Jan. | Feb.

tarnkappe MAGAZIN 06

Liebe Leserinnen und Leser,
die ersten Monate dieses Jahres haben einige Risse in der Webwarez-Szene hinterlassen. Neben den Busts im Usenetbereich sind einige uralte Vertreter wie Cannapower (nur noch Useruploads), Fettrap.com oder Buchpirat.org ohne jede Vorwarnung von heute auf morgen verschwunden. Die genauen Hintergründe sind unklar und werden es wohl auch bleiben.

Im Hintergrund wird gemunkelt, dass viele Seiten offline gehen, weil ihre Betreiber immer mehr Probleme haben, ihr Hobby zu monetisieren. Der Konkurrenzkampf bei den Share- und Streaminghostern ist groß. Die Gewinnmargen, die man in Form von Vermittlungs-Provisionen weitergeben kann, sind in den letzten Jahren immer geringer geworden. Wer in diesem Bereich Geld verdienen will, muss schon jetzt über eine sehr populäre Webseite verfügen, die monatlich mehrere Millionen Seitenzugriffe generieren kann. Ansonsten kommen trotz der laufenden Serverkosten, der Kosten für die Abwehr von DDoS-Angriffen etc. kaum Umsätze herein. Spendenbereitschaft?

Tendenz gegen Null, weswegen auch der nicht öffentliche P2P-Tracker Andraste nächsten Monat die Stecker ziehen wird. Werbung? Wird von mindestens 50 % aller Besucher geblockt, Crypto-Mining ebenfalls. Wer sonst noch Geld verdienen will, müsste so richtig schmutzige Methoden einsetzen. Irgendwelche zweijährigen Verträge müssten per Abzocke an Frau und Mann gebracht, Viren als angebliche Plug-in-Updates ausgegeben oder auf den Zielrechnern Drive-By-Trojaner eingeschleust werden. Doch wer will das schon? Niemand. Denn wenn sich das herumspricht, bleiben die Besucher weg. Zumindest im Fall von Kino.to hat es deren Beliebtheit vor 10 Jahren nicht geschadet. Doch heute wirkt die Szene glücklicherweise etwas fragmentierter, das Monopol von KinoX & Movie4k ist nicht ganz so erdrückend, wie damals das von Kino.to.

Doch ist es wirklich so schlecht, dass man im Graubereich kaum noch Geld verdienen kann? Nicht unbedingt, weil sich dann mit Ausnahme der wenigen großen Fische nur noch die Leute in diesem Bereich tummeln, die beim Betrieb der Seite keine Gewinnabsichten haben und das nur noch zum Spaß machen. Am besten den Machern ist schon vorher klar, dass ihr Projekt dauerhaft ein kostendeckendes Hobby bleiben wird. Machen wir uns nichts vor: Das Internet ist schon lange kein rechtsfreier Raum mehr. Die Situation wird auf Dauer immer schlimmer und nicht besser. Das musste selbst Kim Dotcom vor einigen Jahren feststellen, als man seine Villa stürmte und Megaupload schloss. Oder RapidShare, die sich weder rechtlich gegen die Kläger durchsetzen, noch auf ein funktionierendes legales Geschäftsmodell umstellen konnten. Uploaded.net ist einer der letzten Anbieter, der die Schweiz als Standort gewählt hat. Wer heutzutage einen szenelastigen Online-Speicherdienst führen will, braucht eine Briefkastenadresse außerhalb der EU. Alles andere kann nur schiefgehen.

Schlecht für‘s Geschäft sind natürlich auch die ganzen legalen Flatrates, die in den letzten Jahren aufgekommen sind. Wer braucht noch einen kostenpflichtigen Premiumaccount bei UL.to oder SO.biz, wenn man seine ganze Musik und unzählige Filme und Serien für sprichwörtlich einen Appel und ein Ei streamen kann!? Einzig ein allumfassendes Angebot für E-Books in Form einer Verlags-Flatrate fehlt noch. Die Downloads werden zunehmend von den ausgeprägten Jägern und Sammlern getätigt, die ihre Beute auf der heimischen Festplatte speichern wollen. Immer mehr Nutzer geben sich mit dem reinen Konsum (= Stream) zufrieden.

Fazit. Mir persönlich wäre es am liebsten, die ganze Szene hätte mit dem lieben Geld rein gar nichts mehr zu tun. Einerseits wäre für die Beteiligten die Strafbarkeit im Fall einer Durchsuchung deutlich geringer und andererseits wäre alles wieder das, was es ursprünglich mal war: eine Freizeitbeschäftigung. Last, but not least sind die Piratenjäger dazu übergegangen, der Spur des Geldes zu folgen. Doch was wäre, es gäbe gar keine mehr? Ist das nicht ein Punkt über den es Mit Grüßen aus der Provinz!

Ihr Chefredakteur Lars Sobiraj

SZENE

Anonym

Themenübersicht

LAW

Themenübersicht

DIGITAL

Themenübersicht

SECURITY

Themenübersicht

Goodbye Watchers.to: Streaming-Hoster gibt auf

Der mehrsprachige Streaming-Hoster Watchers.to schließt seine Pforten. Man beendet das Angebot mit sofortiger Wirkung und gibt bekannt, man werde sich künftig auf reine Premium-Dienste für kostenpflichtige Webseiten konzentrieren. Bei über neun Millionen Seitenzugriffen monatlich war Watchers.to alles andere als klein, die meisten Besucher kamen allerdings aus den USA.

Aus die Maus. Wave Goodbye to Watchers.to! Diese Webseite ging erst im Frühjahr vor zwei Jahren online. Zeitgleich bewarb das Team dieses Streaming-Hosters seinen Dienst beim Filesharing-Forum Wjunction. Die bei Wjunction angesprochenen Uploader reagierten anfangs noch recht positiv. Zwar konnten sich einige Uploader die stark schwankende Höhe der Auszahlungen nicht erklären, aber bezahlt wurden sie. Watchers.to hatte sich auf das Speichern von Kinofilmen spezialisiert und richtete sich vor allem an den US-amerikanischen Markt. Pornos waren hingegen strikt verboten.

Die jetzige Abschiedsnachricht zeigt, dass sich der Betrieb nicht mehr finanziell gelohnt hat. Ein internal tätiger Piraterie-Experte, der anonym bleiben möchte, glaubt, es könne an der werbefreien Übertragung der Filme mittels der KODI Boxen liegen. Überall dort wo man keine Werbung ausliefern kann, wird auch kein Geld verdient. Dazu passen auch die Beschwerden, die Auslieferung der Videos per KODI würde nicht mehr funktionieren. Der Support antwortete bei Wjunction, man könne sich den wiederholt auftretenden “Fehler” nicht erklären und versuche zu analysieren, woran der Transfer scheitert. Beim Versuch blieb es dann auch. Warum ist klar: Eine Auslieferung an KODI Boxen ist sinnlos, weil für den Streaming-Hoster darüber keine Werbeeinnahmen generiert werden können. Das gelingt nur, sofern die Zuschauer mit einem Gerät samt Browser online sind. Von daher gab es nie einen Grund dafür zu sorgen, dass die KODI Boxen wieder von Watchers.to unterstützt werden.

Schon im Oktober 2016, also ein halbes Jahr nach der Gründung des Online-Speicherdienstes, wurden bei Wjunction die ersten Beschwerden der Uploader gepostet. Bei Skype sei niemand vom Support erreichbar. Auf die Nachricht per Kontaktformular habe man gar nicht erst reagiert. Ende Oktober kam es gleich mehrfach zu kompletten Ausfällen der Seite.

Wir versuchen derzeit die Administratoren von Watchers.to per Skype zu kontaktieren, bekamen aber auf unsere Presseanfrage bis jetzt keine Antwort. Sofern man unsere Kontaktanfrage bestätigen sollte, fügen wir diesem Beitrag zeitnah ein Update hinzu. Wir baten um ein kurzes Statement, um die Gründe für das kurzfristige Aus besser verstehen zu können. Auch hätten wir gerne gewusst, welche Premium-Dienste man konkret in Zukunft aufbauen möchte. Die Kommunikation hakt wohl schlichtweg an der Zeitverschiebung, weil die Betreiber wahrscheinlich im Gegensatz zur Redaktion in den USA beheimatet sind.

Für den Shutdown gebe es keinen besonderen Grund, so die Betreiber. Ihnen sei es vor allem darum gegangen, weitere Urheberrechtsverletzungen vorzubeugen. Das Uploaden von Pornos sei vom ersten Tag an verboten gewesen. Wenn jemand dabei erwischt wurde oder das Copyright Dritter verletzt habe, wurden die Dateien gelöscht und die Nutzer verbannt. „Sie haben dann einfach einen neuen Account angelegt, um das gleiche wieder zu tun. Deswegen mussten wir etwas dagegen unternehmen“, schrieben uns die Betreiber heute im Chat bei Skype.

Illegaler Handel mit Datensätzen: Polizei nimmt Kölner fest

Gemäß einer Pressemitteilung vom 26.02.2018 gelang der Zentralstelle Cybercrime Bayern und der Kriminalpolizeiinspektion Ingolstadt ein gemeinsamer Schlag gegen den Handel mit illegalen Datensätzen im Internet. Ein 24-jähriger Kölner soll jahrelang im großen Stil illegal erworbene Keditkartendaten in einem Internetforum zum Verkauf angeboten haben. Auf die Spur kamen ihm die Ermittler, als er den Webserver eines Online-Händlers angegriffen hat.

Nachdem der Kölner Mitte 2016 von einem Webserver eines großen bayerischen Online-Versandhändlers mittels SQL-Injektion rund eine halbe Millionen Datensätze von Kunden erbeutet hatte, nahmen Ermittler seine Spur auf und intensive Untersuchungen führten die Staatsanwälte der bei der Generalstaatsanwaltschaft Bamberg errichteten Zentralstelle Cybercrime Bayern und die Computerspezialisten der Kriminalpolizeiinspektion Ingolstadt schließlich zu dem 24-jährigen Tatverdächtigen.

Die Generalstaatsanwaltschaft Bamberg erwirkte daraufhin sowohl einen Haftbefehl, als auch einen Durchsuchungsbeschluss gegen den Beschuldigten. Beide Beschlüsse wurden am 6. Februar in Köln von Beamten der Ingolstädter Kriminalpolizei unterstützt und durch Kollegen aus Nordrhein-Westfalen vollzogen. Zudem waren Kräfte einer Spezialeinheit im Einsatz. Zum Zeitpunkt der Hausdurchsuchung wurde der 24-Jährige in seiner Wohnung angetroffen und widerstandslos festgenommen. Die Beamten stellten einen PC, drei Handys, zwei Notebooks sowie zahlreiche Speichermedien als Beweismittel sicher.

Man geht derzeit davon aus, dass der 24-Jährige im Zeitraum zwischen August 2013 und Mai 2015 auf dem ehemaligen Underground-Economy-Forum „crimenetwork.biz“ aktiv war. Dort soll der Beschuldigte unter seinem Pseudonym in einer Vielzahl von Fällen rechtswidrig erlangte Zugangsdaten zu dem Online-Zahlungsdienstleister Paypal und Kreditkartendaten gewinnbringend verkauft haben. Die Daten soll er sich zuvor durch das massenhafte Versenden von Phishingmails über einen von ihm eigens hierzu betriebenen Server beschafft haben. Die Mailadressen für seine Phishingkampagnen wiederum soll er sich durch Angriffe auf verschiedene Webshops besorgt haben. Seine Kunden auf crimenetwork.biz nutzten die von ihm bezogenen Daten für betrügerische Bestellungen im Internet.

Bereits erste Auswertungen des sichergestellten Beweismaterials haben den Tatverdacht bestätigt und zudem zahlreiche weitere Straftaten ergeben. Somit wurde der Haftbefehl bereits am 22. Februar erweitert. Der Mann sitzt nun in Untersuchungshaft, da der Ermittlungsrichter von Flucht- und Verdunkelungsgefahr ausgeht. Dem 24-Jährigen drohen der Staatsanwaltschaft zufolge bis zu zehn Jahre Haft.

Internetselbstverwaltung á la RIPE NCC: ein Himmelreich für Kriminelle

Der norddeutsche Piraterie-Experte Volker Rieck erläutert in seinem neuesten Artikel, wie die Internetselbstverwaltung RIPE NCC die Online-Piraterie auf internationaler Ebene aktiv unterstützt. Der Beitrag erschien vor sieben Tagen bei Webschauder.de und wird hier mit freundlicher Erlaubnis des Autors veröffentlicht. Jedes Jahr im Januar veröffentlicht das US Handelsministerium (USTR) eine Liste der schlimmsten Rechtsverletzer im Internet für das vergangene Jahr. Dabei geht es sowohl um haptische Ware, also Fälschungen, Replikas usw. als auch um Verletzungen von geistigen Eigentum in Form von nichtregulierter Distribution von Filmen, Büchern, Musik, Software, Apps usw. Es finden sich auf der Liste also Namen wie die chinesischen E-Commerce-Giganten Alibaba und Taobao, aber ebenso Webseiten wie Movie4k, Libgen, The Pirate Bay oder openload.co. Die Liste wird unter anderem gespeist von Verbänden wie der Motion Picture Association of America (MPAA), der US-Filmwirtschaft, oder der Recording Industry Association of America (RIAA), also der US-Musikwirtschaft. Welche Rolle dabei die Internetselbstverwaltung RIPE Network Coordination Centre (NCC) spielt, soll hier weiter beleuchtet werden.

Und ewig grüßt das Murmeltier

Seit Jahren findet sich der Name eines Host Providers auf der USTR Liste: Private Layer aus Panama bzw. der Schweiz. So ganz sicher ist sich der Bericht in dieser Hinsicht nicht. Dieses Unternehmen stellt anderen „Unternehmen“ Serverplatz und Bandbreite zur Verfügung. Zu den „Kunden“ von Private Layer gehörten im Jahr 2017 nach dem USTR Bericht Seiten wie 1337x.to oder primewire.ag. Weitere Kandidaten, die sich der Dienste von Private Layer bedienen, sind z. B. youwatch.org, firedrive.com oder sockshare.com. Allesamt Seiten, die massenhaft Rechte Dritter verletzen.

Der Bericht des Handelsministeriums vermerkt zu Private Layer:

Die Betreiber handeln mehr oder weniger anonym und reagieren nicht auf Inkenntnis-Setzung über Rechteverletzungen. Die Kunden von Private Layer handeln genauso.

Ein genauerer Blick auf das Unternehmen lohnt sich daher. Private Layer ist Mitglied bei RIPE NCC (Réseaux IP Européens Network Coordination Centre), eine von weltweit fünf Organisationen, die in erster Linie für die Vergabe von IP-Adressen und sogenannte Autonomen System Nummern (ASN) verantwortlich sind. Ohne solche Autonome System Nummern und IP-Adressen wäre keine Webseite im Internet erreichbar, von der Einwahl ins Internet ganz zu schweigen.

Das Gebiet, welches RIPE NCC als quasi Arm der Internetselbstverwaltung ICANN dabei verantwortet, umfasst Europa und Teile Asiens. Es umfasst nicht Mittel- und Südamerika, dafür wäre die Schwesterorganisation LACNIC zuständig. Trotzdem kann ein Unternehmen wie Private Layer aus Panama Mitglied bei RIPE NCC werden, dort eine Autonome System Nummer (ASN) erhalten und IP Nummernkreise vergeben, die es zuvor von RIPE NCC erhalten hat.

Eine Nachfrage bei RIPE NCC, wieso ein Unternehmen aus Mittelamerika so problemlos in Europa Geschäfte mit Hilfe von RIPE NCC machen kann, wurde nach mehrmaligen E-Mails so beantwortet:

Sofern ein Unternehmen Aktivitäten in Europe entfaltet, kann es auch Mitglied bei RIPE NCC werden.

So weit, so gut. Wer nun möglicherweise denkt, dass das panamaische Unternehmen ein Rechenzentrum in der Schweiz betreibt, der wird leider enttäuscht. Zwar weist die Anschrift in der RIPE NCC-Datenbank eine Adresse in Zürich aus, es ist aber lediglich die Anschrift eines Briefzentrums (siehe Foto rechts von Christian Bütighofer). Wir gehen an dieser Stelle einmal davon aus, dass ein Postfach (nach deutschem Recht) kein Sitz eines Unternehmens ist und schon gar kein Rechenzentrum darstellt.

Ein Besuch in Panama

Wenn also schon kein Firmensitz in der Schweiz, dann müsste das Unternehmen doch an der von RIPE ausgewiesenen Anschrift in Panama zu finden sein.

Aber auch hier wird man nicht fündig. Ein persönlicher Besuch in Panama im Jahr 2015 an der von RIPE NCC angeführten Anschrift führte zwar zu einem Bürogebäude – aber dort ist kein Unternehmen Private Layer Inc. ansässig. Es gibt kein Büro im 17. Stock von Private Layer, kein Postfach und auch keinen Klingelknopf für die Firma Private Layer.

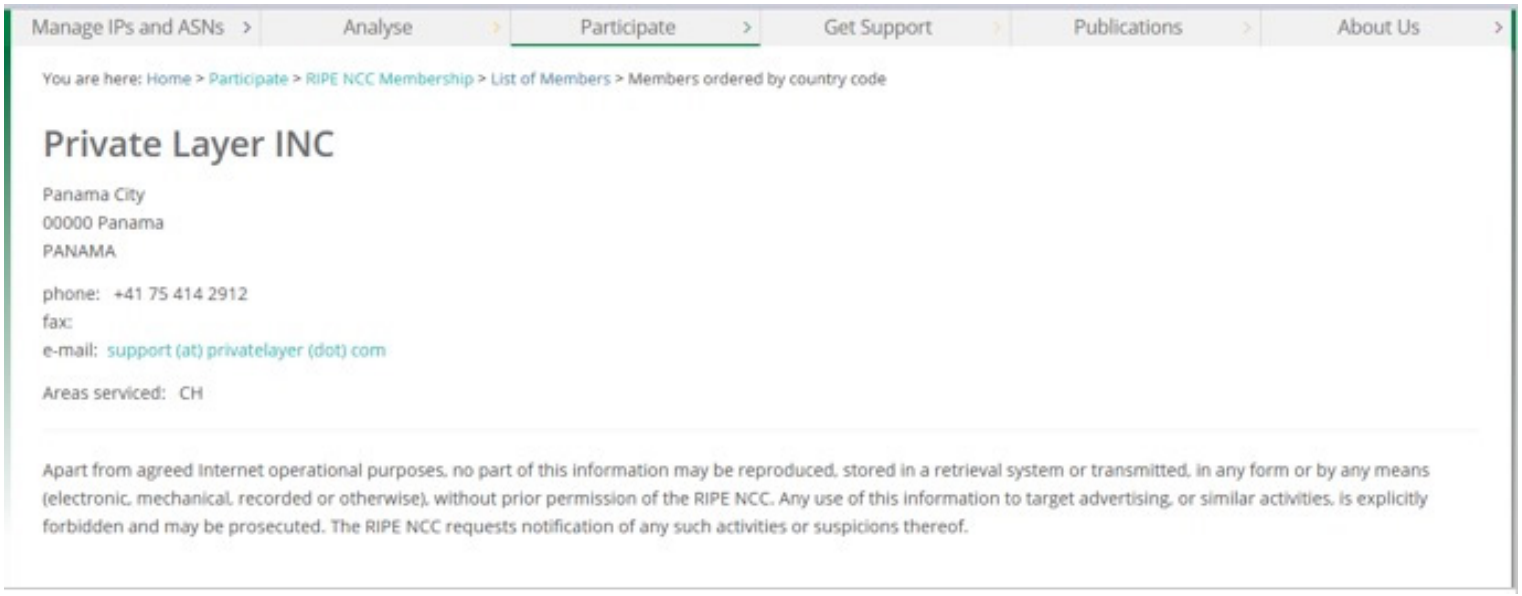
Der Weg nach Zürich

RIPE NCC betreibt keine sogenannte GEO IP Datenbank. Andere Dienste wie z. B. Maxmind aus den USA aber schon. Anhand einer solchen Datenbank kann ermittelt werden, wo sich das Rechenzentrum befindet, das einer bestimmten IP zugeordnet wurde.

Im Fall von Private Layer ist das tatsächlich Zürich, aber nicht das erwähnte Postfach sondern eine der Züricher Außenstellen des US-Unternehmens Equinix Inc. Dort hat Private Layer entweder Server gemietet oder es benutzt Platz im Rechenzentrum von Equinix und hat dort eigene Hardware stehen. Wie man es dreht oder wendet, die Firma Private Layer benutzt also die Infrastruktur von Equinix. Auf die Beteiligung durch Equinix soll in diesem Zusammenhang nicht weiter eingegangen werden.

barkeit, nämlich sowohl der eigenen als auch die der „Kunden". Die o.g. Kunden von Private Layer scheuen die Öffentlichkeit. So gut wie alle WhoIs Einträge (wer betreibt die Domain?) der Seiten, die bei Private Layer gehostet sind, wurden durch spezielle WhoIs Dienste verschleiert. Wer die Seiten in Sachen Rechteverletzung erreichen will, landet allenfalls bei einem Kontaktformular aber niemals bei einem Unternehmen oder gar dem Betreiber. Aber auch der Weg über den Vermieter der Server, also Private Layer, ist ein Dead End.

Wie beschrieben ist der Sitz des Unternehmens entweder ein Postfach in der Schweiz (welches sicher ab und zu geleert wird) oder eine nicht existente Anschrift in Panama. Bei beiden kann man nicht zustellen, geschweige denn jemanden persönlich erreichen. Wer also ungestört seinem



Alles hat seinen Preis

Werfen wir einen Blick auf die Preisliste von Private Layer. Der kleinste Server kostet dort im Monat 89 US-Dollar. Technisch sind die angebotenen Server nicht gerade auf dem neuesten Stand, sie haben einen Prozessor, den Intel im Jahr 2010 auf den Markt gebracht hat und daher ist die Servermiete auch nur schwer mit den Preisen der Konkurrenz vergleichbar. Man findet schlicht kaum einen Anbieter mit derartig veralteter Hardware.

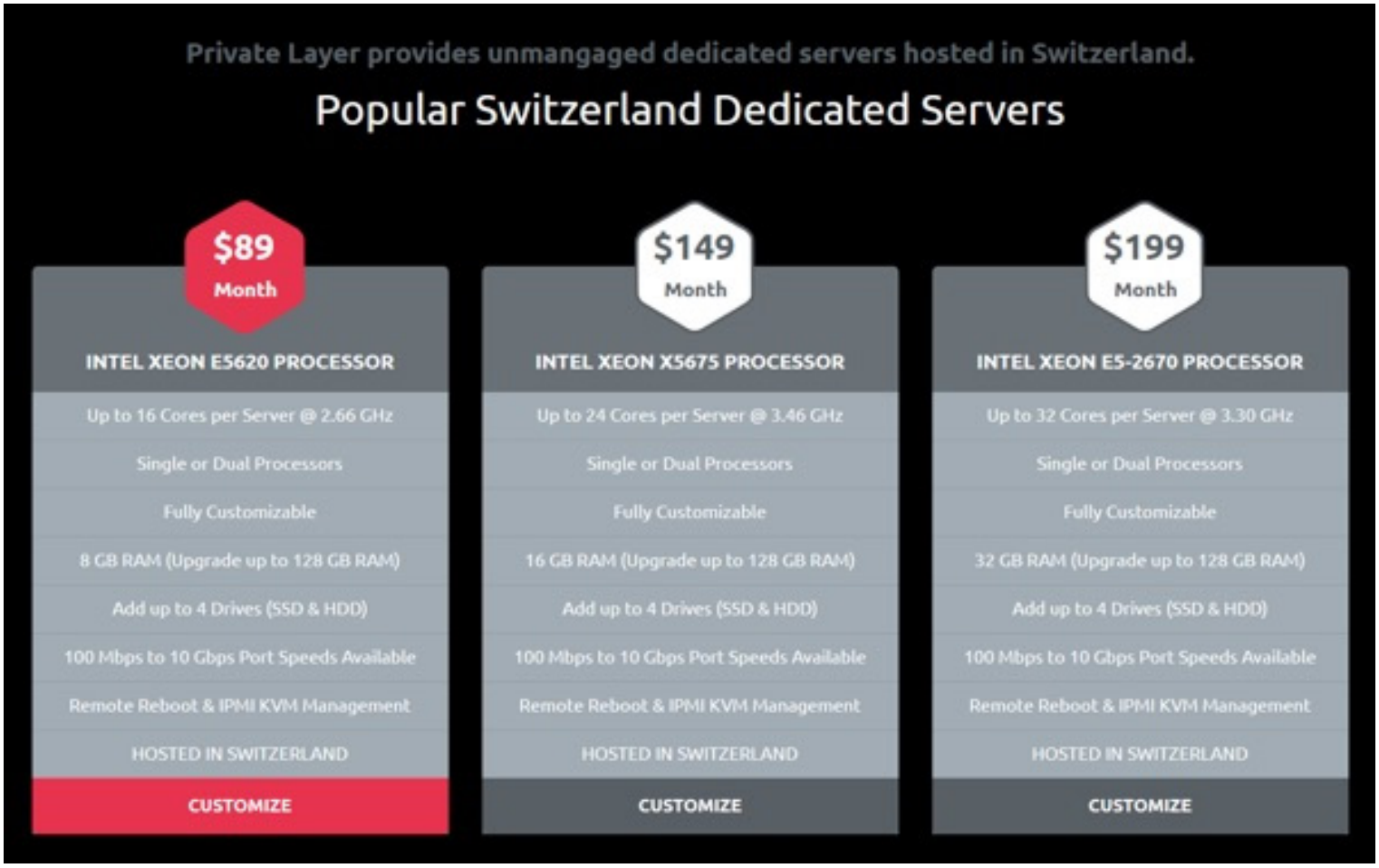
Man kann in Deutschland Webserver mit der ca. vier bis sechsfachen Leistung (inklusive bessere Prozessoren, mehr Arbeitsspeicher usw.) für weniger als die Hälfte des Preises mieten. Es kann also nicht der Preis allein sein, warum Private Layer so lange am Markt agieren kann, denn der ist stark überteuert. Die Antwort findet sich im Papier des US Handelsministerium: Private Layer bietet ein sogenanntes Hidden Feature an und das ist die Nichterreich-

Geschäft nachgehen will, der bezahlt für einen schwachen Server vergleichsweise viel Geld. Dieser Kunde braucht aber keine unangenehmen Nachforschungen zu befürchten.

Alles Fake – uns doch egal

Wie kann ein nicht-existierendes Unternehmen mit einem Briefkasten in Zürich Mitglied in einer Organisation (RIPE NCC) werden, die für den reibungslosen Betrieb des Internet zuständig ist? Ein Unternehmen, dessen Geschäftszweck die Bereitstellung von Infrastruktur und die Abschirmung für Rechtsverletzer ist. Genau diese Frage haben wir RIPE NCC gestellt. Die Antwort ist verblüffend. Natürlich legt RIPE NCC nach eigenen Aussagen Wert auf akkurate Daten. Allerdings unterscheidet man dort zwischen den Mitgliederdaten (also internen und höchst privaten Daten) und den Kontaktdaten, die extern gezeigt werden.

Die internen Daten werden demnach durch Abgleich mit offiziellen Firmendokumenten geprüft. Bei den externen Daten muss das RIPE NCC Mitglied nur eines beachten: Es muss dort irgendeine Anschrift stehen, die allerdings nicht verifiziert wird sowie eine beliebige E-Mail-Adresse. Diese wird allerdings auch nicht verifiziert. Es reicht, wenn sie vorhanden ist, denn RIPE NCC betont, dass man nicht dafür Sorge tragen kann, dass die Mitglieder auch antworten.



Bei offensichtlich falschen Daten „kann“ RIPE das Mitglied kontaktieren und für Klärung sorgen – kann. Aber erst dann, wenn das Mitglied nicht antwortet oder sich Daten als falsch erweisen sollten, kann RIPE NCC es gemäß seiner Statuten ausschließen – kann. Laut eigenen Aussagen sieht RIPE sich nicht in einer strafenden Rolle, RIPE NCC will eigentlich nur Daten bereitstellen. Wie die Qualität der Daten ist, das ist eigentlich egal. Auf Anfrage wurde betont, dass Derjenige, der einen Missbrauch meldet, natürlich keinen Anspruch auf Auskunft hat, was aus dem Fall geworden ist.

Auskunft ist ohnehin ein gutes Stichwort. In einem eigenen Punkt auf der Webseite klärt RIPE NCC über Anfragen von LEA (Law Enforcement Agencies) auf. Weil die Privatsphäre der Mitglieder wichtig sei, werden lediglich die öffentlichen Informationen weitergegeben. Wie man am Beispiel Private Layer sieht, sind diese Informationen falsch und somit wertlos, abgesehen davon, dass man diese Fakes jederzeit in der RIPE NCC Datenbank einsehen kann. Dafür muss niemand anrufen oder sich per E-Mail an die RIPE wenden. Weitergehende Informationen würde man nicht ohne Gerichtsbeschluss oder offizielle Anordnung herausgeben. Natürlich nach niederländischem Recht. Zitat des Statements:

“In such cases, the RIPE NCC strives to protect the interests of its members and will not provide any confidential or private information to LEAs without a court order or other legally enforceable order or request under Dutch law.”

Dass RIPE NCC auch nach niederländischem Recht verpflichtet wäre, bei Urheberrechtsverletzungen die Angaben des Inhabers ohne Richtervorbehalt herauszugeben, hat ein nordholländisches Gericht im Falle EWEKA entschieden. Die Achse der Verantwortungsdiffusion zieht sich also von oben nach unten durch. Leittragende sind die Rechteinhaber, deren Rechte tagtäglich verletzt werden und die kaum eine Chance haben sich dagegen zu wehren, weil auf allen Ebenen getäuscht und getrickst wird.

Fazit

Es ist eigentlich an der Zeit, die Rolle von solchen Selbstverwaltungen und Selbstregulierungen wie ICANN/RIPE NCC kritischer zu betrachten. Die Art und Weise wie hier agiert wird, schafft nahezu rechtsfreie Räume, die ein Traum für jeden Cyberkriminellen darstellen. Das Beispiel Private Layer beweist es eindrucksvoll und ist leider auch kein Einzelfall. Statt also politisch an den Symptomen von Fehlentwicklungen im Internet zu arbeiten, sollten die Ursachen analysiert und eindeutig geregelt werden. Eigentlich nur so wie in der Realität (Kohlenstoffwelt), wo z. B. selbst jeder kleine Wochenmarktstand eine Kennzeichnung des Betreibers braucht. Man stelle sich einen Marktverkauf von verdorbenen Lebensmitteln vor, bei denen der Marktmeister die Herausgabe der Verkäuferdaten mit Verweis auf die eigenen Regeln und die Privatsphäre des Verkäufers verweigert.

Übrigens. Am 13.02.2018, 7 Tage nach der Meldung bei RIPE NCC, werden auf deren Webseite weiterhin völlig falsche Daten über den Kunden Private Layer veröffentlicht. Der Gesetzgeber sollte sich einmal die Frage stellen, wieso er sich im Internetverkehr die Grundregeln des Netzes von nicht demokratisch legitimierten Institutionen diktieren lässt, die sogar aktive Mithilfe bei Rechtsverletzungen leisten.

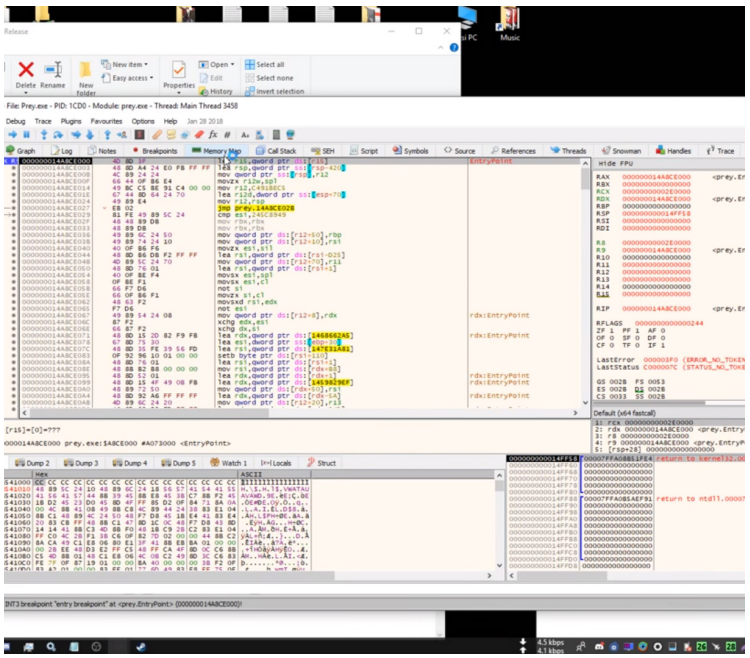
Video: Voksi zeigt, wie Denuvo geknackt wird

Der bulgarische Cracker Voksi von der Release-Group Revolt zeigt ein einem neunzigminütigen Video erstmals live, wie man den aktuellen Kopierschutz der österreichischen Firma Denuvo umgehen kann. Er tut dies anhand eines praktischen Beispiels.

Bis Conspiracy (CPY) kürzlich die Kombination aus drei verschiedenen Schutzsystemen umgangen hat, konnte Ubisofts PC-Spiel „Assassins Creed Origin“ für mehrere Monate in Folge des Kopierschutzes nicht illegal in Umlauf gebracht werden. Bis zum Release des Cracks dürfte der Schutz dem Publisher für einen ausreichenden Umsatz gesorgt haben. Und genau das ist auch das Ziel von Denuvo. Es kann letztlich nicht darum gehen, ein unknackbares System zu erschaffen, weil es das nicht gibt. Es geht darum die Release Groups davon abzuhalten, die Windows-Games direkt nach dem Verkaufsstart illegal zu verbreiten.

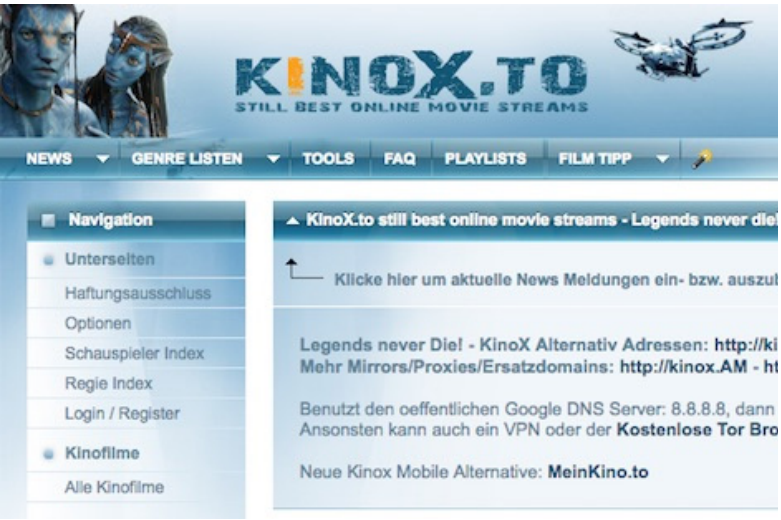
Der bulgarische Cracker Voksi zeigt nun in einem stummgeschalteten Video, wie man Denuvos V4 Anti-Tamper Technologie erfolgreich umgehen kann. Wir haben das Video am Ende dieses Beitrages eingebunden, es ist aber nur etwas für wenige Eingeweihte. Alle anderen Zuschauer können mit Voksis Videoanleitung sicher nur sehr wenig anfangen. Man darf aber gespannt sein, wie lange das Video noch online bleiben wird, zumal man die Zuschauer dort zu einer illegalen Handlung auffordert.

Bei den Kollegen von Torrentfreak erklärt Voksi, Revolt habe als Gruppe mit nur einem Ziel angefangen. Man wollte schwarzkopierten Spielen den fehlenden Multiplayer-Support hinzufügen. Bis dahin hat sich in der Szene sonst niemand damit beschäftigt. Mithilfe der Cracks kann man eigene Server für das Spiel gegeneinander benutzen, ohne die Games kaufen zu müssen. Revolt war außerdem eine der ersten Gruppen, denen das Umgehen des Kopierschutzes von Denuvo gelungen ist. Die Gruppenmitglieder tauschen sich im einem eigenen Forum unter der URL revolt.group aus.



Voksi: "In an ideal world, Denuvo would die."

Wenn es nach dem Bulgaren geht, würde sich Denuvo schon bald in Wohlgefallen auflösen. Den Gefallen wird man ihm aber nicht tun, zumal das Unternehmen seit der Übernahme durch Irdeto international aufgestellt ist und nun über einige neue Techniker der Naspers-Gruppe verfügt, die auf das Thema Verschlüsselung und den Schutz von Inhalten spezialisiert sind. Das Hase-und-Igel-Spiel zwischen der Szene und den Programmierern von Denuvo geht also schlichtweg in die nächste Runde. Da V4 umgangen werden kann, wird der Hersteller sicher schon an einer neuen Version arbeiten.



KinoX für Vodafone-Kabelkunden gesperrt

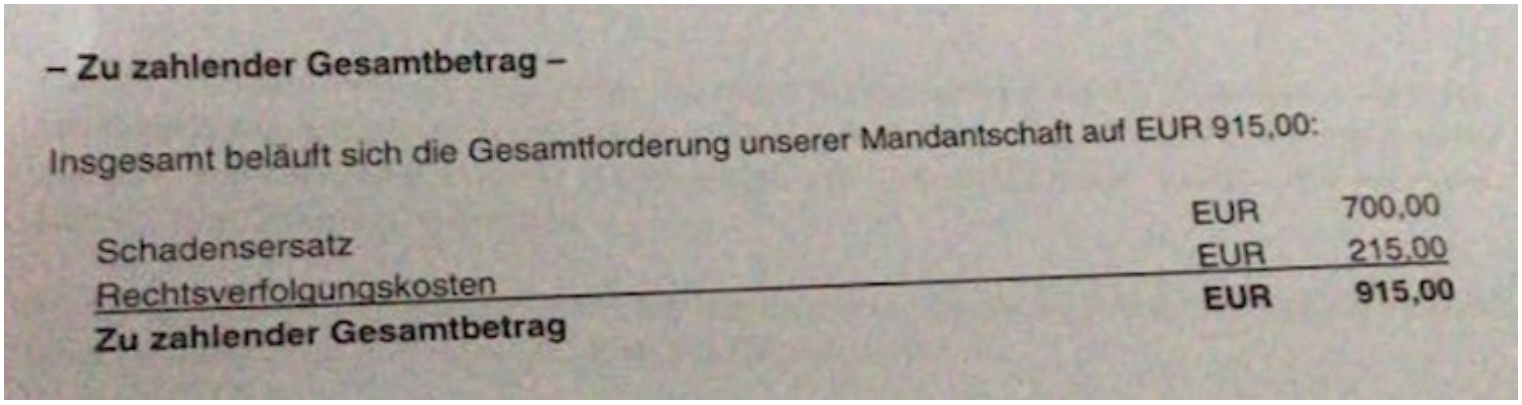
Constantin Film hat Anfang Februar per einstweiliger Verfügung vor dem Landgericht München durchgesetzt, dass Vodafone Kabel all ihren Kunden den Zugang zur Webseite KinoX.to sperren muss. Statt des Streaming-Portals erscheint lediglich die Sperrseite des Kabel-Anbieters. Auf Anfrage der Kollegen von Golem.de hat Vodafone Kabel bestätigt, dass sie aufgrund der einstweiligen Verfügung vom 1. Februar allen Nutzern den Zugang zu KinoX.to sperren müssen. Weil es sich um ein offenes Verfahren handelt, wollte Vodafone dazu keine weitere Stellungnahme abgeben. Constantin Film beruft sich offenbar auf das Filmspeler-Urteil des EuGH, wie Golem mutmaßt. Weder die Bundesnetzagentur, noch Constantin Film wollten bis zum jetzigen Zeitpunkt einen Kommentar zur Sachlage abgeben. Auch KinoX selbst hat dazu auf der Hauptseite noch kein Statement verfasst.

Derzeit erhalten die Kunden beim Aufruf des Kino.to-Nachfolgers lediglich den Hinweis: „Dieses Portal ist aufgrund eines urheberrechtlichen Anspruchs vorläufig nicht verfügbar." Die Sperrung erfolgt offenbar über die Blockade der einzelnen DNS-Einträge und nicht über ausgefeilte Sperr-Techniken. Da der Trafic nicht per Deep Packet Inspection etc. untersucht wird, können die Vodafonen-Kunden die Seite noch immer über den Google-Dienst (8.8.8.8) oder Quad9 (9.9.9.9) erreichen. Im Fall einer dauerhaften Sperre könnte man den DNS-Dienst auch in den Einstellungen des Betriebssystems vermerken, damit die normale DNS gar nicht mehr genutzt wird. Natürlich wäre der Filmgenuss dennoch laut EuGH nicht legal.

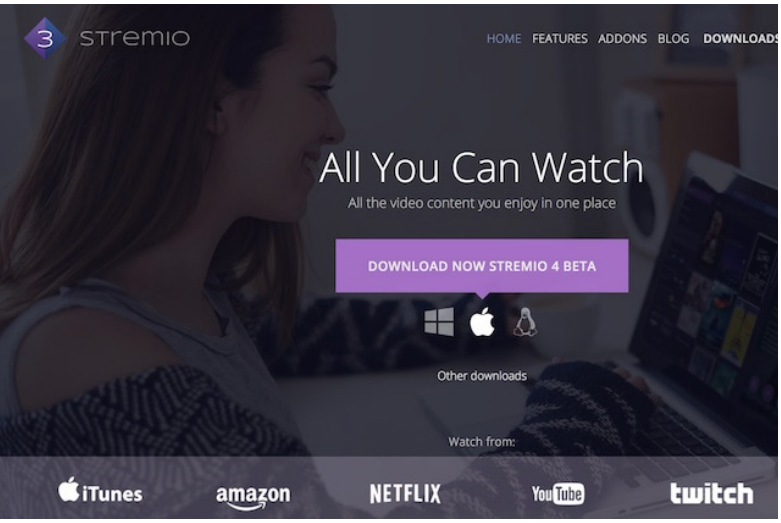
Vodafone-Sperre von KinoX nur der Anfang?

Bisher ist unklar, warum sich Vodafone überhaupt der juristischen Maßnahme des Filmstudios so bereitwillig gebeugt hat. Eine einstweilige Verfügung ist harter Tobak, aber noch lange kein Urteil. Sollte Vodafone bei der Sperre bleiben, würde es wohl auch nicht mehr zu einem Gerichtsverfahren kommen, weil die Gegenseite mithilfe ihres Eilverfahrens ihre Forderung durchgesetzt hat. Wahrscheinlich ist dies nur der Anfang. Es drohen bei anderen Internet-Anbietern weitere Netzsperren, weil man glaubt, damit die eigenen Werke effektiv schützen zu können. Bleibt abzuwarten, ob die anderen ISPs auch so hilfsbereit zur Rechtsdurchsetzung der Content-Firmen beitragen wollen. Wahrscheinlich nicht.

Die Firma @vodafone_de hat #Internetsperren wegen mut-



maßlicher Urheberrechtsverletzungen eingeführt, sperren die demnächst #Twitter? @netzpolitik @sixtus @ChrisStoecker @RAStadler @chaosupdates pic.twitter.com/FyBKBKNQPl — (((i))) (@YoungSocialist) 11. Februar 2018



Warnung vor Stremio: Abmahnungen garantiert!

Nach eigenen Angaben verfügt der Popcorn Time-Nachfolger Stremio über vier Millionen Nutzer. Das Dumme dabei: Wer die Software installiert, wird früher oder später eine Abmahnung kassieren, obwohl man sich noch gar keinen Film angesehen hat. Direkt nach der Installation wird ohne weiteres Zutun schon der erste P2P-Transfer initiiert.

Wir haben bereits im Jahr 2015 ausführlich vor der Nutzung von Stremio gewarnt. Nachdem die P2P-Streaming Software Popcorn Time vom Netz genommen wurde, gingen mehrere Nachfolger online, von denen Stremio seit November 2015 über vier Millionen Nutzer für sich gewinnen konnte. Das Prinzip dahinter ist aber das gleiche wie bei Popcorn Time. Nach der Installation auf iOS- beziehungsweise Android-Smartphones oder auf Linux-, Windows- bzw. Mac OS X- PCs kann man sich diverse aktuelle Kinofilme und Fernsehserien anschauen. Unter der Haube befindet sich nämlich ein ganz normales P2P-Programm, die eigene IP-Adresse wird dabei augenblicklich an alle Tauschpartner übertragen. Von dem gefährlichen Transfer, der nach außen wie Streaming aussehen soll, bekommt der Nutzer aber nichts mit. Auch wenn weder in der Software noch auf der Webseite vor jeglichen Gefahren gewarnt werden, so drohen teure Abmahnungen.

Stremio: Abmahnung in Höhe von 915 Euro auch ohne Filmgenuss

Was Stremio nun noch riskanter macht ist die Tatsache, dass man offenbar auch dann Abmahnungen erhalten kann, wenn man noch gar keinen Film konsumiert hat. Wir haben uns Scans einer Abmahnung zuschicken lassen, die kürzlich die Kanzlei Waldorf Frommer verschickt hat. Am 04.02. wurde vom Leipziger IT Dienstleister Digital Forensics GmbH eine Rechtsverletzung des Filmes „Es (It)“ von Warner Bros. dokumentiert. Der Nutzer schwört aber Stein und Bein, dass er sich weder diesen noch bisher einen anderen Film mittels Stremio angeschaut hat. Wie dem auch sei. Bis zum 27. Februar soll der Abgemahnte 915 Euro bezahlen und schon vorher die unterzeichnete Unterlassungserklärung an die gegnerische Kanzlei übermitteln. Böse gesagt ist dies für die Münchener Kanzlei eine Abmahnung nach dem Copy & Paste-System. Das erklärt auch die schnelle Reaktionszeit von der Urheberrechtsverletzung bis zur verschickten Abmahnung. Lediglich der Name des Empfängers, Werkes und des Mandanten, der individuelle File-Hash, die festgehaltene IP-Adresse und die Tatzeit müssen dabei verändert werden. In der Abmahnung wird sogar explizit vor „vermeintlichen Streaming-Diensten“, wie Time4Popcorn, Popcorn Time, Cuevana, Zone und Isoplex gewarnt. Stremio hatte man in Süddeutschland wohl bisher noch nicht auf dem Schirm. Für Waldorf Frommer macht der Client auch keinen Unterschied, denn der Abgemahnte hat stets beim Filmgenuss die gleiche P2P-Tauschbörse genutzt, egal welches Programm im Einsatz war.

Stremio-Abmahnung erhalten: wie reagieren?

Betroffene sollten sich unbedingt einen Fachanwalt für Medien- und Internetrecht nehmen. Bitte keinen Feld-, Wald- und Wiesenjuristen, der wenig bis gar keine Erfahrung beim Umgang mit P2P-Abmahnungen hat! Wer seinen Film in Kombination mit dem Suchbegriff Abmahnung bei Google eingibt, wird auch einen Fachanwalt in seiner Nähe finden. Der Anwalt wird nach seiner Beauftragung versuchen, die Höhe der Abmahnung zu reduzieren, was auch oft gelingt. Auf gar keinen Fall die geforderte Unterlassungserklärung eigenmächtig unterschreiben, denn damit verzichtet man freiwillig auf alle seine Rechte. Dann kann einem auch kein Anwalt mehr helfen!

Alternativen

Neben Cuevana, Zone oder Isoplex gibt es für das Streaming von Filmen noch zahlreiche Möglichkeiten, die allerdings nicht auf der gefährlichen Filesharing-Technologie basieren. Eine Option von vielen ist beispielsweise die Box bzw. Software von Vavoo.tv, bei der die Daten von einem Sharehoster an die Nutzer übertragen werden.

Nach Angaben des Karlsruher Fachanwaltes Benedikt Klas ist die Benutzung von VAVOO in Deutschland auch nach dem Filmspeler-Urteil des EuGH komplett legal. Dies sei juristisch gesehen wie ein Werkzeug zu sehen. Auch mit einem Browser könne man wahlweise legale als auch illegale Webseiten besuchen, ohne dass die Mozilla Foundation als Browser-Hersteller dafür verklagt wird. Ganz genauso verhält es sich mit der TV Box und der kostenlosen Software Vavoo. Was die Benutzer am Ende des Tages mit ihrem Mediacenter anstellen, bleibt alleine ihnen überlassen.

Infraud: US-Justiz gelingt Schlag gegen Cybercrime-Ring

US-Behörden haben einen groß angelegten Betrug eines weltweit agierenden Rings von Cyberkriminellen aufgedeckt. Insgesamt seien 36 Mitglieder der seit 2010 aktiven Plattform "Infraud" aus den USA und 17 weiteren Ländern angeklagt worden, weltweit wurden 13 Mitglieder der Organisation festgenommen. Die Festnahmen erfolgten in Zusammenarbeit mit den Justizbehörden der jeweiligen Länder, teilte das Justizministerium in Washington am 07.02 mit.

Nach den Erkenntnissen der Ermittler hätten die Verdächtigen das Internetforum "Infraud" als Plattform für den Tausch und Handel mit persönlichen Daten, vor allem mit geknackten Kreditkarten, gestohlenen Ausweisdokumenten, entwendeten Finanz- und Bankinformationen, Schadsoftware, Sozialversicherungsnummern und Passwörtern genutzt. Unter dem Slogan "In Fraud We Trust" habe die Organisation Anfragen nach den illegalen Waren an automatisierte Verkaufsstellen der "Infraud"-Mitglieder im Netz weitergeleitet und abgesichert. "Infraud" zählte noch im März vergangenen Jahres 10.901 Mitglieder.

Das US-Justizministerium bezeichnete das illegale Forum als: "wahrhaft erste Adresse für Cyberkriminelle weltweit". Durch den Ring seien Banken, Unternehmen und Privatkunden um mehr als 530 Millionen Dollar (428 Millionen Euro) geschädigt worden. Weltweit wurden bislang 13 Mitglieder der Organisation festgenommen, darunter stammen fünf aus den USA. Die anderen Beteiligten sind aus Frankreich, Italien, Australien, Großbritannien, Serbien und Albanien. Der in der Ukraine ansässige Svyatoslav B. (34), von dem man glaubt, dass er Infraud im Jahr 2010 gegründet hat und der im Dark Web mit den Tarnnamen „Obnon", „Rector" und „Helkern" unterwegs gewesen sein soll, ist nicht gefasst worden, außer ihm sind noch fünf weitere Verdächtige auf freiem Fuß. Die Nummer zwei, der russische Mitgründer Sergej Medwedew, sei hingegen festgenommen worden. Die Festnahmen und Anklagen gehörten "zu den bislang bedeutendsten im Bereich Cyberkriminalität", so das US-Justizministerium. Die Amerikaner, die mit Infraud zu tun haben, sind bereits vor Gericht erschienen und könnten mit mehr als 30 Jahren Gefängnis rechnen, wenn sie für schuldig befunden werden, berichtet engadget.

Im Zuge der Ermittlungen haben die Strafverfolger detaillierte Informationen über die Funktionsweise von Infraud, deren Mitglieder und Aufgaben erhalten. So hatten Infraud-Insider definierte Rollen innerhalb der Hierarchie der Organisation inne. "Administratoren" verwalteten den täglichen Betrieb und wären verantwortlich gewesen für die strategische Planung, die Überprüfung und Genehmigung der Mitglieder, sie erteilten den Mitgliedern Strafen und Belohnungen. "Super-Moderatoren" überwachten und verwalteten spezifische Themenbereiche innerhalb ihres Fachwissens. "Moderatoren" moderierten ein oder zwei spezifische Unterforen innerhalb ihrer Fachgebiete. "Verkäufer" verkauften illegale Produkte und Dienstleistungen an Infraud-Mitglieder. Schließlich nutzten "VIP-Mitglieder" und "Mitglieder" das Infraud-Forum, um Informationen zu sammeln und ihre kriminellen Aktivitäten abzuwickeln. Die Festnahmen und Anklagen gehörten "zu den bislang bedeutendsten im Bereich Cyberkriminalität".

US-Staatsanwalt Dayle Elieson vom US-Distrikt Nevada gibt bekannt: "Infraud operierte wie ein Unternehmen, um Cyberkriminalität auf globaler Ebene zu ermöglichen." Es habe sich um eine der größten Ermittlungen gehandelt, die jemals vom Justizministerium vorgenommen worden sei. Die US-Justiz weigere

sich, Cyberkriminellen zu erlauben, die wahrgenommene Anonymität des Internets als Schutzschild für ihre Verbrechen zu nutzen: “Wir verpflichten uns, eng mit unseren internationalen Partnern zusammenzuarbeiten, um die Urheber dieser Verbrechen zu identifizieren und vor Gericht zu bringen, wo auch immer auf der Welt sie tätig sein werden. Die US-Staatsanwaltschaft ist dazu verpflichtet, Amerikas nationale und wirtschaftliche Sicherheit zu schützen. Kriminelle können sich nicht hinter ihren Computerbildschirmen verstecken. Wir arbeiten wachsam mit amerikanischen und internationalen Strafverfolgungspartnern zusammen, um transnationale Cybercrime-Organisationen, wie die Infraud-Organisation, zu identifizieren und zu zerstören.”

AUTOSPLOIT: KEIN WEG ZURÜCK

Das neue Werkzeug AUTOSPLOIT, das sich vor allem an Script Kiddis richten dürfte, ist raus und macht Hacking jetzt noch einfacher. Doch es gibt auch kritische Stimmen. Script Kiddis ist ein eher herabwürdigender Ausdruck, der nicht nur in der Hacker Scene gern für Personen verwendet wird, die sich ohne spezielle Fertigkeiten und Kenntnisse, mit Hilfe von fertig konfigurierten Werkzeugen in andere Systeme hacken.

Für sie dürfte das neue Angebot besonders interessant sein. Aber auch für Profis sind derartige Angebote nicht uninteressant, da solche Fertig-Scripts keiner bestimmten Person zugeordnet werden können. Eigenbau-Codes könnten dagegen aufgrund persönlicher Eigenheiten schnell mit einem bestimmten Hacker in Verbindung gebracht werden, was durch Ermittler oder mittels Ermittlungs-Software geschieht.

Jetzt ist also ein neues und wahrscheinlich recht mächtiges Werkzeug herausgekommen, das es auch eher talentfreien Enthusiasten ermöglicht, größere Schäden anzurichten. Das Werkzeug heißt AUTOSPLOIT und wurde gerade von jemandem herausgegeben, der sich auf Twitter @VectorSEC nennt.

Shodan und Metasploit

Das Werkzeug kombiniert zwei gute alte Bekannte, die schon gebräuchlich sind, um Cyberangriffe zu fahren, oder sich gegen solche besser zu schützen. Das eine ist die Suchmaschine Shodan, welche dazu verwendet werden kann, mit dem Internet verbundene Einheiten mit Schwachstellen zu finden. Das andere ist Metasploit, ein weit verbreitetes Pentesting-Tool. Natürlich könnte Metasploit damit auch dafür genutzt werden, echte Angriffe zu fahren, da die Module des Tools eben auch das enthalten, was gemein hin als Angriffs-Code betrachtet werden kann.

Hege mit vollautomatischer Waffe

AUTOSPLOIT tut nun auch nichts anderes, als die mit dem Internet verbundenen, kranken Einheiten zu finden und mithilfe von Metasploit-Modulen herauszuschießen. Jedoch jetzt beinahe vollautomatisch und nur mit Hilfe weniger Tastenklicks. Das Schwierigste ist vermutlich die Installation des auf Python basierenden Werkzeuges.

Lob und Kritik

Selbst wenn @VectorSEC einiges an Lob bekam, gab es auch kritische Stimmen, die sich besorgt äußerten, da es keinen Nutzen für die Sicherheit gäbe. Im Gegenteil handele es sich eher um eine vollautomatische Angriffswaffe, einige taten AUTOSPLOIT gar mit Malware ab. In Sicherheitskreisen gab man sich im Laufe der letzte Woche noch gelangweilt. Das Werkzeug zeige wenig Neues und man sei schon seit Längerem auf Derartiges vorbereitet. Nun, da das Werkzeug allerdings auf dem Markt sei, gäbe es keinen Weg zurück. AUTOSPLOIT wird dafür sorgen, dass eine größere Anzahl von Personen in der Lage sein wird, bessere Angriffe zu fahren.

Neben der Verwendung von modernen Betriebssystemen empfehle ich Euch, Sicherheits-Updates zu installieren. Einheiten, die nicht mit aktuellem Betriebssystem genutzt werden können, sollten vom Netz genommen werden.

Brothers of Usenet bald wieder online

Brothers of Usenet geht nach einigen Wochen Pause wahrscheinlich schon heute Mittag unter neuer Führung wieder ans Netz. Die alten Betreiber haben ihre Daten an die Nachfolger übergeben, damit diese nicht bei Null anfangen müssen. Erholt sich die Szene? Damit wäre zumindest neben dem Wettbewerber “House of Usenet” das zweite große ehemalige Forum wieder in Betrieb. Alle weiteren sind invite only und somit für neue Nutzer uninteressant.

Seit den Usenet-Busts im November letzten Jahres waren nur noch sehr wenige alte Foren online und wenn, dann kann man dort zumeist nur mit einer gültigen Einladung als neuer User landen. Für B-DeadAngel und seine Mitbetreiber war von Anfang an klar, dass jetzt Schluss ist. Ihr Forum war nie ihr Leben und nun war nach den Durchsuchungen und Beschlagnahmungen auch die Sicherheit ihrer Nutzer bedroht. Bisher ist noch unklar, wie die zuständigen Staatsanwaltschaften mit den bei der Razzia erbeuteten Nutzer-Daten umgehen wollen. Ging es bei der polizeilichen Aktion nur um die Betreiber und deren Helfershelfer? Oder will man auch der zahlende Kundschaft ans Leder?

Nachdem wir Anfang Januar nach einem neuen Betreiber von Brothers of Usenet gesucht haben und sich bei B-DeadAngel etwa 50 Personen mit einem sehr unterschiedlichen Kenntnisstand gemeldet haben, soll es aller Voraussicht nach schon heute Mittag wieder losgehen. Der neue Macher des Forums, B-Devil, hat uns vorab ein Statement geschickt, um sein Baby anzukündigen und die User auf das neue Projekt einzustimmen:

Viele Menschen kommen und gehen, doch Brothers of Usenet bleibt bestehen. Trotz der Höhen und Tiefen, welche wir hatten, waren wir dennoch eine große Familie. Wir geben und nehmen. Die einen mehr, die anderen weniger. Und doch trägt jeder etwas dazu bei. Mit diesen Worten werde ich (B-Devil) das Forum von B-DeadAngel übernehmen. Wir danken B-DeadAngel für seine tolle Arbeit. Aufgrund der Busts in letzter Zeit, will er sich als Administrator zurückziehen und das Usenet hinter sich lassen. Nicht nur ich, sondern die ganze deutsche Usenet-Szene verabschiedet sich nun von ihm und wünscht ihm alles Gute auf seinem Weg.

In den letzten Tagen wurde viel Serverarbeit etc. betrieben, um das Forum wieder aufzubauen. Es war nicht ganz einfach, da nur B-DeadAngel die Backups hatte und es seine Zeit gedauert hat, bis diese hochgeladen waren. Ich durfte mich durch Scripte-Müll kämpfen und die Datenbanken reparieren. Für Euch, für die Community.

Brothers of Usenet erfordert eine größere Infrastruktur, als nur eine 0815-Wordpress-Seite. Vor allem im Punkto Sicherheit und Verfügbarkeit wurde aufgestockt. Wir setzen alles daran, dass sich die jüngsten Geschehnisse nicht wiederholen können.

Viele aus dem alten Team sind gegangen, weil das Risiko für sie zu groß wurde. Einige sind geblieben, aus Treue. Denen bin ich natürlich dankbar, aber ich bin auch denen dankbar, die aus Sicherheitsgründen gehen mussten. Danke für all euren Support und für eure Zeit, die ihr investiert habt.

Ich freue mich auf die Zeit, die Erfahrung und die Herausforderung, die auf mich und auf das (neue) Team zukommt!

Euer B-Devil von Brothers of Usenet.

Dignity: Einladung zum besseren Sein

Liebe Mitmenschen, das Neue Jahr hat bereits die Startblöcke verlassen und die meisten von uns sind wieder im Alltag angekommen. Neue Vorsätze sind gefasst oder längst verworfen, einige befinden sich erneut im alten Trott. Die Mienen der Leute werden wieder ernster.

Erfahrungen machen

Ich möchte die Gelegenheit nutzen, um dich zu neuen Umgangsformen einzuladen. Neue, günstigere Erfahrungen machen? Ja, ich will. Ich will Subjekt werden und selbst gestalten. Ich will den Pfad der anonymen Hasskommentare verlassen und selbst mal versuchen einen Beitrag auf Tarnkappe zu verfassen. Ich will aktiver Gestalter eines neuen Lebensprozesses werden.

Ein Bild von dir selbst

Und dann ist es auch schon so weit. Wow, das ging doch. Und die Kommentare der Leser waren gar nicht so schlecht. Vielleicht traue ich mich wieder, das nächste Mal. So nach und nach nimmst du eine ganz neue Haltung ein. Du wirst ein Stück weit ein anderer oder eine andere. Schon hat deine neue Haltung damit begonnen, dein Verhalten zu bestimmen. Aber was bestimmt deine Haltung? Es ist das Bild von dir selbst. Das Bild von dir, wie du sein willst. Was willst du für einer sein? Weshalb willst du in der Welt sein? Willst du feige und anonym aus einem Hinterhalt feuern oder betrittst du als Gladiator die Arena? Willst du für Google Content produzieren und dich über Almosen freuen oder hast du eine Botschaft?

Das Anliegen

Es wäre interessant, wenn wir uns gegenseitig dabei helfen könnten, zu entdecken, wer oder was wir in der Welt sein wollen. Das ist das Anliegen. Und das wird dann wiederum Teil unserer Identität. Clickbait-Fotze für Google oder aktiver Gestalter einer Welt, die du mit anderen teilst.

Individualität

Individualität ist Teil deiner Persönlichkeitsentwicklung. Du unterscheidest dich von deiner Mutter. Du bist jemand anderes als sie. So geht es los. Das ist Individualität. Manche bleiben auf dieser Entwicklungsstufe hängen. Scriptkiddis, die das Leben noch vor sich haben und sich ausprobieren und Kommentarfeld-Terroristen, die es schon geschafft haben, das Leben zu verscheißen. Ihr alle seid eingeladen, den nächsten Schritt zu gehen. Kommt heraus aus eurer Schmollecke, beendet euer Schattendasein und tretet ins Licht.

Identität

Ok, du bist, wie du bist, weil du in dieser Familie, in jenem Dorf (vielleicht in Sachsen-Anhalt) oder sonstwo in diesem Land und in unserem Kulturkreis groß geworden bist. Das ist ok so. Das ist Identität. Identität ist nichts schlechtes per se. Sie ist größer als Individualität, reicher; sie hat mehr Inhalt. Da passt viel mehr rein.

Selbstbild

Manche Menschen machen dann diese besondere Erfahrung. Sie erfahren, dass es noch ganz andere Menschen gibt, ganz andere Menschen, die in ganz anderen Kulturkreisen groß geworden sind. Und dass diese sind, wie sie sind, weil sie in ganz anderen Orten und Kreisen aufgewachsen sind. Manche stellen dann fest, dass sie sogar die gleichen Dinge teilen. Auch eine Thai z.B. will, dass sie:

– gemocht wird,
– dass sie dazu gehört,
– dass sie wachsen kann und darf…

Wenn man das erkennt, entsteht die vielleicht höchste Form von Selbstbild, das ist die Würde (engl. Dignity). Dann hat man eine Vorstellung von der Würde eines Menschen, unabhängig von der Herkunft, unabhängig von dem, was ein Mensch ist; er hat dann Würde. Und wenn du darüber hinaus selbst deine Würde entdeckst, ganz abseits von Google-Werbe-Blocks oder Flamebaits in den Kommentaren, dann entdeckst du deine eigene Subjekthaftigkeit.

Gleich heute

Und beginne gleich heute, am Tage sieben des neuen Jahres und am ersten Tage deines neuen Lebens als aktiver Gestalter deiner eigenen Welt, die du mit anderen teilst. Und wenn du dich als Objekt behandeln lässt, dann entwürdigst du diese Menschen, die Täter und Angreifer und noch schlimmer, wenn du das tust, ist es gar nicht so schlimm, weil der andere, den du so schlecht behandelst, der muss das nicht annehmen. Wenn edoep sagt: “Blöder Kerl, was schreibt der da nur wieder für einen Unsinn zusammen”, sagst du: “Na, was hat die mir denn schon zu sagen”.

Ganz bei dir selbst

Man kann die Würde eines anderen gar nicht so leicht verletzen, wenn derjenige selbst Würde besitzt. Aber man kann seine eigene Würde dadurch verletzen, das man die Würde anderer ständig verletzt. Das nun wäre die höchste Form von Kohärenz, die man in seinem Leben erreichen könnte, dann würde man sich als jemand empfinden, der dazugehört und der gleichzeitig ganz bei sich ist. Lasst uns das neue Jahr zu einem Jahr der Würde machen, zu einem Jahr des höchsten Seins!

Piraterie und Copyright – ein Kommentar

Piraterie & Copyright …sind eigentlich „ernste“ Angelegenheiten. Immer? Häufig! Manchmal hat die ganze Sache auch lustige Aspekte. Ein großer, bekannter und altehrwürdiger Verlag der Naturwissenschaften-Technik, wovon es mehr als einen gibt, lässt momentan das Netz reinigen Das läuft unter Anti-Pirateriemaßnahmen. Bei diesem Verlag ist eine Firma damit beschäftigt, nennen wir sie mal C&B, das Web zu säubern. Macht viel Arbeit, denn die Piraten sind ganz schön fies!

Beim Putzen, können einem schon mal Fehler unterlaufen. Klar, dafür muss man Verständnis aufbringen. Manchmal bekommt man nicht so alle Nuancen mit – das ist ein schwieriges Geschäft. Ich war auch mal dort tätig. Die Arbeit hat aber auch Ihre „heiteren“ Seiten. Im Transparency Report, den Google dankenswerterweise veröffentlicht, findet man die in den Suchmaschinen abgemeldeten Seiten. Gut. Offenheit ist ja auch wichtig, Transparenz, zu Deutsch „Glasnost“ ist eine gute Sache. Manchmal auch eine sehr amüsante. Der SN-Verlag Hamburg ist da besonders fleißig. Am 21. November wurden ca. 132.000 kritische URLs geputzt, d.h. bei der Suchmaschine von Google entfernt. Nun kann man sich natürlich trefflich streiten, ob das Sinn macht. Klar, das Copyright. Das ist das Recht, auf dem Verlage basieren. Ein Vertreter dieses Verlages sagte mir einmal wörtlich: „It´s our god damn right!“ Wo er Recht hat, hat er Recht, oder?

Und nun die Frage: Mal ein kleiner Screenshot der Seite, wo der illegale Inhalt gefunden wurde. (PS. Die Seite gehört einer bekannten Suchmaschine, dafür lädt sie ziemlich langsam. Ist man von dieser Suchmaschine nicht gewohnt!) P.S.: Die E-Mail ist angeblich vom 01. Januar 2031!

Übrigens, die Suchmaschine betreibt auch einen Quantencomputer. Gerüchten zufolge, soll der zu Störungen des Raum-Zeit Gefüges führen, na ja im Jahr 2031 – ganz korrekt ist das Datum wohl nicht, oder war das schon eine dieser Störungen? Bei 132.000 Links auf eine Abmeldung kann das ja schon mal passieren. Mehr als der Rest aller Abmeldungen zusammen in Summe. Die Tatsache, dass Bücher etc. „kostenlos umverteilt“ werden, ist ja nicht neu. Die Mengen sind etwas „überraschend“. Mehr als der Rest in Summe – das nenne ich mal fleißig. Werden sie etwa nach der Menge der abgemeldeten Links bezahlt – was nicht unüblich wäre. Oder haben die einen ganz fixen Sammelroboter!??

KISSlibrary.com – das LuL 3.0

Ja . Und dann sind da noch andere „Besonderheiten“, die auffällig sind.

Nehmen wir mal jene Seite (offensichtlich illegal, oder nicht offensichtlich rechtswidrig??)) – ein E-Book-Shop aus Minsk. Der wird auf die DMCA-Abmeldungsaufforderungen gegebenenfalls „pfeifen“. Die korrekte russische Antwort wäre (bitte die Damen jetzt mal weghören): „Poshel ty na khui!“ (schlecht übersetzbar, aber halt keine „Literatursprache“) Es geht um https://kisslibrary.com und das sieht ein wenig aus wie LuL 3.0. Legal? Illegal? Scheissegal! Wird jedenfalls abgemeldet, der Link.

Nun, ich vermute mal so, was die Jungs und Mädels mit den DMCA-Abmeldungen machen. Die werden wohl auf dem 0-Device landen, dem Computerklo. Bei den Antipiracy-Firmen werden die aber auf der Rechnung auftauchen? Das nennt man gemeinhin, „aus Scheiße Gold machen“. Gold?? Brillianten. Ja, so manche Piratenjäger haben es echt drauf.

Ein Beispiel? Dann sind da noch abgemeldete Links, die in der Rubrik „nackte Tatsachen“ zu finden sind. (Ich mache mal keinen Screenshot, weil sonst Personen unter 18

DMCA (Copyright) Complaint to Google

SENDER
teamGyday
[Private]
, , , VE
Sent on January 01, 2031

RECIPIENT
Google, Inc. [Sites]
[Private]
Mountain View, CA, 94043, US
Received on January 01, 2031

Jahren diese Seite nicht sehen dürften). Das ist Material, was unter Umständen nicht ganz so im klassischen SN Spektrum liegt – das darf zumindest vermutet werden.

Dann ist da noch die „Oberpiratin“ Alexandra Elbakyan aus M. Die hat die wirklich besten E-Booksammlung der Welt. Wir haben sie mal interviewed – ein nettes Mädchen. Die hat Ihre eigene Meinung zum Thema Piraterie. Wir könnten mit Alexandra mal reden, ob sie gegebenenfalls auch deutsche Belletristik aufnimmt? Hmm… eine gute Idee. Da würde einigen Schmonz-Verlagen doch übel werden, na immerhin gibt es noch gedruckte Bücher. Nur mit den digitalen – das könnte dann schwieriger werden? Aber das ist nur eine Vermutung …

Es ist vielleicht nicht NUR der Preis, der bei Alexandra glatt bei 0 liegt. Sie hat auch mehr davon und DMCA – sie hat da eine sehr bestimmte Meinung zu diesem Thema, will mal sagen – nicht ganz so positiv. Eine Frau führt die ganze Branche vor. Das ist doch mal zum Quieken. Ach ja, der SN Verlag hat sie zum Scientist oft the Year gemacht !

SN? Ich muss ja nicht immer alles verstehen. Aber die Entscheidung von SN ist sachlich korrekt! Geschäftlich? Ich bin mir da nicht ganz so sicher. Die Oberpiratin erhält einen Preis von einem ihrer Opfer. Das nenne ich doch mal nobel. Der andere, der STM Verlag, ihr wisst schon welcher, der ältere von beiden – verklagt sie. Das wiederum verstehe ich. Putin (der böse Boss des Landes wo Alexandra wohnt) ist mittlerweile von westlichen Anwälten etwas genervt – das verstehe ich auch. Er hat seinem Internet-Minister eine Verlautbarung diktiert, die vermutlich vor der Überarbeitung ähnliche Begriffe wie weiter oben (da wo die Damen weghören sollten) enthielt. Wladimir P. schien genervt – etwas. Das ist übrigens genau der Internet-Minister, der noch vor zwei Jahren seine eigene Torrent-Seite betrieben hat. Mittlerweile ist Tornado.ru weg vom Fenster.

Es wird eine interessante Story geben. Wir halten euch auf dem Laufenden! Lustig wird es auf alle Fälle. In der Zwischenzeit LUL’t die Kisslibrary samt ladungsfähiger Adresse + Impressum munter weiter, während die deutschen Täter vom Original in der U-Haft schmoren. Das nette Team (siehe Bild oben) der KISSlibrary wirft sicher jeden Tag aufs Neue weitere DMCA-Mails in Richtung Nirwana. Wetten?

Darknet: Wissenschaftler erstellen Landkarte des globalen Online-Drogenmarktes

In einer Weltkarte des Drogenhandels hat das Wissenschaftler-Team Martin Dittus, Joss Wright und Mark Graham, an der University of Oxford die globale Ausdehnung des Drogenhandels im Darknet erfasst, indem sie versucht haben, die führenden Darknet-Handelsplätze geographisch einzuordnen sowie ihre Inhalte zu kennzeichnen.

Das Darknet mit seinen illegalen Handelsplätzen wird sowohl von Dealern als auch von Kunden wegen seiner Anonymität geschätzt. So soll der Markt nach Angaben von Technology Review bei über Indizien, wie den Standort von Dealern oder potentielle Versandorte, mehr über globale Logistikketten herauszufinden.

aktuell mit 150 Millionen Dollar Umsatz jährlich zwar sein Potential noch nicht voll ausgeschöpft haben, "wenn man bedenkt, dass das globale Drogengeschäft Schätzungen zufolge bei 300 Milliarden Dollar liegt", verzeichnet jedoch ein rasantes Wachstum.

Während die Offline-Wege der Drogen vielfach bekannt sind, gehen sie doch über eine fest etablierte Lieferkette, die die Erzeuger mit den Zwischenhändlern, Dealern und den Kunden verbindet, sind über den Darknet-Vertrieb kaum Einzelheiten bekannt. Die Forscher suchten somit Antworten auf Fragen, wie "Verändern sich dadurch die Handelswege?". Dieses Thema stieß auf großes öffentliches Interesse. Man nimmt an, dass das Darknet künftig eine zunehmend große Rolle im Suchtmarkt spielen wird. Da illegale Märkte sich nur schwer erforschen lassen, liefert die Analyse lediglich eine ungefähre Annäherung an die Realität. Und obwohl die Landschaft der Drogenmarktplätze nach den bekannten Plattform-Razzien durch Ermittler 2017 heute ganz anders aussieht, als zum Start des Forschungsprojekts, gibt die Studie doch einige interessante Aspekte auf die Struktur des Darknet-Drogenhandels.

In einer groß angelegten, empirischen Studie ermittelten die Wissenschaftler die Darknet-Handelsgeographie in vier der damals größten Darknet-Märkte: AlphaBay, HansaMarket, TradeRoute und Valhalla, und verglichen ausgewählte Angebote mit der globalen Route, angefangen bei deren Produktion bis hin zum Konsum. Die 4 Märkte vereinten rund 95 Prozent des gesamten Drogeninventars im Darknet. Das Forscherteam versuchte dabei über Indizien, wie den Standort von Dealern oder potentielle Versandorte, mehr über globale Logistikketten herauszufinden. Die Wissenschaftler setzten dabei einen Webcrawler ein, um sich einen Überblick über die vollständigen Produktpaletten der jeweiligen Märkte verschaffen zu können. So erhielten sie eine Momentaufnahme des Darknet-Marktes vom Sommer 2017. Für eine Einschätzung des Handelsvolumens wurde die Anzahl der Nutzerbewertungen, etwa 1,5 Millionen, untersucht. Da nicht jeder Käufer eine Bewertung hinterlassen hat, ist die reale Zahl eher höher. Aus den Bewertungen konnte zudem auf die ungefähre Ortsangabe jedes Käufers und jedes Verkäufers geschlossen werden. Ergebnisse dieses Verfahrens weisen darauf hin, dass nur fünf Länder für 70 Prozent des Darknet-Drogenhandels verantwortlich wären: Die USA (27 Prozent), Großbritannien (22 Prozent), Deutschland und Australien (jeweils 8 Prozent) und die Niederlande (7 Prozent).

Die sich aus den gewonnenen Daten ergebenden Mustern wurden in einem weiteren Schritt mit dem konventionellen Off-

linegeschäft für Suchtmittel verglichen. Als Vergleichsmaterial dienten Regierungsdaten über den Drogenkonsum in jedem Land. Zudem wurde Material von Ermittlungsbehörden einbezogen, wie Angaben bei Razzien, die Aufschluss zur Herkunft der Rauschmittel lieferten. So verschafften sich die Forscher einen Gesamtüberblick über den geografischen Markt für illegale Drogen. Sie gewannen zugleich Erkenntnisse darüber, wie sich das Darknet in die globale Lieferkette einfügt.

Im Prinzip ermöglichen diese Plattformen den Herstellern, einen direkten Verkauf an die Endverbraucher, indem sie traditionelle Handelsrouten umgehen. Und doch geben die Auswertungen Hinweise darauf, dass viele Angebote aus einer kleinen Anzahl aktiver Konsumländern stammen und nicht aus Ländern, die für die Herstellung von Drogen bekannt sind: “Wir können starke Hinweise darauf präsentieren, dass Cannabis-und Kokain-Händler vor allem in einer kleinen Anzahl von Kundenländern sitzen, statt in den Ländern der Hersteller”, ziehen die Wissenschaftler Bilanz. Dies deutet darauf hin, dass der Darknet-Handel auf der “letzten Meile” stattfindet und möglicherweise alte Handelsrouten intakt bleiben, was Cannabis und Kokain anbetrifft. So übernehmen die Darknet-Marktplätze die Rolle lokaler Händler in einer kleinen Zahl reicher Länder und zeigt auch, dass sich die Darknet-Drogendealer vor allem an Kunden in ihren Heimatländern wenden. Die Handelswege bei Opiaten sind dagegen unklarer. Beschränkt sich der Konsum hauptsächlich auf den Nahen Osten, Russland und Asien, werden sie doch in den genannten “Top 5”-Ländern erworben. Offensichtlich kommt es hier zu anderen Vertriebswegen.

Führungswechsel beim Crime Network

Beim deutschsprachigen Fraud-Forum Crime Network (CNW) gab gestern Abend der Administrator zeroday seinen Rücktritt bekannt. In seinem Abschiedspost gab er anhaltende private Probleme als Begründung an. Der neue Admin sicario soll sich ab heute „konsequent / effizient“ um die Anliegen der Nutzer kümmern. Bei manchen Beobachtern blieben beim sauber aussehenden Abgang des ehemaligen Betreibers dennoch so manche Fragen offen.

Der ehemalige Macher des Fraud-Forums (Online Cybercrime-Marktplatz) Crime Network hat sich gestern um kurz vor 21 Uhr offiziell von seinen Nutzern verabschiedet. Seine letzten

Worte zirkulierten schon etwa 20 Minuten vorher bei gut informierten Kreisen. Seine private Krise habe sich über einen längeren Zeitraum hinweg fortgesetzt, weswegen er sich darum statt um das CNW kümmern müsse, so zeroday. Nach eigenen Angaben soll beim Wechsel alles sauber ablaufen, weil er „Exit-Ripps bis auf’s Tiefste“ verurteilt und hasst. Die Wahl des neuen Betreibers fiel auf sicario, weil er ihn als kompetent und zielstrebig ansieht. Ausstehende Gelder sollen zeitnah ausbezahlt und die Anfragen der User ebenso schnell beantwortet werden, wie er schreibt.

Unser gut informierter Insider stellt zumindest die Aussage infrage, dass zeroday schon seit vielen Jahren unter diesem Namen aktiv ist. „So lange“ sei er unter diesem Namen noch gar nicht dabei. Sein Vorgänger, der sich Mr. White nannte, soll zahlreiche Kunden um ihr Geld gebracht haben, indem er mit samt ihrem Geld ohne jede Ankündigung verschwunden ist. Das also ist genau der Exit-Ripp, den zeroday so sehr verabscheut. Entweder zeroday hat zwischenzeitlich sein Pseudonym geändert oder aber er ist nicht langjährig beim CNW dabei, so unser Informant.

Viele Betreiber haben Angst bekommen…

Unser Insider geht davon aus, dass statt privater Probleme die Angst vor einer möglichen Durchsuchung als Motiv beim Abschied des Admins im Vordergrund stand. Die Angst gehe momentan durch alle Reihen und betreffe viele Personen der unterschiedlichsten Bereiche des Untergrunds. Auch waren im November des Vorjahres viele Beobachter erstaunt über das große Interesse der Polizei an den deutschsprachigen Usenet-Foren, dem Provider SSL-News und deren Betreibern. Bis dahin galt dieser Sektor als zu klein und zu speziell, um das Interesse der Behörden zu wecken. Das Crime Network hingegen ist sehr bekannt, hat sehr viel mehr Besucher pro Tag und wird sicher schon seit längerer Zeit intensiv von den Behörden beobachtet. Von daher erscheint die Angst mehr als berechtigt zu sein.

Rezension von “Darknet: Waffen, Drogen, Whistleblower” Das Darknet wird in den Medien immer wieder in der Luft zerrissen. Angeblich diene es nur dem Verkauf illegaler Drogen und Waffen. Doch was steckt wirklich dahinter? Was erwartet uns dort? Und warum ist dessen Existenz wichtig unabhängig davon, ob man in demokratischen Staaten lebt oder nicht. Der Journalist Stefan Mey hat sich für sein Buch ausführlich bei allen möglichen Stellen erkundigt und versucht so sachlich wie möglich darüber zu berichten.

Der Wahlberliner Stefan Mey ist seit 2010 studierter Publizist und Soziologe. Danach hat er in seiner beruflichen Laufbahn einige Experimente durchgeführt, die ihm wohl nicht ausnahmslos alle gelungen sind. Mey war tätig als „Freelancer auf bescheidenem Niveau“, wie er es bei Xing selbst so schön ausdrückt. Er schrieb und schreibt heute für alle möglichen Print- und Online-Medien. 2004 war er Gründer einer eigenen Jugendzeitschrift namens YOUnique, später schlug er sich als Betreiber eines Liebes- und Lifestyleportals oder eben als freier Journalist für heise online, Golem.de, Le Monde Diplomatique u.v.m. durch. Seine Jugendzeitschrift musste mangels finanzieller Grundlage wieder eingestellt werden. Alternative Medien haben es echt schwer, wie er uns per E-Mail mitteilte. Auch beim 2010 gegründeten Lust- & Liebesportal steht nun ein Schweizer statt Mey im Impressum. Letztes Jahr dürfte der umtriebige Autor aber vor allem mit den Recherchen für sein aktuelles Buch beschäftigt gewesen sein.

Das Thema Darknet ist zwar spannend. Doch über kaum etwas anderes wird bei TV, Print oder Rundfunk so viel Blödsinn verzapft, wie dazu. Wer den Berichterstattungen der letzten Monate / Jahre nicht entkommen ist, muss glauben, im Darknet gehe es ausschließlich um verbotene Dienstleistungen wie der Druck gefälschter Pässe, Ausweise, Führerscheine oder den Verkauf illegaler Drogen und Waffen. Ja, darum geht es auch zum Leidwesen der Betreiber von Tor und den Machern der Verschleierungssoftware I2P, Freenet oder RetroShare. Aber eben bei weitem nicht nur. Zudem werden in den Medien diverse Begriffe schlichtweg falsch benutzt oder sogar verkehrt erläutert. Das Deepweb ist beispielsweise nicht das gleiche wie das Darknet. Und das Internet ist weit mehr als nur das, was man mit dem Browser besuchen kann.

Mey nimmt diese Begrifflichkeiten in den Mund. Aber erst, nachdem er sie nacheinander verständlich erläutert hat. Spannend wird es im Buch “Darknet: Waffen, Drogen, Whistleblower” bei der Finanzierung und den vielen Widersprüchen, die sich hinter dem Tor-Netzwerk verbergen. Manche US-Behörden wie das FBI, die DEA oder das Finanzministerium der Vereinigten Staaten würden nichts lieber tun, als Tor sofort abzuschalten und als nächstes den Bitcoin zu verbieten. Andere US-Behörden haben hingegen den langfristigen Betrieb erst mit ihren umfangreichen Spenden ermöglicht. Größere Geldgeber sind zum Beispiel das US-Außen- und Verteidigungsministerium. Also Stellen, von denen manche sogar für die Aufrechterhaltung der NSA zuständig sind. Widersprüchlicher geht es kaum. Im Gegensatz zur Online-Enzyklopädie Wikipedia oder dem Browserhersteller Mozilla haben es die Macher von Tor trotz ihrer Popularität bis heute nicht geschafft, sich von den Zuwendungen staatlicher Stellen unabhängig zu machen. Von daher können die Macher von Tor die bestehenden Widersprüche so bald nicht auflösen.

> Obskur, illegal, gefährlich – das verbindet man mit Darknet. Doch es gebe auch ein “gutes Darknet”, sagt der Journalist Stefan Mey, der ein Buch darüber geschrieben hat. Etwa beim Drogenhandel: kriminelle Dealer würden beim Onlinehandel umgangen. https://t.co/Vh2hPNL9ZB
>
> — Deutschlandfunk Kultur (@dlfkultur) 6. Januar 2018

Darknet – nur eine Art Amazon für den Untergrund?

Stefan Mey bedauert völlig zurecht, dass man aus dem Darknet so viel mehr hätte machen können. Die größte Anlaufstelle im Tor-Netzwerk ist ausgerechnet die Datenkrake Facebook. Wer sich mit seinem Account anmeldet, ist sowieso nicht mehr anonym. Danach kommen ausschließlich Spiegelseiten großer kommerzieller Anbieter wie die New York Times, Washington Post etc. Also einhundertprozentige Kopien von Webseiten, die in gleicher Form auch über das Clearnet erreichbar sind. Zwar gibt es abseits der illegalen Handelsplätze auch vereinzelte Angebote, die exklusiv im Tor-Netzwerk angeboten werden. Doch das ist im Angebracht der Möglichkeiten, die einem das Dar-

knet bietet, extrem wenig. Letzten Sommer wurde zum Beispiel das deutschsprachige Forum Germanyhusicaysx hochgenommen, was ausschließlich mit dem Tor-Browser erreichbar war. Zu ihrem Pech erlaubten die Foren-Betreiber auch Gespräche über illegale Themen, weswegen das BKA im Juni 2017 wahrscheinlich einschritt und nebst einigen Verhaftungen auch den Server vom Netz zu nehmen. In seinen besten Zeiten erreichte germanyhusicaysx.onion bis zu 20.000 Seitenzugriffe täglich, doch im Vergleich zu den meisten anderen Webseiten oder Foren ist dies lächerlich wenig. Die zahlreichen Nachahmer (diverse URLs wurden in den Kommentaren unter unserem Bericht gepostet) dürften noch weniger Zugriffe generieren. Auch die Kommunikations-Software SecureDrop wird im Buch ausführlich vorgestellt. Viele Verlage haben sich diese oder eine ähnliche Möglichkeit zur Kommunikation mit anonymen Hinweisgebern (Whistleblowern) eingerichtet, doch dafür alleine braucht man kein komplett verschlüsseltes Netzwerk.

Interessant sind auch die Gespräche mit diversen Vertretern der Polizei und Cybercrime Units, die sich mit der Verfolgung von anonymen Straftätern beschäftigen. Sie haben in der Zwischenzeit andere Methoden entwickelt, um Anbieter voneinander zu unterscheiden und mögliche Zusammenhänge zwischen den Verkäufern auszumachen. Sie warten zumeist auf den einen entscheidenden Flüchtigkeitsfehler, den ein Uploader von Kinderpornos oder der Anbieter von Gewehren oder Kokain macht. Doch machen wir uns nichts vor. Wer sich ein wenig umschaut, wird all das auch im Clearnet kaufen können. Die Bewertungssysteme der Händler und E-Commerce-Shop-Systeme sind teilweise sogar die gleichen.

Für das Darknet ist es aber noch nicht zu spät. Weder wurde flächendeckend eine Methode entwickelt, um die Nutzer zu identifizieren und auch werden die Menschenrechtsorganisationen oder andere NGOs abgesehen vom höheren technischen Aufwand nicht davon abgehalten, ihre Aktivitäten auf das Darknet auszuweiten oder sogar das Clearnet aus Sicherheitsgründen komplett zu verlassen. Fest steht: Das Darknet würde das Potenzial besitzen, um das Internet komplett umzukrempeln. Man könnte sich total neu und auch besser aufstellen. Diesmal ganz ohne Überwachung durch IT-Konzerne oder Geheimdienste. Und ohne Angst, die eigene Meinung öffentlich zu äußern. NGOs und Verlage könnten daraus deutlich mehr als ein paar Spiegelseiten machen, wenn man denn bereit wäre, auf die Besucherströme der Suchmaschinen und somit auf Aufmerksamkeit und Erlöse aus Banner-Werbung zu verzichten. Doch wer will das schon? Im Moment zumindest kaum jemand. Und so dümpelt das Darknet trotz einer umfangreichen staatlichen Finanzierung weiter vor sich hin …

Fazit

Doch zurück zum Buch. “Darknet: Waffen, Drogen, Whistleblower” ist ohne Einschränkung empfehlenswert. Wer eine unabhängige Quelle sucht, dessen Autor sich dem Thema sachlich und nüchtern angenähert hat, der ist hier genau richtig. Mey ist kein Informatiker. Wohl aber ein Journalist mit viel technischem Grundverständnis. Und jemand, der die technischen Hintergründe gut verständlich darlegen kann.

IRIDIUM BROWSER

Iridium Browser: die datensparsame Chrome-Alternative

Der Iridium Browser kann ganz genauso wie Chrome benutzt werden. Doch im Gegensatz dazu werden keine Daten an Google übertragen. Außerdem wurden diverse Vorkehrungen zum maximalen Schutz der Privatsphäre aller Nutzer getroffen.

Wer schon länger mit Google Chrome arbeitet und dessen Geschwindigkeit genießt, wird sich beim Iridium-Brows-

er auch direkt zurechtfinden. Das ist kein Zufall, denn dieses Projekt der Stuttgarter Open Source Business Alliance beinhaltet in großen Teilen den Quellcode vom Chromium-Projekt. Doch im Gegensatz zu Chrome „funkt“ dieser Browser keine Informationen an Dritte. Ziel des Projekts war es, einen WebRTC-Browser zu entwickeln, der allen Anwendern gleichzeitig ein Maximum an Sicherheit und Privatsphäre bietet. Das geht schon damit los, dass als voreingestellte Suchmaschine Qwant genutzt wird, statt der Datenkrake Google.

Auch wurden Plugins wie Java, Flash etc. bei der Installation standardmäßig deaktiviert. Alle 3rd party cookies werden per default blockiert. Alle Bestandteile von Chrome, die dazu dienen, Informationen über das Nutzerverhalten zu übertragen, wurden ebenfalls entfernt. Zudem werden unabhängig davon, ob es jetzt etwas bringt oder nicht, “DO-Not-Track” Header an alle besuchte Webseiten gesendet. Außerdem werden nach Verlassen einer Webseite alle Cookies und weitere Daten gelöscht. Da es sich um eine zu 100% kompatible Weiterentwicklung von Chrome handelt, sind alle Erweiterungen aus dem Chrome Web Store nutzbar und funktionieren auch im Zusammenspiel mit dem Iridium Browser.

Der Download des Iridium Browser ist für Windows, Mac OS X und die Linux-Distributionen Debian, Fedora, openSuse, Rhel und Ubuntu verfügbar. Sogar der Quellcode des Browsers ist öffentlich einsehbar. Wer sich für die Details interessiert, bei den Kollegen von Botfrei.de werden alle eingebauten Sicherheitsfeatures im Detail aufgeführt.

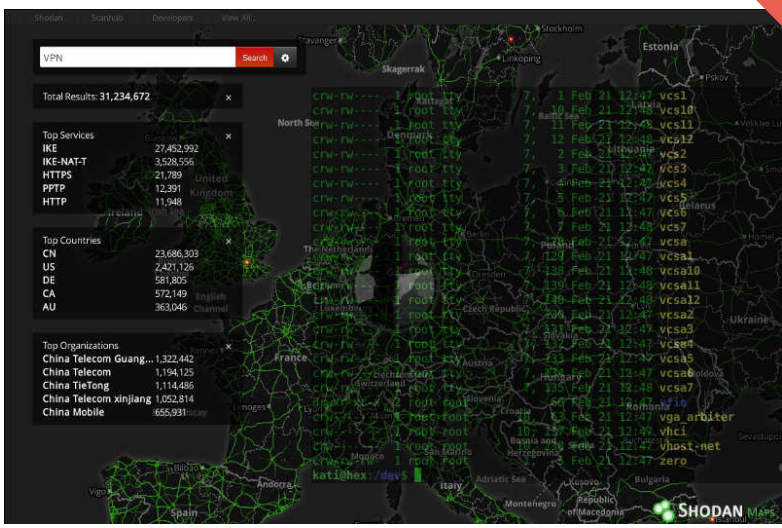
Fazit

Probieren geht in diesem Fall über studieren. Chrome-Anwender müssen sich nicht umstellen. Alle anderen Nutzer werden die hohe Geschwindigkeit schätzen und gar nicht weiter bemerken, was zum Wohl ihrer Privatsphäre so alles unter der Haube geschieht.

Internet-Scanner
Jeder ist betroffen

Wussten Sie, dass Ihr Router, Ihr Smartphone und Ihre anderen Geräte, die über das Internet erreichbar sind, mehrmals am Tag gescannt und somit auf verräterische Zertifikate, Passwörter und Schwachstellen untersucht werden?

Wussten Sie, dass möglicherweise Ihr VPN, Ihr NAS, Ihre



Webcam, Ihr VoIP-Telefon, Ihr Smart-TV, Ihre Heizungsanlage oder Ihre anderen Geräte mit Internet-Anbindung in einer großen Datenbank stehen, auf die jeder Zugriff hat?

Shodan.io

Das Sammeln betrifft nicht nur die kleinen Geräte des Haushalts, sondern ebenso größere Dinge wie Ampeln, Solarkollektoren, Windräder, bis hin zu Trinkwasseranlagen, Stromnetzen und Kernkraftwerken.

Websurfer werden überrascht sein, was man bei shodan.io alles finden kann. Die Betreiber der Internet-Scanner sehen sich als Wohltäter der Menschheit, doch es sind zahlreiche Fälle belegt, in denen sich Kriminelle dort lohnende Ziele, sowie deren technische Details und Passwörter für elektronische Raubzüge besorgt haben.

Den meisten Menschen ist das allerdings völlig egal, da es sich außerhalb ihres Wahrnehmungs- und Erfahrungshorizonts befindet. Das ist wie eine Vorlage für das perfekte Verbrechen, denn die Opfer bemerken es nicht einmal. Aber Dummheit, Faulheit und Unwissenheit werden im Internet gnadenlos bestraft: z.B. durch insecam.org, eine große Sammlung ungesicherter privater Webcams (wir berichteten bereits darüber und fragten bei den Betreibern nach einem Statement).

Heimlich & Co

Dann gibt es noch die weniger auffälligen Datensammler, die aber mit gleicher Hingabe alle weltweit erreichbaren Internetanschlüsse auf verwertbares Material absuchen.

Allen voran die NSA mit ihrem verlängerten Arm shadowserver.org und dem lesenswerten Leistungsspektrum. Deren Spionage-Leitungen lassen sich bis nach Salt Lake City zum Utah Data Center der NSA zurückverfolgen. Das ist der größte Datenspeicher

der Welt, der mittlerweile pro Minute den Inhalt der größten Bibliothek der Welt aufnehmen und verarbeiten kann. Und den Platz braucht es auch für die Milliarden von überwachten Objekten.

Viele Universitäten sind ebenfalls bei den staatlichen Überwachungsprogrammen eingebunden, die mehrmals täglich die Anschlüsse des kompletten Internets abgrasen. Hier eine unvollständige Liste:

☐ Shadowserver NSA scanner: shadowserver.org

☐ Berkeley University research scanning: 169.229.3.91

☐ Cambridge Cybercrime Centre Internet scanner: 128.232.21.75

☐ Michigan University research scanning: 141.212.122.33

☐ Pennsylvania University research scanning: 158.130.6.191

☐ Rapid7 Sonar @ Michigan University: 34.234.1.51

☐ RWTH Aachen University research scanner: 137.226.113.7

Durch deren Schnüffelei kann es sogar zu Problemen in Computern kommen, wie Heise.de berichtet.

Neben den verbündeten Freunden kommen auch die Russen gerne zu Besuch, um fremde Geräte in fernen Ländern kennenzulernen. Doch zahlenmäßig an erster Stelle sind die Internet-Scpanner aus China – wobei man sich wundern muss, wie es die vielen Chinesen durch die Zensur der Großen Firewall nach draußen schaffen, nur um sich hier die Datenleitungen von innen anzusehen.

Solche Dinge erfährt man aber nur, wenn man sich die Mühe macht, Zugriffe auf die heimischen Geräte zu erfassen und auszuwerten. Allerdings ist von solchen Selbstversuchen abzuraten, denn das Speichern und Auswerten der IP-Nummern von virtuellen Einbrechern verstößt sicherlich gegen irgendwelche Datenschutzbestimmungen.

Was man dagegen tun kann

Die Antwort darauf ist einfach und Menschen aus der Zeit vor dem Internet kennen sie vielleicht noch: die Haustür abschließen.

Zunächst sollte man sich einen Überblick verschaffen, welche Türen daheim unverschlossen sind. Hierzu führt man einen Port-Scan mit der eigenen IP durch. Das ist im Prinzip das gleiche Verfahren, was auch die Schnüffler verwenden. So ein Scan-Vorgang geht mit üblichen Netzwerk-Tools wie Nmap, aber auch online beim Heise-Netzwerkcheck. Die gefundenen offen Ports sollten auf den betroffenen Geräten geschlossen werden. Geräte, die nichts im Internet zu suchen haben, wie Drucker, NAS, Online-Festplatten, private Webcams oder Smart-TV, müssen richtig eingestellt werden. Sie sollten nur innerhalb des heimischen LANs erreichbar sein.

Aus dem Internet erreichbare Geräte und Zugänge wie SSH müssen unbedingt sichere Passwörter bekommen. Auf keinen Fall die Voreinstellungen benutzen oder admin, root, geheim, 12345, usw. auswählen! Solche Standard-Phrasen probieren die Scanner zuerst aus. Und die Software muss selbstverständlich auch durch regelmäßige Sicherheitsupdates auf den aktuellen Stand gebracht werden.

Netzwerk-Spanner aussperren

Der schwierigste Schritt ist das Aussperren unerwünschter Besucher. Dazu müssen deren IP-Nummern bekannt sein, was nicht immer ganz einfach zu ermitteln ist. Man kann hierzu einfach alle Zugriffe aufzeichnen und so die ungebetenen Gäste identifizieren. Das dauert etwas, aber führt zum Ziel. Eine kostenlose und vollständige Datenquelle über IP-Bereiche findet man bei MaxMind als Download. Dort sind auch weitere hilfreiche Datenbanken erhältlich.

Die gefundenen IP-Nummern kommen anschließend auf eine Sperrliste, mit deren Hilfe der Computer den Zugriff verweigert. Hier ist als Grundausstattung die Liste unerwünschter IP-Bereiche der oben genannten Scanner:

```
# Shodan.io scanner
66.240.0.0/16
82.221.96.0/19
85.25.0.0/16
93.120.27.0/24
71.6.0.0/16
```

185.163.108.0/23
188.138.0.0/20
198.20.0.0/16
209.126.110.0/23
216.117.0.0/21
Shadowserver scanner
74.82.44.0/22
184.104.0.0/15
216.218.206.0/24
Berkeley University research scanning
169.224.0.0/13
169.232.0.0/14
Cambridge Cybercrime Centre Internet scanner
128.232.0.0/16
Michigan University research scanning
141.212.0.0/15
Pennsylvania University research scanning
158.130.0.0/16
Rapid7 Sonar @ Michigan University
71.6.128.0/19
216.98.128.0/19
RWTH Aachen University research scanning
137.226.0.0/16

Die IP-Bereiche umfassen großzügig den gesamten Subnetz-Block und sind bereits in ein fertiges Tarnkappe-Script eingetragen, das man hier herunterladen kann: block-incoming-ip.sh.gz

Das Script ist mit gzip gepackt und läuft unter Linux. Es wird entpackt, passend umbenannt und ausführbar gemacht. Nach jedem Booten und ebenso bei jeder Änderung der IP-Listen wird es aufgerufen. Es erlaubt alle lokalen Verbindungen im LAN und sperrt unerwünschte IP-Bereiche aus, die sich im Blacklist-Feld befinden.

Die obigen IP-Bereiche sind dort bereits eingetragen. Ebenso die kompletten deutschen Behörden einschließlich Geheimdiensten, sowie deren Untermieter, wie etwa ein Subnetz der CIA, das wohl vom Frankfurter DE-CIX-Knoten über Göttingen in Richtung Harz zu führen scheint. Und in die Gegenrichtung, nach USA / Virginia / Fremont-Langley. Aber das ist eine andere Geschichte.

Wird das Tarnkappe-Script aufgerufen, dann bekommt das Betriebssystems eine Liste an IP-Bereichen mitgeteilt, anhand derer es bereits in der Netzwerkkarte entscheidet, ob eine Verbindung angenommen oder abgewiesen wird. Jeder erstmalige Zugriff einer IP wird geloggt, ebenso jede abgewiesene IP-Nummer. Log-Zeilen mit dem Präfix „IPTables-NewConn:“ sind angenommene Verbindungen, die mit dem Präfix „IPTables-Dropped:“ wurden verweigert. Auch unvollständige Zugriffe (TLS-Handshakes von Zertifikat-Sniffern) werden erfasst. Hingegen sind IPs aus dem Whitelist-Feld immer erlaubt und werden nicht aufgezeichnet.

Ungebetene Besucher können in den Logs unter /var/log/messages, /var/log/syslog o.ä. gefunden werden (der Dateiname ist von der Systemkonfiguration abhängig). Anschließend können die unerwünschten IP-Bereiche über ein Network-Whois identifiziert werden und kommen in die Blacklist. Dann wird das Script erneut aufgerufen. Die gesperrten IPs werden zukünftig abgewiesen. Der Computer reagiert nicht mehr auf Verbindungsversuche und liefert auch keine Fehlermeldung an die Besucher zurück (DROP-Modus).

„Billig-IoT“ und unsichere Hardware, die sich nicht sauber konfigurieren lässt, kann man notfalls per Reverse-Proxy über einen Webserver auf HTTPS und einen höheren Port tunneln und mit einem sicheren Passwort schützen. Auf diese Weise können auch Problemgeräte den Scannern entzogen werden.

„Mannheimer Weg 2.0“: Intelligente Kameras im Einsatz gegen Kriminalität

Das Konzept „Mannheimer Weg 2.0“ ist das Produkt einer Zusammenarbeit zwischen dem Erste Bürgermeister und Sicherheitsdezernent Mannheims, Christian Specht und dem Polizeipräsident Thomas Köber. Ziel des Projektes ist es, dass ein Computerprogramm künftig über 71 Kameras selbstständig Straßenkriminalität erkennen und Polizisten alarmieren soll. Nach langer Planung steht der Start des Pilotprojekts bevor: Mannheim wäre

die erste Kommune Deutschlands mit einem solchen Programm.

So soll erstmalig ein „intelligentes Kamerasystem“ zur Anwendung kommen. Es werden dazu 71 Kameras an 28 Standorten aufgestellt. Die dort aufgefangenen Bilder werden verschlüsselt durch ein Glasfaserkabel zum Lagezentrum der Polizei geschickt. Ein vom Fraunhofer-Institut in Karlsruhe entwickeltes Computerprogramm wertet diese empfangenen Bilder elektronisch mittels Algorithmus aus. Alarm wird ausgelöst in Form einer blinkender Lampe bei untypischen Bewegungsmustern, wie Schlagen, Rennen, Treten, Fallen oder einer plötzlichen Rudelbildung. Dann schaut sich ein Polizist die Szene am Bildschirm an. Auf diese Weise soll ein Computerprogramm in Mannheim für weniger Straßenkriminalität sorgen, denn im Bedarfsfall wird dann eine Streife in gut zwei Minuten vor Ort sein.

Christian Specht ist überzeugt: „Im Zeitalter der Digitalisierung müssen auch Optionen zur Verbesserung der Sicherheit im öffentlichen Raum mitgedacht werden. […] Wir haben die Öffentlichkeit von Anfang an informiert und werden absolut transparent arbeiten.“ Die Aufnahmen würden ohne Ton erfolgen und sollen nach 72 Stunden gelöscht werden. Zudem würden Schilder auf die Überwachung hinweisen und Kriminelle im besten Fall schon präventiv abschrecken. Die veranschlagten Kosten belaufen sich auf 1,1 Millionen Euro. Specht hält das für gut investiertes Geld, denn auch „andere Kommunen schauen mit Spannung auf dieses Pilotprojekt“, meint er. Für Gegner des Systems würde das jedoch nach Überwachungsstaat und „Big Brother“ aussehen, sie befürchten, dass der Staat unbescholtene Bürger bespitzeln und Bewegungsprofile erstellen könnte. Für Specht jedoch steht fest, dass sich nur Kriminelle fürchten müssen: „Es geht um das Erkennen atypischer Bewegungsmuster. Gesichtserkennung oder Tonaufnahmen finden definitiv nicht statt.“

Polizeipräsident Thomas Köber ist ebenso überzeugt von dem Projekt. Bereits von 2001 bis 2007 hatte die Kommune einige Plätze mittels analoger Technik mit Erfolg überwacht. Kober sieht das auch als Grund an, weshalb das Pilotprojekt gerade in Mannheim an nachgewiesenen Kriminalitätsbrennpunkten, wie Paradeplatz, dem Marktplatz, der Breiten Straße und dem Alten Messplatz, startet: „Wir haben Routine und reden nicht wie der Blinde von der Farbe“. Wobei er kritisch anmerkt: „Videoüberwachung ist ein Werkzeug von vielen, die Kamera allein rettet es nicht.“, wobei dem System gerade beigebracht wird, „bei schädlichem Verhalten Alarm zu schlagen. Vieles klingt kompliziert, aber die Message ist eigentlich ganz einfach: Einer schaut hin, und im Bedarfsfall tut der auch was.“ Sein Ziel wäre es zudem, Polizeipräsenz vor Ort zu zeigen: „Ich will die Beamten auf der Straße – nicht vor dem Bildschirm.“

Bei den Mannheimer Grünen stießen bereits die Pläne zum Projekt auf heftige Kritik. Die sicherheitspolitische Sprecherin Nuran Tayanc sagte, mit Investitionen in dieser Höhe könne man viele Polizeibeamte und Sozialarbeiter auf der Straße aktiv werden lassen. Damit würde nachhaltig und langfristig Sicherheit geschaffen. Denn, so Tayanc weiter, der beste Schutz gegen Kriminalität sei Prävention im Sozial- und Bildungsbereich sowie eine gute Integrationsarbeit. Kameras verdrängten die Kriminalität „außer Sichtweite“. Selbst in Städten mit hohem Kameraaufwand habe Terror und Kriminalität stattgefunden, und nicht immer seien dadurch Kriminelle und Terroristen ausfindig gemacht worden, so Tayanc. Es könne auch nicht um Bilder von Kriminellen gehen, es müsse um Prävention, um Verhinderung von Kriminalität gehen.

Jeder ist verdächtig. Überwachung bei Facebook & Co.

Der Verfassungsschutz aus Bremen durchsucht seit einiger Zeit soziale Medien nach auffälligen Meinungen und Aktivitäten. Das erstaunt wohl niemanden, aber immerhin ist es jetzt offiziell, wie Netzpolitik.org berichtet.

Inzwischen wird in Bremen jeder Klick mitgezählt, jedes Wort mitgeschrieben, bewertet, mit den Personendaten von Meldeämtern und Telefonanbietern angereichert und in einer großen Datenbank gesammelt. Wessen Klick-Anzahl und Klick-Häufigkeit über einen bestimmten Wert kommt, gerät automatisch in das Beobachtungsprogramm des Verfassungsschutzes. Danach reicht es schon, wenn man ein paar Mal zu oft auf einen falschen Like-Button drückt, um zu einer Ziel-

person der Behörden zu werden. Sogar die in Texten verwendeten Wörter werden wie Erbsen gezählt, sortiert, analysiert und mit einer Wortliste abgeglichen. Heraus kommen politisch-soziologische Profile von Gesinnungstätern, die den Wünschen einer Gedankenpolizei schon recht nahe kommen.

Damit ist dann auch klar, dass über jeden aktiven Facebook-Nutzer eine Akte geführt wird, in der sich die in Bremen abgeschnorchelten Daten ansammeln. Ohne eine solche umfassende Personen- und Datensammlung sind keine statistischen Aussagen möglich. Und es braucht viele Daten um zuverlässige Aussagen machen zu können. Jede Meinungsäußerung wird gespeichert und bewertet, denn nur eine umfangreiche und langfristige Datensammlung erlaubt es, gültige statistische Aussagen zu machen. Das ist wie beim Würfeln. Ein einziger Wurf sagt nichts über einen Würfel aus, doch nach sehr vielen Würfen kann man einen gezinkten Würfel erkennen. Und solche gezinkten Würfel will der Verfassungsschutz im Internet finden. Also meinungsauffällige Personen, bei denen von Seiten des Staates in der Schlussfolgerung weitere Charaktereigenschaften vermutet werden, in deren zukünftigem Verhalten es möglicherweise zu Konflikten mit dem Staat kommen könnte.

Laut Verfassungsschutz dient die Überwachung dazu, verwertbares Material anzusammeln, um damit Profile zu erstellen und möglicherweise auch juristisch gegen die Personen verwerten zu können. Die Überwachung findet natürlich nicht nur bei Facebook, sondern in allen sozialen Medien statt. Also überall dort, wo im Internet Menschen zusammenkommen und sich austauschen. Dazu zählen genauso die zahllosen Chats und Gruppen bei Telegram, Whatsapp und viele andere Medien mehr.

Interessant wäre zu wissen, nach welchen Standards hier gemessen und bewertet wird, sofern es dazu Standards gibt. Wie lange sind die Speicherzeiten? Werden Fehleinschätzungen erkannt und revidiert? Durchlaufen die Ergebnisse eine Qualitätskontrolle? Hoffentlich. Und so eine Überwachung ist trotz aller Technisierung sehr personalintensiv und teuer. In Bremen kommt inzwischen auf 12 Lehrer ungefähr 1 Verfassungsschutzmitarbeiter. Das ist ein teures Vergnügen für einen verarmten Stadtstaat mit Lehrermangel.

Jeder Einzelne könnte sich vor solcher Überwachung durch Verwendung anonymer Accounts schützen. Theoretisch. Und praktisch nur mit Kenntnis, wie man sich anonym im Internet bewegt. Mehr zu diesem Thema steht im Privacy-Handbuch. Seitenbetreiber könnten die Server des Staates von ihren Webseiten aussperren. Das wäre mal ein interessanter Schritt. Die Server laufen unter der ASN 680 im Netz des DFN.

Ich bin neugierig, wie meine Äußerungen hier bewertet werden…

Edeka-Lieferdienst Bringmeister: Lieferung erfolgt bis in die Wohnung

Der Edeka-Lieferdienst Bringmeister startet in Berlin mit seinem Online-Lieferservice, einer Zustellung der gekauften Waren bis in den heimischen Kühlschrank, ein neues Lieferkonzept. Er arbeitet dabei zusammen mit dem Haushaltsservice Cary von VC/O (Viessmann), der Kunden ein smartes Türschloss vermietet und darüber per Smartphone einem Boten während eines gewünschten Zeitraums Zutritt zur Wohnung gestattet. Kunden können sich so ihren online bestellten Einkauf nach Hause liefern lassen, auch wenn sie selbst nicht da sind. Das Angebot soll pro Monat 9,99 Euro Miete für das Smart-Lock kosten.

Präsentierte noch im Oktober letzten Jahres Amazon in den USA ein neues Projekt, das Smarthome-System namens Key, das dem Paketdienst direkten Zugang in die Wohnung seiner Kunden in den USA ermöglichen soll, haben sich in Deutschland mit dem Edeka-Lieferdienst Bringmeister bereits Nachahmer gefunden. Auch für sie wäre der Weg in die Wohnung ihrer Kunden frei mit Hilfe von elektronisch erstellten Schlüsseln, sogenannten Smart Locks. Um das Angebot zu nutzen, müssen sich Kunden bei Cary registrieren. Für monatlich 9,99 Euro montiert Cary die intelligenten Türschlösser, die über das Smartphone gesteuert werden, und bietet verschiedene Dienstleistungen an. Ein solches Smart Lock kann mit dem alten Schloss verbunden werden.

Der Service, den Edekas Online-Tochter Bringmeister anbietet, beschränkt sich nicht nur auf das Abliefern der Ware, sondern räumt den Einkauf, wenn gewünscht, direkt in den Vorrats- oder Kühlschrank der Kunden. Bestellt wird der Einkauf online bei bringmeister.de. Bringmeister gehört seit Januar 2017 zum Edeka-Verbund. Das Sortiment reicht von Obst und Gemüse, über Fleisch und Käse, bis zu Getränken und Tiefkühlartikeln. Neben dem klassischen Sortiment stünden ebenso 1300 Bio-Produkte verschiedener Marken zur Auswahl. Auch die Rücknahme von Pfand und Getränkekisten wäre über Cary problemlos möglich.

Cary kooperiert u.a. auch mit dem Putzservice-Dienst Bookatiger. Um in die Wohnung zu gelangen, muss der Kurier in der Cary-Zentrale anrufen, die die Wohnungstür ferngesteuert öffnet. So lässt sich kontrollieren, wer wann die Wohnung betritt. Bei Schäden würde der Smart-Lock-Anbieter haften.

Staatstrojaner im Einsatz: BKA hört bei verschlüsselten Smartphone-Messengern mit

Die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) kommt, Berichten von NDR, WDR und Süddeutscher Zeitung zufolge, bereits in laufenden Ermittlungsverfahren zum Einsatz. Demnach überwacht das BKA mit dem neuen Staatstrojaner Mitteilungen per Messenger-Dienste, wie WhatsApp, Telegram oder Signal von verdächtigen Personen .

Gemäß einer im Juni 2017 von der großen Koaliton beschlossenen Gesetzesänderung, dürfen Ermittlungsbehörden bei “schweren Straftaten” die Telekommunikation Verdächtiger überwachen (Paragraf 100a Strafprozessordnung). Allerdings nutzen Dienste, wie WhatsApp, Signal, Telegram und Threema standardmäßig Verschlüsselungen, an denen das BKA bisher gescheitert ist. Um die Verschlüsselung zu umgehen, wird bei der nun eingesetzten Quellen-TKÜ auf dem Handy oder Tablet vom Nutzer unbemerkt ein Programm, der Staatstrojaner, aufs Handy gespielt, das Bildschirmfotos („Screenshots“) von geschriebenen Nachrichten anfertigt und direkt an die Ermittler schickt.

Für die Ermittler ist der aktuelle Einsatz des Staatstrojaners ein Ausweg aus einer Missere, beklagen sie doch schon seit Jahren, dass effektive Überwachung kaum mehr möglich wäre, weil die Verdächtigten zunehmend auf verschlüsselte Dienste ausweichen würden, wie WhatsApp, Telegram und Co. Die Verschlüsselung hat sich als zuverlässig und einbruchssicher erwiesen, lässt aber auch die Ermittler draußen. Das führte dazu, dass laut Angaben der Generalbundesanwaltschaft, nur noch 15 Prozent der überwachten Kommunikation erfasst werden konnte. Auch BKA-Vizepräsident Peter Henzler kritisierte, dass es „zu teils erheblichen Überwachungslücken“ gekommen wäre. Nun setzen also die Beamten ihre Hoffnungen darauf, mittels Quellen-TKÜ an die erforderlichen Daten zu kommen, bevor sie verschlüsselt werden. Bereits aus einem geheimen Bericht des Innenministeriums ging hervor, dass das BKA den Staatstrojaner so schnell wie möglich nutzen wollte.

Sowohl Juristen, als auch Bürgerrechtler und IT-Sicherheitsexperten kritisieren den Einsatz von Staatstrojanern. Sie halten das Gesetz in diesem Umfang für verfassungswidrig. Zudem würden Behörden durch den Einsatz des Staatstrojaners Sicherheitslücken eines Betriebssystems ausnutzen, die der Öffentlichkeit unbekannt sind und die ebenso von Kriminellen zum Ausspionieren von Daten missbraucht werden könnten, denn eine Sicherheitslücke in einem Smartphone betrifft alle Geräte, nicht ausschließlich die krimineller Verdächtiger. IT-Sicherheitsexperten fordern deshalb, entdeckte Lücken zu schließen.

Auf Anfrage wollte das BKA keine Auskünfte über die Häufigkeit der Anwendung des Überwachungsprogramms geben, bestritt jedoch nicht die Existenz des neuen Trojaners.

Pilotprojekt „Schutzranzen“: Sicherheit durch Überwachung

Ein Modellprojekt „Schutzranzen“ ist an zwei Grundschulen in Wolfsburg geplant. Grundschüler sollen mit einem GPS-Tracker ausgestattet werden und an-

hand der Signale sollten Eltern ihre Kinder jederzeit orten können und zudem Autofahrer per Navigations-App gewarnt werden, wenn Kind und Auto sich zu nahe kommen. Das Projekt stößt auf heftige Kritik bei Datenschützern.

Laut Webseite des Schutzranzenherstellers richtet sich das Ziel des Projektes auf die Sicherheit der Grundschüler. So sollen die Schüler für Autofahrer rechtzeitig sichtbar sein, um bereits im Vorfeld Unfälle zu vermeiden. Die Idee zielt darauf ab, dass es ein Peilsender im Schulranzen durch das Senden eines Signals zum einen ermöglicht, dass die Eltern der Kinder mittels App auf ihrem Smartphone stets den Aufenthaltsort ihrer Kinder kennen. Zum anderen sollen aber auch die Autofahrer auf diese Weise informiert werden, wenn sich Kinder in der Nähe befinden, indem sie den Fahrer rechtzeitig vor Gefahrensituationen optisch und/oder akustisch warnt. Zudem will man erreichen, dass Schulkinder mithilfe der App selbstständiger werden, sie sollen auch mal wieder allein zur Schule gehen und nicht mehr auf „Elterntaxis“ angewiesen sein. Die Teilnahme an dem Projekt ist freiwillig. Zu Testzwecken sollen bereits ab Februar in Wolfsburg die Tracker kostenlos an Grundschulkinder verteilt werden.

Am Projekt beteiligt sind neben der Stadt Wolfsburg, dem Hersteller von Schulranzen Scout, der Volkswagen AG, sowie ein Münchener Volvo-Händler, der Sportausrüster Uvex, ein Automobilclub von Deutschland und die Firma Coodriver, die für den Vertrieb zuständig ist.

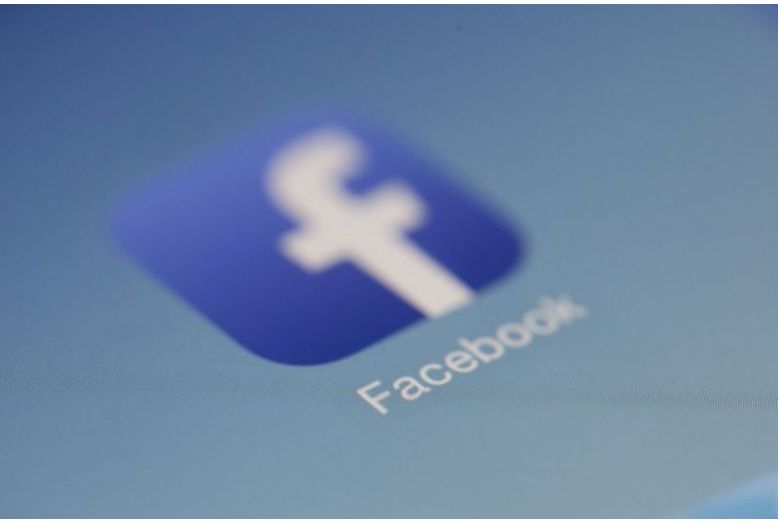
Für Digitalcourage ist digitale Überwachung durch GPS-Tracking nicht der richtige Weg. Zwar wirbt die Website von „Schutzranzen“ damit, dass ohne Zustimmung keine Daten an Dritte weitergegeben werden, dennoch beweisen Analysen von Digitalcourage das Gegenteil: Deren Untersuchungen ergaben, dass die Kinder-App sensible Daten auf US-Amazon-Cloud-Server hochlädt. Die Autofahrer-App würde Facebook kontaktieren. Weitere Daten gehen unter anderem an Server bei 1&1, Microsoft, Google, Akamai & Co. Niemand könne überblicken, wozu diese Daten in der Zukunft verwendet werden, so die Kritik von Digitalcourage in einem Offenen Brief, in dem sie die sofortige Einstellung des Projektes fordern. Allein die Konfiguration des Dienstes wäre „unprofessionell gesichert“, wodurch die aktuellen Aufenthaltsorte der Kinder auch ein leichtes Ziel für Hacker wären. Ferner würde an keiner Stelle darüber aufgeklärt, dass die größten Datensammel-Konzerne der Welt diese Daten bekommen, aber auch die Eltern, Schulen und Lehrer.innen würden nicht umfassend über die Datenweitergabe von „Schutzranzen“ informiert.

Friedemann Ebelt von Digitalcourage beanstandet: „Akute Probleme, wie Gefahren im Straßenverkehr, werden nicht grundsätzlich gelöst, sondern nur ausgenutzt, um Daten zu sammeln, auszuwerten und zu Geld zu machen.“ Zusätzlich sei eines des Hauptrisiken im Straßenverkehr, dass Autofahrer durch Push-up Meldungen abgelenkt seien, so Ebelt weiter. Auch für Kerstin Demuth von Digitalcourage ist es: „schamlos, Grundschulkinder zu überwachen und es als Sicherheitmaßnahme zu verkaufen“.

Die Landesbeauftragte für den Datenschutz in Niedersachsen, Barbara Thiel, teilt in einer Stellungnahme mit: „Durch solche Dienste werden bereits Kinder frühzeitig damit konfrontiert, jederzeit überwacht und getrackt zu werden. Auch Kinder müssen das Recht haben, sich abhängig von ihrem Alter unbeobachtet fortbewegen zu können.“ Thiel stört sich vor allem daran, dass bei einer Nutzung der App die Daten nicht komplett anonym übertragen werden. Die Aussage von Coodriver, dass die Positionsdaten der Kinder nur anonym übermittelt werden, sei zumindest zweifelhaft. Bei Benutzung der App werde auch immer die IP-Adresse übermittelt, weshalb von einer Personenbeziehbarkeit auszugehen sei. Zudem würde die App Funktionen bieten, die nicht ausschließlich der Erhöhung der Verkehrssicherheit dienen. Ihre Aufsichtbehörde werde sich intensiv mit dem Projekt „Schutzranzen“ und den dazugehörigen Systemen auseinandersetzen, kündigte Thiel an.

Auch die Deutsche Kinderhilfe lehnt das Projekt ab: „Nicht alles was geht, ist auch sinnvoll“, sagte der Vorstandsvorsitzende Rainer Becker. „Hinweise des Navis auf ‚Kinder in der Nähe‘ dürften vor allem zu den Stoßzeiten vor größeren Schulen eher zu einer Reizüberflutung der Autofahrer und somit einer Erhöhung des Unfallrisikos führen.“, meint er weiter.

Nach dieser heftigen Kritik der Datenschützer hat die Stadt Wolfsburg empfohlen, das geplante Pilotprojekt „Schutzranzen“ an den zwei Wolfsburger Grundschulen vorerst nicht starten zu lassen. Während die Stadt vor zwei Tagen noch voll hinter dem Projekt stand, ließ sie nun mitteilen, dass es noch „Klärungs- und Kommunikationsbedarf“ gebe. Deshalb sollten alle Beteiligten das Projekt erst mal aussetzen, so ein Sprecher.



Propaganda: Staatsschutz ermittelt wegen Facebook-Post

Ein Cellist der Münchner Philharmoniker hat auf Facebook kommentarlos einen Artikel des öffentlich-rechtlichen Bayerischen Rundfunks auf seiner Facebook-Seite geteilt. Darauf zu sehen war die YPG-Fahne, die in Deutschland verboten ist. Nun ermittelt die Polizei München gegen Johannes König. Laut Bericht vom Bayrischen Rundfunk ist das der erste Fall, bei dem das Posten eines BR-Artikels zu polizeilichen Untersuchungen führt.

Johannes König hatte am 17. August einen Artikel des Bayerischen Rundfunks geteilt, worin berichtet wurde, dass in München 2 Wohnungen wegen eines Verstoßes gegen das Vereinsgesetzes durchsucht worden waren. Die Bewohner dort hatten Fahnen der kurdischen Kampfeinheit YPG im Internet gezeigt. Am Freitag erhielt König Post von der Münchner Polizei. Demnach soll er am 19. März als Beschuldigter bei der Polizei erscheinen. Gegen ihn läuft nun ein Ermittlungsverfahren aus demselben Grund, der zu den Wohnungsdurchsuchungen in München geführt hat: Die öffentliche Darstellung dieser Fahne ist seit einem Schreiben des Bundesinnenministeriums vom März 2017 untersagt: „aber nur insofern, wenn sich ihrer die Arbeiterpartei Kurdistans (PKK) ersatzweise bedient.“ Das geht aus einer Antwort der Bundesregierung auf eine Anfrage der Linken (Seite 11) hervor. Die Symbole stehen auf einer Verbotsliste, die nach dem Vereinsgesetz auf Propaganda für die PKK hinweisen könnte.

Die PKK ist in Deutschland seit 1993 als Terrororganisation verboten. Die Kurden-Miliz YPG ist eng mit der PKK verbunden. Die Türkei betrachtet die kurdischen Volksschutzeinheiten als Ableger der PKK und bekämpft sie deshalb. Der Bayerische Rundfunk berichtete darüber, dass wegen dem Posten solcher Fahnen sogar schon Hausdurchsuchungen durchgeführt werden und zeigte ein Foto mit eben einer solchen verbotener Fahne, hatte jedoch als Berichterstatter auch weitergehende Rechte.

König postete den Artikel, weil er eine kritische Meinung zu dem Verbot von Bundesinnenminister Thomas de Maizière gegen kurdische Symbole hat und wollte mit dem Teilen des Beitrags zudem auf die juristische Verfolgung der kurdischen Symbole aufmerksam machen. Auch gegenüber dem Bayrischen Rundfunk äußerte er sich kritisch: „Dass nun auch das kommentarlose Posten dieses Artikels, der mit der YPG-Fahne bebildert ist, Grund für eine Vorladung zum Staatsschutz sein soll, ist ein neuer irrwitziger Höhepunkt der Repression.“

Die Münchner Polizei verweist auf Anfrage des Bayrischen Rundfunks bezüglich ihres Vorgehens auf die Rechtslage: „Wenn Medien Abbildungen dieser Kennzeichen (zum Beispiel Fahnen) zeigen, dann ist dies nicht strafbar, da nach dem §9/1 S.2 Vereinsgesetz die Verwendung für staatsbürgerliche Aufklärung, zur Abwehr verfassungsfeindlicher Bestrebungen und für ähnliche Zwecke erlaubt ist. Unter ähnliche Zwecke fällt auch die mediale Berichtserstattung. Wenn Mediennutzer dagegen diese oben beschriebenen medialen Abbildungen in sozialen Netzwerken teilen, dann ist dies eine verbotene Verwendung der Kennzeichen und nach §20 Vereinsgesetz eine Straftat.“ Somit sei die Polizei rechtlich verpflichtet, Straftaten zu verfolgen. Demnach haben die Ermittler noch mehr User im Visier, denn der Artikel erhielt bisher insgesamt 1700 Reaktionen und wurde 104 mal getwittert. Ob den Postern das allerdings auch bewusst ist, ist fraglich.

Anklage: Beihilfe zu einer Straftat durch Betreiben eines TOR-Servers

Mit einem interessanten Rechtsfall befasst sich derzeit die Kanzlei Vetter & Mertens. Sie berichten auf ihrem Law-Blog davon. Demnach bekam ein Betreiber eines Torservers, dessen reale IP-Adresse ermittelt werden

konnte, Ärger mit der Staatsanwaltschaft, weil Nutzer den TOR-Service für kriminelle Aktivitäten missbraucht haben.

Bisher konnten solche Fälle problemlos beigelegt werden mangels Tatverdacht und abgesehen von der unvermeidlichen Hausdurchsuchung kam es gewöhnlich zu keinen anderen Repressalien. Nicht aber hier, denn die Staatsanwaltschaft in Nordrhein-Westfalen, klagte den Betreiber des Tor-Servers an.

Die Anklage wird auf die Begründung gestützt, der Torbetreiber hätte sich wegen Beihilfe zur Verbreitung von Kinderpornografie übers Internet strafbar gemacht, immerhin hätte er es ja zugelassen, dass die fraglichen Daten (auch) über seinen Server transportiert wurden. Nun müsse das Gericht über eine Zulassung der Anklage entscheiden.

Als Anwalt appelliert Udo Vetter in Folge, die Eröffnung des Haupverfahrens sei in diesem Fall klar abzulehnen. Er führt als Gründe an, dass das Betreiben eines Tor-Servers in Deutschland legal ist. Dazu trifft den ISP weder eine Haftung für durchgeleitete Daten, noch muss er sein legales Angebot abschalten, falls sich im Nachhinein Ansatzpunkte für vereinzelten Missbrauch zu illegalen Zwecken ergeben. Demnach ist der Beklagte auch nicht dazu verpflichtet zu überprüfen, welche Daten Nutzer des TOR-Dienstes bei ihm durchleiten. Er muss es somit aufgrund klarer, gesetzlicher Vorgaben in Kauf nehmen, dass seine bereitgestellten Dienste auch mitunter für rechtswidrige Handlungen missbraucht werden könnten.

Weder lässt sich folglich ein Beihilfevorsatz aus den gegebenen Fakten ableiten, noch wusste der Beklagte irgendetwas über die begangene Tat, die ihm erst durch die polizeilichen Ermittlungen bekannt geworden ist. Man kann gespannt sein, ob der Fall nun gerichtlich verhandelt wird oder ob sich doch noch eine Einstellung des Verfahrens erreichen lässt. Wie schreibt Udo Vetter indessen so treffend: „Die Hoffnung stirbt ja bekanntlich zuletzt."

Münchner Amoklauf: Sieben Jahre Haft für Waffenhändler

Das Landgericht München I hat Philipp K., den Verkäufer der Tatwaffe, die bei dem Münchner Amoklauf zum Einsatz kam, am Freitag (19.01.2018) zu sieben Jahren Haft verurteilt. Der 18-Jährige Amokläufer David S. erschoss am 22. Juli 2016 am Münchner Olympia-Einkaufszentrum (OEZ) neun Menschen damit und verletzte fünf weitere, ehe er sich selbst tötete.

Waffenhändler Philipp K. hat seine illegalen Waffengeschäfte im Darknet abgewickelt. Dort agierte er unter dem Decknamen „Rico". In Forumsbeiträgen führte Philipp K. aus, wie er Waffen illegal in der Schweiz, Tschechien und der Slowakei erworben habe. Statt Waffen anonym per Post zu verschicken, setzte „Rico" auf persönliche Übergaben, sogenannten „Real Life Treffs". So hatte auch der 18-jährige Schütze David S. die Pistole vom Typ Glock 17 und Hunderte Schuss Munition bei Händler Philipp K. in Marburg (Hessen) abgeholt. Der Waffenhändler war am 16. August 2016 im hessischen Marburg festgenommen worden und sitzt seitdem in Untersuchungshaft. Seine Tat hat er gestanden und sich bei den Angehörigen der Opfer entschuldigt.

Das Gericht sprach nach mehr als 20 Verhandlungstagen den 33-Jährigen Philipp K. wegen fahrlässiger Tötung in neun Fällen, fahrlässiger Körperverletzung in fünf Fällen und Verstößen gegen das Waffengesetz für schuldig. Während die Staatsanwaltschaft sieben Jahre und zwei Monate Haft forderte mit der Begründung, dass erst der Waffendeal die Tat am OEZ ermöglicht hat, plädierte die Verteidigung auf dreieinhalb Jahre Haft wegen Verstößen gegen das Waffengesetz. Sie argumentierte,

eine fahrlässige Tötung, wie von der Staatsanwaltschaft angeklagt, sei nicht gegeben, denn Philipp K. habe nicht absehen können, was mit der Waffe geschehen sollte. Angesichts der langen Untersuchungshaft des im Sommer 2016 festgenommenen K. forderte die Verteidigung außerdem, den Haftbefehl gegen den Angeklagten außer Vollzug zu setzen und ihn freizulassen.

Die Nebenkläger, ca. 25 Angehörige der Opfer sowie deren Anwälte, hatten eine Verurteilung wegen Beihilfe zum Mord gefordert. Die Familien warfen Philipp K. vor, er habe gewusst, was David S. mit der Pistole vorhatte, da beide eine rechtsradikale Gesinnung geteilt hätten. Doch obwohl die Opfer fast alle junge Menschen mit Migrationshintergrund waren, gingen die polizeilichen Ermittler nicht von politischen Motiven aus. Sie nehmen an, dass David S. aus persönlicher Kränkung handelte, denn seine Opfer glichen jenen Altersgenossen von David S., die ihn jahrelang gemobbt hatten. Einige Gutachter kamen jedoch mittlerweile zu der Einschätzung, es habe sich doch um eine rechtsextreme Tat gehandelt. Der Angeklagte Philipp K. betonte im Prozess, er hätte die Waffe nie verkauft, wenn er etwas von den Plänen des Amokläufers geahnt hätte.

Verteidiger David Mühlberger kritisierte in seinem Plädoyer die Nebenklageanwälte scharf, die eine Verurteilung wegen Beihilfe zum Mord verlangt hatten. „Alle Hinterbliebenen haben den Eindruck, er hat die Menschen erschossen“, gibt Mühlberger zu bedenken. Das aber habe David S. getan, der nicht mehr zur Verantwortung gezogen werden könnte. „David S. ist nicht Philipp K. und Philipp K. ist nicht David S.“, sagte Mühlberger. „Und Philipp K. ist auch nicht der Stellvertreter.“ Den Angehörigen sei nicht geholfen, wenn sie den Eindruck bekämen, dass Morde nicht aufgeklärt würden.

Am Montag beklagte eine Mutter, deren Sohn von S. erschossen wurde: Die Angehörigen hätten ein „Recht auf Rechtsprechung, aber kein Anrecht auf Gerechtigkeit“. Der Vater eines anderen Opfers rechnete nach dem Plädoyer der Staatsanwaltschaft bitter vor: „Das sind acht Monate pro Leben.“ Philipp K. sagte in seinem Schlusswort, er wolle den Angehörigen und Hinterbliebenen sein Beileid aussprechen: „Ich habe das nie gewollt. Es tut mir wahnsinnig leid, was passiert ist.“

Mit dem Urteil ging das Gericht mit der Ansicht der Staatsanwaltschaft konform und geht zudem in die Justizgeschichte ein: Erstmals wird damit ein illegaler Waffenhändler mit dem Verkauf einer Schusswaffe für eine Tat verantwortlich gemacht, an der er nicht selbst beteiligt war.

Usenet-Busts: Generalstaatsanwaltschaft Dresden lehnt Verfolgung privater Nutzer ab

Oberstaatsanwalt Wolfgang Klein nahm heute telefonisch Stellung zum Thema User-Verfolgung der Usenet-Busts von Anfang November 2017. Er sieht es nicht als seine Aufgabe an, die Nutzer strafrechtlich zu verfolgen, wie er sagt. Die Generalstaatsanwaltschaft Dresden habe sich bei ihrer Tätigkeit lediglich auf die strafrechtliche Verfolgung der Betreiber konzentriert. Natürlich kann Herr Klein dabei nicht für alle Staatsanwälte sprechen.

OStA Wolfgang Klein fungiert als Pressesprecher der Generalstaatsanwaltschaft Dresden. Die im November des Vorjahres ergriffenen Maßnahmen gegen die Betreiber von Town.ag, Usenetrevolution.info, Usenet-town.com, SSL-News.info & Co. waren ihm ein Begriff.

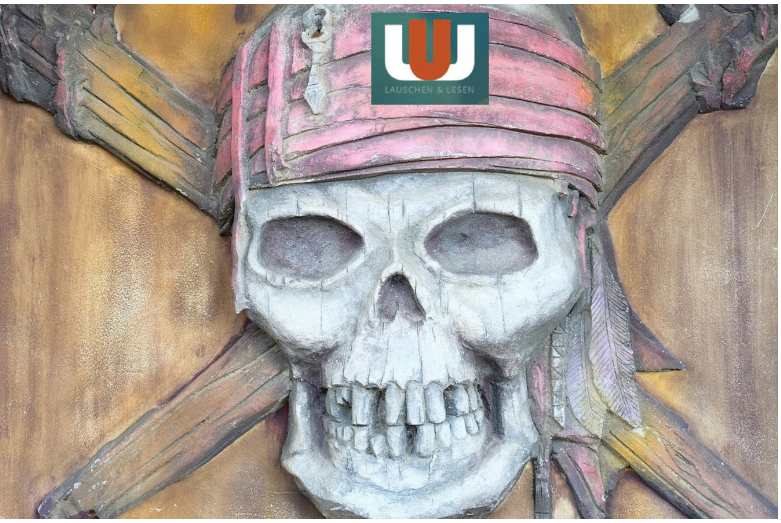
Auf die Frage, ob er bzw. seine Kollegen auch die Nutzer derartiger Foren verfolgen würde, antwortete Herr Klein, dass sich die Behörde bei ihrer Tätigkeit lediglich auf die Betreiber der illegalen Angebote konzentriert. Er sieht es „nicht als seine Aufgabe an“, auch die Foren-Nutzer strafrechtlich zu belangen. Natürlich kann OStA Klein nicht für alle Staatsanwaltschaften der Bundesrepublik Deutschland sprechen.

Vielfach wurde im Internet von Kunden von SSL-News die Sorge geäußert, dass man sie aufgrund ihrer Zahlungen identifizieren könne. SSL-News hat bis zur Razzia als Usenet-Provider Werbung in diversen Usenet-Foren geschaltet und deren Besucher zum Kauf von monatlichen oder längerfristigen Zugängen aufgefordert. Die Foren-Betreiber haben von dieser Werbung profitiert. Der Spur des Geldes zwischen Foren-Betreibern und SSL-News dürften letztlich auch die Ermittler

gefolgt sein, um die Zusammenhänge zwischen den Hintermännern aufzuklären. Die Aussage des Pressesprechers kann man so interpretieren, dass zumindest die Generalstaatsanwaltschaft Dresden nur die Verdächtigen verfolgt, die direkt oder indirekt finanziell von den Urheberrechtsverletzungen profitiert haben. Das ist bei den Nutzern der Foren nicht der Fall.

Usenet-Busts: Deutscher Verdächtiger aus Spanien nach Deutschland überstellt

Ein Verdächtiger der Usenet-Razzia wurde kürzlich von den spanischen Behörden zur Bundesrepublik Deutschland überstellt, damit dieser diese Woche dem Haftrichter in Sachsen vorgestellt werden kann. Es soll sich dabei aber nach Aussage von Wolfgang Klein nicht um den ehemaligen SSL-News-Betreiber Rene T. handeln. Bislang ist uns leider nicht bekannt, um wen es sich dabei handelt.



LuL.to: Ermittlungen zunächst gegen Betreiber

Oberstaatsanwalt Thomas Goger von der Generalstaatsanwaltschaft Bamberg (Zentralstelle Cybercrime Bayern) hat vorhin per E-Mail auf unsere gestrige Presseanfrage reagiert. Nach seiner Auskunft richten sich die Ermittlungen „noch im Schwerpunkt gegen die Betreiber der Seite“ von LuL.to. Zu einer im Raum stehenden Strafbarkeit auch der „Kunden“ könne er zum jetzigen Zeitpunkt deshalb noch keine Angaben machen.

Im Juni 2017 wurde das illegale Download-Portal „Lesen & Lauschen“ (LuL.to) vom Netz genommen. Heute bekamen wir eine Antwort auf unsere Anfrage von Oberstaatsanwalt Thomas Goger von der Generalstaatsanwaltschaft Bamberg, Zentralstelle Cybercrime Bayern. Schon im Oktober des Vorjahres hat der Oberstaatsanwalt die strafrechtliche Verfolgung der zahlenden Kundschaft von LuL.to nicht ausschließen wollen. Daran hat sich bis dato nichts geändert. Auf unsere gestrige Anfrage antwortete er im Originalton:

„Sehr geehrter Herr Sobiraj,

die Ermittlungen richten sich im Moment noch im Schwerpunkt gegen die Betreiber der Seite. Zu einer im Raum stehenden Strafbarkeit auch der „Kunden“ kann ich zum jetzigen Zeitpunkt deshalb noch keine Angaben machen.“

Das passt sehr gut zu den Informationen, die uns von verschiedenen Anwälten zugetragen wurden. Die Ermittlungsbehörden seien mit dem Fall seit Monaten mehr als ausgelastet, das Verfahren zieht sich schon seit längerer Zeit in die Länge. Von daher wird man in Bamberg und anderswo noch mit der Auswertung der beschlagnahmten Asservate beschäftigt sein. Auch habe das Personal zu einem größeren Teil gewechselt, die neuen Mitarbeiter mussten sich in den komplexen Fall natürlich erst einmal einarbeiten, zumal nicht nur LuL.to hochgenommen wurde, sondern auch der Darknet-Marktplatz Hansa Market, die die LuL-Hintermänner vermutlich auch betrieben haben. Das Land Bayern dürfte schon bald aufgrund der beschlagnahmten Wallets von LuL.to und dem Hansa Market zum Bitcoin-Millionär werden.

LuL.to-Nutzer: das ewige Hoffen und Bangen

Schon aufgrund des Personalwechsels dürfte es bis zu einer endgültigen Entscheidung noch etwas dauern. Es wäre auch möglich, dass nur die Personen belangt werden, die ein bestimmtes Download-Kontingent überschritten haben. Wurden also von den Verdächtigen urheberrechtlich geschützte Werke im Wert von mehr als 150 Euro bezogen, um nur mal ein Beispiel zu nennen, dann würde ein Verfahren eingeleitet, ansonsten nicht. Aber auch das wurde noch nicht endgültig entschieden.

Zumindest dürfte es kein großes Problem sein, an die Identität der Kunden zu gelangen. Nachdem beim Bezahl-Portal einige Monate vor dem Bust keine Paysafe Karten mehr eingelöst werden konnten, haben die meisten Nutzer Gutscheine ihrer echten Amazon-Accounts als Zahlungsmittel verwendet. Amazon würde die Identität ihrer Nutzer natürlich auf Anfrage preisgeben, auch wenn das Rechtshilfeersuchen des Amazon-Mutterkonzerns in den USA ein wenig dauert.

Dient deutsches NetzDG nun als Vorbild auf EU-Ebene?

Seit dem 01. Oktober 2017 ist in Deutschland das umstrittene Netzwerkdurchsetzungsgesetz (NetzDG), das Gesetz zum härteren Vorgehen gegen Hass und Hetze im Internet in Kraft getreten. So sind „offensichtlich rechtswidrige Inhalte“, wie wie Volksverhetzung, Bedrohung, Beleidigung oder üble Nachrede nach spätestens 24 Stunden von den Plattformbetreibern von Plattformen mit mehr als zwei Millionen registrierten Nutzern, nach Kenntnisnahme zu löschen. Andernfalls drohen Bußgelder bis zu 50 Millionen Euro. Sieben Tage Zeit bleibt für die Prüfung von weniger eindeutig rechtswidrigen Inhalten. Durch breite, ablehnende Kritik wurde das Gesetz zumindest in Teilen entschärft: auf die ursprünglich geplanten automatischen Inhalte- und Uploadfilter wurde verzichtet. Nun sollen diese jedoch auf EU-Ebene erneut im Rahmen einer Neufassung der EU-Richtlinie zum Urheberrecht forciert werden.

Die Europäischen Kommission fordert aktuell von Internetfirmen eine Entfernung von strafbaren Inhalten in noch größerem Umfang als bisher. Julian King, EU-Sicherheitskommissar, spricht sich für Löschzeiten innerhalb einer Stunde aus und die EU-Kommission kündigt „gesetzgeberische Maßnahmen“ an, die dem deutschen Netzwerkdurchsetzungsgesetz weitgehend entsprechen.

Es stellt sich in dem Zusammenhang die Frage, inwieweit Inhalte im Netz kontrolliert werden sollen und ab welchem Zeitpunkt aus der Kontrolle Zensur wird. Andrej Hunko, europapolitischer Sprecher der Linksfraktion im Bundestag, nimmt zu diesen Problemen in einer Pressemitteilung Stellung. Als Grundlage dazu dienen die Antworten auf eine Kleine Anfrage des Abgeordneten Andrej Hunko u. a. und der Fraktion DIE LINKE: „Drohung der EU-Kommission mit ‚gesetzgeberischen Maßnahmen‘ zur Entfernung von Internetinhalten“.

So meint Hunko, dass der Druck der Europäischen Union zur Entfernung von Internetinhalten aus vielen Gründen heraus problematisch sei. Er führt aus, dass gerade durch die Bearbeitung von Löschanträgen ein „undurchsichtiges Netzwerk von ‚Internetkoordinierungsgruppen‘“ entstehen würde. Dass Europol dabei selbst das Internet absuchen würde, widerspräche den Grundsätzen der Europäischen Union.

Auch würden zu löschende Internetinhalte zunehmend erweitert werden. Waren es zunächst noch terroristische Thematiken, wurde der Umfang bald schon auf Extremismus und Schleuser ausgedehnt und solle alsbald auch noch ‚fremdenfeindliche, rassistische oder Hassreden genauso wie Urheberrechtsverletzungen‘ umfassen. Firmen, wie Facebook, Google, Twitter und Microsoft sollen gemäß EU-Kommission eine Kontrollfunktion erhalten. Zudem ist geplant, dass Internetanbieter vor der EU-Kommission Bericht über Umfang und Tempo der Löschung beanstandeter Inhalte erstatten.

Hunko befürchtet, dass dieser Druck auf die Firmen zum vorauseilenden Löschen führen wird. Er kritisiert insbesondere die Pläne, „wonach der abermalige Upload von Videos und Bildern über einen Filter verhindert werden soll, der auf einem selbstlernenden Algorithmus beruht. Die Forderungen der Kommission sind uferlos, hier steht die Freiheit des Internet auf dem Spiel.“ Solche Filter gleichen alle Inhalte, die hochgeladen werden, mit einer schwarzen Liste ab und löschen Übereinstimmungen sofort.

Denuvo an Naspers-Gruppe verkauft

Die Amsterdamer Verschlüsselungsspezialisten von Irdeto, ein Tochterunternehmen des südafrikanischen Medienkonzerns Naspers, haben zum Jahreswechsel Denuvo übernommen. Der Salzburger Unternehmer Reinhard Blaukovitsch, dem das Unternehmen bisher zum Großteil gehörte, soll auch nach der Übernahme bei Denuvo bleiben. Über den Kaufpreis, den Irdeto für Denuvo bezahlt hat, wurde Stillschweigen vereinbart.

Robert Hernandez, der bis zum Jahreswechsel 30 % besessen hat, war in der Vergangenheit in den USA für den Vertrieb zuständig. Blaukovitsch und Hernandez haben ihr Unternehmen veräußert, um international aktiv werden zu können. Der südafrikanische Medienkonzern Naspers und

dessen niederländische Tochter Irdeto sind global agierende Unternehmen mit Sitz in verschiedenen Kontinenten.

Blaukovitsch soll weiterhin die Unternehmensstrategie von Denuvo steuern, dessen Marke beibehalten werden soll. Auch der Fokus auf Windows-Games soll nicht verändert werden. In den vergangenen Monaten ist das Salzburger Unternehmen immer wieder unter Druck geraten, weil der hauseigene Kopierschutz binnen weniger Tage oder Stunden von verschiedenen Release Groups geknackt werden konnte. Am Wochenende betraf dies auch die aktuelle Version 4.8 von Denuvo, die beim Actionspiel "Sonic Forces" (SEGA) eingesetzt wurde. Blaukovitsch sagte, es gebe keinen Schutz, der ewig hält, weil er unknackbar sei. Niemand könne einen unüberwindbaren Kopierschutz entwickeln. Den Kunden geht es primär um das Release-Fenster von bis zu vier Wochen nach dem Verkaufsstart des Spiels. In diesem Zeitraum werden zwischen 80 bis 90 % des Umsatzes generiert. Der CEO von Irdeto mit Sitz in Amsterdam, Doug Lowther, ergänzte in der eigenen Pressemitteilung:

DENUVO

„The success of any game title is dependent upon the ability of the title to operate as the publisher intended. As a result, protection of both the game itself and the gaming experience for end users is critical."

Denuvo ist nach eigenen Angaben einer der führenden Anbieter zum Thema Gaming-Sicherheit und bietet Kopierschutz für Spiele auf Desktop-PCs, mobilen Geräten, Spielkonsolen und anderer Hardware an. Zudem werden eigene Lösungen zum Schutz von B2B-Software, E-Books und Spielfilmen entwickelt. Kunden sind Verlage, Spielehersteller, Gaming-Plattformen, unabhängige Software-Anbieter und diverse Publisher für verschiedene Bereiche.

Ob der Kauf zu einem Strategiewechsel von Denuvo führen wird, bleibt vorerst abzuwarten. Zumindest habe man jetzt Zugriff auf das Wissen der Ingenieure der gesamten Firmengruppe, darunter sind auch einige Experten für Kryptographie (Verschlüsselungstechnik). Grundsätzlich sei es sehr schwer, geeignetes Personal zu finden. Programmierer, die lediglich eine graphische Benutzeroberfläche erstellen können, könne man nicht gebrauchen, so Blaukovitsch in einer heute veröffentlichten Pressemitteilung. Denuvo brauche Fachkräfte, die einen Assembler beherrschen und die die Maschinensprache verstehen können. Nach der Einstellung neuer Mitarbeiter dauere es stets ungefähr sechs Monate, bis sie ausreichend fortgebildet wurden, um dort aktiv mitarbeiten zu können.

freifunk.

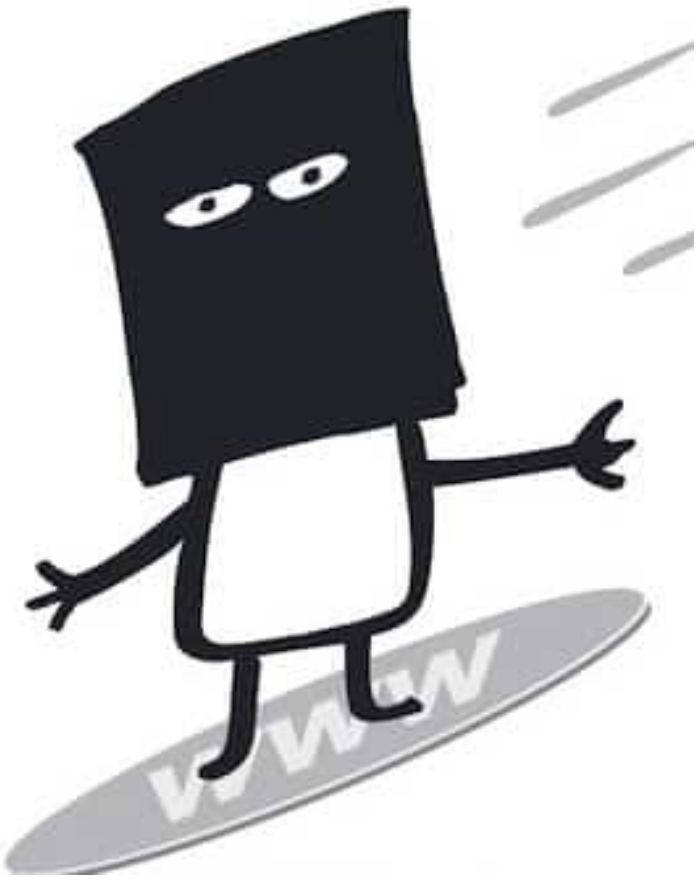
Warum Projekte wie Freifunk nicht funktionieren

Unser Autor Hextor beschreibt in seinem Erlebnisbericht seine ganz persönlichen Eindrücke von einem Freifunkertreffen. Wenn nur Fachidioten aufeinander treffen und diese

nicht offen für fremde Meinungen sind, können neue Gemeinschaften nicht wachsen und gedeihen. Hextor erklärt, warum die Community in seiner Heimatstadt zum Scheitern verurteilt ist.

Nach einiger Zeit wollte ich mal wieder eine Erfahrung mit Euch teilen. Dieser Artikel ist in gewisser Weise als ironisch anzusehen, beruht aber auf Tatsachen.

Eines Abends beim Surfen am Computer, fiel mir ein Artikel im Internet auf, worum es um die altbekannte Thematik „Meshnetzwerke“ ging. Wahrscheinlich handelte es sich um einen Artikel über die neue Firmware-Version der Fritzbox von AVM. Hier sollte es neue Möglichkeiten und Optionen geben, um mehr Mesh-Optionen nutzen zu können. Außerdem las ich davor auch schon einen Artikel über eine neue Katastrophen-App namens „Smarter“, welche Nachrichten ohne das Dasein bzw. Zutun von einem Mobilfunknetzwerk verschicken kann. (Umgesetzt über eine Ad-Hoc Technik, die sich über das W-LAN Netzwerk steuern lässt). Eigentlich ist es doch eine tolle Idee, dezentral Nachrichten zu verschicken! Ich bekam



folglich wieder mehr Lust, mich in das Thema einzulesen und kam natürlich sofort auf die lokale Freifunker Community.

Dies ist eine Community, die über modifizierte Router mit eigener Firmware diverse W-LAN Router miteinander verbinden und so eine Art Meshnetzwerk aufbauen. Kommunikation untereinander mit eigenen Services und die Bereitstellung von Hotspots mit freiem Internetzugang sind die wichtigsten Merkmale dieses Projektes. Um bei dieser guten Idee mitzumachen, suchte ich nach einer lokalen Community mit der ich mich in Verbindung setzen konnte, um eventuell selbst solch einen Router aufstellen zu können, um vielleicht einen weiteren Knoten im Netzwerke anzubieten.

Gesagt, getan. Ich meldete mich über dem E-Mail-Verteiler an und fragte auch gleich nach, ob es lokale Treffen gibt. Zufällig gab es in meiner näheren Umgebung (einer Großstadt) solch ein Treffen. Der Tag kam näher und ich war sehr gespannt, was mich wohl erwarten würde. Das Treffen fand in einem Restaurant statt. Es gab dort anscheinend einen Stammtisch. Ich habe wegen der Größe des Restaurants nicht gleich die richtigen Leute gefunden und fragte deswegen den Kellner. Er wusste sofort Bescheid und zeigte mit dem Finger auf einen Tisch. Ich ging also zu dem besagten Tisch und da ich ein offener Mensch bin, sagte ich: „Hier bin ich. Wer von Euch ist denn Benjamin?“ (Name zum Schutz der Person geändert). Ein Herr sagte: „Ja, hier, setz dich“. Der Tisch war besetzt mit zwei älteren Herren, eines Mannes mittleren Alters und drei recht jungen Herren. Ich setze mich mitten in die Mannschaft und niemand begrüßte mich. Ich versuchte mich mehrfach vorzustellen, weil ich das so gelernt habe. Es erfolgte keine Reaktion von niemanden. Ich war deswegen ein wenig verwirrt. Aber gut, das bist Du ja von Informatikern manchmal gewöhnt, dass sie etwas schüchtern sind. Bevor ich mich vorstellen konnte, war die Bedienung da und fragte, was ich trinken möchte. Ich und die anderen Teilnehmer bestellten unsere Speisen.

Motto des Jahres: #Freifunk first #Bedenken second pic.
twitter.com/6CA0xTOop5
— Freifunk Lëtzebuerg (@FreifunkLux) 11. Februar 2018

Ich musterte für ein paar Sekunden die Leute. Einer war in sein MacBook vertieft und tippte wie wild etwas ein, das ganze Notebook war mit Aufklebern versehen. Der junge Herr neben mir tat das gleiche. Der der mir gegenübersaß sagte kein Wort und starrte nur sein Handy an. Da ich wie gesagt kein Mensch von Vorurteilen bin, legte ich los und sagte so etwas wie „Na gut Jungens, dann erzählt mir doch mal bitte was ihr genau so macht und wie ich mithelfen kann im Freifunk-Netzwerk“. Die Köpfe gingen nach oben. Es fing eine wilde Diskussion rund um die Themen Netzwerk, W-LAN, Richtfunk und andere Gesprächsthemen in diesem Bereich an.

Ich kam leider noch nicht dazu mich vorzustellen und ergriff dann die Gelegenheit, das nun mal anzugehen. Ich stellte mich kurz vor, erwähnte auch meinen Beruf in der Cybersicherheit. Darauf erfolgte schallendes Gelächter von fast allen Teilnehmern. Sie sagten, das sei ja richtiger Unfug, was ich mache. Ich fühlte mich ein wenig auf den Schlips getreten. Aber dachte mir wieder entschuldigend, dass das Informatikstudenten waren, die in ihrer eigenen Welt leben.

Wir diskutierten weiter über Dies und Das. Ich wusste aber immer noch nicht wie die Leute hießen. Von den drei älteren Herren am anderen Tischende kam überhaupt keine Regung. Sie starrten entweder auf ihr Handy oder flüsterten leise aber mit Euphorie über irgendein Netzwerk-Thema. Der Abend wird wohl nicht der Witzigste. Aber nun war ich ja schon mal da und versuchte mich weiter in die Community einzubringen. Als ich ums Eck ging, folgte mir einer der älteren Herren. Ich traf ihn am Waschbecken. Er schaute mich kurz an und guckte dann verschreckt auf den Boden. Er ging dann wortlos zurück zum Stammtisch. Hmm… was das wohl zu bedeuten hatte? War ich vielleicht komisch? Habe ich irgendetwas Falsches gesagt? Gut, ich setzte mich auch wieder an den Stammtisch und unterhielt mich weiter mit dem jüngeren Publikum. Wie sich sich herausstellte, waren tatsächlich zwei von ihnen als Informatikstudenten und einer im Pharma-Sektor tätig. Ist nicht negativ gemeint, aber man sah den Leuten sofort an, was sie studieren. Viel nerdiger gingen die Anziehsachen und Laptops nicht mehr. Es folgten nach jedem Thema immer wieder längere Pausen und jeder vertiefte sich in sein Notebook. Ich hatte keines dabei und musterte weiter das Geschehen.

Freifunk geht in die richtige Richtung! pic.twitter.com/MZirGqoPKv
— Blumi147 (@Blumi147) 11. Februar 2018

Als das Essen kam, fingen alle an zu essen und einer der Jüngeren sagte, warum esst ihr nur Fleisch – das ist alles ungesund. Es folgte eine Diskussion zum Thema veganes Essen. Ich ließ das Thema unkommentiert stehen, obwohl ich dazu eine ganz eigene Meinung habe. Es gibt eine Sorte Mensch mit der diskutiert man besser nicht, da es im heftigen Streit endet. Als die Mahlzeit vorbei war, wollte ich bald gehen, da das Treffen für mich doch sehr ernüchternd war. Auch wurde nicht viel über Meshnetzwerke oder Freifunk gesprochen, was ich mir erhofft hatte.

Verlorene Zeit, dachte ich mir. In dem Moment, als ich gehen wollte, kam einer der Älteren in der Runde und sagte: „Na, dann erzähl mal. Was machst du so und wer bist Du ?“ Ich erzählte also nochmals, dass was ich bereits erwähnt hatte und sagte, dass ich die Idee von Mesh-Netzwerken gut finde und gerne mitmachen würde. In diesem Augenblick dachte ich, dass der Herr neben mir eine Art Schwächeanfall haben musste, da er vom Stuhl halb auf den Boden hängend mit dem Kopf über seinem halb aufgegessenen Schnitzel hing. Ich schaute ratlos die anderen Teilnehmer an. Wie sich herausstellte, machte er in einem vollbesetzten Restaurant ein Nickerchen zwischen Schnitzel und Laptop. Okay, dachte ich mir, das ist ja wohl doch eine etwas andere Welt hier. Dasselbe passierte mit dem Herrn mir gegenüber. Mir war es peinlich. Die anderen Gäste schauten schon herüber und dachten sich bestimmt schon ihren Teil. Meines Wissens ist das kein Benehmen, aber gut – andere Community, andere Sitten. Ich ließ mir nichts anmerken und sprach noch über die Projekte in meiner Stadt.

Es stellte sich heraus, dass die Community nicht wirklich groß war, obwohl die Stadt sehr groß ist. Leider waren auch nur sehr wenige Knotenpunkte miteinander verbunden. Angeblich würde das am Fehlinteresse der Leute liegen und auch am Geld. Richtfunk-Technik sei teuer und deswegen könne man keine größeren Knoten miteinander verbinden. Sie überlegten warum dies so ist und ich schlug vor, diesbezüglich marketingstrategisch vorzugehen, um auch nicht technikaffinen Personen die Vorteile des Freifunks und des dezentralen Gedankens zu erklären. Ich hatte schon ähnliche Kampagnen in anderen Städten beobachtet, jedoch nicht im Detail. Prompt kam der Vorschlag meines Gegenübers doch Router-Workshops anzubieten, wo er erklären würde, wie man Router miteinander verbindet und die Technik erklärt.

Ich erwähnte, dass dies vielleicht etwas zu speziell sei, um den Grundgedanken unter die Leute zu bringen und um neue Freifunker zu werben. Mein Einwand wurde mit teils abstrusen Argumenten totgeschlagen. Anders kann man es leider nicht nennen.

Die Jungs waren hier total auf Technik fixiert, aber mehr leider auch nicht. Es gab für sie anscheinend keine andere Welt als die Technik selbst. Dieser Eindruck wurde die nächsten 30 Minuten weiter verstärkt. Das Thema Marketing und wie man neue Mitglieder werben könnte für den Verein, war wie weggewischt.

Am 06.10.2014 fing hier bei uns alles mit einer Bullet M2 auf dem Dach an und am 08.10.2014 hat sich der Efendi Grill auch #Freifunk in den Laden geholt. Bis heute sind es zwei Jugendräume, ein Friseur und eine Privatperson mehr geworden. pic.twitter.com/PKCxmXbbB8

— Borgifunk (@Borgifunk) 12. Februar 2018

Der Herr neben mir hatte sein Nickerchen abgeschlossen und setze sich ohne einen Ton zu sagen, gleich wieder an sein Notebook, und programmierte wild vor sich hin. Ich habe nicht ganz verstanden was es war. Aber ich glaube, es handelte sich um eine Art TOR zum normal zugänglichen Internet Mapping. Ich weiß noch, dass er etwas davon murmelte, dass er Richtfunk besitze, der so stark sei, dass er „durch Hochhäuser durchlasern könnte. Das ist der geilste Shit ever“. Gut, da hat zumindest jemand Spaß an der Sache, dachte ich mir…

Ich fragte noch einen der älteren Herren, welchen Router ich für den Freifunk Hotspot nehmen könne. Er erklärte mir dies. Es folge eine riesige Diskussion über die richtige Hardware. Ich wollte doch einfach nur wissen, was ich als Anfänger machen kann, um dem Netzwerk etwas beizusteuern. Leider führte dies nicht zum gewünschten Erfolg.

Ich beendete dann irgendwann das Gespräch, zahlte mein Getränk und und sagte, dass ich mich dann nochmals melden würde. Einer der älteren Herren sagte, ich solle doch wieder mal vorbeischauen. Ich ging ohne das es jemanden groß interessiert hätte. Ich glaube, wenn das Restaurant angefangen hätte zu brennen, hätte es auch niemanden interessiert.

Draußen traf ich wieder den gleichen Mann, den ich bereits am Waschbecken getroffen hatte. Er schaute zum Boden, als er mich sah und sagte keinen Ton. Ich ging weiter und dachte mir nur: „Und ihr wundert euch, dass die Community so klein ist und keiner wirklich Lust hat, mehr zum Thema Freifunk zu machen?“

Provisorisch, aber es klappt! @FreifunkDA#freifunk im #Jugendraum#evjlautertalpic.twitter.com/QOuCriAiS0

— Jangeschmiert (@kraulekrankzahn) 6. Februar 2018

Ich glaube, dass viele tolle IT Projekte genau an solch einem Fehlversagen der Community und auch an der Organisation scheitern. Es gibt viele tolle Dinge, die sich über Technik realisieren lassen. Aber wenn „normale“ Menschen auf solch eine Community treffen, sind sie schnell schockiert. Da hat man dann direkt keine Lust mehr, mitzumachen.

Das alles ist wirklich sehr schade, weil ich die Idee hinter dem Thema Freifunk mag. Ich wollte Euch mit diesem Erlebnisbericht einfach einmal zeigen, warum meiner Meinung nach Dinge, wie z.B. Freifunk nicht großflächig funktionieren. Manche Menschen denken leider gerade im Technikbereich einfach zu engstirnig und vergessen komplett das, was um sie herum passiert. Fest steht: So lässt sich eine dezentrale, freie Community, wo jeder mitmachen kann, nicht aufbauen. Für mich war es ein verlorener Abend, für die Umgebung leider eine verlorene wie tolle Idee.

Internet-Drosselung bei Filesharing: US-Provider droht seinen Kunden

Der Internet-Service-Provider Armstrong Zoom droht seinen ca. eine Million Kunden im Nordosten der USA damit, dass die Geschwindigkeit ihres Internetanschlusses bei Urheberrechtsverletzungen, wie Filesharing, reduziert werden kann, berichtet Engadget. Auch IoT-Geräte, wie Thermostate, wären davon betroffen.

In der Regel versenden Copyright-Inhaber Benachrichtigungen an Provider, um Kontoinhaber darauf aufmerksam zu machen, dass jemand ihre Internetverbindung verwendet hat, um urheberrechtlich geschütztes Material herunterzuladen. Internetanbieter sind gesetzlich zwar nicht verpflichtet, die Mitteilungen an ihre Kunden weiterzuleiten, aber viele tun dies dennoch. Wenn man jedoch als Internet Service Provider (ISP) nach dieser Kenntnisnahme die Piraten dennoch an Bord behält, ohne etwas gegen sie zu unternehmen, kann auch der ISP für Urheberrechtsverletzungen haftbar gemacht werden. Es sind bereits Fälle bekannt geworden, in denen Gerichte entsprechend entschieden haben: So hat ein New Yorker Gericht den Versuch des Internet Providers „Windstream“, sich generell von jeglicher Verantwortung für Urheberrechtsverletzungen seiner Kunden loszusagen, abgewiesen. Zudem hat die Musikindustrie den ISP „Grande Communications” verklagt, weil das Unternehmen nichts gegen gewohnheitsmäßige Piraten unter seinen Kunden unternimmt. Auch in einem Verfahren von BMG gegen den Internetprovider Cox Communications hat das Gericht von Virgina, Cox Communications für schuldig befunden, Schadenersatz und die Rechtskosten zu zahlen, denn Cox hatte trotz wiederholter Meldung von Kunden, die BMG-Produkte über den Internetzugang von Cox im Netz verbreitet hatten, diese nicht von weiteren Urheberrechtsverletzungen abgehalten.

Nun zieht der Internet-Service-Provider Armstrong Zoom daraus wohl die Konsequenzen. In einem Warnbrief teilt er seinen Kunden mit, die Verbindung im Falle einer Urheberrechtsverletzung so weit runterzufahren, dass weder die Fernsteuerung eines Thermostats, noch die Funktion von Überwachungskameras mehr funktionieren. Lediglich das „Abrufen von E-Mails“ wäre weiterhin möglich. Kunden, die ihren kompletten Service wiederhergestellt haben wollen, um u.a. die Kontrolle über ihre Thermostate wiederzuerlangen, müssen einen Artikel über Urheberrechtsverletzungen lesen, Fragen dazu beantworten und dann eine Vereinbarung unterschreiben, dass sie informiert wurden. Wenn jedoch zu einem späteren Zeitpunkt weitere Beschwerden eintreffen, würde noch härter durchgegriffen: „… Wenn Armstrong nach dem Unterzeichnen der Bestätigung zusätzliche Benachrichtigungen erhalten hat, wird Ihr Zoom-Internetdienst beendet“, schreibt der Anbieter. Danach könne man erst nach Unterzeichnung einer eidesstattlichen Unterlassungserklärung und gegen eine Gebühr erneut in einen Vertrag einsteigen.

Der beunruhigende Aspekt daran ist, dass bei besonders kalten Wintern, wie sie in der Region üblich sind, ein Ausfall des Thermostats lebensbedrohliche Folgen für die betroffenen Menschen hätte. Es kann zu gefrorenen Rohren, Überschwemmungen, zum Tod von Haustieren und sogar Menschen führen. Engadget schreibt: „Bandbreitenbeschränkung für Kunden in den Bereichen, die Thermostate angeschlossen haben, könnte den Unterschied zwischen Krankheit und Gesundheit oder sogar Leben und Tod bedeuten.“ Das scheint eine extreme Strafe für jene zu sein, die nur mal schnell „Game of Thrones“ unautorisiert runtergeladen haben.

Die Folgen der Aufhebung der Netzneutralität in den USA werden somit nicht nur eine langsame Netflix-Verbindung sein, die das Online-Leben stören könnte. Die tatsächlichen Konsequenzen sind, wie man an diesem Beispiel sieht, viel weitreichender. Wenn, laut den neuen Regeln der Federal Communications Commission (FCC), Provider auch ohne Angabe von Gründen die Internet-Verbindung von Kunden gedrosselt werden darf, bedeutet das für alle vernetzten Geräte im Haushalt, wie Alarmanlagen, smarte Lautsprecher, Lichtsteuerung, Videoüberwachungskameras, Kühlschränke und alles, was eine Internet-Verbindung benötigt, dass keines davon mehr funktionieren würde. Engadget stellt in Frage, ob es einem Provider wirklich zustehen sollte, über solche weitreichenden Dinge zu entscheiden und daran zeigt sich erst die große Bedeutung der Netzneutralität.

Passwortdiebstahl: Neuer Kopierschutz aktiviert Trojaner bei illegaler Nutzung

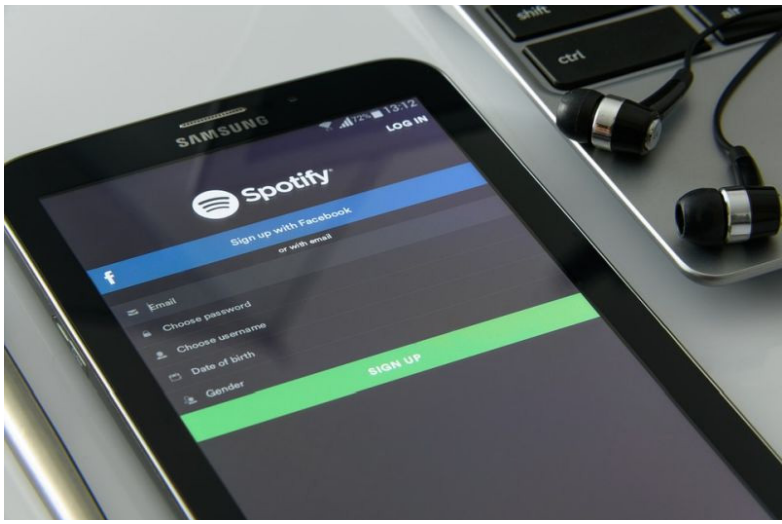
Viele virtuelle Piloten waren sicher begeistert, als das neueste Microsoft-Flugsimulator Add-On, das Erweiterungspaket für Zusatzflugzeuge, des kommerziellen Anbieters Flight Sim Labs Ltd. (FSLabs) erschien. Jedoch war

für die meisten die Freude von nicht langer Dauer. Am Sonntag (18. 02.2018) wurde ein Reddit-Post bekannt, in dem behauptet wurde, dass das FSLabs A320-Installationsprogramm ein Tool zum Extrahieren von Google Chrome-Passwörtern, also einen Trojaner, enthielt, berichtet theregister.

Der User ‚crankyrecursion' stellte fest, dass eine Datei namens ‚test.exe' auf dem Computer des Nutzers extrahiert wurde, als die Installationsdatei von FSLabs „FSLabs_A320X_P3D_v2.0.1.231.exe" ausgeführt wurde. Weitere Untersuchungen ergaben, dass es sich hierbei um den Code eines von SecurityXploded.com stammenden Tools handelt, mit dem sich gespeicherte Passwörter aus Googles Chrome-Browser auslesen lassen. Dieses kann über weitreichende Rechte verfügen, da der Installer der Flugsimulator-Software nach Admin-Rechten verlangt und diese auch an Programmkomponenten vererben kann.

Wie sich dann herausstellte, geht Flight Sim Labs Ltd. völlig neue Wege im Kampf gegen Piraterie, indem sie wenig verhältnismäßige Mittel gegen Nutzer einzusetzen bereit sind. Sie veranlassten, dass bei Usern, die das Produkt ohne ordentlich gekaufte Lizenz verwenden, auf deren Rechnern Malware aktiviert wird, die dann, einmal aktiviert, verschiedene Informationen von dem System ausspionieren soll. Einmal dort eingenistet, sammelt sie alle Benutzernamen und Kennwörter in Google Chrome und sendet diese an den Hersteller. Die Malware wird ohne Zustimmung des Nutzers und ohne dessen Wissen auf sein Benutzersystem übertragen. Fraglich ist, ob das Vorgehen überhaupt legal ist. Das beanstandet u.a. auch Luke Gorman, Softwareentwickler, bei Medium.

Firmenchef von Flight Sim Labs Ltd., Lefteris Kalamaras, versuchte diese Maßnahme als Verteidigungsmaßnahme gegen Piraterie zu rechtfertigen. Die Informationen könnten dann verwendet werden, um Zugang zu illegalen Websites zu erhalten, die von der Crack-Community des Spiels verwendet werden, um sie dann an die Behörden weiterzugeben, meinte er. Aufgrund der allgemeinen Empörung wurde jedoch das umstrittene Installationsprogramm seitdem entfernt. Zudem hat sich Flight Sim Labs bei seinen Usern dafür entschuldigt, dass sie einen solch „übertriebenen Ansatz für unseren DRM-Installer" zum Einsatz brachten.



Genial legal: Betrüger ergaunert Millionen bei Spotify

Ohne sich dabei strafbar zu machen, tickst ein Betrüger das Bezahlsystem von Spotify aus und verdient so ein Vermögen, berichtet Music Business Worldwide, die ihre Informationen von Vertretern der Musikindustrie bezogen haben. Über einen Zeitraum von vier Monaten konnte ein Übeltäter Spotify Tantiemen für mindestens zwei Playlists abluchsen, bevor die Täuschung aufflog. Die Identität des Schwindlers ist bislang unbekannt, er soll sich jedoch in Bulgarien aufhalten.

Mit einer relativ einfachen, ausgeklügelten Idee hat offenbar ein Bulgare Spotifys Auszahlungsmethode so unterwandert, dass er daran Millionen verdient hat. So lud er im Mai 2017 eine große Anzahl von Liedern auf Spotify hoch – als Rechteinhaber aller Stücke – und somit völlig legal. Spotify zahlt an jeden Rechteinhaber, sobald sein Lied mindestens 30 Sekunden gespielt wird, zwischen 0,006 und 0,0084 Dollar aus, wobei die Rechte meist beim Plattenlabel liegen und nicht beim Künstler selbst. Bei einem globalen Hit-Album können laut Angaben von Spotify Tantiemen von ca. 425.000 Dollar im Monat verdient werden.

Das Erfolgsrezept des Betrügers:

Man nehme viele kurze Einzelmusikstücke (die Lieder spielten im Schnitt ca. 43 Sekunden pro Titel, sie lagen somit knapp über den geforderten 30 Sec., für die gezahlt wird), fasse sie zu den beiden Playlists „Soulful Music" und „Music from the heart" (enthielt ca. 467 Tracks) zusammen, generiere 1200 Spotify-Premium-Accounts pro Playlist, programmiere einen Bot, um die eigenen Playlists immerwährend abzuspielen – und schon kann`s losgehen mit dem Geld verdienen.

Der geschätzte Reingewinn: ca. 300.000 Dollar Tantiemen – pro Monat & pro Playlist

Laut geschätzter Hochrechnung von Music Business Worldwide haben die Betrüger auf diese Weise monatlich ca. 300.000 Dollar an Tantiemen pro Playlist von Spotify ausgezahlt bekommen. Sie schreiben, dass monatlich jeder Fake-Account mit Hilfe von Bots 60.000 Tracks mit 43 Sekunden Länge spielen könne, das entspräche bei 1200 Fake-Accounts einer Anzahl von 72 Millionen wiedergegebener Tracks.

Bei Auszahlung von 0,004 Dollar für jede Wiedergabe wären das 288.000 Dollar pro Monat. Da die Playlist mindestens vier Monate online war, könnte sich theoretisch ein Gewinn von 1,152 Millionen Dollar ergeben. An Ausgaben investierten die Betrüger lediglich in die Kosten für die Premium-Abos in Höhe von 12.000 US-Dollar. Alle genannten Angaben beziehen sich nur auf eine einzelne Playlist, wobei zwei Playlists von dem Betrüger bekannt sind, er könnte zudem jedoch noch über weitere, unbekannte verfügen.

Der Erfolg wurde schließlich zum Verhängnis:

Bereits im September 2017 stürmten die durch Bots gehypten Playlists die Top 100 der globalen Spotify-Playlists, in den USA sogar bis Platz 11. So kam es auch, dass ein großes Label das Problem an Spotify meldete und der Streaming-Dienst auf sie aufmerksam wurde. Sie nahmen die Playlists genauer unter die Lupe und stellten fest, dass z.B. „Soulful Music“ zu dieser Zeit weniger als 1.800 Follower hatte und jede der 467 enthaltenen Titel lockte jeden Monat nur rund 1.200 Zuhörer an. Die Frage, die sich dann stellte war, wie konnte man sich daraus abgeleitet den großen Erfolg erklären? Entweder spielten 1.800 Leute einfach immer wieder die Titel, was ziemlich unwahrscheinlich wäre oder aber es handelt sich um den beschriebenen Betrugsversuch. Damit flog der Schwindel auf, die Playlists wurden gesperrt – sie waren zu populär geworden.

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

Ist der Beginn eines neuen Jahres auch sonst ein Zeitpunkt des Neuanfangs? Wir hatten es gehofft – nur um, wie so oft, bitterlich enttäuscht zu werden. Statt schöner neuer Welt gab es wieder einmal viel, womöglich zu viel vom Altbekannten. Überzeugt euch selbst in unserem Monatsrückblick. Subversives von der Fiffi-Front

Zu denjenigen, die sich vermutlich so schnell nicht ändern werden, gehört US-Präsident Donald Trump. Auch im Jahr 2018 ist er weiterhin sein übliches charmantes, eloquentes, weltoffenes Selbst. Das führt natürlich dazu, dass auch Trumps Gegner weiterhin ihrer Agitation gegen den Großmeister des Toupets treu blieben. So veröffentlichte Michael Wolff ein viel beachtetes Trump-Enthüllungsbuch namens „Fire and Fury“. Das allerdings wurde nicht nur in Buchhandlungen in aller Welt verkauft – sondern auch ganz subversiv auf den Enthüllungsplattformen WikiLeaks und Cryptomeveröffentlicht. Warum, weiß keiner so genau, denn eigentlich sind diese Plattformen ja eher für Geheimpapiere zuständig. Ein Buch, dass sich mit zwei Klicks beim Online-Buchhändler der Wahl bestellen lässt, ist ja dann eher… nicht so geheim. Womöglich war die „gefühlte Subversivität“ des Machwerks allein durch die Tatsache, dass es gegen Trump ging, hoch genug…

Dass die Plattformen unbekanntes Terrain betraten, zeigte sich allerdings an ihren Schwierigkeiten, den schwer gefährlichen geheimen Leak auch verfügbar zu halten. Während Cryptome dabei durchaus Erfolg hatte, war der WikiLeaks-Download schon nach kurzer Zeit wegen Problemen mit dem Webspace wieder offline. Wahrscheinlich waren geheime US-Behörden schuld, die auf diese Weise die Verbreitung des geheimen… ähm, whatever. Nach den Details müsst ihr vermutlich Julian Assange persönlich fragen. Der weiß zum Thema „das ist keine Inkompetenz, sondern eine Verschwörung“ eigentlich immer etwas zu sagen.

Apropos Julian Assange: dessen Rolle in dieser Geschichte ist der einzige wirklich überraschende und mysteriöse Teil. Jahrelang sah es immerhin so aus, als sei der Australier getreu

dem Motto „der Feind meines Feindes ist zumindest keinen Leak wert“ durchaus bereit, sich mit Trump gegen die beiden zutiefst verhasste Hillary Clinton zu verbünden. Nun allerdings wirkt es so, als sei er bereit, zumindest pro forma gegen den New Yorker Haarteilhalter vorzugehen. Wir dürfen gespannt sein, wie es weiter geht. Trump seinerseits war ja Assange von Anfang an nicht allzu zugetan, war er doch auf dem Standpunkt, dass WikiLeaks eine Horde von Verrätern sei. In Trumps Weltbild sind eigentlich alle Verräter außer Mutti (oder Leuten, die ihren Wahlkampf von den Russen unterstützen lassen), aber dennoch dürften die Damen und Herren der Enthüllungsplattform das nicht allzu gerne gehört haben. Womöglich zeichnet sich hier ein interessanter neuer Konflikt ab.

Out of London?

Auch in anderer Hinsicht sorgte Julian Assange im vergangenen Monat für Schlagzeilen. Der seit Jahren in der Botschaft Ecuadors in London ausharrende Aktivist schaffte es, sich einen ecuadorianischen Pass zu besorgen. Das heizte wieder einmal Spekulationen darüber an, ob er bald schaffen könnte, sein Exil zu verlassen. Noch sitzt er allerdings dort

fest, spielt mit seiner Katze und twittert. Gelegentlich twittert auch die Katze. Wir dürfen gespannt sein, wie es weiter geht.

Skype: Auf zu neuen alten Ufern

Ein weiteres alt bekanntes Phänomen: wenn es um Features, die jeder haben will, oder um Sicherheit geht, kommt Microsoft grundsätzlich zu spät zur Party. Auch dieser alt bekannten Tatsache blieben wir im Januar treu. Nur zwei Jahre nach einem Großteil der Konkurrenz erhielt nun auch Microsofts Kommunikations-Tool Skype eine Ende-zu-Ende-Verschlüsselung. Damit allerdings verlor Skype sein wichtigstes Alleinstellungsmerkmal. Bisher war Hangouts „das für Google-Angestellte und Ingress-Spieler“, WhatsApp „das für alle einschließlich Oma“, Signal „das für Aktivisten und Paranoide“ und Skype „das für diejenigen, denen der Gedanke gefällt, dass immer die Regierung zuhört“. Wir dürfen gespannt sein, ob sich nun eine neue Nische findet oder Skype den Weg alles Irdischen, konkreter von Windows Phone geht.

Das Pferd auf meinem Smartphone

Wer jetzt allerdings glaubt, bei einem der Skype-Konkurrenten unbedingt besser aufgehoben zu sein, wird ebenfalls enttäuscht. Dank Staatstrojaner können auch verschlüsselte Chats direkt auf dem Gerät des Verdächtigen abgehört werden. Medienberichten zufolge wird das auch schon fleißig praktiziert. Gute Nachrichten für Exhibitionisten, CDU-Politiker und die Anbieter von berittenen Botendiensten. Bei allen anderen dürfte sich die Begeisterung eher in Grenzen halten.

Was man sich allerdings unweigerlich fragt: Wo nehmen die Behörden einen funktionsfähigen Trojaner her? Nach wie vor sind ihnen die nötigen Kenntnisse zum Selbst-Programmieren kaum zuzutrauen. Sie werden doch nicht schon

wieder verbotenerweise extern eingekauft haben…?

Wenig Neues

Traditionalisten können ganz beruhigt sein: auch 2018 scheint alles beim Alten zu bleiben. Kuschelt euch getröstet in die Decke des Vertrauten und genießt das Schauspiel von Donald Trump, Julian Assange und allen Anderen, die uns so tapfer mit ihren aberwitzigen Eskapaden unterhalten. Wir werden ebenfalls für euch dranbleiben und lesen uns im Februar wieder. Bis dahin bleibt gesund und skyped nicht zu viel!

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

Der Februar, das weiß jedes Kind, hat im Gegensatz zu anderen Monaten nur 28 Tage. Das gab den Ton an für die Geschehnisse dieses Monats, denn auch neben dem bedauernswerten Februar selbst gab es in den letzten vier Wochen so einiges, das hinter den Erwartungen zurück blieb. Doch lest selbst im satirischen Monatsrückblick.

Lücken in Trojas Mauern

Nehmen wir zum Beispiel die Sicherheitspolitik der Bundesregierung. Diese hat zwar kürzlich einen Staatstrojaner namens „FinSpy“ für den Einsatz auf den Geräten Verdächtiger freigegeben. Berichte, denen zufolge das Pferdchen schon auf Mobiltelefonen zum Einsatz gekommen ist, erwiesen sich aber als arg übertrieben.

Wo, liebe Leserinnen und Leser, soll das hinführen? Da entstehen doch eklatante Schutzlücken. Die Nutzung moderner Technologie ohne Bundestrojaner sorgt dafür, dass Polizeiarbeit nicht mehr wie gewohnt durchgeführt werden kann. Stellt euch mal vor, ihr könntet eure Briefe einfach in Umschlägen verschicken und niemand würde sie lesen. Oder ihr geht mit dem oder der Liebsten spazieren und niemand hört euren Gesprächen zu. Oder ihr singt gar unter der Dusche, ohne dass jemand GEMA-Gebühr dafür verlangt. Wir hätten in kürzester Zeit Chaos und Anarchie und mindestens einen Terroranschlag pro Stunde.

Aber in der digitalen Welt müssen wir dergleichen anscheinend dulden, nur aufgrund der Inkompetenz unserer Behörden. Schlimme Zeiten…

Brüder und Schwestern im Geiste

Die Bundesregierung, so wurde im Februar ebenfalls bekannt, kann sich aber mit ihrer Abscheu gegen Verschlüsselung in guter Gesellschaft fühlen. Während hierzulande mit wechselndem Erfolg am Staatstrojaner gebastelt wird, ist man in China schon einen Schritt weiter. Auf der Plattform „Sina Weibo“ wurde kurzerhand sämtliche Werbung für Krypto-Themen untersagt.

Da können sich unsere Politikerinnen und Politiker doch richtig gut fühlen. Nichts erweckt so viel Vertrauen in das eigene demokratische Bewusstsein wie Zustimmung aus der Volksre-

publik. Womöglich sollte die Regierung endlich Nägel mit Köpfen machen und eine eigene große Firewall in Erwägung ziehen. „Berliner Mauer“ klingt doch irgendwie geschichtsträchtig…

Der Narr oder der Narr, der ihm folgt?

Wo wir gerade bei internationaler Zusammenarbeit sind: Deutschland hat noch immer eine Vorbildfunktion für die europäischen Nachbarn. Leider, und jetzt kommt die Enttäuschung, geht es dabei weder um unser Bier noch um die großartige Leistung unserer Eishockey-Mannschaft. Anlass zur Nachahmung bietet vielmehr das Netzwerkdurchsetzungsgesetz.

Jetzt könnten optimistische Menschen noch hoffen, dass endlich auch Franzosen, Finnen und Niederländer so tolle zusammengesetzte Substantive bauen wollen wie wir. Netzwerkdurchsetzungsgesetz, Donau-Dampfschifffahrtsgesellschafts-Kapitäns-Patent, Rindfleisch-Ettikettierungs-Überwachungsaufgaben-Übertragungsgetz. Das wäre doch für Leute, die Sprachspiele lieben, ein Experiment wert.

Leider ist das aber auch weit gefehlt. Statt linguistischer Kreativität bewegt die Politikerinnen und Politiker wieder einmal der schlichte Wunsch nach Kontrolle. Sie sind offensichtlich der Ansicht, ein Gesetz, das für eine weiträumige Zensur kontroverser Inhalte sorgt, indem es Plattform-Betreiber (die weder Anwälte noch Richter noch Hellseher sind) mit Strafen für rechtswidrige Postings bedroht, sei eine gute Idee. Wenn das nicht enttäuschend ist, weiß ich es auch nicht.

Meta-Enttäuschung

Mit diesen eher düsteren Beobachtungen verabschiede ich mich von euch. Ich hoffe, der Monatsrückblick hat euch Spaß gemacht, auch wenn es wieder einmal vor allem um Verfehlungen und Unzulänglichkeiten ging. Trösten wir uns damit, dass die Mächtigen immerhin die Erwartung, dass sie uns enttäuschen werden, niemals enttäuschen. In diesem Sinne: bis zum März und somit zum nächsten satirischen Monatsrückblick!

Eure Annika Kremer

Verantwortlich für den redaktionellen Inhalt:

Lars Sobiraj

Redaktion:
Lars Sobiraj
Annika Kremer
Antonia
Andreas Köppen

Verantwortlich für Layout und Design:

Jakob Ginzburg

Ein Angebot von

digital publishing momentum

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

tarnkappe.info MAGAZIN

06

digital
publishing
momentum