die zu klärende Frage wäre allerdings, wie bewusst dies geschehen ist. Da bei LUL.to explizit darauf hingewiesen wurde, dass ihr Angebot nicht der deutschen Gesetzgebung entspricht, wird es schon schwieriger, sich diesbezüglich herauszureden. Daneben verstoßen die Käufer in der Theorie gegen § 259 StGB (Hehlerei), selbst wenn sie die E-Books nur für sich selbst und eben nicht für Dritte bezogen haben. Deswegen fällt hierbei auch der Vorsatz weg, was sich strafmildernd auswirkt. Außerdem wurde für die Hörbücher und E-Books naturgemäß keine Mehrwertsteuer bezahlt, weswegen man zudem nach § 261 Abs. 2 StGB gegen das Geldwäschegesetz verstoßen hat. Die Frage ist aber, ob man überhaupt jemanden ermitteln kann. Die früheren Nutzer müssen sich folgende Fragen stellen:

- habe ich meinen Klarnamen angegeben und sei es in Form meiner E-Mail-Adresse? (also lieschen-mueller1965@gmail.com)
- habe ich beim Besuch einen VPN benutzt?
- wurden andere Angaben gemacht, die meine Identität preisgeben könnten?
- bin ich aufgrund meines für LUL.to gekauften Amazon-Gutscheines auszumachen?

Erwischt werden, wenn überhaupt, wieder nur die Personen, die sich aufgrund ihrer Naivität nicht ausreichend gegen eine Aufdeckung abgesichert haben. Die Frage ist halt, ob der Staatsanwalt für eine Einstellung gegen Auflage (Spende) vorzieht oder überhaupt gegen die User ermitteln will. Ersteres wäre wie ein Schuss vor den Bug, damit sich dieses Fehlverhalten nicht wiederholt.

Udo Vetter: Wer wegen LUL.to Post bekommt, sollte sich anwaltlich beraten lassen.

Laut Udo Vetter sei dieser Fall nicht mit Kino.to oder Popcorn Time gleichsetzbar. Das Missverhältnis zwischen Preis und Leistung sei deutlich größer. Ganz ehrlich: Wer glaubt schon, er könne sich legal ein E-Book für 15 Cent besorgen, wenn es überall sonst ein Vielfaches kostet!? Von daher war LUL.to eindeutig eine offensichtlich rechtswidrige Quelle, die man angezapft hat. Sich da herauszureden, sei schon deutlich schwieriger als bei einem Kinoportal, wo es keine Warnhinweise gibt und wo man für die Werke nicht bezahlt.

„Doch, Herr Sobiraj, was soll bei einem solchen Fall eigentlich herauskommen?“, fragt mich Udo Vetter. Die Schuld sei vergleichbar mit dem ersten Ladendiebstahl, den man begangen hat. Die allermeisten Personen sind wohl bisher nicht negativ aufgefallen und verfügen über keine Vorstrafe. Auch könne man laut Vetter nicht argumentieren, dass die Staatsanwaltschaft ja auf ihre Kosten der Ermittlung kommen müsse. Da ging es ausschließlich um das Ausfindig machen der Betreiber und nicht die Kosten, die man jetzt irgendwelchen Downloadern aufdrücken kann, das seien zwei Paar Schuhe und das dürfe man nicht miteinander vermischen. Von daher wäre die strafrechtliche Verfolgung im Ergebnis „überschaubar“. Vetter rechnet mit Geldstrafen bzw. die Einstellung vor Eröffnung des Gerichtsverfahrens gegen 200 bis maximal 500 Euro, abhängig davon, wie viele Werke dort nachweislich gekauft wurden.

Ganz allgemein gesprochen gebe es zwei Möglichkeiten, wie die Staatsanwaltschaft mit der Sache umgeht. Entweder wird im schlimmsten Fall eine Durchsuchung der Downloader angesetzt, bei der man sich sowieso von einem Fachanwalt vertreten lassen sollte. Oder aber man erhält einen Anhörungsbogen und soll sich selbst als Beschuldigter bei der Polizei zu den Vorwürfen äußern. Auch in diesem Fall sollte man dies ausnahmslos mit Unterstützung eines Fachanwalts für Strafrecht tun, damit von Anfang an „die Weichen richtig gestellt“ werden. Wer will schon wegen einer unglücklichen Aussage zu einer Geldstrafe verurteilt werden, was einer Vorstrafe gleichkommt?

Fazit: Abwarten und Ruhe bewahren. Wer von einer Anwaltskanzlei oder der Polizei Post bekommt, sollte besser nicht versuchen, sich ohne Unterstützung mit der Thematik zu beschäftigen! Kanzleien und Verlagen wird es möglicherweise darum gehen, ein wenig Profit aus der Sache zu schlagen. Und auch die Polizei ist nicht unser Freund und Helfer. Dies wissen laut Udo Vetter leider nur die Menschen, die tagtäglich an der Front tätig sind.

STÖRERHAFTUNG FÄLLT: FREIES WLAN KOMMT

Die Große Koalition hat sich einem Bericht des Handelsblatts zufolge kurz vor der Sommerpause doch noch auf die Abschaffung der sogenannten Störerhaftung für Anbieter öffentlicher WLAN-Netze geeinigt. Somit ist nun der Weg frei für mehr kabelloses Internet in Hotels, Cafes und Innenstädten. Die Verabschiedung soll noch vor der Sommerpause erfolgen.

Bundeswirtschaftsministerin Brigitte Zypries (SPD) habe am Montagmittag mit den Fraktionsvorsitzenden von Union und SPD gesprochen und eine Einigung erzielt. Zuvor war wegen Unstimmigkeiten zwischen diesen Parteien weitgehend unklar, ob das Gesetz noch in der letzten Sitzungswoche vor der Sommerpause, also der letzten Gelegenheit in dieser Legislaturperiode, verabschiedet werden kann.

Die Regierung hatte sich bereits Anfang April auf den entsprechenden Gesetzentwurf verständigt. So stimmten die Parteien dem „Entwurf eines Dritten Gesetzes zur Änderung des Telemediengesetzes“ des Bundeswirtschaftsministeriums, der bereits vom Kabinett absegnet war, vollständig zu. Lediglich auf eine Klarstellung haben sie sich verständigt: Es soll noch deutlicher gemacht werden, dass WLAN-Betreiber, wie Hotels und Gaststätten, auch weiterhin eigene Sicherheitsmaßnahmen, etwa die Vorschaltung eines Passworts, nutzen dürfen, wenn sie das wollen – es wäre aber keine Verpflichtung. Die entsprechende Formulierung lauet: „Davon unberührt bleibt, wenn ein Diensteanbieter auf freiwilliger Basis die Nutzer identifiziert, eine Passworteingabe verlangt oder andere freiwillige Maßnahmen ergreift.“

Mit der Abschaffung der Störerhaftung müssen Betreiber öffentlicher WLAN-Hotspots nun nicht mehr befürchten, für die Vergehen von Nutzern ihres Internetzugangs haftbar gemacht zu werden. Im Gegenzug erhalten Rechteinhaber den Anspruch, die „Sperrung der Nutzung von Informationen [zu] verlangen, um die Wiederholung der Rechtsverletzung zu verhindern“, wenn eine Löschung von Inhalten durch den Webseitenbetreiber oder Hostprovider nicht möglich ist. Auch in diesen Fällen dürfen vor- und außergerichtliche Kosten nicht geltend gemacht werden. Kritiker dieser Regelung befürchten jedoch, dass Anbieter die Netzsperren widerspruchslos umsetzen, um gerichtliche Kosten zu vermeiden.

Kritik gab es ferner dazu besonders aus dem Bereich der Musikindustrie. Florian Drücke vom Bundesverband Musikindustrie befürchtete, damit werde es einen „Leerlauf der Rechtsdurchsetzung“ geben. Dabei sei das „Durchsetzungsverhinderungsgesetz“, das sich an alle möglichen Provider richte, mit europäischen Recht nicht vereinbar. Der Europäische Gerichtshof (EuGH) habe gerade erst mit seinem Urteil gegen The Pirate Bay aufgezeigt, dass es möglich sein müsse, gegen Rechtsverletzer angemessen vorzugehen.

Andreas May von der Generalstaatsanwaltschaft Frankfurt am Main kritisiert, dass WLAN-Betreiber nicht behördlich verpflichtet werden dürften, „Nutzer zu registrieren“ oder die Eingabe eines Passwortes zu verlangen. Dazu komme, dass die meisten Hotspot-Anbieter auch nicht unter die Pflicht zur neuen Vorratsdatenspeicherung fielen. Damit werde die übrige verschärfte Sicherheitsgesetzgebung konterkariert. May bezog sich mit dieser Äußerung auf die neuen Überwachungsmöglichkeiten von Internet-Telefonie und Messenger-Kommunikation.

Volker Tripp vom Verein Digitale Gesellschaft hielt derlei Bedenken hingegen für „herbeigeredet“. Praktische Erfahrungen bei einem Pilotversuch der Medienanstalt Berlin-Brandenburg mit offenen Funknetzen hätten gezeigt, dass kein einziger Fall von Urheberrechtsverletzungen vorgekommen sei. Dabei würde es sich um eine „rein behauptete Gefahr“ handeln.

Der eco-Verband der Internetwirtschaft kritisiert, mit dem Vorschlag solle „eine Rechtsgrundlage für Netzsperren auf Zuruf der Rechteinhaber ohne richterlichen Beschluss“ geschaffen werden. Sie verfehle damit das eigentliche Ziel, „endlich Rechtssicherheit für WLAN-Betreiber zu schaffen“.

ABMAHNGEFAHR? – WHATS-APP-URTEIL SORGT FÜR SCHLAGZEILEN

Das Amtsgericht Bad Hersfeld hat in einem aktuellen Urteil entschieden, dass es nicht erlaubt ist, andere Personen ohne deren Einwilligung in die eigene WhatsApp-Kontaktliste einzutragen. Theoretisch machen sich WhatsApp-Nutzer, zumindest in Deutschland, damit strafbar. Der Grund liegt in der Funktionsweise des Messengers, der Handynummern automatisch mit dem Telefonbuch abgleicht.

Das Urteil ist das Ergebnis eines Sorgenrechtsstreites. In einem familienrechtlichen Verfahren (F 120/17 EASO) ging es um die Smartphone-Nutzung eines elfjährigen Kindes. Gegenstand der Verhandlung war ein Streit zwischen den getrennt lebenden Elternteilen, wie häufig das Kind sein Smartphone nutzen darf. So soll der Kleine sich mitunter um 4.30 Uhr morgens den Wecker gestellt haben, um mit seinem Smartphone zu spielen.

Einerseits erteilte das Gericht der Mutter gewisse Auflagen, wie „mit ihrem Sohn E. eine schriftliche Medien-Nutzungsvereinbarung […] zu schließen […] “. Andererseits – und das ist der eigentliche Grund für die Schlagzeilen – gab der folgende Leitsatz aus dem Urteil der Richter Anlass für die neu angeregte

Diskussion um die Datenweitergabe-Praktiken von WhatsApp:

„Wer den Messenger-Dienst ‚WhatsApp' nutzt, übermittelt nach den technischen Vorgaben des Dienstes fortlaufend Daten in Klardaten-Form von allen in dem eigenen Smartphone-Adressbuch eingetragenen Kontaktpersonen an das hinter dem Dienst stehende Unternehmen. Wer durch seine Nutzung von ‚WhatsApp' diese andauernde Datenweitergabe zulässt, ohne zuvor von seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, begeht gegenüber diesen Personen eine deliktische Handlung und begibt sich in die Gefahr, von den betroffenen Personen kostenpflichtig abgemahnt zu werden."

Das Gericht erläuterte in dem Zusammenhang den Standard-Mechanismus, den WhatsApp nutzt, um die Verbindung zwischen den Nutzern herzustellen: Das Telefonbuch des Nutzers wird dabei an WhatsApp übertragen. Im zweiten Schritt findet dann auf den Servern ein Abgleich mit den Nummern der registrierten Nutzer statt. Stimmen die Nummern überein, erscheint die Person in den WhatsApp-Kontakten. Dieser Vorgang darf dem Gericht zufolge jedoch nicht ohne schriftliche Zustimmung der betroffenen Nutzer, also aller Kontakte im Adressbuch, stattfinden. Liegt eine solche Zustimmung nicht vor, verstößt das gegen geltendes Recht und die Betroffenen hätten damit die Möglichkeit, sich mittels kostenpflichtiger Abmahnung zur Wehr zu setzen, so lautet das Fazit des Gerichts. Denn letzlich wäre die gängige Praxis von WhatsApp ein Verstoß gegen das Grundrecht auf die informationelle Selbstbestimmung und das Datenschutzrecht.

Medienanwalt Christian Solmecke führt dazu auf seinem Blog aus: „Das Urteil ändert rechtlich erst einmal nichts daran, da es sich um eine familienrechtliche Streitigkeit vor einem Amtsgericht handelt, die andere Gerichte nicht bindet. Allerdings hat das Urteil Signalwirkung, gerade weil es nun medial bekannt wird. Viele Menschen werden jetzt erst auf die seit Jahren gängige Praxis des Unternehmens aufmerksam.

In der Praxis wären private Abmahnungen aber in den meisten Fällen widersinnig. Zum einen möchten sicherlich wenige ihre Freunde und Bekannten abmahnen. Weiterhin würde man sich als WhatsApp-Nutzer selbst in die Gefahr begeben, wiederum von dem anderen Nutzer abgemahnt zu werden. Und die wenigen, die WhatsApp nicht selbst nutzen, wissen im Zweifel nicht, dass ihre Freunde und Bekannte ihre Telefonnummern nach Kalifornien übermitteln. Und selbst wenn sie nun – nach diesem medial bekannt gewordenen Urteil – überlegen, jemanden abzumahnen, dann wäre ein solches Vorgehen nicht zielführend und ineffektiv. Denn man müsste ja gegen jede einzelne Person vorgehen, der man jemals seine Nummer gegeben hat, ohne zu wissen, ob sie WhatsApp nutzt."

Demnach dürften wohl in der Praxis teuere Abmahnungen in der Regel ausbleiben, denn wo kein Kläger, da kein Richter. Dennoch hätte dieses Urteil wohl eine Signalwirkung und könnte weitere Klagen von Datenschützern und Verbraucherschützern nach sich ziehen, die sich nicht gegen die Nutzer, sondern den Betreiber, also WhatsApp, richten.

AUF BESCHLUSS DES BUNDESTAGES: AUSSAGEPFLICHT VON ZEUGEN

Mit dem Entwurf des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens wurden nicht nur der Staatstrojaner und die Online-Durchsuchung beschlossen, es sind zudem noch andere, erwähnenswerte Änderungen in Kraft getreten.

So ist neu, dass Zeugen künftig verpflichtet sind, Vorladungen der Polizei Folge zu leisten und zu einer Sache auszusagen: „Zeugen sind verpflichtet, auf Ladung von Ermittlungspersonen der Staatsanwaltschaft zu erscheinen und auszusagen, wenn der Ladung ein Auftrag der Staatsanwaltschaft zugrunde liegt.", so der Wortlaut.

Für Opfer von Straftaten können Zeugen wichtige Unterstützung leisten. Dennoch war bisher niemand verpflichtet, gegenüber der Polizei eine Aussage zu machen und das war zudem völlig unabhängig davon, ob dem Zeugen darüber hinaus noch besondere Zeugnisverweigerungsrechte (zum Beispiel Verwandtschaft mit dem Beschuldigten) oder Aukunftsverweigerungsrechte (Gefahr der Selbstbelastung) zustanden. Dies galt nicht nur bei der ersten Befragung vor Ort. Auch einen Anhörungsbogen als Zeuge musste keiner beantworten. Ebenso brauchte man zu keinem Vernehmungstermin auf der Polizeiwache zu erscheinen.

Die Rechtsanwälte der Kanzlei Vetter & Mertens führen auf ihrem Blog dazu aus: „Die große Frage in der Praxis wird zunächst sein, wie konkret dieser Auftrag der Staatsanwaltschaft sein muss. Das Gesetz bleibt hier unglaublich – man könnte auch sagen unverschämt – vage. […] Außerdem hat der Gesetzgeber darauf verzichtet, eine schriftliche Ladung oder eine bestimmte Ladungsfrist einzuführen. […] Denkbar ist weiterhin, dass die Polizei von ihrer Ladungsmöglichkeit auch in einer Art und Weise Gebrauch macht, welche die Lebensgestaltung eines Zeugen erheblich beeinträchtigt.“ Demnach wären viele Fragen dazu noch offen oder nur angedacht, nicht jedes Detail geregelt.

Die größte Gefahr in der Neuregelung sehen die Anwälte jedoch in einer Grauzone, die sich mitunter bei Ermittlungen ergibt: „Nämlich dann, wenn nicht ganz klar ist, welche Rolle eine Person eigentlich innehat. Ist sie Zeuge? Oder vielleicht doch schon Beschuldigter? Oder möglicherweise beides, wenn es um mehrere Tatkomplexe geht?“. Diese Frage hinge oft von der Einschätzung eines Ermittlers ab, führen sie weiter aus. Als Personen noch nicht zu einer Aussage gezwungen waren, spielte es keine Rolle für sie, ob sie beschuldigt wurden oder nur als Zeuge aussagen würden, denn niemand musste auf Fragen des Ermittlers eingehen. Es bringt nun aber die Gefahr mit sich, dass die Vorgeladenen Angaben zur Sache machen, die sie ohne Pflicht zum Erscheinen nie geäußert hätten. Auch der Zeitpunkt, in dem ein Zeuge zum Beschuldigten wird und entsprechend zu belehren ist, ließe sich somit kreativ weit nach hinten verlagern, wobei bei einer nicht vorhandenen Audioaufnahme, wie es hierzulande üblich ist, nachträglich auch keine konkrete Beschuldigtenbelehrung mehr festzustellen wäre.

Da bereits innerhalb von Sekunden jeder zum Zeugen werden kann, auch völlig unverhofft, denn ganz egal, ob bei einem Unfall, einer Schlägerei oder bei einem Diebstahl – jeder kann einmal in die Situation kommen, eine mögliche Straftat zu beobachten. Nimmt die Polizei die Ermittlungen auf, werden auch Zeugen befragt. So wäre das Fazit der Anwälte der Kanzlei Vetter & Mertens: „Umso wichtiger wird es dann sein, dass man die dürftigen Rechte zumindest ansatzweise kennt, die man im Umgang mit der Polizei künftig noch hat.“

NICHT EU-KONFORM: STEHT DIE VORRATSDATENSPEICHERUNG VOR DEM AUS?

Das Oberverwaltungsgericht Nordrhein-Westfalen, mit Sitz in Münster, hat die anlasslose Speicherung von Telefon- und

Internetdaten in Deutschland durch einen Beschluss vom 22. Juni 2017 für rechtwidrig erklärt (Az. 13 B 238/17). Die pauschale Speicherpflicht widerspreche den Anforderungen, die der EuGH bereits aufgestellt habe. Aus Sicht von Experten ist damit die Vorratsdatenspeicherung gescheitert.

Eigentlich wären die Erbringer öffentlich zugänglicher Telekommunikationsdienste genötigt gewesen, ab spätestens 1. Juli 2017 die Verpflichtung zur Vorratsdatenspeicherung nach §§113a-g des Telekommunikationsgesetzes (TKG) zu erfüllen und umzusetzen und somit die Telefon- und Internetverbindungsdaten aller Bürger zehn Wochen und Standortdaten einen Monat lang zu speichern. Dem Münchener Provider Spacenet ist es aktuell gelungen, dies gerichtlich anzufechten. Mit Unterstützung des IT-Branchenverbands Eco hat das Unternehmen erfolgreich gegen die Vorgaben der Bundesnetzagentur geklagt – was anderen Zugangsanbietern ebenfalls entsprechende Spielräume ermöglichen dürfte. Die Entscheidung im Hauptsacheverfahren steht allerdings noch aus, da der Beschluss nur das Eilverfahren betraf.

Das Münchener IT-Unternehmen Spacenet erbringt u.a. Internetzugangsleistungen für Geschäftskunden in Deutschland und in anderen EU-Mitgliedstaaten. Es hatte sich mit einem Antrag auf Erlass einer einstweiligen Anordnung an das Verwaltungsgericht Köln gewandt, um der Verpflichtung zur Vorratsdatenspeicherung vorläufig bis zur Entscheidung über die gleichzeitig erhobene Klage nicht nachkommen zu müssen. Diesen Antrag hatte das Verwaltungsgericht abgelehnt. Der gegen diese Entscheidung erhobenen Beschwerde der Antragstellerin hat das Oberverwaltungsgericht nunmehr jedoch stattgegeben.

Das Oberverwaltungsgericht Nordrhein-Westfalen hat am 22.06.2017 den ersten Internet-Zugangsanbieter von der Pflicht zur verdachtslosen Vorratsdatenspeicherung befreit, die zum 1. Juli umgesetzt werden soll. Mit der Begründung, das schwarz-rote Gesetz zur Vorratsspeicherung treffe: „unterschiedslos ohne jede personelle, zeitliche oder geographische Begrenzung nahezu sämtliche Nutzer“ und greife unver-

hältnismäßig tief in europäische Grundrechte ein. Erforderlich wäre es jedoch laut einem aktuellen Urteil des Europäischen Gerichtshofs zur Vorratsdatenspeicherung, dass der Kreis der betroffenen Personen von vornherein auf Fälle beschränkt werden müsse, „bei denen ein zumindest mittelbarer Zusammenhang mit der durch das Gesetz bezweckten Verfolgung schwerer Straftaten bzw. der Abwehr schwerwiegender Gefahren für die öffentliche Sicherheit bestehe“. Dies könne etwa durch personelle, zeitliche oder geographische Kriterien geschehen. Angesichts der „bereits feststehenden objektiv-rechtlichen Unrechtswidrigkeit der Speicherpflicht“ bestehe „schon im Ausgangspunkt keine legitimen öffentlichen Interessen an einem vorläufigen Vollzug“ des Gesetzes zur Vorratsdatenspeicherung.

Gemäß dem Urteil des Gerichtshofs könne die anlasslose Speicherung von Daten insbesondere nicht dadurch kompensiert werden, dass die Behörden nur zum Zweck der Verfolgung schwerer Straftaten bzw. der Abwehr schwerwiegender Gefahren Zugang zu den gespeicherten Daten erhielten und strenge Maßnahmen zum Schutz der gespeicherten Daten vor Missbrauch ergriffen würden. Der OVG-Beschluss ist nicht anfechtbar. Ein Gang zum Bundesverfassungsgericht im Hauptsacheverfahren bleibt aber möglich und das könnte letztlich bis zum Europäischen Gerichtshof gebracht werden.

Wenngleich diese Entscheidung zwar (zunächst) nur für das IT-Unternehmen aus München gilt, sendet der Beschluss nach Einschätzung der Grünen und mehrerer Datenschützer ein Signal von viel größerer Tragweite aus. So meinte Vize-Chef der Grünen-Bundestagsfraktion, Konstantin von Notz, gegenüber dem Handelsblatt: „Das Gesetz muss wegen der gravierenden Rechtsunsicherheit, seiner hohen Risiken für die Grundrechte der Bürger und die Kosten für die Unternehmen sofort gestoppt werden. Die Große Koalition ist vorsätzlich in diese Blamage reingelaufen.“ Mit Blick auf das am gestrigen Donnerstag verabschiedete „Staatstrojaner“-Gesetz fügte er hinzu: „Die Grundrechte werden leider im Wochentakt von der Großen Koalition durch immer neue Gesetze geschliffen.“ Da komme das Bundesverfassungsgericht kaum dagegen an.

Jan Philipp Albrecht, stellvertretender Vorsitzender des Innen- und Justizausschusses und innen- und justizpolitischer Sprecher der Grünen im Europäischen Parlament, wertet die Münsteraner Entscheidung als „Meilenstein“ in der Durchsetzung des EU-Grundrechts auf Datenschutz. Dass nun auch höchste Gerichte in Deutschland auf das jüngste Urteil des Europäischen Gerichtshofs (EuGH) gegen das anlasslose Protokollieren von Nutzerspuren verwiesen, „sollte die Bundesregierung unmittelbar veranlassen, das Gesetz zurückzunehmen“. „Außerdem ist die EU-Kommission aufgefordert“, so Albrecht weiter, „das deutliche Urteil des Europäischen Gerichtshofs gegenüber den Mitgliedstaaten per Vertragsverletzungsverfahren umgehend durchzusetzen.“

Andere Provider müssten nun versuchen, mit einem Eilverfahren aktuell selbst gegen die Datenspeicherung zu klagen. Das gilt jedoch nicht für die Deutsche Telekom, die bereits im Mai vor dem Verwaltungsgericht Köln geklagt hatte, um die Speicherung von öffentlichen IP-Adressen bei Mobilfunk- oder WLAN-Nutzern zu vermeiden. Mit der Begründung, weil eine öffentliche IPv4-Adresse durch die sogenannte Network Address Translation (NAT) sehr vielen Nutzern zugeordnet werden könnten, sei eine Speicherung der Daten für die Ermittlungsbehörden nutzlos. Daher will der Provider erforderliche Investitionen in zweistelliger Millionenhöhe vermeiden.

Oliver Süme, eco Vorstand Politik & Recht, meint: „Das Oberverwaltungsgericht hat ausdrücklich ausgeführt, dass die Vorratsdatenspeicherung generell europarechtswidrig ist. Jetzt sollte die Bundesnetzagentur gegenüber allen Telekommunikationsunternehmen klarstellen, dass sie die Daten nicht speichern müssen, bis über die Klage endgültig entschieden ist. […] Jetzt ist es an der Zeit für eine Grundsatzentscheidung, um die Vorratsdatenspeicherung endgültig zu stoppen. Andernfalls laufen die Unternehmen Gefahr, ein europarechts- und verfassungswidriges Gesetz umsetzen zu müssen und damit Gelder in Millionenhöhe in den Sand zu setzen.“, meint er weiter.

Auch für den Arbeitskreis Vorratsdatenspeicherung steht fest, dass „schon im Ausgangspunkt keine legitimen öffentlichen Interessen an einem vorläufigen Vollzug“ des umstrittenen Gesetzes bestünden. In einem Appell fordern sie alle Telefon-, Mobilfunk- und Internetanbieter auf, Klage einzureichen und das Überwachungsmonster Vorratsdatenspeicherung nicht umzusetzen“.

GRÜNES LICHT FÜR STAATSTROJANER: FREIGABE AUCH FÜR DIE ALLTÄGLICHE STRAFVERFOLGUNG

Der Bundestag beschließt – trotz Kritik von Bürgerrechtlern und IT-Branche – im Eilverfahren mit den Stimmen von Union und SPD den Einsatz von Staatstrojanern auch

für die alltägliche Strafverfolgung. So dürfen Strafverfolger künftig in vielen Fällen verschlüsselte Internet-Telefonate und Chats über Messenger, wie WhatsApp, Signal, Telegram oder Threema, rechtlich abgesichert überwachen (Quellen-TKÜ) oder Dateien auslesen (Online-Durchsuchung).

Der Bundestag verabschiedete am Donnerstag (22.06.2017) das Gesetz „zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“. Gemäß dem Gesetzentwurf ist die Quellen-TKÜ künftig bei „schweren Straftaten“ erlaubt, bei denen auch Ermittlungsbehörden die Telekommunikation überwachen dürfen (Paragraf 100a Strafprozessordnung). Dazu zählen neben Mord und Totschlag beispielsweise auch Steuerhinterziehung, Geldfälschung und Computerbetrug. Die Online-Durchsuchung soll nur bei „besonders schweren Straftaten“ erlaubt sein, bei denen eine akustische Wohnraumüberwachung (Großer Lauschangriff) möglich ist (Paragraf 100c Strafprozessordnung). Bisher waren Staatstrojaner zur Terrorbekämpfung zugelassen.

Mit dem Staatstrojaner will die Bundesregierung Strafverfahren „effektiver und praxistauglicher“ machen. Vorraussetzung für den Einsatz wäre, die Geräte der Betroffenen mit Schadsoftware in Form sogenannter Staatstrojaner zu infizieren. Damit wird jedoch die IT-Sicherheit laut Experten allgemein untergraben. Das Gesetz ist umstritten, weil Datenschutz-Probleme und ein Missbrauch von den Behörden bewusst nicht geschlossener Sicherheitslücken befürchtet werden. Zudem wird die Frage aufgeworfen, ob die Reichweite der Maßnahmen mit der Verfassung vereinbar ist.

Die Grünen meinen, die Bundesregierung startet mit dem Gesetz kurz vor Ende der Legislaturperiode „ihren finalen Angriff auf die Bürgerrechte“. Polizei und Sicherheitsbehörden würden damit „zu Chef-Hackern der Republik gemacht“.

Nur noch perfide sei, „dass die Bundesregierung den Staatstrojaner selbst als trojanisches Pferd in einem harmlosen Gesetz zum Fahrverbot als Nebenstrafe versteckt“, teilten die Abgeordneten Konstantin von Notz und Hans-Christian Ströbele mit, denn in dem Gesetzentwurf ging es zunächst nur um eine Strafrechtsreform.

Der Richter und Bürgerrechtler Ulf Buermeyer sieht die Vielzahl an möglichen Einsatzfällen für eine Onlinedurchsuchung als „verfassungsrechtlich nicht zu rechtfertigen“, auch die Quellen-TKÜ werde so weit gefasst, dass sie verfassungswidrig sei.

Kritiker bemängeln u.a., dass die große Koalition den Gesetzentwurf erst Mitte Mai in ein bereits laufendes Gesetzgebungsverfahren eingebracht hatte. Der frühere Bundesdatenschutzbeauftragte Peter Schaar meint, es sei „unverantwortlich, die entsprechenden Überwachungsbefugnisse in einem parlamentarischen Schnelldurchgang ohne Möglichkeit zur gründlichen Prüfung und Debatte zu beschließen“.

Bitkom-Hauptgeschäftsführer Bernhard Rohleder kritisierte ebenfalls das Gesetz. Die Bemühungen der Wirtschaft um eine wirkungsvolle Ende-zu-Ende-Verschlüsselung „werden mit der Ausweitung des Einsatzes von Staatstrojanern konterkariert“, sagte er.

GERICHT: VERLINKUNG AUF LINKVERBOTE DURCH GOOGLE IST NICHT STATTHAFT

Das Oberlandesgericht München entschied in einer einstweiligen Verfügung, dass Google im Falle von entfernten Links auf rechtswidrige Inhalte nicht auf eine Datenbank mit Löschanfragen verlinken darf. Google wurde damit erstmals verboten, Nutzer über einen Hinweis am Ende der Suchergebnisseite auf ein bereits gelöschtes Suchergebnis in der Datenbank „LumenDatabase“ zu lenken (OLG München, Beschluss v. 7.6.2017, Az. 18 W 826/17). So sollen einmal gelöschte Links nicht durch die Hintertür wieder abrufbar sein.

Kläger in diesem Fall war ein Anbieter von Immobilienfonds aus Tübingen, gegen den die Staatsanwaltschaft Stuttgart im Jahr 2014 nach anonymen Anzeigen Ermittlungen aufgenommen hatte. So waren Äußerungen im Internet vorhanden, in de-

nen behauptet wurde, dass gegen das Unternehmen des Klägers Ermittlungen wegen eines Betrugsverdachts laufen. Tatsächlich handelte es sich aber um Ermittlungen wegen eines Verdachts auf Kapitalanlagebetrug. Das OLG München gelangte zur Auffassung, dass sich ein Betrugsverdacht erheblich von einem Kapitalanlagebetrugsverdacht unterscheidet und ordnete diese Äußerungen als unwahre Tatsachenbehauptungen ein. Google wurde verpflichtet entsprechende Suchergebnisse aus dem Index zu löschen. Dem kam Google auch nach, jedoch wurde gleichzeitig darauf hingewiesen, dass Suchergebnisse nicht berücksichtigt werden konnten und auf die Webseite lumendatabase.org verlinkt. Dort wurde offenbar die Löschung dokumentiert und ein Link zu einer weiteren Webseite bereitgehalten auf der dann die rechtsverletzenden Inhalte einsehbar waren. Das Unternehmen wollte deshalb Google zwingen, die Hinweise auf die Lumen-Datenbank unter dem Suchergebnis zu unterlassen.

Ende April hatte das Landgericht München I den Erlass einer Einstweiligen Verfügung zu diesem Zweck abgelehnt, weil es keinen Verfügungsgrund sah. Auf Beschwerde des Immobilienfonds hat das OLG München nun eine Einstweilige Verfügung erlassen. Das OLG ist der Ansicht, dass Google als „mittelbare Störerin“ in die Verantwortung zu nehmen ist. Entgegen der Auffassung des Landgericht sei dabei nicht entscheidend, dass Google nicht selbst auf die Seite mit den gelöschten Suchergebnissen verlinkt, sondern nur auf den Eintrag der Lumen-Datenbank. In der Begründung des Beschlusses vom 7. Juni 2017 durch die Münchner Richter heißt es, Google habe seine Prüfpflichten missachtet, denn auch durch die direkte Verlinkung auf die Löschanträge durch Google werde die betroffene Firma in ihrem Unternehmenspersönlichkeitsrecht verletzt. Das Gericht sieht den „Schwerpunkt“ der Suchmaschine nicht „in dem Setzen eines Links, sondern in ihrer Suchfunktion“. Durch den Hinweis auf die Lumen-Datenbank ermögliche Google seinen Nutzern, die beanstandeten Ergebnisse zu finden.

Nach Angaben der Kanzlei LHR, die das betroffene Unternehmen vertreten hat, handelt es sich um das erste gerichtliche Verbot für Google, das die Verlinkung auf Lumen betrifft.

Das Projekt lumendatabase.org wird von der Berkman Klein Center for Internet & Society at Harvard University betrieben. Das Projekt soll nach eigenen Aussagen die Löschung von Inhalten aus dem Internet dokumentieren. Dabei soll auch vermerkt werden, wer die Löschung veranlasst hat bzw. warum. So werden Unterlassungsverfügungen für Online-Inhalte gesammelt, beispielsweise wegen Urheberrechtsverletzungen. Damit soll die Forschung zu den Themen erleichtert werden. Das Ziel dieser Dokumentation ist die Schaffung von Transparenz.

EUGH-URTEIL: THE PIRATE BAY VERLETZT URHEBERRECHTE

Laut einem EuGH-Urteil vom 14.06.2017 kann nun die Piraten-Plattform „The Pirate Bay“ (TPB) direkt für Urheberrechtsverletzungen verantwortlich gemacht werden. Das Urteil erwirkte die niederländische Anti-Piraterie-Vereinigung Stichting Brein.

Die in Schweden gegründete Tauschbörse The Pirate Bay ist ein Peer-to-Peer-Netzwerk, über das Webseiten-Besucher dezentral kostenlos auf urheberrechtlich geschützte Werke, wie die neuesten Kinofilme, teuere Computerprogramme oder Musikalben, zugreifen können, die auf Rechnern anderer Nutzer liegen.

Auf die Frage, ob Online-Tauschbörsen für Urheberrechtsverletzungen ihrer Nutzer haftbar sind, argumentierten die Betreiber bisher, dass sie lediglich eine technische Plattform bereitstellen, nicht jedoch für die getauschten Inhalte zur Verantwortung gezogen werden können. Dieser Argumentation widersprach der Europäischen Gerichtshofs (EuGH) nun und macht The Pirate Bay direkt für die illegale Downloads verantwortlich.

Nach Ansicht des Europäischen Gerichtshofs (EuGH) erlaubt Pirate Bay eine „öffentliche Wiedergabe“ geschützter Werke auch ohne Einverständnis der Rechteinhaber im Sinne der EU-Urheberrechtsrichtlinie 2001/29/EG. Damit könnten sie das Urheberrecht verletzen, auch wenn es letztlich die Plattformnutzer seien, die den Zugriff auf urheberrechtlich geschützte Medien ermöglichten. Die Betreiber von The Pirate Bay würden sowohl wissen, dass sie dabei helfen, illegal geschützte Werke zu verbreiten, als auch ihre Nutzer dazu veranlassen, Kopien solcher Werke zu erstellen, meint der Europäische Gerichtshof. Zwar stellen die Werke auf The Pirate Bay die User selbst on-

line, doch versehen die Betreiber die Torrent-Dateien mit einem Index, damit die Werke von den Nutzern leicht aufgefunden und heruntergeladen werden können. Außerdem löschten die Betreiber veraltete oder fehlerhafte Torrent-Dateien und filterten aktiv bestimmte Inhalte. In der Pressemitteilung des EuGH heißt es: „Der Gerichtshof räumt zwar ein, dass die geschützten Werke durch die Nutzer online gestellt wurden. Gleichwohl spielen die Betreiber der Plattform beim Zurverfügungstellen dieser Werke eine zentrale Rolle.“ Zudem werde The Pirate Bay mit dem Ziel betrieben, mit Werbung einen Gewinn zu erzielen. Demnach können die Rechteinhaber bei Verstößen nicht nur gegen Filesharing-Nutzer vorgehen, sondern direkt gegen die Plattformbetreiber. Damit folgte das Gericht dem Antrag des Generalanwalts Maciej Szpunar vom Februar 2017.

Anlass des Rechtsstreits war eine Klage der niederländischen Stiftung für Urheberrecht Stichting Brein gegen die Internetanbieter Ziggo und XS4ALL, die Domainnamen und die IP-Adressen von The Pirate Bay sperren sollen, denn ein bedeutender Teil ihrer Abonnenten nutzt die Online-Filesharing-Plattform The Pirate Bay. Das höchste niederländische Gericht, der Hoge Raad der Nederlanden, verwies den Fall an den EuGH. Dieser sollte darüber befinden, ob The Pirate Bay eine „öffentliche Wiedergabe“ im Sinne der Urheberrechtsrichtlinie vorgenommen hatte.

Das EuGH-Urteil ermöglicht nun eine Blockade von TPB, die jedoch nicht mit sofortiger Wirkung eintritt. Was noch fehlt ist eine Bestätigung des niederländischen Höchstgerichtes, die laut TorrentFreak noch einige Monate dauern dürfte.

Die deutsche Musikbranche begrüßte dieses Urteil als schon lange überfällig. Mit ihm werde endlich „die zentrale Rolle dieser Plattform bei der illegalen Verbreitung von Inhalten“ anerkannt, kommentierte Florian Drücke, Geschäftsführer des Bundesverbandes Musikindustrie. Es handele sich um eine richtungsweisende Klarstellung, die die zukünftige Rechtsdurchsetzung gegenüber Plattformen auf eine neue Grundlage stellen werde.

Internetaktivisten vom Chaos Computer Club (CCC) sehen eine mögliche Sperrung von Tauschbörsen jedoch kritisch, denn es bestehe die Gefahr, dass andere Seiten mit legalen Inhalten mitgeblockt würden, sagte CCC-Sprecher Falk Garbsch. Aus seiner Sicht greifen Nutzer auf Pirate Bay und ähnliche Netzwerke zurück, weil es nicht in jedem Land Zugänge zu den legalen Angeboten gebe. Er verwies auch darauf, dass es technisch einfach sei, die Sperren zu umgehen.

Bei The Pirate Bay zeigte man sich nicht beeindruckt von dem Urteil und verwies auf den Umstand, dass Nutzer, die die Seite finden wollen, das auch künftig erreichen werden.

Sebastian Dramburg, Fachanwalt für Medienrecht, hält es für möglich, dass der Gerichtshof in Luxemburg mit diesem Urteil eine Grundsatzentscheidung gefällt hat: „Es ist denkbar, dass dann auch in Deutschland Urheber, deren Werke betroffen sind, von der Telekom verlangen werden, den Zugang zur Onlineplattform zu sperren.“

URTEIL: FERNSEH-MITSCHNITTE AUF YOUTUBE SIND WEITERHIN ILLEGAL

Mit der Begründung, „nicht alles Zumutbare getan“ zu haben, verlor YouTube den Prozess um einen illegalen Fernseh-Mitschnitt. Das Landgericht (LG) Leipzig hat mit einem jetzt bekannt gewordenem Urteil vom 19. Mai 2017 entschieden, dass ein Mitschnitt der Fernseh-Ausstrahlung des Dokumentarfilms »Leben außer Kontrolle« nicht auf der Internetplattform YouTube weiterverbreitet werden darf.

Mit Unterstützung der Arbeitsgemeinschaft Dokumentarfilm e.V. (AG Dok) hat ein Dokumentarfilmer erfolgreich gegen YouTube-Mutter Google geklagt. Ein Dokumentarfilm des Klägers war bei dessen Fernsehausstrahlung im öffentlich-rechtlichen Fernsehen von einem Zuschauer aufgezeichnet und bei YouTube hochgeladen worden. Der Produzent des Films machte YouTube auf den Rechteverstoß aufmerksam und forderte die Löschung des betreffenden Inhalts.

Statt jedoch gegen die offenkundige Urheberrechtsverletzung vorzugehen und den Inhalt zu entfernen, bat YouTube den illegalen Uploader mit dem kämpferischen Nutzernamen „Revo Luzzer“ um seine Stellungnahme. Dieser gab gegenüber YouTube begründend an, als Zahler des Rundfunkbei-

trags sei er Miteigentümer des gesendeten Films geworden und könne damit machen, was er wolle. Diese einseitige Rechtsauslegung akzeptierte YouTube, die Löschung unterblieb folglich. Nachdem auch eine Abmahnung des Produzenten, der dabei von der Berliner Urheberrechtskanzlei KVlegal und von der AG Dok unterstützt wurde, keine Wirkung zeigte, reichte er vor dem Landgericht Leipzig Klage ein.

Nun brachte ein Urteil in diesem Fall (Aktenzeichen 05 O 661/15) Klarheit: Das Gericht vertritt die Ansicht, dass „Die Beklagte", also YouTube, „ihre zumutbaren Prüfpflichten verletzt" habe, „weil sie nach dem Hinweis des Klägers im Rahmen des Beanstandungsverfahrens nicht alles ihr technisch und wirtschaftlich Zumutbare getan hat, um weitere Rechtsverletzungen im Hinblick auf die geschützten Werke zu verhindern". Ferner hätte YouTube „unverzüglich mit dem Ziel tätig werden müssen, die Darstellung des Werkes zu entfernen oder den Zugang zu sperren, sobald sie die erforderliche Kenntnis erlangt hatten". Zudem stellte das Gericht fest, dass die Prüfpflicht bereits gegeben sei, wenn unter Vorlage „aller erforderlicher Angaben" auf eine klare Rechtsverletzung hingewiesen worden war. Diese Prüfung hätte nach Ansicht des Gerichts zwingend „zu einer Löschung führen müssen, da die Zahlung von GEZ-Gebühren offensichtlich nicht zum Erwerb von Veröffentlichungsrechten führt".

KARTELLAMT NIMMT KAMPF GEGEN ABZOCKE IM INTERNET AUF

Im Kampf gegen Online-Abzocke bekommt das Bundeskartellamt mit einer Gesetzesnovelle künftig mehr Rechte beim Verbraucherschutz. So können im Bereich der Internetkriminalität in Zukunft Untersuchungen gegen ganze Branchen geführt werden.

Dank einer entsprechende Änderung am Gesetz gegen Wettbewerbsbeschränkungen (GWB), die am vergangenen Freitag in Kraft getreten ist, darf das Bundeskartellamt künftig Untersuchungen gegen ganze Branchen einleiten, wenn es Hinweise auf die Benachteiligung von Verbrauchern gibt. Zudem darf das Bundeskartellamt nun vor Gericht mit ihrem Fachwissen Stellungnahmen abgeben. Kartellamtspräsident Andreas Mundt begrüßte die Gesetzesanpassung: „Wir begrüßen es, dass der Gesetzgeber uns in einem ersten Schritt neue Untersuchungsinstrumente im Bereich des Verbraucherschutzes übertragen hat. Gerade in der Internetwirtschaft gibt es Fälle, in denen Unternehmen durch eine einzige rechtswidrige Maßnahme Millionen Verbrauchern auf einmal schaden können", erklärte er am Montag. Die Behörde werde deshalb eine neue Abteilung einrichten, um die Verbraucherzentralen zu unterstützen. Die Leitung der neuen Abteilung übernimmt Carsten Becker, der bislang für den Energie- und Mineralölsektor verantwortlich war.

Direkte Sanktionsmöglichkeiten, wie etwa das Abschöpfen widerrechtlicher Gewinne, hat das Kartellamt mit dem Gesetz allerdings nicht erhalten. Die Diskussion über die Befugnisse der Behörde werde sicher nach der Bundestagswahl weitergehen, sagte dazu ein Behördensprecher.

Das Kartellamt setzt sich schon seit längerer Zeit dafür ein, mehr Kompetenzen im Verbraucherschutz zu bekommen und verweist dabei auf entsprechende Regelungen im europäischen Ausland und den USA. Mehr Personal ist bei der Behörde wegen der Rechtsänderung vorerst nicht geplant, wie der Sprecher bekannt gibt. Das Bundeskartellamt hat derzeit rund 350 Mitarbeiter. In den vergangenen Jahren hatte das Amt nach eigenen Angaben in Sektoruntersuchungen mehrere wettbewerbsbezogene Beschränkungen ausgemacht, so bei Tankstellen, der Fernwärmeversorgung, dem Milchmarkt und Ablesediensten.

Matthias Machnig (SPD), Staatssekretär im Bundeswirtschaftsministerium, erklärt: Mit den Änderungen am Gesetz gegen Wettbewerbsbeschränkungen habe die Regierung ein „modernes Wettbewerbsrecht für unser digitales Zeitalter" geschaffen. „Bei der Erarbeitung der Novelle hatten wir die Herausforderungen im Blick, die sich durch die Digitalisierung im Wettbewerb stellen".

OLG MÜNCHEN: UPLOADED.NET HAFTET NICHT AUF SCHADENSERSATZ

Das OLG München hat kürzlich zum Vorteil des Sharehosters Uploaded.net geurteilt. Zwar müsse die Betreibergesellschaft auf Unterlassung haften, in diesem Fall aber nicht auf Schadensersatz. Begründung: Die Cyando AG habe sich an keinen strafbaren Handlungen Dritter beteiligt. Uploaded.net wurde

durch das Urteil aber nicht ausnahmslos von der Haftung befreit. Das Gericht hat diesbezüglich Ausnahmen festgelegt.

Rechtsanwalt Dr. Martin Bahr hielt in seinem Beitrag fest, dass der Sharehoster Uploaded.net im vorliegenden Fall nicht auf Schadenersatz für fremde Urheberrechtsverletzungen haftet (OLG München, Urt. v. 02.03.2017 – Az.: 29 U 1799/16).

Mehrere Rechteinhaber hatten in der Vergangenheit vielfach den rechtswidrigen Upload von Musik- und Filmwerken angezeigt, an denen die Uploader keine Rechte besaßen. Die Kläger beanstandeten nun vor dem OLG München, dass die Cyando AG (Betreiber von Uploaded.net) keine ausreichenden Vorkehrungen getroffen habe, um Re-Uploads, also das erneute Hochladen des gleichen Werkes, zu vermeiden. Man versuchte in der Folge den Betreiber auf Schadenersatz in Anspruch zu nehmen.

Die darunter liegende Instanz, das LG München I (Urteil vom 10.08.2016 – Az.: 31 O 6197/14), hatte in solchen Fällen eine Schadensersatzpflicht bejaht. Die Richter des OLG München schlossen sich im aber vorliegenden Fall nicht dieser Meinung an. Zwar hafte das Schweizer Unternehmen auf Unterlassung, nicht aber auf Schadensersatz.

uploaded.net symbolBegründung: Es könne nicht festgestellt (was wohl bedeuten soll: bewiesen) werden, dass Uploaded.net sich an den fremden, strafbaren Handlungen in irgendeiner Form beteiligt habe. Für die Begründung eines Schadensersatz-Anspruches reiche es nicht aus, wenn es dort in der Vergangenheit vermehrt zu Urheberrechtsverletzungen gekommen sei. Die Tätigkeit der Cyando AG ist nach Ansicht des OLG München grundsätzlich nicht auf Rechtsverstöße ausgerichtet, sondern inhaltlich neutral. Das klingt für das Unternehmen nach einer Entwarnung. Doch für die Regel wurden im Urteil auch Ausnahmen festgelegt, Uploaded.net ist somit nicht ausnahmslos aus der Haftung raus:

„Dies bedeutet nicht, dass die Beklagte in keinem Fall als Gehilfin haftet (…). Ein entsprechender konkret auf die rechtswidrige Handlung bezogener Vorsatz kann etwa dann vorliegen, wenn der Anbieter nach Verletzungshinweis keine Maßnahmen zum Schutz des betroffenen Werkes trifft und dies z. B. dazu führt, dass das betroffene Werk nach Löschung der Datei wiederholt durch denselben Nutzer zeitnah wieder über seine Plattform öffentlich zugänglich gemacht wird.

Erhält der Anbieter Kenntnis von wiederholten Urheberrechtsverletzungen desselben Werkes und stellt fest, dass diese jeweils durch den gleichen Nutzer erfolgten und sperrt gleichwohl nicht dessen Account, ist von einer Kenntnis des Anbieters hinsichtlich weiterer etwaiger konkreter Haupttaten auszugehen.

Vorliegend bestehen aber keine Anhaltspunkte dafür, dass die Beklagte hinsichtlich der streitgegenständlichen Werke Kenntnis von konkret drohenden Haupttaten hatte.“

Das heißt auf Deutsch: Wer als Sharehoster die Re-Uploads seiner Nutzer nicht mit einer Account-Sperre bestraft, kann in Bezug auf den Schadenersatz eben doch in Haftung genommen werden. Das würde zumindest unter anderem das vermehrte Sperren von Uploader-Accounts erklären, was nach meiner Meinung auch mit dem drohenden Gerichtsverfahren vor dem Bundesgerichtshof zusammenhängt. Im April dieses Jahres haben sich in mehreren Untergrund-Foren zahlreiche Uploader darüber beschwert, dass nebst ihrer rechtsverletzenden Dateien auch ihre Accounts mit sofortiger Wirkung über den Jordan geworfen wurden. Der Grund für das straffe Vorgehen ist schnell erklärt: Wenn man der Cyando AG vor Gericht nachweisen kann, dass sie nicht angemessen auf die Wiederholung der Urheberrechtsverletzungen ihrer Nutzer reagiert hat, kann es für die Betreiber so richtig teuer werden (siehe auch der Podcast unten aus April 2017).

CHEMICAL LOVE: MEHRJÄHRIGE HAFTSTRAFEN FÜR ONLINE-DROGENHÄNDLER

Die mutmaßlichen Betreiber einer der größten europäischen Online-Drogenversandringe müssen sich seit März vor dem Landgericht Landau verantworten. Nun ist das Urteil im Prozess um ChemicalLove.to gefallen. Der Hauptbeschuldigte Nicolas K.(30) wurde zu einer Haftstrafe von 14 Jahre und zehn Monaten verurteilt, die beiden Mittäter, die Brüder René L. (32) und Dennis T. (30) müssen für je sieben Jahre und drei Monate in Haft.

Zusätzlich zu der Haftstrafe soll Nicolas K., der Sohn eines früheren Stuttgarter Bundesliga-Fußballers, zehn Millionen Euro an die Staatskasse zahlen, obwohl die damaligen Einnahmen auf 1,3 Millionen Euro geschätzt wurden. Da jedoch die Kunden ausschließlich mit Bitcoins bezahlten, wurde die zwischenzeitliche Wertsteigerung des Bitcoin gleich mit berücksichtigt. Das Gericht ordnete zudem an, dass alle drei von einem gewissen Zeitpunkt der Haft an in einer Entziehungsanstalt untergebracht werden. Nicolas K. habe laut eigener Aussage Drogen in „extremen“ Ausmaßen konsumiert, am Ende bis zu vier Gramm Kokain pro Tag. Das Urteil entsprach weitgehend der Forderung von Staatsanwalt Alexander Fassel.

Mit Werbesprüchen wie: „Höchste Qualität, diskrete Verpackung, günstige Preise“ oder „Wir kennen alle Tricks“ brachte Europas größter Online-Drogenversand Chemical Love (Spitzname: „Zalando für Drogen“) Produkte an seine Kunden. So konnten u.a. Designerdrogen, Psychedelika, Kokain, Ecstasy, Heroin, Crystal Meth, LSD und Amphetamine in dem zumeist deutschsprachigen Forum von Chemical Love bequem nach Hause geordert und mit Bitcoin bezahlt werden. Mehr als 1500 Verkäufe sollen per Post verschickt worden sein. Laut der Staatsanwaltschaft war es der größte Drogen-Webshop Deutschlands.

Obwohl Chemical Love nicht nur im Darknet, sondern auch im Clearnet seine Ware anbot, schien der Shop lange Zeit für die Behörden uneinnehmbar. Im Frühling des vergangenen Jahres kam das Geschäft dann jedoch plötzlich ins Stocken – der Händler schien verschwunden und reagierte nicht mehr auf Anfragen. Nach einer Razzia am 14. April 2016 im pfälzischen Rülzheim saßen nun die drei mutmaßlichen Hintermänner in Landau vor Gericht. Als die Beamten im April vergangenen Jahres das Depot der Bande in Rülzheim durchsuchten, fanden sie neben dem Trio und anderen Beweisen auch eine stattliche Menge Stoff: 55 Kilo Amphetamine, 25.000 XTC-Pillen, 1,3 Kilo Kokain und 4 Kilo Heroin. Das meiste in „sehr guter Qualität“, wie die Staatsanwaltschaft bestätigte.

Die Staatsanwaltschaft wirft den Männern vor, zwischen Januar 2015 und April 2016 über 100 Kilo Drogen nach Deutschland geschmuggelt und von dort aus gewerbsmäßig verkauft zu haben. Den Großteil des Stoffs sollen sie aus den Niederlanden beschafft haben, das Crystal Meth aus Tschechien.

Der Hauptangeklagte Nicolas K. soll unter dem Alias z100 die Fäden hinter Chemical Love gezogen haben: Als Mastermind hinter der Organisation soll er die Mitangeklagten Dennis T. und dessen Bruder René L. erst für sein Business angeworben haben, sie hätte er – wie auch seinen Vater – zur „Umsetzung seines Tatplans“ gebraucht, wie es Staatsanwalt Alexander Fassel formuliert. Ihm wird zur Last gelegt, dass er nicht nur als Verantwortlicher den Online-Drogenshop nach Vorbild der Webseite Silk Road aufgebaut hat, sondern auch persönlich für die Beschaffung der Drogen verantwortlich war. Die beiden mitangeklagten Brüder waren als Kuriere und Versandabfertiger tätig.

Nicolas K. soll mehrere Fahrten in die Niederlande organisiert haben und dazu unter anderem von seinem Vater, einem ehemaligen Stuttgarter Fußballprofi, begleitet worden sein. Auch gegen den Vater des Hauptangeklagten wird im Zusammenhang mit dem Drogenhandel ermittelt. Das Verfahren wurde aber abgetrennt. Zudem hatte die Stuttgarter Staatsanwaltschaft wegen des Vorwurfs des Anlagebetrugs Ermittlungen gegen den Ex-Bundesligaprofi aufgenommen. Er wird sich dazu in einem gesonderten Verfahren vor Gericht verantworten müssen. Vater und Sohn brachten die Drogen über die Grenzen und zu einem Lager, das die beiden Mitangeklagten organisierten.

Digital

Themenübersicht

E-BOOK-MARKT STAGNIERT WEITERHIN

Pünktlich zum Quartalsende veröffentlicht der Börsenverein des Deutschen Buchhandels e.V. erneut seinen E-Book-Quartalsbericht. So ist beim Absatz von E-Books am Publikumsmarkt im ersten Quartal 2017 ein leichter Anstieg um 0,2 Prozent zu verzeichnen. Die Kaufintensität steigt sogar deutlich. Der Umsatz sinkt um 3 Prozent. Mit einem Anteil von 5,6 Prozent Umsatz am Publikumsmarkt ist das E-Book allerdings weiterhin nur ein Nischenprodukt.

Vierteljährlich gibt der Börsenverein des Deutschen Buchhandels e.V. in Zusammenarbeit mit GfK Entertainment die neuesten Ergebnisse der Entwicklungen auf dem E-Book-Markt bekannt. Für aussagefähige Zahlen, wie die Hochrechnungen der E-Book-Absätze und -Umsätze, sorgt das GfK Consumer Panel Media*Scope Buch. In Form einer schriftlichen, repräsentativen Umfrage (ca. 60% Online – Anteil steigend + 40% Paper & Pencil) mittels Tagebuch, das von 25.000 Panelteilnehmern selbst kontinuierlich geführt wird, werden alle Einkäufe im Buchmarkt von diesen deutschen Privatpersonen ab 10 Jahren erfasst. Die Ergebnisse werden auf die Grundgesamtheit der deutschen Bevölkerung (67,7 Mio. Menschen) ab 10 Jahre hochgerechnet.

Der Börsenverein vergleicht in diesem Quartal den Markt mit ruhigen Gewässern, denn der Absatz von E-Books am Publikumsmarkt (ausgenommen sind Schul- und Fachbücher) stieg nur leicht um 0,2 Prozent an. Der Umsatzanteil am Publikumsmarkt steigt von 5,4 Prozent auf 5,6 Prozent im Vergleich zum Vorjahresquartal. Der E-Bookumsatz sinkt insgesamt jedoch um 3 Prozent. Dieser Rückgang bei gleichzeitig steigendem Umsatzanteil resultiert daraus, dass der Umsatz mit Büchern am Publikumsmarkt im ersten Quartal insgesamt rückläufig war. Zudem sinken die im Durchschnitt für E-Books bezahlten Preise, so dass es trotz leicht höherem Absatz insgesamt kein Umsatzplus gibt.

Die Kaufintensität steigt um satte 19,2 Prozent gegenüber dem Vergleichszeitraum, das heißt, wer bereits E-Book-Käufer ist, erwirbt im ersten Quartal 2017 im Durchschnitt 4,4 E-Books aus dem Publikumsbereich. Die Zahl der E-Book-Käufer sinkt im Vergleich zum Vorjahreszeitraum: 1,9 Millionen Kunden kauften im ersten Quartal 2017 mindestens ein E-Book, im Vorjahreszeitraum waren es 2,2 Millionen.

Fazit

Trotz zahlreicher, ansprechender Angebote auf dem E-Book-Markt, denn nahezu jedes gedruckte Buch erscheint gleichzeitig auch als E-Book, ist es bisher offenbar nicht gelungen, mehr Leser für E-Books zu begeistern. Ein Grund dafür könnte in den sehr hohen Preisen liegen, die Verlage für ihre Neuerscheinungen verlangen, die zum Teil nur geringfügig unter den Preisen der Druckversion liegen. So bleibt das Papierbuch immer noch nahezu konkurrenzlos weiterhin die absolute Nummer 1 für alle lesebegeisterten Buchfreunde.

Da können auch die unzähligen Vorteile des E-Books am Ende kaum punkten, zu nennen wären insbesondere das sehr geringe Gewicht eines E-Book-Readers, etwa 180 Gramm und die hohe Platzeinsparung, denn der Reader bietet gleich Raum für eine ganze Bibliothek an elektronischen Büchern. Auch sind solche Features, wie eine variabel einstellbare Schriftgröße, die integrierten Wörterbücher, die Suchfunktion für markierte Lieblingszitate, sehr nützlich.

Natürlich haben die Druckexemplare ebenso ihre Vorzüge. So gibt es besonders fantasievolle Cover und spezielle Ausgaben sehen einfach dekorativ aus im Buchregal. Bücher lassen sich sehr gut verschenken und der unvergleichliche Geruch nach bedrucktem Papier lässt Buchfreunde doch immer wieder gerne tief durchatmen.

Es scheint sich jedoch um einen neuen Trend zu handeln, der wohl auch bei uns angekommen ist: „Echte Bücher“ erleben demnach ein Comeback. Sowohl in Großbritannien als auch den USA sind die Verkäufe von elektronischen Büchern zuletzt um fast 20 Prozent zurückgegangen. Gedruckte Bücher konnten hingegen zulegen, berichtete CNN Money. Wie groß allerdings der Anteil der Selfpublisher und Kleinverleger ist, bleibt in dieser Studie leider außen vor. Denkbar wäre deshalb, dass klassische Verlage bei E-Books absinken, weil Einzelpersonen und Miniverlage so erfolgreich sind. Nirgends genannt werden außerdem E-Book-Flatrates, wie Kindle Unlimited. Die Auswirkungen auf den Gesamtmarkt wären dabei ebenso interessant. Aber auch Gerätehersteller haben bereits seit längerem mit sinkenden Verkaufszahlen zu kämpfen. Die

Verkäufe von E-Readern gingen laut den Marktforschern von Euromonitor International seit 2011 um 40 Prozent zurück.

Der leichte Anstieg des Absatzes von E-Books am Publikumsmarkt im ersten Quartal und die erhöhte Kaufintensität könnten zum Teil zurückzuführen sein auf das doch attraktive Angebot an Neuerscheinungen. So wären hier insbesondere die folgende Bücher zu nennen: von Sebastian Fitzek: Achtnacht, von Jussi Adler-Olsen: Selfies, von Rebecca Gablé: Die fremde Königin und von Jeffrey Archer: Die Wege der Macht.

Facebook: Mit künstlicher Intelligenz gegen Terrorinhalte

Beim Kampf gegen Terror-Propaganda setzt Facebook künftig auch auf selbstlernende Algorithmen. So will Facebook mit Hilfe von Algorithmen zur Bild- und Texterkennung Propaganda von Terroristen schneller aufspüren. Die Initiative soll Anti-Facebook-Gesetze verhindern.

Facebook-Managerin Monika Bickert, die zuvor unter anderem Staatsanwältin in den USA war, erklärt in einem Blogeintrag am Donnerstag, dass es darum gehe, bereits bekannte Bilder und Videos beim erneuten Hochladen zu stoppen. Das soziale Netzwerk experimentiere aber zugleich mit Software, die automatisch eine terroristische Einstellung in Texten erkennen solle. Eine aktuelle Auswertung von Einträgen, die wegen der Unterstützung von Terror-Organisationen, wie Isis oder Al-Kaida, bereits gelöscht wurden, würde genutzt, um einen lernfähigen Algorithmus zu füttern, Posts mit solcher Ausrichtung selbst zu erkennen. Neben Englisch laufe die Arbeit zudem in weiteren Sprachen, auch aus dem arabischen Raum, gab Bickert bekannt.

Die Managerin hob hervor, dass sie zum Ziel hätten: „terroristische Inhalte sofort [zu] entdecken, bevor Menschen in unserer Community sie zu sehen bekommen“. Brian Fishman, dessen Aufgabe beim Online-Netzwerk die Terrorbekämpfung ist, meint dazu: „Wir arbeiten daran, diese Systeme schneller und verlässlicher zu machen.“ Zugleich sei es ein Katz-und-Maus-Spiel: „Wenn wir verhindern, dass Terroristen unsere Plattform erreichen, versuchen sie, neue Wege zu finden.“ Es gebe „keinen Schalter, mit dem man Terrorismus einfach abstellen kann“.

Monika Bickert teilt weiterhin mit, dass inzwischen mehr als die Hälfte der wegen Terror-Propaganda gelöschten Facebook-Accounts vom Netzwerk selbst entdeckt werde. Dennoch wäre Facebook auf Hinweise von Nutzern bezüglich illegaler oder beim Netzwerk untersagter Inhalte angewiesen, denn: «Auch wenn unsere Software immer besser wird, hängt sehr viel auch vom Kontext ab», schränkte Bickert ein. Wenn zum Beispiel in einem Video Isis-Symbole zu sehen seien, könne es sich um Terror-Propaganda oder aber auch um einen Nachrichtenbeitrag handeln. Hier seien im Moment Entscheidungen von Menschen unverzichtbar. Eine Ausnahme ist Kinderpornografie, gegen die unter anderem mit automatisierter Software gekämpft wird.

Ansonsten wird in dem Blogeintrag darauf hingewiesen, dass die so gewonnenen Erkenntnisse aus der Facebook-Plattform zugleich auch übergreifend verwendet werden sollen, um Profile mit terroristischen Inhalten bei anderen Diensten des Online-Netzwerks, wie Instagram und WhatsApp, zu finden. Daher sei es angeraten, dass einzelne Apps Daten an Facebook weiterreichen können. Facebooks Versuch, Zugriff auf einige Informationen von WhatsApp-Nutzern zu bekommen, wurde im vergangenen Jahr in Europa von Datenschützern blockiert.

Die härtere Vorgehensweise im Kampf gegen terroristische Propaganda bei Facebook ist zurückzuführen auf den, vor allem in Europa, gewachsenen politischen Druck. So erklärte die britische Premierministerin Theresa May nach dem jüngsten Attentat auf der London Bridge, Extremismus finde im Netz eine sichere Brutstätte – und die großen Internetunternehmen ließen dies zu. Erst unlängst sprach sich Facebook gegen das von Justizminister Heiko Maas (SPD) geplante Gesetz gegen Hass und Hetze im Netz aus. Das Netzwerk befürchtet, dass am Ende zur Sicherheit auch legitime Beiträge entfernt werden könnten.

DATENDIEBSTAHL: APPLE-MITARBEITER IN CHINA FESTGENOMMEN

22 Personen sollen in China persönliche, sensible Kundendaten des Technologieriesen Apple gestohlen und weiterverkauft haben. Dadurch ist ein Schaden in Millionenhöhe entstanden. Bei

den Tätern habe es sich auch um Mitarbeiter des iPhone-Konzerns gehandelt. Es ist bisher nicht bekannt, ob es sich um die Daten chinesischer oder ausländischer Nutzer handelt, berichtet Engadget.

Wie die Polizei in der Provinz Zhejiang mitteilte, wurden 22 Verdächtige festgenommen, darunter 20 Angestellte von Apple China, die im Direktmarketing und Outsourcing tätig waren. Ihnen wird vorgeworfen, persönliche Daten von iPhone- und Mac-Nutzern entwendet zu haben, wie Namen, Telefonnnummern und Apple-IDs. Dafür sollen sie eine interne Datenbank des Konzerns abgefragt und die Daten anschließend auf dem Schwarzmarkt gewinnbringend veräußert haben.

Für die Datensätze, die unter anderem die Kombinationen von Apple-ID-Nutzernamen, Telefonnummern und andere Angaben enthielten, wurden auf dem Schwarzmarkt immerhin zwischen 10 und 180 Yuan gezahlt, was umgerechnet 1,30 bis 23,50 Euro pro Datensatz entspricht. Bis die Sache auffiel, sollen die Beschuldigten zusammengenommen bereits einen Betrag von über 50 Millionen Yuan (6,5 Millionen Euro) erwirtschaftet haben.

Bisher noch völlig unbekannt ist, wie viele Nutzer von dem Datendiebstahl betroffen sind. Ebenso unklar ist zum jetzigen Zeitpunkt, ob es sich um die Daten chinesischer oder ausländischer Nutzer handelt. Ebenso zu klären wäre, auf welche internen Datenbanken die Mitarbeiter Zugriff hatten und wer die Empfänger dieser Daten gewesen sind.

Klar ist hingegen, dass es schwierig werden dürfte, konkrete Schlussfolgerungen aus der Sache zu ziehen, mit denen vergleichbare Taten zukünftig unterbunden werden können. Denn hier ist es sicherlich nicht damit getan, den Zugang zu den Daten deutlich einzuschränken. Das könnte den Kundendienst weltweit vor ein großes Problem stellen. Denkbar wäre, solche Verfahren zum Einsatz zu bringen, die auffällige Datenabfragen eher erkennen. Vermutlich wird man aber einfach damit leben müssen, dass es nicht vertrauenswürdige Insider in Unternehmen gibt.

Das Netzwerk der Kriminellen wurde nach Angabe der Behörden zerschlagen. Der Polizei zufolge gingen den Festnahmen, die bereits am vergangenen Wochenende in vier Provinzen stattfanden, monatelange Ermittlungen voraus.

WIKILEAKS: 10.000 DOLLAR KOPFGELD AUF EINEN JOURNALISTEN

WikiLeaks hat ein Kopfgeld von 10.000 Dollar für die Identität des Reporters ausgesetzt, der die Whistleblowerin Reality Winner nicht geschützt hat, was in der Folge zu ihrer Verhaftung führte. Sie ist die mutmaßliche Quelle eines geheimen Berichts der NSA, laut dem der russische Geheimdienst GRU versuchte, in die Systeme eines der Produzenten von Software für die Wahlorganisation einzudringen.

Reality Winner, Angestellte eines privaten NSA-Dienstleisters, leitete einen Top-Secret-Bericht der NSA an The Intercept weiter. Aus dem Bericht geht hervor, dass die NSA glaubt, der russische Militärgeheimdienst GRU stecke hinter den Phishing-Attacken auf US-Wahlbehörden im Vorfeld der letzten US-Wahl. Nur zwei Tage nachdem The Intercept einen entsprechenden Artikel veröffentlichte, wurde die NSA-Mitarbeiterin verhaftet und wegen Geheimnisverrats angeklagt.

The Intercept hatte den Leak nicht nur für einen Artikel verwendet, sondern auch direkt bei den Behörden um Stellungnahme gebeten: Laut Gerichtsakte schickte der Journalist einem Geheimdienstler Fotos des geheimen NSA-Berichts, mit der Frage, ob das Dokument echt sei. Diese hatten den Drucker, mit dem die Originaldokumente ausgedruckt wurden, aufgrund der digitalen Punktsignatur erkannt und so ihre Sicherheitslücke ausmachen können und eindeutig als Reality Winner identifiziert. Zudem geht aus dem Antrag auf Haftbefehl gegen Winner hervor, dass dieser Journalist den NSA-Dienstleister informierte, von wo das Dokument laut Poststempel abgesendet war: Augusta, Georgia, dem Sitz von Winners Arbeitgeber.

WikiLeaks macht Matthew Cole, den ersten von insgesamt vier Autoren des Artikels, für die schnelle Verhaftung Reality Winners verantwortlich. Er soll seine Quelle nicht ausreichend geschützt haben und dabei höchst fehlerhaft vorgegangen sein. Cole ist langjähriger Mitarbeiter bei The Intercept. Bereits 2007 soll Mathew Cole ein ähnliches Missgeschick passiert sein: Es hat sich eine weitere Ex-Quelle von ihm zu Wort gemeldet, John Kiriakou. Dieser war CIA-Agent und legte Waterboarding-Fol-

terungen durch die CIA und den Namen eines CIA-Mitarbeiters offen. Daraufhin wurde er zu 30 Monaten Haft verurteilt. Auch in seinem Fall wirft er Cole unzureichenden Informantenschutz vor.

WikiLeaks hat aktuell in einem Tweet vom Dienstag 10.000 Dollar Belohnung für Informationen ausgeschrieben, die zur „öffentlichen Bloßstellung und Entlassung dieses ‚Reporters' führen". WikiLeaks benutzt dabei den englischen Begriff „termination", der neben Entlassung auch Tötung bedeuten kann. Nur kurze Zeit danach meldete sich der im Exil lebende Wikileaks-Gründer Julian Assange über Twitter und verwendet die gleiche zweideutige Wortwahl: „Meistens liebe ich @ TheIntercept, aber wenn das Euer Kerl ist, nennt ihn beim Namen, beschämt ihn öffentlich und entlasst (terminate) ihn."

Offensichtlich will WikiLeaks-Gründer Julian Assange hier besonders öffentlichkeitswirksam ein Exempel für den Schutz von Quellen statuieren. Er dürfte aber mit WikiLeaks ohnehin von dem Fall profitieren, denn potentielle Whistleblower werden sich von The Intercept in Zukunft eher fernhalten, wenn sie mit geheimen Dokumenten an die Öffentlichkeit gehen wollen.

In einem Statement verwies The Intercept darauf, dass die Aussagen der Regierung über eine mögliche Beteiligung eines ihrer Reporter „unbewiesene Behauptungen und Spekulation, die der Agenda der Regierung dienen soll" enthielten. Man wisse ja selbst nicht, ob Winner wirklich die Quelle gewesen sei.

Währenddessen bleibt die 25jährige Reality Winner auch weiterhin in Haft. In einer Gerichtsverhandlung in Georgia am Donnerstag wurde festgelegt, dass sie nicht auf Kaution freikommt. Wie US-Medien berichten, hat sich die Frau bei der Gelegenheit nicht schuldig bekannt. Nach Angaben der Staatsanwaltschaft gab die 25-Jährige am Donnerstag während einer Anhörung in Augusta im US-Bundesstaat Georgia allerdings zu, ein vertrauliches Dokument an ein Medium weitergegeben zu haben.

THOMAS DE MAIZIÈRE: MIT „METHODE FAHRRADHELM" ZU MEHR CYBERSICHERHEIT

Bundesinnenminister Thomas de Maizière räumte die Möglichkeit ein, dass die Bundesregierung Unternehmen härtere Auflagen in Fragen der Cybersicherheit erteilen könnte, wenn sie selbst in dieser Hinsicht nicht genug unternehmen: „Es kann sein, dass der Zeitpunkt kommt, dass die Öffentlichkeit darum bittet, dass wir bestimmte Sicherheitsvorkehrungen vorschreiben", meint er. Zugleich schränkt er jedoch ein: „So weit sind wir noch nicht".

Das Thema Bedrohung durch Cyberangriffe war zuletzt durch den Erpressungstrojaner „WannaCry" verstärkt in den Schlagzeilen, wobei dieser Angriff enormen Schaden angerichtet hat: Die Computer gleich mehrerer britischer Krankenhäuser waren davon genauso infiziert wie die des Autoherstellers Renault und der Deutschen Bahn. Dabei waren nur diejenigen Computer betroffen, bei denen eine seit Monaten bekannte Software-Schwachstelle nicht durch neue Updates geschlossen wurden. Der Fokus hat sich aufgrund dieser Tatsache, gerade weil auch viele große Unternehmen involviert waren, auf den Schutz vor Cyberangriffen gerichtet.

Für Thomas de Maizière bot sich hier ein Vergleich der IT-Sicherheit mit der Helmpflicht an: Es gebe die Helmpflicht für Motorradfahrer – aber zugleich seien auch viele Radfahrer und Skifahrer mit Helmen unterwegs und das reiche aus. Der deutsche Innenminister will die Regeln für IT-Sicherheit gegenwärtig noch nicht ausweiten und setzt auf die „Methode Fahrradhelm": Hoffen auf genug Einsicht. Mit Blick auf die Vorschriften zur Cybersicherheit sagte der Minister: "Im Moment setze ich auf die Methode Fahrradhelm."

Derzeit fordern Unternehmen weiterer Branchen, wie Logistik, ebenfalls als kritische Infrastruktur betrachtet zu werden. Die Liste werde in Zukunft möglicherweise neu gefasst werden müssen. Dieter Kempf, Präsident des Bundesverbandes der Deutschen Industrie (BDI), mahnte jedoch zur Vor-

sicht bei einer Ausweitung dieser Liste: „Ich halte es für gefährlich.“ Kempf und de Maizière traten auf einer Veranstaltung der Initiative Wirtschaftsschutz in Berlin auf.

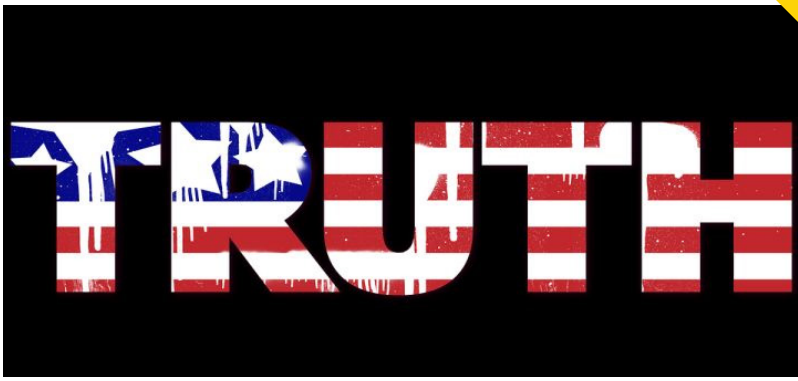
Allianz-Manager Hartmut Mai warnte: „„WannaCry” habe auch gezeigt, dass eine Cyberattacke schnell weltweit alle Unternehmen betreffen könne. Solche Angriffe könnten „die gesamte Versicherungsindustrie an die Grenzen des Darstellbaren bringen”. Die Branche bietet Versicherungen gegen Cyberrisiken an, die sowohl Haftungsrisiken als auch die Kosten von Betriebsausfällen abdecken. Das Geschäft steht aber erst am Anfang: Nach Branchenschätzungen summierten sich die Einnahmen im vergangenen Jahr in Deutschland auf 50 Millionen Euro und europaweit auf 200 Millionen Euro.

Hans-Georg Maaßen, Präsident des Bundesamtes für Verfassungsschutz, empfiehlt, eine mögliche Radikalisierung von Mitarbeitern im Blick zu behalten. „Von Unternehmen erwarte ich, was ich von jedem Bürger erwarte: ein aufmerksames Auge. Wenn man etwas sieht, soll man etwas sagen.”

WHISTLEBLOWER GESUCHT: MICHAEL MOORE STARTET ENTHÜLLUNGSPLATTFORM „TRUMPILEAKS“

Über seine am Dienstag ins Leben gerufene Webseite „Trumpileaks“ ruft Michael Moore zu Enthüllungen bezüglich des US-Präsidenten Donald Trump auf. Berechtigt, sich daran zu beteiligen, sind „patriotische Amerikaner in der Regierung, der Strafverfolgungsbehörde oder dem privaten Sektor, die Wissen haben über Verbrechen, Lügen und generelle Vergehen von Donald Trump und seinen Verbündeten“. Die potentiellen Whistleblower können auf dieser Plattform anonym über verschlüsselte Kommunikationswege brisante Informationen, Dokumente, Fotos, Videos und Audiodateien an Moore und sein Team schicken.

Der durch seine Filme Roger & Me, Bowling for Columbine und Fahrenheit 9/11 populär gewordene US-Regisseur und Autor Michael Moore wollte im Wahlkampf mit der Doku „Michael Moore in Trumpland“ erneut Einfluss auf die aktuelle Politik nehmen. Jetzt legt er mit einer Enthüllungsplattform nach, mit „Trumpileaks“ führt Michael Moore seinen Anti-Trump-Feldzug fort. Moore initiierte damit eine Online-Offensive, worin er „Verbrechen, Lügen und allgemeines Fehlverhalten“ Trumps und seiner Mitarbeiter aufdecken möchte, um „die Vereinigten Staaten vor der Tyrannei eines Einzelnen“ zu bewahren. Auf



der Website beschreibt Moore verschiedene verschlüsselte Messenger-Apps und andere Möglichkeiten, anonym mit ihm und seinem Team in Kontakt zu treten. Hundertprozentig sicher sei keine Form der digitalen Kommunikation, aber die zur Verfügung gestellten Werkzeuge seien die sichersten, die es gibt.

Die Website kam fast zeitgleich zur Festnahme der 25-jährigen Whistleblowerin Reality Winner, die vertrauliche Informationen des Geheimdienstes NSA an „The Intercept“ weitergegeben haben soll. Trump hatte angekündigt, mit aller Macht gegen Leaks und die Weitergabe geheimer Informationen vorzugehen.

Moore begründete sein Angebot damit, dass er mit „Trumpileaks“ das Ansinnen der Gründungsväter der USA vertrete, sich gegen jede Form der Tyrannei zur Wehr zu setzen. Natürlich ist ihm aber auch das Wagnis seiner ins Leben gerufenen Initiative bewusst: „Es könnte gefährlich werden. Es könnte uns in Schwierigkeiten bringen. Aber uns läuft die Zeit davon. Wir müssen handeln. Es ist unsere patriotische Pflicht“, schreibt er in einem auf huffingtonpost veröffentlichten öffentlichen Brief. Weiter heißt es darin: „In der Zeit, in der ihr den Brief anfangt zu lesen, bis zu dem Moment, wo ihr unten angekommen seid, kann es gut sein, dass Donald Trump die Verfassung verletzt, die Gerechtigkeit behindert, das amerikanische Volk belogen, Gewalttaten unterstützt oder begangen hat oder einen schrecklichen Fehler begeht, der die politische Karriere eines anderen Politikers beendet (oder mich oder dich ins Gefängnis schickt). Und wie immer in der Vergangenheit wird er damit davonkommen. Donald Trump glaubt, dass er über dem Gesetz steht.“

In einem folgenden Appell ruft Michael Moore zum Handeln auf: „Macht keinen Fehler – Donald J. Trump hat nicht die Absicht, das Weiße Haus vor dem 20. Januar 2025 zu verlassen. Deshalb sei es „patriotische Pflicht“ zu handeln. „Ich weiß, dass das riskant ist“, schreibt er. „Ich weiß, dass wir vielleicht Probleme bekommen. Aber es steht zuviel auf dem Spiel, um an Sicherheit zu denken.“

REALITY WINNER: MÖGLICHE WHISTLEBLOWERIN ANGEKLAGT

Die US-Webseite The Intercept hat am 5. Juni ein internes, vertrauliches Dokument des US-Geheimdienstes NSA über mutmaßliche russische Cyberangriffe veröffentlicht – und damit offenbar die anonyme Quelle verraten. Nur kurze Zeit nach dem Erscheinen des Artikels wurde eine 25-jährige Frau, Angestellte eines privaten NSA-Dienstleisters, aus dem US-Staat Georgia wegen der Weitergabe vertraulicher Informationen durch das FBI festgenommen, wie das Justizministerium am Montag in Washington mitteilte.

Das auf den 5. Mai datierte und als „Top secret“ eingestufte NSA-Dokument, hatte zum Inhalt, dass Hacker mit Verbindungen zum russischen Militärgeheimdienst GRU über Monate hinweg versuchten, in US-Wahlsysteme einzudringen. Bis kurz vor der US-Präsidentschaftswahl am 8. November habe es mittels Cyberspionage wiederholt Versuche gegeben, Informationen über die bei der Wahl eingesetzte Hard- und Software zu erlangen. Dazu seien unter anderem Phishing-E-Mails versendet worden um Schadsoftware zu platzieren. Außerdem habe es Versuche gegeben, Login-Daten zu stehlen. Wie erfolgreich der Versuch gewesen sei und welche Daten möglicherweise gestohlen wurden, bleibe allerdings unklar, heißt es in dem NSA-Bericht. Demnach hat der russische Militärgeheimdienst doch weitgehender in die Wahl einzugreifen versucht, als bislang bekannt. Jedoch lässt sich die mögliche Schlussfolgerung, ob die Hacker so das US-Wahlergebnis beeinflusst hätten, trotz der neuen Veröffentlichung bislang nicht beweisen.

Das schnelle Enttarnen der Quelle liegt möglicherweise auch am Vorgehen von „The Intercept“. Die Journalisten haben laut dem FBI auf Bitten der NSA eine Kopie des geleakten Dokuments vorgelegt. Das soll den Ermittlern dann Rückschlüsse auf die Quelle ermöglicht haben. Sicherheitsforscher Rob Graham hat in einem Blogeintrag erläutert, wie Überwachungsfunktionen in Farbdruckern der Whistleblowerin zum Verhängnis geworden sein könnten: Es ließe sich mit der Anleitung der sogenannte Machine Identification Code (MIC) analysieren, mit dem das veröffentlichte NSA-Dokument eindeutig zu einem bestimmten Drucker und einer bestimmten Druckzeit zurückverfolgen lässt. Ferner ließen die internen Überwachungssysteme der NSA erkennen, dass das Dokument sechsmal ausgedruckt worden war. Nur eine dieser sechs Personen hatte laut FBI von ihrem Desktop-Rechner aus per E-Mail mit The Intercept kommuniziert.

Reality Leigh Winner, die mutmaßliche NSA-Leakerin, war laut FBI erst seit dem 13. Februar bei der Firma Pluribus International, eines NSA-Dienstleisters, tätig. Davor soll Winner in der Air Force gedient haben. Bereits am 3. Juni wurde die Frau zu Hause verhört, wobei sie gestanden haben soll, das fragliche Dokument ausgedruckt und an ein Onlinemedium geschickt zu haben. Das US-Justizministerium hat Klage eingereicht, die Whistleblowerin ist unter dem Espionage Act angeklagt worden, damit droht ihr nun eine mehrjährige Haftstrafe.

„Die Veröffentlichung von geheimem Material ohne Autorisierung gefährdet die Sicherheit unserer Nation und untergräbt das Vertrauen der Öffentlichkeit in die Regierung“, verurteilt Vizejustizminister Rod Rosenstein die Publikation. Die Regierung von Präsident Donald Trump hatte das Justizministerium zuletzt angewiesen, verstärkt gegen die Weitergabe vertraulicher Informationen vorzugehen.

MAILDIENSTE – DATENKRAKEN, HÄNDLER UND SICHERHEITSFANATIKER

Über 60% aller deutschen Internetnutzer schwören auf kostenlose Maildienste. Die meisten davon nutzen GMX, web.de, Gmail und T-Online. Dass die genannten Provider immer noch zu den meistbenutzten Mailanbietern gehören, hat viele Gründe.

Zum einen ist es die Bequemlichkeit der Internetnutzer. Der Mailaccount wurde vor vielen Jahren aktiviert. Seitdem läuft

sämtlicher Mailverkehr über genau diesen Account. Viele wissen gar nicht, dass man seine E-Mails umleiten kann, wenn ein anderer Account als Standard etabliert werden soll. Der Aufwand, eine neue Adresse anderen mitzuteilen hindert daran, die Adresse zu wechseln. Man erinnere sich nur daran, wenn man eine neue Handynummer allen Kontakten mitteilen möchte.

Der zweite Grund ist die Mentalität, für Internetdienste kein Geld ausgeben zu wollen. Die genannten Dienste bieten zwar neben einem Free-Account, auch Dienste gegen Bezahlung an, aber diese werden hauptsächlich im Firmenumfeld genutzt. Privatanwender schwören auf kostenlose Dienste.

Anders ist es bei den Secure-Maildiensten. Hier bekommt man nur die ersten 30 Tage einen kostenlosen Account. Danach muss ein Betrag von 1 oder 2 Euro im Monat entrichtet werden. Man bekommt dafür allerdings auch viel Sicherheit. Im Gegensatz zu den freien Diensten, wo man regelmäßig mit Werbung und Angeboten von Fremdfirmen versorgt wird. Diese Werbung ist oft auf den Nutzer zugeschnitten. Anhand der Werbung kann man unter Umständen sogar sein eigenes Surfverhalten analysieren.

Machen wir uns nichts vor: Vielen ist es im Grunde egal, was mit seinen Daten passiert. Dass der Mailanbieter die Adresse, Telefonnummer, Trackingdaten usw. sammelt. Es wird sich darüber zwar aufgeregt, aber wenn es um die eigene Person geht, sieht man schnell drüber hinweg. Es wird ignoriert, dass die genannten Provider mitunter die größten Daten-Sammler sind.

Maildienste: Viele offerieren ihre Daten statt eine Gebühr bezahlen zu wollen.

Der Nutzer denkt, dass ihm sowieso nichts passieren wird. Leider herrscht hierzulande immer noch das Vorurteil, dass nur Kriminelle oder jene, die was zu verbergen haben, Secure-Mail Anbieter nutzen. So kann man in Internetforen viele Diskussionen verfolgen, wenn es um dieses Thema geht. Die Befürworter solcher sicheren Maildienste werden immer wieder vorverurteilt und angefeindet, weil der Glaube groß ist, diese Leute nutzen das Internet für rechtswidrige Sachen. Dass es aber um den Schutz der eigenen Privatsphäre und das sichere Versenden von Crypt-Mails geht, ignorieren die Gegner. Die meisten Free-Anbieter bieten zwar mittlerweile auch standardmäßig Verschlüsselung an, aber hier ist die Umsetzung oftmals unzureichend und wird eher als unnötige Last behandelt. Die Verschlüsselung wird somit bei vielen Anbietern erschwert, statt diese zu erleichtern.

Auch wenn immer mehr Nutzer zu sicheren Diensten wechseln, ist das Image dieser Anbieter in der Öffentlichkeit noch immer nicht das allerbeste. Das liegt sicher auch daran, dass Aktivisten wie Assange oder Snowden für ihre Veröffentlichungen Secure-Mailanbieter nutzten. In den USA geht es sogar soweit, dass die Behörden Nutzer solcher Dienste intensiv beobachten. Einige solcher Anbieter wie Lavabit, sind vom Staat geschlossen worden oder mussten aufgeben, weil der Druck zu groß wurde.

In Europa ist es derzeit nicht möglich, einen Anbieter aufgrund von Verdachtsmomenten zu schließen oder zu beobachten. Es gibt aber immer noch keine gesetzliche Vorgabe, wo die Weitergabe von personenbezogenen Daten geregelt ist.

Nehmen wir als Beispiele für sichere Dienste, Posteo und Mailbox.org. Außer diesen gibt es zwar noch protonmail und secure-mail.biz, aber in Deutschland sind diese beiden die derzeit bekanntesten. Diese Anbieter setzen ihren Fokus klar auf Sicherheit, Datenschutz und Transparenz. Sie erheben keine personenbezogenen Daten, setzen keine Tracking-Tools ein, und erlauben eine anonyme Bezahlung des eigenen Accounts. Der Mailverkehr, die Server und Postfächer sind mit den neuesten Verschlüsselungstechnologien ausgestattet. Das ist z.B. DANE + TLS für den Mailtransport, Zugriffsverschlüsselung, Zwei-Faktor Authentifizierung, Verschlüsselung aller Daten auf den Mail-Servern und Crypto-Mailspeicher, um nur eini-

ge Funktionen zu nennen. DANE gilt als eine der sichersten Netzwerkprotokolle zur verschlüsselten Datenübertragungen im World Wide Web. Welcher Anbieter DANE nutzt, kann man unter folgender URL prüfen: https://dane.sys4.de.

Die Server von Posteo und mailbox.org stehen ausschließlich in Deutschland, wo ein hoher Datenschutz gewährleistet ist. Bei aktiviertem Crypto-Mailspeicher, kann nur der Nutzer seine E-Mails lesen. Wenn jemand Zugriff auf die Server bzw. auf die gespeicherten Mails erlangt, kann er mit dem Mails ohne das Passwort des Nutzers zu kennen, nichts anfangen. Zusätzlich gibt es noch die Möglichkeit seinen Maileingang zu verschlüsseln. Das heißt, jede eingegangene Mail wird extra verschlüsselt. Somit ist es auch hier nicht möglich, über Mailprogramme heruntergeladene E-Mails, ohne Passwort lesen zu können. Das sind nur einige Sicherheitsmaßnahmen, die Secure-Maildienste anbieten.

Was viele Nutzer gar nicht wissen ist, dass Maildienste z.B. von der Regelung zur Vorratsdatenspeicherung komplett befreit sind. Nur halten sich leider nicht alle Anbieter dran und speichern trotzdem die Trackingdaten ihrer Kunden. Posteo ist einer der wenigen Anbieter der regelmäßigen seinen Transparenzbericht veröffentlicht. Dieser Bericht gibt einen Überblick über alle Auskunftsersuchen von Strafverfolgungsbehörden und Geheimdiensten an das Unternehmen. Mittlerweile veröffentlichen zwar auch andere Anbieter ihre Transparenzberich-

te, allerdings macht das keiner auf so radikale Art und Weise wie Posteo. Hier werden auch mal rechtswidrige oder peinlich fehlerhafte Anfragen veröffentlicht. Posteo spricht dabei sogar von chaotischen Zuständen, wie Behörden ihre Ersuchen stellen.

Meinung: Dass persönliche Daten im Internet weit verstreut sind, kann man aber auch mit sicheren Mailanbietern nicht verhindern. Ganz im Gegenteil, die offensichtliche Sicherheit ist trügerisch. Was nutzt es mir, wenn mein Mailverkehr sicher ist, ich aber auf anderen Seiten und Dienste meine Spuren hinterlasse. Auch ein VPN bietet keine hundertprozentige Anonymität.

Was aber jeder einzelne für sich machen kann und sollte, ist, keinem Dienst zu vertrauen, der an persönlichen Daten Dritter sein Geld verdient. Und genau hier bin ich wieder am Anfang dieses Blogs, bei Anbietern wie GMX, Gmail oder web.de. Hier geht es nicht nur um das Hinterlassen von Spuren im Internet, Daten-Tracking oder Datenspeicherung. Nein, hier geht es um vertrauliche Daten der eigenen Person. Gmail erstellt anhand der Mails detaillierte Bilder eines Menschen. Dazu gehören persönlichen Daten, Vorzüge, das soziale Umfeld, Surf- und Kaufverhalten des Nutzers, seine Freunde, Familie, Einkommen, Vermögen u.v.m.

Das ist nichts anderes als moderner, virtueller Menschenhandel. Unternehmen bereichern sich dadurch, indem sie den Internetnutzer verkaufen. Jedoch hat niemand das Recht, mit der Persönlichkeit des Menschen Geld zu verdienen.

Hier ist vor allem die Rechtsprechung gefragt, wie mit persönlichen Daten umgegangen werden darf. Es braucht eine gesetzliche Vorgabe, wo man als Kunde nicht der Dumme ist, sondern der Einzige, der über sich selbst bestimmen darf. Das ist die letzten Jahre extrem aus dem Ruder gelaufen. Es wird Zeit, dass wir Nutzer das Wissen über uns selber, nur den engsten Vertrauten überlassen und nicht Unternehmen, die damit Milliardenumsätze generieren.

FINANZEXPERTE JONATHAN HARRIS: KRYPTOWÄHRUNGEN SIND WERTLOS

Jonathan Harris, der in der US-Finanzbranche dafür bekannt sein soll, klare Kante zu zeigen, hat Bitcoin und andere Kryptowährungen gegenüber der Financial Times (FT) als Schneeballsystem bezeichnet. Harris hält Kryptowährungen generell für komplett wertlos. Die Community schäumt.

Während Startups wie Bitwala versuchen, kleinen wie großen Unternehmen Kryptowährungen wegen der geringen Transferkosten von Überweisungen ins Ausland schmackhaft zu machen, polterte Jonathan Harris in der Financial Times herum. Harris vertritt in dem kostenpflichtigen Artikel die Auffassung, dass der Bitcoin exakt „null“ wert sei. Der Finanzexperte verfügt dabei u.a. über einen Bachelor and Master of Science und ist schon seit mehr als 20 Jahren in der Finanzbranche tätig.

Bitcoin laut Jonathan Harris nichts als ein Schneeballsystem

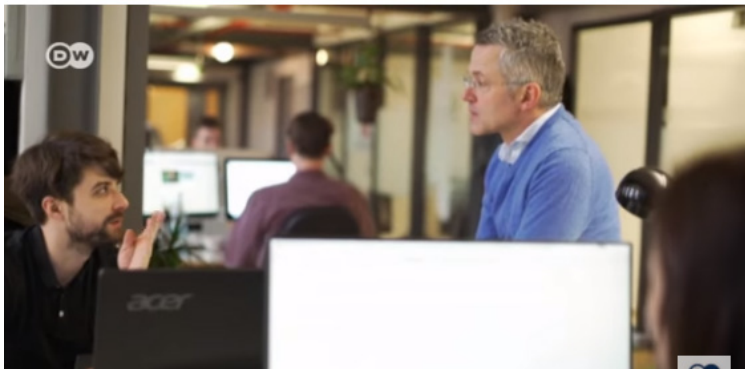
Viele Analysten haben ein Problem damit, dass für sie eine virtuelle Währung einfach nicht greifbar ist. Immer wieder wird der Bitcoin als inhärent (= nicht existierend) bezeichnet. Harris glaubt, Bitcoins zu kaufen bringt den Anlegern nicht mehr, als einen Betrag auf ein Konto zu buchen. „Alles, was man damit tun kann, ist, sie an jemand anderen zu verkaufen." Harris bemängelt zudem, dass man mit diesem Geld bisher noch so gut wie nirgendwo eine Ware oder Dienstleistung an der Kasse bezahlen kann. Die Akzeptanz der Bitcoins in den Ladengeschäften lässt hierzulande tatsächlich sehr zu wünschen übrig. Allerdings gibt es ein paar wenige Enthusiasten, wie beispielsweise Kneipen oder Science Fiction-Bücherläden (siehe Video unten), wo man virtuell bezahlen kann. Den Ausführungen von Harris zufolge glaubt er, nur weil aufgrund des Hypes viele Anleger in den Markt eingestiegen sind, konnte sich der Wert derart positiv entwickeln. Sollten alle Spekulanten ihre Einlagen auf einen Schlag aus diesem Markt herausziehen, würde der Kurs naturgemäß ins Bodenlose fallen.

Der Finanzexperte beschreibt beim Gespräch außerdem Optionen, wie man das Bitcoin besser kontrollieren könne, was das Wachstum bremsen würde. Doch die Abwesenheit einer einzelnen Zentralbank als Kontrollinstanz ist ja genau das, was diese Währung ausmacht.

Meine Einschätzung: Klar ist, dass das Bitcoin und alle anderen virtuellen Währungen teils erheblichen Schwankungen unterliegen. Das trifft in dieser Ausprägung auf die meisten „echten" Währungen nicht zu. Um nur ein Beispiel zu nennen: Im Mai dieses Jahres fiel der Wert des Bitcoin in nur zwei Tagen um 700 Dollar ab, um sich dann wieder ganz langsam zu erholen.

Bei Coinbase kostet ein Bitcoin derzeit 2.506,73 US-Dollar, das sind umgerechnet etwas über 2.240 Euro. Für uns Otto-Normal-Verbraucher ist diese Währung nur bei einer mittel- bis langfristigen Anlage interessant. So stieg der Wert innerhalb der letzten 12 Monate um fast um 2.000 US-Dollar an. Die Gründe dafür sind schwer nachvollziehbar, vielfältig und haben IMHO nur teilweise etwas mit dem anhaltenden Bitcoin-Hype zu tun, der tatsächlich einige Zocker angelockt hat. Es wird gemunkelt: Unter anderem wegen der Sekunden-Trader zogen sich letzte Woche unzählige Bitcoin-Transfers extrem in die Länge. Manche Anbieter wie Coinbase wurden durch Anfragen derart geflutet, dass die Technik mit der Masse an Seitenzugriffen und Aufträgen überfordert war, wie uns ein Servicemitarbeiter per E-Mail mitteilte.

P.S.: Der Rant von Harris ist schon uralt, das Interview wurde Ende Januar dieses Jahres veröffentlicht. Es dauerte allerdings mehr als ein halbes Jahr, bis das Thema von den meisten englisch- bzw. deutschsprachigen Bitcoin-Newsportalen aufgegriffen wurde. Natürlich gibt es auch eine Entgegnung, die sich kritisch mit den Aussagen des „Finanzexperten" auseinandersetzt. Die Wahrheit liegt wahrscheinlich wie üblich irgendwo in der Mitte.



P.S.S.: Sehr spaßig ist dieser Kommentar eines Lesers, den man mal gelesen haben sollte:

Good for him… another clown economic „expert".

I look forward to him and his peers being unemployed, sitting on a street corner holding a cup for change… or better yet, a QR Code with a sign „Spare a little Bitcoin. Anything helps!"

STUDIE: FACEBOOK-VERHALTEN OFFENBART SUCHTPOTENTIAL

In einer Studie haben US-Forscher einen statistischen Zusammenhang (Korrelation) zwischen dem Social Media-Verhalten eines Benutzers (z. B. Wortverwendung oder Likes) und einem Substanzgebrauch nachgewiesen. So kann aus Facebook-Statusmeldungen und Likes eine Vorhersage getroffen werden, ob ein Nutzer zu Alkoholkonsum, Zigaretten oder Drogenkonsum neigt, berichtet Netzpolitik.org.

Laut einer aktuellen Studie des Addiction Recovery Research Centers in Roanoke im US-Bundesstaat Virginia lassen sich aus den unterschiedlichen Nutzeraktivitäten auf Facebook Verhaltensmuster ableiten, die mit hoher Genauigkeit Voraussagen zum Suchtverhalten ermöglichen.

Ziel der Studie war es, diejenigen Leute herauszufiltern, die durch den Konsum bewusstseinsverändernder Substanzen eine psychische „Störung“ (Substance Use Disorder) erleiden oder dafür anfällig sein könnten. Dazu wurden Verhaltensmuster von elf Millionen Facebook-Nutzern und 22 Millionen Status-Updates von insgesamt 150.000 Usern analysiert, wobei als Basis sowohl Like-Angaben als auch Status-Updates dienten. Anhand dieses Materials entwickelten die Wissenschaftler Algorithmen, die erkennen lassen, welche User für welche Art von Sucht anfällig sind. Das Suchtverhalten spiegelt sich dabei in bestimmten Verhaltensmustern wider, die über das Facebook-Profil und die Nutzungsgewohnheiten auf der Plattform abgelesen werden können. So ließ sich mit einer hohen Wahrscheinlichkeit vorhersagen, welche User Gebrauch von legalen und illegalen Drogen wie Alkohol, Tabak, Cannabis und anderen Suchtmitteln machten. Aus diesen Daten können wiederum Prognosen für andere Facebook-Nutzer erstellt werden, die den Missbrauch anzeigen können.

Für die Auswertung der Studienergebnisse kamen hochmodernes maschinelles Lernen sowie das „Mining“ von Texten zum Einsatz. Die Wissenschaftler entwickelten eine Software, die auf einem lernfähigen Algorithmus basiert. Dieser kann anhand der gewonnenen Daten Zusammenhänge und Muster erkennen und zugleich auch für die Zukunft Voraussagen treffen. So ließen sich Verknüpfungen bestimmter Schlüsselwörter vorangegangener Untersuchungen, die Menschen mit psychischen Erkrankungen aufgrund des Konsums von Drogen und anderen Substanzen verwenden, adäquat auch für diese Studie mit heranziehen. Zu solchen Wörtern gehören Schimpfwörter genauso wie Aussagen über den körperlichen und geistigen Zustand und Begriffe mit sexueller Konnotation. Zudem wurden Musik-, Film- oder andere Unterhaltungspräferenzen ausgewertet. Laut den Forschern wären Zeichentrickfilm-Liebhaber mit geringer Wahrscheinlichkeit exzessive Alkoholkonsumenten, wer jedoch „V for Vendetta“ anschaut, hingegen schon eher.

Die Vorhersagemethoden wiesen eine hohe Erkennungsrate auf. So konnten Tabaknutzung mit 86 Prozent, übermäßiger Alkoholkonsum mit 81 Prozent, Drogenmissbrauch mit 84 Prozent und Psychische Erkrankungen im Zusammenhang mit Substanzen mit einer Genauigkeit von 80 Prozent vorausgesagt werden. Im Fazit gelangten die Wissenschaftler zu der Erkenntnis, dass die Art der Erkennung auf sozialen Medien alle anderen derzeit gängigen Methoden zur Suchterkennung klar schlägt, wenn es darum geht, Drogenkonsum sichtbar zu machen und die Prävention zu fördern.

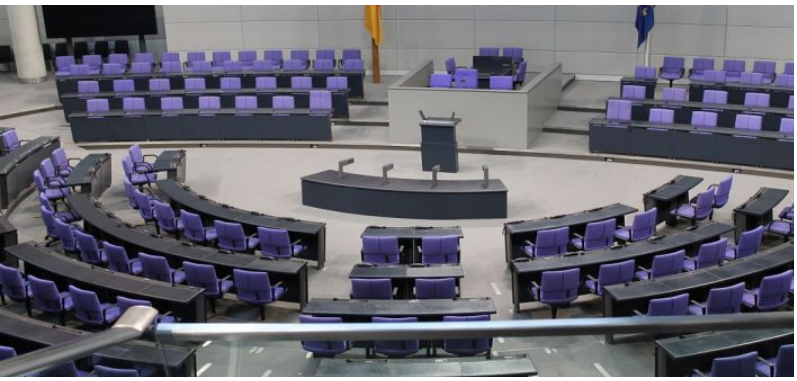
Als besonders interessant dürften sich die erhobenen Daten dieser Studie für Unternehmen, die Werbung auf Facebook schalten, erweisen oder auch für staatliche Behörden, die Verstößen gegen das Betäubungsmittelgesetz (BtMG) auf der Spur sind.

STAATSTROJANER: ANHÖRUNG IM BUNDESTAG

Am Mittwoch, dem 31.05.2017, ging es in einer Debatte im Bundestag um eine Gesetzesinitiative, wonach Ermittlern der Einsatz von Staatstrojanern im Kampf gegen schwere Verbrechen gestattet werden soll. Die Standpunkte von Justiz und Polizeibehörden versus Juristen und IT-Experten konnten unterschiedlicher kaum sein.

Die Große Koalition möchte nach einem Vorschlag des Bundesministeriums für Justiz und Verbraucherschutz (BMJV) die Überwachung erweitern und nicht mehr wie bisher nur bei den Providern ansetzen. Vielmehr möchte Justizminister Heiko Maas zusätzlich auf breiter Front Staatstrojaner einsetzen lassen. So sollen in einer Gesetzesänderung zum einen sowohl die Quellen-Telekommunikationsüberwachung oder Quellen-TKÜ zugelassen werden, d.h., das Abfangen der Daten, noch bevor sie verschlüsselt werden. Zum zweiten soll zudem die Online-Durchsuchung unter besonders strengen Voraussetzungen erlaubt sein, also das Durchsuchen eines kompletten elektronischen Gerätes nach verdächtigen Daten. In beiden Fällen muss auf dem Gerät heimlich ein Spionageprogramm installiert werden, der sogenannte Staatstrojaner.

Diese Überwachungssoftware, die der Staat bisher nur zur Gefahrenabwehr, insbesondere zur Verhinderung von Terroranschlägen, einsetzen durfte, soll nach einem Änderungsantrag der



CDU-/CSU- und SPD-Fraktionen, den die Bundesregierung Mitte Mai kurzfristig durch eine Formulierungshilfe auf den Weg gebracht hat, zukünftig auch zur Strafverfolgung eingesetzt werden.

Während IT-Experten und Juristen davor warnten, Strafverfolgern auch zur Bekämpfung von Alltagskriminalität den Einsatz des Staatstrojaners zu gestatten, begrüßten Staatsanwälte und das BKA das Vorhaben. Im Rahmen der Sachverständigen-Anhörung sprachen sich die Vertreter der Ermittlungsbehörden eindeutig für die Einführung der neuen Eingriffsbefugnisse durch die geplanten Gesetzesänderungen aus: Als Mittel zur Aufklärung von Straftaten müsse der Einsatz des Staatstrojaners erlaubt werden.

Linus Neumann, als Vertreter des Chaos Computer Clubs (CCC), warnte in einer Stellungnahme eindringlich vor einem Einsatz des Staatstrojaners und wies auf die Folgen für alle Computer- und Handynutzer hin. Zur Installation der Schadsoftware seien IT-Schwachstellen eine zwingende Voraussetzungen. Das Bestehen von Sicherheitslücken auf allen Systemen wäre also zukünftig im staatlichen Interesse. Um die Möglichkeit zu haben, wenige Geräte von Verdächtigen infizieren zu können, werde die Sicherheit von Millionen anderer Nutzer gefährdet.

Dr. Ulf Buermeyer, Richter am Landgericht Berlin, bezeichnete die geplante Überwachungsausweitung bei der Anhörung treffend als „das ganz große Besteck des Strafprozessrechts“. Die Betroffenen würden damit derart gläsern, wie es das Strafrecht bisher nicht kenne: „Hier geht es ums Ganze rechtsstaatlich betrachtet.“ Die Systeme dürfen von den Strafverfolgungsbehörden nur soweit manipuliert werden, wie es für die Überwachung notwendig ist. Es dürfen also keine Beweismittel manipuliert oder gar untergeschoben werden. Wirksam kontrollieren lässt sich diese Begrenzung allerdings nicht. Völlig ungeklärt bleibt die Frage, wie die Behörden sicherstellen wollen, dass ein Trojaner zur Kommunikationsüberwachung tatsächlich keine anderen Funktionen hat: „Wir können nur hoffen und beten, dass die Vorgaben eingehalten werden“, sagte Buermeyer.

BKA-Vizepräsident Peter Henzler verwies in diesem Zusammenhang auf die sogenannte Standardisierte Leistungsbeschreibung, die erfüllt werden müsse. Dies werde durch eine externe Firma geprüft. Demnach gebe es den Trojaner nur in „verfassungskonformer Form“. Die Software sei dabei ein „technisches Unikat“, das auf den jeweiligen Täter zugeschnitten sei und „längst nicht auf jeden passt“. Henzler verteidigt zudem die Möglichkeit, mit Hilfe der Onlinedurchsuchung die Inhalte von Computern auszuspähen, denn es seien bisher von 125 Datenträgern fast jeder vierte verschlüsselt gewesen.

Auch der Nürnberger Oberstaatsanwalt Alfred Huber stimmte dem Vorschlag der Bundesregierung zu: „Sie müssen uns den Schlüssel zur Verfügung stellen, damit wir auf Augenhöhe mit den Tätern kommen“, sagte er und erklärte die Quellen-TKÜ für „absolut unabdingbar“. Im übrigen sei es eine politische Frage, ob man die organisierte Kriminalität oder Einbrecher überhaupt bekämpfen wolle: „Wir schützen lieber die Daten, oder schützen Sie damit nicht die Täter?“, meinte er.

Die Bundesdatenschutzbeauftragte Andrea Voßhoff, die selbst nicht anwesend war und nach eigenen Angaben von dem Plan erst aus den Medien erfuhr, warnt in einer Stellungnahme (veröffentlicht durch netzpolitik.org) vor „erheblichen datenschutzrechtlichen Risiken“ und einem „klaren Verfassungsverstoß“. Dieser drohe durch eine Klausel, mit der die Quellen-TKÜ im Einzelfall zur „vollwertigen“ Online-Durchsuchung ausgebaut werde.

METHODEN-PATENT: MICROSOFT GEHT GEGEN FILESHARING VOR

Der Software-Konzern Microsoft hat sich in einem Methoden-Patent ein System patentieren lassen, dass es ermöglicht, insbesondere diejenigen Nutzer, die häufiger urheberrechtlich geschützte Inhalte teilen, zu selektieren, die Weitergabe des geschützten Contents zu blockieren, ohne jedoch dabei die User generell als Kunden zu verlieren, berichtet TorrentFreak.

Abgesehen von den traditionellen Piratenwegen werden auch soziale Netzwerke und Cloud-Hosting-Dienste wie Dropbox, Google Drive und Microsoft OneDrive häufig verwendet, um urheberrechtlich geschützte Inhalte zu teilen. Microsoft hat nun ein Patent entwickelt, um diese Urheberrechtsverletzungen einzudämmen. Es geht insbesondere um Sharing-Blockaden in den eigenen Cloud-Diensten.

Unter der treffenden Bezeichnung „Deaktivieren von verbotenen Inhalten und Identifizieren von Wiederholungsstraftätern in Dienstanbieterspeichersystemen“ beschreibt das Methoden-Patent ein System, in dem Urheberrechtsverletzer und diejenigen, die andere anstößige Inhalte in einer Cloud speichern und diese Inhalte widerrechtlich teilen, so markiert und in einer Chronik verzeichnet werden, dass besonders Wiederholungsstraftäter erfasst werden. Darauf basierend können Nutzerkonten geschlossen oder Rechte entzogen werden. Betroffene User sollen dann etwa weiterhin in der Lage sein, ein Album im MP3-Format auf ihren Cloud-Storage zu legen und mit den eigenen Geräten zu nutzen, Dritten soll der Zugriff jedoch verwehrt werden.

Microsoft möchte mit diesem Patent Nutzer disziplinieren, die beispielsweise ein Musikalbum auf ihren Cloud-Speicher hochladen und den Download an eine nicht allzu große Zahl anderer Nutzer freigeben, denn auch diese Methode des Teilens kann schnell über die üblichen Fair-Use-Prinzipien hinausgehen, wird bisher aber kaum kontrolliert oder behindert. Mit Sperren wird man erst dann rechnen müssen, wenn der Freigabe-Link auf einer größeren Download-Plattform auftaucht, nicht aber, wenn man ihn in einer geschlossenen Facebook-Gruppe teilt und rund 20 andere User das Angebot annehmen. Wer häufig die Richtlinien missachtet, kann immer stärker reglementiert werden, während eine komplette Sperrung des Accounts dann nur am Ende einer ganzen Reihe von Maßnahmen stünde. Genaue Anwendungsregeln, welche Vergehen bestimmte Maßnahmen nach sich ziehen, beschreibt das Patent jedoch nicht.

Zudem soll das im Patent dargelegte System Storage-Anbietern ermöglichen, Vorfälle von Nutzern in einem Verlauf abzuspeichern. Mit dieser Chronik hat dann der Provider eine Basis, auf dessen Grundlage er entscheiden kann, ob dem Nutzer bestimmte Rechte, wie der Zugriff auf gefragte Dateien, entzogen werden oder ein Account sofort gesperrt wird.

Das System identifiziert betroffene Dateien, indem diese mit einer für den Endnutzer unsichtbaren Markierung versehen werden. Sowohl Google, als auch YouTube und Dropbox nutzen für ihre Cloud-Dienste ein ganz ähnliches Verfahren, wie das System von Microsoft. Dieses basiert auf einzigartigen Hash-Summen, die zum Aufspüren illegaler Kopien verwendet werden.

Gemäß dem Digital Millennium Copyright Act (DMCA) müssen in den USA Anbieter von Cloud Storage eine geeignete Vorgehensweise gegen Urheberrechtsverstöße implementieren. Dem wäre dann durch die Anwendung eines solchen Patentes Genüge getan. Außerdem hat sich gezeigt, dass das Löschen von Schwarzkopien im Internet bisher oftmals ein unzureichendes Mittel war. So sperrt Microsoft hier gleich die Quelle.

Fazit

Es wäre immerhin denkbar, dass das System nicht nur in den USA zur Anwendung kommt, auch in der EU besteht Handlungsbedarf, wenn es um Urheberrechtsverletzungen geht. Ein erst kürzlich veröffentlichtes Urteil vom EuGH wegen der Nutzung illegaler Streamingdienste macht das deutlich. Jedoch muss dazu natürlich das Produkt erst einmal auf dem Markt sein…

STUDIE: KODI WIRD MILLIONENFACH VERWENDET MIT PIRATEN-ADD-ONS IN NORDAMERIKANISCHEN HAUSHALTEN

Neue Daten einer Studie des kanadischen Netzwerk-Unternehmens Sandvine zeigen, dass nahezu 9 Prozent aller nordamerikanischen Haushalte mindestens ein Kodi-basiertes Gerät nutzen. Etwa zwei Drittel davon verwenden aktiv Piraten-Add-ons, berichtet TorrentFreak.

Die Kodi Media Player Software, die früher auch unter dem Namen Xbox Media Center (XBMC) bekannt war, ist in den letzten Jahren immer populärer geworden. Kodi ist ein Open-Source-Projekt, das Plugins unterstützt, und ist in seinen, auch für PCs, Smartphones und Tablets vertriebenen Versionen, ein be-

liebtes Tool, um auf Geräten, wie dem Amazon Fire TV Stick, eine alternative Oberfläche für den Medienkonsum zu nutzen. Allerdings bietet Kodi eben auch die Möglichkeit, eigentlich kostenpflichtige Programme und Serien, Filme und anderes zu konsumieren, weil es mittels inoffizieller Add-ons das Streamen von neuem Content aus dubiosen Quellen unterstützt.

Zwar nahm man immer an, dass Kodi weitverbreitet ist, es gab jedoch bisher keine repräsentative Statistik, die diese Aussage konkret bestätigt hätte. Eine neue Studie des kanadischen Netzwerk-Unternehmens Sandvine, die am 04.05.2017 veröffentlicht wurde, soll diese Aussage jedoch bestätigen. Weltweite Zahlen zur Kodi-Nutzung liegen derzeit nicht vor, Sandvine hat aber den nordamerikanischen Markt untersucht und herausgefunden, wie weit verbreitet Kodi dort mittlerweile ist.

Dazu analysierte Sandvine einen Datensatz von mehreren nordamerikanischen Festnetzanbietern, der über 250.000 anonyme Haushalte in ganz Nordamerika umfasst. Anhand dieser Daten ließ sich ermitteln, wie viele Haushalte mindestens ein Kodi-basiertes Gerät verwenden. Insgesamt stellte Sandvine fest, dass diese Tatsache für 8,8% der Haushalte mit Internet-Zugang in Nordamerika zutrifft. Als Hardware kommen dabei PCs, Set-Top-Boxen, Smartphones und Tablets in Frage. Der genannte Anteil lässt sich in etliche Millionen Haushalte umrechnen. Allein in Kanada besitzen über 10% der Haushalte ein Kodi-basiertes Gerät.

An sich ist die Nutzung von Kodi vollkommen legal, wenn nicht die Software per Erweiterung so modifiziert wird, um auf illegale Inhalte aus dem Internet zugreifen zu können. Laut Sandvine machen sehr viele von dieser Option Gebrauch. Man hat sich unterschiedliche Quellen für die per Streaming übermittelten Daten angesehen und so herausgefunden, dass unter den „Kodi-Haushalten“ 68,6 Prozent inoffizielle oder „Piraten“ Add-ons verwenden.

Die Studie wurde zum Teil durch ein erhöhtes Interesse von Content Service Providern, Urheberrechtsinhabern und Regulatoren angeregt. Einige von ihnen sahen in der Kodi-Software die Wurzel des Piraterieproblems, aber Sandvine distanziert sich von dieser Behauptung: „Kodi würde lediglich als Frontend dienen“, meinen sie. Wenn Kodi morgen verschwände, dann würde sich nichts ändern, denn dann würden die Nutzer einfach über andere Kanäle, wie Browser oder andere Mediaplayer, auf die illegalen Inhalte zugreifen: „In einigen Diskussionen, die wir mit Inhalte-Anbietern hatten, wird Kodi als Wurzel dieses illegalen Streaming gesehen, aber das ist falsch.“, stellt Sandvine fest. Für diese klare Aussage verdiene Sandvine Anerkennung, so TorrentFreak, denn viele Medien berichten anders und geben dem Projekt einen schlechten Ruf mit auf den Weg und das verursacht oft große Frustration unter den Kodi-Entwicklern. Es wäre interessant zu sehen, wie diese Entwicklung in einigen Jahren voranschreitet. Falls sich die Anzahl der Kodi-Nutzer bis dahin vervielfacht, wäre dies wohl keine große Überraschung, so TorrentFreak.

APP ANNIE: DEUTSCHE VERBRINGEN TÄGLICH 2 STUNDEN MIT APPS

Die App-Daten- und -Analyse-Plattform App Annie hat eine neue, aktuelle Studie zur App-Nutzung in Deutschland veröffentlicht. Demnach verbringen Deutsche knapp 2 Stunden am Tag mit Apps. Der durchschnittliche deutsche Smartphone-Nutzer verwendet fast 40 Apps pro Monat.

Die neue Studie von App Annie bringt einige aufschlussreiche Ergebnisse: Auf das Jahr gerechnet befasst sich der durchschnittliche User hierzulande 730 Stunden mit der App-Nutzung. Weltweit ist die App-Nutzungsdauer um 25 Prozent angestiegen. Rund um den Globus haben Nutzer zwischen Januar und März 2017 etwa 175 Milliarden Stunden mit Apps verbracht.

Damit ist eine deutliche Steigerung bei der Nutzung von Apps gegenüber den beiden letzten Jahren gegeben. Im ersten Quartal 2015 waren es nach Angaben von App Annie noch 90 Minuten und im ersten Quartal 2016 knapp 105 Minuten. Auch ein Anstieg der Gesamtnutzungsdauer ist zu verzeichnen: So ist diese weltweit vom ersten Quartal 2016 (circa 140 Mrd. Stunden) zum ersten Quartal 2017 (circa 175 Mrd. Stunden) um 25 Prozent angestiegen.

Der durchschnittliche Smartphone-Nutzer verwendete in allen analysierten Ländern mehr als 30 Apps im Monat und neun Apps am Tag. In Deutschland waren es nahezu 40 monatlich aktive Apps. Im Durchschnitt wurden

zwischen einem Drittel und der Hälfte der auf den Smartphones installierten Apps jeden Monat genutzt. Die bereits vorinstallierten Dienstprogramme werden dabei häufiger genutzt als die sozialen Netzwerke oder Kommunikationsprogramme. Die weltweite Gesamtzahl der Downloads von Apps in 2016 zeigt, dass mobile Anwendungen zum wichtigsten Kanal geworden sind: Im gesamten Jahr 2016 wurden 90 Milliarden Apps heruntergeladen, was einen Zuwachs von über 13 Milliarden im iOS App Store und auf Google Play bedeutet. Die Gesamtnutzungdauer lag 2016 bei fast 900 Milliarden Stunden.

iPhone Nutzer verwendeten eine etwas größere Zahl von Apps als Android Nutzer. Im Durchschnitt nutzten Android-User über 30% mehr Spiele als iPhone-Nutzer, auch wenn sie insgesamt weniger Apps nutzen. Allerdings führt iOS dank dem höheren durchschnittlichen Umsatz pro Nutzer immer noch nach Spieleumsätzen.

Hier die Zusammenfassung der Hauptpunkte der Analyse:

- In Brasilien, Indien und China werden Apps am häufigsten genutzt
- Der durchschnittliche Smartphone-Anwender nutzt im Monat über 30 Apps
- Mindestens neun Apps werden täglich genutzt
- Bevorzugt werden Dating- und Produktivitäts-Apps
- Platz 2 nehmen Social-Media- und Kommunikations-Apps ein
- Vorinstallierte Apps werden als Dienstprogramme am häufigsten aufgerufen

Mit mehr als fünf Millionen Apps, die sowohl auf Google Play als auch im iOS App Store verfügbar sind, und einer durchschnittlichen Nutzung von gut 30 Apps pro User und Monat in den Schlüsselmärkten, herrscht im App-Markt ein extremer Wettbewerbsdruck. Laut App Annie kann ein Unternehmen seine Position in diesem kompetitiven Umfeld nur verteidigen, wenn es sich gut mit Techniken zur App-Store-Optimierung und App-spezifischer User-Generierung auskennt und in der Lage ist, eine Daten-gestützte App-Strategie zu entwickeln.

Martje Abeldt, Central European Territory Director bei App Annie, weist darauf hin, dass Mobilgeräte zum Touchpoint werden für viele Verbraucher, „um mit Marken in Kontakt zu treten. Das heißt, das Marketing innerhalb der mobilen Kanäle entwickelt sich sehr schnell. Allein Downloads zu studieren reicht nicht mehr aus. Nur durch die Nutzung einer Monitoring-App können heute Marketingverantwortliche die wirklich relevanten Ziel-Apps für ihre Kampagnen finden."

App Annie stützt die eigenen Daten auf die Zusammenarbeit mit zahlreichen Entwicklern. So unterstützt App Annie Unternehmen bei der Entwicklung ihres App-Business und wird von 94 der Top 100 Publisher weltweit genutzt.

WURDE AACS 2.0 GEKNACKT?

Kürzlich wurde die Blu-ray Disc „The Smurfs 2" (Die Schlümpfe) auf einem privaten BitTorrent-Tracker veröffentlicht, die mit dem Advance Access Content System (kurz AACS 2.0) versehen war. Das Release hat den stolzen Umfang von 53.1 GB. Mittlerweile ist der englischsprachige Film auch bei ExtraTorrent.cc gelandet und wird sich trotz der enormen Größe sicher sehr schnell verbreiten.

Kurz notiert: Auf einem privaten Torrent-Tracker namens UltraHDClub.com wurde gestern offenbar der zweite Teil der Schlümpfe veröffentlicht. Dies wurde vor zwölf Stunden bei Reddit berichtet.

„The Smurfs 2" ist aber mittlerweile auch öffentlich bei Extratorrent.cc verfügbar. Dies wäre demnach die erste Veröffentlichung eines 4k Films, der mit dem Kopierschutz AACS 2.0 versehen war. Bislang galt dieser als komplett unüberwindbar. Die Industrie setzte bisher ihre Hoffnung darauf, dass man ihre hochauflösenden Filme nicht illegal in Umlauf bringen kann.

Auch die technischen Details dieses Releases wurden bekannt gegeben. Bisher ist allerdings unklar, wie man den Kopierschutz AACS 2.0 geknackt haben will. Von daher bleibt abzuwarten, ob dieser Release nicht doch ein Fake ist. Als Beweis wurde auch ein extrem kurzer Ausschnitt des Films bei einem Sharehoster veröffentlicht.

Wer sich für den Transfer dieser illegalen Dateien interessiert, darf auf keinen Fall den Einsatz eines VPN unterlassen!

Security

Themenübersicht

„CRAZY BAD“: SCHWERE WINDOWS-SICHERHEITSLÜCKE ENTDECKT

IT-Sicherheitsforscher haben eine schwere Sicherheitslücke im Betriebssystem Windows entdeckt. Diese findet sich in Standard-Installationen des Betriebssystems und lässt sich per Schadsoftware ausnutzen.

Schlimm und automatisiert nutzbar

Die beiden IT-Sicherheitsforscher Tavis Ormandy und Natalie Silvanovic, Mitglieder von Googles „Project Zero„ haben nach eigenen Angaben eine der ernstesten Windows-Sicherheitslücken der letzten Jahre entdeckt. Über die Schwachstelle lässt sich Code ausführen und sie ist auch über das Netzwerk angreifbar. Zudem, so Ormandy, eignet sie sich auch für die Ausnutzung durch automatisierte Schadsoftware, etwa in Form eines Computer-Wurms. Ormandy bezeichnete die Lücke in einem Tweet als „crazy bad“, also etwa „unglaublich schlimm“.

Rätselraten um Details

Welche Komponente des Betriebssystems die Schwachstelle aufweist, teilten die Sicherheitsforscher bislang nicht mit. Allerdings lässt sich schlussfolgern, dass es sich um eine Komponente handeln muss, die standardmäßig mit dem Betriebssystem installiert wird. In Fachkreisen wurden etwa .NET, die Krypto-Bibliothek SChannel und sogar die Windows-Firewall als mögliche Kandidaten genannt. Ormandy bestätigte keine der Theorien, erklärte aber, dass es sich bei der betroffenen Software nicht um .NET handle.

Sicherheitsexpertinnen und -Experten ebenso wie besorgte Nutzer mag diese Vorgehensweise frustrieren. Sie ist jedoch äußerst sinnvoll. Einzelheiten werden der Öffentlichkeit wohl erst bekannt gegeben, wenn die Verantwortlichen – in diesem Fall Microsoft – Zeit zum Beheben der Lücke hatten. Das gehört zur sogenannten“Responsible Disclosure„. Traditionell bekommen Software-Unternehmen von Project Zero 90 Tage zum Beheben gefundener Sicherheitslücken eingeräumt.

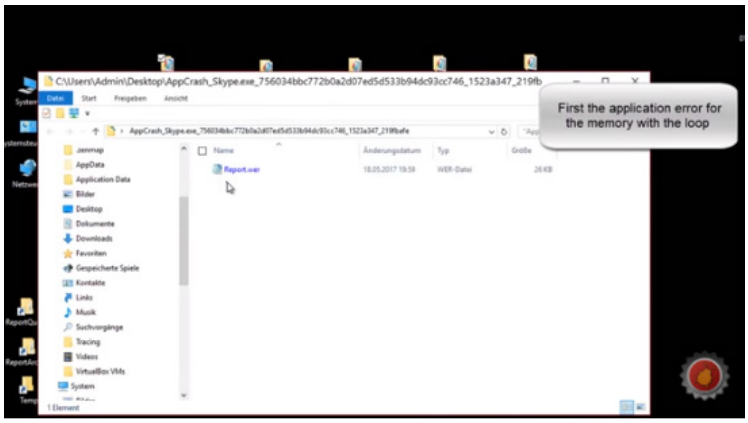
KRITISCHE SKYPE-SICHERHEITSLÜCKE GESCHLOSSEN

Durch eine kürzlich gefixte Sicherheitslücke in der Messaging-Software Skype konnten Angreifer bislang Windows-Systeme mit Schadcode infizieren. Tarnkappe.info berichtet.

Benjamin Kunz Mejri von Vulnerability Lab sowie das Blog “ Vulnerability Magazine“ haben eine, bis nach dem Patch von Microsoft, sogenannte Zero Day Sicherheitslücke in der Messaging-Software Skype gefunden welche eine Remotecode-Ausführung erlaubt. Natürlich wird auch Skype gerne in offenen WLAN-Netzen genutzt. Cyberkriminelle konnten damit bis gestern einige Probleme auf den Computern der Opfer hervorrufen.

Die Sicherheitslücke CVE-2017-9948 in der Windows-Bibliothek MSFTEDIT.DLL steckte in den Versionen 7.2, 7.35 und 7.36. Ein Angreifer konnte auf den Zielrechnern mit präparierten Bildern Schadcode einzuschleusen, auszuführen und auch einen Absturz der Anwendung auszulösen. Im Sicherheitsteam hat man eine Bilddatei aus der Zwischenablage in das Skype-Fenster kopiert, die die Grenzen für eine Übertragung übersteigt (Pufferüberlauf). Das führte zu einem Skype-Stacküberlauf samt Absturz des Programms. Die Angriffe lassen sich laut Mejri lokal und eben remote (z.B. per RDP-Sitzung) ausnutzen. Außerdem betonte er, dass keine Interaktion mit einem Nutzer notwendig ist. Einzige Voraussetzung sei ein Skype-Konto.

Im Mai informierte Kunz Mejri Microsoft über das Problem, das schließlich einen Fix ankündigte und diesen seit dem 8. Juni mit dem Update auf die Version 7.37.178 ausliefert. Seit dem 26. Juni 2017 ist der kritische Fehler nun öffentlich, eine Aktualisierung auf die letzte Skype-Version ist also höchst ratsam, wenn noch nicht geschehen.



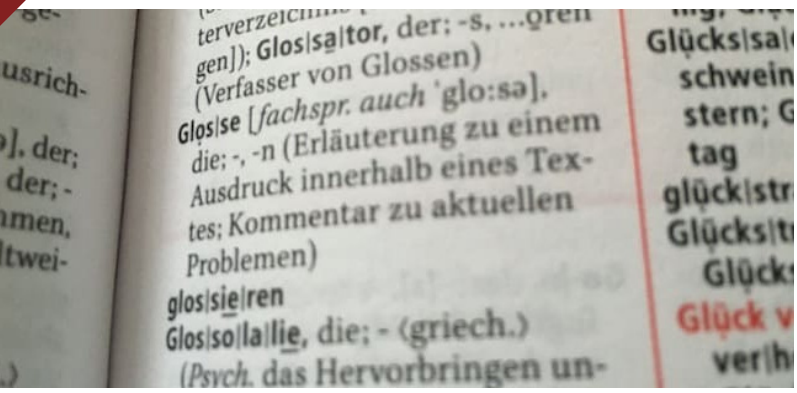
Vulnerability Lab bewertete die Schwachstelle mit 7,2 Punkten im zehnstufigen CVSS Test (Common Vulnerability Scoring System). Nach Schätzungen des Unternehmens sollte der Zero-Day-Bug auf dem Schwarzmarkt einen Preis von 25.000 bis 35.000 Euro erzielt haben. Die Funktionsweise des Exploits zeigt das Unternehmen zudem in einem Video.

SICHERHEIT VON PASSWÖRTERN GEFÄHRDET DURCH HIRNWELLEN-AUSWERTUNG

Schädliche Software könnte Gehirn-Computer-Schnittstellen, wie ein EEG-Headset, dazu verwenden, um Passwörter und andere private Daten zu stehlen. Das fanden Forscher an der University of Alabama in Birmingham in einer Studie heraus, berichtet technologyreview.

Eine neue Studie der University of Alabama in Birmingham prüfte die Möglichkeit, ob sich ein schon relativ einfaches EEG-Gerät dazu missbrauchen ließe, um über die analysierten Hirnwellen PIN und Passwörter herauszufinden. Dazu trugen Probanden ein EEG-Headset. Zunächst spielten sie ein Computerspiel, dann wurden sie aufgefordert, sich in ein Online-Konto einzuloggen. Daraufhin gaben die Probanden zufällige PINs und Passwörter ein, so dass die Software die Verbindungen zwischen ihrem Tippen und den dabei entstehenden Hirnwellen lernen konnte. Mit speziellen Mustererkennungsprogrammen wird die Software darauf trainiert, die Besonderheiten der Signale aus dem Gehirn seines Anwenders immer besser zu deuten. In der Realität ließe sich das laut Nitesh Saxena, Associate Professor an der University of Alabama in Birmingham, erreichen, indem ein Spiel Nutzer im Rahmen der Handlung auffordert, Zahlenfolgen oder Text einzugeben.

In dem Fall brauchten die Algorithmen die Eingabe von etwa 200 Zeichen für die Analyse. In der Folge konnten sie allein anhand der empfangenen EEG-Daten zielgenaue Schätzungen dazu abgeben, welche weiteren Zeichen dann noch getippt werden. Das System funktioniert bislang zwar nicht perfekt, dennoch erhöht es die Wahrscheinlichkeit dafür, eine PIN mit sechs Ziffern herauszufinden, von 1 zu 10.000 auf 1 zu 20; bei einem Passwort mit sechs Zeichen erhöht sich die Trefferwahrscheinlichkeit um den Faktor 500.000 auf etwa 1 zu 500. Folglich könnte ein in krimineller Absicht geschriebenes Spiel Nutzer ausspionieren, die zwischendurch im Web surfen.



Unter dem Radar: Der satirische Monatsrückblick

Der Juni, zwischen dem romatisch verklärten Wonnemonat Mai und den Sommerferien gelegen, sollte eigentlich zur Freude Anlass geben. Passend dazu zeigte sich zumindest das Wetter auch von seiner besten Seite. Alles gut also? Eher nicht. Wie so oft trügt wohl auch hier der Schein – oder aber manche Monate haben schlichtweg die bessere PR-Abteilung. Von Harmonie, Entspannung und sonnig schönen Gefühlen jedenfalls war in den letzten Wochen wieder einmal nicht viel zu merken. Stattdessen eskalierten wieder einmal die Ego-Streitigkeiten und Kleinkriege, wurden fleißig Fake News und alternative Fakten verbreitet und extremistische Cybers zogen marodierend durch das Land. Der ganz normale Wahnsinn also, wie unser Monatsrückblick aufdeckt.

Die CDU und das Grauen in der Wiege

Wie gesagt: das Böse lauert mitunter dort, wo man es nicht unbedingt vermutet, zum Beispiel in Kindergärten und auf Spielplätzen. Horrorfilm-Fans ist das seit „Omen“ und „The Ring“ nichts neues mehr, doch nun hat es sich anscheinend auch bis zur Politik herumgesprochen: Kinder sind böse und gefährlich, zumindest einige.

Und was macht man, wenn unter einer großen Gruppe potentiell ein bis drei Terroristen/Extremisten/Filesharer/Dämonen/extremistische Cybers sind? Richtig, einfach die ganze Gruppe überwachen. Dieser heroischen Maxime deutscher Politik der Gegenwart folgend, zog jetzt Bayerns Innenminister Joachim Hermann (CSU), für derlei Heldentaten immer zu haben, die einzig logische Schlussfolgerung: Kinder müssen endlich überwacht werden dürfen. Das wurde ja auch Zeit. Sonst lesen wir demnächst von marodierenden Kinder-Horden, die mit Keksen werfend und lautstark Rolf Zuckowski hörend plündernd und brandschatzend durch die Innenstädte ziehen, gelenkt von Satan und angefeuert von extremistischen Cybers… eine wahre Horrorvision…

Tainted Love

Auch mit der Liebe ist es mitunter kompliziert. Damit ist jetzt nicht nur der Beziehungsstatus gemeint. Es ist vielmehr so, dass auch dieses edle Gefühl mitnichten immer dort zu finden ist, wo dies behauptet wird. So verbarg sich hinter der Bezeichnung „Chemical Love“ etwa – ein schnöder Online-Drogenhändler. Bekanntlich wird im Internet ja alles gehandelt, wofür es eine Nachfrage gibt, also neben Waffen, Trojanern und Windows-Schwachstellen unter anderem auch Drogen. Der Unterschied ist, dass die Bundesregierung an Drogen, im Gegensatz zum Rest, allenfalls ein privates Interesse hat, weswegen ihr Verkauf durchaus häufiger sanktioniert wird. Folgerichtig wurden auch die Betreiber von „Chemical Love“ nun verurteilt, auf dass wieder Gerechtigkeit herrscht im Cyberland – oder sowas ähnliches zumindest.

Der geheimnisvolle Apfel

Dass man sich auf die Ehrlichkeit der Mitarbeiterinnen und Mitarbeiter nicht immer verlassen kann, musste der Technologie-Gigant Apple erfahren. Eine chinesische Mitarbeiterin des Konzerns mit dem angebissenen Obst hatte sensible Interna ausspioniert und weiterverkauft. Deswegen wurde sie nun festgenommen.

Interessant ist dabei natürlich die Frage, was für geniale Design-Ideen Apple da so versteckt. Gerade nach der wunderbaren Idee „Kopfhörer ohne Kabel für nur dreimal soviel Geld wie normale Kopfhörer“ liegt die Messlatte diesbezüglich hoch. Womöglich handelt es sich um einen Laptop, bei dem auch noch der letzte USB-Port eingespart wurde? Ein Ladegerät ohne Kabel, zu dem ein vergoldetes Adapter-Kabel für nur zweihundert US-Dollar dazu gekauft werden kann? Eine ansprechend designte Sirene, die losgeht, wann immer jemand in der Umgebung Google-Software nutzt? Oder womöglich doch endlich etwas, worauf Apple-Fans seit Jahren warten: ein Smartphone, das wasserfest ist und winterliche Temperaturen sowie einen Sturz aus 30cm Höhe auf einen flauschigen Teppich aushält… Wir dürfen gespannt sein!

Die Aussichten: wolkig bis stürmisch

GlosseWie ihr seht, sind Harmonie und Tugend nur selten zu finden. Stattdessen regieren eher die dunklen Mächte. Es ist davon auszugehen, dass das in den kommenden Monaten noch weitaus schlimmer wird – immerhin steuern wir geradewegs auf den Wahlkampf zu. Trösten wir uns damit, dass uns immerhin der Stoff für weitere satirische Betrachtungen so schnell nicht ausgehen wird. Bis es soweit ist, macht es gut und bleibt uns treu!

GROSSE EREIGNISSE WERFEN IHRE SCHATTEN VORAUS, KLEINE AUCH.

Wer sich gewundert hat, warum von mir in letzter Zeit so wenige Beiträge auf dem Blog erschienen sind, dürfte die Hintergründe nach diesem Schlusswort ein wenig besser verstehen.

Nicht nur die Erstellung des Magazins inklusive aller zusätzlichen Inhalte, die man auf Tarnkappe.info so bald nicht finden wird, nimmt viel Zeit in Anspruch. Auch hinter den Kulissen hat sich so einiges getan. Unser Kolja von Sagorski.it ***[i]*** bereitet derzeit unseren Relaunch vor. Tarnkappe.info gönnt sich dank der bislang eingegangenen Spenden ***[i]*** ein neues Wordpress-Theme und somit ein völlig neues Aussehen. Modern und schick wird es sein, wenn dann mal alles fertig ist. Und natürlich werden alle altbekannten Bestandteile wieder im Konzept enthalten sein. Manch verloren gegangene Funktion kehrt sogar zurück. Mit dem neuen Design wird es endlich wieder möglich sein, Kommentare zu liken. Diese Funktion wurde in den letzten Wochen von manchen Usern lautstark vermisst. Auch wurden in der Zwischenzeit einige Plug-ins installiert, die sich positiv auf Euer Lese-Erlebnis oder unseren Workflow auswirken sollen.

Geplant sind noch viele weitere Features, wie beispielsweise ein neues Logo und hoffentlich demnächst eine eigene gut klingende .onion-Adresse, um uns direkt im Deepweb besuchen zu können. Natürlich könnte man einfach den Tor-Browser nehmen und darin unsere reguläre URL eingeben, doch die eigene Präsenz abseits des Clearwebs dürfte unserem Image helfen, selbst wenn es bei uns niemals etwas Illegales zu kaufen oder zu laden geben wird. „Schuld“ daran ist unser Impressum und die Entscheidung, stets mit offenem Visier aufzutreten. Wir sind nicht nur der einzige deutschsprachige Blog mit dem Schwerpunkt Urheberrecht. Wir sind in diesem Bereich auch weit und breit die einzige Webseite, die offiziell mit korrekter Anschrift, Kontaktdaten, einer Betreibergesellschaft und einer separaten Steuererklärung auftritt. Letzteres brachte kürzlich sogar das örtliche Finanzamt in Erklärungsnot. Der Herr im Amt konnte uns nämlich auf Anhieb nicht erläutern, wie man Bitcoin-Einnahmen versteuern muss. *[i]*

Darüber würde man nächstes Jahr auf Basis der von uns eingereichten Belege entscheiden, teilte uns der nette Mitarbeiter aus dem provinziellen Bergisch Gladbach mit. Und nein, eine derartige Anfrage habe es bei ihm noch nie zuvor gegeben, wurde mir glaubhaft versichert. Alles andere hätte mich auch ehrlich gesagt verwundert.

Tarnkappe.info war und ist irgendwie schon seit jeher ein bisschen wie eine Boulevard-Zeitung. Auch das Produkt des Springer-Konzerns will offiziell niemand gelesen haben und trotzdem weiß aus sonderbaren Gründen jeder, was drin steht. Komisch, oder? So ähnlich wie mit der Blöd-Zeitung verhält es sich auch mit der Tarnkappe. Nur wenige geben freiwillig zu, sie zu mögen oder regelmäßig zu lesen und dennoch sprechen unsere Zugriffszahlen ihre eigene Sprache.

Wir sind ein Brennpunkt, und das nicht erst seit der Hausdurchsuchung im November 2014. Bei uns kommen häufig beide Seiten zu Wort. Das sorgt hoffentlich beim einen oder anderen

Leser für eine neue Perspektive oder dafür, dass wir ihren Horizont erweitern konnten. Wo sonst diskutieren Autoren und Piratenjäger mit Personen aus dem Graubereich? Nirgendwo. Aber genau das ist es, was der Redaktion gefällt.

Auf den meisten Konferenzen zum Thema Urheberrecht sind kontroverse Diskussionen durchweg unerwünscht. Ziel vieler Kongresse ist es, den Teilnehmern ein gutes Gefühl zu vermitteln. Da könnte den angereisten Besuchern jemand von der Gegenseite so richtig die Laune vermiesen, was kein Veranstalter will. Dann sind halt lieber nur Personen mit ähnlichen Ansichten auf dem Podium zu sehen und zu hören, das tut keinem weh. Aber es bringt gleichzeitig viel Langeweile mit sich und bringt niemanden weiter. Ein bisschen Krawall oder zumindest ein ehrlicher Meinungsaustausch auf der Bühne ist alles andere als verkehrt, finde ich. Aber gut, die Geschmäcker sind halt verschieden. Wir bleiben so oder so am Ball und entwickeln das Projekt munter weiter. Drum: Wenn mal wieder weniger vom Cheffe zu lesen sein sollte, seid Euch gewiss, dass es auch hinter den Kulissen stets viel zu erledigen gibt. Manches kann man aufschieben, wofür ich ausgewiesener Experte bin. Wer‘s nicht glaubt, der frage bitte meine Lebensgefährtin. Dinge wie die Steuererklärung kann man hingegen leider nicht auf die lange Bank schieben...

Wir sehen uns dann wieder in 8 Wochen zur nächsten Ausgabe des Tarnkappe Magazins. Bis dahin alles Gute!

Euer Lars Sobiraj.

Verantwortlich für den redaktionellen Inhalt:

Lars Sobiraj

Redaktion:
Lars Sobiraj
Annika Kremer
Antonia
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

02

digital
publishing
momentum