tarnkappe MAGAZIN 03
Juli | August

Deutschland

Hat die Wahl.

Liebe Leserinnen und Leser,

netzpolitische Themen interessieren dieses Jahr im Wahlkampf keine Sau, um es auf den Punkt zu bringen. Wir schauen einmal gemeinsam, warum das so ist.

Keine der zur Wahl stehenden Parteien, außer der Piratenpartei, hat in diesem Jahr digitale Themen in den Fokus ihrer Wahlkampagne gerückt. Die FDP setzt sich immerhin in Teilen damit auseinander. Allerdings werden in deren Plakatwerbung Datenschützer als ewige Bedenkenträger und wirtschaftliche Bremsklötze abgestempelt, weswegen man fordert: „Digital first. Bedenken second.“ Der Liberalisierung der Finanzmärkte soll nun offenbar der absolute Kontrollverlust über all unsere Daten folgen. Bequeme Einstellung, denn in dem Fall müsste man zum Schutz unserer Daten rein gar nichts tun.

Dabei gab es früher mal eine Partei, die sich solchen Fragestellungen kritisch und mit Erfolg angenommen hat. Angefangen hat die Piratenbewegung übrigens in Schweden, wo zum Jahreswechsel 2005/2006 die Beschlagnahmung der Server von The Pirate Bay für die Entstehung der gleichnamigen politischen Bewegung sorgte. Zehn Monate später trafen sich Politikinteressierte in der Berliner c-base, um die Piratenpartei Deutschland zu gründen. Aus den 53 Teilnehmern sind vergleichsweise schnell über 10.000 Mitglieder geworden. Alles Menschen, denen es nicht egal ist, ob Apple, Google & Co und somit auch diverse Geheimdienste mit ihren Daten machen können, was immer sie wollen. Doch die Sache mit den Piraten wurde, wie wir alle wissen, trotz der anfänglichen Euphorie, leider keine Erfolgsgeschichte.

Leider keine Erfolgsgeschichte...

Als ich den Piraten im Mai 2010 erstmals live und in Farbe begegnete, sah deren Zukunft noch rosig aus. Wie ein kreatives Chaos wirkte der Bundesparteitag im wunderschönen Bingen am Rhein. Die Halle hatte damals der Breakpoint-Organisator und IT-Unternehmer Simon „Scamp“ Kissel besorgt, der aus dem Staunen nicht mehr herauskam. Es gab außerhalb der Demoszene tatsächlich Leute, die ihm noch mehr auf den Keks gehen konnten, wie er erstaunt zum Besten gab. Wer von den Piraten gegen seinen Willen nach draußen befördert wurde, hat seinem Frust nicht nur wie ein Demoszener lautstark Luft gemacht. Nein, sie kramten ihr Smartphone mit samt Paragraphen und Kommentaren hervor, um daraus zu zitieren. Kissel wurde nicht selten in Grund und Boden

geredet, um die angeblich fehlende juristische Grundlage für das von ihm erteilte Hausverbot ausführlichst zu erörtern.

Wenige Monate später war ich im Ruhrgebiet auf einem Landesparteitag der NRW-Piraten zugegen. Der frühere Kassenwart hatte dem Vorstand nichts als einen Haufen unsortierter Zettel hinterlassen. Von einer geordneten Buchführung oder nachvollziehbaren Parteifinanzierung keine Rede. Niemand konnte erörtern, woher die vorhandenen Gelder kamen oder wofür sie ausgegeben wurden. Bekanntlich blieb dies nicht das letzte Mal, dass so etwas geschah.

Nach dem triumphalen Einzug ins Berliner Abgeordnetenhaus 2011 ging es leider nur noch steil bergab. Nicht diejenigen Personen, die sich zum Wohl der Bürgerinnen und Bürger einsetzen wollten, hatten dort das Sagen. Die Führung hatten die wenige Menschen inne, die sich aufgrund der Größe ihres Egos und ihrer Ellenbogen am meisten dazu berufen fühlten. Doch Probleme gab es nicht nur im Abgeordnetenhaus. Es folgte ein Bundesvorsitzender auf den nächsten. Niemand war dazu in der Lage, das Schiff vor dem Kentern zu retten. Die Berliner Fraktion hatte als Vorreiter auch auf Bundesebene die Führung übernommen und steuerte das Boot hart in Richtung Abgrund. Wehe, jemand wollte sie davon abhalten, der musste Kiel holen gehen und ward nie wieder gesehen. Wer es genauer wissen will, kann sich eines der Bücher kaufen, in denen das Scheitern der Orangen, wie sie auch manchmal genannt werden, im Detail behandelt wird. Und wenn man hinterher nicht viel schlauer sein sollte, dann hat man wenigstens einen der Fachbuch-Autoren durchgefüttert, das ist doch auch was wert.

Wie dem auch sei. Nach einiger Zeit offenbarten sich die Probleme der Piratenpartei sehr deutlich. Auch der Welpenschutz, den jede neue politische Bewegung genießt, ist

irgendwann vorbei. Dann wird die getane Arbeit bilanziert und im wahrsten Sinne des Wortes abgerechnet. Schnell zeigte sich, anders zu sein als die anderen Volksvertreter, reicht auf Dauer nicht. Substanz musste her, da kam aber aus Berlin lange Zeit nichts rüber. Auch in Düsseldorf machten manche Abgeordnete wie Birgit Rydlewski mehr Reden von ihren geplatzten Kondom und der letzten Nacht mit einem Unbekannten, als von ihrer Oppositionsarbeit.

Dazu kam und kommt der arrogante Tonfall, der bei den Piraten bei technischen Themen bis heute vorherrscht. Doch wenn man stets mit erhobenem Zeigefinger auf die Fehler Dritter hinweist und glaubt alles besser zu wissen, so schlägt das Pendel irgendwann gnadenlos zurück. Auch an den öffentlich ausgetragenen Streitereien (zumeist bei Twitter) änderte sich im Laufe der Jahre nichts. Selbst dann nicht, als klar war, dass man im ersten Anlauf den Einzug in den Bundestag verpassen würde. Nun wird sich die Geschichte wiederholen. Allerdings mit dem Unterschied, dass die Piraten schon lange von den Medien ignoriert werden.

Dazu kommt, dass die Piratenpartei ihre besten Leute schon vor langer Zeit verloren hat. Mit der Führungsriege von 2010 hat die heutige nichts mehr gemeinsam. Man kämpft gegeneinander noch immer mit allen Mitteln, obwohl es kaum noch etwas zu erreichen gibt. Es bleibt sogar abzuwarten, ob es den Piraten auf Kommunalebene dauerhaft gelingen wird, ihren Fuß in der Tür zu halten. Mehr zu erreichen ist eh schon lange nicht mehr denkbar.

Auf den Hund gekommen: der frühere Bundesvorsitzende Bernd Schlömer, jetzt FDP-Mitglied.

Netzpolitik: auf der Strecke geblieben

Was dabei leider letzten Endes auf der Strecke blieb und bis heute bleibt, ist die Netzpolitik an sich. Wir haben in dieser Ausgabe des Tarnkappe Magazins zusammengetragen, welche Tiefpunkte sich die Große Koalition innerhalb der letzten Jahre in allen digitalen Belangen geleistet hat. Fest steht schon jetzt, es sind nicht wenige! Und trotzdem steuert unsere Republik auf eine schwarz-gelbe Koalition hin, wenn man den Umfragen Glauben schenken darf.

Nach dem Aufkommen der Piraten wurden netzpolitische Themen schnell von der politischen Konkurrenz übernommen, um sie später wieder zu vergessen. Warum? Ganz einfach, weil man mit Datenschutz, dem Kampf gegen Filesharing-Abmahnungen, Netzsperren oder behördlicher Zensur schlichtweg keine Wahl gewinnen kann.

Die Menschen interessieren sich für den Erhalt ihres Arbeitsplatzes, für ihr Einkommen und ihre kommende Rente. Sie wollen lebenswerte Bedingungen für sich und ihre Kinder. Ob die NSA oder Google Schindluder mit unseren Daten treibt, juckt niemanden. Der Grund dafür ist einfach: Die Verwertung bzw. den Verkauf von Informationen riecht man nicht, hört man nicht und schmeckt man nicht. Daten erscheinen den meisten flüchtig zu sein. Und was soll es eigentlich? Solange man seinen Mail-Anbieter oder sein Lieblings-Netzwerk für lau nutzen kann, spielt der Rest doch eh keine Rolle, oder? Datenschutz ist ja ganz nett. So richtig wichtig ist es vielen Nutzern nicht. Würde Facebook im Umkehrschluss eine Monatsgebühr von 5 Euro einführen, wäre es bald sehr leer dort. Man bezahlt halt lieber lautlos mit seinen Daten, statt das Girokonto dafür anrühren zu müssen.

Die AfD, so ekelhaft wie erfolgreich

Und die AfD? Die mag parteiintern ihre eigenen Fehler be-

gehen, daran besteht kein Zweifel. Doch diese Partei war stets erfolgreich darin, Ängste in der Bevölkerung zu schüren. Angst vor Überfremdung. Angst davor, dass das hart erarbeitete Gehalt beim nächsten Bankencrash nichts mehr wert sein könnte, wenn der Euro ins Bodenlose stürzt. Angst davor, dass sich unsere Gesellschaft weiter in Richtung Multi-Kulti verwandelt oder hierzulande zu viele Flüchtlinge aufgenommen werden. Doch wie viele Kulturen sind zu wenig oder gar genug? Ab welcher Anzahl Flüchtlinge sind es zu viele, die Schutz bei uns suchen? Wie kann man die politisch Verfolgten sehr viel schneller von den reinen Wirtschaftsflüchtlingen trennen? Wo richten wir die Grenzen nach außen hin ein und mit welchen Mitteln sollen diese verteidigt werden? Mit Unterstützung von Soldaten, Knüppeln und Stacheldraht? Ungelöst ist auch: Was sollen wir tun mit den Banken, die in Berlin oder Brüssel niemand kontrollieren kann oder will? Viele Fragen und keine Antworten.

Doch genau das ist das Erfolgsrezept der AfD. Sie präsentieren uns jede Menge Probleme, aber geben keine Antworten, wie man diese wieder los wird. Das nämlich wäre schwierig, weil derartige Probleme niemand mal eben im Vorbeigehen lösen kann. Und dann müsste man zugeben, dass es neben Schwarz und Weiß auch noch andere Zwischentöne gibt. Dass Politik kompliziert ist und stets die Suche nach gehbaren Kompromissen beinhaltet, die möglichst wenigen wehtut. Allen kann man es sowieso nicht recht machen. Und wirklich schnell geht in einer Demokratie auch keine Veränderung vonstatten. Doch nichts anderes ist es ja, was man uns auf den AfD-Plakaten anpreist.

Doch Ängste vor Veränderung und einfache Parolen, die auch das einfache Volk versteht, das zieht. Denn dabei geht es um die Befriedigung unserer Grundbedürfnisse. Es geht darum, seinen Lebensstandard zu halten, die Rente zu sichern und seinen Kindern eine gute Schul- und Berufsausbildung angedeihen zu lassen, damit auch sie später gute Chancen auf dem Arbeitsmarkt haben. Und nicht viel anderes versprechen auch die anderen etablierten Parteien. Die Grünen haben sich noch einen Hauch Umweltschutz mit auf die Fahnen geschrieben.

„Jedes Volk bekommt die Regierung, die es verdient."

Doch Datenschutz, so wichtig er ist: Das ist kein Grundbedürfnis und auch nichts, womit ich als Otto-Normalverbraucher am Monatsende meinen Kühlschrank füllen kann. Angst kann man mit dem Thema auch niemandem einjagen. Edward Snowden? Wer war das nochmal? Auch er ist längst vergessen und wird von den Medien ignoriert, wenn man ehrlich ist. NSA, BND, oder LmaA., das interessiert bis auf ein paar CCC-Jünger (ich bin selbst einer, deswegen darf ich das sagen) niemanden mehr.

Mein Politiklehrer sagte mal etwas vor Urzeiten, was bis heute nichts an Wahrheit eingebüßt hat: Jedes Volk bekommt die Regierung, die es verdient.

Oh weh, schaut man über den großen Teich hinüber zum „USA first" Trumpel-Tier, so sind dies wahrlich keine guten Vorzeichen. Doch seien wir ehrlich: ohne Mama Merkel oder den US-Elefanten im Ego-Laden hätten wir nichts mehr, worüber wir uns aufregen könnten, oder?

In diesem Sinne...

Euer Chefredakteur
Lars Sobiraj

SZENE

LUL.TO: WIE WURDEN DIE BETREIBER ERWISCHT?

Im Netz kursieren einige Thesen, wie man die deutschen Betreiber des illegalen Bezahl-Portals Lesen & Lauschen (LuL.to) identifiziert hat. Welche Thesen sind wahrscheinlich? Wie gehen die Ermittler in solchen Fällen vor? Wir haben nachgeforscht.

Schwarzkopierer sind Robben, keine Haie!

Wir haben uns kürzlich mit einem Piratenjäger unterhalten, der anonym bleiben möchte. Die Person vergleicht die Betreiber von P2P-Index-, Streaming- bzw. Kauf-Portalen mit Robben. Immer sei die Rede, dass die Schwarzkopierer wie gefräßige Haie im Meer herumschwimmen würden und ihnen keiner etwas könne. Das stimme so aber nicht, sagte mir der Anti-Piracy-Ermittler, der im Auftrag diverser Rechteinhaber tätig ist. Haie müssen ihr schützendes Meer nie verlassen, Robben hingegen schon. Sie suchen zum Beispiel Luftlöcher in der Eisdecke, weil sie sonst ersticken würden.

So sei es auch mit den Piraten. Ihr Sauerstoff, ihr Schwachpunkt, sei das Geld, welches sie wie die Meerestiere zum Atmen brauchen. Privatwirtschaftliche als auch behördliche Ermittler würden oft der Spur des Geldes folgen. Dabei spiele es keine Rolle, ob die Piraten für ihr Vorhaben im Ausland extra eine Limited oder eine andere Firma inklusive Briefkasten-Adresse gegründet haben. Irgendwann später wollen sie Zugriff auf das Guthaben der Konten der Offshore-Firma haben, was nicht ungefährlich ist. Dazu kommt: Kaum jemand verdient mit seinen Portalen genügend Geld für einen Auslandsaufenthalt oder möchte Deutschland dauerhaft verlassen, um sich den hiesigen Behörden zu entziehen.

Wie also könnte man konkret versucht haben, LuL.to auszuheben? Das Recherchieren der Werbepartner fiel weg, dort wurden keine Banner geschaltet. Man konnte bei LuL.to vorgeben einzukaufen, um mit einem Amazon-Gutschein zu bezahlen. Paysafe Karten werden dort ja schon seit einiger Zeit nicht mehr akzeptiert. Wahrscheinlich, weil Paysafe von einem Rechteinhaber oder dessen Rechtsanwaltskanzlei darauf hingewiesen wurde, dass über ihr Unternehmen Geldwäsche in Verbindung mit gewerblichen Urheberrechtsverletzungen durchgeführt wurde. Die Grundlagen der verschiedenen Rechtsverstöße, die die LuL-Nutzer begangen haben, haben wir ja ausführlich in unserem Hintergrundbericht behandelt, der hier verfügbar ist.

Doch zurück zu den Amazon-Gutscheinen, mit denen verschiedene Ermittler ihr Guthaben bei LuL.to aufgeladen haben könnten. Diese Gutscheine werden zeitnah von einem der Betreiber oder einem im Team integrierten Einkäufer bei Amazon eingelöst. So wandert das Geld entweder direkt beim echten Account oder Fake-Account des Betreibers oder des Einkäufers. Die Behörde, die nun wissen will, wer für das Einlösen des Gutscheines verantwortlich ist, muss sich an den Herausgeber der Gutscheine wenden. Das geht nach Auskunft des Piratenjägers in bestimmten Fällen nur mittels eines Rechtshilfeersuchens (Herausgeber sitzt nicht in Deutschland, die deutsche Amazon-Tochter gibt nämlich keine Auskunft), was viele Monate in Anspruch nehmen kann. Da heißt konkret: Eine deutsche Behörde (Staatsanwaltschaft) fragt per Amtshilfe z. B. bei der zuständigen US-Behörde nach, wenn der Gutscheinherausgeber seinen Sitz in den USA hat. Diese stellt dann eine Anfrage beim Unternehmen mit Sitz in den USA, hier Amazon. Bis die Informationen über den Eigentümer des Accounts, der die Gutscheine eingelöst hat, in Deutschland angelangt sind, kann einige Zeit vergehen. Das wird aller Wahrscheinlichkeit nach der Grund sein, warum es so lange gedauert hat, die drei Hintermänner von LuL.to zu identifizieren.

Doch die Staatsanwaltschaft will ja nicht nur die einzelne Person dingfest machen, die den Amazon-Gutschein eingelöst hat. Im Idealfall sollen alle Beteiligten überführt werden, die direkt oder indirekt etwas am Betrieb der Webseite verdient haben. Auch das nimmt seine Zeit in Anspruch.

Ein Trick der Ermittler: Amazon-Gutscheine, die sich plötzlich in Luft auflösen

Manche Gutscheine bei Amazon sind getürkt, um Piraten zu überführen. Spiegelbest hat der Redaktion von Tarnkappe.info damals erzählt, dass er Amazon-Gutscheine zum Kauf von E-Books bei Amazon.de nutzen wollte. Wenn man den Kauf der E-Books auf diese Gutscheine tätigt, beispielsweise um diese im eigenen Bezahl-Portal anzubieten, so wird man feststellen, dass die Gutscheine nach einiger Zeit ungültig sind, weil sie durch die Ermittler entwertet wurden. Auch die Fake-Gutscheine sind ja bei Eingabe des Gutscheincodes unwiderruflich mit dem ent-

sprechenden Amazon-Konto verknüpft, mit dem man eingeloggt war. War das Konto nun gefaked (sprich: mit falschen Daten versehen) und man kauft mit diesem Account ein Buch mit so einem gefakten Gutschein ein, so passiert in der Regel Folgendes: Man erhält von Amazon das gekaufte E-Book, kurz darauf wird aber der Gutschein, womit das Buch bezahlt wurde, ungültig. Ein Fake-Account kann nicht an eine echte Bankverbindung geknüpft sein, mit der man noch alternativ zahlen könnte, also hätte man dann ein Buch erhalten ohne zu bezahlen. So wird der Fake-Account unverzüglich von Amazon gelöscht – eben weil man nicht für den getätigten Kauf bezahlt hat. Bis man einen neuen Fake-Account mit zahlreichen überprüfbaren Daten aufbauen kann, dauert eine ganze Weile. Das soll den Einkauf bei Amazon für E-Book-Piraten so aufwändig gestalten, dass diese ihre Werke woanders beziehen. Doch wer so unvorsichtig war, seinen echten Account für das Einlösen der Fake-Gutscheine der Piratenjäger zu nutzen, wurde im selben Moment überführt. Da kann man sich nicht mehr herausreden. Wie will man bitte der Polizei erklären, wie man an den Gutscheincode gelangt ist, außer man hat mit der Beschaffung der E-Books oder dem Betrieb des Portals etwas zu tun!? Deswegen werden von verschiedenen Ermittlern immer wieder gerne gefälschte Amazon-Gutscheine gezielt zur Bezahlung benutzt, um die Piraten zu überführen oder ihnen das Geschäft zumindest deutlich zu erschweren. Zumindest Spiegelbest hat es damals nach einigen geplatzten Amazon-Accounts vorgezogen, seine Quelle für E-Books zu wechseln.

Wandelten zwei Eincasher für LuL.to Amazon-Gutscheine in Bitcoin um?

Im Forum Bitcointalk.org wird seit der Razzia gemutmaßt, dass dort zwei Anbieter Amazon-Gutscheine für LuL.to in Bitcoin umgewandelt haben sollen. Diese Aussage lässt sich von uns leider nicht ohne weiteres überprüfen. Der User MrDJ war bei Bitcointalk einen Tag vor dem Bust das letzte Mal online. MrLehmann, in der Szene ist das Pseudonym nicht unbekannt, war hingegen zwei Tage nach dem Bust eingeloggt, was gegen dieses Gerücht spricht – außer er war es nicht selbst. Wir erinnern uns: Nur die wenigsten Szenemitglieder verschlüsseln ihre Computer, worüber sich GVU & Co. natürlich sehr freuen. MrLehmann hat bei Bitcointalk sogar seine Bitcoin-Adresse öffentlich im Profil angegeben, womit man jegliche Bitcoin-Transaktion öffentlich einsehen kann, sofern seine Bitcoin-Adresse noch stimmt beziehungsweise aktuell ist.

MrDJ wird von MrLehmann im Werbe-Thread übrigens als sein „offizieller Mitarbeiter“ bezeichnet. Tatsache ist, dass Spiegelbest damals mindestens einen Eincasher an LuL.to vermittelt hat, wie er damals berichtet hat. Später war das Verhältnis zwischen ihm und LuL.to bekanntlich sehr gespalten, anfangs half er ihnen noch. Vor seinem Ausstieg aus der Szene hat Spiegelbest sowohl auf seinem eigenen Blog als auch bei Tarnkappe.info sehr negativ über die Macher von LuL.to berichtet. Ihm war wirklich jedes Mittel recht, um ihnen einen reinzuwürgen.

Da Bitcoin-Transaktionen nur vorgeblich anonym sind, musste die Spur des Geldes mittels eines Bitcoin-Mixing-Dienstes nach dem Umtausch der Gutscheine in die virtuelle Währung verschleiert werden. Wer Mathematiker ist und tief genug in der Materie steckt, darf uns bei passender Gelegenheit gerne erläutern, unter welchen Voraussetzungen derartige Vermischungen der Bitcoin-Guthaben zum gewünschten Ziel führen. Tja, oder eben nicht.

Downloads liefen über Cloudflare

Wie dem auch sei. Geld gebraucht haben die Betreiber von LuL.to auch noch aus anderen Gründen. Alle Downloads wurden in den letzten Monaten über den Dienstleister Cloudflare realisiert. Das war sehr teuer, weil dies nicht Teil des regulären Angebots ist. Der Bezug der E-Books und Hörbücher über Cloudflare hatte für die drei Hintermänner aber den Vorteil, dass man von außen nicht erkennen konnte, wo ihre Server lokalisiert waren. Deutsche Server sind hierzulande mit Abstand am preiswertesten und verfügen über eine vergleichsweise schnelle Anbindung. Kostenlos sind sie freilich nicht. Auch von daher wurde Geld benötigt und ausgegeben, was offenbar seine eigenen Spuren hinterlassen hat.

Die LuL.to-Betreiber waren keine guten Menschen!

Doch machen wir uns bitte nichts vor: Die wenigsten Piraten gehen ihrer Tätigkeit aus altruistischen Gründen nach. Geld zu machen, ist eine Sache. Es verschwinden zu lassen, ist, wie man sehen kann, sehr viel komplizierter. Immerhin haben sich ja laut Pressemitteilung im Falle LuL.to rund 100.000 Euro auf mehreren Konten befunden, die die Behörden beschlagnahmt haben. Halten wir fest: Aus Selbstlosigkeit oder als reine Freizeitbeschäftigung wurde dieses Portal zumindest nicht betrieben. Ähnlich wie bei TorBoox ging es den Machern um das große Geld. In der Causa TorBoox wurden die Nutzer zumindest anfangs beschenkt, bei LuL.to sollten sie von Beginn an bezahlen.

ALPHABAY: WURDE DER DARKNET-MARKT-PLATZ BESTOHLEN?

AlphaBay Market, einer der größten Umschlagplätze im Darknet, ist seit Dienstag Nacht nicht mehr erreichbar. Die User des Online-Anbieters befürchten Betrug, berichtet The Verge.

AlphaBay ist ein im Tor-Netzwerk als Hidden Service betriebener Darknet-Markt, der bereits seit 2014 besteht und auf dem vor allem Betrugs- und digitale Güter, aber auch illegale Drogen, verschreibungspflichtige Medikamente und Waffen gehandelt werden. Als Zahlungsmittel wird die anonyme Kryptowährung Bitcoin akzeptiert.

Ein Administrator gab auf Reddit bekannt, dass die Website aufgrund von technischer Wartungsarbeiten vorübergehend offline ist. Da die Plattform aber bereits seit dem 4. Juli unerreichbar und auch nicht über Ausweichseiten, also Mirrors, erreichbar ist, bezweifeln viele User, dass es sich tatsächlich um Wartungsarbeiten handelt. In dem Zusammenhang sollen zudem massive Bitcoin-Abhebungen im Wert von ca. 3,8 Millionen US-Dollar durch die Accounts der Seite durchgeführt worden sein.

Diese Tatsache hat auf Reddit und Twitter zu Spekulationen geführt, dass die Verantwortlichen die Seite geschlossen haben, um die AlphaBay-Nutzer zu bestehlen. „Exit Scam“ sind in dieser „Branche“ nicht ungewöhnlich: Es gab bereits Fälle, wo die Betreiber solcher Marktplätze mit dem Geld ihrer Kunden verschwanden. Zwar wird die Schuld gerne Hackern zugeschoben, beides lässt sich jedoch nur schwer beweisen.

Ob es sich auch bei AlphaBay um ein „Exit Scam“ handelt, ist bisher nur eine Vermutung. Kenner der Plattform verweisen darauf, dass dort sehr viel mehr Geld stecken würde, als die bisher entwendeten knapp vier Millionen Dollar.

NACH DEM BUST VON LUL.TO: QUO VADIS E-BOOK SZENE?

Ist die illegale E-Bookquelle mit dem Bust von LuL.to nun für immer versiegt? Genau diese Frage wird sich wohl so mancher Lesefreund, der auf kostenlosen oder preisgünstigen Lesestoff – aus welchen Gründen heraus auch immer – nicht verzichten möchte, schon gestellt haben. Denn auf den einschlägigen Seiten, wie den Boersen, dem Usenet, MyGully, aber auch bei Sumsels Lesen.to bleibt nun seither der Nachschub an Lesestoff offenbar aus. Alles, was in der Release-Szene derzeit noch erscheint, sind ausschließlich aktuelle Zeitungen & Zeitschriften.

Deshalb wäre daraus zu schlussfolgern, dass das Team von LuL.to die einzigen Einkäufer von E-Books gewesen sind, die diese der breiten Öffentlichkeit auch zur Verfügung gestellt haben. Verteiler, die nur darauf gewartet haben, was bei LuL.to gerade erscheint, gab es demnach zur Genüge. Sie haben abgegriffen, was tagtäglich dort gepostet wurde und dann auf dem Portal ihrer Wahl hochgeladen. So wurden bisher scheinbar alle versorgt. Doch wie geht es nun weiter?

Was für die Verlagsautoren, wie Andreas Eschbach, als auch für die zahlreichen Selbstpublisher ein Grund zur Freude ist, lässt in der Szene doch schon einige Unruhe, bzw. Verlustängste aufkommen: Bis jetzt ist noch kein neues, illegales Portal mit Neuerscheinungen, Spiegelbestsellern, den Lieblingsserien oder dem Lieblingsautor am Start.

Da anzunehmen ist, die Ermittler verfolgten die Spur des Geldes, läge nun die Vermutung nahe, dass gerade dieser Umstand ein solches Unternehmen von vorn herein als zu riskant erscheinen lässt. Auch kann nicht jeder X-Beliebige plötzlich sagen:

„Ach, ich eröffne mal so eben ein illegales Buchportal, weil ich schnell reich werden will.“ Es wäre selbst hier schon ein gewisses Wissen über Bücher angebracht. Man sollte zumindest über die Erscheinungsdaten der Titel informiert sein – und das bei jedem Genre. Auch Bescheid zu wissen über Trends auf dem Buchmarkt, wäre von Vorteil. Und wie man bei Spiegelbest gesehen hat: ohne Programmiererfahrung läuft ebenso wenig etwas.

Zwei Vorraussetzungen also, die unabdingbar vorhanden sein müssen, für die Eröffnung eines neuen, illegalen Buchportals. Sicher keine unüberwindbaren Hürden, aber dennoch… Wie es weitergeht, wird sich zeigen. Meine Vermutung ist, dass sich eben nicht so schnell, wie bereits hier in den Kommentaren geäußert, ein Nachfolger finden wird, der ein solches Risiko auf sich nehmen wird.

Ich würde auch meinen, dass es für die Buchbranche insgesamt gut ist, nun über eine längere Zeitperiode nicht piratisiert zu werden. Ein Umstand, der bei vielen Autoren die Lust am Schreiben ganz sicher neu aufleben lassen wird – und ist es nicht gerade das, was sich auch die Leser, mich eingeschlossen, wünschen?

OBOOM REAKTIVIERT VERGÜTUNG FÜR UPLOADER

OBOOM versus Uploaded & Share-Online.biz. Der Kampf um den deutschsprachigen Markt geht in die nächste Runde. Im Laufe des heutigen Abends werden die Nutzer des chinesischen Anbieters OBOOM per Newsletter darüber informiert, dass man die Downloadvergütung reaktiviert hat. Ab dem heutigen Montag werden den Uploadern wieder ihre Transfers in Richtung Deutschland, Österreich und die Schweiz vergütet.

Kurz notiert: Während dem Branchenprimus Uploaded aufgrund seiner Lokalisierung in der Schweiz Ungemach in Form diverser Klagen droht, wo vor Gericht noch nicht das letzte Wort gesprochen wurde, hat sich der Filehoster OBOOM mit Sitz in Hong Kong dazu entschlossen, seine Downloadvergütung wieder aufzunehmen. Seit mehreren Stunden wird der Newsletter an alle registrierten Nutzer von OBOOM verteilt.

Die Uploader, die wieder einsteigen wollen, müssen auf der Webseite des Sharehosters ihr „Partnerprogramm-Modell auf PPD“ umstellen, wie es in der E-Mail heißt. Wie üblich spielt bei der Höhe der Downloadvergütung die Dateigröße der bezogenen Files eine entscheidende Rolle, weswegen sich der Upload von Warez wie E-Books absolut nicht lohnt.

Die Lieferanten der Szene (= Uploader) haben jetzt also die Wahl zwischen dem gut zahlenden Uploaded.net und somit der Gefahr, früher oder später auf Druck der Rechteinhaber aufgrund ihrer Urheberrechtsverletzungen gesperrt zu werden, womit augenblicklich ihre Umsätze verloren gehen. Oder aber sie laden ihre Archive bei Share-Online.biz oder OBOOM hoch im Wissen, dass sie dort zwar nicht gesperrt aber im gleichen Atemzug schlechter entlohnt werden. Im Prinzip haben die Uploader nun die Wahl zwischen dem Teufel und dem Belzebub, genauer betrachtet zwischen mehreren schlechten Alternativen.

Die Stimmung ist in diesem Sektor übrigens schon seit längerer Zeit gereizt. Im Herbst 2015 zeigte sich ein Aachener Abrechnungs-Unternehmen, das für einen populären Online-Speicher-Dienst aus Belmopan tätig ist, recht dünnhäutig. Wir erhielten eine Abmahnung der Online-Media24 Ltd., weil wir zuvor entgegen des Willens des Online-Media24-Geschäftsführers Manuel Chionoudakis auf unserer Webseite eine in bestimmten Kreisen bekannte Kontonummer der Sparkasse Aachen angegeben haben. Ohne Namensnennung einer Firma oder Privatperson im Beitrag ist keine Rufschädigung und somit keine Abmahnung möglich, dachten wir. Falsch gedacht. Herr Chionoudakis oder vielleicht auch nur sein Anwalt vertraten damals in ihrem Schreiben eine andere Meinung.

Wie dem auch sei. OBOOM hat mit der Wiederaufnahme der Downloadvergütung die Zügel ein wenig angezogen und hofft, damit Druck auf die Konkurrenten Uploaded & Share-Online auszuüben. Man darf gespannt sein, wie sich der Kampf um den deutschsprachigen Warez-Markt weiter entwickelt. In diversen Foren laufen schon Wetten, wann die Betreibergesellschaft von Uploaded ins Ausland jenseits der EU-Grenzen abwandert.

HANSA MARKET: ERMITTLER NEHMEN WEITEREN DARKNET-MARKTPLATZ VOM NETZ

Laut einer Pressemitteilung von Europol vom 20.07.2017 haben Monate der Vorbereitung und Koordination nun Ergebnisse gezeigt, die beiden Darknet-Märkte AlphaBay und Hansa wären nun für immer vom Netz genommen. Zwei bedeutende Strafverfolgungsmaßnahmen, die unter Beteiligung des Federal Bureau of Investigation (FBI), der US Drug Enforcement Agency (DEA), der Dutch National Police und mit Unterstützung von Europol durchgeführt wurden.

Hansa Market warb damit, extrem sicher zu sein. Man behauptete, es gäbe keine Möglichkeit, dass jemand mit den Bitcoins der Kunden wegläuft – weder Verkäufer noch die Website selbst und er wäre grundsätzlich immun gegen Exit-Scam. Man wollte sich von den anderen Marktplätzen durch ein „vertrauenswürdiges Zahlungssystem“ abheben. Die Produktpalette war vielfältig. Zum Portfolio gehörten Drogen genauso, wie verschreibungspflichtige Medikamente, Tutorials für Cyberkriminelle, anonyme Hostingdienste, Falschgeld, gefälschte Pässe, gehackte Kreditkartendaten und zudem Waffen. Ein „einfach zu bedienendes Zahlungssystem und ein einladendes Layout“ sollte viele Kunden anlocken.

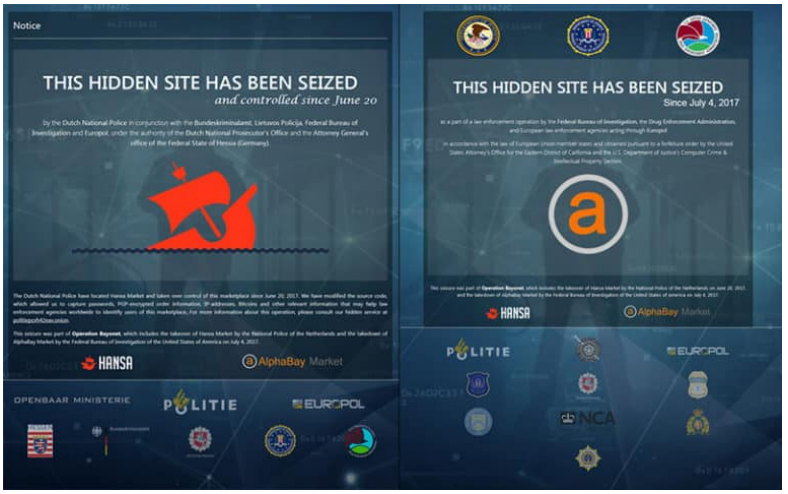
Das Konzept ist demnach aufgegangen: Hansa Market war nach Europol-Angaben der drittgrößte Untergrund-Marktplatz. Drogenhandel soll dort in ähnlicher Größenordnung betrieben worden sein wie bei AlphaBay. Die zwei Hansa-Administratoren wurden in Deutschland festgenommen, Server in den Niederlanden, Deutschland und Litauen beschlagnahmt.

Hansa Market ist am 20.07.2017 offline gegangen. Zuvor sicherte sich die niederländische Polizei noch „wertvolle Informationen“ über „hochrangige Ziele“ und Lieferadressen für eine größere Zahl von Bestellungen. 10.000 Adressen ausländischer Hansa-Kunden seien dabei an Europol weitergegeben worden und werden nun für weitere Ermittlungen ausgewertet.

Die niederländische Polizei hat auf der ehemaligen Hansa-Seite einen Hinweis geschaltet, laut dem die Seite der Polizei bereits seit dem 20. Juni als Honeypot diente, wobei der Code so verändert wurde, dass man in der Lage war, Passwörter mitzuschneiden, die den Strafverfolgern helfen könnten auch Nutzer des Marktplatzes zu identifizieren und die Überwachung der kriminellen Aktivitäten auf der Plattform zu erleichtern. Das Vorgehen war Teil der sogenannten „Operation Bayonet“, zu der auch das Zerschlagen von AlphaBay gehörte.

Was diese gemeinsam durchgeführte Aktion so besonders machte, war die Strategie, die von allen Beteiligten gemeinsam entwickelt wurde: Zuerst wurde Alphabay vom Netz genommen. Die meisten der dortigen Nutzer suchten sich aufgrund der Schließung eine neue Bleibe. Hansa Market verzeichnete nach dem Abschalten von AlphaBay eine achtfache Zunahme der Zahl an neuen Mitgliedern, die allerdings sofort in die von den Ermittlern aufgestellte Falle tappten. Einige der gewonnenen Informationen enthielten auch wertvolle Informationen über das Ziel von Drogen und die Behörden werden die betroffenen Länder über geplante Sendungen von Drogen entsprechend informieren.

Um eine reibungslose Koordination zwischen den beiden Untersuchungen bei AlphaBay und Hansa zu gewährleisten, ver-



anstaltete Europol ein Koordinationstreffen mit führenden Strafverfolgungspartnern. Insgesamt waren 12 verschiedene Agenturen beteiligt und einigten sich auf eine Gesamtstrategie für die beiden Operationen. Auch weiterhin unterstützt Europol das FBI, die DEA, die Dutch National Police und andere Partner bei der forensischen Arbeit, die aufgrund der riesigen Menge an beschlagnahmtem Material notwendig geworden ist.

Rob Wainwright, Direktor von Europol in Den Haag, gab be-

kannt: „Dies ist ein herausragender Erfolg der Behörden in Europa und den USA. […] Wie sich durch die gemeinsame Umsetzung der erfolgreichen Strategie gezeigt hat, haben die Strafverfolgungbehörden nun eine klare Botschaft: Wir haben die Mittel, um die Kriminalität aufzudecken, selbst in Bereichen des Darknet. Es gibt noch mehr von diesen Operationen“, fügte er hinzu.

Betreiber von LuL.to und Hansa Market sind identisch

Laut Medieninformationen wären die Betreiber der Portale LuL.to und Hansa Market offenbar identisch. Demnach handelt es sich um zwei Deutsche, gegen die Anfang Juli im Zusammenhang mit Hansa-Market ein Haftbefehl erlassen wurde. Der 31-Jährige aus Köln und ein 30-Jähriger aus dem Landkreis Siegen-Wittgenstein befanden sich seit dem 21. Juni 2017 in Untersuchungshaft. Das teilte die Generalstaatsanwaltschaft Frankfurt am Main mit.

Beide gelten als Betreiber des Darknet-Marktplatzes Hansa Market und stehen ferner im Verdacht, das illegale Portal LuL.to zum Verkauf urheberrechtlich geschützter Medien betrieben zu haben.

Bei Durchsuchungen der Wohnungen der beiden Verdächtigen seien „zahlreiche Beweismittel, insbesondere Computer und Datenträger, sichergestellt“ worden, hieß es in der Erklärung der Generalstaatsanwaltschaft weiter.

DARKNET: ZOLLFAHNDUNG DECKT ILLEGALEN WAFFENHANDEL AUF

Laut einer Pressemitteilung des Zollfahndungsamtes Frankfurt am Main vom Donnertag (13.07.2017) sollen drei Tatverdächtige, Waffen und Munition für 25.000 Euro im Darknet bestellt haben. Die Ermittlungen richteten sich gegen einen 81-Jährigen aus dem Landkreis Northeim (Niedersachsen), einen 54-Jährigen aus Dortmund und einen 46-Jährigen aus dem Landkreis Altenkirchen (Rheinland-Pfalz).

Bei den drei Tatverdächtigen haben Beamte des Zollfahndungsamtes Frankfurt am Main in drei voneinander unabhängigen Ermittlungsverfahren insgesamt 17 erlaubnispflichtige Schusswaffen, 2.312 Schuss Munition, zehn verbotene Gegenstände (2 Messer, 8 Schlagringe) sowie 2.711 verbotene pyrotechnische Gegenstände beschlagnahmt. Die Sicherstellungen erfolgten Ende Mai und im Juni 2017 bei den Durchsuchungen der Wohnungen der Beschuldigten.

Hans-Jürgen Schmidt, Sprecher des Zollfahndungsamtes Frankfurt am Main gab zu den Fällen bekannt: „Eine besondere Gefährdungssituation ergab sich für unsere Einsatzkräfte bei dem 81-Jährigen aus dem Landkreis Northeim, der einen Teil der bei ihm sichergestellten Schusswaffen schussbereit in seinem Zugriffsbereich aufbewahrte. Nach seinen Angaben wollte er auf alle Eventualitäten vorbereitet sein, deshalb sein Waffenarsenal“.

Bereits im Frühjahr 2017 wurden die Strafverfahren gegen die drei Beschuldigten bei der Staatsanwaltschaft Köln eingeleitet unter der Sachleitung der Generalstaatsanwaltschaft Frankfurt am Main bzw. der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW). Diese Ermittlungserfolge sind das Resultat der Arbeit einer sechsköpfigen Ermittlungskommission des Zollfahndungsamtes Frankfurt am Main, die seit April 2016 gezielt gegen den organisierten Handel und Schmuggel von illegalen Schusswaffen vorgeht.

STREAMDREAM.WS NACH MEHREREN MONATEN WIEDER DA

Das nicht sonderlich populäre Kinoportal StreamDream.ws ist seit kurzem nach mehreren Monaten Downtime wieder online. Wegen privater Zeitprobleme der Betreiber dauerte die Zwangspause länger, als ursprünglich geplant.

Wir wurden per Kommentar als auch per Kontaktformular mehrfach angesprochen, was mit dem illegalen Portal StreamDream.ws passiert sei. Auch in den einschlägigen Quellen wie der Szenebox oder bei MyBoerse.BZ konnten wir auf die von uns gestellte Frage nach dem Verbleib der Seite keine Antwort erhalten.

Nachdem die Webseite nun seit wenigen Wochen wieder online ist, haben wir Kontakt zu den Machern aufgenommen. Die-

se teilten uns mit: „Unsere Seite war nur mangels Zeit für eine Weile in der Downtime.“ So wurde es nach eigenen Angaben versäumt, die Gebühren für die Server zu begleichen. Dort erschien für einige Zeit lediglich die Fehlermeldung: „The server is temporarily unable to service your request due to maintenance downtime or capacity problems. Please try again later.“

Als Alleinstellungsmerkmal streichen die Admins heraus, dass sie bei StreamDream.ws die Mehrzahl der Filme sowohl in geringer als auch hoher Qualität anbieten. „Die User können für unterwegs z.B. die SD-Qualität wählen, damit nicht so viel Datenvolumen verbraucht wird und die Filme dann zu Hause in sehr guter HD-Qualität weiterschauen.“ Wem bei dem vergleichbar kleinen Angebot etwas fehlen sollte, der kann seine Kinofilme oder TV-Serien in der Wunschbox eintragen, damit diese vom Team später als Stream verfügbar gemacht werden.

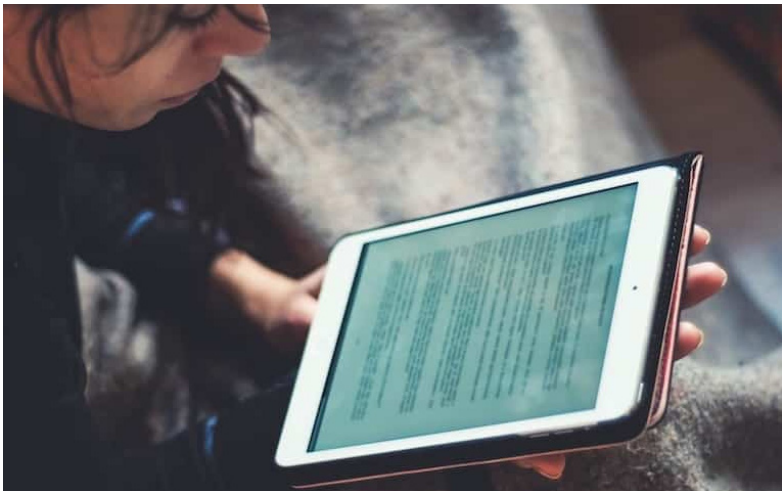
Fazit: Wer eine All-inclusive-Filmflatrate erwartet, dürfte herbe enttäuscht werden. Tatsächlich finden sich dort aber auch einige Raritäten, die speziell für die Zuschauer älteren Semesters interessant sind. Unser Kontakt schrieb uns: „Wir bieten Filme an, die es auf anderen Streamingseiten gar nicht gibt und die man auch nicht als DVD oder Blu-ray Disc kaufen kann.“

STELLUNGNAHME VON ANDREAS ESCHBACH ZUR SCHLIESSUNG VON LUL.TO

Andreas Eschbach erzielte mit Romanen, wie „Die Haarteppichknüpfer“, erschienen 1995, der Space Opera „Quest“ (2001) oder mit dem Thriller „Solarstation“ große Erfolge. Es gelingt ihm dabei auch genreübergreifend utopische Elemente mit denen eines Thrillers zu verbinden. Sein erster Bestseller war der Roman „Das Jesus Video“ (1998). Eschbach studierte in Stuttgart Luft- und Raumfahrttechnik, schloss dieses Studium jedoch nicht ab. Er arbeitete als Softwareentwickler und Unternehmer, bis seine Erfolge als Schriftsteller es ihm erlaubten, sich völlig auf das Schreiben zu konzentrieren. Seit 2003 lebt er mit seiner zweiten Frau Marianne Eschbach in der Bretagne.

Das Piraten-Portal LuL.to bot über einen Zeitraum von ca. drei Jahren Bücher, darunter auch zahlreiche Neuerscheinungen und Spiegelbestseller, an, die weit unter den Verkaufspreisen der Verlage, bzw. Autoren lagen. Die illegale Plattform wurde durch das CyberCrimeCompetenceCenter (SN4C) des LKA Sachsen am 21. Juni 2017 für immer vom Netz genommen. Gegen die drei Betreiber laufen umfangreiche Ermittlungen. Sie befinden sich derzeit in Untersuchungshaft.

Wir vom Team Tarnkappe.info haben den Schriftsteller Andreas Eschbach gefragt, was die Schließung des Piratenportals LuL.to für ihn persönlich bedeutet. Er antwortete uns: „Von der Schließung von lul.to höre ich zum ersten Mal; mir war die Existenz dieses Portals ehrlich gesagt gar nicht bewusst: Wie die meisten Autoren versuche ich, nicht allzu viele Gedanken an Piraterie zu verschwenden. Zu erfahren, dass ein solches Portal geschlossen wurde und die Hintermänner gesiebte Luft atmen, befriedigt mich natürlich.“



Für ihn als Verlagsautor ergeben sich bezüglich der Bekämpfung von Piraterie nicht die gleichen Probleme, wie für die Selbstpublisher, denn: „Nicht die Autoren bekämpfen die Piraterie, sondern die Verlage als Verwerter der Rechte. Fast jeder Verlag arbeitet heute mit auf derlei Vergehen spezialisierten Dienstleistern zusammen, die so eine Mischung aus Rechtsanwaltskanzlei und Cyber-Crime-Unit sind. Die suchen gezielt nach illegalen Kopien von Büchern, Hörbüchern usw., an de-

nen die beauftragenden Verlage Rechte haben, sorgen für Takedowns und unternehmen auch sonst so allerlei (Details erfährt man logischerweise keine). Die werden das Problem natürlich nicht endgültig lösen – aber es tauchen ja sicher immer wieder neue „Helden“ auf, die blöd genug sind, dafür zu sorgen, dass diese Leute gut im Geschäft bleiben“, teilt uns Herr Eschbach mit. Weiterhin äußerte er: „Für Selfpublisher kann ich nicht sprechen, da ich keine einschlägigen Erfahrungen habe und nicht weiß, welche juristischen Möglichkeiten man als solcher hat.“

Auf die Frage, ob auch die User von LuL.to mit juristischen Konsequenzen rechnen müssen meinte er: „Ich habe keine Ahnung, bin aber sehr gespannt.“

Gerne wäre Herr Eschbach auch bereit, noch zusätzliche Fragen, die sich aus den Kommentaren ergeben, zu beantworten: „Ich kann nichts versprechen, aber wir können es versuchen, vielleicht, falls sich in der Diskussion bei Ihnen bestimmte Fragen auftun, die man mir sinnvoll stellen könnte. Generell meine ich aber, dass ein Interview mit dem Justiziar eines Publikumsverlages der interessantere Stoff wäre.“

SCRIPTZBASE.ORG NACH DOMAINPROBLEMEN WIEDER ONLINE

ScriptzBase.org, das führende illegale Forum im deutschsprachigen Bereich für so genannte „Nulled Scripts“, ist wieder online. Über mehrere Tage hinweg war dort lediglich ein Warnhinweis der internationalen Domainvergabestelle ICANN zu sehen.

Kurz notiert: Eines der aktivsten Foren im deutschsprachigen Bereich zum Thema „Nulled Scripts“ ist seit einigen Stunden wieder online. Zuvor wurde schon gemunkelt, die Downtime könne etwas mit den Razzien der vergangenen Tage zu tun haben. Auch am heutigen Montag sollen im Laufe des Tages erneut Verdächtige des Darknet-Umschlagplatzes AlphaBay Besuch von der Polizei bekommen haben. So soll es Durchsuchungen in privaten Räumlichkeiten in Hamburg und Frankfurt am Main zuzüglich zu Beschlagnahmungen von Servern gegeben haben, die mit diesem Online-Drogenshop im Zusammenhang stehen. Wir werden erneut berichten, sobald es etwas Konkretes dazu gibt.

Doch zurück zu ScriptzBase.org. Administrator PyTh@n teilte uns heute mittels privater Nachricht mit, es habe schlichtweg etwas länger gedauert, bis er die überfällige Verlängerung der Domain in Angriff genommen habe. So sei es zur Fehlermeldung der ICANN gekommen. Das Forum, wo mitunter auch offensichtlich rechtswidrige Inhalte kostenlos angeboten werden, ist jetzt wieder im vollen Umfang nutzbar.

Was sind eigentlich Nulled Scripts?

Darunter versteht man kommerzielle Web-Skripte, deren Kopierschutz beziehungsweise die Kenntlichmachung mit einer Seriennummer o.ä. vor der illegalen Veröffentlichung entfernt wurden. Derartige Releases werden in der Szene auch als „Nullified Scripts“ bezeichnet. Der alles entscheidende Punkt beim Programmieren ist, dass man den Käufer der Skripte hinterher nicht mehr identifizieren kann. Auch geht es darum, die Funktionalität bei der Bearbeitung des Quellcodes nicht zu beeinträchtigen. In manchen Fällen ist dafür sehr viel technisches Wissen nötig. Das mag auch der Grund sein, warum hierzulande als auch im

englischsprachigen Raum die Szene für schwarzkopierte Scripts vergleichsweise klein ist. Angeboten werden bei Scriptzbase.org und vergleichbaren Foren übrigens auch Erweiterungen für WordPress und andere Content Management Systeme, die allerdings von den Herstellern kostenpflichtig angeboten werden.

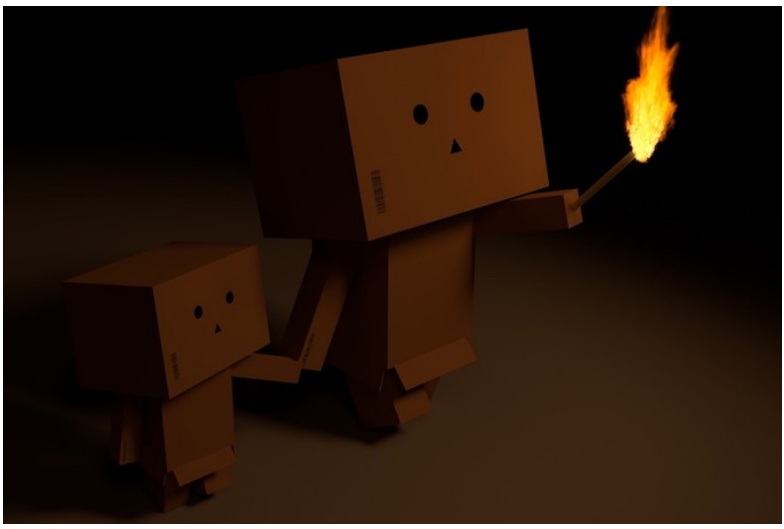
DARKNET: POLIZEI SPERRT DROGENHÄNDLER AUS

Einige Darknet-Drogenhändler verwendeten ein identisches Passwort gleich auf mehreren Darknet-Plattformen. Dadurch ist es der niederländische Polizei gelungen, diese Drogenhändler aus ihren Konten auszusperren, berichtet der Security-Blog BleepingComputer.

Bevor Hansa Market, die drittgrößte illegale Handelsplattform im Darknet, für immer vom Netz genommen wurde (20.07.2017), diente der Marktplatz der Polizei noch einen ganzen Monat als Honeypot, wobei der Code so verändert wurde, dass man in der Lage war, Passwörter mitzuschneiden. 10.000 Adressen ausländischer Hansa-Kunden seien dabei an Europol weitergegeben worden und werden nun für weitere Ermittlungen ausgewertet. So war es der niederländischen Polizei seit dem 20. Juni weiterhin möglich, die Kontendaten zahlreicher Drogenhändler herauszubekommen.

Die Ermittler verwendeten einfach die bei Hansa Market hinterlegten Zugangsdaten und loggten sich damit bei dem immer noch aktiven Konkurrenten „Dream Market“ ein, um die Händler dort auszusperren. Bei 14 Konten wurde so das Passwort bzw. der Zugangsschlüssel geändert. Einer der Anbieter bestätigte auf Reddit, dass er den Zugang zu seinem Dream Market-Konto verloren hatte, weil er die gleichen Passwörter sowohl auf Hansa Market, als auch auf Dream Market verwendete.

Weiterhin arbeiteten die Ermittler mit manipulierten Locktime-Dateien. Gewöhnlich dienen solche Dateien zum Speichern von Informationen über eine Markttransaktion eines Verkäufers, wie Details über das verkaufte Produkt, den Käufer, die Zeit des Verkaufs, den Preis sowie die Bestätigung (Unterschrift) durch den „Hansa Market“. Die Dateien werden als Authentifizierung von Anbietern verwendet, um die Freigabe von Bitcoin-Fonds nach dem Verkauf zu verlangen oder wenn der Markt aus technischen Gründen down ist. Die Behörden haben die Textdateien jedoch mit manipulierten Excel-Dateien ersetzt, in denen ein unsichtbares Bild versteckt wurde. Sobald die Datei geöffnet wird, wird das Bild geladen und die Behörden erfahren die IP-Adresse des Nutzers, die durch den Hansa-Server gespeichert wurde. Da diese Dateien vor allem als Beleg dienen, falls der „Hansa Market“ nicht erreichbar ist, dürften einige Nutzer aus Panik diese Dateien geöffnet und sich so offenbart haben.



OCCUPY DARKNET

Wie ihr noch heute eure eigene Seite im Darknet einrichtet. Es ist betrüblich, dass das Tor-Netzwerk oft mit kriminellen Aktivitäten in Verbindung gebracht wird. Damit gerät es völlig zu Unrecht in Verruf. Überlassen wir dieses wunderbare Netzwerk nicht länger den Spitzbuben. Bringt Licht ins Dunkle und hinterlasst eure eigene Visitenkarte im Darknet! So geht es.

Spätestens seit dem Tor-Browser-Bundle, welches ihr unter https://www.torproject.org/ bekommt, ist es sehr einfach geworden, das Netzwerk zu nutzen. Auch wir werden es hier verwenden. Nach dem Download entpackst du alles in ein Verzeichnis deiner Wahl, zum Beispiel: „Hidemyass“. Starte den Browser

und du kannst sofort mit dem anonymen Surfen beginnen. Neben den Seiten des World Wide Web wie: www.tarnkappe.info (Clearnet) steht dir nun auch das sogenannte Darknet zur Verfügung. Wenn du Tor installiert hast, kannst du diese Testseite http://ohj2k3x3lizwm7ur.onion/ aufrufen. Eine Suchmaschine für das Darknet ist zum Beispiel AHMIA unter msydqstlz2kzerdg.onion.

So weit, so gut. Aber wir wollen ja unsere eigene Seite, vielleicht eine private Homepage oder einen Blog im Darknet aufsetzen.

Dein Browser-Bundle ermöglicht dir nicht nur den Zugriff auf eine neue Welt, sondern du kannst auch Teil dieser neuen Welt sein, indem du selbst einen „Hidden-Service“ anbietest. Torseiten benötigen keine IP-Adressen. So kannst du problemlos hinter deiner Firewall agieren. Bevor wir beginnen, musst du sicherstellen, dass Tor richtig eingerichtet ist und richtig läuft.

Für den Inhalt bist du selbst verantwortlich. Das Gerüst, welches du dann später mit Fleisch bepacken kannst, ist in unserem Fall „Jekyll“: https://jekyllrb.com/. Es ist in jedem Fall eine nähere Betrachtung wert. Schon nach kurzem Einlesen kannst du hier starten. Du solltest dich aber eingehend mit den sehr gut gemachten Erläuterungen befassen, damit keine Anfängerfehler deine Freude trüben (RTFM!).

Wie du an dem „rb“ im Seitennamen erkennst, steckt neben etwas Schweiß und Ruby-Code in Jekyll. Installiere erst Ruby und dann Jekyll aus den Ruby-Gems. Alles ist für die meisten Betriebssysteme verfügbar. Windows hat einen Installer: https://rubyinstaller.org/ , auf den meisten Linux-Kisten ist es schon drauf, du kannst es mit: „ruby –version“ testen oder mit „su (sudo) apt install ruby“ nachinstallieren, und auch für Mac‘s gibt es da sicher irgendwas von Ratiopharm.

Unter Ubuntu zum Beispiel holst du dir Jekyll mit: >>gem install jekyll bundler<<. Öffne dazu ein Root-Terminal. So baut Jekyll deine Seite: >>jekyll new meinedarknetseite<<. Wechsel in das Seitenverzeichnis erfolgt mit: >>cd meinedarknetseite<<. Cool: Jekyll bringt seinen eigenen Server gleich mit und durch die Eingabe: >>bundle exec jekyll serve<< ist deine Seite unter: http://localhost:4000 in einem Standard-Browser erreichbar. Probiere es gleich aus. Das Grundgerüst deiner Seite ist fertig und die kannst es jetzt mit viel Inhalt, CSS, HTML, Markdown und was auch immer behängen. Den Server stoppst du bei Bedarf mit Str c (Ctrl c).

Weiter mit Tor.

So konfigurierst du den „Hidden-Service“: Öffne die >>torrc<< mit einem Editor deiner Wahl. Du findest die Datei hier: Browser/TorBrowser/Data/Tor/torrc , in deinem Tor-Bundle-Browser-Verzeichnis. Schreibe folgende Zeilen in deine torrc: HiddenServiceDir /Library/Tor/var/lib/tor/hidden_service/ HiddenServicePort 80 127.0.0.1:4000 Ok. Jetzt speicherst du die Datei und startest dein Tor-Browser-Bundle neu. Wenn Tor neu startet, ist alles gut. Wenn nicht, bekommst du eine Fehlermeldung, die dir eventuell weiter hilft. Meist handelt es sich um einen Schreibfehler in der eben erstellten torrc. Prüfe noch einmal alles durch. Wenn Tor startet, erstellt es dir automatisch zwei Dateien: private_key und hostname in das von dir zuvor angegebene Verzeichnis, hier ist es: hidden_service. private_key Teile den hier enthaltenen Schlüssel mit niemanden! Er ist nur für dich gedacht.

hostname

Die zweite Datei die Tor erzeugt hat heißt: hostname. Sie enthält etwas das zum Beispiel so aussieht: ohj2k3x3lizwm7ur.onion/ (hier nur ein Beispiel) In deiner eigenen Datei findest du nun also den öffentlichen Namen für deine offizielle Darknet-Seite. Du kannst sie mit anderen teilen, oder auf deine Visitenkarte drucken. Das ist alles. Willkommen im Darknet! Denke daran, damit alles funktioniert, muss sowohl der Jekyll-Server laufen >>jekyll serve<< als auch das Tor-Browser-Bundle.

Keine Panik, wenn dein „Hidden-Service“ nicht gleich erreichbar ist. Er braucht ein bisschen Zeit. Lade deine Onion-Adresse einfach gleich nochmal nach.

Hinweis: Dies ist nur ein Beispiel von vielen, um eine Seite im Darknet einzurichten. Ich übernehme keine Garantie dafür, dass ihr wirklich „hidden“ seid. Die Auswahl und das „Abhärten“ eines Servers ist eine komplizierte Sache. Am besten ihr lasst euch von einem guten Freund dabei helfen.

Wir sehen uns (im Darknet) !

TATA.TO OFFLINE, WECHSELT ZU CLOUD-FLARE

Die Streaming-Webseite tata.to befindet sich im Umbau. Derzeit ist dort bis auf die Mitteilung über den Umzug der Daten zu neuen Servern nichts zu sehen. Im Hintergrund hat sich aber zwischenzeitlich schon einiges geändert, die Betreiber wechselten von Google Drive zu Cloudflare als Streaming-Hoster, um der dritten Löschung aller hochgeladenen Werke zuvorzukommen. Die Sache hat allerdings einen Haken.

In einschlägigen Foren wurde im Vormonat behauptet, dass tata.to über mehrere Tage hinweg offline war, weil man zu einem neuen Anbieter wechseln musste. Tatsache ist, dass Google Drive für Streaming-Webseiten als Online-Speichermedium zwar preiswert ist. Dafür löscht Google auf Verlangen der Rechteinhaber mittlerweile vergleichsweise zügig die dort hochgeladenen Kinofilme und TV-Serien. In der Folge mussten sich der bzw. die Betreiber jeweils eine neue Fake-Identität zulegen, einen neuen Account bei Google Drive anmelden, alle Filme neu hochladen, die Verknüpfungen auf der eigenen Webseite anpassen, die Nutzer beruhigen und hoffen, dass das ganze Spiel nicht wieder von Neuem losgeht.

Doch genau das ist schon mehrfach passiert. Bevor es zu einem dritten Re-Upload gekommen wäre, erfolgte der Wechsel zum US-amerikanischen Dienstleister Cloudflare. Übrigens: Auch das illegale Hörbuch- und E-Book-Portal Lesen & Lauschen (LuL.to) beauftragte Cloudflare mit der Übertragung der Daten von ihren Servern zu den LuL-Kunden. Das sorgte dafür, dass man den tatsächlichen Standort der LuL.to-Server zwar nicht von außen ausmachen konnte. Dafür lässt sich Cloudflare aber fürstlich bezahlen. In Anbetracht der gigantischen Datenmengen müssen Streaming-Portale im Gegensatz zu illegalen Verbreitern von E-Books, die winzig im Vergleich sind, mit monatlichen Kosten von bis zu 300 Euro rechnen.

Die Frage wird aber sein, wie man derart hohe Kosten wieder reinholen will!? Die üblichen Verdächtigen, Online-Vermarkter wie OnClick, Propeller Ads Media etc. zahlen selbst Webmastern gut genutzer Seiten keine Unsummen. Dabei sind die monatlichen page impressions (Seitenzugriffe) bei tata nach den wiederholt gelöschten Streams ziemlich in den Keller gegangen. Die letzten Löschungen in Verbindung mit dem Sommerloch (Urlaubszeit etc.) kosteten die Betreiber rund 600.000 Zugriffe im Monat (siehe Grafik unten). Die Filme wie früher auf hauseigenen Servern unterzubringen, kam für tata.to auch nicht mehr infrage, wahrscheinlich wegen der entstandenen Kosten.

Vavoo bedient sich einfach bei tata.to

Die anonymen Macher der Bundle-URL vavoo.to bedienen sich derweil dreist beim Wettbewerb. Untersuchungen vor etwa drei Wochen ergaben, dass man einfach die Streams des Pay-TV-Senders Sky angezapft hat, die tata.to ausstrahlte, um diese den Nutzern der Software und der bald verfügbaren Set-Top-Box Vavoo kostenlos anzuzeigen. Natürlich nur, sobald man als Bundle-URL vavoo.to eingegeben hat. Wer stattdessen bei den Einstellungen die legale Variante vavoo.tv/repo eingibt, erhält selbstredend nur legale Quellen, die man sich darüber anschauen kann.

SKRIPTE VON "GAME OF THRONES" ERBEUTET: HACKER ERPRESSEN PAY-TV-SENDER HBO

Hacker, mit dem Namen ‚Mr. Smith', haben Server des US-Senders HBO geknackt und 1,5 Terabyte an Daten gestohlen. Mit einer Lösegeldforderung erpressen sie nun HBO und drohen damit, das erbeutete Material, darunter Filme, Serien, unveröffentlichte Manuskripte und persönliche Daten, zu veröffentlichen.

Unter dem geraubten Material sollen sich neben internen Dokumenten und persönlichen Daten auch eine Zusammenfassung des Skripts für die kommende fünfte Folge der aktuellen Staffel von „Game of Thrones“ sowie E-Mails einer Führungskraft des Bezahlsenders befinden. Zudem wären die Serien „Ballers“ und „Room 104“ vom Hack betroffen.

Die Dokumente seien online zugänglich gemacht und zugleich an mehrere Medien geschickt worden, berichtet The Hollywood Reporter. Die Hacker verlangen von HBO ein nicht näher beziffertes Lösegeld. Falls kein Geld fließt, wollen sie weiteres Material öffentlich ins Netz stellen: In einem an HBO-Chef Richard Plepler adressierten Videobotschaft forderten sie eine hohe Geldsumme, die in der öffentlichen Version unkenntlich gemacht wurde. In dieser Nachricht geben die Hacker weiterhin bekannt, dass HBO eines ihrer „schwierigeren Ziele“ war und dass sie etwa 6 Monate gebraucht haben, um ins Firmen-Netzwerk einzudringen. HBO wäre bereits ihr 17. Ziel und nur drei hätten bisher nicht gezahlt.

Wie Entertainment Weekly informiert, teil HBO CEO Richard Plepler in einer internen Mail seinen Mitarbeitern mit, dass sie sowohl mit Strafverfolgungsbehörden als auch mit Cybersicherheitsfirmen daran arbeiten, den Vorfall zu untersuchen, auch um den Schaden einzuschätzen und einzudämmen. Eine forensische Untersuchung sei im Gange und eine bisherige Überprüfung hätte nichts ergeben, das darauf hindeuten könnte, dass das E-Mail-System als Ganzes kompromittiert wurde.

Am Sonntag schickten die Hacker eine anonyme E-Mail an viele Reporter, worin der Hack angekündigt wurde: „Hallo an alle. Der größte Leak des Zeitalters des Cyberspace passiert gerade. Wie heißt er? Oh, das hatte ich vergessen zu sagen. HBO und Game of Thrones……!!!!!! Ihr habt das Glück, die ersten zu sein, die den Leak herunterladen können. Genießt es und verbreitet die Nachricht. Wer am besten berichtet, bekommt ein Interview mit uns. HBO fällt.“, schrieben sie darin.

Trotz ihrer Lösegeldforderung behaupten die Hacker gemäß einem Artikel von Wired, dass sie „White Hats“ und keine Kriminellen seien: „Es ist ein Spiel für uns. Geld ist nicht unser Hauptzweck“. Sie wollen nur einen „klitzekleinen Teil“ des großen Einkommens des Senders für sich.

HBO kämpft seit Jahren damit, Handlungen neuer Folgen geheim zu halten und deren illegale Verbreitung zu verhindern. Bereits die ersten vier Episoden von “Game of Thrones” der fünfte Staffel wurden kurz vor der Premiere im Jahr 2015 veröffentlicht, nachdem DVDs für Rezensionen an die Presse und Branchen-Insider verschickt worden waren. Das mehrfach ausgezeichnete Fantasy-Drama war Mitte Juli in den USA in die siebte Staffel gestartet.

DEF CON: TOR-MITGRÜNDER ROGER DINGLEDINE MEINT: „ES GIBT KEIN DARK WEB“

US-amerikanischer Co-Entwickler und Projektleiter des Tor-Netzwerks, Roger Dingledine, kritisiert auf der Def Con die negative Außendarstellung des Anonymisierungs-Netzwerks. Er meint, das Netzwerk würde zu Unrecht oft nur mit illegalen Aktivitäten in Verbindung gebracht. Tatsächlich spiele es statistisch gesehen keine Rolle, denn der Anteil der Hidden Services wäre nur sehr gering: „Es gibt grundsätzlich kein Dark Web. Es existiert nicht. Es sind nur sehr wenige Webseiten.“, berichtet The Register.

In jüngster Zeit machten vor allem durch die Existenz und Schließung von illegalen Handelsplattformen, wie Silk Road, AlphaBay, Hansa Market und Co., auf denen oft verbotene Güter die Besitzer wechselten, negative Schlagzeilen die Runde. Betrieben wurden diese über die „Tor Hidden Services“, bekannt für ihre „.onion“-Domains. Tor-Mitgründer Roger Dingledine sieht Tor jedoch zu Unrecht negativ abgestempelt.

Rund zwei Millionen Menschen nutzen das kostenlose Anonymisierungs-Netzwerk „Tor“ täglich, um ihre Privatsphäre zu schützen. Roger Dingledine kam es auf der Def Con in in Las Vegas, der größten Veranstaltungen für Hacker weltweit, darauf an, Irrtümer um das Tor-Netzwerk aufzuklären. Er sieht den Anonymisierungsdienst zu Unrecht als Hilfsmittel krimineller Machenschaften dargestellt und lieferte auf der Def Con Zahlen (PDF). In seinem Vortrag betont Dingledine, dass das Tor-Netzwerk

eben nicht, wie viele Menschen annehmen, primär von Drogendealern und Pädophilen verwendet wird, um sich vor den Behörden zu verstecken. Tatsächlich betrage der gesamte Traffic aller Hidden Services insgesamt nur drei Prozent vom Gesamttraffic. Die Skala des dunklen Netzes – mit seinen Drogengeschäften, Waffenverkäufen und Kindesmissbrauch – ist unbedeutend, wenn man es in einem größeren Rahmen betrachtet, argumentiert er. Zudem wäre es auch als kurzfristig genutztes Kommunikationsmittel für Terroristen viel zu aufwändig, Tor-Nodes einzurichten. Diese hätten einfachere Möglichkeiten zur Verfügung.

Das deutet darauf hin, dass die überwiegende Mehrheit der Leute das Tornetzwerk verwenden, um unerkannt öffentliche Webseiten für völlig legitime Zwecke zu durchsuchen und so ihre Identität vor Website-Besitzern zu maskieren. Genutzt würde es somit, um anonym und unbehelligt durch Zensoren, andere staatliche Stellen oder die Werbeindustrie, auf ganz normale Webseiten zuzugreifen. Bewohner von Staaten, wie dem Iran, hingegen sind auf die Anonymisierungsdienste von Tor angewiesen, um überhaupt ohne Zensur surfen und kommunizieren zu können. Für sie ist es eine Rettungsleine, die einzige Möglichkeit, sicher auf die Online-Dienste zuzugreifen.

Wenngleich es natürlich dubiose Plattformen gibt, existieren auch reguläre Services, die über den Tor-Dienst einen zusätzlich gesicherten Zugang ermöglichen. Ein legaler Dienst ist sogar ganz vorne in der Statistik: Der am stärksten frequentierte Onion Service wäre die Tor-Version von Facebook. Facebook betreibt seit dem Jahr 2014 einen eigenen Hidden Service als Portal zu seinem sozialen Netzwerk, um den Zugriff auf den Dienst in Ländern mit Internetzensur zuzulassen. Nach Facebooks eigenen Angaben nutzten bereits vor einem Jahr eine Million Menschen den Dienst monatlich.

Zudem widersprach Dingledine Annahmen, wonach Geheimdienste das Netzwerk einfach unterwandern könnten, indem sie eigene Tor-Nodes betreiben. Zwar hätten die Snowden-Dokumente belegt, dass Geheimdienste einen Teil der Relays betrieben – aber nicht genug, um Tor aushebeln zu können. Dingledine gibt an, rund zwei Drittel der Personen persönlich zu kennen, die die insgesamt 8000 Relays betreiben und könne daher ausschließen, dass Strafverfolger und Geheimdienste die Tor-Infrastruktur unterwandert haben.

MICROSOFT STORE: QUELLE EINER GROSSEN ANZAHL ILLEGALER STREAMING-APPS

Im Store von Microsoft lassen sich zahlreiche Apps finden, die ohne jeglichen Aufwand per Streaming Zugang zu urheberrechtlich geschützten Inhalten ermöglichen. Wie TorrentFreak berichtet, sind dort illegale Streaming-Apps sowohl für Filme und Serien, als auch für Musik verfügbar.

In den letzten Jahren ist die Streamingpiraterie zu einem beliebten Zeitvertreib für viele Menschen geworden und kam zuletzt im Zusammenhang mit vollständig vorkonfigurierten Kodi-Set-Top-Boxen in die Schlagzeilen. So hat in den vergangenen Monaten Hollywood viele seiner Anti-Piraterie-Bemühungen auf nicht autorisierte Kodi-Add-ons und mehrere beliebte Piraten-Streaming-Seiten gerichtet, die Filme und TV-Shows ohne Erlaubnis anbieten. Jedoch bisher völlig unbeachtet blieb der Windows App Store, zu dem Millionen Menschen Zugang haben.

Legaler Streaming Service, wie Netflix und Amazon, boomen. Zugleich gibt es aber auch einen dunklen Markt von Tausenden von Piraten-Streaming-Tools. Jedoch muss man offenbar keine illegalen Plattformen im Internet ansteuern, um illegale Piratenangebote aufzuspüren, denn bereits im „vertrauenswürdigen“ Microsoft App-Store wird man fündig. Zwar wirbt Microsoft damit, über den hauseigenen App Store ein sorgfältig ausgewähltes und vor allem sicheres Angebot an Apps bereitzustellen, jedoch hat TorrentFreak herausgefunden, dass eben auch illegale Inhalte über den Store verbreitet werden.

Genauso überraschend ist die Tatsache, dass viele der Programme anscheinend bereits seit längerem im Store verfügbar sind.

So genügte im amerikanischen Windows Store bereits eine Sucheingabe, um „Free Movies"-Apps zu finden, die unter anderem mit dem kostenlosen Streaming von aktuellen Hollywood-Blockbustern werben, darunter „Wonder Woman", „Spider-Man: Homecoming" oder „Die Mumie". Die gleichen Programme sind auch im deutschsprachigen Raum zu finden. Laut Torrentfreak handelt es sich hierbei um keine Einzelfälle, sondern es gibt dutzende Anwendungen dieser Art. Die Apps lassen sich auf Mobilgeräten, Windows-Computern und teils sogar auf der Xbox nutzen. Die betreffenden Apps machen aus ihren illegalen Inhalten auch kaum einen Hehl, als Einnahmequelle setzen die Entwickler entweder auf Werbeschaltungen oder sogar auf Abo-Modelle. Zudem werden Werbeanzeigen innerhalb der Applikationen über die Microsoft Ad Monetarization Platform geschaltet – dem offiziellen Software Development Kit für Werbeanzeigen.

Bezüglich der illegalen Inhalte hat TorrentFreak Microsoft kontaktiert. Die Antwort vom Unternehmen: „Wenn Besitzer von geistigem Eigentum eine App in unserem Store finden, die ihrer Meinung nach ihre Rechte verletzt, können sie eine Beschwerde über die Microsoft Handelsmarken- und Urheberrechtsseite einreichen. Darüber hinaus möchten wir Kunden dazu aufrufen, uns Probleme mit dem Windows Store zu melden. Für die meisten Probleme können Kunden den „Report Concern to Microsoft" Link im Windows Store verwenden", sagte ein Microsoft-Sprecher.

WATCHHD.TO WURDE GEHACKT

Seit Ende August wird von Hacker Akiko die komplette Datenbank des illegalen Bezahl-Streaming-Portals WATCHHD.TO (ehemals WatchHD.biz) zum Kauf angeboten. Allerdings wurde seine Offerte mit Ausnahme von Scriptzbase.org überall sofort wieder von den Foren entfernt.

Der neue User Akiko hat sich offenbar eigens dafür am gleichen Tag bei Scriptzbase.org, mygully.com und der Szenebox registriert, um sein Angebot zu veröffentlichen. Er bietet die Übermittlung aller Daten von WATCHHD.TO an, «Stand 28.08.2017 vollständig mit Script, Cronjobs, Datenbank und allen Nutzern mit Anleitung für die Installation«. Dem Angebot des Leaks für 200 US-Dollar in Form von Bitcoin wurden einige Screenshots beigefügt.

Sein Problem ist nur, dass man sein Posting sofort wieder bei mygully.com und vom Werbethread der Szenebox entfernt hat. Dort wurde auch von manchen Diskussionsteilnehmern geäußert, dass sie glauben, dass der Käufer die Passwörter binnen kürzester Zeit entschlüsseln könne. Die Abonnenten hätten dann im Fall einer Weitergabe der Nutzerdaten beispielsweise an Sky Deutschland mit ähnlichen zivil- und strafrechtlichen Problemen zu rechnen, wie die von LuL.to. Wer sich von den früheren WatchHD-Premium-Usern ausreichend gegen eine Aufdeckung geschützt hat, weiß niemand, außer den Personen selbst. Man würde ihnen im schlimmsten denkbaren Fall vorwerfen, dass sie kostenpflichtige Streams kommerzieller Anbieter sehr günstig, weil illegal, erworben haben.

Von den Betreibern von WATCHHD.TO (ehemals WatchHD.biz) erfolgte gestern Abend folgendes Statement in der Szenebox:

Durch eine Lücke im System konnte ein Angreifer Zugriff auf unser System erlangen und somit einen Auszug der Datenbank anfertigen. Die Passwörter in der DB sind verschlüsselt, allerdings wurde eine Login-Datei so modifiziert sodass Username + PW + IP Adresse in eine Datei gespeichert wurden. (deswegen der kleine Auszug mit den IP-Adressen)

Wir bedauern es sehr dass es dazu kommen musste, ich bin aber auch etwas enttäuscht darüber wie sich die deutsche Szene selbst zerstören möchte. Wir wurden erpresst mit 5000$. Selbst wenn wir die gezahlt hätten, dann wäre die DB im Umlauf. Wir können das leider nicht verhindern, dass es solche Menschen gibt. Statt sich zu helfen wird alles daran gesetzt sich selbst kaputt zu machen bzw. die deutsche Szene.

Da es nicht illegal ist sich bei uns anzumelden, dürftet ihr auch nichts befürchten. Es gibt keine Logs oder Sonstiges

wo ersichtlich ist, das ihr überhaupt Streams geschaut habt.

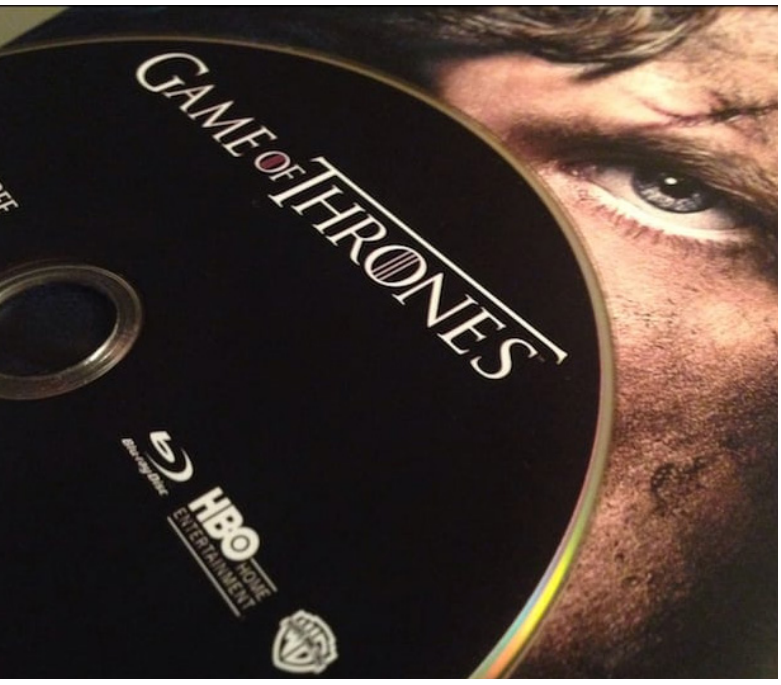
Es tut uns wie gesagt sehr Leid, dass es so gekommen ist, wie es ist. Wir haben die Seite offline genommen um im Hintergrund alles Weitere zu klären und zu beheben.

Eure Passwörter könnt ihr jederzeit im Forum ändern. Die Passwörter für die Lines können wir auch jederzeit ändern, wenn es gewünscht ist.

Wann unsere Hauptseite wieder online kommt, kann ich nach jetzigen Stand noch nicht sagen, da privat viel ansteht.

Wie umfangreich der Hack tatsächlich ist, bleibt also vorerst abzuwarten. Fakt ist, dass derzeit nur das Forum von WatchHD nutzbar ist. Von jeglichen moralischen Aspekten und der destruktiven Wirkung des „Angebots" des Hackers einmal ganz abgesehen. Wir haben in der Zwischenzeit sowohl die Betreiber als auch Akiko per PN und E-Mail angeschrieben und warten auf eine Reaktion.

Wem die Webseite WatchHD.to noch gar nichts sagen sollte, wir haben vor einiger Zeit mal ein Community-Interview mit den Betreibern durchgeführt.



GAME OF THRONES: AUSSTRAHLUNG BRICHT ALLE REKORDE – ABER NICHT NUR LEGALE ANGEBOTE WERDEN GENUTZT

Der Hype um Game of Thrones ist ungebrochen. Die neueste und vorletzte Staffel 7 von Game of Thrones startete am 16. Juli und spielte einen Rekord für den US-Sender HBO ein. Über alle Plattformen des Senders hinweg sahen in den ersten Tagen 16,1 Millionen Menschen die erste Episode. Das sind 50 Prozent mehr als bei der Premiere von Staffel 6, berichtet das Portal Entertainment Weekly.

Seit dem 17. Juli läuft die 7. Staffel der Fantasy-Serie Game of Thrones hierzulande unter anderem auf Sky und bereits kurz nach Ausstrahlung verkündete der Pay-TV-Anbieter den großen Erfolg der neuen Folgen, unter anderem mit 470.000 Live-Zuschauern und der damit stärksten Erstausstrahlung in der Serienhistorie. Weitere 210.000 Serienfans sahen die Wiederholungen am Abend und allein die erste Folge verzeichnete in der ersten Woche 1,09 Millionen Abrufe.

Allerdings verlief der Start der Serie nicht ganz störungsfrei in Deutschland. Sky war vom Ansturm überlastet, die Fans klagten über Probleme bei der Registrierung. „Der Winter ist da … und hat ein paar Leitungen vereist", räumte Sky Ticket daraufhin bei Facebook ein. Doch auch in Australien kam es bei der Ausstrahlung immer wieder zu technischen Aussetzern – wohl wegen der hohen Nachfrage nach der Fantasyserie. „Wir sind betroffen, dass einige Fans technische Störungen hatten", sagte ein Foxtel-Sprecher. Die Premiere habe auf der ganzen Welt zu Abstürzen von Webseiten geführt, auch in den USA und in Lateinamerika, so der Fernsehsender.

Laut den Marktanalysten von MUSO war die Zahl der Zuschauer, die sich das Werk über nicht genehmigte Anbieter angeschaut haben, aber noch deutlich höher, berichtete Torrentfreak, wobei die Daten von über 200 Millionen Geräten gesammelt werden, die sich in mehr als 200 Ländern befinden. So sollen sich die erste Folge der siebten Staffel der Serie Game of Thronesv"Dragonstone", 90 Millionen Zuschauer auf diesem Weg angesehen haben. 77,9 Millionen Mal wurde Dragonstone demnach gestreamt, 8,3 Millionen Mal wurde die Folge über öffentliche Torrent-Tracker bezogen, 4,9 Millionen Mal über diverse Downloadplattformen und 500.000 Mal über private Torrent-Tracker. 15,1 Millionen solcher Zugriffe gab es damit aus den USA, 6,2 Millionen aus Großbritannien und 4,9 Millionen in Deutschland. Andy Chatterley, CEO von MUSO und Mitbegründer, stellte fest, dass die ermittelten Ergebnisse für einige Branchen-Insider eine Überraschung sein könnten. „Es wäre nicht zu leugnen, dass diese Zahlen riesig sind.", meinte er.

Bereits 10 Tage nach dem Erscheinen der neuen GoT-Staffel soll laut einer Untersuchung der Internetforensiker von FDS

File Defense Service ein umfangreiches Angebot an illegalen Versionen der beiden ersten Episoden auf einschlägigen Piratenportalen für Deutschland mit insgesamt 540 verschiedenen Einträgen bereit gestanden haben, wovon 431 zu einem Downloadangebot verlinkten und 109 zu einem Streamingangebot. Im Vergleich zum Angebot der 6. Staffel würde sich die gewachsene Popularität des Streamings zeigen, das seinen Anteil am Angebot mit 20,2% mehr als verdoppelte. Wie oft allerdings die bereitstehenden Angebote genutzt worden sind, das wissen allein die Betreiber der illegalen Plattformen.

Allerdings geht nun HBO gegen die illegalen Raubkopierer vor. Wie Torrentfreak berichtet, versandte IP Echelon, der Anti-Piraterie-Partner von HBO, Warnungen, die gerichtet sind an Torrentuser. Die ISPs werden angewiesen, ihre Abonnenten zu warnen, um weitere Verstöße zu verhindern. Nach US-Urheberrechtsgesetz sind ISPs nicht verpflichtet, diese E-Mails weiterzuleiten. Allerdings tun es die meisten doch, aus Höflichkeit gegenüber dem betroffenen Rechteinhaber. HBO weist in dem Schreiben darauf hin, dass der Torrent-Download von Game of Thrones eine Urheberrechtsverletzung darstelle und damit illegal sei. Zudem fordert die Mail dazu auf, ein legales Abonnement abzuschließen. Außerdem in der E-Mail enthalten: Die IP-Adresse, die zum Herunterladen der Datei benutzt wurde, die jedoch noch keinen Rückschluss auf den tatsächlichen Nutzer zulässt. Dafür müsste HBO den User anzeigen und das wäre ziemlich unwahrscheinlich, zumindest ist das bislang noch nie der Fall gewesen. Realistischer wäre, dass HBO weiterhin E-Mails verschickt und auf einen moralischen Wandel hofft.

Unglücklich ist daher, dass die illegalen Streams bestens funktionierten, während einige offizielle Streaming-Server Probleme bei der Game of Thrones Premiere durch die hohen Zugriffszahlen hatten. Eine stabile Infrastruktur würde sich natürlich positiv auf potentielle Abonnenten auswirken.

GELDFÄLSCHER BEANSTANDET ERMITTLUNGSRESULTATE DER POLIZEI

In einem Verfahren gegen zwei Männer im Alter von 23 und 24 Jahren aus dem niedersächsischen Lingen, die gefälschte 50-Euro-Geldscheine hergestellt und in Umlauf gebracht haben sollen und zudem unter Verdacht stehen, mit Betäubungsmitteln gehandelt zu haben, wurde im Prozessverlauf die polizeiliche Auswertung eines Mobiltelefons angeordnet. Ein Angeklagter unterstellte jedoch den Behörden, dass das für ihn belastende Material erst nach seiner Festnahme von der Polizei darauf abgespeichert worden sei, berichtet die Osnabrücker Zeitung.

Zwischen August 2015 und August 2016 sollen zwei Männer in einer Fälscherwerkstatt bei Schüttorf mindestens 7200 gefälschte 50-Euro-Scheine hergestellt und über das Internet unter dem Namen HQCNS (High Quality Counterfeit Notes Store) in Deutschland und dem europäischen Ausland veräußert haben. Im Forum warben sie mit dem Motto: „Take me to paradise“ für ihr Produkt. Laut einem dort gepostetem Kommentar soll es sich dabei um „die besten nachgemachten Scheine, die man online kaufen könne“, gehandelt haben.

Zudem soll zumindest einer der Angeschuldigten seit Mitte 2016 auf dem Dachboden der Werkstatt eine Marihuana-Plantage mit über 170 Pflanzen betrieben haben. Die Anklageschrift ist das Ergebnis von Ermittlungen der „Task Force“ Cybercrime, der Zentralen Kriminalinspektion Osnabrück, und der Polizeiinspektion Emsland/Grafschaft Bentheim. Seit August 2016 befinden sich die Angeklagten in Untersuchungshaft.

Während die Angeklagten beim Prozess die ihnen von der Staatsanwaltschaft zur Last gelegten Vorwürfe bezüglich des Falschgeldes im Wesentlichen eingestanden haben, blieben hinsichtlich des Betreibens der gleichfalls vorgefundenen Drogenplantage noch Fragen offen. Zwar hatte der Angeklagte A angegeben, von der Plantage gewusst zu haben, den Raum jedoch an eine andere Person vermietet zu haben und ansonsten bestritt er, in die Sache involviert gewesen zu sein. Mit ähnlichen Argumenten gelang es dem Angeklagten B sogar, die Staatsanwaltschaft von seiner Unschuld zu überzeugen.

Folglich mussten Beweise gefunden werden, um den Verdacht gegen A bestätigen zu können. Aufschluss darüber sollte eine

Auswertung von Daten mehrerer Mobiltelefone des Angeklagten A liefern. Jedoch war eines der Telefone gegen den Zugriff unbefugter Dritter gesichert. Der Angeklagte gab sein Passwort nicht preis, die Anklage entschied sich nun, eine Spezialfirma aus Israel damit zu beauftragen, das Handy zu entsperren.

In einem am 24.08.2017 vor dem Landgericht Osnabrück vermittelten Bericht über die polizeiliche Auswertung des Mobiltelefons ließen überdies Zweifel aufkommen an der Aussage des Angeklagten B, nichts mit den Drogen zu tun zu haben. Der Angeklagte A zweifelte jedoch seinerseits diese Ergebnisse an, die einen tatsächlichen Einblick gaben in wirklich jede Aktion, die auf dem Telefon jemals stattgefunden hat. Sowohl Anrufe, als auch Fotos, E-Mails und Notizen — alles ist nachvollziehbar, einschließlich Kommunikationspartner, Telefonnummern und der genauen Position. A ist vielmehr der Meinung, dass die Polizei das belastende Material erst nach seiner Festnahme auf seinem Mobiltelefon abgespeichert habe. Diesem Vorwurf wird die Staatsanwaltschaft nun zeitnahe nachgehen.

HACKER LOCKEN GAME OF THRONES-FANS MIT E-MAIL IN VIRENFALLE

Wie die „The Verge“ berichtet, sind aktuell E-Mails in Umlauf, die pikante Details zur Hit-Serie Game of Thrones versprechen. Chinesische Hacker setzen auch hier auf die Neugierde der Empfänger, das anstehende und sehnsüchtig erwartete Finale im Voraus sehen zu wollen. So versprechen sie, die ausstehenden letzten Folgen vorab zu zeigen. Wer jedoch auf den im Anhang der verschickten Datei enthaltenen Link klickt, den erwarten nicht etwa die versprochenen letzten Folgen der Serie – sondern Viren.

Den Sicherheitsforschern von Proofpoint sind bereits seit dem 10. August diese E-Mail-Nachrichten bekannt, die mit dem Titel „Wanna see the Game of Thrones in advance?“ (Willst du Game of Thrones schon vorher sehen) verschickt werden. Dem Nutzer werden darin die Episoden 5 bis 7 für je 10, 20 oder 30 US-Dollar pro Stück angeboten. In dem, im Anhang enthaltenen Word-File, befindet sich eine angekündigte Vorschau auf die Folgen. Klickt der Empfänger auf den darin enthaltenen Link, wird der Trojaner unbemerkt installiert.

Die IT-Sicherheitsfirma Proofpoint hat die Kampagne im Detail analysiert und herausgefunden, dass es sich bei dem Trojaner um den „9002“ getauften Fernzugriffs-Trojaner (Remote Access Trojan, RAT), handelt. Die im Bild gezeigte E-Mail enthält einen Microsoft Word-Anhang mit dem Namen „game of thrones preview.docx“. Einmal angeklickt entpuppt sich die „Vorschau auf die künftigen Folgen“ als ein eingebettetes .LNK (ein OLE Packager Shell-Objekt), das beim Ausführen ein bösartiges PowerShell-Skript ausführt, das zur Installation des diskless „9002“ RAT führt, der einen Zugriff von außerhalb auf den heimischen Computer ermöglicht.

Da es bereits ganz ähnliche Angriffe in der Vergangenheit gab, hat Proofpoint die Hacker-Gruppe Deputy Dog, auch bekannt als APT17, unter Verdacht. Es soll sich hierbei um Hacker handeln, die mit der chinesischen Regierung in Verbindung stehen und vom chinesischen Staat unterstützt würden. Sie versuchen immer wieder mit dementsprechenden Methoden, Zugriff auf andere Systeme zu erlangen. Mit dem verlockenden Angebot gerade populärer Titel, wird Schadsoftware zur Infiltration bereit gehalten. In der Vergangenheit wurden Spiele, wie Pokémon Go und Super Mario Run für diese Zwecke genutzt.

Man wird jedoch mit der „Game of Thrones“-Ankündigung ohnedies nur wenige Leute überzeugen können: die fünfte und sechste Folge wurde bereits ausgestrahlt, die siebte und finale Episode folgt am Sonntag. Allerdings haben die Hacker, die den US-Sender HBO mit gestohlenen Daten erpressten, bereits das Ende der siebten Staffel veröffentlicht, berichtete Mashable. Dass es sich bei den Verschickern der infizierten E-Mails um dieselben Hacker handelt, die für die HBO-Leaks verantwortlich waren, gilt jedoch als unwahrscheinlich.

UMFRAGE: FAST DIE HÄLFTE DER BRITISCHEN FUSSBALLFANS NUTZEN ILLEGALE STREAMINGANGEBOTE

Im Auftrag der BBC wurde eine neue Umfrage initialisiert. So befragte ComRes, ein Marktforschungsinsti-

tut mit Sitz in London, für BBC 5 Live 1.000 erwachsene Fans, die regelmäßig Premier League anschauen, online zwischen dem 7. und 15. März, berichtet TorrentFreak.

In England ist es für Fußballfans völlig normal, dass sie für Live-Übertragungen bezahlen müssen, denn gerade dieser Markt hat massiv auf Bezahlübertragungen gesetzt. Im Schnitt zahlen Briten im Jahr 500 Pfund, wenn sie Premier League-Fußball sehen wollen. Derzeit halten Sky und BT Sport die Rechte, sie haben allerdings dafür mehr als fünf Milliarden Pfund (für drei Jahre) bezahlt. Auch sind Premier League Fußballer sehr hoch bezahlt, dieses Geld muss somit aus den Taschen der Fans erstmal wieder eingespielt werden.

Dennoch nutzen nicht alle Zuschauer diese legale Bezahl-Quelle für Fußball-Live-Übertragungen: Laut einer aktuellen Umfrage ist der Zugriff auf illegale Streams für etwa die Hälfte der Premier League-Fans üblich, rund ein Drittel macht das sogar regelmäßig. So haben 47 Prozent der Fans mindestens einmal in der Vergangenheit ein Spiel durch einen inoffiziellen Anbieter gesehen. Weiterhin streamen 36 Prozent der Premier League-Fans Spiele mindestens einmal im Monat, 22 Prozent schauen sich einmal die Woche einen illegalen Stream an.

Besonders die Zahl der jungen Fußball-Piraten ist bedeutend höher: Im Alter von 18 bis 34 Jahren gaben zwei Drittel (65 Prozent) an, dass sie einmal im Monat ein Spiel online über einen inoffiziellen Anbieter illegal streamen. Bei 34- bis 54-Jährigen verringert sich der Wert auf 33 Prozent, bei 55-Jährigen und älteren liegt er lediglich nur noch bei 13 Prozent.

Das Umfrageergebnis überrascht eigentlich nicht wirklich, aber dennoch sind die Zahlen bemerkenswert hoch. Einer der wichtigsten Gründe, warum auf Streams aus illegaler Quelle zugegriffen wird – und das meinen immerhin 24 Prozent der Fußballfans – ist, dass die Bezahl-Pakete kein gutes Preis/Leistungs-Verhältnis bieten würden. Weitere Gründe sind, dass Familienmitglieder das anschauen und die Befragten schauen lediglich mit zu (29%), auch wäre die Qualität des Online-Streaming gut, das gaben immerhin 25% der Befragten an.

Erst im April gab es dazu ein aktuelles Urteil des Europäischen Gerichtshofs. Demnach stellt das Streaming von einer unlizenzierten Quelle eine Urheberrechtsverletzung dar. Streamen ist grundsätzlich dann illegal, sofern die Webseite für die Nutzer offensichtlich rechtswidrig aussieht. Wenn also ein Portal Fußballspiele kostenlos anbietet, für die man sonst bezahlen müsste, muss auch der weniger technikaffine Nutzer davon ausgehen, dass hier nicht alles mit „rechten Dingen" zugeht und sie könnten dafür auch künftig abgemahnt werden, falls deren IP-Adressen bekannt wären. Laut der Umfrage wussten knapp unter einem Drittel der Befragten nicht einmal, dass das Streamen nunmehr illegal ist, 12% Prozent der Premier League-Fans dachten sogar, es wäre legal.

Kieron Sharp, Generaldirektor von The Federation Against Copyright Theft (FACT), sagte: „Die Leute müssen sich bewusst sein, dass dieser Bereich nun nicht mehr grau ist. Wenn Sie kostenlos auf Inhalte wie Sport, TV und Filme zugreifen, für die Sie normalerweise ein Abonnement benötigen oder ins Kino gehen oder eine DVD kaufen, ist das illegal. Genau wie schon das alte Sprichwort sagt, wenn etwas zu gut aussieht, um wahr zu sein, dann ist das sehr wahrscheinlich so (illegal)."

Ein Sprecher der BBC meinte dazu: „Die Fans sollten wissen, dass diese vorkonfigurierten Kodi-Boxen Piratenübertragungen von Premier League Fußball und anderen beliebten Inhalten zwar ermöglichen, aber dennoch illegal sind. Menschen, die sie bereit stellen, wurden bereits in Haft genommen oder sie mussten erhebliche finanzielle Strafen zahlen. […] Die Premier League wird weiterhin ihr Urheberrecht und die legitime Investition ihrer Rundfunkpartner schützen. Ihr Beitrag ermöglicht es unseren Clubs, Spieler zu entwickeln und zu erwerben, in Einrichtungen zu investieren und die breitere Fußballpyramide zu unterstützen – alles, was die Fans genießen und wovon die Gesellschaft profitiert."

Anonym

Themenübersicht

BUNDESTAG BESCHLIESST NETZWERK-DURCHSETZUNGSGESETZ

Kurz vor der Sommerpause, hat der Bundestag das umstrittene Gesetz beschlossen, das Online-Netzwerke zu einem härteren Vorgehen gegen Hass, Verleumdung, Hetze und Terror-Propaganda verpflichten soll. Das Parlament stimmte mit den Stimmen von Union und SPD gegen die Linke und bei Enthaltung der Grünen für das sogenannte Netzwerkdurchsetzungsgesetz (NetzDG). Der Bundesrat wird sich voraussichtlich am 7. Juli abschließend damit befassen.

Das Gesetz regelt unter anderem, dass Netzwerke, wie Facebook, Twitter und Youtube, dazu verpflichtet werden, klar strafbare Inhalte binnen 24 Stunden nach einem Hinweis darauf zu löschen. Für nicht eindeutige Fälle ist eine Frist von sieben Tagen vorgesehen. Bei systematischen Verstößen drohen Strafen von bis zu 50 Millionen Euro.

Die große Koalition hat sich zuvor noch auf eine neue Fassung für das Netzwerkdurchsetzungsgesetz geeinigt. Anbieter sozialer Netzwerke können die Entscheidung über nicht offensichtlich rechtswidrige Inhalte an eine Art freiwillige Selbstkontrolle abgeben. Eine solche „anerkannte Einrichtung der regulierten Selbstregulierung“ muss staatlich zugelassen und vom Bundesamt für Justiz überwacht werden. Diese Stelle müsse dabei von mehreren Anbietern getragen werden. Bei umstrittenen Löschanfragen können Betreiber auch mehr Zeit für eine Bewertung verlangen. Ferner sollen nun Dienste für „Individualkommunikation“ und „spezifische“ Kommunikation, wie Messenger, ausgeschlossen werden, zudem Berufliche Netzwerke, Fachportale, Online-Spiele und Verkaufsplattformen. Auch soll eine Grenze von mindestens zwei Millionen registrierten Nutzern in Deutschland verhindern, dass Startups durch das Gesetz in ihrer Entwicklung beeinträchtigt werden. Gestrichen haben die Regierungsfraktionen ferner eine Klausel, wonach die Betreiber sämtliche auf den Plattformen befindlichen Kopien illegaler Inhalte ebenfalls unverzüglich entfernen und dafür weitgehende Filter installieren hätten müssen. Der neue zivilrechtlichen Auskunftsanspruch bei schwerwiegenden Persönlichkeitsrechtsverletzungen wird unter Richtervorbehalt gestellt. Große Plattformen wie Facebook werden verpflichtet, hierzulande einen „Zustellungsbevollmächtigten“ für die Behörden bereitzuhalten, der binnen 48 Stunden auf Beschwerden reagieren soll.

Kritiker sehen diese hohen Auflagen als Grundproblem an. Sie meinen, dass damit im Zweifelsfall vorauseilend auch rechtmäßige Äußerungen entfernt würden und so der Schaden für die Meinungsfreiheit groß sei. Bei komplexeren Fällen soll in der Regel eine Sieben-Tages-Frist gelten, um über eine Löschung zu entscheiden. Außerdem wäre bedenklich, dass damit den Unternehmen die Entscheidung darüber überlassen werde, was rechtmäßig sei.

Bundesjustizminister Heiko Maas (SPD) hingegen sieht in dem Gesetz eine „Garantie der Meinungsfreiheit. […] mit diesem Gesetz beenden wir das digitale Faustrecht im Netz“, sagte er. „Denn die Vergangenheit hat gezeigt: Ohne Druck werden die großen Plattformen ihre Verpflichtungen nicht erfüllen.“

Die Grünen-Abgeordnete Renate Künast betonte: „Ich habe immer noch das Gefühl, dass der Reiz zu löschen größer ist als der Reiz, die Meinungsfreiheit einzuhalten“. Ferner warnte sie davor, dass mit dem Gesetz „ganz grundlegende Weichen für das digitale Zeitalter“ gestellt würden. Es schauten andere Länder, auch nicht-demokratische, auf Deutschland.

Die Linke Petra Sitte gab zu bedenken, es sei völlig offen, ob der Entwurf überhaupt verfassungs- und europarechtlich zu halten ist. Strafverfolgung müsse Sache der Justiz sein, nicht von privaten Plattformbetreibern.

Der Digitalverband Bitkom sieht in dem Gesetz weiterhin Probleme mit Verfassung und europäischem Recht: „Es ist sehr wahrscheinlich, dass das unausgereifte NetzDG genauso wie die Vorratsdatenspeicherung gerichtlich gekippt wird“, sagte Bitkom-Hauptgeschäftsführer Bernhard Rohleder.

Facebook befindet, „die mangelnde Gründlichkeit und Beratung“ bei dem Gesetz werde dem Thema nicht gerecht.

WESHALB IHR AB HEUTE EURE E-MAILS VERSCHLÜSSELN WERDET!

Die Antwort ist simpel: Weil Ihr es könnt. Eure letzte Standard-E-Mail konnte vermutlich noch jeder, wie eine öffentliche Postkarte, mitlesen und ohne besonderen Aufwand einfach auswerten. So wurdet auch Ihr analysiert und jeder von Euch zu einem offenen Buch.

Hier drei Wege die man beschreiten kann. Den einfachen Weg, den harten Weg und den smarten Weg. Es liegt ganz bei Euch, welchen Ihr wählt. Am Ende steht die vollständig verschlüsselte E-Mail-Kommunikation.

E-Mails verschlüsseln – der leichte Weg

Nutze ab sofort Protonmail aus der Schweiz! Lade Dir die App herunter und installiere sie Dir auf dein mobiles Endgerät. Du kannst Dir sofort einen kostenlosen Account einrichten. Vorteile: Viele Namen sind noch verfügbar, die Schweiz ist nicht die USA, die Verschlüsselung läuft ohne Dein Zutun automatisch an, wenn dein Gegenüber ebenfalls Protonmail verwendet, was er tun wird, nachdem er diesen Artikel gelesen hat. Lassen sich Deine Bekannten nicht überzeugen, kannst Du ihnen mit Protonmail auch zukünftig, dann allerdings unverschlüsselt über Amerika schreiben.

Du schreibst Deine Nachrichten lieber am Laptop oder PC und möchtest im Übrigen gar kein extra Programm dafür nutzen? Rufe einfach: www.protonmail.com auf und leg los. Wer im Tor-Netzwerk aktiv ist, kann auch folgende Adresse versuchen: https://protonirockerxow.onion.

Der harte Weg

Auch der harte Weg ist nicht mehr so schwer zu beschreiten, wie noch vor einiger Zeit. Soweit noch nicht vorhanden, installiere Thunderbird und richte Dir eine E-Mail-Adresse ein, Du findest Thunderbird in einer Suchmaschine Deiner Wahl und Enigmail über das Plugin-Menu von Thunderbird . Jetzt braucht es einen Neustart von Thunderbird. Nach dem Neustart findest Du Enigmail in der Menu-Leiste. Gehe auf Einrichten, wähle den Assistenten und folge den Anweisungen. Schreibe Deine E-Mail wie gewohnt. Du hast nun zusätzlich die Möglichkeit zu verschlüsseln. Sende Deinen Kontakten Deinen öffentlichen Schlüssel (siehe Menu-Leiste) und speichere öffentliche Schlüssel von Anderen über das Kontextmenu ab. Probier es gleich aus.

Du hast niemanden, der Dir einen öffentlichen Schlüssel (public key) geben kann? Auf https://pgp.mit.edu kannst

Du nach Personen und deren öffentlichen Schlüsseln suchen. Du erhältst hier Schlüssel und E-Mail-Adresse. Hinterlasse doch bei der Gelegenheit auch Deine Daten. So können auch Andere Dich finden und erreichen. Zu hardcore?

Hier ist der smarte Weg

Versuche es mal mit www.keybase.io. Keybase ist, wie der Name schon sagt, ein Schlüsselverzeichnis. Du kannst hier öffentliche Schlüssel finden, die Du eventuell auf dem harten Weg kennengelernt hast. Du kannst aber auch direkt Nachrichten verfassen. Besonders smart ist, dass von hier aus nicht nur die Suche auf Keybase möglich ist, sondern auch zu Twitter, Facebook, Github, Reddit und Hackernews connecten. Apps gibt's für alle gängigen Systeme.

Viel Spaß beim Verschlüsseln!

INDIEN: MOBILFUNKANBIETER „JIO" GEHACKT, 120 MILLIONEN KUNDENDATEN IM NETZ

Der Mobilfunkanbieter „Jio", welcher vor allem mit seinen „Freemium„-Angeboten den indischen Mobilfunkmarkt neu definierte, ist wohl kürzlich gehackt worden. Die Datenbank mit den vertrauliche Daten soll am Sonntag, den 09. Juli, auf der Webseite „Magicapk" veröffentlicht worden sein. Das Unternehmen ist zwischenzeitlich juristisch gegen die Veröffentlichung des Leaks vorgegangen, in der Folge wurde Magicapk von den indischen Behörden vom Netz genommen, wie mehrere indische Medien übereinstimmend berichten.

Abhängig davon, wie viele Informationen die Kunden bei ihrer Anmeldung angegeben haben, war der Name, Vorname, Telefonnummer, E-Mail-Adresse, Aktivierungsdatum und -Uhrzeit der SIM-Karte, die Nummer des Bundesstaates (circle-ID), sowie die 12 Zeichen lange einzigartige biometrische Identitätsnummer frei einsehbar (siehe Screenshot).

Diese Informationen wurden jeweils bei der Registrierung einer neuen SIM-Karte in Indien erfasst und abgespeichert.

Die Echtheit der Daten konnte von mehreren indischen Journalisten sowie Kunden bestätigt werden. Ein Pressesprecher von Jio stellte die Echtheit der Datensätze infrage, versprach aber eine sofortige Untersuchung und die enge Zusammenarbeit mit den indischen Behörden.

First Name:-VARUN
MiddleName:-
Last Name:
mobileNumber:
Email-Id:
circle-Id:-
SIM Activation Date and Time:
aadhaarNumber:-

First Name:-SRIVATSAN
MiddleName:-
Last Name:-
mobileNumber:
Email-Id:-
circle-Id:-
SIM Activation Date and Time:
aadhaarNumber:-

First Name:-SURESH
MiddleName:-
Last Name:-
mobileNumber:-
Email-Id:-
circle-Id:-
SIM Activation Date and Time:-
aadhaarNumber:-

„We have come across the unverified and unsubstantiated claims of the website and are investigating it. Prima facie, the data appears to be unauthentic. We want to assure our subscribers that their data is safe and maintained with highest security. Data is only shared with authorities as per their requirement. We have informed law enforcement agencies about the claims of the website and will follow through to ensure strict action is taken."

Es scheint sich bei den aufgetauchten Informationen um eine sehr aktuelle Kopie der Datenbank zu handeln. Ersten Untersuchungen zufolge sind alle Kundendaten von Käufen bis zu einer Woche vor der Veröffentlichung einsehbar.

Bislang ist nicht bekannt, ob die Daten weiterverbreitet bzw. abgegriffen wurden, um sie anderswo öffentlich verfügbar zu machen. Die Seite Magicapk war bis zur Abschaltung wahrscheinlich aufgrund der Überlastung wenig bis gar nicht erreichbar. Wenn es etwas Neues gibt, werden wir den Artikel zeitnah aktualisieren.

SPEKTAKULÄRER GEFÄNGNISAUSBRUCH MITTELS DROHNE GELUNGEN

Jimmy Causey, ein Häftling im US-Bundesstaat South Carolina, brach aus einem Hochsicherheitsgefängnis aus. Dazu gab am Freitag ein Beamter bekannt, dass der Häftling den dazu benötigten Seitenschneider per Drohne bekommen hätte. Weiterhin habe Causey ein in die Haftanstalt geschmuggeltes Handy benutzt, um die Aktion zu koordinieren. Es war bereits sein zweiter Fluchtversuch innerhalb von 12 Jahren. Dieser wäre jedoch einem Hollywood-Skript würdig, berichtet Associated Press (AP).

Der 46-Jährige Causey war vor 13 Jahren wegen Entführung und bewaffneten Raubes an seinem eigenen Anwalt, dem prominenten Verteidiger Jack Swerling, zu einer lebenslangen Haftstrafe verurteilt worden. Er gab dabei an, zu glauben, der Verteidiger habe damals nicht genug für ihn getan.

Bereits im Jahr 2005 flohen er und sein Mitinsasse Johnny Brewer aus einer Haftanstalt, dem Broad River Correctional Institution in Columbia. Auch hier zeichneten sie sich durch besonderen Einfallsreichtum aus: Die beiden benutzten Toilettenpapierköpfe, die von anderen Gefangenen angefertigt wurden, und legten sie in ihre Betten, um sich einen Vorsprung zu verschaffen. Damals versteckten sie sich in einem Müllwagen, der das Hochsicherheits-Gefängnis verließ. Sie wurden drei Tage später jedoch erneut verhaftet.

Auch dieses Mal gelang es Causey mit einem behelfsmäßigen Dummy in seinem Bett, die Wärter zu täuschen. Am amerikanischen Unabhängigkeitstag, dem 4. Juli, bei Anbruch der Dämmerung, benutzte er den per Drohne zugesandten Seitenschneider, um damit vier Zäune zu zertrennen und so zu entkommen. Er erhielt auf diese Weise einen 18-stündigen Vorsprung. Die Flucht

an sich war jedoch nur von kurzer Dauer. Bereits drei Tage nach seinem Ausbruch wurde Causey in einem Motel in Texas erneut festgenommen. Ein Tipp führte Texas Rangers zu einem Motelzimmer in Austin, wo sie Causey schlafend vorgefunden haben, gaben die Behörden bekannt. Causey hatte zu diesem Zeitpunkt ca. 48.000 US-Dollar in bar, einen neuen Ausweis und zwei Pistolen bei sich. Er hatte inzwischen 1225 Meilen zurückgelegt.

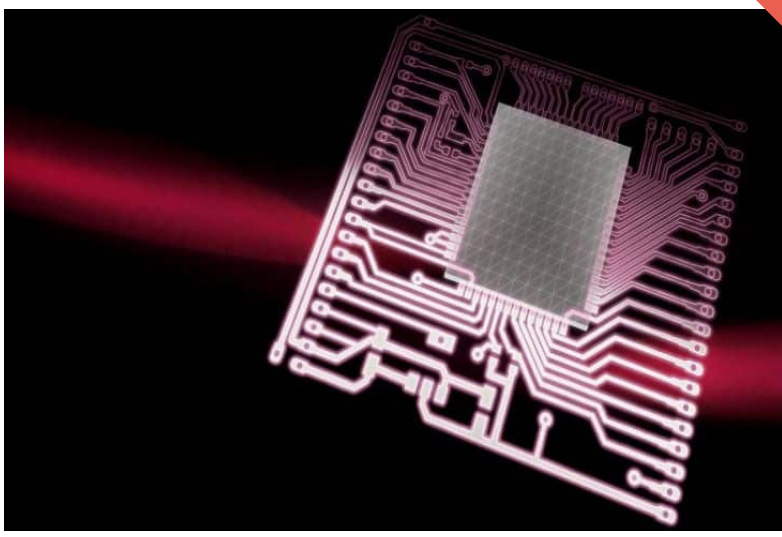
Bryan Stirling, South Carolina Corrections Direktor, meinte zu dem geglückten Gefängnisausbruch: „Wir glauben, dass eine Drohne benutzt wurde, um ihm das entsprechende Werkzeug zu bringen, das ihm das Entkommen ermöglichte“. Wie genau ihm die Drohne das Werkzeug zustellte, ist noch unbekannt. Es sei „teuflisch schwer, die Lieferungen aus der Luft“ auszumachen, meldete die örtliche Polizei am Freitag. Ein offizielles Luftbild des Gefängnisses zeigt einen Kreis von hohen Zäunen mit einer Weite von mehr als 50 Metern zwischen den Gefängnismauern und den Blöcken, sodass es unwahrscheinlich sei, „dass jemand die Werkzeuge geworfen oder katapultiert haben könnte“. „Die Drohne müsse landen, um die Schmuggelware zu liefern“, so der Experte Kevin Tamez, ein 30-jähriger Strafverfolgungsbeamter: „Man könne die Ware nicht wie eine Bombe fallen lassen. […] Die Bereitstellung von etwas, das als Ausbruchswerkzeug taugt, würde einen anspruchsvollen Plan und eine leistungsstarke Drohne erfordern. […] Fortschrittliche Technologie und hoch motivierte Gefangene können eine gefährliche Kombination darstellen.“

Drohnen werden demnach zu einem zunehmenden Problem für Strafvollzugsanstalten. Geschmuggelt werden damit zudem neben Ausbruchswerkzeugen auch bevorzugt Handys, Drogen und Waffen.

RFID-TECHNOLOGIE: US-FIRMA CHIPT MITARBEITER

Das in River Falls, Wisconsin, ansässige IT-Unternehmen Three Square Market (32M), implantiert am 01. August im Rahmen einer Chip-Party ihren Mitarbeitern einen RFID-Chip (radio-frequency identification – „Identifizierung mit Hilfe elektromagnetischer Wellen“) zwischen Daumen und Zeigefinger einer Hand.

Laut Wikipedia bezeichnet RFID eine Technologie für Sender-Empfänger-Systeme zum automatischen und berührungslosen Identifizieren und Lokalisieren von Objekten und Lebewesen mit Radiowellen. Ein RFID-System besteht aus einem Transponder, der sich am oder im Gegenstand bzw. Lebewesen



befindet und einen kennzeichnenden Code enthält, sowie einem Lesegerät zum Auslesen dieser Kennung. Die Kopplung geschieht durch vom Lesegerät erzeugte magnetische Wechselfelder in geringer Reichweite oder durch hochfrequente Radiowellen. Damit werden nicht nur Daten übertragen, sondern auch der Transponder mit Energie versorgt. Die Vorteile dieser Technik ergeben sich aus der Kombination der geringen Größe, der unauffälligen Auslesemöglichkeit (z. B. bei dem am 1. November 2010 neu eingeführten Personalausweis in Deutschland) und dem geringen Preis der Transponder (teilweise im Cent-Bereich).

Der Funkchip wird, einmal implantiert, zur drahtlosen Identifikation der Personen dienen. Er ermöglicht ihnen, Käufe zu tätigen, wie das Zahlen in der Cafeteria , Türen zu öffnen, sich auf Computer einzuloggen, auch Geräte wie Drucker und Kopierer können damit bedient werden. Zudem werden darauf medizinische Informationen gespeichert. Die Firma erwartet, dass sich ihre über fünfzig Angestellten freiwillig chippen lassen.

Als Vorzeigemodell im eigenen Geschäftsbereich wirbt das Unternehmen 32M mit dem Chippen der Mitarbeiter zugleich für die eigene Sache. Das Unternehmen gilt als Marktführer in der Mikro-Markt-Technologie und bietet IT-Systeme und Dienstleistungen für Kleinstgeschäfte in Büros und anderen Arbeitsplätzen an. Das sind kleine Selbstbedienungsläden, die die Pausenversorgung von Mitarbeitern in Pausenräumen von Unternehmen ermöglichen. 32M betreibt derzeit über 2.000 solcher Kioske in Europa, Asien, Australien und Nordamerika. Die Schwesterfirma, TurnKey Corrections, ist mit mehr als 6.000 Kiosken in Gefängnissen vertreten.

Ideengeber war laut 32M die schwedische Firma BioHax International aus Helsingborg, die ihre Angestellten bereits gechipt hat. 32M-Manager Patrick McMullan strebt

eine Zusammenarbeit mit der Firma BioHax an: „Wir freuen uns darauf, mit [BioHax] zusammenzuarbeiten und unseren Marktanteil auf ein anderes Level zu bringen“, gibt er bekannt. 32M hofft darauf, später auch die Mitarbeiter ihrer Kunden für das Chip-Programm gewinnen zu können.

32M-CEO Todd Westby, sieht für den Chip eine große Zukunft. Er meint: „Eines Tages wird diese Technik standardisiert sein und Ihnen ermöglichen, [den Chip] als Reisepass und Fahrausweis sowie für alle Einkaufsmöglichkeiten und mehr zu nutzen.“

Bedenken gibt es jedoch auf Seiten der Datenschützer: Mit den Chips ließen Menschen sich umfassend überwachen, ihre Einkäufe, Zahlungen, Vorlieben, Bewegungen – all das könnte kontrolliert werden und sie so völlig gläsern machen.

CHINA: REGIERUNG FORDERT ÜBERWACHUNGS-APP FÜR BÜRGER IN DER PROVINZ XINJIANG

Die chinesische Regierung fordert von den Bürger in der Provinz Xinjiang, eine Zensur- und Überwachungs-App auf ihren Smartphones zu installieren. Das Ziel der Maßnahme wäre nach offiziellen Angaben der Regierung die Bekämpfung terroristischer Aktivitäten. Überwacht wird die Einhaltung der Anordnung mittels Stichprobenkontrollen durch die Polizei. Wer sich der Anweisung widersetzt, riskiert eine zehntägige Haftstrafe, berichtet Mashable.

Wie Radio Free Asia berichtet, gab die Tianshan-Bezirksregierung in der Landeshauptstadt Urumqi in einer Richtlinie vom 10. Juli bekannt, dass ein Technologieunternehmen, das mit der kommunalen Polizeibehörde verbunden ist, eine App entwickelt hat, die terroristische Video- und Audioinhalte herausfiltern könne. Ursprünglich war diese App dazu gedacht, Minderjährige vor unangemessenen Inhalten oder vor Viren zu schützen.

Genau diese App zwingt die chinesische Regierung der Minderheit der Uiguren im Westen Chinas auf, die es von ihnen zu installieren gilt. Die Maßnahme wurde öffentlich, unter anderem per WeChat, bekannt gegeben. So wurde allen Bewohnern in Xinjiangs Hauptstadt Ürümqi mitgeteilt, dass sie innerhalb einer Woche die App „Jing Wang – „Clean-WebGuard“ verpflichtend auf ihren Mobilgeräten vorweisen müssen. Die Einhaltung dieser Maßnahme werde stichprobenartig durch die Polizei kontrolliert, wobei jenen eine 10-tägige Haftstrafe droht, die der Aufforderung nicht nachkommen.

Über einen QR-Code wird CleanWebGuard als Teil der Messenger-App WeChat installiert. Sie durchsucht in der Folge dann automatisch alle Dateien, wie Dokumente, Bilder, Audio- und Videodateien, die auf dem Smartphone vorhanden sind, nach „Inhalten mit terroristischem oder illegalem religiösen Inhalt“ und gleicht sie zu diesem Zweck mit einer Datenbank der Regierung ab, wobei diese illegale Inhalte automatisch gelöscht werden sollen, zudem auch Bilder, E-Books, Dokumente und andere Dateien, die als gefährdende Inhalte eingestuft wurden. Die App zeichnet zudem sämtliche Konversationen auf, die der Nutzer in den Chat-Apps Weibo und WeChat führt. Protokolliert werden auch Identifikationsnummern der verwendeten Geräte, die verwendeten SIM-Karten und WLAN-Zugangsdaten. Doch damit nicht genug, verfügt die App doch zusätzlich über Möglichkeiten für den Fernzugriff durch die Behörden auf die Smartphones. Ferner kann die App bestimmte Webseiten blockieren und eine Installation anderer Anwendungen verhindern.

Das Ziel der Regierung dürfte es sein, vor allem Minderheiten zu überwachen, wie die muslimischen Uiguren. Die Uiguren sind eine turksprachige, islamische Minderheit, die in China rund acht Millionen Mitglieder hat. Die Regierung versucht bereits seit Jahren, deren Unabhängigkeitsbestrebungen zu unterdrücken. Xinjiang ist dazu auch die Heimat verschiedener anderer Minderheiten und wird als autonomes Gebiet von Peking kontrolliert.

Kritik an der Maßnahme kommt von Menschenrechtsorganisationen, wie Human Rights Watch (HRW): „Die Regierung müssen einiges zu dieser Software erklären, inklusive seinen Funktionen“, fordert Maya Wang von HRW. „Die Regierung hat die Aufgabe die öffentliche Sicherheit zu gewährleisten und Terrorismus zu bekämpfen, aber das massenhafte Sammeln von Daten von gewöhnlichen Leuten ist eine Form der Massenüberwachung und ein Eindringen in die Privatsphäre.“

Joshua Rosenzweig, ein in Hongkong ansässiger Analyst bei Amnesty International, verleiht auch seiner Besorgnis Ausdruck: „Ich denke, es gibt Grund besorgt darüber zu sein, welche Arten von Daten diese Apps über Benutzer und ihre Tätigkeit ohne ihr Wissen oder ihre Zustimmung sammeln können."

CHINA: EINFÜHRUNG VON KLARNAMENSPFLICHT FÜR INTERNETFOREN

In China gibt es eine neue Regelung im Rahmen des neuen Cybersecurity-Gesetzes. Laut einer am 25.08.2017 bekannt gemachten Verfügung, will die chinesische Internet-Regulierungsbehörde Anonymität in Internetforen abschaffen. Internet- und Tech-Unternehmen sowie Internetportale sind künftig dazu verpflichtet, ab dem 01.10.2017, keine Beiträge mehr von nicht identifizierten Nutzern zu veröffentlichen, umgekehrt heißt das, auch für Anwender, die Onlinekommentare verfassen wollen, besteht Klarnamen-Registrierungspflicht beim jeweiligen Anbieter, bevor ihre Posts online zugelassen werden, berichtet die South China Morning Post.

Nachdem die chinesische Zentralregierung bereits Maßnahmen eingeleitet hat für ein nationales Internet, um westliche Dienste, wie Google, Facebook, Twitter, YouTube und Wikipedia, für seine Bürgern möglichst unerreichbar zu machen sowie bis zum 01.02.2018 den Zugang von Einzelpersonen zu Virtual Private Networks (VPN) zu blockieren, gehen sie nun noch einen deutlichen Schritt weiter: Das Ziel der Führung vor dem anstehenden 19. Parteitag der Kommunistischen Partei ist es, das Internet noch besser kontrollieren zu können.

Mit der Einführung der Klarnamenspflicht wolle man „die nationale Sicherheit und die öffentlichen Interessen schützen", heißt es. Weiterhin gehe es darum: „die gesunde und geordnete Entwicklung der Internetgemeinschaft zu fördern […] die legitimen Rechte und Interessen der Bürger zu schützen". Zudem sollen Postings verhindert werden, die „Pornografie, gefälschte Werbung, blutige Gewalt, beleidigende Verleumdungen, persönliche Informationen und andere illegale Informationen" zum Inhalt haben, berichtet The Register.

Die neue Regelung gilt für alle Webseiten, Smartphone-Anwendungen, interaktive Kommunikationsplattformen und „jede andere Kommunikationsplattform, auf denen Nachrichten oder Mitteilungen veröffentlicht werden, die dazu dienen könnten, Anwender zu mobilisieren", heißt es in der Verfügung. Desweiteren sollen die Inhalte der Diskussionen überprüft werden. Anwender werden dazu verpflichtet, die als illegal bewerteten Inhalte an die Überwachungsbehörden zu melden. Ebenso sollen die in Echtzeit kommentierbaren Live-Videos, in China danmu genannt, stärker als bisher überwacht werden. Hier sind die Anbieter künftig dazu angewiesen, ein Protokoll der Kommentare zu veröffentlichen. Zwar sind Dienstleister schon vorher angehalten worden, ihre Nutzer zu identifizieren, aber da die neue Regelung nun im Rahmen des neuen Cybersecurity-Gesetzes gilt, zieht es nun bei Nichtbefolgung auch Strafen nach sich. Freigestellt bleibt es den Nutzern lediglich, ob sie in den Foren unter ihrem Klarnamen oder mit einem Pseudonym auftreten wollen, der jeweilige Anbieter müsse jedoch Pseudonyme den echten Namen der Personen zuordnen können.

Aus vorauseilendem Gehorsam haben bereits einige Webseiten damit begonnen, die künftige Regelung umzusetzen. So hat die Chinesische Suchmaschine Baidu ihre Nutzer dazu aufgefordert, sich noch vor Juni unter echtem Namen zu registrieren. Ebenso forderte die beliebte Frage-und-Antwort-Website Zhihu ihre User auf, ihre Namen mit Hilfe ihrer Mobilfunknummern zu verifizieren, da diese Nummern in China an die Realnamen gebunden sind. Andernfalls würden sie künftig von der Nutzung der Website ausgeschlossen.

WARNUNG VOR DEM WAHL-O-MAT

Anlässlich der Bundestagswahl am 24. September wurde gestern von der Bundeszentrale für politische Bildung (bpb) der neue Wahl-O-Mat vorgestellt. Wir können vor der Nutzung dieser App nur warnen! Sojuniter erläutert im Beitrag, welche Schattenseiten dieses eigentlich nützliche Tool beinhaltet.

Anlässlich der bevorstehenden Wahl möchte ich ausdrücklich vor

der Nutzung des Wahl-O-Mat und ähnlichen Angeboten warnen. Als Informatiker und Datenschützer sehe ich mich verpflichtet zu erläutern, warum die Nutzung nicht ohne Risiko einhergeht.

Das Beantworten von politischen Fragen ist ein sehr heikler Akt, da dabei (gewollt) Einblicke in die politische Gesinnung des Befragten offenbart werden.

Vermeintliche harmlose Fragen können schnell eine Vorverurteilung nach sich ziehen. Eigentlich sehr praktisch, ein paar Fragen beantworten und schon weiß man, wen man wählen soll. Doch was passiert eigentlich mit den Daten nach der Auswertung?

Zuerst einmal sollte bedacht werden, dass der Wahl-O-Mat nicht etwa von einer regierungsunabhängigen Organisation betrieben wird, sondern durch die Bundeszentrale für politische Bildung, einer nicht rechtsfähigen Bundesanstalt, die dem Bundesministerium des Innern unterstellt ist. Selbiges Ministerium hat unter anderem das Verbot von Linksunten.indymedia.org veranlasst.

Eigentlich sollte alles anonym sein, doch sichergehen kann man nicht, ob die gewonnen Informationen auch wirklich gelöscht werden und kein Missbrauch stattfindet.

So findet sich in der Datenschutzerklärung des bpb folgende Aussage:
Jeder Zugriff auf unsere Homepage und jeder Abruf einer auf der Homepage hinterlegten Datei werden protokolliert. Die Speicherung dient internen systembezogenen und statistischen Zwecken. Protokolliert werden: Name der abgerufenen Datei, Datum und Uhrzeit des Abrufs, übertragene Datenmenge, Meldung über erfolgreichen Abruf, Webbrowser und anfragende Domain. Die IP-Adressen der anfragenden Rechner werden anonymisiert protokolliert, eine Rückverfolgung ist nicht möglich. Die Logfiles selbst werden maximal vier Wochen gespeichert, sie werden monatlich automatisch gelöscht.

Wer weiß, ob nicht der Verfassungsschutz Daten nutzt, um vermeintlich Links- oder Rechts-Gesinnte bzw. -Extreme zu identifizieren.

Anstatt die Daten der Auswertung lokal auf dem Computer des Nutzers zu speichern, werden diese auf dem Server des bpb gespeichert. Es ist somit für jeden mit Zugriff auf den Netzwerkverkehr möglich, die politische Gesinnung der Nutzer zu protokollieren.

Auch in der Datenschutzerklärung des Wahl-O-mat selbst findet sich folgende Aussage:

Personenbezogene Daten werden von dem Anbieter nur dann erhoben, genutzt und weiter gegeben, wenn dies gesetzlich erlaubt ist oder die Nutzer in die Datenerhebung einwilligen.

Doch wie soll das funktionieren, ohne das ich angebe, wer ich bin, werden sich mache fragen?

Zuerst einmal kann die IP-Adresse des Aufrufers gespeichert werden. Auch eine Verschleierung durch z.b. ein VPN bietet nicht unbedingt ausreichenden Schutz. Das Identifizieren ist auch alleine durch den sogenannten User Agent des Webbrowsers möglich. Der User Agent des Webbrowser bildet durch das Einbeziehen von Informationen über die Hard- und Software des Computers einen einzigartigen Fingerabdruck. Das Verfälschen vom User Agent durch Browser Plugins bietet auch keinen Schutz. Es macht es eher noch einfacher, da die Verfälschung hervorsticht.

Ein Wahl-O-Mat sollte unabhängig von Institutionen, Ministerien, Bundeszentralen, Konzernen und Parteien sein, auch das Speichern jeglicher Nutzerdaten sowie das Protokollieren von Seitenaufrufen darf nicht stattfinden, nur so wird die Gefahr von Missbrauch und Manipulation geringer ausfallen.

Wer wirklich sichergehen will, liest unter der Anwendung üblicher Anonymisierung-Techniken die Parteiprogramme auf den Webseiten der Partei selbst. So ist auch eine Manipulation der Standpunkte der Parteien nicht gegeben.

JOACHIM HERRMANN: MEHR VIDEOÜBERWACHUNG FÜR BAYERN

Wie Innenminister Joachim Herrmann heute (22.08.2017) angekündigt hat, soll die Videoüberwachung in Bayern massiv ausgebaut werden. Das Konzept sieht mehr Überwachung von Brennpunkten, Großveranstaltungen, aber vor allem im öffentlichen Personenverkehr vor.

Die bayerische Landesregierung will für mehr Sicherheit im Freistaat die Videoüberwachung in allen Bereichen des öffentlichen Lebens ausbauen. Dafür sollen zusätzliche Kameras vor allem an Kriminalitätsbrennpunkten im öffentlichen Raum installiert werden: „Wir werden die Videoüberwachung nur dort ausbauen, wo es für mehr Sicherheit unserer Bürgerinnen und Bürger zwingend erforderlich ist“, kündigt Innenminister Joachim Herrmann (CSU) am Dienstag in München an. Dies würde der Polizei entscheidend bei der Fahndung nach Kriminellen oder auch bei möglichen terroristischen Anschlägen helfen. „Zusätzlich stärkt die Videoüberwachung das Sicherheitsgefühl und kann abschreckend auf potenzielle Straftäter wirken.“

Das Konzept des Landesinnenministeriums umfasst fünf Schwerpunkte:

-
- mehr festinstallierte Videoüberwachungsanlagen,
- die Ausweitung der mobilen Videoüberwachung,
- den weiteren Ausbau der kommunalen Videoüberwachung gerade in Bus und Bahn,
- mehr Videoüberwachung in öffentlichen Gebäuden, wie Einkaufszentren oder Konzerthallen sowie
- den verstärkten Einsatz hochmoderner und innovativer Videoüberwachungsmöglichkeiten
- Bei der Deutschen Bahn und im Nahverkehr setzt man auf noch mehr Kameras an Bahnhöfen und in Zügen, wie auf eine Echtzeitübertragung aus U-Bahn-Wagen.

Herrmann erklärte die Videoüberwachung schon in der Vergangenheit zum „Erfolgsmodell“ und verwies dabei auf die Statistik: „Wir haben überall eigentlich, wo wir Videoüberwachung einsetzen die Erfahrung gemacht, dass Kriminalität anschließend zurückgeht. Das können Kriminalitäts-Brennpunkte sein, wo zum Beispiel vorher ein Schwerpunkt von Drogendelikten lag. Das können im U-Bahn-Bereich Körperverletzungsdelikte sein, das können Überfälle sein.“

Der SPD-Fraktionschef im Landtag Markus Rinderspacher verlangt vom Innenminister, dass es nicht nur bei den Ankündigungen bleibt, sondern vor allem mehr S-Bahnhöfe überwacht werden. Bislang sind es im Raum München nur rund ein Drittel.

GESICHTSERKENNUNG AM BAHNHOF SÜDKREUZ: DIGITALCOURAGE E.V. FORDERT TESTABBRUCH

Seit dem 01.08.2017 läuft am Bahnhof Südkreuz ein sechsmonatiges Pilotprojekt, in dem die Möglichkeit getestet wird, aus Menschenmassen heraus Personen per Kamera automatisch zu erkennen, deren Gesichter zuvor gespeichert wurden. Unter den 275 freiwilligen Testpersonen ist auch padeluun von Digitalcourage. Er hat den Transponder genauer untersucht und dabei herausgefunden, dass der wesentlich mehr kann, als den Testpersonen mitgeteilt wurde. Digitalcourage fordert nun, dass der Test sofort abgebrochen wird.

Für die sich am Projekt „Erprobung intelligenter Videotechnik zur Gesichtserkennung“ beteiligten Testpersonen wurde es am 01.08.2017 ernst. Das Vorhaben startete und die Pendler, die täglich die Teststrecke des Bahnhofs durchqueren, werden nunmehr videotechnisch erfasst. Mittels eines ihnen ausgehändigten Transponders soll festgestellt werden, ob das System die Person tatsächlich immer erkennt, wenn sie einen markierten Bereich im Bahnhof betritt. Dieser Bereich ist mit RFID-Baken „abgezäunt“. Die Freiwilligen mit den RFID-Transpondern sollen so auf jeden Fall erkannt werden, sobald sie die Fläche betreten. Wenn der Algorithmus also das Gesicht nicht erkennt, wird die Person über den Transponder dennoch identifiziert. Damit werde die Zuverlässigkeit der Gesichtserkennung verbessert, so die offiziellen Angaben.

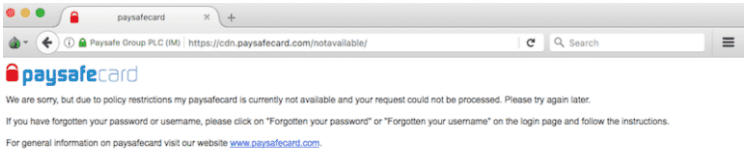
Auch padeluun, der Gründungsvorstand von Digitalcourage

e.V., hat sich als Testperson für das Projekt zur Verfügung gestellt. Er hat den ausgehändigten Transponder unter die Lupe genommen und dabei festgestellt, dass es sich nicht, wie von der Bundespolizei vorher angekündigt, um einen RFID-Chip handelt, sondern, dass er einen iBeacon in Empfang nahm. Das ist ein aktiv sendender Bluetooth-Transponder, mit 20 Metern Reichweite, der in der Lage ist, noch weitaus mehr Informationen zu erfassen, als für den Test nötig sind. Dazu gehören Temperatur, Neigung und Beschleunigung. Der iBeacon kann diese Informationen aufzeichnen, speichern und weitergeben. Diese Daten könnten mit einer App aus Googles Play Store ausgelesen werden. Aufgrund dessen wäre es möglich herzuleiten, was die Personen auch außerhalb des Bahnhofs gemacht haben – also auch außerhalb des Testbereichs.

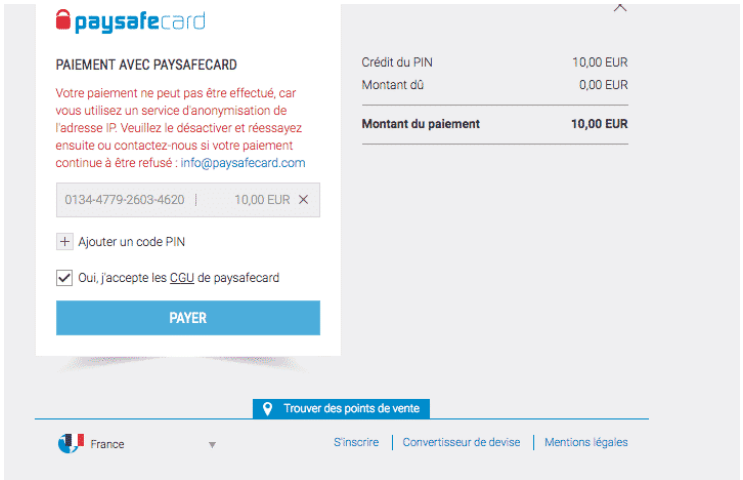
Der Bielefelder Datenschutzverein Digitalcourage fordert einen sofortigen Abbruch der Tests zur Gesichtserkennung am Südkreuz mit der Begründung, dass die Bundespolizei die Testpersonen falsch über die eingesetzte Technik informiert habe. Es wurde dabei Technik eingesetzt, der die Testpersonen nicht zugestimmt haben. Zudem würden auch die Gesichter von Personen erfasst, die nicht am Test teilnehmen. Ebenso würden die Lesegeräte neben den blukii iBeacons noch andere Bluetooth-Geräte erfassen. Auch dazu haben die betroffenen Personen nicht ihre Einwilligung gegeben.

PAYSAFECARD – ANONYMITÄT WAR GESTERN

Im Sommer 2014 warb der Bezahldienstleister paysafecard noch damit, dass man mithilfe ihres sechzehnstelligen PIN-Codes «anonym und sicher im Internet bezahlen» könne. Doch wer tatsächlich versucht, die eigene IP-Adresse beim Einlösen des Guthabens mittels TOR oder diverser VPN-Anbieter zu verschleiern, erlebt sein blaues Wunder. Warum? Das anonyme Bezahlen ist dort schlichtweg unerwünscht. Wir haben uns einmal bei der Pressestelle der Wiener paysafecard.com Wertkarten GmbH erkundigt. Noch immer vertreten viele Nutzer von paysafecard (PSC) die Ansicht, dass sie mit ihren bar gekauften Guthabenkarten online alle möglichen Waren oder Dienstleistungen erwerben können, ohne dabei Spuren zu hinterlassen. Diese Vorstellung sollte man aber besser schnell vergessen. Das stimmt so nämlich schon lange nicht mehr.



Die Vorbereitungen für unseren Testkauf fanden bei ALDI SÜD in Bergisch Gladbach-Frankenforst statt. Dort kauften wir für 10 Euro den PSC PIN-Code in bar, der so ähnlich wie ein Kassenbon aussieht (siehe Bild unten rechts). Ein anonymer Hinweisgeber hatte uns schon vor ein paar Wochen mitteilen lassen, dass PSC vielfach versucht, beim Bezahlvorgang an die IP-Adressen seiner Kunden zu gelangen. Der Grund dafür ist einfach: Das Unternehmen besitzt eine Banklizenz. Deren Schwesterunternehmen, die britische Prepaid Services Company Limited, wird von der Behörde Financial Conduct Authority (FCA) reguliert. Dementsprechend ist dieser Anbieter für Zahlungsdienste naturgemäß dazu verpflichtet, gegen Geldwäsche und andere juristische Verstöße aktiv vorzugehen. Als sicherer Hafen für Schwarzkopierer und Geldwäscher gilt PSC in Insider-Kreisen schon lange nicht mehr. In den Köpfen vieler Käufer hat sich dieses Bild aber noch nicht gewandelt.



Nachdem wir diverse TOR Exit-Nodes erfolglos durchprobiert haben, war gestern der VPN-Anbieter nVPN dran. Wir haben uns dafür mit deren Server in Straßburg vom Datencenter von ovh.com verbunden, das erklärt auch die Fehlermeldung in der französ-

sischen Sprache (siehe Screenshot oben). Auf Deutsch lautet die Fehlermeldung:«Ihre Zahlung kann nicht erfolgen, weil Sie einen anonymen IP-Adressdienst verwenden. Bitte deaktivieren Sie es und versuchen Sie es nochmals oder kontaktieren Sie uns, wenn Ihre Zahlung weiterhin abgelehnt wird: info@paysafecard.com«.

Mehr Erfolg hatte am gestrigen Dienstag ein guter Bekannter der Redaktion, der ebenfalls mit unserem PIN-Code versuchte, einen kostenpflichtigen Account beim Downloading-Service Premiumize.me einzulösen. Der nutzt allerdings den VPN-Dienstleister PIA (privateinternetaccess.com) und wurde somit über einen anderen Server in den Niederlanden mit der Abwicklungs-Stelle von PSC verbunden. Dort klappte es. Der 30-Tage-Account bei Premiumize.me konnte mittels PIA auch ohne Angabe der eigenen IP-Adresse erworben werden.

Bezugnehmend auf unsere Presseanfrage antwortete uns am 11.08.2017 eine Public Relations und Communications Managerin von paysafecard:

(...) Die aktive Bekämpfung von Betrugsfällen im Zusammenhang mit paysafecard-PINs und die Unterstützung bei deren Verfolgung haben bei paysafecard höchste Priorität. Aufgrund geldwäscherechtlicher Bestimmungen ist paysafecard verpflichtet, eine paysafecard unverzüglich zu sperren oder den Vertrag zu kündigen, wenn unsererseits der Verdacht eines Betruges oder Missbrauches oder sonstige Sicherheitsbedenken bestehen.

Hinweise dazu, finden Sie in unseren Allgemeinen Geschäftsbedingungen, die auf unserer Webseite zur Verfügung gestellt werden.Der Punkt 6.4. weißt explizit auf eine eventuelle Sperrung aufgrund von Sicherheitsbedenken hin.

Im Punkt 4.5. finden Sie auch den Hinweis, dass es aus geldwäscherechtlichen Vorgaben auch manchmal zu einer Kundenidentifizierung kommen kann.

Wir hatten im Vorfeld in Erfahrung gebracht, dass es in den vergangenen Jahren vermehrt zu Guthaben-Sperren kam, die man nur mithilfe eines POSTIDENT Verfahrens wieder aufheben konnte. Weil man dabei allerdings in jedem Fall seine Identität preisgeben muss, haben die Betroffenen zu ihrem eigenen Schutz lieber auf ihr Guthaben verzichtet. Auf die Rückfrage, warum PSC-Karten überhaupt bei der Verschleierung der IP-Adresse gesperrt werden, bzw. warum man keine anonyme Einlösung erlauben will, erhielten wir die Antwort:

„Um die Sicherheit des Zahlungsprozesses unserer Kunden zu gewährleisten, gibt es einen risikobasierten Entscheidungsprozess, der bei Betrugsverdacht zur Sperrung von paysafecard PINs führen kann."

Doch auch mit dieser sehr allgemein formulierten Aussage wollten wir uns nicht zufriedengeben. Auch die nächste E-Mail der Pressestelle fiel wieder sehr allgemein aus:

„Zum Thema Kartensperre bitten wir um ihr Verständnis, dass wir aus Sicherheitsgründen keine genauen Details über den exakten Prozess, der zu einer eventuellen Sperre führt nennen können. Wir möchten aber nochmals betonen, dass die Gewährleistung eines sicheren Zahlungsablaufs höchste Priorität für uns hat."

Fazit

Geprüft wird die IP-Adresse des Gutschein-Einlösers in jedem Fall. Wer das und als Anschlussinhaber die mögliche Weitergabe der eigenen Anschrift an die Behörden innerhalb von sieben Tagen verhindern will, muss beispielsweise einen der weniger bekannten VPN-Anbieter, Freifunk (öffentliches WLAN) oder ein Internetcafé seiner Wahl benutzen. Mit TOR kommt man auf keinen Fall weiter. Und auch die VPN-Anbieter werden blockiert, sobald sie eines der größeren Datencenter für ihre Server in Anspruch nehmen. Vielleicht stellt ja mal jemand eine Liste auf, wo die anonyme Nutzung derzeit überall möglich ist – das wäre in jedem Fall eine sinnvolle Ergänzung zu diesem Artikel. Übrigens gehören die Karten der Wettbewerber von Neteller und Skrill zur gleichen Unternehmensgruppe, dort soll es in letzter Zeit aber zu keinen Problemen via VPN gekommen sein. Warum das so ist, konnte oder wollte uns die Wiener PR-Dame natürlich nicht mitteilen.

WHO AM I?
RAT‘ MAL WER ICH BIN!

Wie man sich eine falsche Identität zulegt und warum. Erstellen kompletter Personenprofile, Ausweis, Telefonnummer – was geht und was eher nicht. Ihr erfahrt es gleich hier. Bitte sehr!

Identitätsmissbrauch ist ein gesellschaftliches Problem, das haben neben den Behörden und Diensten auch Versicherer erkannt; man kann sich mittlerweile gegen Identitätsdiebstahl versichern. Ich werde das jetzt nicht weiter kommentieren und es gibt hier auch keinen Link.

Die Gründe für Identitätsmissbrauch, und darum handelt es sich ja im eigentlichen Sinne, sind so vielfältig wie die Menschen selbst, in all ihren Schattierungen; immer liegt die Motivation im politischen, kriminellen oder wirtschaftlichen Bereich (und auch im sexuellen, höre ich gerade aus der Küche). Ja, von mir aus auch im Sexuellen, manchmal ist es auch eine Mischung aus alle dem. Terrorismus, günstiges Reisen oder die Beschaffung eines weiteren Einkommens durch Missbrauch der sozialen Systeme oder Menschenhandel. Reiche Männer kaufen Frauen, Frauen kaufen Kinder, Firmen beschaffen sich Humankapital. Ich möchte das hier nicht bewerten, darum soll es heute nicht gehen.

Denn es gibt da noch etwas anderes, nämlich die persönliche Entscheidung möglichst frei und anonym zu leben, oder es lockt das Abenteuer oder eine innere Stimme ruft zum überschreiten persönlicher Grenzen oder zum Spielen auf. Das ist ein durchaus legitimes Ansinnen und nur darum soll es auch gehen. Wenn man sich für eine falsche Identität entscheidet, hat das Gründe.

Schutz vor Mobbing, Feigheit vor dem politischen Feind, das Dr.-Kimble-Syndrom, Schutz der eigenen Persönlichkeit bei VIPs, Megareichen oder Schauspielern. Letztere greifen nicht nur beruflich zu diesem Mittel sondern auch in der öffentlichen Erscheinung. Polizisten, Politiker tun es aus beruflichem Anlass, aber auch online, um sich vor negativen Folgen für das reale Leben zu schützen. Bockwurst-Benno betreibt Eigensicherung im Flirt-Portal. Bodo ist in seinem sozialen Netzwerk Anwalt und nicht Klopse-Eintüter bei Pfanni. Auch Enno von der Werft nennt keine Berufsbezeichnung; in seinem Expertenforum möchte er weiter als qualifizierter Helfer wahrgenommen werden. Lehrer Arno ist nur im BDSM-Darkroom Arzt oder Hund oder Beides usw…

Falsche Identität: Max MustermannDie Angebote sind vielfältig. Eine komplettes Profil kannst du zum Beispiel mit dem Fakenamegenerator erstellen. Deinen Lichtbildausweis erstellst, du dir hier im Shop von digitalcourage. Eine globale Telefonkarte mit vorinstallierter US-Nummer und der Option auf zwei weiteren Nummern in einem Land deiner Wahl bekommst du auf: www.knowroaming.com. Viel Spaß wünsche ich und immer schön sauber bleiben. Denn einige der genannten Anbieter arbeiten zur Aufklärung von Straftaten mit den Behörden zusammen und überhaupt solltet ihr keine Straftaten begehen, ihr wisst schon…

Aber mal ernsthaft, rechtfertigt allumfassende Auskundschafterei nicht entsprechende Gegenmaßnahmen oder wird nicht sogar komplette Überwachungsemigration zur Pflicht? Ich meine, es bedarf gar keiner Rechtfertigung. Es handelt sich nicht um kriminelle Energie sondern um einen ganz natürlichen affektiven Vorgang. Der Mensch als Individuum, als Bundle-of-perceptions wehrt sich instinktiv gegen eine allumfassende Zwangsvereinnahmung und Totalüberwachung durch die Gesellschaft. Das Individuum ist eben nicht Maschinenmensch, oder Zahnrad im Getriebe eines Systems. Es will exklusiv leben. Als selbständige Entität die Gesellschaft nutzen, sich ihrer bedienen oder zu ihr beitragen, nach eigenen Gutdünken.

In diesem Sinne: Lasst euch nicht überwachen!

BAMF: AB SEPTEMBER ERFOLGT HANDYDATEN-AUSWERTUNG BEI FLÜCHTLINGEN

Gemäß dem „Gesetz zur besseren Durchsetzung der Ausreisepflicht“ wird trotz heftiger Kritik das Bundesamt für Migration und Flüchtlinge (BAMF) nun ab September bundesweit damit beginnen, die Smartphones und Datenträger von Asylbewerbern auszulesen. Das BAMF war bisher noch auf die Zustimmung der Asylsu-

chenden angewiesen, wollte es auf deren Handydaten zugreifen.

Auch die neue Technik zur Umsetzung dieser Maßnahme steht bald bereit: Das Bundesamt für Migration und Flüchtlinge (BAMF) wird ab sofort digitale Assistenzsysteme des sogenannten „Bamberger Modells“ einsetzen. Bevor die Systeme zur Anwendung kommen, wurden sie im Ankunftszentrum des BAMF in Bamberg mehrere Monate getestet. Das System beinhaltet 5 Stufen und umfasst einen Fotoabgleich genauso, wie eine Spracherkennung, die eine Zuordnung nach Herkunftsland möglich macht, bis hin zum Auslesen der Handydaten der Asylbewerber. Dieses Verfahren soll den Asyl-Entscheidern dabei helfen, die Herkunft und die Angaben von Asylbewerbern zu überprüfen sowie Mehrfachidentitäten auszuschließen. Die Assistenzsysteme sollen bereits in einigen Monaten bundesweit in allen Einrichtungen der BAMF zur Verfügung stehen.

Sowohl Anwälte, Hilfsorganisationen, als auch Datenschützer hatten das Auslesen der Handydaten von Flüchtlingen als einen zu weitgehenden Eingriff kritisiert. Die Datenschutzbeauftragte Andrea Voßhoff hat erhebliche Bedenken gegen die Handyüberwachung von Flüchtlingen geäußert. In einer Stellungnahme an den Bundestag gibt sie zu bedenken, dass das Vorhaben einen massiven Eingriff in deren Grundrechte darstellt und sie bezweifelt, dass das verfassungsgemäß ist. Sie gibt an, dass sich auf den Mobiltelefonen der Asylbewerber eine Fülle teils höchst persönlicher Daten befinden würden und auch unbeteiligte Kontaktpersonen durch die Auswertung erfasst würden. Da sich zudem mit den Handydaten höchstens Indizien für eine Identitätsprüfung sammeln ließen, wäre die geplante Regelung damit unverhältnismäßig und verstoße gegen Vorgaben des Grundgesetzes. Auch der Deutsche Anwaltverein befürchtet als Folge des Gesetzes gravierende Verletzungen des Persönlichkeitsrechtes von Geflüchteten und äußert daher verfassungsrechtliche Bedenken. Die Menschenrechtsorganisation Pro Asyl gibt zu bedenken, dass durch die Massenauslesung von Handydaten „gläserne Flüchtlinge“ geschaffen würden.

Nun hat die Chefin des Bundesamtes für Migration und Flüchtlinge (BAMF), Jutta Cordt, die Auswertung der Handydaten von Asylbewerbern gegen diese Kritik verteidigt: „Es ist ein zusätzliches System, eine Unterstützung für unsere Entscheider, um in der Anhörung noch gezielter nachfragen zu können und letztendlich auch sicherer zu entscheiden“, sagte Cordt. Sie betonte, die Handy-Daten sollten nur als „Ultima Ratio“ genutzt werden, „wenn wir Zweifel an der Herkunft haben, die wir nicht anders verifizieren können“, berichtet unter anderem Zeit Online. Bereits beim ersten Kontakt der Asylbewerber mit dem BAMF, werden ihre Telefone ausgelesen, gibt Jutta Cordt bekannt. Diese Daten gelangen dann in eine Art „technischen Safe“ zur weiteren Speicherung. Wenn in einer Anhörung des Bewerbers klar werde, dass die Daten gebraucht werden, müsste ein Volljurist sie freigeben. Zudem gebe es weitere Prüftechniken, die bei der Antragstellung Standard werden sollen, wie die einheitliche Namensübersetzung und die Sprachprobe. „Wenn ich mir deren Ergebnis zusammen mit der Fluchtgeschichte anschaue, kann das in vielen Fällen definitiv ausreichen. Dann braucht man die Handydaten gar nicht“, sagte Cordt. Nach Schätzungen des Bamf würden etwa 60 Prozent der Asylbewerber in Deutschland ohne Identitätsdokumente eintreffen. Wie oft die Handy-Daten künftig wirklich genutzt werden, konnte Cordt zum jetzigen Zeitpunkt noch nicht einschätzen: „Wir müssen jetzt sehen, welche Erfahrungen wir machen. Wir werden etwa ein Quartal brauchen, um eine Datenbasis für eine erste Bewertung zu haben.“

THOMAS DE MAIZIÈRE STREBT FLÄCHENDECKENDE VIDEOÜBERWACHUNG AN

Laut einer Pressemitteilung hat sich bei einem Vor-Ort-Besuch am 24.08.2017 Bundesinnenminister Thomas de Maizière von der Bundespolizei über die Technik für den auf sechs Monate angelegten Test zur biometrischen Gesichtserkennung per Videoüberwachung am Berliner Bahnhof Südkreuz informieren lassen. Indessen kritisieren Datenschützer und Digitalverbände das Projekt.

Ungeachtet aller Kritik gab sich Innenminister Thomas de Maizière optimistisch und hat die Vorhaltungen von Datenschützern und Digitalverbänden am Pilotprojekt zur automatischen Gesichtserkennung am Berliner Bahnhof Südkreuz zurückgewiesen, denn: „Eine Videokamera zeichnet schon jetzt Menschen

auf – befristet, ohne die Offenlegung der Identität. Videoüberwachung ist sehr wichtig, um Straftaten im Nachhinein aufzuklären. Durch diese neue Technik würden Unbeteiligte nicht zusätzlich gespeichert, innerhalb von Sekunden wird nur abgeglichen, ob sie auf einer Fahndungsdatei stehen, und nur im Trefferfall wird dann die Person gespeichert und dann hoffentlich verhaftet. Deswegen verstehe ich einen Teil der Kritik nicht, vor allen Dingen halte ich es für wichtig, dass wir die Effizienz ausprobieren, um dann auch vernünftige Entscheidungen treffen zu können.“ Zudem geschähen die Tests mit ca. 300 Personen auf freiwilliger Basis, sagte de Maizière am Donnerstag bei seinem Besuch vor Ort.

Getestet werden solle, ob mit moderner Technik die Fahndung per Videokamera nach Terroristen, Gefährdern und schweren Straftätern verbessert werden könne. Bereits seit dem 01.08.2017 läuft am Bahnhof Südkreuz das sechsmonatiges Pilotprojekt, der Test zur biometrischen Gesichtserkennung per Videoüberwachung. Es soll dabei anhand von 275 freiwilligen Testpersonen die Möglichkeit erprobt werden, aus Menschenmassen heraus, Personen per Kamera automatisch zu erkennen, deren Gesichter zuvor gespeichert wurden. Später befasst sich ein zweiter Test mit einer Mustererkennung. Dabei sollen hilflose Personen, herrenlose Koffer und andere „Gefahrenszenarien“ erkannt werden.

So habe sich schon in den ersten Wochen an den überwiegend hellen Augusttagen eine erstaunliche Treffsicherheit gezeigt, berichtete de Maizière. Zudem gehe es aber noch darum, die Gesichtserkennung unter anderen Bedingungen zu erproben, wie an dunklen Novembertagen. Auch müsse die Zuverlässigkeit getestet werden, wenn jemand Sonnenbrille, Mütze oder Kapuze – wie hier von Leuten getragen, die unerkannt bleiben wollen – aufgesetzt habe. Nun sei de Maizière „sehr gespannt auf die Ergebnisse“, denn: „Wenn das gelänge, dann wäre das ein unglaublicher Sicherheitsgewinn für die Bevölkerung der Bundesrepublik Deutschland. Und dann können wir entscheiden, in etwa einem halben Jahr, unter welchen rechtsstaatlichen Bedingungen im Einzelnen diese Technik auch flächendeckend eingesetzt werden kann.“, so gab de Maizière bekannt.

Wie wir bereits berichtet haben, stellte sich als freiwillige Testperson auch padeluun, der Gründungsvorstand von Digitalcourage e.V. zur Verfügung. Er untersuchte den ihm ausgehändigten Transponder näher und stellte dabei fest, dass er, nicht wie angekündigt, einen RFID-Chip bekam, sondern ihm wurde ein iBeacon ausgehändigt. Das ist ein aktiv sendender Bluetooth-Transponder, mit 20 Metern Reichweite, der in der Lage ist, noch weitaus mehr Informationen zu erfassen, als für den Test nötig sind, wie Temperatur, Neigung und Beschleunigung. Zudem könnten diese Daten mit einer App aus Googles Play Store ausgelesen werden. Aufgrund dessen wäre es möglich herzuleiten, was die Testpersonen auch außerhalb des Bahnhofs gemacht haben – also auch außerhalb des Testbereichs, so padeluun. Der Bielefelder Datenschutzverein Digitalcourage fordert deshalb einen sofortigen Abbruch der Tests, denn die Bundespolizei habe offensichtlich die Testpersonen falsch über die eingesetzte Technik informiert.

Dieser Umstand rief die Bundesdatenschutzbeauftragte Andrea Voßhoff auf den Plan, denn „Gerade bei Verfahren, die mangels anderweitiger Rechtsgrundlagen auf Einwilligungen zurückgreifen, ist es essenziell, dass den Betroffenen sämtliche Informationen zur Verfügung gestellt werden, die sie benötigen um eine wohlüberlegte Entscheidung zu treffen“, meint sie. Selbst wenn die von dem Transponder ausgesendeten Informationen datenschutzrechtlich nicht besonders sensibel wären, handle es bei dem Aufklärungsversäumnis der Sicherheitsbehörde um keine Lappalie. In einer Stellungnahme weist sie darauf hin, dass der Testlauf derzeit ohne Rechtsgrundlage stattfinde und daher auszusetzen sei. Die Bundespolizei müsse zunächst von den rund 300 freiwilligen Teilnehmern eine erneute datenschutzrechtliche Einwilligung einholen.

SPD-Fraktionsvize Eva Högl forderte ebenso den Abbruch des Testlaufs und einen Neustart. Sie äußerte gleichermaßen den Verdacht, dass gegen datenschutzrechtliche Vorgaben verstoßen wurde: „Deshalb sollte dieser Versuch abgebrochen werden und ein neuer Versuch gestartet werden, bei dem es keine Zweifel an seiner ordnungsgemäßen Durchführung gibt“, meinte sie.

Kritik übte zudem Stefan Brink, der baden-württembergische Landesbeauftragte für Datenschutz. Er verwies heute darauf, dass der Mensch „einen Teil seiner Unverwechselbarkeit und Einmaligkeit preis (gebe), sei es für ein Unterneh-

men oder eine Sicherheitsbehörde“, und müsse sich in Fragen biometrischer Merkmale „im Klaren sein, dass er für den Rest seines Leben weltweit eindeutig identifiziert werden kann“.

Inzwischen hat die Bundespolizei eingeräumt, dass sie Bluetooth-Transponder mit iBeacon-Funktion ausgegeben hat. Ein Sprecher klärte jedoch auf, die Empfangsgeräte am Bahnhof wären so konfiguriert, dass sie die Daten nicht aufnehmen. Auch seien die Beschleunigungsssensoren in den kleinen Geräten, die alle Versuchsteilnehmer in der Tasche tragen sollen, deaktiviert worden.

Bundesinnenminister Thomas de Maizière schloss sich der Aussage an und hat die Kritik zurückgewiesen. Er sehe „überhaupt keinen Grund, jetzt diesen Test abzubrechen“, denn Voßhoffs Bedenken beruhten auf unzutreffenden Informationen des Internetverbandes. Der Transponder diene nur dazu festzustellen, ob es sich um eine Testperson handele. An anderen Informationen bestehe kein Interesse, und die Transponder seien entsprechend inaktiv geschaltet worden: „Ich möchte darauf hinweisen, dass die Datenschutzbeauftragte im Vorhinein damit einverstanden war und wegen der Freiwilligkeit keine Bedenken hatte. Sie hat auch angeregt, die Testpersonen nochmal um eine zusätzliche Einwilligung zu bitten – das prüfen wir jetzt. Ich glaube nicht, dass das notwendig ist, jeder kann aussteigen. Aber meines Erachtens beruhen diese Bedenken auf einer fehlerhaften Vorinformation, als würde der Transponder mehr Informationen speichern, als er tatsächlich speichert“, meinte de Maizière heute beim Ortstermin.

ONAVO: VPN & DATA MANAGER SPIONIERT FÜR FACEBOOK

Wie das Wall Street Journal berichtet, speichert und analysiert der kostenlose Protect Free VPN & Data Manager Onavo den Datenverkehr, also welche Internetdienste und Apps – im Falle von Android – seine Nutzer verwenden und wertet diesen anschließend aus. Die so gewonnenen Erkenntnisse werden vom ursprünglich israelische VPN-Anbieter Onavo an Facebook weitergegeben. Das soziale Netzwerk hatte Onavo 2013 für die geschätzte Summe von etwa 100 bis 200 Millionen Dollar gekauft.

Die App für mobile Datennutzung und VPN von Onavo bietet den Nutzern zum einen eine bequeme Lösung für ein allgegenwärtiges Problem, das daraus resultiert, dass das mobile Datenvolumen durch Facebook, Spotify und Co. schnell verbraucht ist. So kann es auch teuer werden, wenn man jeden Monat weitere Datenpakete zukauft. Doch mit Onavo bekommen Android-Nutzer einen besseren Überblick über ihren mobilen Datenverbrauch. Onavo visualisiert diese Angaben anhand von aussagefähigen Grafiken.

Zum anderen kann man die App noch zusätzlich als VPN zum Schutz in öffentlichen WLANs und zum anonymen surfen nutzen. Auch dieser Dienst ist praktisch, denn wer in einem öffentlich bzw. ungesicherten WLAN-Netzwerk unterwegs ist, sollte eine VPN-App oder einen VPN-Client nutzen. Andernfalls könnte der eigene Datenverkehr von Dritten abgefangen werden und weil dieser in der Regel unverschlüsselt ist, könnten so Passwörter in die Hände von Unbefugten fallen. Eine VPN-Verbindung dagegen verschlüsselt den Datenstrom, sodass die Privatsphäre und somit auch die Sicherheit des Nutzer gewährleistet ist. So sollte es jedenfalls sein.

Als VPN-Dienstleister hat Onavo die Möglichkeit zu sehen, was die Nutzer übertragen und Facebook bekommt auf diesem Weg auch Informationen über User, die gar nicht Mitglied des sozialen Netzwerks sind. Die Privatspäre der Anwender dieser App bleibt somit schon mal nicht gewahrt. Mehr als zehn Millionen Nutzer haben allein die Android-Version der kostenlosen App installiert. Während die App für iOS lediglich unverschlüsselten Datenverkehr über den Browser ausspionieren kann, sind die Informationen, die Onavo über Android-Geräte gewinnt, wesentlich umfassender. Facebook kann so schon früh neue Trends erkennen und darauf entsprechend reagieren und erhält zugleich Einblick in die Nutzung von Konkurrenzangeboten, wie Snapchat oder aufstrebenden Start-ups, wie Houseparty. Die kauft oder kopiert Facebook dann rechtzeitig, bevor diese eine Nische besetzen, die auch für Facebook interessant wäre.

Zwar ist das Vorgehen, dass der Datenverkehr analysiert und weitergegeben wird, von Onavo nicht illegal, aber für den Nutzer auch nicht auf den ersten Blick so einfach zu erkennen: Es ist weder in der App-Beschreibung noch in den Frequently As-

ked Questions (FAQ) auf der Entwicklerwebsite zu finden und wird auch nicht erwähnt in den App-Stores von Google oder bei Apple. „Onavo Protect schützt Sie und Ihre Daten – wo immer Sie sich aufhalten“, heißt es dort stattdessen. Lediglich in einer Datenschutzerklärung versteckt, wird erklärt, dass personenbezogene Daten für verschiedene Zwecke an Dritte, darunter Facebook, übertragen werden. Die Nutzer stimmen dem Ganzen also sogar unwissend zu, denn kaum einer wird sich das so genau durchgelesen haben. Laut diesen Richtlinien gibt es die Option, der Datenauswertung durch Onavo zumindest in Teilen zu widersprechen. Der angegebene Link zur Seite mit weiterführenden Informationen funktioniert jedoch nicht und führt zu einer 404-Seite. Wer als Nutzer dieser App vor Spionage sicher sein will, sollte diese so schnell wie möglich entfernen, so nützlich die angebotenen Features auch sein mögen.

PIZZA CONNECTIONS: KOMMUNIKATION ÜBER DARKNET-ERROR-LOGS

Oder wie Giovanni nach Italien funkt. Kommunikation über Darknet-Error-Logs, so wird es gemacht.

Ich war nicht immer Freund der italienischen Küche, doch als mein Lieblings-Grieche wegen undurchsichtiger Mafia-Kontakte und dem Vorwurf Geldwäsche zu betreiben seine Pforten schließen musste, zog ich nicht wie der Jet Set dem Sternekoch hinterher um alles in Kauf zu nehmen, jede Strapaze zu ertragen oder jeden Preis zu zahlen um dem geliebten Leibkoch nahe zu sein und weiterhin in den Genuss seiner Künste zu kommen, sondern ich tat es der Hauskatze gleich und blieb ortsgebunden. Irgendwie würde man sich schon, kulinarisch, mit den neuen Eigentümern arrangieren können; doch der italienischen Küche kam ich nicht näher. Abgesehen vom obligatorischen Ramazzotti danach, konnte ich mich nicht recht an das Neue gewöhnen. Nach meinem Wissen hatte der Italiener keine Verbindungen zur Mafia, kochte aber miserabel und ward bald ebenfalls nicht mehr gesehen. Dann kam Giovanni, ein Meister seines Faches. Er erklärte mir, das der vorherige Italiener eigentlich Kroate war, und nur aufgrund von Meinungsverschiedenheiten mit dem Finanzamt das Weite gesucht hatte. Die Küche war nun allerdings exzellent und ich saß fast jeden Abend in Giovannis Kneipe. Eines Tages hatte er Computerprobleme und bat mich seinem Schätzchen mal unter die Haube zu sehen. An intimate moment of trust – gleich dem Ergründen des Geheimnisses eines leichten Sommerkleides. Bald war das Gesuchte gefunden und etwas anderes machte mich neugierig.

Offenbar betrieb Giovanni einen Server, ganz ähnlich dem, den wir in „Occupy Darknet“ aufgesetzt hatten, nur ohne jeglichen Inhalt. Nach einigen Ramazzotti war ich „well done“ und das Rätsel gelüftet. Giovanni, der alte Fuchs, wollte sich nicht von PRISM und anderen Surveillance-Programmen in die Zutaten-Liste gucken lassen, die er direkt nach Italien schickte. Denn er bezog alles, was er so brauchte direkt aus Kalabrien. Wie er, hatte auch sein Gegenüber einen mit dem Tor-Netzwerk verbundenen Leer-Server und beide chatteten nun über die Error-Logs der Server. Jeder hatte zwei Fenster geöffnet. Das Terminal mit dem der Server gestartet wurde, und in dem nun ab und zu Error-Logs von hackenden Script-Kiddies auftauchten, die nach wallet.dat’s suchten, und den Tor-Browser vom Tor-Browser-Bundle mit dem die Verbindung zwischen Server und Darknet aufgebaut wurde (siehe Occupy Darknet).

Wenn nun Kalabrien:

>>ohj2k3x3lizwm7ur.onion/chiao_giovanni<< (Beispieladresse)

in den Tor-Browser hackte, erhielt Giovanni folgenden Error-Log:

>>[2017-05-23 23:42:42] ERROR `/chiao_giovanni‘ not found.<<

Nach einer kurzen Sicherheitsabfrage wie:

>>[2017-05-23 23:43:48] ERROR `/dein_erstes_auto_farbe‘ not found.<<

funkte Giovanni die Antwort über seinen Tor-Browser:

>>facebookcorewwwi.onion/fiat_500_rot<< (Beispieladresse). Die Bestellungen selbst erfolgten dann unter Verwendung von Buchstabenpaaren wie: FU_CK_UP_NU… und anderer Zeichen aus Krypto-Listen. Ganz retro und manuell. Giovanni ist dann immer sehr ernst und konzentriert. Natürlich ist das Ganze so aufwändig wie seine Küche, aber Qualität hat eben ihren Preis und geht mal wieder italienisch essen!

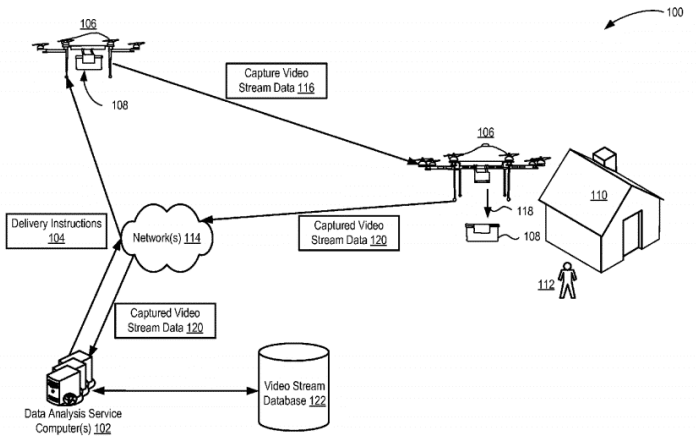
AMAZON-PATENT: DROHNE ERMITTELT WARENBEDARF BEI KUNDEN

Mit dem Patent 9,714,089 unter der Bezeichnung „Trigger Agents in Video Streams from Drones“ hat Amazon sich die Idee für eine neue Technik patentieren lassen: Eine Drohne wird mit einer Videokamera ausgerüstet. Sobald diese die Lieferadresse erreicht hat, sondiert sie die Umgebung. Der Stream wird in eine Zentrale übermittelt und dort ausgewertet. Daraufhin werden dem Kunden Angebote unterbreitet durch Amazon, die exakt auf seine Bedürfnisse zugeschnitten sind. Datenschützer dürften von einem solchen Szenario beunruhigt sein.

Demnach umkreist eine Drohne den Lieferort, macht Videoaufnahmen von den Örtlichkeiten, stellt eventuelle Mängel fest, wie das Fehlen von Dachschindeln auf einem Haus oder sie bemerkt, der Rasen müsse gemäht werden. Genau da würde der Kunde dann nicht nur entsprechende Produktangebote, wie Vorschläge für einen Rasenmäher, sondern auch Serviceangebote zum Reparieren des Daches von Amazon erhalten, die sich genau mit seinem Bedarf decken würden.

Zwar betont Amazon in dem Patent, dass sie die Privatsphäre der Nutzer dabei respektieren wollen und nur die Grundstücke jener Kunden auszuwerten, die das zulassen und entsprechend eingewilligt haben, jedoch kann niemand wirklich prüfen, was mit den Daten passiert, die in die Amazon-Zentrale eingehen.

Ähnlich wie bei den Daten von Amazon Echo u.ä. muss der Nutzer darauf vertrauen, dass Amazon die Auswertungen auch tatsächlich nur intern verwendet und diese nicht missbraucht.



Grafik aus dem Patent zu dem geplanten Vorgehen: Nach dem Scanvorgang soll der Nutzer eine Nachricht in der App oder im Browser erhalten und bekommt dort Angebote aufgelistet.

DATUM HAT DAS NEUE ÖL? MACH DEINE DATEN SELBST ZU GELD!

Die Datum Network Ltd. mit Sitz in Hongkong versucht demnächst möglichst viele Menschen dazu zu bewegen, ihr eigenes Nutzungsverhalten gegen klingende Münze zu veräußern. Datum hat dazu kürzlich eine globale Aktion gestartet, bei der Daten in handelbare Güter wie Amazon-Gutscheine etc. verwandelt werden können. Daten sind das neue Öl. Das ist nicht völlig neu, vielen ist es jedoch noch immer nicht ganz klar. Vielleicht wird dieses Startup daran etwas ändern!??

Egal ob wir uns dessen bewusst sind, jede Online-Aktion generiert Daten. Wenn du deine wissenschaftliche Lieblings-Website besucht hast, oder du etwas auf „FB“ einstellst,

oder du kaufst irgendwo ein Produkt, hinterlässt du eine Datenspur, die dem Seitenbetreiber und dem dahinter liegenden Business mehr über dein Verhalten und deine Gewohnheiten verrät, als du im Augenblick der Nutzung realisierst.

Und es geht hierbei nicht nur um mich oder um Gandalf: 3.7 Milliarden Andere, die gesamte weltweite Internetpopulation, macht es genauso. Sie generiert 2.5 Quintillion neue Bytes pro Tag! Diese Daten machen deine virtuelle Identität aus. Aber diese „Virtuelle Identität“ gehört nicht dir. Und das ist das Problem. Große Mengen deiner Daten werden von Regierungen und weltweit agierenden Konzernen in zentralen Daten-Silos gespeichert. Das Ganze geschieht außerhalb deiner Kontrolle und ohne deine Eigentumsrechte zu beachten. Dennoch, deine Daten werden schon lange zu Geld gemacht.

Die Firma Datum verspricht nun, deine individuellen Eigentumsrechte anzuerkennen. Du bekommst die volle Kontrolle über deine Daten zurück und erhältst zudem die Möglichkeit, Geld mit deinen Daten zu verdienen. Der Vorverkauf der Datum-Genesis-Token (DATG*) hat begonnen:

Presale Cap: 5000 ETH (Ethereum)
Current ETH raised to date: 1693.87 ETH
Current Bonus: 70% (Ends in ~10 hours on 29th August 2017 14:00 GMT)
Current Rate: 1 ETH = 17,000 DATG*
Presale ends: 11th September 2017 14:00 UTC

Mit der Geschäftsidee von Datum eröffnet sich ein 120-Billion-Dollar-Markt von User- und Devices generierter Daten. Alle Transaktionen laufen über ein eigenes Ökosystem von Datum. Die einzelnen Gutscheine werden DAT-Token genannt. Sie stellen „Smart Contracts“ dar, die nach Angaben von Datum sicher und verschlüsselt aufbewahrt werden. Die so gespeicherten Informationen werden nur zu den Konditionen veräußert, die der Nutzer selbst zuvor festgelegt hat. Anschließend kann man das erworbene Guthaben in Form von Gutscheinen von Alibaba, Amazon und anderen Online-Handelsplattformen ausbezahlt bekommen. Umso mehr man von sich selbst preisgibt, umso höher soll der Ertrag ausfallen. Soweit zumindest die Theorie.

Weitere Informationen gibt’s direkt auf der Anbieterseite unter https://datum.network und auf dem von Roger Haenni verfassten White Paper des Unternehmens. Sell your soul, sell your data. Seid ihr mit dabei?

ELTERNKLAGE WEGEN BEFÜRCHTETEN MISSBRAUCHS BEIM DATENSAMMELN VON DISNEY-SPIELEN

Am 03.08.2017 haben Eltern eine Klage gegen Disney und weitere Spieleentwickler in Nord-Kalifornien eingereicht. Der Grund: Diverse Spiele-Apps für Android und iOS würden angeblich ohne Einwilligung der Eltern, Nutzungsdaten ihrer Kinder an Server von Disney schicken, berichtet The Register.

Die Klägerin, Amanda Rushing, klagt auch im Namen von anderen Eltern, deren Kinder „Disney Princess Palace Pets“ und 42 weitere Disney-Marken-Smartphone- und Tablettspiele, wie „Beauty and the Beast: Perfect Match“, „DuckTales: Remastered“, „Star Wars: Puzzle Droids“, „Temple Run: Oz“ und „Where’s My Water?“, spielten, die möglicherweise gegen das Kinder-Online-Datenschutzgesetz (COPPA) verstoßen würden.

Die über 40 Spiele-Apps von Disney und den Entwicklern Kochava Inc., Unity Technologies und Upsight Inc. sollen ohne Genehmigung der Eltern Nutzerdaten von Kindern sammeln, die beispielsweise solche Daten, wie Standorte und Aktivitäten der Kinder ermitteln könnten. Die drei verklagten Spieleentwickler nutzen in den Apps das für das Datensammeln zuständige Werbe-Software Development Kit (SDK) von Disney. So gesammelte Daten sollen dabei auf den Servern von Disney landen. Die Kläger befürchten gemäß der Anklageschrift, dass es Disney so möglich wäre, Nutzungsprofile von Kindern für kommerzielle Zwecke zu erstellen, um gezielte Werbeanzeigen zu verschicken.

Den verklagten Unternehem wird vorgeworfen, gegen das US-Gesetz Children’s Online Privacy Protection Act of 1998 (COPPA) zu verstoßen. Das geht aus der Anklageschrift hervor, die betroffene Eltern beim nordkalifornischen US-Distriktgericht in San Francisco eingereicht haben.

Deutschland

Hat die Wahl.

NETZPOLITISCHE BILANZ DER LEGISLATURPERIODE

Die Große Koalition hat in den letzten vier Jahren eine Reihe von wegweisenden Entscheidungen zum Thema Netzpolitik getroffen. In den meisten Fällen folgte sie dabei dem Trend der letzten Jahre, Freiheiten einzuschränken und die Möglichkeiten der Behörden zum Eingreifen zu erweitern. Neben der Überwachung war vor allem die Bekämpfung unerwünschter Inhalte wie Hasspostings und Fake News ein großes Thema. Auch hierbei entschied sich die Regierung letztlich für eine relativ autoritäre Vorgehensweise. Einen Erfolg feierten Netzaktivistinnen und -aktivisten dagegen mit der erst teilweisen, dann kompletten Abschaffung der Störerhaftung.

Die lange Debatte um die Vorratsdatenspeicherung

Auch nachdem sie 2010 aus verfassungsrechtlichen Gründen ausgesetzt wurde, war die Vorratsdatenspeicherung ein netzpolitisches Dauerbrenner-Thema. Die von 2009 bis 2013 regierende schwarz-gelbe Koalition konnte sich nicht auf eine neue, verfassungsmäßige Umsetzung einigen. Zu groß war der Widerstand der alten FDP-Garde gegen die umstrittene Sicherheitsmaßnahme. Doch die 2013 gewählte Große Koalition griff das Thema sofort wieder auf und suchte verstärkt nach einem verfassungsmäßigen und innerhalb der Regierung konsensfähigen Umsetzung.

Innerhalb der SPD kam es aufgrund dieses Themas zu einigen Reibereien, weil prominente Politiker, vor allem Bundesinnenminister Heiko Maas, ihre Positionen zu diesem Thema radikal änderten. Verkündeten sie zunächst, die Vorratsdatenspeicherung entschieden abzulehnen, wurden sie angesichts politischen Drucks schnell zu ebenso entschiedenen Befürwortern einer Wiedereinführung. So wurde binnen kürzester Zeit eine Neuregelung der Vorratsdatenspeicherung beschlossen. Eine öffentliche Debatte wurde durch das schnelle Tempo - und die geschickte Ausnutzung ablenkender Faktoren - fast völlig vermieden.

Nötig ist die Vorratsdatenspeicherung angeblich vor allem zur Bekämpfung des Terrorismus. Kaum beschlossen, soll sie jedoch schon auf eine ganze Reihe harmloserer Delikte, unter anderem Einbruchdiebstahl, ausgeweitet werden. Damit setzt sich ein Muster fort, das in den letzten Jahren häufig zu beobachten war.

Ob es jedoch tatsächlich zu einer flächendeckenden Einführung der Vorratsdatenspeicherung kommt, ist fraglich. Die NGO Digitalcourage hat Verfassungsbeschwerde gegen das Gesetz eingereicht. Zudem ist die Vorratsdatenspeicherung auch auf EU-Ebene mehr als umstritten, seit der EuGH zu dem Schluss kam, dass eine anlasslose Speicherung, wie sie die Vorratsdatenspeicherung zweifellos darstellt, gegen die EU-Grundrechtscharta verstößt. Somit ist davon auszugehen, dass die Diskussion über die Vorratsdatenspeicherung auch die im September neu zu wählende Bundesregierung noch beschäftigen wird.

Neues von den Behörden-Trojanern

Die Nutzung von Staatstrojanern wurde in der nun ablaufenden Legislaturperiode massiv voran getrieben. Dabei ließ sich die Bundesregierung von technischen und juristischen Bedenken keineswegs abhalten.

Immer mehr Menschen nutzen bei ihrer Kommunikation per Internet digitale Selbstverteidigungsmaßnahmen, insbesondere Verschlüsselung. Das liegt einerseits an einem (unter anderem durch die Snowden-Enthüllungen begründeten) steigenden Bewusstsein für IT-Sicherheit und Datenschutz in der Bevölkerung begründet. Andererseits stellen aktuell immer mehr populäre Messenger auf eine standardmäßige oder zumindest einfach nutzbare Verschlüsselung um.

Die Bundesregierung ist der Ansicht, dass diese Tendenz hin zu mehr Verschlüsselung die Kriminalitätsbekämpfung erschwert. Deswegen forcieren sie die Nutzung des Staatstrojaners für die sogenannte Quellen-Telekommunikationsüberwachung. Dabei wird die behördliche Überwachungs-Software auf dem Zielgerät installiert und anschließend dazu benutzt, digitale Kommunikation mitzulesen, bevor sie für die Übertragung verschlüsselt wird. Kürzlich wurde die Nutzung des Staatstrojaners sogar auch für Alltagskriminalität freigegeben.

Nachdem bisherige, von Drittanbietern gekaufte Software sich als technisch unzureichend und juristisch nicht

tragbar erwies, wurde das BKA verpflichtet, eine eigene Überwachungs-Software zu entwickeln. Diese soll nach einigen Schwierigkeiten und Verzögerungen laut eigener Aussage des BKA noch vor Jahresende fertig werden.

Es ist somit davon auszugehen, dass die Nutzung von Staatstrojanern nach dem Willen der Bundesregierung nicht eingeschränkt, sondern im Gegenteil noch ausgebaut werden soll. Darauf weisen die Bemühungen der letzten Jahre deutlich hin.

Wenig Greifbares vom NSA-Untersuchungsausschuss

Eines der großen netzpolitischen Themen dieser Legislaturperiode war der NSA-Untersuchungsausschuss. Dieser wurde ins Leben gerufen, um die von Edward Snowden aufgedeckten Überwachungsprogramme der NSA und insbesondere die Beteiligung deutscher Behörden an diesen kritisch zu durchleuchten.

Im Laufe seiner Arbeit deckte der Ausschuss viele relevante und schockierende Details der staatlichen Überwachung auf. Dazu zählen zum Beispiel Einzelheiten über die Geheimdienst-Überwachung am Netzknotenpunkt De-Cix in Frankfurt am Main sowie Informationen über die Überwachung von Journalisten durch den BND.

Allerdings fand von Anfang an ein erheblicher Teil der Ausschuss-Arbeit unter Ausschluss der Öffentlichkeit statt. Das ging so weit, dass ein Teil der Protokolle schließlich seinen Weg zu WikiLeaks fand und dort veröffentlicht wurde. Auch sonst wurden dem Ausschuss vielfach Steine in den Weg gelegt. So lässt sich abschließend sagen: die Ergebnisse des NSA-Untersuchungsausschusses sind zweifellos ebenso interessant wie bedeutsam. Erschöpfend indes sind sie auf keinen Fall. Es lässt sich nur spekulieren, welche weiteren Geheimdienst-Skandale bislang unaufgeklärt geblieben sind.

Das BND-Gesetz

Eng verbunden mit der Diskussion über die Arbeit des NSA-Untersuchungsausschusses ist die über das BND-Gesetz. Auch dieses Gesetz zählt zu den wichtigsten - und für Datenschützerinnen und Datenschützern besorgniserregendsten - Entwicklungen in der Netzpolitik im Laufe der nun zu Ende gehenden Legislaturperiode. Das BND-Gesetz soll nach Angaben der Bundesregierung dafür sorgen, dass die Geheimdienste besser demokratisch kontrolliert werden. In der Praxis ist aber eher das Gegenteil der Fall. Der BND erhält bedenkliche Zusatzbefugnisse, das Trennungsgebot zwischen Polizei und Geheimdiensten wird weiter aufgeweicht.

Besonders bedenklich ist eine Klausel, die kurzerhand definiert, dass alle Netzwerke, die (auch) ausländische Datenpakete transportieren, dem Ausland zuzuordnen sind. Damit darf der BND als Auslandsgeheimdienst Internet-Datenverkehr überwachen, selbst wenn sich die Netzwerk-Infrastruktur auf deutschem Boden befindet. Die vom NSA-Untersuchungsausschuss aufgedeckte Überwachung am De-Cix, bislang in einer rechtlichen Grauzone angesiedelt, wird dadurch legalisiert. Ein Gutachten des Chaos Computer Club kam zu dem Schluss, dass diese Praxis ungerechtfertigt ist. Es ist anzunehmen, dass dieses Gesetz noch Gegenstand politischer Diskussionen wie auch gerichtlicher Auseinandersetzungen sein wird.

Die Abschaffung der Störerhaftung

Die Störerhaftung war jahrelang vielen Aktivistinnen und Aktivisten im Bereich der Netzpolitik ein Dorn im Auge. Sie besagte, dass im Falle eines Gesetzesverstoßes nicht nur der oder die eigentlich Schuldige, sondern auch die für die Netzwerk-Infrastruktur verantwortliche Person mit zur Rechenschaft gezogen werden konnte. Diese Konstruktion führte dazu, dass es in Deutschland eine wesentlich schlechtere Versorgung mit offenen WLANs gab als in den meisten anderen EU-Ländern. Aus Sorge vor juristischen Konsequenzen trauten sich viele Deutsche nicht, offenes WLAN zur Verfügung zu stellen.

In dieser Hinsicht wurde in der vergangenen Legislaturperiode ein Durchbruch erzielt. Nach jahrelangen Kämpfen wurde die Störerhaftung erst mit Einschränkungen, kurz darauf komplett abgeschafft. Somit ist der Weg frei für eine flächendeckende WLAN-Versorgung. Einer der Auslöser war eine Entscheidung des EuGH im September 2016, die zu dem Schluss kam, dass zumindest geschäftliche WLAN-Betreiber nicht für Gesetzesverstöße ihrer Kundinnen und Kunden verantwortlich gemacht werden können.

Das Netzwerkdurchsetzungsgesetz: Autoritär gegen Hate Speech und Fake News

Schon längst ist das Internet auch ein Ort von politischen Auseinandersetzungen und Propaganda. Auf themenbezogenen Seiten, aber auch auf Social-Media-Plattformen stehen entsprechende Fragestellungen häufig im Vordergrund. Leider handelt es sich dabei keineswegs immer um sachliche und respektvolle Diskussionen. Häufig mischen sich Beleidigungen und Hetze oder aber Lügen, Manipulation und Propaganda in den Dialog. Hate Speech, also hasserfüllte und diskriminierende Angriffe, die sich häufig gegen Minderheiten richten, sind online ein großes Problem. Ebenso problematisch sind Fake News, also propagandistische, manipulative Nachrichten, die sich als sachliche Berichterstattung tarnen.

Um dieser Problematik Herr zu werden, verabschiedete die Bundesregierung kürzlich das sogenannte Netzwerkdurchsetzungsgesetz. Dieses verpflichtet Plattform-Betreiber, Hate Speech und Fake News innerhalb einer definierten Frist zu löschen. Kommen sie dieser Verpflichtung nicht nach, drohen empfindliche Geldbußen.

Eine derart autoritäre Herangehensweise birgt allerdings einige Probleme. Insbesondere droht eine Überregulation - Infrastruktur-Betreiber, die ein Bußgeld fürchten, löschen Postings auf Verdacht. So drohen viele kontroverse, aber rechtmäßige Postings der Löschung zum Opfer zu fallen. Eine demokratische Diskussion wird dadurch erschwert. Schon George Orwell schrieb 1945 im Nachwort zu seinem Roman „Animal Farm: A Fairy Story“ folgendes: „Falls Freiheit überhaupt etwas bedeutet, dann bedeutet sie das Recht darauf, den Leuten das zu sagen, was sie nicht hören wollen.“ Genau dieses Recht wird durch wohlmeinende, aber schlecht durchdachte und unnötig restriktive Gesetze wie das Netzwerkdurchsetzungsgesetz eingeschränkt - zu Lasten der Demokratie und der Freiheit. Unter anderem deswegen zieht das Netzwerkdurchsetzungsgesetz derzeit viel Kritik auf sich. Es ist davon auszugehen, dass diese Diskussion andauern wird.

Fazit: Wenig Licht, viel Schatten in der Netzpolitik

In den letzten vier Jahren hat sich vieles getan in der deutschen Netzpolitik. Trotz des Erfolgs bei der Störerhaftung hat sich aber aus aktivistischer Sicht vieles eher zum Schlechteren verändert. Eine Umkehrung dieses Trends ist angesichts aktueller Wahl-Prognosen und der Aussagen einflussreicher Politikerinnen und Politiker eher unwahrscheinlich. Das Thema Netzpolitik, so viel lässt sich wohl auch ohne Blick in die Kristallkugel sagen, wird auf absehbare Zeit ein kontroverses und heiß umkämpftes bleiben.

MAASLOSE DISKUSSIONSFAULHEIT: HEIKO MAAS IN MÜNCHEN AUF WAHLKAMPFTOUR

Man muss Heiko Maas zumindest das Zugeständnis machen, dass er sich derzeit in einer schwierigen Lage befindet. Auf der einen Seite soll er Martin Schulz den Rücken stärken und den ziemlich ins Straucheln geratenen Schulz-Zug anschieben. Auf der anderen Seite bekommt er für sein erfolgreiches Engagement und die damit verbundene Umsetzung des NetzDG viel Hass ab. Dabei sollte die systematische und durch die Regierung bewilligte Zensur der Meinungsfreiheit doch genau diesen Hass, den Hatespeech, verhindern. Um die Wogen zu glätten und den Wahlkampf voranzutreiben, lud Heiko Maas am 18. Juli Kritiker und Anhänger zu einer Diskussionsrunde zum Thema „Hatespeech und Fakenews“ ein. Eine ähnliche Veranstaltung rund um den umstrittenen Politiker wurde am Tag zuvor in Dresden abgehalten. Doch während in Ostdeutschland Heiko Maas von mehreren hunderten Demonstranten „begrüßt“ und als Volksverräter beschimpft wurde, blieb es in der beschaulichen Hauptstadt Bayerns vergleichsweise ru-

hig. Einzig die AfD tat mit Transparaten ihrer Meinung in einer lächerlich sicheren Entfernung vom Veranstaltungsort kund. Bloß keine Konfrontation. Und bitte auch kein Hatespeech. Der Austragungsort, der Bürgersaal Fürstenried, füllte sich binnen weniger Minuten. Die anwesende Presse wurde durch den Veranstalter darauf hingewiesen, bitte nur das Podium und nicht die anwesenden Gäste zu fotografieren. Welch Ironie – Anonymität im Real Life aber bitte Klarnamen in Sozialen Netzwerken. Für eine leichtere und bequemere Verfolgung von Straftaten.

Nach einer Vorstellungsrunde der anwesenden Redner und

einer kurzen Ausführung von Heiko Maas, wieso das Netzdurchsetzungsgesetz so wichtig ist, durfte das Publikum eigene Fragen einreichen. Die Diskussionsrunde bestand dann aus den jeweiligen Antworten zu ausgewählten Fragen durch das Podium. Nicht vergessen sollte man, dass es sich um eine Wahlkampfveranstaltung handelte und bei solchen, besonders kritische Fragen nicht zu erwarten sind. So auch in München. Dennoch war die Diskussionsrunde durchaus informativ und konnte kleinen Eindruck zu internen Prozessen und Haltungen der SPD vermitteln.

Ein kleines Aufbäumen

Gerade einmal 60 Parlamentarier haben sich Ende Juni bei der Abstimmung zum NetzDG beteiligt. Das war nur ein Bruchteil der Anwesenden, die sich bei der Entscheidung zum Hype-Thema „Ehe für alle“ im Saal befanden. Laut Aussage von Maas passt sein Gesetzesentwurf nur einige Feinheiten im Detail der aktuellen Rechtsprechung an. Man hätte sich bereits seit mehreren Jahren über das Gesetzt aufregen können, denn die Kernaussage wird durch das NetzDG nicht verändert oder verschärft. Eine Zensur findet ebenso wenig statt. Das Interesse und die Beteiligung bei der „Ehe für Alle“-Diskussion und Abstimmung begründet das Podium damit, dass es die Kanzlerin selbst ist, die bisher gegen die Ehe für alle war. Es war also ein Schulterschluss der Parteien für eine gemeinsame Sache. Übersetzt heißt das: Ein vergleichbar „einfaches“ Thema, mit einem sehr emotional reagierenden Publikum – aber somit auch einer großen potentiellen Wählerschaft.

Genügend Aufklärung

Außerdem wurden laut eigener Aussage durch das Maas-Ministerium eine Vielzahl an Sitzungen abgehalten, um interessierte Abgeordnete zu informieren. In gab es Runden ebenso Details zum Gesetzesentwurf. Umso mehr stellt sich dann aber die Frage, wieso es bei ausreichender Informationsmenge doch noch zu dem bekannten Ergebnis gekommen ist. Dr. Bernhard Goodwin hingegeben kann es nicht verstehen, dass der Deutsche Journalisten Verband sich gegen das NetzDG stellt. Dabei soll dieses doch die Qualität der News und auch der allgemeinen digitalen Diskussionskultur in Deutschland zugutekommen. Noch ein weiterer Abstecher in das Themengebiet Aufklärung. Diese fehlt oft bei jüngeren sowie älteren Generationen gleichermaßen. Beispielsweise wird Mobbing an Schulen durch die vergiftete Diskussionskultur auf sozialen Kanälen befeuert, Eltern sind jedoch machtlos und wissen nicht, was zu tun ist. Man wolle mehr Geld und Kraft in die Aufklärung an Schulen investieren. Konkrete Pläne gab es nicht.

Where is the love?

Doch das hat man an dem Abend grundsätzlich vermisst. Ein wenig entstand der Eindruck, auf einer CDU/CSU-Veranstaltung zu sein, so oft fiel der Satz „ich glaube“. Wo all der Hass denn plötzlich hergekommen sei, möchte eine Dame aus dem Publikum wissen. Das Podium glaubt, er war schon immer da, hat in den sozialen Netzwerken aber eine Bühne gefunden. Besonders an solchen Fragen merkt man, wie wenig Hintergrundwissen die Redner haben. Sie scheinen nicht zu wissen, dass es schon längst Foren und Communities gibt, die sich abseits der gesellschaftlichen Formen unterhalten. Und sind es nicht Reddit oder 4chan, so sind die die Chats im Darknet. Eine Regulierung wird hier kaum möglich sein, ebenso wenig eine strafrechtliche Verfolgung. Anonymität ist grundsätzlich ein guter Weg, das NetzDG auszuhebeln – verrät Heiko Maas ganz beiläufig. Fast gebetsmühlenartig ist von der Bühne zu hören, dass das Web kein rechtsfreier Raum ist. Dass verletzende und hetzerische Aussagen im Internet, ebenso bestraffen werden müssen, als würden diese einem im Real Life ins Gesicht gesagt werden. Ignoriert wird jedoch auch, dass die Gesellschaft ein gewisses Maß an Kritik und harschem Ton verträgt – oder vertragen sollte. Das NetzDG wird anonyme Communities und Foren weiterhin fördern und die Diskussion aus dem Sichtbereich der Masse be-

wegen. Die ignorante Haltung von Heiko Maas, das neue Gesetz könnte den Umgang miteinander unter Zwang verbessern, ist ein Trugschluss. Die Haltung von Maas „lieber zu viel, als zu wenig löschen“ löst nicht das Problem von Hate Speech. Wenn es denn überhaupt ein Problem mit Hate Speech gibt.

Keine Rückfragen, keine Zeit

Leider war die Zeit von Heiko Maas an diesem Abend sehr knapp bemessen. Ein echter Austausch mit den Gästen fand kaum bis gar nicht satt. Die Hand voll Fragen, die das Publikum stellen konnte, reichen für den Titel „Diskussionsrunde“, wie die Veranstaltung beworben wurde, bei weitem nicht aus. Ebenso ist es fraglich ist, ob Maas die Kritiker umstimmen und potentielle Wähler überzeugen konnte. Es war eine Wahlkampfveranstaltung mit vielen Worten aber wenig Inhalten. Viel Glaube, wenig Wissen. Viel Maas, wenig SPD.

INNENMINISTERIUM VERBIETET INDYMEDIA LINKSUNTEN

Mit den Worten „Der Weiterbetrieb der Seite ist ab sofort eine Straftat“ hat Bundesinnenminister Thomas de Maizière die Anfang 2009 gestartete linksextremistische Internetplattform „linksunten.indymedia.org“ verboten. In der Begründung für das Vorgehen gegen die Website heißt es in der Pressemitteilung des Ministeriums, das Portal laufe »nach Zweck und Tätigkeit den Strafgesetzen zuwider« und richte sich gegen die »verfassungsmäßige Ordnung«.

So informierte Thomas de Maizière die Öffentlichkeit am Freitagvormittag in Berlin über Details. Laut Innenminister wäre Linksunten.indymedia „die bedeutendste Internetseite für gewaltbereite Linksextremisten in Deutschland“. Weiter führte er an: „Seit Jahren nutzen sie diese Plattform, um Hass gegen Andersdenkende zu säen.“ Sie würden gezielt zu Angriffen gegen Personen und Sachen aufrufen und detaillierte Anleitungen zum Bau von Brandsätzen veröffentlichen. „Es darf keine Rückzugsräume für Extremisten von links und von rechts geben – weder außerhalb noch innerhalb des Internets“, sagte der Minister am Freitag in Berlin.

In seiner Erklärung bezeichnete Bundesinnenminister Thomas de Maizière den Verein als „linksextremistisch“ und machte ihn für die gewaltsamen Ausschreitungen bei den G20-Protesten in Hamburg mit verantwortlich: „Der Aufruf zu Gewalt gegen Polizisten und deren Bezeichnung als ‚Schweine‘ und ‚Mörder‘ soll Gewalthandlungen gegen Polizisten legitimieren. Er ist Ausdruck einer Haltung, die die Menschenwürde mit Füßen tritt. Das ist absolut inakzeptabel und mit unserer freiheitlichen demokratischen Grundordnung nicht vereinbar“.

Der Inhalt der Seite sei eine „fundamentale Missachtung unserer Gesetze und verstößt gegen die Werteordnung unseres Grundgesetzes“, sagte de Maizière. Er bezog sich dabei auf eine siebenseitige Auflistung mit Beiträgen auf „linksunten.indymedia“. Darunter waren Texte mit strafbaren und verfassungsfeindlichen Inhalten sowie Bekennerschreiben zu Straftaten. Das Ministerium verbreitete am Freitag Beispiele, wie: „Wir wollen Genoss*innen motivieren in Hamburg und anderswo zum G20 Krawall zu machen“, heißt es in einem Artikel. „Wir haben den Fuhrpark der Bundespolizei in Magdeburg in Brand gesetzt“, in einem anderen. „Mit einer Feuerwerksbatterie lassen sich die Bullen unter Dauerfeuer nehmen“, im nächsten.

Genutzt wurde linksunten.indymedia auch von Linksextremisten, die dort u.a. Bekennerschreiben veröffentlichten, darunter zu Brandanschlägen auf Bundeswehr- und Polizeifahrzeuge oder auf Signalanlagen der Bahn. Zudem sind Chat-Verläu-

fe und Telefonlisten über die Plattform veröffentlicht worden, ein Grund, weshalb die Plattform im Verfassungsschutzbericht 2016 auftauchte. Zum Geschäftsprinzip von linksunten.indymedia gehörte es allerdings, ihre Autoren nicht zu kennen.

Begründet wurde das Verbot mit einem Paragraph des Vereinsgesetzes und umfasst laut Veröffentlichung im Bundesanzeiger das Verbot, die Internetseite zu betreiben sowie sonstige „Internetpräsenzen des Vereins“, wie auf Twitter. Dabei ist „linksunten.indymedia“ kein Verein, sondern wurde von einem globalen Netzwerk von Medienaktivisten betrieben. Die Betreiber wurden demnach von den Behörden als Verein eingestuft, obwohl es formal gar keinen solchen gibt. Den Weg über das Vereinsverbot begründete der Minister damit, dass es schwierig sei, gegen einzelne Artikel auf der Plattform strafrechtlich vorzugehen, da diese in der Regel anonym veröffentlicht würden. Daher hätten Behörden kaum Möglichkeiten, gegen die Autoren zu ermitteln. Mit dem Verbot des deutschen Ablegers des weltweiten Netzwerkes Indymedia sollen dem Minister zufolge der „dahinter stehende Verein“ zerschlagen und zudem die dahinter stehenden Gelder eingezogen werden. Somit handelt es sich, auch wenn Linksunten.Indymedia nicht in ein Vereinsregister eingetragen ist, dem Bundesinnenministerium nach faktisch um einen Verein, dessen Mitglieder keine schriftlichen, sondern lediglich mündliche Verträge schließen mussten.

Als maßgebliche Köpfe hinter „linksunten.indymedia“ hat das Bundesamt für Verfassungsschutz drei Personen identifiziert. Laut Spiegel-Bericht handelt es sich dabei um die Freiburger Aktivisten Marco L., Fiona P. und Stephan W., die als Betreiber des radikalen Forums galten. Polizisten stellten ihnen am Freitagmorgen gegen 5.30 Uhr die Verbotsverfügungen zu und durchsuchten unter anderem ihre Wohnungen. Dabei fanden die Beamten nach offiziellen Angaben nicht nur Computer und IT-Technik, sondern auch Messer, Stöcke, Rohre, Zwillen, einen Teleskopschlagstock sowie Butterflymesser. Insgesamt jedoch durchsuchten Beamte der baden-württembergischen Polizei fünf Objekte in Freiburg. Zudem erhöhte die Polizei ihre Präsenz dort – unter anderem für den Fall, dass es Protestaktionen geben sollte. Auch in anderen Ländern stellten sich die Sicherheitsbehörden auf Reaktionen der linksextremen Szene ein. Strafrechtliche Ermittlungen laufen gegen sie noch nicht: Zwar wäre es strafbar, wenn sie linksunten.indymedia.org weiterhin betreiben, allerdings wurde die Seite ja noch am Freitag vom Netz genommen und rückwirkend gilt das Verbot nicht.

Kritik am Verbot gab es, wie erwartet von linker Seite, aber auch – und das unvermutet – von der Polizei: Gegenüber dem Hamburger Abendblatt äußerte sich Jan Reinecke, Hamburger Landesvorsitzende des Bundes Deutscher Kriminalbeamter (BDK) dahingehend, dass das Verbot „mehr Wahlkampf-Symbolik als sinnvoller Kampf gegen Linksradikale“ sei. Vielmehr sei die Plattform sogar nützlich gewesen, sie war „polizeitaktisch sogar wichtig, um die Szene, ihre Pläne und Bekennerschreiben zu beobachten. Das fehlt den Polizisten nun in Zukunft“.

Bundesjustizminister Heiko Maas begrüßte das Verbot: Extremismus dürfe keinen Platz haben, auch nicht im Internet. Auch Sachsens Innenminister Markus Ulbig nannte das Verbot als „außerordentlich wichtig“. Die Seite habe Linksextremisten immer wieder eine Plattform geboten, „um öffentlich zur Begehung von Straftaten aufzurufen, Gewaltaktionen zu planen und diese anschließend zu verherrlichen“.

Die innenpolitische Sprecherin der Linksfraktion, Ulla Jelpke, bezeichnet das Verbot von indymedia.linksunten in einer Pressemitteilung als „illegitimem Akt der Zensur“. Der linke Bundestagsabgeordnete Andrej Hunko sieht in der Maßnahme ein „fatales Signal gegen linken Journalismus“.

Der sächsische Grünen-Politiker und Rechtsanwalt Jürgen Kasek hält das Verbot für gewagt: »Dass auf der Internetseite auch strafrechtlich relevante Texte standen, ist unbestritten. Allerdings reicht das nicht aus, sondern der Verein selber muss dies aktiv fördern und verbreiten«, heißt es in einer Stellungnahme. Das Ministerium habe im vorliegenden Fall eine Haftung für die eingestellten Inhalte »konstruiert«. Kasek ist sich daher keinesfalls sicher, ob das Verbot rechtlich Bestand hat. »Bei Licht betrachtet dürfte es vor allen Dingen darum gehen, ein Zeichen gegen ‘Linksextremimus’ zu setzen und im Wahlkampf Handlungsfähigkeit und Stärke zu demonstrieren.«

Für juristisch fragwürdig hält auch die netzpolitische Sprecherin der Linksfraktion im Bundestag, Halina Wawzyniak, das Verbot auf Grundlage des Vereinsgesetzes. »Aber seit wann ist eine Plattform ein Verein?«, fragt die LINKEN-Netzexpertin auf Twitter.

SICHERE STIMMABGABE PER KLICK? SO STEHT DEUTSCHLAND ZUM THEMA INTERNET-WAHLEN

Am 24. September 2017 findet die Bundestagswahl statt; es entscheidet sich, wer das Land vier weitere Jahre regieren darf. In Zeiten der zunehmenden Digitalisierung kann man durchaus die Frage stellen, ob digitale Wahlen durchführbar sind; und wie aufgeschlossen die Wählerschaft demgegenüber steht. Denn: Die Digitalisierung von Gesellschaft und Staat schreitet voran. Die Schweiz beispielsweise will zukünftig Online-Wahlen neben der Urne und Briefwahl als gleichberechtigte Möglichkeit der Stimmabgabe anbieten [1].

Daher hat sich Kaspersky Lab in einer groß angelegten Untersuchung „Stimmabgabe per Klick - So steht Deutschland zum Thema Online-Wahl“ explizit mit den Themen Online-Wahlen, Datenschutz und Cybersicherheit beschäftigt. Die Studie stellt neben den repräsentativen Umfrageergebnissen von Statista [2] auch eine Übersicht zu politischen Rahmenbedingungen, aktuellen Forschungsergebnissen sowie den derzeitigen Positionen von Politikern und Parteien zum Thema zur Verfügung.

Hier die wichtigsten Ergebnisse der Umfrage unter 3.000 Deutschen auf einen Blick:

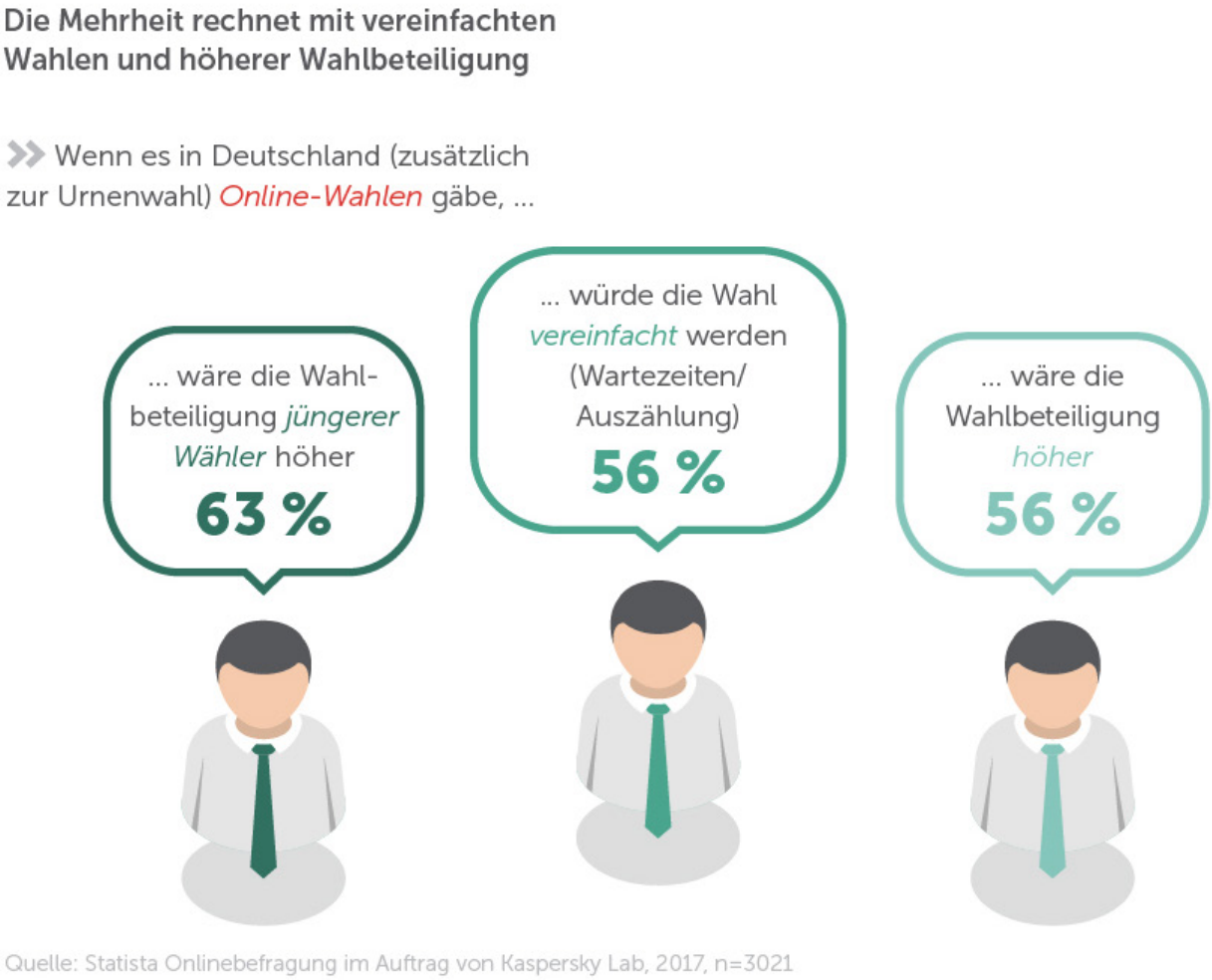
- Mehrheit für Online-Wahlen: Mehr als jeder zweite wahlberechtigte Deutsche (56 Prozent) würde bei der Bundestagswahl 2017 seine Stimme gerne über das Internet abgeben.
- Höhere Wahlbeteiligung erwartet: 56 Prozent sind der Meinung, dass mit der Möglichkeit der Online-Wahl die Wahlbeteiligung steigen könnte und ebenso viele sehen darin eine Vereinfachung des Wahlvorgangs.
- Jungwähler sind sehr affin für Internet-Wahlen: 73 Prozent der 18- bis 29-Jährigen (im Vergleich zu 63 Prozent unter allen Befragten) sind der Meinung, dass die Wahlbeteiligung unter jüngeren Wählerinnen und Wählern höher wäre, da Online-Wahlen ihrem Nutzungsverhalten entgegen kommen würden.

Quelle: Statista Onlinebefragung im Auftrag von Kaspersky Lab, 2017, n=3021

Auch in Deutschland stellt sich irgendwann die Frage der digitalen Stimmabgabe. Spätestens dann müssen wir aus Perspektive der Cybersicherheit gerüstet sein; denn wer Manipulation bei Online-Wahlen vermeiden will, muss ganze neue Antworten auf die Frage der sicheren Identität im Netz und der Sicherheit von Stimmabgaben finden.

- Ältere Wählerinnern und Wähler sind die größten Befürworter digitaler Wahlen in der Politik: Überraschenderweise würden 59 Prozent der Über-50-Jährigen gerne bei der kommenden Bundestagswahl ihre Stimme über das Internet abgeben wollen, im Vergleich zu 56 Prozent im Bevölkerungsdurchschnitt und 51 Prozent bei den 18-bis-29-Jährigen.

- Mehrheitliche Zustimmung für Internet-Wahlen über alle Parteigrenzen: Die Anhänger aller Parteien würden ihre Stimme bei der Bundestagswahl gerne online abgeben können. AfD-Wähler sind mit 60 Prozent die größten Befürworter von Online-Wahlen; auch die Anhänger von CDU/CSU (59 Prozent), FDP (58 Prozent), Die Linke (57 Prozent), SPD (56 Prozent) sowie Bündnis 90/ Die Grünen (54 Prozent) würden mehrheitlich gerne digital wählen.



Die Befragung zeigt auch, dass die Themen Datenschutz und Cybersicherheit für die deutschen Bürgerinnen und Bürger grundsätzlich sehr wichtig sind. Nur etwa jeder Vierte (29 Prozent) hält seine Daten im Internet für sicher. Die Hälfte (49 Prozent) wünscht sich mehr Datenschutz. Auch stimmten 49 Prozent der Aussage zu, dass der gläserne Bürger bereits real sei, und sie nicht mehr Daten preisgeben möchten.

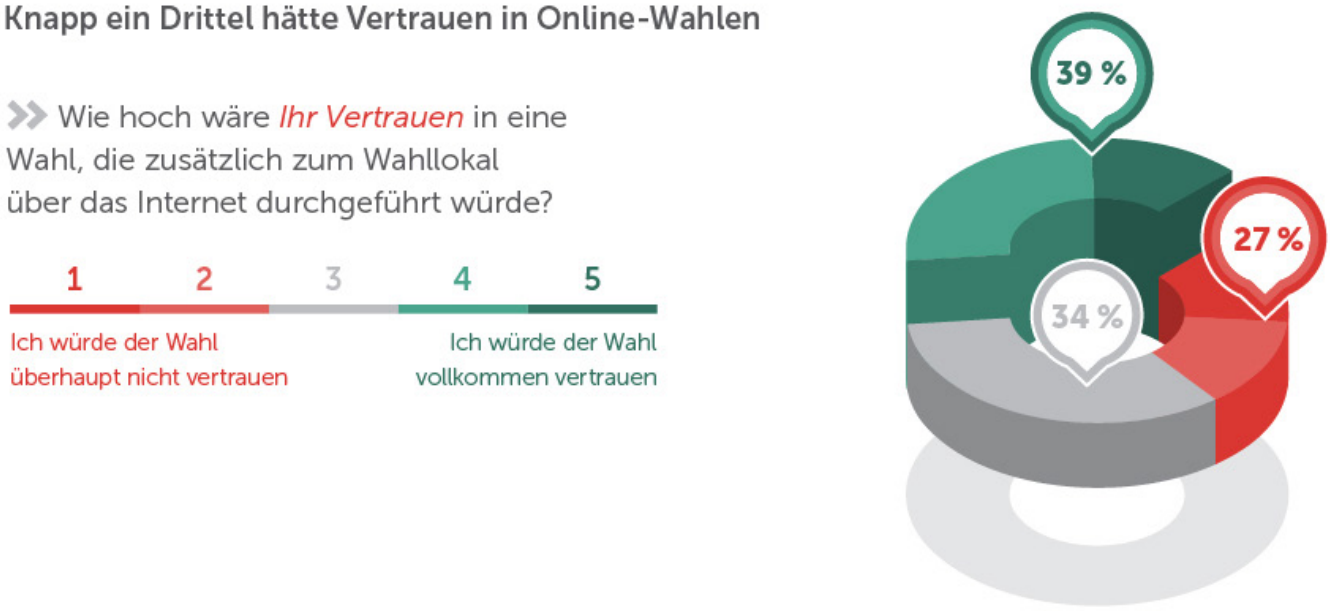
Basis: Cybersicherheit und Datenschutz

Grundsätzlich zeigt die Kaspersky-Studie: die deutschen Wählerinnen und Wähler stehen über Parteigrenzen hinweg Online-Wahlen positiv gegenüber. Aus technischer Sicht sind jedoch noch etliche Schritte zu gehen, um politische Online-Wahlen als Wahlalternative bedenkenlos anbieten zu können. Denn Wahlen sind ein Ausdruck des politischen Willens der Bürgerinnen und Bürger und verdienen daher den größtmöglichen Schutz vor Cyberangriffen und -manipulationen. Es gilt: Man benötigt eine Authentifizierung, damit die Stimmabgabe nur einmalig und ausschließlich für Wahlberechtigte möglich ist. Gleichzeitig muss der Grundsatz der geheimen Wahl hundertprozentig gewahrt bleiben.

Die Experten von Kaspersky Lab sehen bei elektronischen Wahlverfahren mehrere Angriffs- und Manipulationsmöglichkeiten. Dazu gehören

- Distributed Denial-of-Service-Angriffe (DDoS), um den Wahlvorgang generell zu behindern,
- Attacken auf die eingesetzte Software und entsprechende Schnittstellen,
- komplexe Angriffsszenarien auf Infrastruktur und Datenbanken hinter dem Wahlsystem,
- und schließlich Angriffe auf die Wähler selbst, um deren Stimmabgabe zu unterbinden.

Eines ist sicher: es ist noch ein langer Weg zu gehen, um ernst-



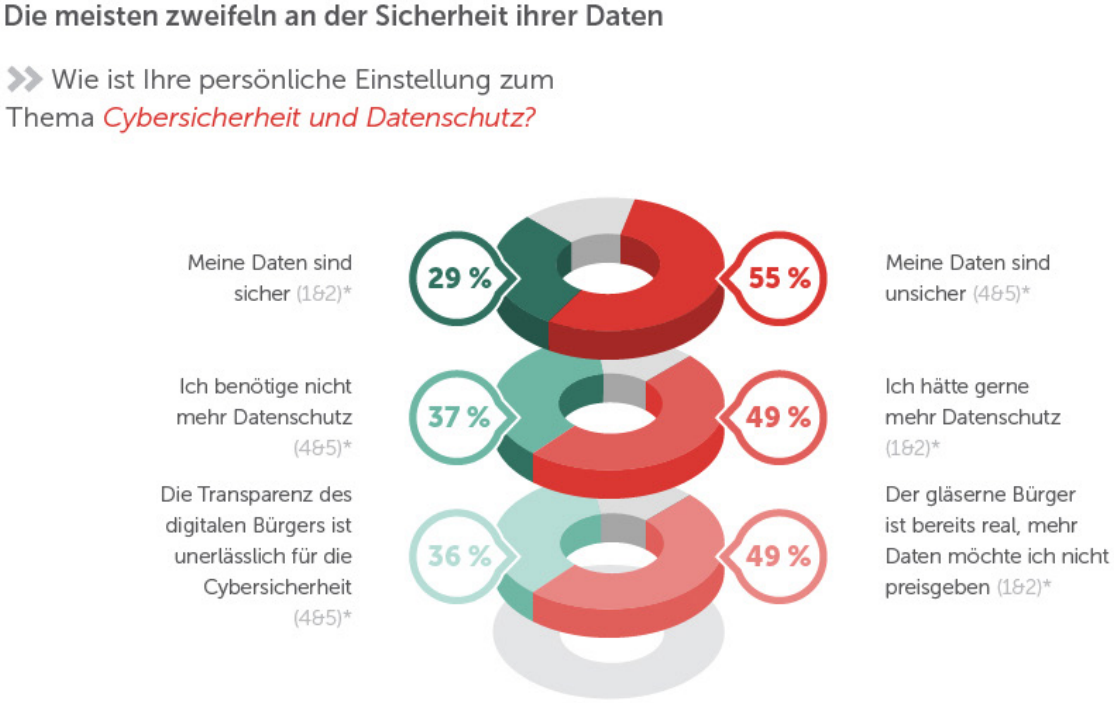
Quelle: Statista Onlinebefragung im Auftrag von Kaspersky Lab, 2017, n=3021

haft über die Einführung cybersicherer Online-Wahlsysteme zu sprechen, das haben auch Cyberangriffe im Vorfeld der US-Präsidentschaftswahlen 2016 gezeigt [3], sowie ein unlängst von den US-Republikanern ausgelöster Wähler-Daten-Leak [4]. Die größte Herausforderung: Von Beginn an müssen bei dem Thema elektronischer Wahlsysteme IT-Sicherheitsaspekte einbezogen werden – ähnlich wie bei Anwendungen des Internet der Dinge.

Sind Online-Wahlen in Deutschland umsetzbar?

Die Studie beschäftigt sich auch mit der Frage, inwieweit Online-Wahlen in Deutschland auf Bundes- oder Europa-Ebene politisch realisierbar wären?

Online-Wahlen müssen sich an die vom Grundgesetz vorgeschriebenen Wahlgrundsätze halten. Laut einem Urteil des Bundesverfassungsgerichts aus dem Jahr 2009 sind diese Grundsätze nicht gegeben. Das Urteil schließt Online-Wahlen allerdings unter bestimmten Voraussetzungen nicht aus. Zu einem ähnlichen Ergebnis kommt der Bundeswahlleiter im Jahr 2015. Diverse Experten auf nationaler sowie europäischer Ebene kommen in ihren Arbeiten unter anderem zu dem Schluss, dass Online-Wahlen bei entsprechendem Schutz



* Antwortmöglichkeiten: Skala von 1 bis 5

Quelle: Statista Onlinebefragung im Auftrag von Kaspersky Lab, 2017, n=3021

der Wahlsysteme sowie breiter Akzeptanz unter der Bevölkerung durchaus zeitgemäß seien und bestimmte Vorteile böten.

Zwei ausführliche Studien haben sich bereits in der Vergangenheit tiefgreifend mit der Frage der Realisierbarkeit politischer Online-Wahlen befasst – unter anderem der Wissenschaftliche Dienst des Deutschen Bundestags im Jahr 2014 [5] sowie das Europäische Parlament im Jahr 2016 [6]. Beide kommen zu dem Schluss, dass Online-Wahlen bei entsprechendem Schutz der Wahlsysteme sowie breiter Akzeptanz unter der Bevölkerung durchaus zeitgemäß seien und bestimmte Vorteile böten.

Wie anfällig sind derzeit genutzte Systeme

Wahlcomputer, ob mit oder ohne Internetanschluss, sind in Deutschland nicht grundsätzlich verboten. Aber die Hürden für ihren Einsatz sind seit 2009 hoch. Das Fachmagazin c't [7] kommentierte das Urteil damals so: „[D]as Bundesverfassungsgericht hat das Pflichtenheft für die Entwickler von e-Voting-Systemen neu geschrieben – und zwar anders, als es die Protagonisten erwarteten. Obgleich die Hüter des Grundgesetzes im Rahmen einer Wahlanfechtung lediglich die Bundeswahlgeräte-Verordnung sowie die bislang vereinzelt eingesetzten und nicht vernetzten Nedap-Wahlgeräte für verfassungswidrig erklärten, weist doch die Art, wie sie dabei – neben der Allgemeinheit, Unmittelbarkeit, Freiheit, Gleichheit und Geheimheit – als sechsten Grundsatz demokratischer Wahlen die öffentliche Kontrolle definierten, weit über den ursprünglichen Streitgegenstand hinaus. […] Der Hausjurist des Bundeswirtschaftsministeriums […] war […] von einem TÜV-Modell ausgegangen. Danach würden Experten stellvertretend für die Bürger die öffentliche Kontrolle wahrnehmen."

Anlässlich der US-Präsidentschaftswahlen 2016 kam die c't auch zu dem Schluss, dass computergesteuerte Wahlsysteme, die in den USA beispielsweise zur Stimmauszählung verwendet werden, „[…] nach europäischen Maßstäben kaum einer Überprüfung standhalten würden." Unabhängig von originären Wahlsystemen kommt bereits heute auch in Deutschland Software zum Einsatz, die beispielsweise zur Vorabkalkulation und anschließender Veröffentlichung von Wahlergebnissen dient – in verschiedenen Bundesländern, vom Bundeswahlleiter und vom Statistischen Bundesamt. Der Chaos Computer Club wies allerdings im Jahr 2017 auf die Schwachstellen der Software hin [8].

Blockchain: Neuer Schwung für Diskussion über Online-Wahlen

Elektronische Wahlsysteme benötigen technologische Ansätze, die höchstmögliche Cybersicherheit gewährleisten. So könnte die Blockchain-Technologie [9] neue Impulse für eine elektronische Stimmabgabe beziehungsweise Online-Wahlen setzen, indem – ähnlich wie beim Online-Banking oder -Shopping – Apps alte Verfahren ablösen und damit den demokratischen Prozess stützen. Definitionsgemäß entspricht die Blockchain einem verteilten System, ähnlich einem Hauptbuch für Transaktionen. Sie kann nicht leicht manipuliert werden und kann die ideale Grundlage für eine elektronische Stimmabgabe bilden.

Die Informationen werden nicht nur einmal und in einem einzigen System hinterlegt, sondern stecken in einer Sequenz von gespiegelten Dateien, den „blocks", die über unzählige unterschiedliche „Knoten" in einem Netzwerk verteilt sind. Die Datenbasis wird damit breit gestreut, die Inhalte kommen ohne Zugriffsberechtigungen aus, sind transparent und unveränderbar.

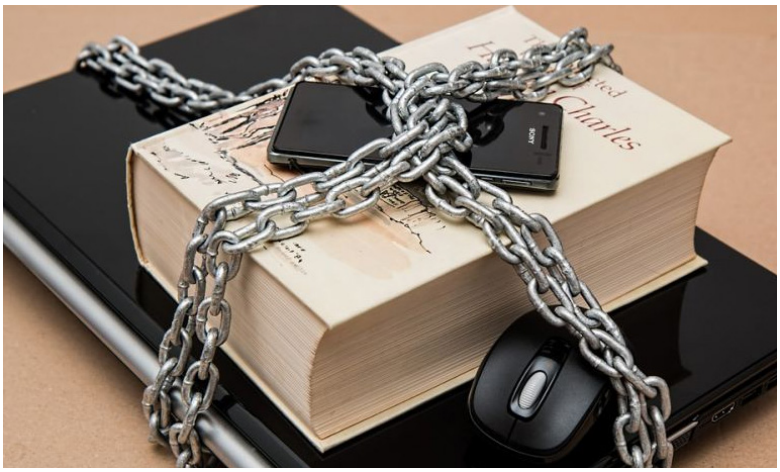
Es gibt keine zentrale Datenbank, die gehackt werden könnte, und keine herausragende Schwachstelle im System selbst. Angreifer, die das Hauptbuch manipulieren wollten, müssten gleichzeitig jedes Glied in der Kette attackieren - und damit Millionen oder gar Milliarden von Rechnern von Freiwilligen, die alle die verteilten Einträge in Echtzeit führen.

Die gleichen Mechanismen, mit denen in der Finanzwelt doppelte Zahlungen vermieden werden, können auch eine doppelte Stimmabgabe in demokratischen Prozessen verhindern. Weder Geld noch Stimmen werden mehrfach gewertet.

Ein Fachbeitrag von Stefan Rojacher,
Corporate Communications Manager DACH & CEE bei
Kaspersky Lab

LAW

Themenübersicht



CHINA VERSCHÄRFT SPÜRBAR ZENSUR IM INTERNET

Anfang der vorigen Woche berichtete Bloomberg, die chinesische Zentralregierung wolle die „Great Chinese Firewall“ noch weiter hochziehen. Darunter fallen Maßnahmen des Staates, ein nationales Internet zu schaffen und westliche Dienste, wie Google, Facebook, Twitter, YouTube und Wikipedia, für seine Bürgern möglichst unerreichbar zu machen. Die chinesische Regierung hat die Telekommunikationsanbieter angewiesen, den Zugang von Einzelpersonen zu Virtual Private Networks (VPN) bis zum 1. Februar 2018 zu blockieren.

Anders als hier in Deutschland hat China eine heterogene Online-Landschaft, die vielfältige Plattformen umfasst. Alles beherrschende Anbieter, wie Facebook, gibt es dort nicht. Eigentlich sollte damit eine zentral gelenkte, staatliche Zensur erschwert sein, allerdings hat das Regime doch Wege gefunden.

Aktuell hat dazu die Regierung die staatlichen Telekommunikations-Anbieter, wie China Mobile, China Unicom und China Telekom angewiesen, VPNs zu Beginn des kommenden Jahres zu blockieren. Ausländische VPN-Anbieter können nur dann weiter in China operieren, wenn sie sich dort registrieren lassen. Der Einsatz von VPN-Tunneln erlaubt es den Nutzern, vorzutäuschen, dass sie von einem anderen Land aus auf das Internet zugreifen, denn neben Facebook, Twitter, Instagram und Google sind zudem auch verschiedene westliche Nachrichtenportale für Nutzer in China gesperrt.

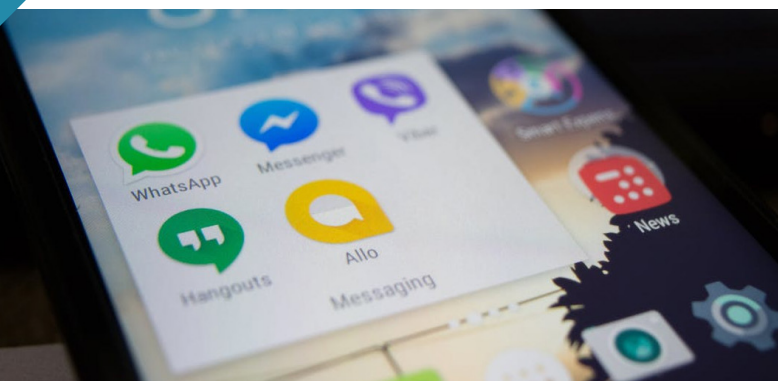
Schon seit Jahren ist die chinesische Regierung bestrebt, die Internetnutzung ihrer Bürger und der im Land beheimateten Firmen zu kontrollieren, so kommt auch das Verbot von VPNs nicht gänzlich überraschend. Für Staatschef Xi Jingping allerdings bedeutet diese Zensur „nationale Souveränität im Internet“. Die Wahrung der Souveränität gleicht allerdings einem Balanceakt, denn einerseits sollen kritische Stimmen ungehört bleiben und andererseits will Chinas Bildungselite genügend persönlichen Freiraum. Auch für ausländische Unternehmen im Land wird die Internetzensur zunehmend zu einem negativen Standortfaktor. Sie brauchen ein gutes Geschäftsklima, um im Land agieren zu können.

Ein weitere Zensur wurde erst heute bekannt. Laut Medienberichten ist aktuell Pu der Bär, eine beliebte Kinderbuchfigur des Autors Alan Alexander Milne, aus den sozialen Medien Chinas fast vollständig verbannt. Fans von Pu wissen: Der kleine Bär ist zwar „von sehr geringem Verstand“, will aber niemandem etwas Böses. Er ist verträumt, etwas begriffsstutzig und doch voller Weisheit. Dennoch ist die Kinderbuchfigur in China in Ungnade gefallen. Der Grund: Zu viel Ähnlichkeit mit dem chinesischen Staatschef Xi Jinping. So wurde Präsident Xi Jinping in der Vergangenheit im Internet wiederholt in Montagen abgebildet, in denen er die Position des Bären einnahm.

Bereits 2013 tauchten Bildmontagen, in denen Xi Jinping mit Pu in Verbindung gebracht wurde, in den sozialen Netzwerken auf: Xi wurde zusammen mit dem damaligen US-Präsidenten Barack Obama bei einem Spaziergang gezeigt, daneben Pu der Bär in fast identischen Pose mit seinem Kumpel Tiger. Ein Jahr später kam dann eine weitere Montage hinzu, auf der Xi dem japanischen Ministerpräsidenten Shinzo Abe die Hand schüttelt – parallel zu Pu und dem traurig wirkendem Esel I-Aah.

Eine offizielle Begründung für die Zensur gegen Pu gab die chinesische Regierung nicht bekannt. Anfragen in den Suchmaschinen wurden aber mit einem Error-Zeichen beantwortet. Darin enthalten war ein Hinweis, es handle sich um „illegalen Inhalt“. Im sozialen Netzwerk WeChat wurden zudem Pu-Sticker aus der offiziellen Sticker-Galerie gelöscht. Offensichtlich soll in diesem Fall die politische Führung nicht ins Lächerliche gezogen werden und hält einen Vergleich mit einem Bär „von geringem Verstand“ wohl eher für unangebracht.

Nach den vorangegangen, umfassenden Zensurmaßnahmen testen nun Internetnutzer die noch verbliebenen Spielräume aus. So wurden animierte GIF-Bilddateien bislang noch nicht gelöscht. Ein Weibo-User schrieb: „Armer kleiner Pu. Was hat dieser kleine Honigbär je getan, um andere zu provozieren?“



FILESHARING: BUNDESGERICHTSHOF SPRICHT SICH GEGEN BEWEISVERWERTUNGSVERBOT AUS

Bei Verstößen gegen das Urheberrecht, wie dem illegalen Tausch von Musik, Filmen, Software oder E-Books über Tauschbörsen, müssen die Netzbetreiber die Nutzerdaten bzgl. der IP-Adresse herausgeben, wenn eine Richtergenehmigung vorliegt. Der für das Urheberrecht zuständige I. Zivilsenat des Bundesgerichtshofs erweiterte am Donnerstag in einem Urteil den Wirkungsbereich dieser Richtergenehmigungen auch auf Reseller, dem Nutzer einer Netzinfrastruktur als Wiederverkäufer. Bislang musste in solchen Fällen eine weitere Richtergenehmigung beantragt werden.

Der Beklagten wurde zur Last gelegt, sie hätte in einer Internet-Tauschbörse das Computerspiel „Dead Island“ zum Herunterladen angeboten. Die Koch Media GmbH, vertreten durch die Abmahnkanzlei Reichelt Klute Assmann (RKA), machte ihre Rechte geltend, Inhaberin der ausschließlichen Nutzungs- und Verwertungsrechte an dem Computerspiel zu sein. Die Klägerin verlangt von der Beklagten die Zahlung von Abmahnkosten (859,80 €) und Schadensersatz (500 €). Der Auskunftsanspruch richtete sich gegen die Deutsche Telekom AG, ihr Provider jedoch war die „X AG“.

Nach der Identifikation der IP-Adresse hatte ein Richter die Forderung auf Herausgabe der Nutzerdaten vom Netzbetreiber genehmigt. Dieser war allerdings die Deutsche Telekom, von welcher die „X AG“ die Netzinfrastruktur als Wiederverkäufer nutzt. Die „X AG“ hatte zwar auf Nachfrage der Telekom die Nutzerdaten der Frau herausgegeben. Name und Anschrift waren als Beweismittel in vorherigen Instanzen jedoch nicht anerkannt worden, da die Richtergenehmigung sich auf die Telekom als Netzbetreiber bezogen hatte und die vom Provider, der „X AG“, erteilten Auskünfte einem Beweisverwertungsverbot unterlägen, sodass nicht festgestellt werden könne, ob das Computerspiel „Dead Island“ zum Herunterladen über den Anschluss der Beklagten erfolgt sei: „Seien Netzbetreiber (Deutsche Telekom AG) und Endkundenanbieter (Provider „X AG“) nicht identisch, so müsse der als Vertragspartner des Anschlussinhabers in Erscheinung tretende Endkundenanbieter („X AG“) beteiligt werden“, so urteilte das Landgericht (LG) Frankenthal (Az. 6 S 149/15). Weil die Auskunft der „X AG“ nicht gestattet wurde, könnten ihre Auskünfte auch nicht verwertet werden.

Bisher wurde also nach geltendem Recht geurteilt, dass bei einer solchen Konstellation Name und Adresse des jeweils Betroffenen überhaupt nicht hätten herausgegeben werden dürfen, diese Daten unterlagen einem Beweisverwertungsverbot. Dem Rechteinhaber wurde es somit unmöglich, eine Urheberrechtsverletzung überhaupt nachzuweisen.

Der BGH urteilte nun jedoch grundsätzlich anders, indem er ausführte, dass bei diesen Gegebenheiten kein Beweisverwertungsverbot bestehe. Somit wären die von Provider „X AG“ mitgeteilten Nutzerdaten auch als Beweismittel zulässig. Begründet wurde das dadurch, dass es sich dabei nicht um Internet-Verkehrsdaten wie IP-Adresse, Tag und Uhrzeit handelte, sondern um Bestandsdaten, nämlich Namen und Adresse des Kunden. Hierzu ist kein weiterer Auskunftsanspruch notwendig, ein richterlicher Beschluss gemäß § 109 Abs. 9 Satz 1 UrhG wäre lediglich für Verkehrsdaten erforderlich.

Für diesen Fall bedeutet das, dass aufgrund der neuen Beweislage eine weitere Verhandlung anberaumt werden wird, in der eine rechtskräftige Verurteilung der Beklagten sehr wahrscheinlich ist, da die Beweismittel ja bereits vorliegen und jetzt auch verwertet werden dürfen.

Fazit

Indem nun die herausgegeben Kundendaten als Bestandsdaten verwertet werden dürfen und keinem Beweisverwertungsverbot mehr unterliegen, hat hat sich das Risiko für aktive Filesharer, erwischt und belangt zu werden nun nochmals deutlich erhöht. Während sich einige Piraten vorher noch hinter Netzkunden der Deutschen Telekom verstecken konnten, ist seit diesem Urteil eine einmalig ausgestellte Richtergenehmigung automatisch auch für diese gültig, die Auskünfte somit auch als Beweismittel zulässig.

FILESHARING: DAS FESTSTELLEN EINER IP-ADRESSE FÜHRT NICHT IMMER ZUM ABMAHNERFOLG

In einem Rechtsstreit der Warner Bros. Entertainment GmbH als Klägerin, vertreten durch die Münchener Abmahnkanzlei Waldorf Frommer und einem Mandanten der Anwaltskanzlei Wilde Beuger Solmecke hat das Amtsgericht (AG) Köln in einem Urteil entschieden, dass es als Tatbeweis nicht ausreicht, wenn ein Anschluss mehrfach über die gleiche IP-Adresse ermittelt worden ist.

Der Beklagte wurde des Filesharings beschuldigt und im Auftrag der Warner Bros. Entertainment GmBH durch die Rechtsanwaltskanzlei Waldorf Frommer entsprechend abgemahnt. Es wurde ihm vorgeworfen, dass er als Anschlussinhaber die Serienfolge „Person of Interest – The Day The World Went Away“ Dritten im Internet zum Download angeboten habe.

Folglich sollte er den Ersatz des Lizenzschadens in Höhe von 500 Euro und Ersatz der Abmahnkosten in Höhe von 168,50 Euro zahlen. Als Beweis führte die Rechtsanwaltskanzlei Waldorf Frommer an, dass eine Ermittlungsfirma mittels Ermittlungssoftware im Abstand von etwa 10 Minuten zweimal dieselbe IP-Adresse festgestellt habe. Die Nachfrage beim Provider habe dann ergeben, dass diese dem abgemahnten Anschlussinhaber zugeordnet gewesen sei.

In einem Urteil vom 28.06.2017 (Az. 125 C 571/16) entschied das Amtsgericht Köln in diesem Fall, dass die Warner Bros. Entertainment GmbH keinerlei Ansprüche gegenüber dem Beklagten hat. In der Begründung heißt es, es bestünden Zweifel daran, ob der Anschlussinhaber auch tatsächlich zuverlässig ermittelt worden sei. Eine hinreichende Sicherheit für eine Verurteilung sei nur dann gewährleistet, sofern mehrere Ermittlungen über unterschiedliche IP-Adressen vom Internetprovider demselben Anschluss zugeordnet werden konnten. Es gebe hohe Fehlerquoten bei der Ermittlung der IP-Adresse und der Zuordnung des Anschlussinhabers. Dass bei der Ermittlung einer einzelnen IP-Adresse eine besonders hohe Fehlerquote besteht, ergibt sich aus einem Urteil des AG Köln vom 02.05.2016, Az. 137 C 450/15. Das Gericht ging von einer Fehlerquote bis zu 50% aus.

EUGH-URTEIL IN AUSSICHT ÜBER DEN VERKAUF GEBRAUCHTER E-BOOKS

Laut einem News-Beitrag der Rechtsanwaltskanzlei Waldorf Frommer steht eine Entscheidung des EuGH noch darüber aus, ob der Verkauf gebrauchter E-Books rechtmäßig wäre. In den Niederlanden währt nun bereits seit Jahren ein Rechtsstreit der örtlichen Verlage mit den Betreibern der Plattform „Tom Kabinet“. Diesbezüglich hat die „Rechtbank Den Haag“ mehrere Vorlagefragen formuliert, zu denen die Parteien noch bis zum 30.08.2017 Stellung nehmen können. Daraufhin bekommt der EuGH diese Fragen vorgelgt als Basis für ein Urteil.

In den Niederlanden hat mit TomKabinet.nl bereits seit dem Jahre 2014 eine Second-Hand-Plattform für „gebrauchte“ E-Books ihren Betrieb aufgenommen. Der Verkauf der dort angebotenen digitalen Bücher soll rechtlich einwandfrei sein. Deshalb sind beim Verkauf einige Regeln zu beachten: Verkäufer und Käufer müssen sich registrieren, um ein E-Book (ver-)kaufen zu können. Weiterhin dürfen nur E-Books im ePub-Format verkauft werden, die bei den holländischen Händlern E-Book.nl und BOL.com legal erworben wurden. Eine spezielle Software soll dazu noch sicherstellen, dass die E-Books bei den Verkäufern von der Festplatte komplett gelöscht werden. Die E-Books werden mit einem neuen Wasserzeichen versehen, sodass ein illegales Kopieren unmöglich gemacht werden soll. Fraglich wäre jedoch, wie realistisch solche Maßnahmen sind, denn ein Missbrauch wäre keineswegs ausgeschlossen. Auch wenn die E-Books auf der Festplatte des Verkäufers gelöscht werden, könnten sie ja

noch auf einem anderen Datenträger bei ihm gespeichert sein.

Der niederländische Verlegerverband (GAU/NUV) klagte gleich unmittelbar nach der Eröffnung vor Gericht. Tom Kabinet berief sich auf ein EU-Urteil aus dem Jahr 2012, nach dem der Weiterverkauf von Software legal sei. Der Verlegerverband hingegen verwies auf ein Urteil des Landgericht Bielefeld aus dem Jahr 2013, gemäß dem sich dieses EU-Urteil wirklich nur auf Software beziehe (geklagt hatte damals die Verbraucherzentrale gegen einen deutschen Store). Das Amsterdamer Gericht hat diese Klage gegen Tom Kabinet abgewiesen, der Wiederverkauf von E-Books sei unter bestimmten Umständen legal. Das EU-Urteil sei nicht eindeutig, argumentierten die Richter. Der Chef des Verlegerverbandes zeigte sich in einer Pressemitteilung "überrascht" von dem Urteil und kündigten daraufhin weitere Schritte an.

Hier in Deutschland gibt es zwei relevante Urteile dazu: Zum einen das Urteil des Oberlandesgerichts (OLG) Hamm vom Mai 2014 und zum anderen das Urteil vom OLG Hamburg vom 24.03.2015. Für Hörbücher hatte das OLG Hamm im Jahr 2014 entschieden, dass für sie keine Erschöpfung eintritt, sie also nicht frei weiterverkauft werden dürfen (OLG Hamm, Urt. v. 15.5.2014, Az. 22 U 60/13). Das OLG Hamburg hat für E-Books ebenso entschieden (OLG Hamburg, Hinweisbeschl. v. 4.12.2014, Az. 10 U 5/11).

Es gilt für physische Produkte, wie Bücher oder CDs, dass man mit dem Kauf automatisch zum Eigentümer wird. Das umfasst auch einen beliebigen Weiterverkauf. In dem Fall sprechen Juristen von einem Erschöpfungsgrundsatz. Ob dies jedoch auch für immaterielle Güter, wie MP3s, Software oder E-Books gilt, ist immer noch umstritten. In Deutschland gilt bisher: Man kauft ein E-Book nicht, sondern erwirbt nur ein unbegrenztes Nutzungsrecht. Das Nutzungsrecht wiederum gilt ausschließlich nur für den Käufer. Das gekaufte E-Book darf folglich nicht weiter veräußert werden. Schriftlich fixiert ist das in der Regel in den AGBs der jeweiligen E-Book-Anbieter und mit dem Kauf eines E-Books erklärt man sich automatisch damit einverstanden. Folglich ist der Weiterverkauf von E-Books in Deutschland nach der momentan geltenden Gesetzeslage nicht legal.

Allerdings steht diesbezüglich noch eine Entscheidung des Europäischen Gerichtshofs aus, scheint aber jetzt in greifbarer Nähe. Auf der Blogseite der Anwaltskanzlei Waldorf Frommer ist dazu zu lesen, dass man aus hiesiger Sicht davon ausgehen kann, „dass der EuGH eine „digitale Erschöpfung" ablehnen wird.", denn bereits aus den Erwägungsgründen der Urheberrechtsrichtlinie (2001/29/EG) ergibt sich, dass der Gesetzgeber an körperliche Vervielfältigungsstücke dachte: „Der unter diese Richtlinie fallende Urheberrechtsschutz schließt auch das ausschließliche Recht ein, die Verbreitung eines in einem Gegenstand verkörperten Werks zu kontrollieren. Mit dem Erstverkauf des Originals oder dem Erstverkauf von Vervielfältigungsstücken des Originals in der Gemeinschaft durch den Rechtsinhaber oder mit dessen Zustimmung erschöpft sich das Recht, den Wiederverkauf dieses Gegenstands innerhalb der Gemeinschaft zu kontrollieren."

STAATSTROJANER KOMMT NOCH IN DIESEM JAHR ZUM EINSATZ

Das Bundeskriminalamt (BKA) hat die Entwicklung des Staatstrojaners fast vollendet und will diesen noch gegen Ende des Jahres 2017 zum Einsatz bringen. In der aktuellen Version wird er auch die Überwachung von mobilen Betriebssystemen ermöglichen, wie Smartphones und damit vollen Zugriff auf Messenger-Apps, wie WhatsApp gewährleisten. Das geht aus einem als geheim eingestuften Bericht des Innenministeriums hervor, den Netzpolitik.org veröffentlicht hat.

Bereits vor einem Monat hat der Bundestag grünes Licht zu einer massiven Ausweitung des Einsatzes von Staatstrojanern gegeben. Das im Eilverfahren durch Parlament getriebene Gesetz erlaubt es künftig den Ermittlern, in einer Vielzahl von Fällen verschlüsselte Internet-Telefonate und Chats über Messenger, wie WhatsApp, Signal, Telegram oder Threema rechtlich abgesichert zu überwachen. Ferner dürfen sie beim Verdacht auf „besonders schwere Straftaten" komplette IT-Systeme, wie Computer oder Smartphones ausspähen. Dafür werden die Geräte der Betroffenen mit dem Staatstrojaner infiziert. Grundrechtsschonende Alternativen will das BKA geprüft haben, die gäbe es jedoch nicht.

Gemäß dem Bericht des Innenministeriums hat die Entwicklung des Staatstrojaners oder Remote Communication Interception Software 2.0 (RCIS) schon 2016 begonnen und sie soll noch 2017 freigegeben werden. Der Vorgänger, RCIS Version 1.0, konnte nur Skype auf Windows abhören, die Version 2.0 kann zudem nun auch Messenger auf mobilen Plattformen wie Android, iOS und Blackberry überwachen.

Zum Zwecke der Redundanz, wie für den Entdeckungsfall der eingesetzten Software, wurde die zusätzlich kommerziell beschaffte Quellen-TKÜ-Software „FinSpy“ durch den Hersteller FinFisher auf die neuen Erfordernisse hin angepasst. Eingekauft wurde diese Software bereits im Oktober 2012, als Konsequenz nach dem Staatstrojaner-Debakel im Jahr 2011. Auch für sie ist eine Freigabe des Einsatzes durch das Bundesministerium des Innern geplant, insofern die durchgeführten Tests positiv verlaufen. Mit FinSpy lassen sich Windows-Systeme, Rechner mit macOS und Linux attackieren, sowie die mobilen Plattformen Android, iOS, BlackBerry, Symbian und Windows Mobile.

Insbesondere diesen Einsatz der kommerziellen Software bewerten Netzaktivisten sehr kritisch. Bei FinSpy handele es sich laut Netzpolitik.org um eine „immens mächtige“ Hacker-Software, die mehr können würde, als das Gesetz erlaube. Ein weiteres Problem ist zudem noch die Kontrolle. So äußerte der CCC-Sprecher Falk Garbsch gegenüber netzpolitik.org: „Sobald die Zugriffsmöglichkeiten per Gesetz in Kraft sind, schert sich niemand mehr um die Versprechen, die einst gegeben wurden: Jetzt werden zum Staatshacken wieder Dienstleistungen von Unternehmen in Anspruch genommen, in die kein Beamter oder Kontrolleur hineinschauen durfte. Man vertraut stattdessen den Zusicherungen und Präsentationen von kommerziellen Anbietern, deren Leumund nur unter Diktatoren fabelhaft ist.

Das staatliche Hacken weiterhin als eine bloße Überwachungsmaßnahme wie jede andere zu verkaufen, ist angesichts der jetzt veröffentlichten Papiere eine dreiste Entstellung der Wahrheit. Kaum ist das Staatstrojaner-Gesetz durch den Bundestag, geht der Staat einerseits auf Shopping-Tour bei mehr als zweifelhaften Anbietern und lässt sich andererseits bei seiner Trojaner-Eigenentwicklung von niemandem in die Karten schauen. Wie nebenbei wird ein Trojaner-Arsenal aufgebaut, als sei es schon normal, dass der Staat die Digitalhirne seiner Bürger hackt.“

Sowohl Juristen, als auch Bürgerrechtler halten das Gesetz in diesem Umfang für verfassungswidrig, Klagen wurden bereits angekündigt. Ein weiterer Kritikpunk ist, dass Behörden durch den Staatstrojaner Sicherheitslücken ausnutzen würden, die auch Kriminelle missbrauchen können.

HÖCHSTGERICHT: ÜBERWACHUNG VON KIM DOTCOM ILLEGAL

Freute sich Kim Dotcom unlängst erst über die Zurückerlangung seiner Vermögenswerte, denn kürzlich entschied ein Gericht in Hongkong, dass Dotcom dort beschlagnahmtes Vermögen zurückbekommt, so kann er nun einen erneuten Erfolg für sich verbuchen. Dotcom wurde laut Dokumenten des neuseeländischen Nachrichtendienstes Government Communications Security Bureau (GCSB) illegal von der US-amerikanischen National Security Agency (NSA) überwacht. Offensichtlich war laut dem neuseeländischen High Court die Überwachung aller Beteiligten nicht rechtens. Laut DIE WELT könnte diese Aktion dazu führen, dass Dotcoms Auslieferung an die USA scheitert.

Bereits vor kurzem wurde bekannt, dass Dotcom laut Dokumenten des neuseeländischen Nachrichtendienstes Government Communications Security Bureau (GCSB) illegal von der US-amerikanischen National Security Agency (NSA) überwacht worden ist. Die illegale Abhöraktion wurde durch Gerichtsdokumente bekannt, die im Zusammenhang mit dem Auslieferungsverfahren gegen Dotcom veröffentlicht wurden.

Das GCSB hat dem neuseeländischen High Court mitgeteilt, dass es zunächst zusammen mit der NSA bei Dotcom mitgehört habe, die Überwachung aber Anfang 2012 beendet war. Den Unterlagen zufolge hat das GCSB Telefonanrufe und E-Mails zwischen Dotcom und seinem Mitarbeiter Bram der Volk verfolgt. Ein Teil Dotcoms Kommunikation sei jedoch weiterhin ohne Wissen des GCSB mit dessen Technik abgehört worden. So wurde Dotcom insgesamt in der Zeit vom 16. Dezember

2011 bis zum 22. März 2012 überwacht. Das sind zwei Monate länger als der frühere Premierminister John Key eingestanden hatte, für diese zwei Monaten war offenbar die NSA allein verantwortlich. Premierminister John Key räumte ein, dass die Aktion des GCSB illegal war und kündigte eine Untersuchung an: „Ich erwarte, dass unsere Geheimdienste sich stets in den Grenzen bewegen, die das Gesetz vorgibt“, erklärte er.

Generell ist ist dem GCSB verboten, neuseeländischen Bürger auszuspionieren, das gilt ebenso für Menschen, die wie Kim Dotcom den Status als „Permanent Resident“, also dauerhafter Einwohner/Bürger, haben. So muss der GCSB seine Beteiligung an der Durchsuchung der Villa von Dotcom offenlegen. Als die Überwachung bekannt wurde, hat Dotcom rechtliche Schritte in die Wege geleitet und wollte Zugriff auf die entsprechenden Informationen erlangen. Nun hat das neuseeländische Höchstgericht festgestellt, dass diese Überwachungsaktionen nicht rechtens waren.

Kim Dotcom, war auf US-Antrag 2012 nahe Auckland vorübergehend festgenommen worden. Die US-Ankläger gaben an, Musik- und Filmproduzenten hätten eine halbe Milliarde Dollar an Lizenzgebühren verloren, weil Nutzer über Dotcoms Plattform Megaupload urheberrechtlich geschütztes Material ausgetauscht haben sollen. Dotcom befürchtet nun schon seit Jahren, wegen Urheberrechtsstreitereien in die USA ausgeliefert zu werden. Wegen dieses Vorwurfs wurde die Plattform Megaupload auf Betreiben des US-Justizministeriums Anfang 2012 geschlossen, Dotcoms Villa durchsucht, seine Rechner und Speicher beschlagnahmt. Zuletzt erlaubte das oberste Gericht Neuseelands eine Auslieferung Dotcoms an die USA. Dem 43-Jährigen droht im Falle einer Abschiebung in die USA eine Strafe von maximal 20 Jahren wegen krimineller Geschäfte. Die US-Regierung wirft Dotcom unter anderem Geldwäsche, Erpressung und Betrug mittels elektronischer Kommunikationsmittel vor.

Der illegale Lauschangriff könnte nach einem Bericht der neuseeländischen Tageszeitung „Dominion Post“, wie Die Welt mitteilt, nun das Auslieferungsverfahren zum Scheitern bringen. Die Anwälte von Dotcom können aufgrund der Entwicklung einen Stopp des Verfahrens verlangen, das eigentlich im kommenden März mit Anhörungen fortgesetzt werden sollte. Rechtsanwalt Peter Williams meinte: „Ich würde vom Gericht verlangen, dass Kim Dotcom wegen des massiven Fehlverhaltens der Strafverfolger nicht abgeschoben wird“.

Erst vor einigen Tagen wurde „Kim Dotcom: Caught in the Web“ veröffentlicht und bereits nach kurzer Zeit führte der Film die Download-Film-Charts an. Es geht darin um das Leben des Internetunternehmers, das ja untrennbar mit dem Filehoster Megaupload verbunden ist und all den Geschehnissen, die diese Gründung so nach sich zog. Laut TorrentFreak ist die Doku über Dotcom bereits auf auf Pirate Bay & Co. aufgetaucht. Da man den Film allerdings ausschließlich im US-iTunes-Store kaufen kann, zeigte Dotcom deshalb auf Twitter Verständnis für alle, die den Film über nicht offizielle Quellen beziehen.

OLG MÜNCHEN: ADBLOCKER VERSTOSSEN NICHT GEGEN GELTENDES RECHT

Laut Pressemitteilung des Oberlandesgerichts (OLG) München vom 17.08.2017 verstoßen Ad-Blocker nicht gegen Kartell-, Wettbewerbs- und Urheberrecht. Damit wies das Gericht am Donnerstag in drei Parallelverfahren die Klagen mehrerer Webseitenbetreiber gegen den Kölner Adblock-Plus-Anbieter Eyeo zurück und bestätigte damit zugleich die Urteile früherer Instanzen.

Süddeutsche Zeitung, ProSiebenSat.1 und die RTL-Tochter IP Deutschland haben im Kampf gegen ein Programm, das Werbung im Internet blockiert, eine Niederlage vor dem OLG München hinnehmen müssen und im Gegensatz zum Oberlandesgericht Köln sehen die Münchner Richter in dem bezahlten Whitelisting unaufdringlicher Anzeigen auch keine verbotene aggressive Werbung.

Das Thema Adblocker sorgt seit Jahren für anhaltende Diskussionen zwischen Nutzern, Anbietern der Werbeindustrie und den Entwicklern dieser Anwendungen zur Ausblendung von Werbeanzeigen. Mit einem Urteil des Münchner Oberlandesgerichtes (OLG) vom Donnerstag steht nun fest: Die Kölner Eyeo GmbH darf ihren Dienst AdBlock Plus (ABP) weiterhin anbieten. Auch das umstrittene Geschäftsmodell, Werbung durch den Eintrag in eine sogenannte „Whitelist“ gegen Geld wieder zu ermöglichen,

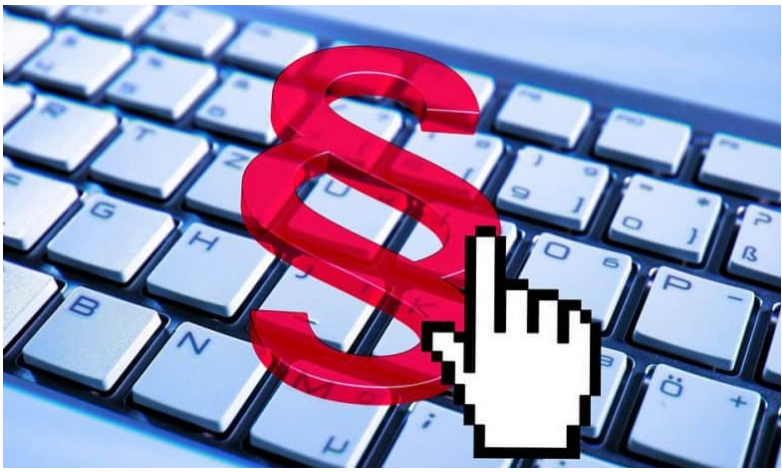
halten die Münchner Richter für rechtmäßig (Urt. v. 17.08.2017, Az. 29 U 1917/16, U 2184/15 Kart, U 2225/15 Kart). Die kartellrechtlichen Forderungen verneinte das OLG ebenfalls: Denn dazu fehle es Eyeo an der „marktbeherrschende Stellung auf dem Markt des Zugangs zu allen Internetnutzern für Werbung“.

Bereits seit 2011 vertreibt Eyeo die für den Nutzer unentgeltliche Open-Source-Software „AdBlock Plus“. Der Dienst dient der Unterdrückung von Werbeeinblendungen beim Aufruf einer Internetseite. Das Programm selbst besitzt keine eigene Filter-Funktionalität, sondern muss mit Vorgaben ergänzt werden, welche Inhalte blockiert werden sollen. Diese sind in sogenannten Filterlisten („Blacklists“) enthalten, die dem Nutzer standardmäßig vorgeschlagen werden. Nach dem Download ist der Adblocker so eingestellt, dass Werbung, die nach seinen Kriterien als nicht störend eingestuft wird („Whitelist“), angezeigt werden kann. Jeder Webseitenbetreiber hat die Möglichkeit, am „Whitelisting“ teilzunehmen und seine Seiten von Eyeo freischalten zu lassen. Von Betreibern größerer Webseiten verlangt Eyeo dafür eine Lizenzzahlung.

Eyeo wurde wegen des Adblockers aktuell von den drei Klägern unter anderem Marktmissbrauch, Verstöße gegen Urheberrechte und Aushöhlung der Pressefreiheit vorgeworfen. Ferner nötige Eyeo die Werbeindustrie, teure Verträge zur Durchleitung der Anzeigen abzuschließen. Die sich daraus ergebenden Forderungen: Neben der Einstellung des Vertriebs des AdBlock Plus müsste auch die Erstellung der Blockliste Easylist verboten werden. Darüber hinaus sahen die Kläger auch Anlass zur Erhebung von Schadensersatzansprüchen wegen entgangener Werbegewinne. In München wurden jetzt alle diese Ansprüche abgelehnt.

Wegen einer abweichenden Entscheidung des OLG Köln zu den wettbewerbsrechtlichen Ansprüchen wurde jedoch eine Revision zum Bundesgerichtshof (BGH) zugelassen: Das OLG Köln hatte in seinem Urteil vom Juni 2016 das Geschäftsmodell von Eyeo für unzulässig erklärt. Demnach darf das Unternehmen kein Geld für die Aufnahme von Webseiten des Axel-Springer-Verlages in das sogenannte Acceptable-Ads-Programm verlangen. Das Blockieren von Anzeigen an sich hatte das OLG aber für zulässig erklärt. Die letzte Entscheidung in der Sache obliegt nun also dem Bundesgerichtshof (BGH). Eine Verhandlung wird für kommendes Jahr erwartet, ein Termin steht noch nicht fest.

Eyeo-Geschäftsführer Till Faida begrüßt die Entscheidung des OLG München: „Das Urteil bestärkt wieder einmal die Nutzerrechte, für die wir uns mit unseren Produkten einsetzen. Wir hoffen, jetzt außerhalb des Gerichtssaals einen konstruktiven Dialog mit den Verlagen und Website-Betreibern beginnen zu können“, meint er. Sein Unternehmen wolle nun Lösungen finden, „die für Nutzer und Anbieter gleichermaßen gut funktionieren“.



BUNDESARBEITSGERICHT: KEYLOGGER SIND NUR IN AUSNAHMEFÄLLEN LEGAL

Das Bundesarbeitsgericht Erfurt hat der Überwachung von Mitarbeitern am Arbeitsplatz in einem aktuellen Urteil Grenzen gesetzt. Es wurde entschieden, dass der Einsatz von „Keyloggern“ unzulässig ist (2 AZR 681/16). Das gelte nur dann nicht, wenn ein konkreter Verdacht auf eine Straftat oder eine schwerwiegende Pflichtverletzung des Arbeitnehmers bestehe.

Im verhandelten Fall hatte ein Arbeitgeber aus Nordrhein-Westfalen im Zusammenhang mit einer Freigabe eines Netzwerkes im eigenen Haus im April 2015 mitgeteilt, dass der gesamte Internetverkehr und die Benutzung ihrer Systeme mitgeloggt würden: „Hiermit informiere ich Euch offiziell, dass sämtlicher Internet Traffic und die Benutzung der Systeme der Company mitgelogged und dauerhaft gespeichert wird. Solltet Ihr damit nicht einverstanden sein, bitte ich Euch, mir dieses innerhalb dieser Woche mitzuteilen.“ Da kein Widerspruch gegen die angekündigten Maßnahmen erfolgte, ging die Firma davon aus, dass der Einsatz von Keylogger-Software akzeptiert wäre. Daraufhin wurde auf den Dienstcomputern der Mitarbeiter eine Software installiert, die nicht nur den Internetverkehr protokollierte, sondern darüber hinaus jede Tatatureingabe erfasste und speicherte. Zudem fertigte sie regelmäßig Screenshots an.

Anfang Mai, wenige Tage nach der Instllation des Programms, erhielt der 32-Jährige Kläger, ein seit 2011 bei der Firma beschäftigter Webentwickler, die Kündigung. Der Vorwurf

lautete, er begehe Arbeitszeitbetrug. Daraufhin räumte der Mitarbeiter ein, den Dienstcomputer während der Arbeitszeit privat genutzt zu haben, allerdings nur in geringem Umfang und in der Regel in den Pausen ein Computerspiel programmiert zu haben. Auch habe er täglich etwa zehn Minuten dazu verwandt, um den E-Mailverkehr für die Firma seines Vaters zu erledigen. Eine Pflichtverletzung wies er dennoch zurück. Die Datenerhebung mit dem Tastaturspion sei unzulässig gewesen. Der Angestellte klagte gegen die Kündigung.

Das Bundesarbeitsgericht hält die Beweise für das Fehlverhalten des Mannes nicht für verwertbar: Die durch den Keylogger gewonnenen Erkenntnisse über die Privattätigkeiten des Arbeitnehmers dürften im Gerichtsaal nicht verwendet werden. Gemäß § 32 Abs. 1 BDSG wäre eine solche verdeckte Überwachung und Kontrolle des Arbeitnehmers unzulässig. Ebenso haben schon die Vorinstanzen, das Arbeitsgericht Herne und das Landesarbeitsgericht Hamm, entschieden. Die Richter verweisen darauf, dass auch Arbeitnehmer am Arbeitsplatz ein Recht auf informationelle Selbstbestimmung haben. Eine derart engmaschige Überwachung verstoße gegen dieses Recht. „Jeder soll selbst über die Preisgabe persönlicher Daten entscheiden können. Dieses Recht gilt natürlich auch im Betrieb.“, sagte der Richter. Die Beklagte hatte beim Einsatz der Software gegenüber dem Kläger keinen auf Tatsachen beruhenden Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung. Die von der Firma „ins Blaue“ hinein veranlasste Überwachung sei unverhältnismäßig gewesen. Das Urteil gilt als Grundsatzurteil.

Zwar sei der Einsatz von Spähsoftware am Arbeitsplatz noch kein Massenphänomen, aber Gerichtspräsidentin Ingrid Schmidt meint, die Zahl ähnlich gelagerter Fälle am Bundesarbeitsgericht stiege an, denn: „Mit der Digitalisierung nehmen die Überwachungsmöglichkeiten zu“. Folglich wäre noch in diesem Jahr mit mehreren solcher Entscheidungen des Bundesarbeitsgerichts zu rechnen.

EUROPÄISCHE KOMMISSION: ERLEICHTERTER ZUGRIFF VON FAHNDERN AUF DATEN BEI FACEBOOK & CO. GEPLANT

Nach Auskunft der Bundesregierung auf eine kleine Anfrage der Linken beabsichtigt die Europäische Kommission Veränderungen hinsichtlich des Zugriffs auf Daten amerikanischer Kommunikationsdienstleister, wie Facebook und Google: Es sollen künftig innerhalb der Europäischen Union Ansprechpunkte eingerichtet

werden, eine Herausgabe der Daten durch US-Firmen darüber erfolgen, berichtet die „Rheinische Post“ in ihrer Samstagausgabe.

Die Strafverfolgungsbehörden würden in der Folge unmittelbar mit den in den USA ansässigen Unternehmen zusammenarbeiten, das förmliche Rechtshilfeverfahren wäre dadurch überflüssig. Unter Federführung des deutschen Bundeskriminalamts seien bereits Gespräche mit Facebook, Google, eBay und Microsoft geführt worden. „Einige Anbieter stellen dazu eigens entwickelte Abfrageportale zur Verfügung“, heißt es in dem Bericht der Bundesregierung. Die Bundesregierung prüft derzeit, ob mit dem Verfahren nur Nutzer-Adressen und Zeitpunkte der Kommunikation abgefragt werden sollen, oder auch Inhalte.

Zu diesem Zweck wird Ende Oktober das neue Portal „Sirius“ der Polizeiagentur Europol die Arbeit aufnehmen. Geplant ist, die Online-Ermittlungen der teilnehmenden Polizeibehörden dort zu bündeln.

Linken-Europapolitiker Andrej Hunko nannte es besorgniserregend, welchen Druck der Staat auf die Internetdienstleister ausübe. „Die Firmen werden zusehends zu Handlangern von Polizei und Diensten gemacht“, sagte er. Stattdessen müssten die Behörden transparenter machen, auf welche Weise sie Clouds und Messenger-Dienste überwachten. Die Umgehung des internationalen Rechtswegs zur Abfrage von Verkehrs-, Bestands- oder sogar Inhaltsdaten der Nutzer von Facebook & Co. sei ein „weiterer schwerer Eingriff in die Privatheit der Telekommunikation“, so Hunko.

Digital

Themenübersicht

LTE mit bis zu 500 Mbit/s – ein reiner Werbetrick

Unser anonymer Autor war früher Mitarbeiter des führenden Düsseldorfer Mobilfunkanbieters. Schon nach wenigen Wochen war klar, dass ihre Kunden als reines „Bezahlvieh" angesehen werden. In mehreren Beiträgen wird er auf Tarnkappe.info einige Hintergründe zu den Tricks der Mobilfunk-Branche beleuchten. Im ersten Artikel geht es um 500 Mbit pro Sekunde, und warum sich dieses Werbeversprechen bei näherem Hinsehen in nichts als heiße Luft auflöst.

Der Mobilfunkmarkt ist seit einigen Jahren komplett übersättigt mit Anbietern, die sich alle in Preis und Leistung gegenseitig zu unterbieten versuchen. Da ist augenscheinlich kaum noch Platz für Alternativen, oder irgendwelche echte Innovationen.

Leider gelten immer noch die Gesetze des Marktes, und die großen Premium-Unternehmen müssen sich irgendwie dennoch von der Konkurrenz absetzen. Anstatt sich dabei jedoch auf exzellenten Kundenservice, hochwertige Leistungen mit echtem Mehrwert oder revolutionäre Neutechniken zu verlassen, macht sich immer mehr eine andere Unsitte breit: Das Bewerben sinnloser Leistungen, die sich für den normalen Kunden in keiner Form nutzen lassen.

Bestes Beispiel ist hierfür die sogenannte „LTE-M*x"-Leistung der Anbieter V*******. und T-M****. Während o², kleinere Discounter und Reseller (Wiederverkäufer) wie Yourfone, sich einfach auf die grundlegenden Leistungen besinnen, versuchen sich die beiden vermeintlichen Topanbieter in Werbeversprechen, die zwar auf dem Papier gut aussehen: Surfgeschwindigkeiten von bis zu 500 Mbits werden versprochen, schneller als mit beinahe allen gängigen DSL- und Kabelverbindungen.

Warum ich das als Unfug ansehe, möchte ich in diesem Artikel etwas näher beleuchten. Dabei tasten wir uns zuerst an die simplen Grundlagen heran und gelangen dann sukzessive zu den größeren Problemen.

Falle Nr. 1: 500 Mbit – eine Leistung, die es fast nirgendwo gibt

Wenn in der Werbung von maximaler Geschwindigkeit gesprochen wird, wird meistens verschwiegen, dass es sich dabei lediglich um ein theoretisches Maximum handelt, dass höchstens an einigen, wenigen Standorten erreicht werden kann. Das liegt daran, dass die entsprechende Technik relativ teuer ist, und daher zu Beginn immer nur an wenigen Ballungspunkten angekauft wird.

In kleineren, abgelegeneren Gebieten gibt es oft nur die herkömmliche LTE-Abdeckung. Nicht schlecht, aber eben auch nicht „Fullspeed". Es scheint fast so, als finanzierten sie mit ihrem überhöhten Tarif lediglich einige wenige, glückliche Großstadtbewohner, die sich über entsprechend schnelle Transfer-Raten freuen dürfen.

Falle Nr. 2: 500 Mbit/s – eine Leistung, die keiner braucht

Im Mobilfunknetz surfen die meisten Nutzer auf Webseiten, laden gelegentlich vielleicht noch eine App herunter, sehen sich auf YouTube um. In den wenigsten Fällen kommen Sie jedoch auf die Idee, ihr Smartphone an den Computer anzuschließen und so unterwegs online zu gehen (was in vielen Fällen sogar vom Mobilfunkanbieter verboten wird), oder einen großen Download zu starten. Was denn auch? Wer lädt schon auf seinem Handy große Dateien hoch, betreibt Videoschnitt ohne Komprimierung oder verschickt Softwarepakete?

Selbst wenn ein Nutzer einmal auf die Idee kommt, beispielsweise ein großes Spiel aus dem Appstore über LTE herunterzuladen, warnt das iPhone direkt vor: Wollen Sie diese Datei nicht doch lieber per WLAN herunterladen? Ihr Datenvolumen könnte sonst schnell aufgebraucht sein!

Ein Schelm, wer Böses denkt. Zu was ist diese sogenannte Leistung denn nun wirklich zu gebrauchen?

Falle Nr. 3: 500 Mbit – eine Leistung, die es nicht für alle gleichzeitig gibt

Unter welchen Bedingungen sind die „Höchstgeschwindkeiten" denn überhaupt zu gebrauchen? Dazu ist es erst einmal wichtig, kurz zu erklären, wie eine Funkzelle in etwa funktioniert. Im ganzen Land sind diese Masten verteilt, und das Handy ist immer in genau eine eingebucht.

Innerhalb einer Zelle gibt es eine gewisse, maximale Bandbrei-

te, die sich alle Teilnehmer teilen müssen. Das bedeutet, dass für die Erreichung der Maximalgeschwindigkeit aus der Werbung auch die notwendigen Ressourcen zur Verfügung stehen müssen. Leider ist das oftmals nicht der Fall: Selbst unter Idealbedingungen können immer nur einige wenige Nutzer die volle Bandbreite gleichzeitig nutzen, ehe das System eingreifen muss und die verfügbare Geschwindigkeit unter den Kunden aufteilt.

Falle Nr. 4: Schlechte Verbindung – Wenn der Empfang nicht perfekt ist

Nehmen wir nun einmal an, Sie stehen mit Ihrem Handy gerade in der richtigen Zelle, die zufälligerweise die versprochenen 500 Mbit erreicht. Zufällig ist es gerade 3 Uhr morgens, die ganze Welt schläft, und alle anderen in Ihrem Umkreis haben gerade das Handy aus oder nutzen es nicht.

Freudig schalten Sie das Handy ein und starten einen Download. Doch, oh Wunder: Die maximale Geschwindigkeit wird immer noch nicht erreicht. Sie prüfen irritiert den Server, von dem Sie die Datei gerade beziehen, und stellen fest, dass dieser nicht das Problem darstellt.

Was ist geschehen? Die Bandbreite von 500 Mbit wird natürlich nur dann erreicht, wenn der Empfang gerade beinahe perfekt ist. Probieren Sie doch mal, auf die dunkle Straße zu laufen und bis gerade vor den Sendemast zu laufen. Direkt unter dem Mast ist Empfang allerdings noch schlechter, daher sollten Sie vielleicht noch ein wenig hin- und herlaufen, bis endlich alle Balken an der Verbindungsanzeige erscheinen.

Steht kein Baum, kein Busch, kein Laternenpfahl mehr im Weg? Herzlichen Glückwunsch, 500 Mbit sind erreicht! Vergnügt schalten Sie den Download ein und…

Falle Nr. 5: Das leidige Datenvolumen

… nach wenigen Minuten kommt die SMS. „Sehr geehrter Kunde, Ihr Datenvolumen ist aufgebraucht. Bitte laden Sie es für nur 5 Euro pro 1 GB auf, um mit maximaler Geschwindigkeit weitersurfen zu können. Ansonsten werden Sie auf maximal 32 Kbit (!) gedrosselt.“

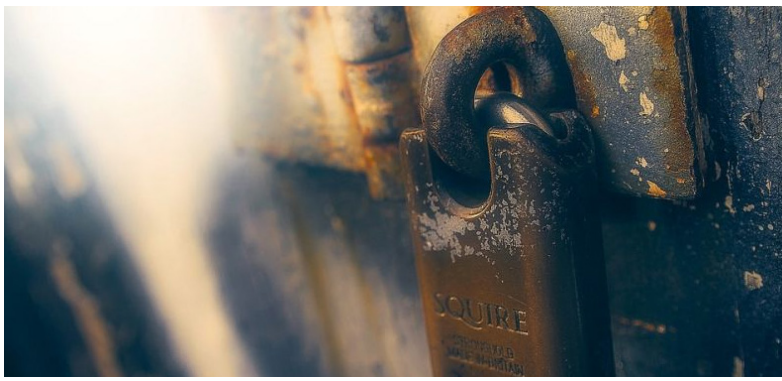
Haben Sie etwa vergessen, dass Ihr Tarif nur maximal einige, wenige Gigabyte beinhaltet? Was mit einer normalen Geschwindigkeit schon sehr schnell zum Hindernis wird, ist mit bis zu 500 Mbit ein Garant für entweder sehr kurzes Vergnügen oder eine sehr hohe Handyrechnung, denn Sie schaufeln ca. 4 GB auf Ihre Festplatte – pro Minute!

Damit saugen Sie selbst das aktuell größte Datenpaket (Stand 10.08.2017) für Privatverbraucher, den Bl*ck-Tarif, innerhalb von 7,5 Minuten (!!) leer. Die einzige Ausnahme bieten hier einige, wenige, sehr teure Tarife mit unbegrenztem Datenvolumen. 200 Euro legen Sie dafür bei der Deutschen Telekom (T-Mobile) hin. Für alle anderen heißt es: Zahlen, bis der Arzt oder der Schuldnerberater Peter Zwegat mit RTL2 im Schlepptau, bei Ihnen vorbeikommt.

Fazit: Eigentlich sind 500 Mbit pro Sekunde für die wenigsten Kunden interessant.

Selbst wenn Sie zufällig zur richtigen Zeit am richtigen Ort sind, ist es doch relativ unwahrscheinlich, dass irgendjemand einen großen Nutzen von der hohen Bandbreite hat, der nicht gerade ein gut situierter Geschäftskunde ist. Sollten größere Bandbreitenreserven zur Verfügung gestellt werden, und sich vor allem das völlig überteuerte Datenvolumen ein wenig weiter erhöht, wird die Sache vermutlich anders aussehen.

So jedoch ist das Ganze momentan nicht mehr, als ein bloßer Werbegag.



MASS EFFECT: ANDROMEDA: WELTRAUM-ABENTEUER MITTELS PATCH 1.09 NUN OHNE DENUVO-KOPIERSCHUTZ

Mit dem Patch 1.09 haben Electronic Arts und Bioware die Kopierschutz-Software Denuvo aus Mass Effect: Andromeda entfernt. Die Änderung lässt sich allerdings nicht in den Patch-Notes finden. So wurde bereits die Frage laut, ob es sich dabei um eine dauerhafte Entscheidung oder eher um ein Versehen gehandelt hat, berichtet DSOGaming.

Mass Effect: Andromeda erschien am 23. März 2017 für PC, Playstation 4 und Xbox One. Nun steht für Mass Effect:

Andromeda der Patch 1.09 zum Download bereit. Mit dem vor wenigen Tagen herausgegebenen Update werden sowohl einige Verbesserungen der bereits viel kritisierten Gesichtsanimationen und der Filmsequenzen vorgenommen, sowie auch sonstige Probleme behoben. Zudem haben die Entwickler den Mehrspieler-Modus mit der Platin-Schwierigkeit und einer „neuen, gemischten feindlichen Gruppierung“ erweitert.

Jedoch brachte der Patch 1.09 gleichzeitig eine Entfernung des Denuvo-Kopierschutzes. Das Action-RPG wird zwar immer noch durch Electronic Arts hauseigenes DRM-Online-System Origin geschützt, doch mit Denuvo verschwindet zugleich ein häufiger Kritikpunkt von Seiten der Gaming-Community: Der Kopierschutz erforderte zeitweise eine Internetverbindung. Auf diese Weise prüfte Denuvo, ob die gespielte Version legal und aktiviert ist. Einige Spieler haben jedoch nicht ständig Zugriff auf das Internet und sollten die Server von Denuvo einmal nicht erreichbar sein, wäre ein Zugriff auf das jeweilige Spiel dann nicht mehr möglich.

Mit dem Entfernen des Denuvo-Kopierschutzes schließt sich Mass Effect: Andromeda nun einer Reihe von Spielen an, für die die Entwickler den Kopierschutz genau dann entfernt haben, sobald dieser für ihre Spiele geknackt wurde. Dazu gehörten bisher schon DOOM, HITMAN, RiME und Homefront: Die Revolution.

HELLBLADE: SENUAS’S SACRIFICE OHNE DRM

Das britische Studio Ninja Theory, die Entwickler von Hellblade: Senuas’s Sacrifice, haben sich gegen einen DRM-Schutz in ihrem Spiel entschieden. Mit ihrer neuesten Kreation wollen sie zudem beweisen, dass es mehr gibt als nur Blockbuster Spiele zu Blockbuster-Preisen oder Nischentitel für den kleinen Geldbeutel. Mit Hellblade: Senua’s Sacrifice kündigen sie ein Action-Adventure an, mit dem sie AAA-Qualität in kleinerem Rahmen, zu kleinerem Preis bieten wollen. Das Spiel Hellblade: Senuas’s Sacrifice ist neben Steam und der PS4 auch auf GOG.com erschienen – und damit ohne DRM-Schutz. In einem Interview mit GameStar geben die Spieleentwickler bekannt, dass sie sich der Gefahren der Piraterie bewusst sind und sich dennoch für eine DRM-freie Version des Spieles entschieden haben: „Ja, aber das ist eine schwierige Entscheidung: Es wird wahrscheinlich sowieso dazu kommen und in dieser Situation sorgt man dafür, dass ausgerechnet die ehrlichen Käufer einen Nachteil haben. Wir haben uns den DRM angesehen und versuchen, den Spielern so viel guten Willen wie möglich zu zeigen, weil Hellblade die Art von Spiel ist, das sich nur mit gutem Willen verkauft und überleben kann, ohne aggressives Marketing und sowas.“

Digitale Inhalte sind leicht zu kopieren, zum Schutz kommen deshalb häufig DRM-Lösungen zum Einsatz. Doch bringt ein DRM-Schutz zum einen Konsumenten oftmals Nachteile und wird von vielen Nutzern deshalb als reine Schikane angesehen. Zum anderen hält ein solcher Schutz Piraten nur selten auf. Früher oder später landen die Spiele alle inklusive Crack auf einschlägigen illegalen Plattformen, selbst der „unknackbare“ Denuvo-Kopierschutz wird mittlerweile binnen kürzester Zeit ausgehebelt. Aus diesen Gründen hat sich das Entwicklerstudio Ninja Theory bei ihrem neuesten Spiel gegen DRM entschieden. Sie hoffen vielmehr auf den guten Willen der Spieler. Raubkopien will man mit niedrigen Verkaufspreisen entgegenwirken. Hellblade ist seit dem 8. August zu günstigen 30 Euro erhältlich, zusätzlich habe man Preisanpassungen je nach Region vorgenommen: „Unser Gedanke dabei ist, dass es durch den fairen Preis weniger raubkopiert wird und mehr Leute das Spiel kaufen, weil sie eine Wahl haben.“, so die Spieleentwickler. Da das Spiel aktuell die Top-Seller auf GOG.com anführt und bei Steam auf Platz 3 liegt, hatte Ninja Theory mit dieser Strategie wohl Erfolg.

PRINZIPIA ICO BRICHT ALLE REKORDE.

In einer kurzen Erklärung gab der Internetunternehmer Andreas Köppen (der Ältere) auf der WEB-Site des Andreas „Andi“ Köppen (der Jüngere) www.andisseite.com den Start einer neuen Internetwährung bekannt. Der Coin basiert auf einer handschriftlichen Notiz zur allgemeinen Verwirrung. Der Kurs wird täglich neu festgesetzt und über Twitter bekanntgegeben. Die Ausgabe ist ab sofort möglich. Hierzu schreibst du dem Herausgeber eine Email. Die Coin-Wallets gehen dann zum aktuellen Tageskurs raus. Genaue Infos gibt es auf der Anbieterseite. Man gehe aber von einem „exponentiellen,

wenn auch nicht durchweg linearem Wachstum“ aus, so Köppen (der Ältere) und weiter: „…ja leckt mich am Arsch, wenn der Wert sich nicht innerhalb eines jeden Monats verdoppelt!“.

Der Boom alternativer Coins ist ungebrochen. Der Bitcoin-Kurs liegt aktuell bei über 3400 Dollar, ETH gibt`s für 330 Dollar. Seit Donnerstag, 16.00 Uhr bietet ein norwegisches Unternehmen mit Sitz in Singapur https://www.hubii.network/ eine neue Möglichkeit für Venturekapital an. Man hofft hier auf fünf bis 50 Mio. Dollar. Schon im Vorfeld machte der bestbezahlte Sportler der Welt Floyd „Crypto“ Mayweather Reklame auf Twitter, wo er über 20 Mio. Folllower hat.

Bezahlt werden die sogenannten Hubiits mit ETH. Mit Hubiits kann man dann auf dem hauseigenen Marktplatz für News, Musik, Film, und Sport, dem Hubii-Network, bezahlen.

Aber Achtung! Diese Art der Geldbeschaffung breitet sich gerade wie ein Steppenbrand im World Wide Web aus. Will man hier den aktuellen „Internet-Hype“ ausnutzen, um auf Kosten der „armen“ Venturekapitalisten Kasse zu machen? Skeptiker warnen bereits vor den Gefahren einer neuen „Dotcom-Blase“ und verweisen auf die derzeit günstigen Gold- und Silberpreise. Köppen hingegen ist von der soliden Basis von PRINZIPIA überzeugt, fuße sie doch auf einem unerschöpflichen Fundament. Also lauft und kauft (was auch immer)!

YIPPIE YA YEAH, IRC!

Wie ich einen heute fast schon vergessenen Teil des Internets betrat und was es mit mir machte, als ich ihn fand. Es gibt nicht nur das Darknet. Deshalb möchte ich hier mal auf einen, heute fast schon vergessenen Bereich des Internets hinweisen, indem es immer noch Schätze zu finden gibt. Dem IRC oder „Internet Relay Chat“.

In den 80-igern, noch bevor das WWW oder „World Wide Web“ groß heraus kam, wurde hier schon gelesen, getauscht, gehandelt, gefrutzelt. Warez gab es aus dem IRChat. Denn mithilfe einer kleinen Software konnte man hier nicht nur Chatten, sondern auch Dateien tauschen. Zu beginn hatte man es hier vorwiegend mit abgeschotteten Hackergruppen zu tun, die in geschlossenen Bereichen/ Gruppen agierten.

Doch spätestens seit den 90-igern hatte es sich herumgesprochen, der IRC wurde Mainstream. Plötzlich öffneten sich Gruppen, neue wurden erstellt und der Freund/ Kollege, der die eine oder andere Raubkopie aus seinem Schreibtisch heraus handelte, bekam plötzlich Konkurrenz im IRC. Hier gab es nichts, was es nicht gab. Doch am interessantesten war der Informationsaustausch. Hier konnte man sich stundenlang aufhalten und es wurde nie langweilig. Es waren wohl eher Tage und Nächte. Irgendwann war der Mainstream, der damit begonnen hatte hier Hausfrauenprobleme, Kuchenrezepte und Monatsbeschwerden zu diskutieren, weiter gezogen. Man war wieder unter sich. Doch das machte den IRC nicht weniger interessant. Ganz im Gegenteil. Viele waren nie weg, und ich? Ich bin wieder hier. Mit IRSSI, einem Client für den IRC, mache ich erneut mystische Erfahrungen.

Wer sich einen Eindruck verschaffen will, tut das mit einem IRC-Clienten z.B. XChat: http://www.xchat.org oder HexChat: https://hexchat.github.io. Du bist Linuxer und arbeitest lieber am Terminal? Dann sei dir http://www.irssi.org wärmstens empfohlen: >>sudo apt-get install irssi<< ! Es ist eine Messe! #freenode ist ein beliebter Server. Guckt dich ein bisschen um, und finde einen Bereich, der deinen Interessen entspricht. Spätestens jetzt sei darauf hingewiesen, dass auch hier nach den Regeln des guten Benehmens zu handeln ist. Nettikette! Im Kanal #d03 findet ihr zum Beispiel den „Harten Kern“ der deutschen Debian-Entwickler-Szene versammelt. Banknetzwerker, Versandhaus-Gurus, Hochschullehrer, Politiker, Journalisten, Telekommunikationsbosse u.v.m. Hier fließen Informationen, wertvoll wie Goldstaub, manchmal banal, meistens aber hoch informativ, lehrreich und high class.

Andere Gruppen heißen #ubuntu, #freakshow oder #berlin.

Einige Server lassen den Zugang über das Tor-Netzwerk zu, andere nicht, wieder andere erschweren den Zugang beträchtlich. Deshalb klärt gleich zu Beginn ab, ob der jeweilige Hoster euren Sicherheitsbedürfnissen entspricht, noch bevor ihr euch in einer Gruppe geborgen fühlt. Du hast einen freundlichen Anbieter? Dann ist das der Weg:

Suche im Meny so etwas wie Einstellungen, Settings oder Preferences. Gehe zu Netzwerk oder Netzwerkeinstellungen. Dort aktiviere Proxy und gib Hostname: 127.0.0.1 und Port: 9150 für Tor-Browser-Bundle ein. Ansonsten 9050. Type: Socks5. Aktiviere Proxy for All Connections. Das ist es schon. Bekommst du jetzt Fehlermeldungen, liegt es wahrscheinlich daran, das der Hoster kein Tor-Netzwerk zulässt, oder den Zugang erschwert. So geht's zum Beispiel dennoch bei #freenode: https://freenode.net/kb/answer/chat. Man muss es nicht mögen.

Ich meine, der IRC ist ein Relikt aus der Vergangenheit, aber immer noch ein geiles Hintergrundfenster auf jedem drögen Büro-Desktop. Wir sehen uns im IRC.

KONKURRENZ FÜR EBAY: FACEBOOK STARTET MARKETPLACE

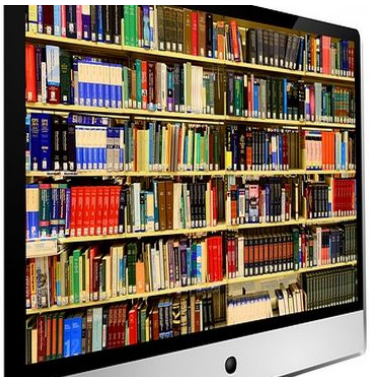
Wie im Facebook Newsroom mitgeteilt wird, eröffnet Facebook in 17 europäischen Ländern einen Marketplace. Der Online-Flohmarkt startet noch in dieser Woche, darunter in Deutschland, Österreich und der Schweiz. Die Plattform läuft in den USA, Großbritannien, Mexiko und vier weiteren Ländern bereits seit knapp einem Jahr. Nutzer können darauf privat lokal kaufen und verkaufen. Der Dienst ist derzeit kostenlos nutzbar.

Facebooknutzer können bei Marketplace sowohl Artikel zum Verkauf anbieten, als auch nach Artikel suchen. Die Angebote sind dabei aktuell nur in den Landesgrenzen sichtbar. Die Plattform ist als zusätzliche Ergänzung zu den vorhandenen An- und Verkaufsgruppen gedacht, die sich bereits einer großen Beliebtheit erfreuen: Über 550 Millionen Menschen sind global und jeden Monat dort auf Facebook aktiv. Kaufen- und Verkaufengruppen werden weiterhin eine wichtige Rolle auf Facebook einnehmen. Nutzer dieser Gruppen erhalten nun außerdem die Möglichkeit, ihre Annoncen parallel im Marketplace zu schalten, damit erhöhen sich die Verkaufschancen. Eine Filterfunktion weist die Angebote nochmals gesondert nach Ort, Preis und Kategorie aus. Das Finden von speziellen Artikeln erleichtert eine Suchmaske. Ein Inserat in der neuen Facebook-App ist leicht zu erstellen: Man stellt ein Foto vom zu veräußernden Gegenstand ein, gibt Produktinfos an, wählt dann Ort und Kategorie aus – fertig. Potentielle Kunden erhalten nach dem Tippen auf das ausgewählte Artikelbild noch zusätzliche Informationen, wie eine Produktbeschreibung, Namen und Profilbild des Verkäufers sowie Standortangaben. Im Hilfebereich finden sich zudem Informationen darüber, wie man auf Marketplace sicher kaufen und verkaufen kann. Hierzulande müssen die Marketplace-Nutzer die Details zum Versand und zur Bezahlung privat, im Verlauf des Nachrichtenaustauschs, unter sich regeln. In den USA hingegen können Nutzer über den Bezahlungsservice von Messenger auch gleich das Geld für die Artikel überweisen.

Als entscheidenden Pluspunkt seines Systems sieht Facebook, dass „die öffentlichen Profile von Käufer und Verkäufer einsehbar sind" und so „deutlich wird, wie lange die Beteiligten bereits auf Facebook sind" und zudem „gemeinsame Freunde angezeigt werden", wodurch der Kauf und Verkauf auf Marketplace den Menschen Sicherheit bieten würde, indem man weiß, mit wem man es zu tun hat, so das Unternehmen.

Weiterhin geplant: Facebook überarbeitet News Feed

Auch im Facebook-Newsroom angekündigt, möchte Facebook den News Feed zu einem „einfacheren Ort zum Verbinden und Navigieren" machen. Das soll heißen, er wird konversationsfreundlicher, einfacher zu lesen und zudem wird die Navigation besser gestaltet: Profilbilder werden rund, die Farbe ändert sich zu dezentem Grau. Kommentare erscheinen nun in einem abgerundeten, grau hinterlegten Kästchen. So soll es einfacher sein, auf den ersten Blick zu erkennen, wer wem direkt antwortet. Zu den weiteren Maßnahmen zählt ein höherer Farbkontrast in der Darstellung, damit soll die Typografie besser zur Geltung kommen. Link-Previews werden größer, ebenso die Icons für Gefällt mir, Kommentieren und Teilen. In den kommenden Wochen soll das neue Design dann für alle Nutzer zugänglich werden.



E-BOOK-MARKT: ANZAHL KÄUFER UND UMSATZ BIS SOMMER 2017 RÜCKLÄUFIG

Vierteljährlich gibt der Börsenverein des Deutschen Buchhandels e.V. in seinem E-Book-Quartalsbericht in Zusammenarbeit mit GfK Entertainment die neuesten Ergebnisse der Entwicklungen auf dem E-Book-Markt bekannt. Zur Auswertung bereit standen dieses Mal die Zahlen der ersten beiden Quartale, also von Januar bis einschließlich Juni 2017. Bezeichnend für diesen Zeitraum ist, dass die Kaufintensität steigt, die Käuferzahl zurückging und der Umsatz sank. Mit einem konstanten Umsatzanteil von 5,4 Prozent bleibt das E-Book somit weiterhin ein Nischenprodukt.

Auch im ersten Halbjahr 2017 legten E-Book-Käufer erneut mehr Titel in ihren Warenkorb als im Vorjahreszeitraum. So nahm die Kaufsintensität bei E-Books am Publikumsmarkt (ohne Schul- und Fachbücher) in den ersten beiden Quartalen 2017 im Vergleich zum Vorjahr um 15,2 Prozent zu und der Absatz stieg um 1 % leicht an. Die E-Book-Käufer erwarben in der ersten Jahreshälfte 2017 im Durchschnitt 5,7 E-Books (2016: 4,9; 2015: 4,8). Insgesant gesunken (um 12,3 % gegenüber dem Vorjahr) ist allerdings die Käuferzahl von 2,9 Mio. auf nunmehr 2,5 Mio. Käufer. Da die Käufer im Durchschnitt 4,4 % weniger pro E-Book bezahlten, gingen die E-Book-Umsätze am Publikumsmarkt in den ersten beiden Quartalen gegenüber dem Vorjahreszeitraum um 3,4 Prozent zurück. Der Umsatzanteil bleibt mit 5,4 Prozent konstant.

Die Hochrechnungen der E-Book-Absätze und -Umsätze stammen aus dem GfK Consumer Panel Media*Scope Buch. Es beteiligen sich daran insgesamt 25.000 Personen. Diese sind repräsentativ für die deutsche Wohnbevölkerung ab zehn Jahren, also für insgesamt 67,7 Mio. Menschen. In Form einer schriftlichen, repräsentativen Umfrage (ca. 60% Online – Anteil steigend + 40% Paper & Pencil) mittels Tagebuch, werden alle Einkäufe im Buchmarkt von diesen deutschen Privatpersonen ab 10 Jahren erfasst, die Ergebnisse werden dann auf die Grundgesamtheit der deutschen Bevölkerung (67,7 Mio. Menschen) ab 10 Jahre hochgerechnet. Die Studie beleuchtet die Perspektive der Kunden genauso, wie die des Handels und der Verlage.

Fazit

Der Trend setzt sich nun auch in diesem Quartal fort: Die Anzahl der E-Book-Käufer hat weiterhin abgenommen. Dafür kaufen aber die verbliebenen Kunden mehr E-Books. Allerdings entschieden sich diese wohl eher für geringpreisige Titel oder sie nutzten Angebotspreise, denn sie zahlten im Durchschnitt 4,4 % weniger pro E-Book, was in der Folge zu sinkenden Umsatzzahlen im Vergleich zum Vorjahreszeitraum führte.

WHOPPERCOIN: EIGENE KRYPTOWÄHRUNG FÜR BURGER KING RUSSLAND

Kryptowährungen liegen voll im Trend, wobei der Preis der Währung „bis zum Mond anwachsen“ oder minutenschnell „in den Keller stürzen“ kann. Für den Bitcoin, der wohl bekanntesten Krypto-Währung, hat sich der Preis in den letzten 24 Monaten sogar um sagenhafte 650 Prozent erhöht. Nun hat auch Burger King Russland seine eigene Kryptowährung, den Whoppercoin. Allerdings ist bisher noch unklar, wo dessen künftige Einsatzgebiete genau liegen werden, berichtet RUSBASE.

Eine eigene Kryptowährung hat die US-Fast-Food-Kette Burger King mit „Whoppercoin“ auf der Plattform des russischen Start-ups Waves veröffentlicht. Derzeit sind diese Whoppercoin nur in Russland erhältlich und vorerst auf eine Milliarde limitiert. Laut dem US-Konzern wären zusätzliche Emissionen später aber noch möglich. Burger-King-Kunden, die einen „Whopper“ kaufen, erhalten dazu einen Whoppercoin ausbezahlt. Sie müssen lediglich ein Foto der Rechnung vorweisen können.

Bisher gibt es nur wenige Informationen über das Projekt. So ist noch ungeklärt, wofür man Whoppercoins genau einsetzen kann, zumindest sollen sie in den Filialen der Fast-Food-Kette akzeptiert werden. Ein Vertreter der Schnellrestaurantkette gab an, dass die

anfängliche Verwendung der Kryptowährung im Rahmen eines Treueprogramms erfolge, es sich somit um ein Kundenbindungsprojekt handeln könnte. Vorstellbar wäre, dass das Unternehmen den Whoppercoin auch für zukünftige Werbeaktionen nutzen werden. Bereits im Juni informierte Burger King Russland darüber, dass sie fortan Bitcoins als Zahlungsmittel zulassen wollen.

Nachdem Kryptowährungen in Russland Jahre lang weitestgehend gemieden wurden, schlägt das Land nun einen neuen Kurs ein. Gemäß Informationen von Deutsche Wirtschafts Nachrichten plant das russische Unternehmen Russian Miner Coin einen massiven Einstieg in die digitale Generierung von Bitcoins, dem sogenannten Bitcoin-Mining. Dessen Miteigentümer ist ein Internet-Berater von Russlands Präsident Wladimir Putin. Der Vorstoß des Putin-Beraters zeigt deutlich das Interesse des Landes an den Kryptowährungen und an der dahinter stehenden Blockchain-Technologie. Auch dürfte ein Treffen zwischen Präsident Wladimir Putin und dem Ethereum-Erfinder Vitalik Buterin für eine Wende gesorgt haben. Demnach scheint es nur noch eine Frage der Zeit zu sein, bis Russland Kryptowährungen und deren Technologie rechtlich anerkennen wird. Die russische Regierung arbeitet zudem an einem Gesetz, welches Kryptowährungen rechtlich für die Wirtschaftsbranche einstufen soll. Außerdem interessieren sich immer mehr Unternehmen für den Einsatz der Blockchain-Technologie. Das jüngste Beispiel ist nun der Fast-Food-Riese Burger King.

Es bleibt abzuwarten, ob auch Filialen der Kette in anderen Ländern bei den Whoppercoins einsteigen. Es wäre sicherlich ein ausgeklügeltes Marketing-Konzept, das auch mit keinem großen zusätzlichem Aufwand verbunden wäre. Es wird erwartet, dass das Unternehmen weitere Details über das Projekt in absehbarer Zeit veröffentlichen wird.

WESHALB IHR EURE BITCOINS GENAU JETZT NACH HAUSE HOLEN WERDET!

Auch für Euch ist das Bitcoin ein Buch mit sieben Siegeln? Wir sorgen für Abhilfe. Was davon ist wirklich sicher: Ein Online-Wallet, Hardware-Wallet oder gar ein Paper-Wallet!? Andreas Koeppen klärt auf, wie man sein Erspartes sicher aufbewahren kann. Im Beitrag geht es auch um die geplante Abspaltung in BTC & BCC und die Konsequenzen, die daraus folgen werden.

Die Lage ist unübersichtlich und keiner weiß genau, was passiert. Wenn Euch Euer Geld also wichtig ist und Ihr es be-

halten wollt, dann holt Ihr es jetzt, ganz schnell nach Hause.

Euch ist der eigene, mit dem Internet verbundene, Rechner zu unsicher und Ihr scheut die Anschaffungskosten für ein Hardware-Wallet? Dann ist jetzt vielleicht ein Paper-Wallet genau das Richtige. Wichtig ist nur, dass Deine Bitcoins augenblicklich nicht auf irgendeiner Exchange- oder Onlinewallet herumliegen, denn sicher ist zur Zeit gar nichts.

Die SegWit activation als Heilsbringer?

Zu wenig Transaktionen pro Sekunde, 2,5, alle zehn Minuten ein Block, max. 1000 Transaktionen pro Block das ist vielen zu wenig! Kreditkartenunternehmen schaffen bis zu 2500 Transaktionen pro Sekunde. Da will man hin. Die Einen wollen größere Blöcke haben, die Anderen nicht. Eine Idee, das anders zu machen, ist die SegWit activation. Alles wird ein bisschen anders gespeichert. So kann man mehr in den Block packen, ohne die Größe wesentlich zu verändern. Wenn in zwei Wochen 95% der Nodes mitmachen, also das Bit für SegWit activation gesetzt haben, dann wird sich die Veränderung aktivieren. Die Bitcoin-Coder sind dafür, die großen Bitcoin-Miner waren lange dagegen. Diese verdienten nämlich sehr gut an den höheren Transaktionsgebühren, die sich entwickeln konnten, weil nicht genug Transaktionen in einen Block passten. Je höher die Gebühr, die man bereit ist zu zahlen, desto eher ist die Transaktion im nächsten Block mit dabei. Kurz: viele Miner wollten nicht mitmachen. Deshalb haben sich die Coder den User-Activated-Softfork ausgedacht. User sollen ihre Nodes so fahren, dass, wenn SegWit activation nicht gesetzt ist, die Blöcke nicht bearbeitet werden; also als Müll betrachtet werden. Miner, die nicht mitmachen, hätten so den Nachteil, das ihre Blöcke nicht mehr so gut verteilt werden würden. Wenn viele User ihre Nodes umstellen, müssten die Miner mitmachen, um keinen Nachteil zu haben. Soweit die Idee.

Halten die Miner jedoch alle zusammen und machen einfach weiter, hätten sie trotzdem keinen Nachteil. Aber wie man im Augenblick auch in der deutschen Autoindustrie (Stichwort: Kartell) sehen kann, bricht immer Einer aus, um sich Vortei-

le zu verschaffen. Wer SegWit activation einschaltet, bekommt die eigenen Blöcke besser verteilt. Die eigenen Blöcke kommen durch die User-Nodes – die Blöcke der anderen Leute nicht. Das wäre am 1. August der Fall. Also schon in ein paar Stunden. Ab dem 1. August werden also Blöcke von den nicht Umgestellten User-Nodes weggeschmissen, die nicht das SegWit-Activation-Bit gesetzt haben. Die Nodes sind schon mit Beginn Dezember 2016 durch Patches/ Updates umgestellt worden. Die Meisten jedenfalls. Es reicht dazu aus, dass nur ein paar Nodes die aktuelle Software fahren. Es reichen schon 10, 20, vielleicht 30% aus. Es reicht schon, wenn Miner überzeugt sind, einen, wenn zunächst auch eher kleinen Vorteil zu haben, gegenüber den Anderen, der Konkurrenz. So spielt man die Miner gegeneinander aus, wie es der Staat gerade mit den Autobauern vorgeführt hat. Es genügt, wenn ein Teilnehmer umfällt und umstellt. Die Anderen würden dann umgehend nachziehen weil sie sonst erst recht einen Nachteil zu befürchten hätten.

Was geschied am 1. August? Wird die Mehrheit das SegWit-Activation-Bit nutzen und könnten innerhalb von zwei Wochen die 95% erreicht werden? Dann wäre die neue Version, also Bitcoin Cash (BCC) aktiviert, und Bitcoin (BTC) würde wie eine nicht beachtete Zimmerpflanze im Büro eines Sommerurlaubers verkümmern. Wenn nicht, dann nicht. Bliebe dann alles beim Alten und BTC könnte die Oberhand behalten? Was genau kommen wird, ist derweilen völlig unklar, da es so etwas bei der Bitcoin-Blockchain bisher noch nicht gab.

BCC hat mit SegWit activation noch Zeit bis max 15. November, da das Bit, auf dem die SegWit-Activation-Info gespeichert ist, nur temporär zur Verfügung steht. Ist BCC bis dahin nicht über 95%, also nicht aktiviert, ist Feierabend. Was wird, weiß keiner.

„Dann wird es richtig kompliziert."

Noch was: Die großen Miner fanden es nicht witzig, von den Codern so erpresst zu werden. Vor einer Woche haben sie jetzt ein eigenes Bit gesetzt mit dem zudem die Blockgröße verdoppelt werden sollte. Dieses Bit brauchte nur drei Tage um sich zu aktivieren. Die Miner setzten jetzt also, den User-Nodes zuvorkommend, ebenfalls ein SegWit-Activation-Bit und haben es auch schon aktiviert bekommen. Sie sind einem User-Activated-Fork (selbst gemachte Abspaltung) mit dem Risiko eines Chain Splits also erstmal zuvorgekommen. Die Frage ist, was sie jetzt damit machen. Werden sie es wieder fallen lassen? Die Miner könnten die alte Blochchain ohne SegWit activation wachsen lassen. Bei einem Chain Split kämen noch einmal unvorhersehbare Probleme auf die Bitcoin-Gemeinde zu. Dann wird es richtig kompliziert. Ihr solltet also in nächster Zeit auf Nummer Sicher gehen und eure Coins nach Hause hohlen, absichern oder Paperwallets erstellen. Verzichtet auf Transaktionen wenn ab dem 1. August Chain Splits enstanden sein sollten. Haltet Euch bis zum 10. August zurück. Dann soll BCC aktiviert sein. Alle, die BTC favorisieren, steigen ab dem 1. August aus. Abspaltungen sind also vom 1. bis zum 10.August möglich. BCC hat dann noch bis zum 15. November Zeit, sich zu etablieren oder weg zu sein.

Es ist schwierig. Machen die Miner weiter oder werden sie einen Rückzieher machen? Wenn ja, wenn sie also weiter das SegWit-Activation-Bit setzen, hat BCC eine gute Chance stabil zu laufen und zu wachsen. Wenn nicht, wird es Chaos geben, der User-Activatet-Fork würde anlaufen, auch BCC würde das tun. Das aber schwächer und fände sich dann zudem einer durch Unterlassung oder Zurückname des SegWit-Activation-Bits entstandenen und vielleicht erstarkten BTC-Blockchain gegenüber wieder. Der Chain Split wäre Realität! Eure Coins wären zunächst in beiden Chains verfügbar. Erst wenn Ihr eine Transaktion ausführen wollt, müsstet Ihr Euch entscheiden. Wie genau das gehen soll, ist noch unklar. Bitstamp.net und andere große Marktführer haben sich positioniert und wollen keine Hard-Fork-Coins traden. Sie favorisieren also BTC und betrachten BCC als eine Art neuen Altcoin und die sind dort unerwünscht. Lasst Euer Geld nicht bei Dritten herumdümpeln. Es ist unklar, was sie damit machen. Also entweder raus aus den Coins und rein in das Fiatgeld (z.B.: Dollar, Euro etc.). Oder Ihr erstellt alternativ Paperwallets.

So erstellst Du ein Paperwallet:

Ein Anbieter für Paperwallets ist www.bitcoinpaperwallet.com. Er ist ein Fork von www.bitaddress.org, einem Bitcoin-Adress-Generator, nur umfangreicher und schöner.

Geht auf „Print a Wallet". Wählt eine Sprache, die Euch gefällt. Folgt den Schritten zur Calibrierung Eures Druckers und druckt Vorder- und Rückseite Eures Wallets im Landscape-Modus aus.

So bekommst Du Deine Coins auf die Paperwallet:

Öffne Dein Software- oder Online-Wallet. Übertrage Deine Bitcoins auf die Adresse Deines Paperwallets. Fertig. Deine Coins sind nun auf dem Paperwallet.

So bekommst Du Deine Coins vom Paperwallet zurück:

bitcoinsÖffne Dein Software- oder Onlinewallet. Über „Import“ erhältst Du Zugang auf Dein Guthaben. Hole Dir immer den vollständigen Betrag vom Paperwallet und teile den Betrag nicht von dort auf verschiedene Empänger auf. Prüfe zuvor, ob Dein Wallet die „Import-Privat-Key-Funktion besitzt. Nicht 100% aller Anbieter unterstützen diese Funktion, aber der größte Teil aller Exchanches, Apps, und Online-Web-Services schon.

An dieser Stelle sei gesagt, ich übernehme keine Garantie für gemachte Angaben, Prognosen oder Funktionen von Dienstleistern. Es geht teilweise um viel Geld, um Euer Geld. Deshalb prüft alles genau nach, bevor ihr etwas tut. Natürlich könnt Ihr auch alles so lassen, wie es ist. Euer Bier. Aber heult mir hinterher nicht die Ohren voll.

PRIVATSENDER FORDERN ANTEIL AN RUNDFUNKGEBÜHREN

ProSieben-Sat1-Chef Conrad Albert fordert mit dem Argument, man leiste schließlich seinen Teil zur Grundversorgung, einen Anteil an den Gebühren des öffentlich-rechtlichen Rundfunks. Das gab Conrad Albert der „Frankfurter Allgemeinen Sonntagszeitung“ bekannt. Jedes Medienhaus, das gesellschaftlich relevante Inhalte liefere, sollte über öffentliche Gelder gefördert werden – und nicht nur ARD und ZDF, sagte der Manager.

Der Rundfunkbeitrag wird in Deutschland zur Finanzierung der öffentlich-rechtlichen Rundfunkanstalten erhoben. Der Beitrag wird seit 2013 von jedem beitragsschuldigen Inhaber einer Wohnung erhoben, wobei es egal ist, ob und wie viele Rundfunkgeräte vorhanden sind. Privatsender haben keinen Zugriff auf diese öffentliche Gelder – die sind bisher ausschließlich ARD und ZDF vorbehalten. Conrad Albert, ProSieben-Sat.1-Vorstand, fordert indes einen Systemwechsel und die Auszahlung an Privatsender.

Die Einnahmen aus dem Rundfunkbeitrag lagen im Jahr 2016 bei rund 7,98 Milliarden Euro. Das entsprach einem Rückgang von rund 153 Millionen Euro im Vergleich zum Vorjahr, wie der Beitragsservice Ende Juni mitgeteilt hatte. Der Rundfunkbeitrag war mit Wirkung zum April 2015 für die Rezipienten von zuvor 17,98 Euro auf 17,50 Euro gesenkt worden. Bei dieser Höhe soll es bis 2020 bleiben.

„In dem Maße, in dem wir – die privaten TV-Vollprogramme – die Grundversorgung vor allem in jungen Segmenten de facto mitübernehmen, finden wir es sachgerecht, dass diese Inhalte aus öffentlichen Mitteln finanziert oder mitfinanziert werden“, sagte Albert der „Frankfurter Allgemeinen Sonntagszeitung„. Er wünsche sich deshalb einen „Systemwechsel, damit die öffentliche Finanzierung sich nicht länger an der Institution fest macht, sondern am Inhalt.“ Das System der öffentlich-rechtlichen Sender sei zwar wichtig für die Meinungsvielfalt in Deutschland und solle auch weiter bestehen, so Albert weiter. Man könne aber fragen: „Warum leisten wir uns eigentlich zwei Anstalten, ARD und ZDF? Braucht es wirklich acht Milliarden Euro, um den öffentlich-rechtlichen Auftrag zu erfüllen?“ ARD und ZDF müssten sich fragen lassen, ob sie ihren Auftrag überhaupt noch erfüllen, da sie nur noch einen Teil der Gesellschaft erreichen, stellt Albert fest: „Nur fünf Prozent der Zuschauer von ARD und ZDF sind unter 30 Jahre alt. In der Zielgruppe von 14 bis 29 Jahren erreichen wir mit ‚Pro7 News‘ deutlich mehr Zuschauer als Tagesschau und Heute zusammen.“

Das ist bereits der zweite Vorstoß mit Anspruch auf den Rundfunkbeitrag in dieser Woche. So fordert auch der mittelständische Fachverband Rundfunk- und Breitbandkommunikation (FRK) eine Beteiligung lokaler und regionaler Sender an diesen Gebühren im ländlichen Raum in Höhe von 250 Millionen Euro: Die Ausdünnung der lokal-regionalen Berichterstattung von Landesrundfunkanstalten verleihe dem privaten Rundfunk eine öffentlich-rechtliche Ersatzfunktion, die auch finanziell honoriert werden müsse. Der Fachverband Rundfunk- und BreitbandKommunikation (FRK) vertritt die auf dem Gebiet der Empfangsantennen und Kabelanlagen tätigen Fachbetriebe sowie Unternehmen, die solche Anlagen unterhalten oder unterhalten lassen.

Security

Themenübersicht

DEVIL'S IVY: ZAHLREICHE IOT-ÜBERWACHUNGSKAMERAS VON SICHERHEITSLÜCKE BETROFFEN

Sicherheitsforscher von Senrio haben eine Schwachstelle (CVE-2017-9765), genannt Devil's Ivy, im Software Development Kit gSOAP, einer Open-Source-Komponente für Security-Hardware entdeckt. Unbefugte können sie ausnutzen, um den Video-Feed von vernetzten Kameras einzusehen, abzuschalten oder zu unterbrechen. Von Marktführer Axis sind 249 Kameramodelle betroffen, die ihren Einsatz finden in Flughäfen, Banken bis hin zum Babyphone. Zudem sind Produkte von 34 weiteren Herstellern unsicher.

Der Fehler lag in der, in den Kameras verwendeten, Open-Source-Software gSOAP, einem Software Development Kit für auf SOAP/XML basierende Web-Services in C/C++, der einen Pufferüberlauf auslösen und damit dem Angreifer die volle Kontrolle über ein Gerät geben kann. Sie erlaubte es den Sicherheitsforschern, den Video-Feed einer Überwachungskamera auszuspähen, die Aufnahme anzuhalten oder die Kamera abzuschalten.

Die Forscher nannten die Sicherheitslücke Devil's Ivy und ziehen damit Parallelen zu einer wissenschaftlich als Epipremnum aureum bezeichenten Pflanze: Deren Kulturformen sind zwar beliebte und weit verbreitete Zimmerpflanzen, in der Natur in ihrer Heimat Asien und Australien sind sie jedoch dafür bekannt, dass sie sich schnell ausbreiten und kaum auf Dauer entfernen lassen.

Auf die Lücke aufmerksam wurden die Security-Experten von Senrio bei einer Untersuchung von Axis-Sicherheitskameras, speziell für die Security-Kamera Axis M3004, die ironischerweise in Hochsicherheitsbereichen – unter der Decke montiert – zum Einsatz kommt. Allein bei Axis sind 249 Kamera-Modelle von diesem Problem betroffen. Angesichts der Download-Zahlen von gSOAP gehen die Forscher von Senrio jedoch von einer sehr viel weiteren Verbreitung aus und sprechen sogar davon, dass wahrscheinlich insgesamt "Millionen andere Geräte" angreifbar für die auf Devil's Ivy getaufte Lücke sind. Nach Angaben von Genivia, das hinter der Entwicklung von gSOAP steht, wurde die Software mehr als eine Millionen Mal heruntergeladen.

Das schwedische Unternehmen Axis ist einer der wichtigsten Anbieter von internetfähigen Überwachungskameras und insbesondere auch im gewerblichen Bereich gut vertreten. Die Kameras kommen an Flughäfen, in zahlreichen Unternehmen, aber auch im öffentlichen Nahverkehr zum Einsatz. Zu den Kunden im deutschsprachigen Raum zählen Sparkassen, aber auch österreichische Justizbehörden.

Mehrere Tausend Überwachungskameras von Axis wären offen über das Internet zugänglich. Das ergab eine Suche über Shodan durch die Forscher bei Senrio. Deshalb raten die Experten, die Kameras nur noch in einem privaten Netzwerk zu verbinden und hinter einer Firewall zu verstecken.

Die Lücke konnte erfolgreich geschlossen werden. Axis stellt Updates für die betroffenen Kameras bereit und hat offenbar seine Kunden über deren Verfügbarkeit unterrichtet. Auch der Hersteller von gSOAP, Genivia, hat den Devil's-Ivy – Bug in Version 2.8.48 gefixt. Fraglich wäre jedoch noch, wie lange es dauert, bis dieses Update seinen Weg in alle betroffenen Produkte gefunden hat.

PWNED PASSWORDS: DIE SICHERE ENTSCHEIDUNGSHILFE ZUR PASSWORTNUTZUNG

Der neue Dienst Pwned Passwords macht geknackte Passwörter auffindbar. Sicherheitsforscher Troy Hunt bietet schon länger den Dienst „Have I Been Pwned" an. Darüber konnte nach Mailadressen oder Benutzernamen gesucht werden, die in letzter Zeit gehackt wurden. Nun gibt es dort zudem die neue Funktion Pwned Passwords, die diese Suchmöglichkeit auch auf Passwörter erweitert, berichtet engadget.

Mit Pwned Passwords kann man herausfinden, ob das Passwort, das man gerne verwenden möchte, bereits einmal in gehackten Datensätzen vorgekommen ist. Nach der Eingabe eines Passworts zeigt die Webseite an, ob es bereits in einem der Leaks enthalten war. Gibt man ein sicheres Passwort ein, erscheint „Good News – no pownage found!“. Ist das Passwort in der Datenbank, sieht man ein rotes Feld mit „Oh no, pwned!“ Falls dies der Fall sein sollte, macht es Sinn, das Passwort zu ändern. Wird es tatsächlich als gefunden angezeigt, wäre es wahrscheinlich, dass die Login-Daten kompromittiert sind, denn es könnte in einer solchen Liste schon vorkommen, die bei Brute-Force-Attacken auf Webseiten und Dienste verwendet werden. Solche Passwörter gelten daher als unsicher und sollten nicht mehr genutzt werden. Zu Vergleichszwecken greift der Dienst dabei zurück auf einen Datensatz von 306 Millionen Passwörtern aus diversen Lecks.

Für Web-Administratoren, die sicherstellen wollen, dass nur sichere Passwörter verwendet werden, bietet Hunt eine API an, über die die Datenbank automatisch abgefragt werden kann. So können Neu-Registrierungen bei Webseiten kompromittierte Passwörter direkt ablehnen. Zudem ist es möglich, über den Dienst auch SHA1-Hashes von Passwörtern abzugefragen.

Hunt weist allerdings ausdrücklich darauf hin, dass allein die Tatsache, dass er ein Passwort nicht in seinem Datensatz hat, nicht automatisch bedeutet, dass es wirklich sicher ist.

STANDARDISIERTER ADMIN-ZUGANG: GEFAHR FÜR TAUSENDE ANLAGEN WELTWEIT

Die Firma ComAp liefert Ethernet Module und SCADA-Kontrollsoftware für Industriesysteme in alle Herren Länder. Der WhiteHat Hacker Sojuniter fand im Frühjahr heraus, dass man eine firmeneigene Web-App für Generatoren, Turbinen und Windkraftwerke in vielen Fällen mit einfachsten Mitteln übernehmen kann. Das Unternehmen schiebt die Verantwortung von sich in Richtung ihrer eigenen Kunden.

Sojuniter kontaktierte uns Anfang April, um auf Sicherheitslücken in gleich mehreren Steuerprogrammen unterschiedlicher Anbieter aufmerksam zu machen. Dieser Artikel ist demnach der Anfang, aber noch nicht das Ende unserer Berichterstattung. Es geht um Bugs oder fehlende Sicherheitsmaßnahmen, um die man sich zeitnah kümmern muss. Der Hacker machte für die Ethernet-Karte IB-Lite innerhalb einer Stunde 400 IP-Adressen ausfindig. Er geht nach aktuellem Stand allerdings von einigen tausend Anlagen aus, die er übernehmen könnte, sofern er seinen Crawler entsprechend optimiert. Nach 40.000 möglichen Angriffszielen, die zu einem Blackout führen könnten, hörte er auf zu zählen.

„Ich kann an vielen Orten der Welt den Strom ausfallen lassen.“

Der Hintergrund

Der deutschsprachige Datenschützer hatte in Eigenarbeit einen Code erstellt, mit dem man das Internet nach bestimmten Merkmalen durchsuchen kann. Sein Programm ähnelt den Webcrawlern von Google, nur muss sein Crawler nicht so komplex sein. Gesucht wird nach der Steuersoftware von IP-Lite. Dies ist eine Ethernet-Karte zum Einstecken, die zu vielen unterschiedlichen Controllern der Firma ComAp, wie etwa das InteliCompact-NT, kompatibel ist.

Sojuniter wurde auf der Suche nach den passenden IP-Adressen recht schnell fündig. Wer die URL zur Hand hat, kann von daheim und unterwegs Wind- und Heizkraftwerke, Pumpwerke oder Generatoren aller Art kontrollieren. Bei einem Telefonat sagte uns der Datenschützer, er könne mit diesen Angaben im Nahen Osten Quadratkilometer weit den Strom ausfallen lassen. Betroffen seien auch Kraftwerke, die die technische Infrastruktur versorgen, um das dortige Mobilfunknetz zu betreiben. Ebenfalls die Stromversorgung vom Visalia Main Jail in Kalifornien oder der Polizei in der Tschechoslowakei. Für ihn wäre es kein Problem, die Anlagen abzustellen oder sogar durch Überhitzen zu zerstören. Das Problem: Was ihm gelang, könnte auch anderen Programmierern, so etwa Kriminellen oder Terroristen, gelingen. Hürden sind vorhanden aber sie sind nach Ansicht des WhiteHat Hackers nicht unüberwindbar. Ihm selbst ging es von Anfang an um Aufklärung und darum, Schäden zu vermeiden, die Cyberkriminelle anrichten könnten.

ComAp erwähnt voreingestelltes Passwort in der Anleitung

Nach erfolgter Registrierung mit Name und E-Mail-Adresse kann man sich einige Anleitungen der Geräte wie bei-

spielsweise vom Ethernet Modul IB-Lite herunterladen. Im IB-LITE-1-8-Reference-Guide-R1 steht wortwörtlich auf Seite 19: „Try the web interface (…) (with) access code 0“. Bis auf die Gültigkeit der E-Mail-Adresse wird vom Hersteller nicht geprüft, ob man auf die Anleitungen mit einem berechtigten Interesse zugreifen will. Nach unserer Anmeldung hatten wir unmittelbar Zugang zu allen PDF-Dokumenten, die natürlich auch der Werbung in eigener Sache dienen.

Kontaktaufnahme schwierig

Schon am 6. April schrieben wir eine E-Mail an die ComAp-Pressesprecherin Barbora Bednaríková, die allerdings als unzustellbar zurückkam. Daraufhin baten wir am gleichen Tag mittels der Kontakt-Adresse cee@momap.cz darum, der Dame unsere Informationen weiterzureichen. Diese Nachricht kam an, geschehen ist aber in den vergangenen drei Monaten nichts. Das trifft auch auf den Springer Konzern zu, der die uns vorliegenden Informationen ebenfalls schon im April 2017 erhalten aber bis heute nicht aufgegriffen hat. Nach Ablauf der drei Monate, die wir dem Unternehmen als Schonfrist einräumten, versuchten wir am 24.07.2017 wieder unser Glück. Erneut kontaktierten wir Frau Bednaríková sowie den deutschen Vertrieb unter anfrage@comap-control.com.

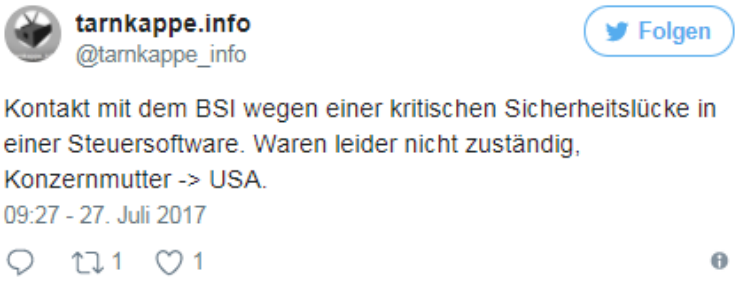
Einen Tag später nahmen wir Kontakt zum Bundesamt für Sicherheit in der Informationstechnik (BSI) auf. Wir erhielten von einer zuständigen Mitarbeiterin, die sich auf SCADA-Kontrollsysteme spezialisiert hat, zeitnah eine Antwort: eine Absage! Das BSI sei nicht zuständig, weil der Mutterkonzern seinen Hauptsitz in den USA habe, hieß es. „Das Unternehmen ComAp LLC ist in Illinois, USA registriert, wo BSI juristisch gesehen, keine Handhabe hat. Das ICS-CERT ist die zuständige Behörde in (den) USA.“ Das Industrial Control Systems Cyber Emergency Response Team (kurz: ICS-CERT) gehört zum US-Heimatschutzministerium DHS und kümmert sich um den Schutz kritischer Infrastrukturen. Doch leider wurde unsere Anfrage vom 25.7. an das ICS-CERT bislang nicht beantwortet.

Am gestrigen Mittwoch erhielten wir von der Pressesprecherin Bednaríková einige E-Mails und Telefonate später dann doch noch eine Antwort:

„Hello, I forwarded your messages to my IT colleagues. You can also have a look in our IB-Lite manual here. There it is written that the access code is 0 (see attachment). For further information, please contact my colleague Tomas Bilek.“

Ihre Nachricht könnte man verkürzt übersetzen: Schauen Sie her, das ist alles kein Geheimnis, dort im PDF-Dokument steht doch, wie unser voreingestelltes Passwort lautet. Ihr Kollege, der Chief Product Analyst von ComAp in der Tschechoslowakei, antwortete uns heute:

„The web interface of the mentioned device „IB-Lite“, as well as other types of interfaces/devices that can be exposed to public network infrastructures, use a credential called „Access Code“ to verify that the person attempting to connect to the device is authorized to do so or not. The Access Code is a string of up to15 characters and the default setting is „0“. However, it is fully up to the user what string they adjust there. Moreover, if the user connects to a device using default credentials he gets a big warning window informing that is it strongly recommended not to leave default credentials there. Unfortunately, many users still underestimate the cybernetic security and leave default values anyway. This results the in the alarming fact, that there is huge amount of various connected devices that are freely accessible as there are default credentials. This alarming situation is not related only to home wifi routers (what you may read often in various articles about this topic) but also related to industrial systems and other „IoT“ devices like ComAp IB-Lite module.“



Ein wenig überspitzt könnte man auch sagen: Die 0 ist als Zu-

gangscode voreinstellt. Es obliegt den Käufern der Hardware, ob sie den einfach zu merkenden Zugangscode so belassen oder sich ein neues Passwort mit bis zu 15 Stellen aussuchen. Als Sicherheitsmaßnahme wird den Nutzern lediglich jedes Mal ein Warnhinweis eingeblendet, dass sie ihre Voreinstellungen noch nicht geändert haben. Das ist alles. Schauen wir uns die Trefferquote des Hackers an, so war diese Maßnahme offenbar nicht ausreichend, um die kritische Infrastruktur der Kunden effektiv vor Angriffen von außen abzusichern.

Die Hackerparagrafen verbieten uns jegliche Überprüfung

Die Gesetzgebung ist klar: Ein unerlaubter Zugriff auf gesicherte Infrastrukturen und Daten ist verboten und ein „Hack“ wäre ohne rechtliche Konsequenzen nicht möglich, um den Sachverhalt zu reproduzieren. Außerdem könnte ein unnötiges Risiko für die betroffenen Anlagen bestehen. Um die Gefahrenlage dennoch abschätzen zu können, haben wir F-Secure, den finnischen Anbieter von Sicherheitslösungen, befragt. Wir schilderten den finnischen Experten die Erkenntnisse des Hackers und erhielten auf dieser Basis eine entsprechende Einschätzung, die wir unseren Lesern natürlich nicht vorenthalten wollen.

„Die Infrastruktur ist angeblich direkt über das Internet erreichbar. Sie ist weder hinter einem VPN, noch wird der Zugriff über Access Control Listen auf Whitelist-Basis kontrolliert.

Dem Unternehmen war offensichtlich klar, dass die Infrastruktur öffentlich erreichbar ist. Das Unternehmen soll diese Tatsache auch im Handbuch beschrieben haben. Wenn dem so ist, dann ist dem Unternehmen nicht klar, welche Konsequenzen mit dieser Aktion zu erwarten sei. Die Verantwortung dem IT-Administrator zu überlassen wäre verantwortungslos und hochfahrlässig.

Angeblich wurde der Zugang zum System von nur einem Faktor, einem Passwort, geschützt. Es gab keine einzelnen Benutzerkonten, entsprechend gibt es Probleme bei der Nachvollziehbarkeit sowohl beim Überprüfen der Systeme oder beim Behandeln von Zwischenfällen. Ein einzelnes Kennwort bedeutet Probleme bei der Verteilung und Verwaltung des Zugangs, 2FA-Lösungen (Zwei-Faktor-Authentifizierung: z.B. mittels eines Codes, der per SMS verschickt wird und beim Login zusätzlich eingegeben werden muss) kamen nicht zum Einsatz.“

„Firmen können sich nicht gegen Gefahren schützen, die sie nicht kennen.“

„Firmen können sich nicht gegen Gefahren schützen, die sie nicht kennen. Dienste wie die Discovery Scans von F-Secure RADAR, kombiniert mit OSINT-Tools wie F-Secure RIDDLER können Kunden eine bessere Übersicht zu potentiellen Risiken liefern. Unternehmen, die industrielle Kontrollsysteme nutzen, haben allerdings ein großes Problem: Die Zuständigkeiten der IT-Abteilung gegen die Zuständigkeiten des Personals, dass sich um industrielle Automatisierung kümmert. Beide Seiten müssen zusammenkommen und Kompromisse finden. Es muss ein Abwägen stattfinden, damit Unternehmen den Anforderungen des Marktes gerecht werden können, während sie gleichzeitig ihre IT-Umgebung sicher und stabil skalieren. Denn geht die Sicherheit verloren, kann dies bei Firmen im industriellen Umfeld gravierende Auswirkungen haben, bis zum Verlust von Menschenleben. Sicherheit wurde in diesen Unternehmen schon immer groß geschrieben, die IT kann sich daher oft auf klassische Sicherheitsmaßnahmen und –prozeduren verlassen. Im Lauf der Zeit ist die Anfangs hohe Aufmerksamkeit für die IT-Infrastruktur zurückgegangen. Mitverantwortlich sind hier auch die Budgets, die sich größten Teils deutlich zurückentwickelt haben.

Die optimale Vorgehensweise für Systeme, die für andere Anbieter erreichbar sein müssen, wäre eine beschränkte Punkt-zu-Punkt-Verbindung. Diese sollte sowohl gegen Lauscher schützen wie auch das Verändern von Daten unmöglich machen. Alle anderen Dienste, etwa Remote-Zugriff, E-Mail, die Kontrolle von Systemen oder andere Aspekte der internetbasierten Kommunikation sollten nur über eine VPN-gesicherte Verbindung zugänglich sein. Zudem sollten einzelne, zuordnungsbare Benutzerkonten verwendet werden, die mittels einem 2-Faktor-Ansatz geschützt sind. Wo Abweichungen von dieser Regel notwendig sind, lässt sich eine „Glashaus“-Lösung verwenden. Dabei kann es sich beispielsweise um virtuelle Betriebssysteme oder virtualisierte Anwendungen handeln, die „Jump Hosts“ oder andere Formen der Trennung verschiedener Umgebungen ermöglichen. Das Ziel dabei muss sein, sicherzustellen, dass Nutzer nur auf

die für sie passenden Systeme Zugriff haben. Die Zugänge sollten mit den allgemeinen Sicherheitsrichtlinien des Unternehmens sowie Erfahrungswerten in Einklang gebracht werden.

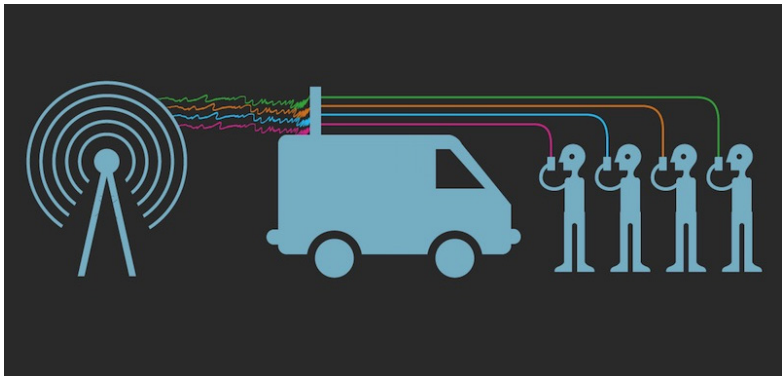
Dazu gehören Prozesse zur Verwaltung von Schwachstellen. Diese sollten regelmäßige Überprüfungen der Systeme sowie Schwachstellen-Scans beinhalten, kombiniert mit manuellen Tests und Mechanismen, die Probleme im Unternehmen sowie bei der Kommunikation mit Partnern erkennen. So können Firmen sicherstellen, dass sie potentiellen Angreifern einen Schritt voraus sind und Bedrohungen effektiv managen. Der Erfolg eines solchen Programms hängt aber davon ab zu wissen, welche Gefahren lauern. Unternehmen müssen sich mit unterschiedlichen Realitäten beschäftigen, abhängig von den Blickwinkeln auf die IT. Hier spielt etwa die Dokumentation der genutzten APIs von Drittherstellern eine Rolle, der Aufbau des internen Netzwerks und wie es wahrgenommen wird sowie genutzte IP-Adressen und Adressblöcke und wie diese dem Unternehmen bekannt oder nicht bekannt sind. Diese Vorgaben können sich beim Wachstum der Firma ständig ändern. Im täglichen Betrieb der IT können sich Fehler einschleichen, diese können in kleineren Problemen oder ausgewachsenen Sicherheitsrisiken enden. Nur der gezielte Einsatz spezialisierter, ethischer Hacker kann genau aufdecken, welche Gefahren lauern und welche Risiken für das Unternehmen bestehen. Und nur mit diesem Wissen lässt sich eine Strategie entwickeln, mit der sich die Firma jetzt und in Zukunft schützen lässt.“

Fazit: Leider sind sich manche Unternehmen der wachsenden Gefahren trotz

vieler Negativbeispiele noch immer nicht bewusst. Neben der Technik muss den Kunden auch das nötige Fachwissen vermittelt werden, damit das höchstmögliche Maß an Sicherheit gewährleistet ist. Ein wichtiger Bestandteil der Kundenbindung ist die fortlaufende Kundenkommunikation. Zu dieser müssen Produktschulungen bei jedem großen Soft- und Hardware-Update gehören. Wie die Experten von F-Secure schon anmerkten, sind zeitaktuelle Sicherheitsmaßnahmen für einen Fernzugriff unabdingbar, um die Gefahr durch Hacker und Terroristen so gut es geht zu minimieren. Die Technologien sind da – ihr Einsatz darf keine Option, sondern muss eine Pflicht sein.

Das aktuelle Beispiel zeigt ebenso, wie schwer und langwierig die Kommunikation mit einem Unternehmen sein kann. Hier herrscht auf breiter Ebene großer Nachholbedarf. Anonyme und sichere Kommunikationskanäle können es WhiteHat Hackern erleichtern, kritische Informationen über Sicherheitslücken und Probleme, an die zuständigen Personen zu melden. Und dies ohne die eigene Identität preiszugeben. Die Presse- bzw. Marketing-Abteilung kann nicht der einzige Weg sein, mit dem Unternehmen in Kontakt zu treten. PGP wäre ein Anfang. Eine Threema ID wäre möglich, eine Nummer bei Signal oder Telegram – die Möglichkeiten sind vielseitig.

Ebenso haben sich Unternehmen auf den Ernstfall vorzubereiten. Das sollte nicht bei der Krisenkommunikation durch eine Presse-Agentur enden. In Deutschland gibt es eine Vielzahl an Anlaufstellen, die eine qualifizierte Hilfestellung bieten: Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) oder Informationsstellen wie dem ZD.B und deren Pendants in anderen Bundesländern. Unternehmen, die auf digitale Strukturen setzen, müssen sich noch heute – am besten schon gestern – ein realistisches Bild ihrer Sicherheitsmaßnahmen machen. Nur so sind wir sowohl in der analogen als auch in der digitalen Welt bestens geschützt.



IMSI, IF YOU CAN: WIE MAN SICH FÜR UNTER 10 EUR EINEN IMSI-CATCHER BAUT

Ein IMSI-Catcher ist ein Gerät, mit dem die auf der Mobilfunkkarte eines Mobiltelefons gespeicherte IMSI ausgelesen und der Standort der Mobiltelefone innerhalb einer Funkzelle eingegrenzt werden kann. Die Polizei setzt das Gerät z.B. gerne auf Demos ein, um alle Mobilfunktelefonate mitzuhören u.v.m.

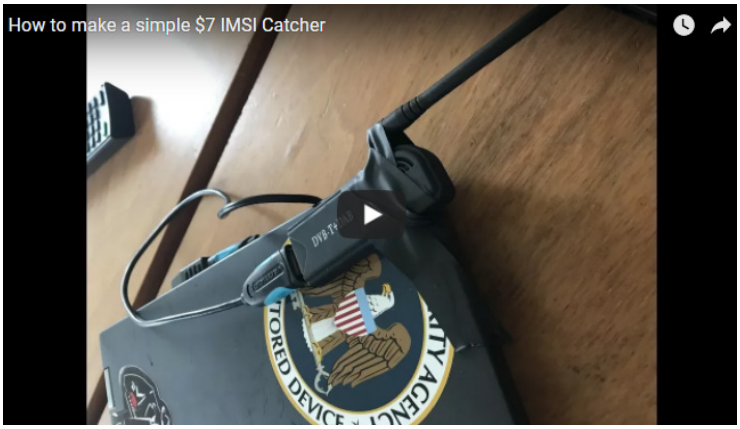
Sicherheitsdienste nutzen sie seit langem. Mit sogenannten IMSI-Catchern kann man International Mobile Subscriber Identity (IMSI)-Nummern aufspüren. Diese sorgen dafür, dass ein bestimmtes Endgerät den richtigen Anruf erhält. Hier erfahrt ihr, wie man mit geringem finanziellen Aufwand und etwas Python feststellen kann, welche SIM-Karten in der Nähe aktiv sind und somit ein entsprechendes Telefon und den damit verbundenen Besitzer aufklärt. Ihr könnt damit also Person, Ort und Zeitpunk bestimmen.

Döner-Mann hat IMSI an

Wenn also euer Lieblings-Döner-Mann zukünftig einen IMSI-Catcher in seiner Bude hängen hätte, und es käme in der Nacht zu einem Einbruch in der Raffinerie, könnte der Grand Chef anhand der Signalstärke herausfinden, welche IMSI-Nummern sich zur Tatzeit innerhalb seiner Gefilde befunden haben. Käme es etwa zu einem Überfall oder einem Anschlag, könnten so Täter und wichtige Zeugen aufgedeckt und aufgespürt werden. So könnte man einigen Behörden und Diensten helfend unter die Arme greifen, die ja in der Vergangenheit teilweise erhebliche Probleme damit hatten, bei schweren Straftaten (Beispiel NSU), Zeugen oder Täter zu benennen. Die Polizei könnte dann die IMSI-Nummern mit den stärksten Signalen heraussuchen, sich an die jeweiligen Telekommunikationsanbieter wenden, um die dazugehörigen SIM-Karten und deren Besitzer zu ermitteln.

Die Technik ist nicht neu. Interessant ist jetzt aber, wie billig und einfach alles zu realisieren ist. Die Hardware bekommst du „für 'nen Appel und 'nen Ei“ bei eBay:

Die passende Software dafür ist gratis und kann von jedem innerhalb kürzester Zeit installiert werden. Es gibt sogar eine Youtube-Anleitung dafür:



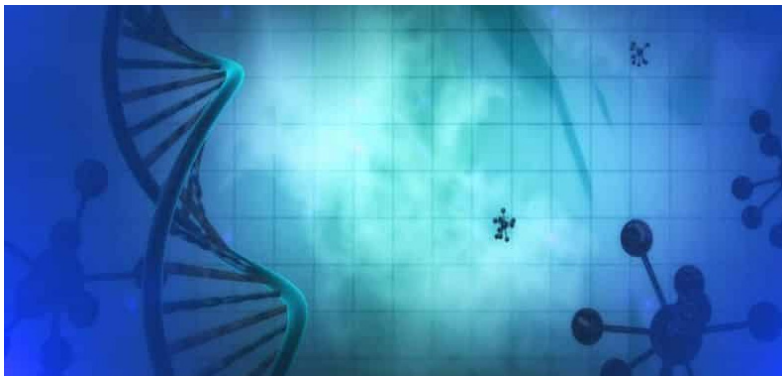
Weitere Details zum Download der eingesetzten Software findest Du in der Beschreibung des oben gezeigten YouTube-Videos.

Wer mobil sein wollte, könnte statt der eigenen Linux-Kiste noch einen Raspberry Pi verwenden und den IMSI-Catcher so ins eigene Auto, einen Bus oder ins Taxi hängen. Die Software würde sich auch dort schnell zu Hause fühlen.

Natürlich müsstet ihr vor einem eventuellen Einsatz die rechtliche Seite abklären. Keinesfalls solltet ihr damit, wie überhaupt in eurem Leben, Straftaten begehen. Mein Artikel beschreibt lediglich ein Experiment unter Laborbedingungen, für den Inhalt des Videos ist ausschließlich der Youtuber verantwortlich.

Übrigens: Das Dönermann-Beispiel ist fiktiv (nicht fremdenfeindlich, auf jeden Fall vegan) und stellt keine Aufforderung zu einem bestimmten Verhalten, erst recht zu keiner strafbaren Handlung, dar.

Und nicht vergessen: Seid freundlich zu eurem Döner-Mann, denn man weiß ja nie, was er so alles in seiner Bude hängen hat.



BIO-HACKING: ÜBERNAHME EINES COMPUTERS MITTELS MANIPULIERTER DNA MÖGLICH

Vieles, das gestern noch wie Science Fiction klingt, ist heute schon machbar. So hat eine Gruppe von Forschern, im Team von Tadayoshi Kohno an der University of Washington, erstmals gezeigt, dass es möglich ist, schädliche Software in physikalische DNA-Stränge zu codieren und einen Computer mithilfe dieser manipulierten DNA zu übernehmen, berichtete Wired. Konkrete Details dazu wird das Team auf dem 26. USENIX Security Symposium vom 16. bis zum 18. August in Vancouver bekannt geben.

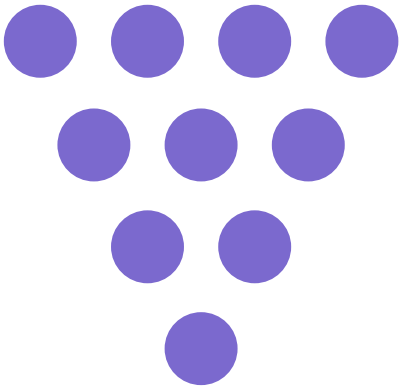
Biohackern ist es nun erstmals gelungen, DNA so zu manipulieren, dass Infektionsgefahr nicht mehr ausschließlich für Lebewesen, sondern auch für Computer besteht; eine biologische Ansteckung technischer Geräte wird nun real. Forscher kodierten dazu in einem DNA-Strang schädliche Software. Wenn ein Gerät das Erbgut dann sequenziert, greift das in der DNA kodierte Programm die Software des Sequenzierautomaten an und gewährt den Angreifern in der Folge vollständigen Fernzugriff auf den Computer. Die Forscher haben dafür eine bekannte Sicherheitslücke einer DNA-Sequenzierungs-Software ausgenutzt.

Allerdings stellt der beschriebene Angriff eher eine Machbarkeitsstudie (Proof-of-Concept) dar, als eine reale Bedrohung, er wäre zudem derzeit völlig unrealistisch: „Wir haben keine Hin-

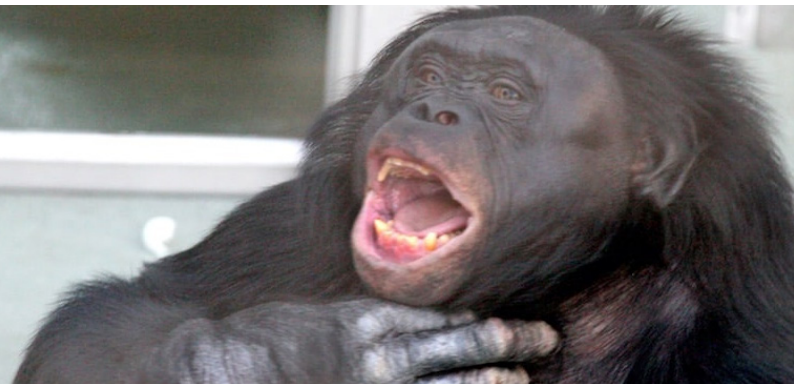
weise darauf, dass die Sicherheit der DNA-Sequenzierung oder der DNA-Daten im Allgemeinen derzeit angegriffen wird.“, geben die Autoren der Studie bekannt. So wäre der Aufwand, eine entsprechende DNA-Sequenz zu designen, herzustellen und in das gewünschte Sequenziersystem einzuschleusen, weitaus größer als für andere Angriffsstrategien. Das Forscherteam wollte aber dennoch darauf aufmerksam machen, dass diese Angriffsmethode realisierbar sei und dementsprechend von den Entwicklern ernstgenommen werden muss, denn DNA-Sequencing werde mit der Zeit immer alltäglicher und leistungsstärker. Somit wächst auch die Gefahr, dass es zu Missbrauch kommt.

Ulrich Greveler, Professor für Angewandte Informatik und IT-Sicherheit an der Universität Rhein-Waal, sieht ebenso wie die Forscher in Kohnos Arbeitsgruppe ein grundsätzliches Sicherheitsproblem bei Systemen, die auf solche nicht-digitalen Daten zugreifen: „In gleicher Weise wäre denkbar, dass Fingerabdruck- oder Iris-Scanner auf diese Weise gehackt werden. Ein Gerät könnte übernommen werden, um nicht-autorisierte Personen zuzulassen oder weitere Rechner im Netzwerk anzugreifen“, warnt er.

Kohnos Team fand bei ihrer Untersuchung „konkrete Belege für schlechte Sicherheitspraxis im gesamten DNA-Prozessierungssektor“. Auf Grundlage dieser Befunde will die Arbeitsgruppe nun gezielt bessere Bedingungen zur Datensicherheit in der Bioinformatik schaffen.



Der Einsatz von DNA als Datenspeicher der Zukunft wird bereits seit mehreren Jahren erschlossen. So hat die Forschung schon Wege aufgezeigt, die es möglich machen, Daten mit DNA zu übertragen. Im April 2016 demonstrierten Microsoft und die University of Washington eine Technik zum Speichern und Abrufen von digitalen Bildern mit DNA. Forschern der US-Universität Harvard ist es zudem gelungen, einen kurzen Film in der DNA von lebenden Bakterien zu speichern. Diese Forschung zielt darauf ab, DNA zu einem lebensfähigen Speichermedium für digitale Informationen zu machen, indem sie ihre einzigartigen Eigenschaften verwendet, um riesige Mengen an Informationen in winzigen Mengen an Flüssigkeit zu speichern. Derzeit gibt es Überlegungen, wie sich diese Methode als Langzeitspeicher für Cloud-Speicherdienste einsetzen lässt. Allerdings erschwert jedoch neben den hohen Kosten die geringe Übertragungsgeschwindigkeit von 400 Byte pro Sekunde den Einsatz außerhalb des wissenschaftlichen Bereichs zu Studienzwecken.



Unter dem Radar: Der satirische Monatsrückblick

Es ist Juli und vielerorts sind Sommerferien. Zeit, so mag man glauben, für klassische Sommerloch-Themen – Monster in schottischen Gewässern, Krokodile im Baggersee und die Veränderungen des Benzinpreises sind nur einige der mehr oder weniger relevanten Vorkommnisse, die man aktuell in den Medien erwartet. Da können wir direkt froh sein, dass wieder einige Zeitreisende aus dem 20. oder noch früheren Jahrhunderten in die Bresche springen und mit ihrem brachialen Mangel an Verständnis für moderne Technik und deren Auswirkungen die Nachrichtenlage ein wenig auflockern.

Das gleiche gilt für den Wahlkampf. Wenn sich so viele Menschen so gekonnt zum Affen machen (siehe Bild oben), wird es wenigstens auch bei 30 Grad nicht langweilig. Wer noch nicht überzeugt ist, kann in unserem Monatsrückblick einige schöne Beispiele nachlesen.

Der Voll-Stuss, wo jeder mit muss

Wer ist verantwortlich, wenn jemand faschistischen Blödsinn oder verbotene Äußerungen ans schwarze Brett pinnt? Richtig, derjenige, der die Pinnwand aufgehängt hat. Ist doch logisch. Nach diesem bestechenden Prinzip funktioniert auch das jüngst verabschiedete Netzwerkdurchsetzungsgesetz – schreiben Leute gefährlichen, gemeinen oder gemeingefährlichen Unsinn ins Netz, muss der Betreiber der betreffenden Plattform diesen binnen bestimmter Fristen entfernen. Anderenfalls drohen empfindliche Strafen (empfindlich in dem Sinne, dass es selbst Mark Zuckerberg nicht mal eben aus der Kaffeekasse zahlt).

Nun ist es natürlich eine lobenswerte Absicht, Hetze und Hass im Netz eindämmen zu wollen (und wenn es eine Möglichkeit gäbe, die Verbreitung schlecht fotografierter Kaffeebecher zu kriminalisieren, wäre ich auch nicht abgeneigt). Die Wahl der Mittel allerdings ist (wieder einmal) das Gegenteil von gekonnt. Statt mit Kanonen wird auch in diesem Fall wieder mit einer Zensur-Infrastruktur auf Spatzen(hirne) geschossen. Denn was tut ein profitorientiertes Unternehmen, das mit einem solchen Netzwerkausdruckungsgesetz konfrontiert wird? Richtig, der Verantwortliche denkt sich „Hmm, diese Katze da auf dem Bild könnte dann doch ein schwarzes Hitlerbärtchen haben. Ich lösche das mal lieber, bevor sich jemand beschwert und mein Taschengeld für den nächsten Segeltörn auf den Bahamas draufgeht.“ Was das für die Meinungsfreiheit bedeutet, kann sich jeder, der mehr Gehirnzellen hat als ein durschnittlicher Facebook-Hassprediger (oder ein Mitglied des Bundestages) selbst ausdenken.

Über den Mauern, muss die Freiheit wohl grenzenlos sein

Manche Geschichten, die das Leben schreibt, dürften sich Romanautorinnen und -autoren nicht ausdenken, weil ihnen dann mangelnder Realismus vorgeworfen würde. Um so schöner ist es, diese Geschichten dann in den Nachrichten verfolgen zu dürfen. In diese Kategorie fällt beispielsweise ein spektakulärer Gefängnisausbruch mit Hilfe einer Drohne, wie ihn sich Hermann Joha nicht besser hätte ausdenken können.

Das einzige Problem: Wenn nach derselben „Logik“ vorgegangen wird, wie bei Verschlüsselung und IT-Sicherheitstools, werden Drohnen demnächst als Terroristen-Werkzeug kriminalisiert. Zuerst kommen Schockbilder von extremistischen Cybers auf die Verpackung und später muss sich jeder, der so ein Ding kaufen will, mit Namen, Adresse, Personal-Ausweisnummer und Lieblings-Haribosorte bei den Behörden registrieren.

Das gilt natürlich nur für die zivile Variante, mit der man Fotos machen, Rennen fliegen und Kunststücke vorführen kann. Die Sorte Drohne, mit der man auf Knopfdruck ganze Hochzeitsgesellschaften auslöschen kann, ist selbstverständlich legal und lobenswert. Und weil ihr euch das jetzt gerade gefragt habt, lasst ihr euch am besten auch gleich prophylaktisch in die Terroristen-Datei eintragen. Zweifel am Kampf gegen den Terror und der nationalen Sicherheit sind ein sicheres Zeichen für eine extremistische Gesinnung.

The Truth is Out There

Nach so vielen spektakulären Fehlschlägen konnten unsere Mächtigen allerdings auch einen Erfolg melden: der neue Staatstrojaner ist fertig und soll noch in diesem Jahr zum Einsatz kommen. Allerdings stellt sich aufmerksamen Leserinnen und Lesern durchaus die Frage, wie es zu diesem scheinbaren Triumph der Behörden gekommen ist, erweck-

ten diese doch bisher glaubhaft den Anschein, schon mit einem „Hello World“ in Turbo Pascal überfordert zu sein.

Die eine Möglichkeit ist natürlich, dass das selbe passiert ist, was Regierungsbehörden meistens tun: irgendein halbfertiger, löchriger, vorschriftswidriger Schrott wurde kurzerhand als fertig definiert in der Hoffnung, die unweigerlich, aber zu unbestimmtem späterem Zeitpunkt zu erwartende Blamage dem Amtsnachfolger in die Schuhe schieben zu können. Für diese Theorie spricht zweifellos so einiges. Ob sie stimmt, wird uns wohl in nicht allzu ferner Zukunft der Chaos Computer Club mitteilen.

Ansonsten bleibt eigentlich nur noch die Spekulation, dass die Damen und Herren Regierungs-Codemonkeys heimlich Hilfe von außen hatten. Bloß von wem? Irgendeiner zwielichtigen Cybercrime-Firma, die ihre gegen jede Hackerethik verstoßenden Machenschaften damit legitimiert, dass sie sie zugunsten zahlender Regierungen betreibt? Als Doppelagenten rekrutierten extremistischen Cybers? Den Amis? Den Israelis? Oder hat Erich von Däniken womöglich doch recht und es waren wie immer die Aliens? Eine allzu große Anpassung an außerirdische Gewohnheiten würde zumindest den Kommunikationsstil von Heiko Maas erklären…

Mitunter heißt es von einer Person, einer Sache oder einer Idee, er oder sie sei einfach seiner oder ihrer Zeit voraus. Aktuell haben wir das zum Beispiel mit dem Herbst. Der Sommer hat gefühlt noch gar nicht richtig angefangen, da ist er auch schon wieder vorbei. Kühle Nächte, Landregen und fallende Blätter sind allerdings nicht die einzigen Dinge, die absolut zum falschen Zeitpunkt kommen. Im Wahlkampf-Chaos ließ es auch so manche Politikerin und mancher Politiker am Gespür für Timing vermissen. Einen Einblick in das Chaos liefert der satirische Monatsrückblick.

Die Fast-Kryptowährung

Manche Dinge passieren, wie oben erklärt, einfach zum falschen Zeitpunkt und wirken dadurch peinlich, schrullig oder beides. Dann gibt es aber auch Dinge, die passieren, obwohl es für sie schlichtweg keinen richtigen Zeitpunkt gibt. Beispiel gefällig? Eine Firma, die behauptet, eine Krypto-Währung anzubieten, welche die Anonymität schützt, nur um dann auf höfliche Nachfrage der Behörden hin diese Daten auf einem Silbertablett zu überreichen. Der Name des übereifrigen Butlers? Die Bitcoin Deutschland AG. Warum die Betreibergesellschaft schneller umfällt, als die SPD in der Bundestagsdebatte, wird wohl ihr Geheimnis bleiben, aber das Vertrauen der Nutzergemeinde dürfte erst einmal dahin sein. Aber auch das ist ja dann eine weitere Parallele zur SPD…

Übrigens: wer per PaySafeCard anonym bezahlen will, ist auch nicht viel besser dran. Letztendlich bleibt wohl nur wieder, Wolle gegen Getreide zu tauschen oder etwas in der Art…

Per Schneckenpost in die Vergangenheit

Entgegen der generellen Tendenz wüsste ich eine Idee, deren Zeit definitiv gekommen ist: Schnelles Surfen im Mobilfunk-Netz für alle. Leider ist auch das in Deutschland Zukunftsmusik. Manch einer mag nun einwenden, dass das, zumindest in Ballungsgebieten, doch bereits möglich ist. Aber leider schlägt hier der viel zitierte Unterschied zwischen Theorie und Praxis zu Buche.

Viele Mobilfunk-Provider werben mit Surfgeschwindigkeiten von bis zu 500 MBit pro Sekunde im LTE-Netz. Das hört sich durchaus beeindruckend an. Nun stellte sich aber heraus, dass diese Werte in der Praxis kaum jemals erreicht werden. Ein „reiner Werbetrick“ seien diese Aussagen, kritisiert nun ein Whistleblower. Für die Kundinnen und Kunden ist das ein wenig so, als hätten sie einen schnittigen Ferrari gekauft, um dann zuhause unter der Motorhaube nur einen Smart-Motor vorzufinden.

In Deutschland müssen wir wohl auf schnelles LTE noch eine Weile warten. Einzige Alternative wäre womöglich, die Nutzung der Einwahlmasten drastisch zu reduzieren – frei nach dem Motto „hör auf zu telefonieren, ich will ins Internet“… Damit hätten wir zumindest den Kreis geschlossen und wären beim Thema „pure Nostalgie“. Zumindest dürften das AOL-Einwahlgeräusch und der markante Signalton von ICQ den Kindern der 1990er die Wartezeit auf ihr Video verkürzen…

Die Schatten der Vergangenheit

Neben Ideen, die so richtig zu keinem Raum-Zeit-Kontinuum zu passen scheinen, und solchen, die schon lange überfällig sind, aber noch auf sich warten lassen, gibt es auch solche, die eigentlich veralteter sind als ein 56k-Modem. Problematisch wird es dann, wenn die Herrchen und Frauchen dieser eigentlich eher bedauernswerten Geschöpfe das dann nicht merken und ihre Zombie-Missgeburten immer wieder in die Öffentlichkeit zerren. So eine Idee ist beispielsweise die exzessive Überwachung. Dieses Thema wurde in den frühen Nullerjahren nun wirklich schon zur Genüge diskutiert; Ergebnis: bringt nichts und außer der Politik wollen es die Wenigsten wirklich haben. Das allerdings ficht einige Politikerinnen und Politiker nur bedingt an. Jüngstes Beispiel: Zombiedompteur Joachim Hermann, der erst kürzlich wieder eine flächendeckende Videoüberwachung für Bayern forderte. Vielleicht hat er Angst, dass sich irgendwo zwischen den Gipfeln extremistische Cybers verstecken….

Unterstützt wurde Hermann auf Bundesebene sogleich von Thomas de Maizière. Unser Bundesinnenminister hat ja schon lange bewiesen, dass streberhaftes Aussehen leider keineswegs mit der Klugheit und Empathie einer Hermine Granger einhergehen muss – und tritt diesen Beweis in Überwachungsfragen gerne jeden Tag erneut an. Er wünscht sich nicht nur eine Erweiterung der Videoüberwachung, sondern zusätzlich noch die Möglichkeit der Gesichtserkennung – man muss ja wissen, welches extremistische Cyber einem da gerade so über den Weg läuft.

Meine Herren, 1984 hat angerufen. Es will seine dummen Ideen zurück.

Mit Vollgas in den Wahnsinn

Wie diese kleine Auswahl zeigt, beweisen viele Menschen ein wirklich erbärmliches Gespür für den Lauf der Dinge und den richtigen Zeitpunkt. Das dürfte sich in den nächsten Wochen sogar noch verschlimmern, nähert sich doch – so viel lässt sich trotz aller Verwirrung über den zeitlichen Lauf der Dinge sicher sagen – die Bundestagswahl mit großen Schritten.

Verantwortlich für den redaktionellen Inhalt:

Lars Sobiraj

Redaktion:
Lars Sobiraj
Annika Kremer
Antonia
Andreas Köppen
Jakob Ginzburg

Verantwortlich für Layout und Design:

Jakob Ginzburg

Ein Angebot von

digital publishing momentum

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

tarnkappe.info MAGAZIN

03

digital
publishing
momentum