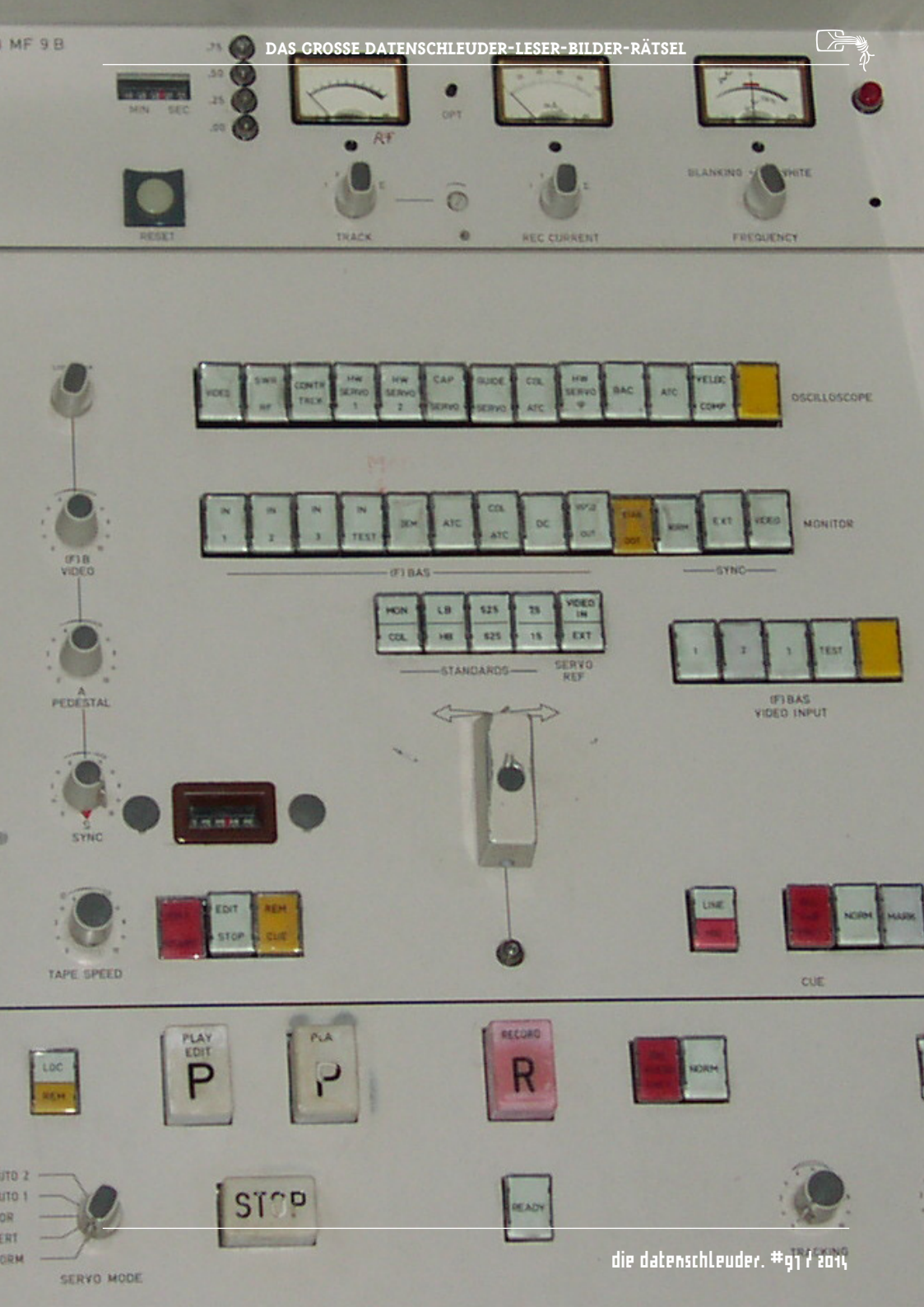
die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

Schöne Scheiße

ISSN 0930-1054 • 2014
Euro 2,50

#97


MF 9 B
MIN
SEC
RF
OPT
RESET
TRACK
REC CURRENT
BLANKING
WHITE
FREQUENCY
OSCILLOSCOPE
MONITOR
(F)B
VIDEO
(F)BAS
SYNC
A
PEDESTAL
STANDARDS
SERVO
REF
(F)BAS
VIDEO INPUT
S
SYNC
EDIT
STOP
REM
CUE
TAPE SPEED
LINE
NORM
MARK
CUE
LOC
REM
PLAY
EDIT
P
P
RECORD
R
NORM
STOP
READY
SERVO MODE
TRACKING

Da bringt man mal ein paar Monate keine Datenschleuder raus, schon muß man sich im Geleitwort mit einer echten Zeitenwende auseinandersetzen. Denn das mit dem „Nationalen Cyber-Abwehrzentrum“ war ja mal anders gemeint. Seit dem Erscheinen der vorigen Ausgabe ist der Begriff des „Cyberkriminellen“ vollständig neudefiniert worden. Ein paar Hacker hatten es schon länger behauptet, nun ist es Allgemeinwissen: Der „Cyberkriminelle“ neuer Bauart ist nicht der in düsteren Ecken einhändig tippende, mit der anderen Hand den Laptop balancierende, finster dreinblickende Sturmhaubenträger, den wir aus den verzweifelten Versuchen der Medien kennen, das „Cyber“-Thema zu bebildern. Vielmehr ist er ein bestens rasierter und gewandeter, aus den Milliardenschatullen der Schattenhaushalte regelmäßig bezahlter Geheimdienst-Lohnsklave mit hinreichenden Kenntnissen über Netzwerke und Systemlöcher, der sein Klo mit NDAs tapezieren könnte. Sein Büroalltag besteht aus staatlich beauftragten ungenierten, systematischen digitalen Angriffen, Ausspähversuchen – und ein bißchen zwischenzeitlichem Datenbank-Browsen zur Befriedigung der Spanner-Seele.

Für die Beweiserhebung dieser dank der Snowden-Enthüllungen letzthin öffentlich stärker beäugten cyberkriminellen Aktivitäten ist nun eigens ein parlamentarischer Untersuchungsausschuß im Bundestag eingerichtet worden. Der soll sich dem widmen, was das Parlament im Grunde alltäglich zu tun hätte: Die geheimdienstlichen Beamten und ihre privatwirtschaftlichen Komplizen beaufsichtigen. Die bisherigen Ergebnisse sind überraschenderweise nicht etwa die erwartete Nullösung, sondern durchaus aufschlußreich, allerdings weniger durch den harten Ermittlungseifer der Regierungsabgeordneten als durch die den Ausschuß begleitenden Leaks und Presseberichte.

Es ist derzeit recht hip, neben der dräuenden Rentnerschwemme auch über die Presse zu schimpfen. Doch nach dem ersten Snowden-Jahr muß man festhalten, daß ohne die anhaltende und hartnäckige internationale Berichterstattung aus den Snowden-Papieren niemals der Wandel hätte eingeleitet werden können, auf den wir für die nächsten Jahre wenigstens hoffen dürfen. Edward Snowden schrieb uns anläßlich der Pulitzer-Preisverleihung an den Guardian und die Washington Post ins Stammbuch: „My efforts would have been meaningless without the dedication, passion, and skill of these newspapers, and they have my gratitude and respect for their extraordinary service to our society.“

Tatsächliche Veränderung geschieht ja – bevor irgendwann die aufgebrachten Massen mit Mistgabeln und Fackeln vor den Geheimdienstzentralen stehen – vorwiegend durch Gesetze und Gerichtsurteile. Nun ist es untertanenseitig strukturell etwas schwierig, von Deutschland aus die NSA juristisch anzugehen. Es gibt aber auf den Inseln, die sich wegen schottischer Furchtsamkeit immer noch Groß-Britannien nennen können, einen ebenso dreisten wie mächtigen Ableger der Five Eyes, das „Government Communications Head Quarter“, kurz GCHQ. Deren Überwachungsoperationen fallen also derzeit – noch – unter europäische Jurisdiktion.

Wir als Hacker sind, zusammen mit Privacy International, gegen das GCHQ vor Gericht gezogen, [1] denn frei nach dem alten und neuen Innenminister gilt: Hacker werden immer irgendwas hacken, selbst Rechtssysteme. Denn noch der ignoranteste Werbeplattform-Insasse hat verdammt nochmal das Recht, seine Timeline ungestört zu befüllen und dabei von den eigenen und ausländischen Geheimdiensten grundsätzlich unbehelligt zu bleiben und eben nicht im großen Cyberkriminellen-Datenhortungszentrum in Utah zu landen. Denn auch für die europäischen Schäfchen, die Yahoo, Facebook oder Hotmail noch nutzen, gilt: Die Dienste sind außerhalb Großbritanniens „externe Kommunikation“, die anlaßlos und ganz ohne Anfangsverdacht erhoben werden darf, um im Jargon der staatlichen Cyberkriminellen zu bleiben. Alle Internetkommunikation ist schließlich im Grunde irgendwo Auslandskommunikation.

Auf diesen Grundsatz beruft sich auch der BND bei seinen Versuchen, seine gemeinsamen Abschnorchel-Aktionen mit der NSA an deutschen Netzknoten zu legitimieren – alles natürlich, um den bösen Terrorismus einzudämmen.

Dumm nur, daß nach diesem Snowden-Jahr jeder, wer mit der ausgeleierten Floskel von der „Terror-Abwehr“ daherkommt, nur noch müdes Lachen erntet. Eine Ausnahme wäre höchstens zu machen, wenn man sich auf einen gehaltvollen Disput dazu einlassen wollte, ob Merkel, de Maizière oder Kiesewetter Terroristen in weiterem oder engerem Sinne wären, die man überwachen müßte – selbstredend äußerst grundrechtsschonend und alternativlos.

Gerade für Merkel und Co. bietet unser Heft praktische Lebenshilfe gegen Abhörbegehrlichkeiten aller Art: Ab Seite 18 kann sich der angehende Torrorist mit dem Anonymisierungswerkzeug Tor vertraut machen. Gleichzeitig setzen wir einen Schwerpunkt bei den zukünftigen Geheimdienstskandalen rund um biometrische, inklusive genetische sowie medizinische Daten (Seiten 35, 41, 45), außerdem Heimautomation (Seite 53), Automaten-Aushorchen (Seite 65), die unvermeidliche Cloud (Seite 81) und WLAN-Angriffe (Seite 58), wo noch einiges zu holen wäre.

Die dunkle Seite der Macht wird ab Seite 24 thematisiert, ein Must-read für alle, deren Leben nicht nur aus schmackhaften Fohlenrollen mit gedünsteten Möhrchen und abendlichen Quizshows besteht, für die wir ab Seite 77 (Post Privacy) und ab Seite 52 (Videoüberwachung) aber auch etwas im Angebot haben. Offene Gedanken zu Cryptowährungen gibt es ab Seite 69.

Auch wenn der Winter kommt und eine politische Lösung des Geheimdienstproblems noch ein wenig dauert, sind wir nicht ohne Hoffnung. Daher steht der Chaos Communication Congress 31C3 in Hamburg unter dem Motto „A New Dawn“. Nachdem wir nun endlich wissen, was auf der dunklen Seite der Macht wirklich passiert, können wir beginnen, aktiv etwas dagegen zu tun: bessere Verschlüsselungs- und Anonymisierungsmethoden entwickeln und überall einbauen, korrupte Hard- und Software reparieren oder neuschreiben und politische Systeme umbauen, um die Dienste letztendlich abzuschaffen.

[1] *http://ccc.de/updates/2014/chaos-computer-club-klagt-gegen-gchq*

Die Datenschleuder Nr. 97

Herausgeber (Abos, Adressen, Verwaltungstechnisches, etc.)
CCC e. V., Humboldtstraße 53, 22083 Hamburg
☎ +49.40.401801-0, Fax: +49.40.401801-41
office@ccc.de PGP: E0FF F5BD C953 22A1 A3AC 428E 9553 98C8 **129F DF75**

Redaktion (Artikel, Leserbriefe, Inhaltliches, Geldspenden, etc.)
Redaktion Datenschleuder, Postfach 64 02 36, 10048 Berlin, **<ds@ccc.de>**
☎ +49.40.401801-44, Fax: +49.40.401801-54

Druck Pinguindruck Berlin **http://pinguindruck.de/**
ViSdP Dirk Engling **<erdgeist@erdgeist.org>**
Chefredaktion hc, koeart, Bine, 46halbe, erdgeist
Layout hukl, erdgeist
Titelfoto; Rückseite Dominik Keller; prom

Inhalt

Aachen :: CCCAC :: Voidspace	Jülicher Str. 191, 52070 Aachen mittwochs ab 20 Uhr :: http://aachen.ccc.de/ :: mail@aachen.ccc.de
Berlin :: CCCB e. V.	Marienstr. 11, 10117 Berlin Club Discordia: dienstags und donnerstags ab 17 Uhr :: http://berlin.ccc.de/ :: mail@berlin.ccc.de
Bremen :: CCCHB e. V.	c/o AUCOOP, Weberstraße 18, 28203 Bremen dienstags ab 20 Uhr :: http://ccchb.de/ :: vorstand@ccchb.de PGP: D7AF 2B4C 37CD 3261 8354 9343 D36A 5E05 **AE3E CF64**
Chaos Darmstadt e. V. :: Trollhöhle	Wilhelm-Leuschner-Str. 36, 64293 Darmstadt dienstags ab 20 Uhr :: http://chaos-darmstadt.de/ :: info@chaos-darmstadt.de
Dresden :: Netzbiotop e. V.	GCHQ (Great Chaos Headquarter), Lingnerallee 3, 01069 Dresden offenes Chaos dienstags und donnerstags :: http://www.c3d2.de/ :: mail@c3d2.de
Düsseldorf :: Chaosdorf e. V.	Hüttenstr. 25, 40215 Düsseldorf freitags ab 18 Uhr :: https://chaosdorf.de/ :: mail@chaosdorf.de
Erlangen/Nürnberg/Fürth :: Bits'n'Bugs e. V.	E-Werk Erlangen, Fuchsenwiese 1, Gruppenraum 5 dienstags ab 19:30 Uhr :: http://erlangen.ccc.de/ :: mail@erlangen.ccc.de
Essen :: Chaospott	c/o foobar e. V., Sibyllastraße 9, 45136 Essen mittwochs ab 19 Uhr :: https://www.chaospott.de/ :: info@die-foobar.de
CCC Frankfurt e. V.	Schmidtstraße 12, 60326 Frankfurt, Rebstock donnerstags ab 19 Uhr :: http://ccc-ffm.de/ :: noreply@ccc-ffm.de
CCC Freiburg e. V.	ArTik, Kaiser-Joseph-Straße 141, 79089 Freiburg dienstags ab 19 Uhr :: http://www.cccfr.de/ :: mail@cccfr.de
CCC Göttingen :: Chaostreff Göttingen e. V.	NOKLAB, Neustadt 7 jeden 2. Dienstag ab 20 Uhr :: https://cccgoe.de/ :: hallo@cccgoe.de PGP: 50F3 137D 0114 7DB8 BCF3 84CE 2264 27FD **E4CF B4F8**
CCC Hansestadt Hamburg e. V.	Zeiseweg 9, Viktoria-Kaserne, Raum 119 (1. Stock, Ost-Flügel), 22765 Hamburg jeder letzte Donnerstag im Monat, ab 20 Uhr :: http://hamburg.ccc.de/ :: mail@hamburg.ccc.de
CCC Hannover :: Leitstelle 511 e. V.	Bürgerschule, Klaus-Müller-Kilian-Weg 2 (Schaufelder Str.), 30167 Hannover jeden 2. Mittwoch um 20 Uhr, letzten Sonntag ab 16 Uhr :: http://hannover.ccc.de :: kontakt@hannover.ccc.de PGP: 080D 1284 1646 706F E9DA 6A66 E29A 9635 **57FF 8AC8**
Kaiserslautern :: Chaos inKL. e. V.	Rudolf-Breitscheid-Straße 65, 67655 Kaiserslautern samstags ab 19 Uhr :: http://www.chaos-inkl.de/ :: info@chaos-inkl.de
Karlsruhe :: Entropia e. V.	Steinstr. 23 (Gewerbehof), sonntags ab 19:30 Uhr :: http://www.entropia.de/ :: info@entropia.de
CCC Kassel	Uni Kassel, Raum -1307, Wilhelmshöher Allee 71 (Ing.-Schule) erster Donnerstag ab 17 Uhr, http://kassel.ccc.de/ :: info@kassel.ccc.de
Köln, CCC Cologne (C4) e. V.	Heliosstr. 6a, 50825 Köln, donnerstags ab 18:00 Uhr, https://koeln.ccc.de :: mail@koeln.ccc.de
Mainz/Wiesbaden	Sedanplatz 7, 65183 Wiesbaden dienstags ab 19 Uhr :: http://www.cccmz.de/ :: kontakt@cccmz.de
CCC Mannheim e. V. :: C3MA	3. OG, Raum 2.4.15, Neckarauer Str. 106-116, 68163 Mannheim freitags ab 19 Uhr :: http://www.ccc-mannheim.de/ :: info@ccc-mannheim.de
CCC München e. V.	Schleißheimer Str. ++41, 80797 München jeden zweiten Dienstag im Monat ab 19:30 Uhr :: https://muc.ccc.de/ :: info@muc.ccc.de
Paderborn :: C3PB e.V.	Westernmauer 12-16, 33098 Paderborn, mittwochs ab 19 Uhr :: https://www.c3pb.de/
CCC Stuttgart e. V.	1. Dienstag Zadu-Bar (Reuchlinstraße 4b); 3. Mittwoch im shackspace (Ulmer Straße 255) je ab 18:30 Uhr :: https://www.cccs.de/ :: public@cccs.de
Ulm	BECI-Büro/Linux-Pool im Gebäudekreuz O27, Niveau 1, an der Uni Ulm montags ab 19:30 Uhr, http://ulm.ccc.de/ :: mail@ulm.ccc.de
Wien :: Metalab	Rathausstr. 6, 1010 Wien, Österreich, ab 19 Uhr :: http://www.metalab.at/ :: core@metalab.at
Chaos Computer Club Zürich CCCZH	Röschibachstrasse 26, 8037 Zürich :: mittwochs ab 19 Uhr :: https://www.ccczh.ch/

Es gibt in den folgenden Städten Chaostreffs: Aargau, Augsburg, Bamberg, Basel, Bielefeld, Bochum, Chemnitz, Dortmund, Frankfurt, Fulda, Gießen, Graz, Hanau, Heidelberg, Heilbronn, Hildesheim, Ingolstadt, Itzehoe, Jena, Kiel, Lahn-Dill-Kreis, Leipzig, Lübeck, Lëtzebuerg, Münster, Neuss, Offenburg, Regensburg, Rothenburg ob der Tauber, Salzburg, Siegen, Trier, Wetzlar, Würzburg, Wuppertal. Detailinformationen unter *http://www.ccc.de/regional/*

Re: Bilderrätsel #96

Die Redaktion war höchst erfreut, denn wir bekamen gleich mehrere korrekte Antworten auf unser letztes Bilderrätsel. Am detailliertesten beschreibt Casandro, was da zu sehen war:

Servus, das ist ein EBT 430 der Firma Schiederwerk aus Nürnberg. Ich glaube, das ist die Version mit Blindstopfen anstelle des Schlüsselschalters, da bin ich mir aber nicht sicher.

Das davor ist natürlich ein Inspizientensystem von der Firma Salzbrenner Stagetec aus Buttenheim. Ich vermute, das ist aus einem Theater. Das Grundgerät ist, glaube ich, eine Stage 300 oder ein Vorgängermodell. Die Geräte werden individuell gebaut. Das Inspizientensystem ermöglicht es dem Inspizienten im Theater, Signale an die anderen Abteilungen weiterzugeben. Beispielsweise ist da ein 100V-Rufsystem drin, mit dem man die Schauspieler in den Umkleidekabinen rufen kann. (100 Volt, damit man lange dünne Drähte verwenden kann.) Der Inspizient kann den Abteilungen auch Lichtsignale geben, anscheinend leuchtet dann eine rote Lampe in der entsprechenden Abteilung auf, kurz bevor die was machen müssen.

Ich denke, daß hier ganz konkret oben die Intercom- und Mithöranlage abgebildet ist, über die der Inspizient das Geschehen auf der Bühne verfolgen und Leute rufen kann. Vermutlich kann er über das Tastenfeld bestimmen, welche Lautsprecher er ansprechen will. Die Plätze für die Bildschirme sind wohl für die Mitschauanlage, die zu den Kameras führt, über die der Inspizient das Geschehen vor und hinter der Bühne [und den Dirigenten, Anm. d. Red] verfolgen kann. Über den Joystick (rechts auf dem Tisch) kann er eine Kamera steuern. Das ist aber nicht mein Fachgebiet, mit so was kenne ich mich nicht wirklich aus. *<Casandro>*

Herzlichen Glückwunsch, Casandro, Du hast schon wieder gewonnen! Wie man Casandros Ausführungen entnehmen kann, ist ein Inspizient so eine Art Fluglotse am Theater – mit dem Unterschied, daß er es nicht mit unbeständigem Wetter, hohen Gagen und dem einen oder anderen denkresistenten Piloten, sondern mit launischen Intendantinnen und (mitunter lampenfiebrigen) (Sänger-)Darstellern zu tun hat. Casandro, da Du in letzter Zeit jedes Bildrätsel gelöst hast, drucken wir in dieser Ausgabe das von Dir eingesandte Bilderrätsel ab!

Casandro erläutert: *„Das Gerät ist, wie man unschwer erkennen kann, ein deutsches Fabrikat aus Darmstadt. Es wurden ungefähr 100 bis 200 zum Listenpreis von etwa 250.000 DM gebaut und verkauft. Die Amerikaner haben damals grob 5.000 Stück von ihren etwa gleichwertigen Geräten verkauft. In der Billigversion kennt das Teil fast jeder, wobei diese Datenverarbeitungsanlagen immer seltener vorkommen."*

Leserbriefe

Sehr geehrte Damen und Herren, der Torfkurier hat im März das Schwerpunktthema „Menschen ohne PC". Wir werden in einer Reihe von Artikeln unter verschiedenen Gesichtspunkten diesem Thema nachgehen und würden gerne dafür auch einen Vertreter des Chaos Computer Clubs interviewen. Stünde jemand kurzfristig dafür bereit? Wenn ja, melden Sie sich doch bitte unter 0621-4XXXXXX. Vielen Dank, mit freundlichen Grüßen ... *<Nicolas S.>*

Sehr geehrte Damen und Herren. Leider können wir Ihnen zum Thema „Menschen ohne PC" nichts sagen, das ist nicht unser Fachgebiet. Viele Grüße, <dodger>

Sehr geehrte Damen und Herren, hallo mein Nachbar wollte mir in der letzten Woche Skype schmackhaft machen, nach sehr kurzer Überlegung habe ich mich dort eingeloggt. Und schon wieder sind Daten von mir im Netz, was ich im Nachhinein eigentlich nicht wollte. Und als ich mein Namen googelte oh Schreck, gab es von mir eine Facebookseite. Meine Frage: Gibt es ein Zusammenhang zwischen Skype und Facebook, und hat diese Facebookseite wirklich was mit mir zu tun ? Hab mich mit meinen Daten versucht bei Facebook einzuloggen bekomme aber kein Zugang. Ich habe den Verdacht das die beiden Skype und Facebook sich die Daten zu schieben.

Groteske Diskussion

Zu unserem Artikel „Vorsicht, Sie werden gefilmt!" (TV vom 22. März) schreibt dieser Leser:

Selten hat mich ein Artikel so amüsiert wie jener über die Kritik des Chaos Computer Clubs Trier und der Piratenpartei über das Vorhaben der Polizei, Überwachungskameras zur Heilig-Rock-Wallfahrt einzusetzen.

Die Piratenpartei und der Chaos Computer Club als Gralshüter der Privatsphäre, besser geht es nicht!

Genau jene Organisationen, die für ein absolut freies Internet plädieren, wo Tausende von Menschen jeden Tag in youtube und ähnlichen Portalen ohne Erlaubnis gefilmt und vor Millionen Menschen lächerlich gemacht werden!

Genauso grotesk ist die Diskussion über das Thema Überwachung bei Facebook, wo sich mittlerweile ein breites Publikum über die täglichen Toilettengewohnheiten eines 16-Jährigen informieren kann.

Und das vor zehn Millionen Webcams!

Vor Lachen kann ich den Artikel kaum noch zu Ende lesen. Jetzt kommt es aber: Der Piratenkapitän Christian Hautmann stellt fest, „die Ausübung des Glaubens sei eine intime Angelegenheit"!

Das stimmt natürlich, nur aus dem Munde eines Internetrebells hört es sich ein wenig heuchlerisch an ...

■ Eine Sku

Trier. „Lebenslir Fadenskulptur, d Höhe entsteht. I schnüren ist ein

GESUNDHEIT

Mit Louis

Zu unserer Them

Ich möchte mich freund bedanke ganze Seite den Down-Syndrom ihrem Tag gewi wird Zeit, dass wie l(i)ebenswe schen sind. Für selbstverständli

QUELLE: OFFLINE

Vielleicht hat der ccc. eine Antwort Wenn ja vielen Dank und schöne Weihnachten. <Stephan>

Lieber Stephan, nach kurzer Überlegung habe ich Deine E-Mail als Leserbrief aufgenommen. Und schon wieder sind ein paar Textzeilen mehr zu setzen, wieder eine Seite mehr, die deshalb gedruckt werden muß, was ich im Nachhinein eigentlich nicht wollte. Eine Frage: Gibt es eigentlich einen Zusammenhang zwischen dem Computer-ADAC und dem CCC? Habe den Verdacht, daß der eine dem anderen Leute zuschiebt. Vielleicht weißt Du. ja eine Wenn ja vielen Dank und schöne Weihnachten. <hc>

hallo, könntet Ihr einmal in der „datenschleuder" nahfragen, wer an 33 Mio. domainnamen ggf. Interesse hat? 12 Mio. domains stammen von vor ca. 8. Jahren und haben je eine PIN. Jetzt habe ih 33 Mio. domains, aber die Prüfung mit PING ist doch sehr aufwendig. Mehrere Programme und Prozeduren liefern die PIN und auch eine Umleitung über eine andere domain und deren PIN, bzw. einen Fehler, wenn der DNS die domain nicht kennt. Diese Programme und Prozeduren und den bisher gesammelten Datenbestand könnte ich Euch bei Interesse überlassen. Herzliche Grüße und viel Erfolg im neuen Jahr! <Erhard>

Antwort: Na klar, hiermit geschehen. Wir übermitteln Dir dann die Liste der Interessenten. <hc>

Hallo Caos Computer Club, Sehr verehrte Damen und Herren, Lassen Sie den Datenverkehr im Inside fehlerfrei arbeiten. Mit Ihrer Internetkriminaltät und Bedrohungen wird das mal unberechenbar enden. Arbeiten Sie lieber an der Entwicklung eines uralten neuen Zeichens, das in die Betriebesysteme in den Zeichensatz integriert werden soll mit. „Die Null mit zwei schräg zueinander paralell angeordneten Strichen in der Null". [(\\) so in etwa.] siehe auch Dateianhang Mit freundlichen Grüßen <Jürgen B.>

Wir haben uns in den letzten Monaten verstärkt bemüht, den Datenverkehr im Inside korrekt arbeiten zu lassen. Unsere Internetkriminalität konnte im selben Zeitraum gegenüber der Autokriminalität, der Telefonkriminalität, der Briefkriminalität und der Wirtschaftskriminalität zurückgedrängt werden. Wir bedauern allerdings mitteilen zu müssen, bei den Betriebesystemen gescheitert zu sein. <conz>

Presse-Anfrage Hallo, mein Name ist Thomas Röthemeier von der BILD-Hamburg. Habe eine Frage zum Thema passwortgeschütze Festplatten. Vielleicht könnte mich der Presse-Sprecher oder ein Experte für die aktuelle Ausgabe zurückrufen. Mit freundlichen Grüßen <Thomas Röthemeier Axel Springer AG BILD, Axel-Springer-Platz 1>

Antwort: ...und mein Name ist Constanze von dieser Hackergruppe da. Leider übernehmen wir keinen Support für Boulevard-Blätter. <conz>

Freitagsrätsel der FAZ „Homerisches Gelächter beim Chaos Computer Club gab es bei dieser Staatsattacke“ - 15 Buchstaben)

Der Bildbeweis wird gerne unter ds@ccc.de entgegengenommen.

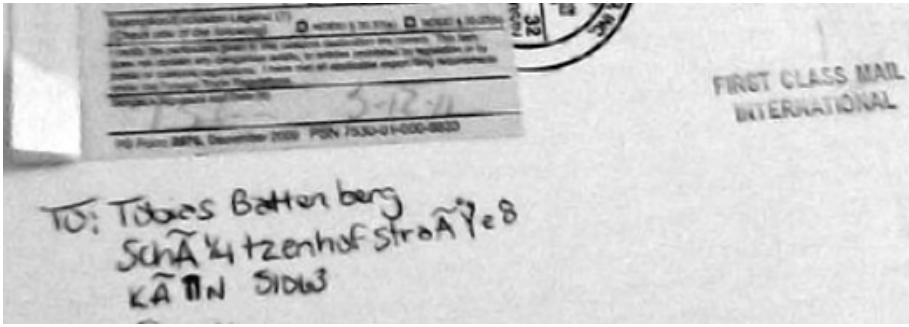
Hallo CCC, eine Frage: Gibt es einen GEMA-Trojaner im Verbund mit Microsoft unter Win.32. GEMA - angezeigt von Spybot - ? *<M.Sp.>*

Antwort: Sicher nicht, denn Trojaner schreiben ist streng verboten. <hc>

Sehr geehrte Damen und Herren, ich habe am 03.11.2012 im Auftrag der Foo Bar AG, 8 Ausgaben der Datenschleuder bei Ihnen bestellt. Am 12.12.2011 erhielt ich von Ihrem Mitarbeiter Herr starbug eine Mail, mit dem Hinweis, dass der Betrag in Höhe von 32,00 Euro erst beglichen werden muss, bevor uns eine Rechnung bzw. die Ausgaben der Datenschleuder zu geschickt werden können. Am 13.12.2011 antwortete ich Herrn starbug mit der Bitte um Zusendung der Rechnung, da es uns nicht möglich ist, in unserer Verwaltung eine Zahlung anzuweisen ohne Rechnung. Bis zum 13.01.2012 erhielt ich weder eine Information von Herrn starbug, noch eine Rechnung oder Lieferung. Daraufhin schrieb ich Herrn starbug nochmals an, mit der Bitte um Antwort bzw. Bearbeitung. Bis zum heutigen Tag erhielt ich immer noch keine Antwort. Die Kollegen benötigen die Ausgaben der Datenschleuder für Ihre dienstliche Arbeit. Somit möchte ich Sie nochmals um Antwort oder Stellungnahme bitten bzw. Zusendung der Rechnung und den 8 Ausgaben der Datenschleuder zum Stand ab 03.11.2011. Mit freundlichen Grüßen *<am>*

Antwort: Liebe potentielle Abonnenten, wir bitten um Verzeihung für unseren Mitarbeiter, den wir aufgrund der Pflichtverletzung ins Darknet entlassen mußten. Jedoch ist der von Ihnen gewünschte Service leider nur in der Datenschleuder-Gold-Edition enthalten, die Sie gern bei uns in Auftrag geben können. Zu diesem Zwecke überweisen Sie bitte die Aufnahmegebühr in Höhe von nur 2998,98 Euro auf unser Verlagskonto. Unmittelbar nach Verbuchung und Vereinnahmung geht Ihnen neben der Datenschleuder – von der Sie alte Ausgaben als Premium-Mitglied übrigens exklusiv per https und gopher von ds.ccc.de herunterladen können – natürlich auch unser hochwertiger Präsentkorb als persönliches Dankeschön zu. <die Redaktion>

ich werde auf den tag an dem ihr etwas schafft worauf ihr ein urheberrecht beanspruchen könnt das euch erlaubt anständig zu leben - da werdet ihr aufheulen wenn jeder dann sagt, ihr könnt euch eure tantiemen in den arsch stecken - bis dahin seid ihr unkreative leute die zwar einen sozialen zweck erfüllen aber zur produktivität in



der gesellschaft herzlich wenig beitragen - von was leben eigentlich all die freiwilligen, die bei euch mitmachen? von den eltern, von der stütze, teilweise ja auch von (sogar zum teil erheblichen) erbschaften! da muss also jemand etwas produziert haben, damit all diese „freiwilligen" „uneigennützig" bei euch mitmachen können - in zehn jahren wird jeder merken, was ihr heute schon seit, die grössten spiesser - ihr produziert nichts, ihr redet viel scheisse, ihr lebt vom geld der anderen und derer die euch mit geld unterstützen - wo kommt die kohle denn her? einer muss ja arbeiten, ihr seid das nicht - die welt braucht euch nicht, denkt mal daran - - also überlegt mal gefälligst ehe ihr euren blödsinn verzapft - nur weil man hacken kann ist kein zeichen von intelligenz, und schon garnicht von sozialer relevanz - ps: habt ihr schon mal daran gedacht, dass ihr euch euer brot beim bäcker gratis downloaden könnt? und eure klamotten? - not a dime anymore, never again! *<John T.>*

Lieber John, es tut uns außerordentlich leid, eine solche Verzweiflung aus Deinem Brief herauslesen zu müssen. Auch Deine Wortwahl sowie Orthographie läßt uns innehalten. Aber da Du konkrete Fragen stellst, möchte ich Dir auch konkret antworten: Ja, ich denke oft daran, mir Brot oder Klamotten zu downloaden. Ich fände das ungemein praktisch. Du etwa nicht?! Und weißt Du, wer an genau solchen Technologien arbeitet, die dieses und ähnliches bald möglich machen werden? Und an den Technologien, die möglich gemacht haben, daß Du uns diesen Brief schreibst? Richtig. Wir. Die, die nichts Produktives beizutragen haben. Herzliche Grüße <Bine>

Hallo Datenschleuder-Redaktion, ich bin auch Mitglied beim CCC (Chaos-Nr.: 4223) und sehe das Thema immaterielle Monopolrechte auch aus Sicht des Wissenschaftlers sowie eines Kreativen, der neben Skripten und Programmen nicht nur Zeitschriften-Artikel und Bücher geschrieben hat, sondern auch Patente und Marken hat und daher auch Mitglied ist bei VG Wort und DEV (Deutscher Erfinder-Verband). An dem offenen Brief der Tatort-Drehbuchschreiber und ähnlicher Urheberrechts-Propaganda finde ich am meisten empörend, dass diese einfachen Urheber möchten, dass so ziemlich alles bezahlt wird und der Eindruck erweckt wird, dass Kostenloses illegal ist, aber dabei sind die einfachen Urheber selber die schlimmsten Kostenlos-Fanatiker, denn die zahlen keine Anmeldegebühr, keine Prüfungsgebühr und keine Jahresgebühr - obwohl selbst ein kleiner Erfinder all diese Gebühren für sein immaterielles Monopolrecht (Patent) zahlen muss, wobei u.a. noch hinzu kommt, dass der Erfinder Anmelden und Offenlegen muss und er nur im jeweiligen Land für relativ kurze Zeit das Monopolrecht erhält. Ähnlich ist es mit Marken und vielen anderen immateriellen Monopolrechten. Aus Sicht der Erfinder, Markeninhaber usw. leben die einfachen Urheber in einer Umsonstkultur und begehen mit ihrem kostenlosen und weltweiten Urheberrecht eine neokoloniale gewerbliche Gebührenhinterziehung und Rechteerschleichung auf chaotische und anarchistische Weise. Umgekehrt ist es nicht selten gesetzlich vorgeschrieben, dass kostenlos und ohne einschränkende Nutzungsbedingungen zur Verfügung gestellt werden muss. Ein Beispiel sind Doktorarbeiten, die nicht nur arbeitsmäßig aufwendig sind, sondern auch eine wissenschaftliche Schöpfungshöhe nachweisen müssen und kostenlos der Universitätsbibliothek zur Verfügung gestellt werden müssen. Beispielsweise kann man meine Dissertation, die ich nach der Promotionsordnung auch an die Universitätsbibliothek geben musste,barrierefrei von *http://vts.uni-ulm.de/docs/2007/5887/vts_5887_7873.pdf* downloaden, wie viele andere Dissertationen auch. Zu dem Thema habe ich deshalb einen Aufsatz geschrieben: *http://www.true-random.com/homepage/projects/liberal/zensur/urheberrecht_digital.odf* Mit freundlichen Grüßen, <Dr. Rolf Freitag>

Kein Kommentar, der Leserbrief sagt mehr über den Leser als über die Tatort-Drehbuchschreiber.

Hallo liebe CCC´ler, da bei uns im Hause die Beantragung eines neuen Reisepaß ins Haus steht, habe ich mich nochmals ausführlich mit der Situation in Sachen E-Pass und dem damit verbundenen Zwang zur Abgabe von Fingerabdrücken auseinandergesetzt.

Meine Frage: Gibt es andere sinnvolle Handlungsempfehlung, als den Boykott des E-Pass und damit als einzige Möglichkeit die Beantragung eines vorl. Reisepass (wobei hier auch glaubhaft die „Eile“ dargelegt werden muß)?

Gibt es zwischenzeitlich Erfahrungswerte anderer Bürger, wie hier vorgegangen werden kann um keine Fingerabdrücke abgegen zu müssen, Erfahrungen aus der „Situation“ bei der Beantragung?

Ich habe mir den sehr unterhaltsammen Vortrag vom 24c3 „Meine Finger gehören mir“ angesehen, das war zwar sehr informativ jedoch ist dieser Vortrag ja auch zu einer Zeit entstanden, als das System noch ganz am Anfang stand.

Fakt ist, hier möchte niemand seine Fingerabdrücke dem Staat zur Verfügung stellen. <Moe>

Hallo Moe, was die biometrischen Paßbilder angeht, kann man oft schon beim Fotografen manipulationen vornehmen lassen (Stauchen oder sonstiges Verzerren der Proportionen, die dem menschlichen Auge nicht auffallen).

Bei den Fingerabdrucken hilft aus unserer Erfahrung nur Sekundenkleber, der zuverlässig dazu führt, daß keine Abdrücke vom Sensor aufgenommen werden können. Allerdings braucht man eine gewisse Geduld, da es meistens mehrfach versucht wird, Abdrücke zu nehmen, bis der Beamte auf dem Bürgeramt dann den „keine Finger“-Button drückt. Es schadet auch nicht, auf häufigen beruflichen Kontakt mit Chemikalien hinzuweisen. Ich habe beispielsweise behauptet, daß ich als Friseur arbeite.

Wenn man sich das nicht traut, kann man sich auch eine Hand oder mehrere Finger verbinden, um eben nur den übriggebliebenen Ringfinger einer hand abgeben zu müssen oder so was. Was natürlich nachher hilft, ist das Deaktivieren des Chips, der die Digitaldaten der Biometrie enthält. Dazu ist aber ohnehin zu raten.

Ansonsten läuft ein Verfahren u. a. eines Deutschen vor dem europäischen Gerichtshof, bei dem aber noch keine Entscheidung ergangen ist. (Vermutlich wird das leider nicht zugunsten des Beschwerdeführers ausgehen.) https://www.ccc.de/de/updates/2013/eugh-biometrie <aluburka>

Hallo DS-Team, hallo Herr Palm, endlich hat sich jemand dem Thema „KV-SafeNet“ angenommen. Sollten Sie weiterhin an dem Thema dran bleiben, hier ein paar Infos: – KV-SafeNet ist tot (gescheitert) -> „Alternative 2012“ ist das neue Thema zusammen mit der eGK – Mit DGN haben Sie leider den falschen Provider im Fokus gehabt (wurde nur aus kartellrechtlichen Gründen nicht von dem wirklichen Proviteur gekauft – siehe weiter Unten).

GN wurde inzwischen „geparkt“ und wird von den Gesellschaftern der „Frey ADV GmbH“ (GUS Box – lol) geführt. – 23 (25) Provider waren eindeutig 22 zu viel, darum wird sich das ändern und ein echtes Monopol geschaffen –Für das „neue“ SafeNet (eGK-Netz) wird es nur noch einen Hersteller für Konnektoren geben KoCo-Box: *http://www.kococonnector.com/* cui bono?

Seit 10 Jahren konsulidiert ein Unternehmen den gesamten „IT-technischen“ Medizinmarkt:

http://www.cgm.com/ Gewinn 2010: 67 Millionen Euro. Dort tummeln sich unter anderem: Frank Gotthardt Vorstandsvorsitzender, CEO Prof. Dr. Klaus Steffens, Vorsitzender ehem. Geschäftsführer der MTU Aero Engines GmbH Dr. Klaus Esser, stellv. Vorsitzender ehem. Vorstandsvorsitzender der Mannesmann AG Martanteil Deutschland >60% Die KoCo Connector AG hat als einziges Unternehmen einen eGK Connector auf dem Markt, der in Step 2 der „alternative 2012" zum Einsatz kommen kann. Frank Gotthardt ist an der KoCo Connector AG (!vermutlich! – sehr vermutlich ;-)) beteiligt (ursprünglich gemeinsames Projekt von Gottahrd und dem ehemaligen Siemens Verantwortlichen für das KV-SafeNet Norbert Kollack), diese taucht aber seit 2009 nicht mehr in dem Geschäftsbericht der CGM auf. Der einzige deutsche ernst zu nehmende Konkurrent „MCS" arbeitet über die Schweiz bereits mit „seinem größten Rivalen" im Bereich EGK-Konnektor zusammen.

Alle Unternehmen der Compugroup werden massiv bedrängt, die KoCo-Box zu promoten (Konventionalstrafen, bei nicht erreichen der Vorgabeziele). KV-SafeNet ist im Übrigen löchrig wie ein schweizer Käse. Die Passworte für die konfiguration der „BlackBoxen" kennt so zimlich jeder, der die teile vor Ort einrichten muss. Die Fernadministration hat leider einen anderen Hintergrund – die Techniker vor Ort wären zum Großteil damit einfach überfordert. Es geht bei KV-SafeNet bzw. der eGK nicht um besseren Service, Mehrwert, bessere Gesundheitsversorgung (lol), abhören von Arztpraxen oder irgendeinem anderen Thema, es geht nur und ausschließlich um Marktmacht! Wenn ihr weiter an dem Thema dran bleiben wollt, schaut euch mal die „KoCo-Box" der KoCo Connector AG genauer an. Und ich meine nicht nur unbedingt technisch – sondern eher „politisch". Offiziell hat die KoCo-Box nichts mit der CGM zu tun, ist aber dennoch die Schnittstelle, die alle miteinander verbindet. Aber daran denken, wer anfängt in der Scheisse zu rühren ... Noch ein Goodie zum Schluss: Macht ja nicht die Batterie aus der KoCo-Box, falls ihr eine in die Finger bekommt, ihr werdet sehen warum (und nicht schütteln!). Falls ihr ein Gerät haben wollt, sollte das kein Problem sein, denn der CCC Berlin und die KoCo Connector AG sind ja Nachbarn.

P.S: Hallo Herr Palm, aus ihrer Perspektive (und technisch) war der Artikel richtig, aber er kratzt noch nicht einmal am Lack des eigentlichen Skandals. Leider ist er auch nicht mehr ganz up to date – trotzdem ein Dankeschön. Und ganz zum Schluss: Warum ich euch das schreibe? Weil ich keinen Bock darauf habe, dass meine Gesundheit zukünftig von einem einzigen Konzern abhängt! Seit nicht zu erfogreich, sonst bin ich arbeitslos. *<DS Leser>*

Hallo, da ich auf der Internetseite von CCC keine andere Kontaktadresse gefunden habe, schreibe ich eben dem Vereinsblatt. Ich bin froh, dass die Polizei ein Instrument in der Hand hatte (das hat CCC ja toll ausposaunt) mit dem sie den Verbrechern und Terroristen unter Umständen einen Schritt voraus sein konnte. Denkt bei euch eigentlich mal jemand über die Konsequenzen eurer illegalen Tätigkeit nach?????? Durch die Veröffentlichung der Erkenntnis über die Überwachungssoftware gefährdet ihr uns alle ! Ihr zwingt unsere Einrichtung für unsere Sicherheit in Deutschland (=Polizei) mit der Steinschleuder gegen die Maschinenpistolen der Mafia und den Sprengsätzen der Terroristen vorzugehen. Wer von euch traut sich solche Erkenntnisse über die Mafia oder Terroristenvereinigungen öffentlich in der Presse zu bringen?

Ich möchte es noch mal sagen: was CCC hier gemacht hat ist unverantwortlich und gefährdet uns normale Bürger. Menschen mit soviel Intelligenz sollten auch mal Verstand und Gehirn benutzen. Sollten Sie nicht der richtige Adressat sein, wäre es nett von Ihnen, wenn Sie dieses Mail an den Computerclub weiterleiten würden. Gruß *<Renate>*

P.S. Ich bin eine 50 jährige Durchschnittsbürgerin

Hallo Renate, wir sind schon der richtige Adressat für gehaltvolle Leserbriefe. Leider müssen wir Ihnen mitteilen, daß die Polizei mit dem Instrument Staats-

trojaner in der vorliegenden Form niemandem einen Schritt voraus ist, schon gar nicht „Terroristen mit Sprengsätzen". Daß wir nach Ihrer Ansicht nur ein paar dümmliche Gestalten sind, wenn wir fragen, was die Tatsachen bei staatlicher Spionagesoftware und bei der Einhaltung der Grundrechte sind, bedauern wir sehr. Aus Ihrem Brief geht aber unzweifelhaft hervor, daß eine Diskussion hierüber wenig erfolgversprechend ist. Ihren Vorschlag, statt Intelligenz mal Verstand und Gehirn zu benutzen, haben wir jedoch vereinsintern weitergeleitet, und er wird nun in unseren Ausschüssen und Unterausschüssen sehr ernstgenommen und kontrovers diskutiert. <hc>

^M schrieb uns ganz aufgebracht:

Hallo liebe Leute,^M ^Mleider passiert mir zu wenig bei und über euch. Nicht mal die Datenschleuder bekomme ich gesendet.^MStaubig ist die Webseite und wohl der Rest auch. ach naja, ich hatte mit das anders vorgestellt.^M ^MIch bitte um ^MKündigung der Mitgliedschaft^Mzum nächstmöglichen Termin.^M ^MBitte bestätigen, danke.^M^MMit freundlichen Grüßen aus Oberursel,^M<^Marcus>

Antwort: Sehr geehrter ^Marcus, Sie erhalten diese Nachricht, weil Sie sich über unseren Service beschwert haben. Mit Bedauern bestätigen wir Ihnen die Durchführung des Auftrages zur Mitgliedschaftskündigung unter Ihrer Chaosnummer 2342. Die Kündigung der Mitgliedschaft wurde vollständig durch uns bearbeitet. Unter Umständen hat etwas nicht so funktioniert, wie Sie es sich gewünscht hätten, oder waren Sie unzufrieden? Wenn wir etwas besser hätten machen können oder wir Sie doch weiterhin betreuen dürfen, freuen wir uns über eine kurze Nachricht. <CCC Support>

Sehr geheerter Empfänger des CCC Ich würde gerne Hacken lernen, aber ich weis nicht wie!Muss ich eine Programmiersprache können-Wenn JA welche (Java, C, C++ etc.)Welche Kenntnisse sollte ich habe um Hacker zu +werden? <Jaro>

Ich glaube zunächst müssen wir mal feststellen, was du unter „Hacken" verstehst und was zum Beispiel der CCC damit verbindet. Ich nehme mal an, Du hast die üblichen Informationen auf http://ccc.de/ *schon mal so grob studiert? Insbesondere die Hackerethik lege ich dir kurz ans Herz.*

Ich versuchs mal konfuzianisch: Der einzige Weg zu hacken ist zu hacken.

Umständlicher ausgedrückt: beschäftige Dich mit der Technik um Dich herum, finde interessante Wege die Dinge um dich herum zu verwenden, zu verändern oder zu kombinieren und du bist mitten im Hackerparadies. Es gibt die faszinierendsten Dinge zu machen. (Mein aktuelles Lieblingsteil ist ein Laserplotter aus den Teilen zweier alter CD-Brenner, kreativstes Upcycling der feinsten Sorte, da steh ich drauf.) Im Clubumfeld gibt es Leute, die alles mögliche erschaffen, von der Richtfunkantenne bis zum Mehrpunkt-Touchscreen im Format 1,5 zu 1 Meter.

Genauso wie die Wege nach Rom, führen alle Werkzeuge nach Hack. Das einzig wichtige Werkzeug trägst du in deiner Hirnschale spazieren. Lerne, Hinterfrage, Denke, Probiere und Scheitere einige Male, am Ende bist Du klüger.

Wenn Du denn unbedingt was mit Computern machen willst ... Hängt die Sprache ebenso ernsthaft davon ab, was du machen willst. Kaum einer würde auf die Idee kommen, einen Webserver in Assembler zu bauen. – Und auch nicht viele wollen einen Hardware-Treiber in R hacken. Auch wenns witzig wäre und ein echter Hack.

Zuletzt willst Du vielleicht auch einfach mal bei einem Chaostreff, Erfa oder Hackerspace vorbeischauen.

Solltest du letztendlich auf „Praktische IT-Sicherheit" anspielen, dann gibts auch dazu ein ganzes Internet voller Dinge. Ich empfehle aber zumindest mal, rudimentäres Wissen über Programmierung,Rechnerarchitektur, Rechnernetze und Betriebssysteme anzuhäufen. <Lars>

Jaro geht in sich und antwortet:

Ich würde gerne in PC's mit Windows oder mac hacken können und Webserver hacken und pc's austricksen können! <Jaro>

```
0x20 Plonk!
0x10 Du bist kein Troll.
0x08 Du bist in der Lage, eine Suchmaschine
     zu benutzen.
0x04 Du hast die Dir gegebenen Hinweise
     verstanden.
0x02 Du bist hier falsch.
0x01 Ich würde gerne zaubern können.
     set_flag(you, 0x13);
```

Komm wieder, wenn Du verstehst, warum eine Bitinvertierung Dir an dieser Stelle weiterhilft, aber vorsichtig verwendet werden sollte. <lars>

Doch Jaro läßt nicht locker:

HAllo... Ich möchte gerne Hacken lernen, unter ‚hacken' verstehe ich : - In fremde PC's & Server eindringen +- Windows7 und mac Passworteingabe umgehenWas muss ich können? -Programmiersprachen(Java, C++, c, asp, php, vb, Assembler, php, sql, Haskell)?? Wenn JA welche und WO kann ich +die ausführlich lernen??-Systemanforderungen(Windows 32 oder 64 bit)??-Bei Windows Ahnung mit CMD und batch?? In wiefern ist hacken legal?? Post Scriptum:-ich kann die Batch grunglagen reichen diese?Ich wäre froh so schnell wie möchlich auf meine FRagen antworten zubekommen <Jaro>

Dem aufmerksamen Leser wird nicht entgangen sein, daß er ‚Haskell' in die Liste seiner Programmiersprachen aufgenommen hat und außerdem nun erklärt, was er unter ‚hacken' versteht, dafür aber leider auf Lars' Bitinvertierung überhaupt nicht eingeht. :]

Hallo CCC (via Datenschleuder) – danke für Eure Antwort auf den Offenen Brief, dessen Mitunterzeichner ich bin. Vorab eines: Über die Antwort war ich glücklicher als über den Brief selber, der imho den falschen Ton erwischt. Böser Fehler, die Netzgemeinde in einen großen Topf zu werfen, ohne nachzusehen, was da alles drinnen schwimmt.

Reden wir über Realitäten. Autor sein ist keine Nebenbeschäftigung. Geschichten zu finden und zu erzählen braucht Zeit und einen freien Kopf. Der läßt sich deutlich leichter herstellen, wenn man nicht Sorge haben muß, daß einem gleich der Strom abgestellt wird. Die Frage ist, ob diese Art der Geschichten noch erwünscht ist. Ich rede ausdrücklich nicht über Tatort-Autoren, sondern über unsere Kultur. Alles was uns aus der Vergangenheit geblieben ist, was wir erinnern, was uns vielleicht davon abhält, uns gegenseitig mit großen Keulen die Köpfe einzuschlagen, sind die Werke, die irgendwann einmal von jemandem erschaffen wurden, der sich einen geistigen Freiraum erschaffen hat. Was passiert, wenn es keine Geschichten mehr gibt, keine Songs, keine Filme, weil diejenigen, die sie erschaffen, sich einen anderen Lebenserwerb suchen müssen? Klar sind wir im digitalen Zeitalter angekommen, keine Frage. Nur - ist es sinnvoll, die Freiheit der Netz-Kommunikation gleich zu setzen mit einem: „Es bedarf keiner Schöpfer mehr, die Community liefert die Inhalte kostenfrei?" Ich frage mich, was von dem ganzen täglichen elektronischen Grundrauschen für meine Urenkel erhalten bleiben wird. Vermutlich wenig.

Nicht daß Ihr jetzt denkt, ich würde „Tatorte“ zum Kulturgut der Menschheit rechnen. Aber eine langsame Aufweichung und Zerstörung der Lebensgrundlagen betrifft ja nicht nur die Tatort-Autoren, sondern alle, die ihre Lebenszeit investieren, um etwas Bleibendes, Weitergebbares, ein paar helle Gedanken in einen stupiden Alltag Zauberndes zu erschaffen.

Ich persönlich glaube nicht, daß die Netzgemeinde samt und sonders daran interessiert ist, eine „apokalyptische Zeit der Kulturlosigkeit“ einzuläuten. Im Gegenteil. Ich brauche die Freiheit des Netzes und ihre mühelose und atemberaubend fortschrittliche Möglichkeit, die Welt endlich neu zu begreifen. Ich bin überzeugt davon, daß sich neben dem ganzen Gelabere heute die hellsten und klarsten Gedanken im Netz finden. Aber wird das bleiben, was an Ideen, Anregungen, Veränderungen täglich verschossen wird? Ihr habt möglicherweise recht mit Eurer Sicht, daß die meisten Autoren anderen Tribut schulden, auf deren Schultern sie stehen, nicht unbedingt nur E. A. Poe, wie Sir Conan Doyle meint. Aber jedes Buch, jedes Musikstück, jeder Film und vermutlich auch jede Software baut auf den Gedanken anderer auf. Nur muß sich jemand hinsetzen, seinen Verstand benutzen, sein Wissen, sein Erfahrenes und Erlesenes, um aus dieser kulturellen Ursuppe Neues erschaffen zu können.

Wenn unsere Gesellschaft insgesamt davon profitiert, daß sie auf so Erschaffenes zurück greifen kann, dann frage ich mich schon, wer eigentlich ein Interesse daran haben kann, diesen Sammlern und Schöpfern unserer Kultur die Lebensberechtigung abzusprechen. Wer meinen kann, daß man sie einfach einsparen sollte und durch das kollektive Austauschen der Community ersetzen. Denn: Auch wenn diese Community überragende Arbeit darin leistet, alle Gedanken der Welt zu sammeln, Enzyklopädien des menschlichen Wissens zu erschaffen – irgendwann kommt der Punkt, an dem alles Wissen eingesammelt, alles Vorhandene vernetzt ist. Und dann? Gibt es dann noch große, neue Ideen? Gibt es Romane, die die gemeinsame Fantasie in neue Welten führen, Filme, die jeder Mensch sehen möchte, Musik, die viele tauschen und die sie zusammen glücklich macht? Gibt es dann den einen, großen, singulären Input, den auch die Community braucht, um ihre eigenen Ideen entwickeln zu können?

Was hat das mit ACTA zu tun? ACTA ist einfach ein rundum unglücklicher Weg, sich quasi per Erlaß in die immanente Unterschiedlichkeit der Interessen zwischen Schaffen und Teilen einzumischen. Wie immer, wenn Staat und Gesellschaft versuchen, etwas festzuschreiben, kommt dabei eine Verkürzung heraus, die eher schadet als nützt. Viel wichtiger wären grundsätzliche Überlegungen: Wer verdient an der Freiheit des Netzes? Wer schafft sich Milliardenvermögen dadurch, daß er anderer Menschen Geist und Arbeit für seine Zwecke einsetzt? Und, vor allem: Wieso bedienen wir alle, mich eingeschlossen, uns jeden Tag so klammheimlich und bedenkenlos all dessen, was Andere erschaffen haben? Ich fürchte die Anonymisierung und Vergemeinschaftung geistiger Werke könnte eines Tages zum großen Problem unserer Kultur werden. Wenn eine Gesellschaft keinen Respekt mehr zeigt vor dem, was einzelne ihrer Mitglieder leisten, dann verliert sie womöglich auch insgesamt den Respekt vor den Individuen, aus denen sie sich zusammensetzt.

Man kann lange über Schutzfristen und deren Notwendigkeit diskutieren. Es gibt Beispiele, in denen Enkelgenerationen gedankenlos von Vermögen zehren, die ein Vorfahre mit einem geistigen Werk erarbeitet hat. Es gibt die Gegenbewegung der völligen Ausbeutung durch gnadenlose Stückverträge, an denen nur noch clevere Vermarkter profitieren. All das geht am Kern der Diskussion vorbei. Der da wäre: Warum geben wir ohne Murren unsere Kohle an Immobilienbesitzer, Mineralölkonzerne, Lebensmittelgiganten, stehlen uns aber einfach zusammen, was wir an geistiger Grundausstattung benötigen? Leisten wir uns Kultur, auch wenn sie schutzloser ist als eine panzerglasgesicherte Bank und deutlich nahrhafter als das tägliche Fast Food unserer (!) Community? *<LG Michael Wogh>*

Dieser Leserbrief stellt die persönliche Meinung Michael Woghs dar.

Sehr geehrte Damen und Herren, mit Interesse (und auch ein paar Wochen Verspätung) habe ich die Replik des CCC auf den offenen Brief der Tatort-Autoren zum Thema Urheberrecht gelesen. Eine Sache hat mich dabei irritiert: Während der Brief der 51 Autoren mit 51 leicht zuzuordnenden Namen unterschrieben war, vermisse ich Selbiges bei Ihrer Antwort. Explizit verweisen Sie in Ihrer Replik darauf, daß dies eine Erwiederung von 51 Persönlichkeiten sei, die ebenfalls Urheber sind. Hacker, Musiker usw.

Nun ist ja der Witz von Gemeinschaftsbriefen der, daß sie gemeinschaftlich unterzeichnet werden. Ansonsten könnte ja jeder behaupten, daß er hier einen offenen Brief im Namen von z.Bsp 51 Komponisten schreibe, die alle spektakulär die Abschaffung des Urheberrechts fordern. Mich würde also interessieren, wer denn nun wirklich mit seinem Namen (und damit auch, soweit googlable, seiner Biographie) für die von Ihnen geschriebene Replik einsteht. Daß man Urheber, Musiker dazu, im Boot hat, ist irgendwie halt auch leicht gesagt. Man kann den Tatort-Brief für einiges schelten, aber er wurde immerhin mit offenem Visier geschrieben. Beste Grüße, <Helge von Niswandt>

Antwort: Sehr geehrter Herr von Niswandt, Sie haben Ihre E-Mail an die Redaktion der „Datenschleuder" gerichtet, die Vereinszeitschrift des CCC. An dem offenen Brief haben sich auch Datenschleuder-Redakteure beteiligt, sie sind sowohl Urheber als auch Hacker. Eine namentliche Nennung aller 51 Hacker war jedoch nicht geplant, einige der Hacker haben das allerdings von sich aus getan.

Natürlich könnte jeder behaupten, er schriebe im Namen anderer. Allerdings fiele es ihm dann schwer, das auf ccc.de zu tun. Anders als vielleicht unter hauptberuflichen Künstlern ist es in der Hackerszene nicht immer üblich, offen mit seinem Namen zu agieren. Das hat verschiedene Gründe: berufliche, politische, strafrechtliche, private. Daher hat sich in den drei Jahrzehnten des Bestehens des CCC eine Kultur der Pseudonyme etabliert, auch der Kampf um das Recht auf Anonymität hat bei uns eine lange Tradition. Im Unterschied dazu agieren allerdings die Sprecher des CCC in der Außenkommunikation mit ihren bürgerlichen Namen.

Ob es eine Namensliste der Unterzeichner gibt, ist der Redaktion der Datenschleuder nicht bekannt. Würde uns eine vorliegen, würden wir sie nicht öffentlich machen. Ich selbst zähle mich zu den Unterstützern des offenen Briefes. Sie können mich nun googeln, wenn Sie das möchten. Mit freundlichem Gruß,
<conz> Hackerin, Urheberin, Autorin, Wissenschaftlerin, Datenschleuder-Redakteurin

Die Leiden des ehrgeizigen Bachelorstudenten

Sehr geehrte Damen und Herren, mein Name ist Matthias M., ich habe am 23.09.2012 eine Anfrage zwecks Beantwortung meines Fragenkataloges (Bachelorthesis) an Frau Constanze Kurz gesendet. Am 23.09.2012 15:40, schrieb Frau Kurz: „Sehr geehrter Herr Münster, das können wir gern machen, sofern die Beantwortung keine fünf Seiten Text sind. Mit freundlichem Gruß aus Berlin, Constanze Kurz"

Daraufhin habe ich am 24.09.2012 meinen Fragenkatalog an *presse@ccc.de* (z. Hd. Frau Constanze Kurz) gesendet. Ich hatte eine Bearbeitungszeit bis zum 10.10.2012 gesetzt, bis dahin sollte der Fragenkatalog beantwortet an obige Emailadresse zurückgesendet werden.

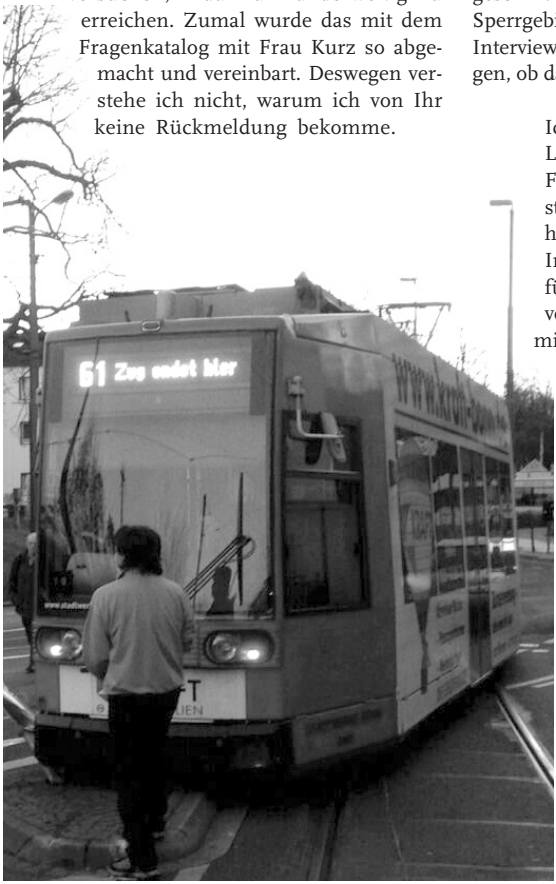
Am 09.10.2012 habe ich versucht Frau Kurz mittels einer erneuten Email zu kontaktieren: „Hallo Frau Kurz,kamen Sie zurecht mit der Beantwortung meines Ihnen zugesendeten Fragebogens (Elektronischer Personalausweis)? Ich bitte um kurze Rückmeldung (Haben Sie eine telefonische Direktwahl für Rückfragen ?) mit freundlichen Grüßen M."

Jedoch ohne Erfolg. Ich habe bis jetzt noch keine Rückmeldung. Wenn ich eine Telefonnummer von Frau Kurz hätte, könnte ich Sie selbst telefonisch anrufen und nachfragen. Da ich dies jedoch nicht habe schicke ich diese Email an den oben aufgelisteten Verteiler in der Hoffnung dass meine Nachricht schnellstmöglichst bei Frau Kurz ankommt, da ich unter massivem Zeitdruck stehe. Ich bitte den oder diejenige die diese Email ließt, freundlicherweise Frau Kurz mein Darliegen zu schildern und mich bitte per

EMail oder Handy zu kontaktieren, sodass ich überhaupt weis, wie der aktuelle Stand ist, bzw. ob ein Problem besteht. [*Diverse Kontaktadressen weggelassen*] Ich bedanke mich im voraus und warte auf eine Antwort *<Matthias M.>*

Hallo Matthias, hui, so formuliert mein zuständiges Finanzamt immer, wenn ich meine Steuererklärung nicht rechtzeitig gemacht habe. Ich kann Dir nur anbieten, Deine E-Mail ggf. als (und ggf. gekürzeten) Leserbrief in der nächsten DS zu veröffentlichen, um sie auf Dein Anliegen aufmerksam zu machen ... Was meinst Du? Cheers, <HC>

Zweite E-Mail: Hallo Herr [<hc>], ich danke für die Rückmeldung. Ich bevorzuge es vorerst zu versuchen, Frau Kurz anderweitig zu erreichen. Zumal wurde das mit dem Fragenkatalog mit Frau Kurz so abgemacht und vereinbart. Deswegen verstehe ich nicht, warum ich von Ihr keine Rückmeldung bekomme.



Vielleicht ist sie im Urlaub, ich weiß es nicht. Ich werde auf Sie zurückgreifen, wenn sich keine andere Möglichkeit mehr eröffnet. Vielen Dank *<M.>*

Antwort: Hallo Matthias, viel Zeit ist vergangen, und Du hast noch immer nicht auf mich zurückgegriffen, aber Du nimmst es mir hoffentlich nicht übel, wenn ich hier auf dein Geschreibsel hier als Stoff für einen Leserbrief zurückgreife? Danke schonmal, gell! <hc>

Hallo liebes Interview Team des CCC, ich habe in der Ausgabe #96 des „Datenschleuder" geschmöckert und eurer Interview „Militärisches Sperrgebiet Internet" gelesen. Nachdem ich das Interview nun gelesen habe, muss ich euch fragen, ob das Satire ist, was da gedruckt wurde?

Ich weiß es sind schon zwei Jahre ins Land gegangen, aber die Antwort auf die Frage ist so spannend. Ich mein das meiste von dem was der Nato-Berater gesagt hat kann er ja nicht ernst gemeint haben. Im letzteren Teil des Interviews, hat er für komplett die Zurechnungsfähigkeit verloren und indem Moment fragte ich mich auch, ob ich gerade ein Satire-Interview lese. Also ist es Satire? *<Philipp Ludewig>*

Lieber Philipp, vielen Dank an Deinem Interesse an unserem Militarisierungsprojekt. Gern leiten wir Deine Bewerbung an Dein lokales Kreiswehrersatzamt weiter.

Unser kompetenter Militärsatirespezialexperte, Sandro G., steht Dir für die Beantwortung all Deiner Fragen rund um das Thema zur Verfügung. Achtung! <Major a. D. Georg-U. U., Nato-Berater für strategische Fragen, Stabsabteilungsleiter Militärpolitik a. D., Fellow der Deutschen Atlantischen Gesellschaft >

„Meinen Dank an Euch“

von Sam Becker, auticare e. V.

Folgender offener Brief erreichte uns von Sam Becker. Sam ist Autistin und berichtet uns hier von Ihren Erfahrungen auf dem 29c3, den Umgang mit Ihr und warum wir Schuld am Projekt „auticare“ sind.

Hallo ihr Lieben, meine Name ist Sam Becker. Den meisten unter Euch wird mein Name nicht viel sagen.

Einige jedoch erinnern sich vielleicht an meinen offenen Brief an den CCC nach der Creeper-Card-Geschichte auf dem 29C3 in Hamburg.

Ich bin die kleine Autistin, die mit dem komischen Autismus-„Erklär“-Shirt auf dem Congress rumgelaufen ist.

Bevor ich zu unserer Geschichte seither komme, muß ich ein wenig ausholen. Ich hoffe, Ihr verzeiht mir das, aber das ist zum Verständnis wichtig.

Ich habe damals geschrieben, daß ich trotz meiner Ängste und Kontaktschwierigkeiten, die so typisch für Menschen aus dem autistischen Spektrum sind, mich bei Euch sogleich wohlgefühlt habe. Obwohl ich eigentlich selbst im Gegensatz zu meinem Freund kein richtiger Nerd bin, sondern eher technisch interessiert, lag in der Art, wie ich die Menschen auf dem Congress kennengelernt habe, etwas Vertrautes. Da waren so viele Ähnlichkeiten in der Art, wie ihr Eure Umgebung wahrnehmt. Da war die gleiche kritische Aufmerksamkeit, die ich von uns Autisten kenne. In der Tat gelten doch für Hakker und Nerds in vielen Bereichen die gleichen Tugenden, die man uns Autisten als Symptom nachsagt: die Fähigkeit, sich lange auf bestimmte Dinge konzentrieren zu können, der unbedingte Wille, sich in seinem Spezialinteresse bis zur Perfektion weiterzubilden.

Auf unserer Seite sieht es leider nicht ganz so rosig aus. Zwar gibt es unter uns Autisten viele, die sogar überdurchschnittlich intelligent sind, aber Autismus ist ein breites Spektrum. In den schwersten Varianten ist ein selbstbestimmtes Leben gar nicht mehr möglich. Andere wieder können nicht öffentlich zu ihrem Autismus stehen, da sie wegen der immer noch sehr starken Diskriminierung um ihren Arbeitsplatz fürchten müssen.

Was hat das nun mit unserer Geschichte zu tun?

Ganz einfach: Nachdem ich Eure Community

und Eure Art zu Leben zuvor über Jahre nur aus der Ferne kannte, da ich mich nie zu einer Veranstaltung hingetraut habe, war ich von Eurer Art so angetan, daß mir und meinem Freund eine Idee kam: An einem chilligen Abend sprachen wir mal wieder darüber, wie es weitergehen sollte.

Nun gehören wir beide nicht zu der Sorte Menschen, die einfach nichts tun können. Wir mußten einen Weg finden, wieder etwas zu tun. Nach den vielen tollen und teils unglaublichen Erfah-

rungen, die wir im Anschluß an den Congress mit Euch gemacht haben, kam uns die Idee, einen eigenen Verein zu gründen. Eine Hilfsorganisation, die nach dem Vorbild Eurer kreativen Art und Eurer modernen, offenen Lebensweise autistischen Menschen um uns herum helfen soll. Es war zunächst eine verrückte Idee. Aber was lag näher, als die eingangs erwähnte Ähnlichkeit zwischen uns zu nutzen: eine Idee, die funktionieren könnte.

So überlegten wir uns, daß wir zum Beispiel auch die technischen Talente der Autisten nutzen könnten, um ganz im Open-Source- und Open-Hardware-Gedanken Hilfsmittel für Behinderte zu entwickeln. Wir wollen unter anderem wirklich bezahlbare Fair-Profit-Produkte bauen. Fair Profit bedeutet für uns, der Preis deckt die Produktionskosten, und die restliche Marge die bleibt, wird für Unterstützungskampagnen und die Entwicklung weiterer neuer Produkte genutzt. Auf diese Weise werden wir hoffentlich letztlich auch Arbeitsplätze für Autisten schaffen, und zwar keine Arbeitsbeschaffungsmaßnahmen, sondern echte Jobs, in denen meine autistischen Kollegen ihre zahlreichen Talente voll ausleben können.

Also haben wir unsere Organisation auticare gegründet. Und wir haben mit unserer Idee in ein Wespennest gestochen. Innerhalb von nur acht Wochen hatten wir ein Vereinsheim, online wie offline beinahe dreißig freiwillige Mitarbeiter und weitere ehrenamtliche Helfer. Darunter Kinder- und Jugendpsychologen, eine Verhaltensbiologin, einen Kunsttherapeuten und Pädagogen, eine Kultur- und Eventmanagerin, Autoren, eine Projektmanagerin, einen Journalisten und viele weitere mehr – die meisten von ihnen selbst Autisten. Sie alle setzen sich mit Feuer und Flamme für unsere Idee ein, so daß wir im September schon unser erstes eigenes lokales Symposium mit Vorträgen von bekannten Fachleuten und Laien abhalten können, bei dem auf Augenhöhe diskutiert werden kann.

Und das ist Eure Schuld. :)

Ihr habt hier etwas in Bewegung gesetzt. Täglich bilden sich neue Ideen und Synergien. Neue Kommunikationswege tun sich auf. Frische Ideen kommen auf den Tisch und immer mehr Autisten scheinen aus ihrer teilweisen Lethargie zu erwachen. Einige von ihnen hatten schon für sich akzeptiert, niemals Teil einer Gesellschaft sein zu können. Manch einer will es schon gar nicht mehr, ist Autismus doch inzwischen in der Presselandschaft und in der Politik zum Schimpfwort verkommen. Doch hier ist eine immer größer werdende Gruppe von Menschen, die das nicht akzeptieren wollen.

Wir glauben, daß es ein langer Weg sein mag, aber wir glauben, daß wir mit unseren Aktionen und im Dialog mit der artverwandten „Spezies“ und dem ganzen Rest der Gesellschaft über die Jahre einen Imagewechsel einläuten können. So wir Ihr Nerds Euer Image vom Kellerkind und ungeliebten Streber hin zu den coolen Technik-Geeks, die den anderen ihre unverzichtbaren Handys und Tablets reparieren können, gewandelt habt. So wie Ihr Hacker Euer Image in den letzten Jahren von den kleinkriminellen Computerkids hin zu ernstzunehmenden Experten in Sachen Sicherheit gewandelt habt. So hoffen auch wir zu erreichen, daß wir uns mit unserer Idee und mehr Öffentlichkeit endlich so darstellen können, wie wir wirklich sind. Wir sind so vielfältig und individuell wie Ihr.

Mein Fazit

Ich schulde Euch meinen Dank, weil Ihr, ohne es zu wissen, etwas Wunderbares angestoßen habt. Eure Kultur und Eure Art zu kommunizieren, ist der unseren so ähnlich, daß Ihr auf der Seite der Autisten jetzt eine Idee angestoßen habt, der sich

täglich mehr Menschen anschließen. Es bildet sich eine Gemeinschaft von Autisten, die ähnlich der Euren funktioniert.

Sie ist wie die Eure, nicht auf die Technik beschränkt, sondern umfaßt ebenfalls die vielen, vielen Variationen der menschlichen Interessen, die wir auch auf der Seite der neurotypischen – also nicht-autistischen – Menschen finden. Sie ist sozusagen ein Spiegelbild. Unsere Hoffnung und Idee ist es jedoch, daß wir uns irgendwann in der Zukunft so weit angenähert haben, daß Autismus nicht mehr als Behinderung gesehen wird, sondern einfach als eine andere Art, seine Umgebung wahrzunehmen.

Wir wissen, daß dies ein hohes und vielleicht schwer erreichbares Ziel ist. Aber selbst wenn wir das Ideal nie erreichen, ist schon viel gewonnen, wenn wir daran arbeiten.

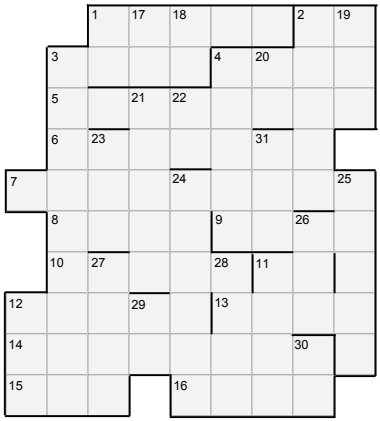
Eines ist jedoch sicher. Ohne Euch, ohne Euren verständnisvollen und respektvollen Umgang mit mir, würde es auticare nicht geben. Und das alles ganz ohne grüne, gelbe oder rote Karten.

Mein ganz besonderer Dank geht übrigens noch an Constanze Kurz, Fefe und Frank Rieger. Mit Euren Erwähnungen habt ihr erst den Anstoß dazu gegeben, daß in drei Tagen über 30.000 Menschen meinen offenen Brief gelesen haben und mir mit ihren vielen Kommentaren Mut gemacht haben, meinen Traum zu leben. Jungs, Eure Tweets und Blogs haben echt Durchschlagskraft. Dagegen war der Link von Heise ein laues Lüftchen. Sorry Heise-Jungs, ich mag Euch trotzdem. :)

In diesem Sinne, danke an alle aus dem CCC und drumherum, die mir so viel entgegengekommen sind und das alles möglich gemacht haben. Ihr seid toll.

Eure (glückliche) Sam.

P. S.: Wir sehen uns spätestens in Hamburg.



Du hast eine bessere Formulierung für einen Hinweis? Immer her damit: @pallas23 auf Twitter

Dank an @tbaldauf für das Finden von Worten "mit 4 Buchstaben, 2. muss ein B sein" und ähnlich gelagerten Anfragen

Waagerecht

1 - Friendship ist für so jemanden Magic
2 - Gegenstück zu "fg"
3 - "lkwpeter" war DAS Passwort hierfür
4 - "So tun als ob" für Erwachsene
5 - "0" ist das vom Shutdown
6 - Lineare ...
7 - Wer hat's erfunden? Assange!
8 - 10^-9
9 - Beliebter Portscanner
10 - Häufige Commitmessage
11 - Strg+C und +V auf der Konsole
12 - In regulierten Umfeldern gibt es oft solch einen
13 - Swift gewährt ihnen Zugriff auf deutsche Bankdaten
14 - Evil Overlord des Universe mit naheliegendem Typo*
15 - Gerätetreiber sind bei unixoiden Betriebssystemen häufig solche (Abkz.)
16 - Was die machen ist fucking rocket science

Senkrecht

1 - Angeblich ist jeder ein bisschen ...
2 - Have a ...
3 - Programmiersprache mit nur 8 Befehlen
4 - 1UP
11 - Damit konstruiert man integrierte Schaltkreise
12 - Phantasieloser Chat-Anfang
17 - _ _ M (M für Memory)
18 - Richard Stallman ist Begründer dieser Bewegung (Abkz.)
19 - Die beliebteste bei OpenSource Projekten. Danach kommen MIT und Artistic
20 - Solchen Nerds verdanken wir die lückenlose Aufzeichnung der Congresse
21 - Schneller Webserver
22 - <=
23 - Teil der jeweiligen Polizeibehörde im Bundesland
24 - Dabei nicht zu weit vorne anpacken!
25 - Viel ... am Gerät!
26 - Programmierschnittstelle
27 - Schön wenn Funktionen ...potent sind
28 - Brent Spiners bekannteste Rolle
29 - Was für Mail das Killfile, ist für ICQ dieses (Abkz.)
30 - Udo Vetter ist einer (Abkz.)
31 - Ist öfter mal Ursache scheinbar unzusammenhängender Rechner-Ausfälle

* Sorry für den Typo, aber wollt's unbedingt drin haben - Was nicht passt wird passend gemacht ;D

Tor Bridges

von Moritz <moritz@zwiebelfreunde.de>

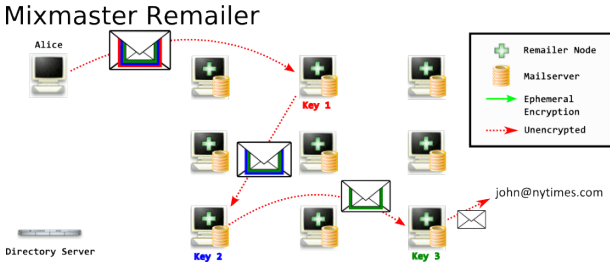
Der ehemalige NSA-Analyst Thomas Drake forderte „We need more Tororists“ auf dem vorletzten Chaos Communication Congress 29C3. [1] Hierfür erntete er großen Applaus. Höchste Zeit, erneut einen Blick auf das Anonymisierungswerkzeug Tor zu werfen.

Anonymisierung ist nicht gleich Verschlüsselung. Dank langsam, aber stetig um sich greifender Verschlüsselungsverfahren stützt sich die Arbeit von Geheimdiensten heutzutage immer weniger auf den Inhalt von Kommunikation, als auf die Erfassung und Analyse von Beziehungsstrukturen selbst: Wer hat mit wem wie lange und wie häufig kommuniziert? Studien aus den Jahren 2008 [2] und 2010 [3] nutzen Verfahren aus der künstlichen Intelligenz und Sprachverarbeitung, um im verschlüsselten Datenstrom von Voice-over-IP-Gesprächen Sätze zu identifizieren, mit einer Erkennungsrate von durchschnittlich 50 % und für einige häufige Wörter mit über 90 % Trefferquote.

Eine weitere Studie beschäftigt sich mit der Erkennung abgerufener Inhalte auf Webseiten, anhand der Größe und den Zeitabständen zwischen den einzelnen Requests. [4] Bei der Anonymisierung von Kommunikation geht es hingegen darum, den Kommunikationspfad selbst zu verschleiern, es also Angreifern zu erschweren, überhaupt nachvollziehen zu können, wer mit wem wann Informationen austauscht. Angreifer können prinzipiell auf jedem Abschnitt der Wegstrecke zwischen Sender und Empfänger lauern: Sie können gezielt den Sender oder den Empfänger überwachen, oder eine oder mehrere der dazwischen liegenden Kommunikationseinrichtungen.

Mixes

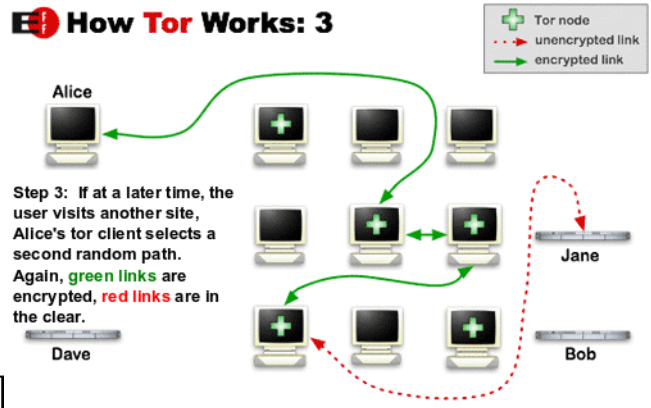
Der Mathematiker David Chaum formulierte 1981 ein grundlegendes Modell für anonyme Kommunikation via E-Mail. [5] Ein „Mix“ wird beschrieben als ein Mailserver, der Mails nicht sofort weiterreicht, sondern eine Weile „anstaut“ und dann in anderer Reihenfolge weitergibt. Eine „Mix-Kaskade“, also mehrere solcher Mailserver hintereinander, verschleiern so effektiv den eigentlichen Sender und Empfänger. Chaum beschreibt auch Ideen für anonymisierte Antworten. Mit einigen Ausnahmen wie Andreas Pfitzmanns Mixes für ISDN beschäftigte sich der Forschungsbereich in der Folge die nächsten zwanzig Jahre vor allem mit diesem Bereich, der verzögerten anonymisierten Kommunikation (“high latency anonymity“, Anonymität mit hoher Latenz). Eine schöne, aktuelle und gut lesbare Einführung in die später Remailer genannten Technologien hat Tom Ritter für das Crypto Project geschrieben. [6]



Onion Routing

Onion Routing als Begriff wurde 1996 von Forschern der US Navy geprägt. [7] Die Idee ist recht simpel: Statt direkt zu kommunizieren, schaltet man Proxies („Stellvertreter“) dazwischen. Damit ein einzelner Proxy die übertragenen Inhalte nicht mit Sender und Empfänger kor-

relieren kann, wählt man mindestens zwei solcher Proxies, und verschlüsselt wie folgt: Der erste Proxy, später in der Literatur „entry node“ genannt, sieht den Sender und weiß, an welchen zweiten Proxy er das verschlüsselte Paket weiterreichen soll – kennt aber weder Inhalt noch Zieladresse. Der letzte Proxy, später „exit node“ genannt, spricht mit dem eigentlichen Empfänger, kann aber nicht nachvollziehen, woher die Anfrage ursprünglich stammt, da er sie nicht direkt vom Sender erhalten hat. Die gegebenenfalls dazwischen liegenden weiteren Proxies reichen nur verschlüsselte Inhalte weiter. Der Sender präpariert die eigentlichen Inhalte also für den gesamten Pfad und legt so pro Proxy eine Schicht an Verschlüsselung um diese Inhalte – ähnlich den Schichten einer Zwiebel.



Im Gegensatz zu Mixes wird also auf eine Verzögerung und Vermischung von Paketen verzichtet. Der wesentliche Vorteil ist, daß sich Onion Routing somit für Dienste wie Web, XMPP und sogar VoIP eignet, die auf niedrigere Latenz angewiesen sind. Der große Nachteil ist, daß das Verfahren keinen Schutz vor „Ende-zu-Ende-Traffickorrelation“ bietet: Wird sowohl in das Anonymisierungsnetz eingehender Verkehr als auch aus dem Anonymisierungsnetz austretender Verkehr überwacht, lässt sich die Anonymisierung aushebeln. Eine gute Übersicht über aktive und passive Verfahren findet sich im Torproject-Blog. [8]

Trotz der offensichtlich „besseren“ Anonymisierung durch Mixes und hohe Latenz sieht man das Remailer-Modell heute größtenteils als gescheitert an: Es ist für viele Nutzer und Einsatzzwecke nicht geeignet, und auch das beste Anonymisierungsverfahren hilft nichts, wenn die Nutzer fehlen. Nur dann nämlich kann ein „Untertauchen in der Masse“ gewährleistet sein. [9] Spannend bleibt das Feld aber durchaus, neuere Ansätze wie das „Alpha-Mixing“ wollen beide Verfahren verschmelzen. Aber dazu an anderer Stelle oder in einer Fortsetzung mehr. [10]

Tor: Der Prototyp mit 500.000 Nutzern täglich

Natürlich wollte man sich nicht mit theoretischer Forschung zufriedengeben, bereits 1996 gab es erste Prototypen. Tor wurde dann 2004 als „Second Generation Onion Routing“ vorgestellt und seitdem beständig weiterentwickelt. Auf die einzelnen Änderungen im Protokoll einzugehen wäre zu umfangreich für diesen Artikel, einen guten Einblick in die Details bieten drei Blog-Artikel von 2012. [11] Was als weiterer Prototyp und als Forschungsspielfeld gedacht war, wurde bald zu einem auch für reale Szenarios eingesetzten Werkzeug. Auch für die Forschung braucht man möglichst echte Daten als Grundlage. Tor versteht sich auch heute noch als ein Forschungsprojekt, jedes Jahr werden neue Papers veröffentlicht, die sich mit Tor auseinandersetzen.

An der Grundidee von Tor hat sich im Laufe der Jahre nichts geändert: Ein generischer Proxy nimmt lokal Anwendungsverkehr entgegen, schleust ihn durch das Tor-Netzwerk und gibt Antworten an die Anwendung zurück. Tor kann dabei immer nur ein Baustein zur anonymen Kommunikation sein. In den ersten Jahren war den Anwendern, zumeist aus unseren Kreisen, klar, daß Ende-zu-Ende-Verschlüsselung und umsichtige Nutzung dazu gehört. Tor manipuliert den Inhalt der Kommunikation nicht – es

ist wenig hilfreich, wenn im Datenstrom selbst identifizierende Merkmale enthalten sind. Inzwischen haben auch eine Menge unbedarfter Nutzer berechtigtes Interesse an Anonymisierung, weshalb im Dunstkreis von Tor weitere Entwicklungen entstanden sind, um Nutzer zu schützen. Kursierten lange Zeit Anleitungen, um einen Browser einigermaßen zu härten, damit nicht z. B. externe Plugins wie Java oder Flash von Webseiten eingesetzt werden können um lokale Eigenschaften zu sammeln und zu übertragen, versuchte man es zuletzt erst mit einer Browser-Extension (TorButton) und, nachdem klar wurde daß man leider den Browsern einige gefährliche Dinge (noch) nicht per Extension abgewöhnen kann, mit einem speziell gepatchten Firefox. Chromium eignet sich als Basis momentan nicht, andere Browser schon gar nicht, weil sie nicht Open Source sind.

Eine weitere hilfreiche Extension, die vom EFF und Tor-Entwicklern betreut wird, ist „HTTPS Everywhere“, im Tor Browser integriert und auch als als eigenständige Extension wichtig: Umfangreiche Regelsätze bringen den Browser dazu, HTTPS-gesicherte Verbindungen zu Webseiten zu bevorzugen. Leider ist es ja immer noch gang und gäbe, ungesicherte Protokolle über Tor oder beispielsweise in offenen WLANs einzusetzen. Bei Tor ist dies besonders problematisch: Da der letzte Proxy, der „exit node“, die ursprüngliche Anfrage ins Internet absetzt, kann er Inhalte mitschneiden (Nicht: den Absender identifizieren, es sei denn, der Inhalt selbst lässt Rückschlüsse zu, wie etwa Login-Informationen). Man munkelt ja, daß ein solcher Mitschnitt zur Gründung von WikiLeaks geführt hat... Die Überzeugungsarbeit geht weiter. Immerhin hat Facebook inzwischen TLS sowohl für die Webseite als auch für den Chat auf XMPP-Basis eingeführt. Lange genug hats gedauert.

Anonymisierung ist über die Jahre zu einem umfangreichen Ökosystem geworden. Die Torproject-Website listet aktuell über 35 Komponenten, die alle um Mitarbeit werben. [12] Einige davon wurden auf dem 29C3 vorgestellt, der einstündige Vortrag sei jedem ans Herz gelegt, der tiefer in die Materie einsteigen will. [13]

Internetzensur und gegenseitige Aufrüstung

Immer interessanter wurde Tor auch als effektives Werkzeug zur Zensurumgehung, die heutzutage mehr und mehr um sich greift – auch weil Internetzugang langsam in alle möglichen und unmöglichen Weltregionen sickert. Zunächst einmal bieten die öffentlich zugänglichen Tor-Proxies („Tor Relays“) eine große Anzahl an erreichbaren IPs, und eingehende Verbindungen werden ja sowieso bereits designmässig verschlüsselt. Da der letzte Proxy in der Kette, der „exit (relay)“, hoffentlich irgendwo wenig oder gar nicht zensiert steht, bietet Tor schon von klein auf einen freien und schwer überwachbaren Internetzugang. Und eine Anonymisierung des Kommunikationspfades liegt im Regelfall durchaus im Interesse derjenigen, die von Zensur betroffen sind. Auch dann, wenn sie am anderen Ende „nur“ eine aus anderen Gründen negativ zu beurteilende zentralisierte US-Plattform wie Facebook erreichen wollen...

Ohne ins Detail zu gehen, wird ein Problem deutlich: Damit Tor auf Clientseite einen Pfad durch das Tor-Netz bestimmen und die Pakete entsprechend verschlüsseln kann, müssen alle beteiligten Relays, also deren IP-Adresse, Port und Public Key, für die Verschlüsselung öffentlich bekannt sein. Das macht es Zensoren relativ leicht, Tor zu blockieren: Man besorge sich regelmässig die Liste aller Torknoten und blockiere ausgehende Verbindungen dorthin. Bonuspunkt, wenn der entsprechende Teilnehmeranschluss für genauere Beobachtungen geflagged wird... Prompt liefern westliche und östliche Firewall-Hersteller entsprechende Regelsätze aus, die dann in repressiven Staaten und genauso repressiven Unternehmen zum Einsatz kommen. Oft auch gar nicht bewusst, sondern weil der Admin bequem den Haken setzt und „gut is‘“.

Das erste und universelle Design gegen eine solche Blockade sind „Tor Bridges“, 2007 eingeführt. Tor Bridges sind Relays, die nicht im öffentlichen Verzeichnis gelistet werden. Sie lassen sich dem eigenen Tor Client manuell beibringen, und dienen als alternative Einstiegspunkte ins Tor-Netz (als „entry node“). Wie

Tor in einer nützlichen Anwendung

kommt man als Nutzer nun an Bridges, und das, ohne dem Zensor alle Bridge-Adressen auf dem Tablett zu liefern? Ein Bridge-Betreiber kann wählen, ob die eigene Bridge automatisch verteilt werden soll (etwa per Webformular, Email oder [echte] soziale Netze), oder ob er selbst für eine Weitergabe sorgen will. Limitierungen wie ein CAPTCHA und die Herausgabe von immer nur einer Handvoll Adressen sollen dafür sorgen, daß ein Zensor nicht einfach an eine große Menge an Bridges herankommt.

Als nächster Schritt im Zensurwettrüsten blieb den Zensoren und Filter-Herstellern der etwas ressourcenintensivere Weg, sich die Pakete genauer anzuschauen (Deep Packet Inspection). Tor versucht zwar, den Verbindungsaufbau einigermaßen wie den gängiger Browser aussehen zu lassen, ganz verhindern lässt sich aber eine Erkennung der Pakete nicht. China legte bald eine erstaunliche Methode nach, um Torverbindungen zu erkennen: Wird ein generischer TLS-Handshake erkannt, verbindet sich die Große Böse Firewall aktiv mit der Zieladresse und spricht dabei das Tor-Protokoll. Antwortet der Relay, kappen sie die Verbindungen und blockieren die Ziel-IP für einige Zeit. [14] Egal wie sehr man also den Handshake anpasst, China muss sich nur den Gegebenheiten anpassen und das jeweils aktuelle „Tor sprechen“. Ein dauerhafterer Weg, eine Erkennung zu erschweren, führte zur Entwicklung der sogenannten „pluggable transports“.

Die Idee hinter „pluggable transports“ ist, verschiedene erweiterbare Verschleierungsalgorithmen über die Verbindung zu legen und so eine Erkennung per DPI zu erschweren. Idealerweise entstehen so im Laufe der Zeit möglichst vielfältige Methoden der Verschleierung. Experimentell gibt es beispielsweise den SkypeMorph-Transport, der Tor-Verkehr in Skype-Pakete einbettet. [15] Dabei sinkt zwar die Datenrate, eine Blockade von Tor ohne Seiteneffekte wie z. B. auf Skype sind dann auf Firewallseite nicht mehr auszuschließen. StegoTorus ist ein generisches Framework und bringt ein steganographisches Modul, das dann „wie HTTP aussieht“.

Zum Einsatz kommen aktuell die einfachen und effizienten Verfahren „obfs2“ und „obfs3“. Es gibt ein fertiges Paket mit Tor Browser, Tor und eben einem „pluggable transport“, der diese Protokolle spricht (Obfsproxy Bundle, [16]), und bislang hat kein Land geschafft, diese Verbindungen zu blockieren (das wird aber sicher kommen).

Auch China sollten diese Methoden Probleme bereiten. Kann man den Verbindungsaufbau nicht mehr eindeutig Tor zuordnen, müss(t)en sie aktive Tests für praktisch alle Verbindungen überhaupt durchführen.

Nutzerzahlen

Auf der Metrics-Seite gibt es aktuelle Zahlen zum Netzwerk und zu den Nutzern aus den verschiedenen Ländern. [17] Ende Januar 2013 waren es grob geschätzt 500.000 tägliche sich direkt verbindende Nutzer, die führenden Länder waren dabei USA, Italien, Deutschland, Spanien, Frankreich, Iran, Brasilien und Russland (in absteigender Reihenfolge). Iran wird da bald rausfliegen, da sie inzwischen Tor und Bridges blockieren (Das Obfsproxy-Bundle funktioniert noch wunderbar).

Bridge-Nutzer sah Tor im Januar 2013 etwa 25.000 täglich, führende Länder hier Iran, Italien, USA, Syrien, China, Spanien und Frankreich. Auch die Zahl der Relays im Tor-Netz nimmt langsam aber stetig zu. Im Januar 2013 gab es etwa 3.000 Relays und 1.000 Bridges. Die Gesamtkapazität betrug rund 23 Gbit. Dabei fallen knapp über 30% der (wesentlichen) Exitkapazität auf die USA, 27% auf Deutschland, 11% auf Schweden, gefolgt von 3% auf Dänemark. [18]

Wer betreibt das Tor-Netz?

Die Basis einer erfolgreichen Anonymisierung ist Diversität, je vielfältiger die Nutzer, desto besser. Allerdings gilt dies auch auf Betreiberseite, denn wie bereits erwähnt, kann ein Angreifer die Anonymität aushebeln, wenn er gleichzeitig eingehenden und ausgehenden Verkehr überwachen kann, oder wenn er „entry node“ und „exit node“ gar selbst betreibt. Wichtig ist also neben einer breiten geographischen Verteilung eine hohe Anzahl unabhängiger Betreiber, und daß der Datenverkehr über viele Provider läuft.

Traditionell spielt der CCC dabei keine unwesentliche Rolle. Momentan läuft über 20% des Exittraffics über einen Provider in Deutschland (AS39138 rrbone), administriert wird der Server vom CCC e.V. Die Bandbreite wird gebraucht: Je langsamer das Anonymisierungsnetz, desto mehr Nutzer springen ab und wählen unsicherere Alternativen. Allerdings sind über 20% in den Händen einer einzelnen Organisation, eines einzelnen Providers und eines Landes aus genannten Gründen ungünstig.

Zweitgrößter Betreiber von Tor Exits ist der vom mir ins Leben gerufene gemeinnützige Verein Zwiebelfreunde e.V. mit seiner Plattform torservers.net – ebenfalls in Deutschland beheimatet. Dank Eurer Spenden und der Unterstützung durch die Wau-Holland-Stiftung pumpen wir momentan etwa 4 Gbit/s, verteilt auf mehrere Provider in unterschiedlichen Ländern.

Ich würde mir wünschen, daß sich mehr Gruppierungen aktiv am Betrieb beteiligen würden. Es wäre ein Leichtes, auf dem Mitgliedsformular eines Hackerspaces die Möglichkeit zur regelmäßigen Zusatzspende für Exits vorzusehen. Der Hackerspace Noisebridge macht das mit dem Projekt NoiseTor, speziell dafür gegründete Organisationen nach Zwiebelfreunde-Vorbild entstehen oder existieren momentan in Frankreich (Nos Oignons), Schweden (DFRI), Luxemburg (Frënn vun der Ënn), Schweiz (Swiss Privacy Foundation) und Holland.

Schon ein wenig schade, daß wir das in den Erfas bislang nicht hinkriegen. Sollte sich lokal niemand finden, der die Administration übernimmt, oder reichen die Geldbeträge nicht aus, kann man die Spenden immer noch an andere Organisationen weitergeben (aber natürlich wäre das nicht ganz im Sinne der Aktion). Hilfreich sind für potentielle Betreiber die „Tor Exit Guidelines“, die ich im Laufe der Zeit zusammengetragen habe. [19] Ich helfe gerne auch persönlich weiter, wenn es konkrete Fragen gibt.

Potentielle Sponsoren wurden bislang von Torproject abgewiesen, weil die Anzahl möglicher vertrauenswürdiger Betreiber nicht ausgereicht hat, um Geldmittel sinnvoll zu verteilen. Bald wird es die Möglichkeit geben, finanzielle Unterstützung zu erhalten. An der Diskussion darüber kann man sich gerne beteiligen. [20]

Es gibt sicher unter Euch auch einige mit Kontakten in die ISP-Branche. Übrige Kapazitäten verteilen wir gerne unter den existierenden Organisationen, und der ISP muss sich über eventuelle Haftungsfragen keine Sorgen machen, wenn wir das übernehmen.

Mit dem Tor Cloud-Projekt existiert eine einfache Möglichkeit, ganz ohne Geldeinsatz und ohne technisches Vorwissen Bridges hochzuziehen: Amazon bietet ein Jahr kostenlose Nutzung ihrer Infrastruktur, ein fertiges Betriebssystemabbild wird zur Verfügung gestellt. [21] Für einen dauerhaften Betrieb von Bridges und Relays eigenen sich billige VPS-Provider, wie sie beispielsweise bei LowEndBox vorgestellt werden. [22]

Referenzen

[1] Enemies of the State: What Happens When Telling the Truth about Secret US Government Power Becomes a Crime. Vortrag 27.12.2012 Chaos Communication Congress Hamburg. *https://events.ccc.de/congress/2012/Fahrplan/events/5338.en.html*

[2] Ballard, L.; Coull, S.E.; Monrose, F.; Masson, G.M.: Spot Me if You Can: Uncovering Spoken Phrases in Encrypted VoIP Conversations, IEEE Symposium on Security and Privacy, May 2008. *http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4531143*

[3] Wright, C.; Ballard, L.; Coull, S.; Monrose, F; Masson, G.: Uncovering Spoken Phrases in Encrypted Voice over IP Conversations, ACM Transactions on Information and System Security, Dez 2010. *https://dl.acm.org/citation.cfm?doid=1880022.1880029*

[4] zum Beispiel vorgestellt auf dem 27C3: Herrmann, D.: Contemporary Profiling of Web Users – On Using Anonymizers and Still Get Fucked. Vortrag 27.12.2010 Chaos Communication Congress Berlin. *https://events.ccc.de/congress/2010/Fahrplan/events/4140.en.html*

[5] Chaum, D.: Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms. Communications of the ACM, Feb 1981. *https://dl.acm.org/citation.cfm?id=358563*

[6] Tom Ritter: What is a Remailer? und weitere Artikel. Jan 2013. *https://crypto.is/blog/*

[7] Goldschlag, D.; Reed, G.; Syverson, P.: Hiding Routing Information. Springer-Verlag LLNCS 1174, Mai 1996. *http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=569678*

[8] Dingledine, R.: „One cell is enough to break Tor's anonymity". Feb 2009. *https://blog.torproject.org/blog/one-cell-enough*

[9] Dingledine, R.; Matthewson, N.: Anonymity Loves Company: Usability and the Network Effect. Proceedings of the Fifth Workshop on the Economics of Information Security. 2006. *http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.61.510*

[10] Dingledine, R.; Serjantov, A.; Syverson, P.: Blending different latency traffic with alpha-mixing. Proceedings of the 6th international conference on Privacy Enhancing Technologies. 2006. *https://dl.acm.org/citation.cfm?i d=2166535*

[11] Matthewson, N.: Top changes in Tor since the 2004 design paper (Part 1). Okt 2012. *https://blog.torproject.org/blog/top-changes-tor-2004-design-paper-part-1*

[12] Tor: Volunteer *https://www.torproject.org/getinvolved/volunteer.html.en*

[13] The Tor Software Ecosystem. Vortrag 28.12.2012 Chaos Communication Congress 29C3. *https://events.ccc.de/congress/2012/Fahrplan/events/5306.en.html*

[14] Wilde, T.: Knock Knock Knockin' on Bridges' Doors. Jan 2012. *https://blog.torproject.org/blog/knock-knock-knockin-bridges-doors*

[15] Moghaddam, H.; Li, B.; Derakhshani, M.; Goldberg, I.: SkypeMorph: protocol obfuscation for Tor bridges. Proceedings of the 2012 ACM conference on Computer and communications security. 2012. *https://dl.acm.org/citation.cfm?id=2382210*

[16] Torproject: Obfsproxy *https://www.torproject.org/projects/obfsproxy.html.en*

[17] Tor Metrics Portal *https://metrics.torproject.org/*

[18] Tor Compass *https://compass.torproject.org/*

[19] Tor Exit Guidelines *https://trac.torproject.org/projects/tor/wiki/doc/TorExitGuidelines*

[20] Call for discussion: turning funding into more exit relays. Jan 2013. *https://lists.torproject.org/pipermail/tor-relays/2013-January/001827.html*

[21] Tor Cloud *https://cloud.torproject.org/*

[22] Low End Box Cheap VPS Hosting *http://www.lowendbox.com/*

Letzter Ausstieg Gewissen

von frank, 46halbe und erdgeist <ds@ccc.de>

In den letzten Monaten ist eine recht lichtscheue Industrie verstärkt in den Fokus der Öffentlichkeit geraten, deren Hauptakteure mit dem auf der Welle der Terrorhysterie schwimmenden Geld ein einträgliches Geschäft wittern und den technologisch überforderten Polizeien und Geheimdiensten der Welt versprechen, Licht ins Dunkel der Festplatten und Internetforen von „Verdächtigen" aller Coleur zu bringen.

Zu sagen, die dort vermarkteten Technologien der „IT-Sicherheitsforschung" seien ein zweischneidiges Schwert, wäre dabei eine gewaltige Untertreibung. Direkt an den Lebensadern der Kommunikationsgesellschaft den intimsten Austausch aller Gedanken seiner Bürger in Erfahrung zu bringen, ist seit Urzeiten der heilige Gral aller repressiven Regimes. Doch zeigt sich, daß es für die technische Umsetzung der Werkzeuge zum Spionieren und Fernsteuern schlaue Köpfe braucht, um peinliche Debakel, wie sie der Firma DigiTask mit ihrem an deutsche Kriminalämter verkauften Bundestrojaner passiert sind, zu vermeiden.

Akt 1 – Die Akteure

Wer sind diese Berufshacker, die ganz in der Tradition der Atomwaffenforscher an der vordersten Front der Entwicklung stehen, wie sehen sie ihre Arbeit, wie gehen sie mit Nachrichten aus Regionen um, wo der Einsatz ihrer Software zu nächtlichen Hausbesuchen der Geheimpolizei führt. Was sind Motive und Sachzwänge, und stimmt es, daß es keine Option gibt, zu Aufträgen dieser Art „nein" zu sagen – vielleicht aus finanziellen Verpflichtungen, oder daß es gar egal ist, weil „es sonst halt jemand anderes tut"?

Im Diskurs mit zwei Aussteigern aus der Industrie der IT-Angriffswerkzeuge bekommen wir in der Redaktion „Die Datenschleuder" einen Eindruck von den Mechanismen und Entwicklungen der dort Forschenden und Arbeitenden. Es wird klarer, wie eine Mischung aus Ehrgeiz, Loyalität, dem Anspruch sich professionell zu verhalten und – natürlich – dem Gedanken an die nächste Miete, gepaart mit Naivität und fehlgerichtetem Vertrauen zu einem Wendepunkt führt. An diesem Punkt wurde eine Auseinandersetzung mit dem Lebensentwurf unausweichlich, da die Widersprüche zu ihren eigenen Überzeugungen so offenbar wurden.

Wir treffen Simon*, Mittdreißiger, großer, uriger Berliner Typ mit dem festen Händedruck eines Handwerkers und nachdenklichem Lächeln. Simon trägt eine Kluft, die viel über seine Vergangenheit verrät: Aus dem politisch aktiven Umfeld Berlins stammend, hat er Jahre seiner Jugend in diversen Initiativen gegen die Militarisierung der deutschen Gesellschaft, gegen Kriegs- und Zwangsdienste, Rassismus und Faschismus gekämpft, verloren oder gefeiert. Als klar wurde, daß die Staatsgewalt zunehmend im Digitalen ausgeübt wird, hat er sich autodidaktisch – wie er sagt – „das mit den Computern" beigebracht und seinen erlernten Beruf an den Nagel gehängt – weil er Hacker werden wollte.

Als klassischer Quer-Einsteiger in die IT- und somit auch in die IT-Security-Branche hat er seine Neugier zum Beruf gemacht: Neugier und den Drang, alle Hintergründe verstehen zu wollen, den Spaß, sich in absurden technischen Details festzubeißen, um die Lücke im

System zu finden. Simon sagt, Hacker beziehen ihr Lob und die Anerkennung aus Diskussionen mit Anderen, aus unkonventionellem Lernen und Lehren – und von zahlenden Kunden aus der Branche. Es gibt auch Hacker, für die ist ein Diplom der Mathematik oder Informatik Anerkennung und Bestätigung genug. Zu denen zählt er sich jedoch nicht. Simons politische Aktivitäten wurden auf's Internet ausgedehnt, es gab neue Bedrohungen durch Regierungen, die das Netz sofort als feindlich klassifizierten – aus ihrer Sicht möglicherweise zu Recht, denn alles wurde transparenter, und Informationen konnten schneller transportiert werden.

Nachwuchssorgen

Es war Simons Idee, seine Geschichte aufzuschreiben, als Warnung einerseits, wie sich selbst politisch bewußte und reflektierte Menschen plötzlich auf der falschen Seite einer vorher unvermuteten Barrikade wiederfinden, doch auch als Signal, daß dieser Weg keineswegs unausweichlich zur Karriere auf der dunklen Seite führen muß. Er erzählt uns, daß er – während er sich auf der einen Seite politisch gegen die drohenden Zensurmechanismen in Gesetzen und in der Technik zur Wehr setzte, gegen die allgegenwärtigen Überwachungstechnologien, gegen die Kriminalisierung von Hackern und die verdachtsunabhängige Speicherung von Verbindungsdaten, doch eines morgens aufwachte und feststellen mußte, einen nicht unwichtigen Baustein für eine digitale Waffe gebaut zu haben, die von einer Firma namens Gamma/Elaman an Regierungen verkauft wird, an Regierungen, die damit das eigene Volk ausspähen, kompromittieren und unterdrücken.

Simon erzählt, daß ein Großteil dieser Industrie in Deutschland und Europa ein Problem mit der Rekrutierung neuer Mitarbeiter hat. Mit „dieser Industrie“ meint er vor allen Dingen die kleinen Firmen wie Gamma oder DigiTask, die eine sehr spezielle Nische bedienen. In dieser Nische wird eine Nachfrage nach Werkzeugen für die Phasen vor und nach einer Infektion mit einer Überwachungssoftware bedient und allem, was technisch minderbegabte Bedarfsträger brauchen, um noch geheime Schwachstellen in fremden Systemen auszunutzen. Desweiteren – und das ist insbesondere für Staaten von besonderem Interesse, die eine allumfängliche Überwachung des eigenen Volkes anstreben – verkaufen, installieren und warten diese Firmen Hard- und Software für Netzwerkkomponenten, die an geeigneten zentralen Knoten und Übergabepunkten in den internationalen Internet-Verkehr eingehängt werden können – gerne auch persönlich vor Ort.

In Anlehnung an den „Signal Intelligence“ genannten Teil geheimdienstlicher Arbeit, dem Abschöpfen elektronischer Signale aller Art, wird die Branche auch unter dem Kürzel SIGINT zusammengefaßt.

Am dringlichsten sucht die Branche – und neuerdings auch ihre Behördenkunden – erfahrene Malware-Autoren, also Programmierer von Schadsoftware, die nicht in vermutlich profitableren, illegalen Netzwerken fischen. Ziel sind Leute, die Spaß am Hacken und Forschen haben, die bestimmte Fähigkeiten mitbringen, welche man nicht an Hochschulen lernt. Natürlich zählen hierzu auch viele der professionellen IT-Sicherheitsberater.

Diese haben jedoch meist entweder bereits eine Anstellung oder besitzen eine gefestigte und gesunde ethisch-moralische Grundeinstellung und wollen keine Malware schreiben – egal für wen. Daß reines technisches Fachwissen nicht ausreicht, haben Firmen und Behörden bereits mehrfach unter Beweis gestellt: Die meisten Maßnahmen und Techniken erwiesen sich als völlig ungeeignet umgesetzt und als Lachnummer. Woher bekommt man nun also fortgeschrittene Hacker-Kompetenz, die einem aber „technopolitisch" bei der Umsetzung von moralisch fragwürdigen Projekten nicht in die Quere kommen?

Firmen wie Gamma oder DigiTask müssen in der Regel selber Forschung betreiben, um inhaltlich und technisch am Ball zu bleiben, das heißt ihren „Warenbestand" an Sicherheitslücken und Exploits frisch zu halten. Das Geschäft in der Grauzone beruht darauf, digitale Einbruchs- und Überwachungswerkzeuge zu entwickeln, für deren Nutzung man nicht das gesamte Wissen und Können der Hacker braucht, die die Lücken entdeckt haben. Die Kunden: vor allem Geheimdienste und Polizeibehörden, die klandestin in Computer und Netzwerke einbrechen und Informationen abschöpfen wollen. Die Entwicklung solcher Werkzeuge ist forschungsintensiv, oft nicht gut planbar und komplex. Grundlagenforschung an neuen Methoden der Umgehung von Sicherheitsmaßnahmen wirft aber nicht unmittelbar Profit ab.

Daher wird solche Forschung oft in Form von externer Expertise bei Selbständigen oder kleinen Sicherheitsboutique-Firmen eingekauft. Die stehen dann vor dem Dilemma – lehnen sie zwielichtige Ausschreibung ab oder nehmen sie teil? Wer heutzutage an eine Firma wie Gamma Wissen und Werkzeuge verkauft, um elektronische Alltagsgegenstände zu kompromittieren, weiß auch, daß im Grunde eine Waffe geliefert wird, die in undemokratischen Regimes gegen Oppositionelle eingesetzt werden wird.

Das weiß man aber nicht nur dann, wenn man an Gamma verkauft: Wer bei solchen Techniken mit „Dual Use", also einer friedlichen Nutzung digitaler Angriffswaffen argumentiert, bewegt sich oft auf sehr dünnem Eis. Die Frage, wofür Forschung und Werkzeuge aus solchen Aufträgen benutzt werden, ist keine akademische mehr.

Die Szene der Computersicherheitsforscher im deutschsprachigen Raum ist eher übersichtlich, bei einem gemeinsamen Kunden in der Schweiz lief Simon dem Schweizer Hakker Bernd* über den Weg, der aufgrund diverser gemeinsamer Projektinteressen schnell ein guter und bester Freund wurde. Bernd erlangte bereits Jahre vor ihrer ersten Begegnung mit diversen neuen Techniken und Werkzeugen eine gewisse Bekanntheit. Schon damals entwikkelte er, gemeinsam mit rund einem knappen Dutzend Hackern und Forschern aus der ganzen Welt Werkzeuge, die heute in jedem Werkzeugkoffer von Sicherheitsberatern anzutreffen sind. Schlußendlich entwickelte die Gruppe von Freizeithackern, die mittlerweile einen gewissen Bekanntheitsgrad in der Szene erreicht hatte, eine Linux-Distribution von Hackern für Hacker: „Backtrack", den vollständigsten Werkzeugkoffer, den ein IT-Sicherheitsberater heutzutage mit sich herumtragen kann.

Eines Tages ging eine britische Firma namens „Gamma International" auf die Gruppe zu: Etwa 2006 fragte das seinerzeit in der Szene wenig bekannte Unternehmen an, ob ein Mitglied dieser Entwicklergruppe zur Verfügung stünde, für die britische Gamma ein technisches „Penetration Test Training" durchzuführen. Hierbei handelt es sich um eine persönliche Schulung von Mitarbeitern größerer und mittlerer Unternehmen für aktive Sicherheitsforschung. Solcherlei Anfragen wurden nicht kommerziell bearbeitet, es gab schließlich keine Firma, einzig einen losen Verbund von Hackern. Wenn es um bezahlte Projekte im Rahmen der privaten Projekte ging, haben die Mitentwickler der Linux-Distribution unter sich ausgemacht: Wer gerade Lust und Zeit hatte, konnte sich damit einen Nebenverdienst sichern.

Martin Münch, ein damaliger Mitstreiter aus besagter Gruppe, zu dem Bernd durchaus eine gute, freundschaftliche Beziehung hatte, griff zu. Was genau während oder nach diesem Training in England geschah, ist nicht bekannt. Heute

firmiert Münch als Geschäftsführer der Gamma International Deutschland GmbH in München.

Zu dieser Zeit wußte niemand etwas über Art und Umfang des Angebots der Firma Gamma und deren weitreichende Verstrickungen in die Grauzonen der Überwachungstechnologie. Die Tatsache, daß dort ein bekanntes Gesicht – für Bernd sogar Freund – tätig war, wirkte sich dabei positiv auf das Gewissen von Bernd und Simon aus und beseitigte nach Lektüre der damals sehr inhaltsarmen Webseite der britischen Gamma aufkommende Zweifel. Gamma zeigte Interesse an Schulungen und der Backtrack-Linux-Distribution. Als es hieß, man würde primär an Regierungen bzw. staatliche Stellen liefern, löste dies anfangs keine besonderen Alarmsignale aus, Sorge hatte man schließlich eher vor Kriminellen, nicht vor den Gesetzeshütern.

Neusprech

Der sogenannte „**Neusprech**“ – also die euphemistische Verschleierung unangenehmer Wahrheiten in griffigere oder blumigere Slogans – war damals in der SIGINT-Branche sehr erfolgreich. Gamma bot neben Personenschutz, Penetrationstests (das sind vom Betreiber bestellte Angriffe auf seine IT-Systeme, um deren Sicherheitsniveau aus Sicht eines Angreifers einschätzen zu können) und Schulungen auch forensische Analysen an: „Forensics“ und „Remote Forensics“. Im Grunde genommen sind das alles Dinge, die zum Standard-Repertoire eines professionellen Sicherheitsberaters gehören und keineswegs verdächtig sind: sogenannte „Offensive Security Workshops“ gehörten schon allein durch die im zivilen Rahmen entwickelte und genutzte Backtrack-Linux-Distribution zum alltäglichen Bild.

Korrekt dekodiert werfen diese Begriffe rückwirkend jedoch einen deutliche Silhouette der Aktivitäten der Firma:

„**Offensive Security Workshops**“ werden beispielsweise von Konzernen als Fortbildungsmaßnahme für das eigene technische Personal eingekauft. Ziel solcher Schulungen ist es, Techniker über den eigenen Tellerrand blicken zu lassen und mit den Denkweisen und Werkzeugen von Angreifern vertraut zu machen. Der Aspekt des Doppelnutzens hierbei liegt auf der Hand: Wer gelernt hat, wie ein Angreifer zu denken und zu hacken, kann auch andere Systeme als die eigenen angreifen.

„**Forensik**“ bezeichnet ursprünglich das Verfahren einer Beweissicherung im Rahmen polizeilicher Ermittlungen. Hier werden kriminelle Tätigkeiten untersucht, identifiziert und klassifiziert. Als deutliches Beispiel von Neusprech wurde dieser Begriff schnell adaptiert, um rechtlich bedenkliche Vorgehensweisen und Werkzeuge zu verniedlichen und somit ethisch-moralisch zu legitimieren. Unter einer „digitalen Forensik“ versteht man im Kontext einer polizeilichen Ermittlung genau das oben Beschriebene: eine Datenspurensuche auf sämtlichen Speichermedien eines Ziel-PCs zur Sammlung von Indizien, die später ein Richter in angemessenem Kontext beurteilen muß.

An dieses Gedankengebäude läßt sich nun leicht anbauen: Es gibt sogar „**Remote Forensic**“. Darunter versteht man ebenso Verfahren, um die oben genannte Schadsoftware in das System einzubringen. Hierbei bedient man sich fast ausschließlich einer Kombination aus technischen Angriffswerkzeugen, wie etwa „Exploits“ genannte Programmfragmente zum Ausnutzen von Fehlern in System, sowie „Social Engineering“, also letztlich den Schwächen der Zielperson selbst.

All dies sind Verfahren, die wir bereits aus der Welt der Spammer und Betrüger kennen. Der Begriff „Remote Forensic“ ist im Grunde genommen ein Paradoxon, hört sich jedoch harmlos genug an. Ein jeder kann sich leicht eine Ausrede zurechtlegen, warum eigentlich ganz harmlos ist, was man da gerade baut oder verkauft. Wenn der staatliche Kunde – von dem man annahm, daß er nach Recht und Gesetz handelt – nicht direkt an den Rechner des Verdächtigen kam, dann wurde die „Forensik“ eben aus der Ferne durchgeführt.

Ganz plastisch muß man sich das folgendermaßen verdeutlichen: eine „kriminalistische Untersuchung“ über ein beliebig unsicheres Netz-

werk, man denke nur an den Staatstrojaner und das unter dem Namen `0zapftis` bekannt gewordene Projekt seiner Demontage. Im Grunde genommen übersetzt man den Begriff Forensik in diesem Kontext so: eine vollständige Kompromittierung eines lokalen Zielsystems mit allen Mitteln, um Daten statisch und dynamisch (also zur Laufzeit) auszuwerten und zu protokollieren. Zur Durchsetzung eines langfristigen „forensischen" Zugangs zum System kann auch illegale Software wie beispielsweise ein Rootkit zum Einsatz kommen, im Volksmund sind letztere auch als „Trojaner" bekannt. Diese Hintertüren werden dann „Remote Forensic Tools" genannt und fortan mehreren Eingeweihten Zugang über das Internet gewähren. Früher sprach man eben nicht von Krieg, sondern von einer bedauerlicherweise nötigen „robusten" Maßnahme zur Abwendung einer humanitären Katastrophe.

Akt 2 – Abrutschen in die Szene

Die Bekanntschaft zu Bernd war es, die Simon

nach vielen Jahren Arbeit als Berater und bezahlter Hacker in der deutschen IT-Security-Branche zu dem Schweizer Unternehmen wechseln ließ, in dem auch Bernd tätig war. Bernd leitete ein kleines, technisches Team der Berner Firma Dreamlab in Winterthur, Simon fing im Team an. Und genau hier fingen die Dinge an, kompliziert zu werden: Gamma bot an, mit den beiden zusammenzuarbeiten. Die Anfrage kam direkt von Münch, mit allem Vorschußvertrauen, das man einem alten Kumpel mitgibt. Münch fragte an, ob nicht Interesse an einem bezahlten Forschungsprojekt bestünde – Thema: Forensik. Eigentlich keine Neuigkeit, die zu untersuchende Technologie schon seit 2005 auf diversen Sicherheitskonferenzen öffentlich vorgetragen – nach IT-Security-Maßstäben eine Ewigkeit. Es gab sogar schon zahlreiche „Forensik"-Werkzeuge, um das Verfahren anzuwenden.

Neue Waffen

Die Idee ist eigentlich sehr einfach und erlaubt, beliebige Rechner bei physikalischem Zugriff vollständig zu kompromittieren, indem der Login-Mechanismus zuverlässig umgangen wird. Sie beruht auf einer architekturbedingten Schwachstelle in fast allen modernen PCs: der Möglichkeit, über eine externe Schnittstelle wie Firewire oder PCMCIA/Cardbus mittels DMA (Direct Memory Access) auf besonders sensible Speicherbereiche zuzugreifen. Man kann dieses Problem vielleicht folgendermaßen anschaulich beschreiben:

Nehmen wir an, es gäbe besonders sichere Einfamilienhäuser mit Fenstern und Türen, die durch nichts und niemanden zu manipulieren sind, halten jedem Einbruchsversuch stand. Dieses Haus hat zudem eine Garage, die direkt ans Haus grenzt und kein Tor besitzt – also nach vorne offen ist. Das Ministerium für Bequemlichkeit & Zeitersparnis hat nun erlassen, daß alle Türen von der Garage ins Haus stets offen zu stehen haben, damit man Einkäufe ohne Verletzungsrisiko direkt vom Auto in die Küche tragen kann.

Im Jahr 2005 hat ein Sicherheitsforscher einer staunenden Öffentlichkeit gezeigt, wie man nun als Fremder durch die Garage ins Haus laufen kann, um ein normales Fenster zu öffnen. Vier oder fünf Jahre später entwickelte Simon im Auftrag von Gamma nun einen allgemeinen Plan, wie man durch die Garage in das Haus laufen und die besonders einbruchsichere Tür von innen per Klinke öffnen kann, um während der

fünften Jahreszeit einen Karnevalsverein unbemerkt ins Haus zu schleusen.

Der Stand war laut Münch, daß Gamma bereits ein Forensik-Werkzeug entwickeln würde und dieses um diverse Funktionen erweitern wollte: Zu Beginn sollte ein Prototyp entworfen werden, der die Machbarkeit auf moderneren Betriebssystemen nachweist. Die alten Demos aus dem Jahr 2005 waren sämtlichst gegen Systeme mit dem Betriebssystem Windows XP für 32-Bit-Prozessoren gerichtet, und in der Szene ging das Gerücht, die Technik würde bei einem Windows Vista nicht mehr funktionieren.

Das war für einen Hacker mit ausgeprägtem Spieltrieb natürlich ein schönes Projekt. Man hatte Spaß an der Arbeit, und eine alte Idee wurde mit zahlreichen neuen Einflüssen neu erfunden. Über einen langen Zeitraum verteilt kamen dann immer wieder neue Anforderungen an den ursprünglichen Prototypen, welche aus diesem letztlich ein fertiges Werkzeug machten. Am Ende bastelte das Team sogar ein wenig über den Auftrag hinaus an dem Werkzeug, da es eine nette Abwechslung aus dem manchmal recht tristen Arbeitsalltag darstellte und Münch zudem zugesichert hatte, man dürfe mit den eigenen Werkzeugen und Verfahren machen, was man möchte, es also nicht exklusiv sei.

Am Ende der Entwicklung stand ein Werkzeug, welches es technisch unbegabten Menschen ermöglichte, nahezu jeden PC und jedes Notebook durch schlichtes Verbinden mit einem Linux-PC an die Firewire- oder z. B. bei Notebooks die pccard-Schnittstelle zu kompromittieren – egal, ob es sich um einen hebräischen 64-bit-Windows-8-PC handelt, um ein Mac OSX Lion oder ein beliebiges Linux/BSD-Betriebssystem. In anderen Worten: Kabel rein – kurz warten – Rechner übernommen.

Bewußtwerdung

Allmählich dämmerte Simon, daß er an einem recht mächtigen Werkzeug arbeitete, welches durch staatliche Hände auch mißbraucht werden könnte. Allerdings überwog zu diesem Zeitpunkt der positive Charakter des Projektes, schließlich war der Auftraggeber ein langjähriger Bekannter, und der eigene Arbeitgeber als beobachtende Instanz hatte keine Bedenken geäußert. Er nahm an, er würde an einem Forensik-Werkzeug für legitime, kriminalistische Indiziensicherung feilen, dessen zugrundeliegende Technik einmal robust, zuverlässig und einfach bedienbar implementiert werden sollte – schwer abzusehen, daß in der Folge ein Produkt namens FinFireWire entstehen sollte, welches im Rahmen der FinFisher-Produktpalette an beliebige Staaten veräußert werden würde.

Simon beschreibt, daß in diesem Zeitraum der Geschäftsführer von Dreamlab, Nicolas Mayencourt, damaliger Chef der beiden, vermehrt mit Gamma in Kontakt zu treten begann – allerdings nicht ausschließlich mit Münch. Mayencourt gefiel es wohl, mit Behörden und deren Zulieferern an solchen Technologien zu arbeiten. Daher wurden sämtliche Verhandlungs- und Vertriebstätigkeiten in diesem Bereich am Firmensitz in Bern zentralisiert, und die sich anbahnenden Geschäfte waren weit weniger transparent als der Kontakt zuvor.

Zwar hielt es Simon durchaus für legitim, wenn solche Techniken bei der Verbrechensbekämpfung unter strengen richterlichen Auflagen zum Einsatz kommen. Schließlich versicherte man ihm, daß in der Schweiz – anders als in Deutschland – weit besser kontrolliert werden würde, ob und wie umfassend eine Behörde in die Privatsphäre eines Verdächtigen eingreifen kann und darf. Mayencourt versicherte ihm damals auch, man verkaufe ausschließlich an die Schweizer Behörden bzw. ISPs.

Und unter dem Strich klang alles plausibel: Simons Vertrauen in Dreamlab war groß. Die Firma präsentierte und verhielt sich in der Öffentlichkeit politisch korrekt, sponsorte Open-Source-Projekte und veranstaltete kostenlose, geschlossene Parties und Konferenzen von und für ein internationales Hackerpublikum in der Schweiz. Sie förderte aktiv offene Standards in der IT-Security und offene Software in der Gesellschaft. Alles machte einen rundherum politisch korrekten Eindruck, und es lag nahe, daß eine Firma, die sich „Ethical Hacking", also ethisch korrektes Einbrechen in Computer, auf die Fahnen schreibt, auch über etwaige, nicht gewollte Tendenzen innerhalb der Firma wacht und diese entsprechend lenkt.

Doch offenbar sollte es nicht so sein: Die beiden Kollegen beschlich bald die Ahnung, über Bernds Bekannten wäre ein weiteres Geschäftsfeld aufgetan worden, um die in der Schweiz bislang erfolgreich eingesetzte Überwachungstechnik auch zu exportieren. Mayencourt fand es wohl ehrenhaft, von Regierungen als ernsthafter Partner im Kampf gegen Verbrechen wahrgenommen zu werden, mutmaßt Simon. Da ist es wieder, das bereits beschriebene Bedürfnis nach Bestätigung, seine Technik auch jenseits der Schweiz zu vertreiben – vielleicht ging es aber auch einfach nur um Geld.

Daß Dreamlab derart feste Strukturen in den Gremien und Behörden erschloß, die sich mit „Lawful Interception" befassen, überraschte Simon. Auch daß sein Arbeitgeber schon seit Jahren Geräte herstellte, die es Ermittlungsbehörden in der Schweiz erlaubten, den Internetverkehr von Verdächtigen abzufangen, übersah oder ignorierte er lieber. Ferner hielt Dreamlab laut der neuesten Informationen von Wikileaks (s. u.) einen sogenannten „Infection Proxy" in seinem Portfolio vor – ein Gerät, welches an Internet-Knotenpunkten zentral genutzt werden kann, um bestimmten Nutzern und Nutzergruppen gezielt und unbemerkt eine eigens präparierte Schadsoftware unterzuschieben. Der „Infection Proxy" verändert Webseiten oder Datei-Downloads, während sie sowieso vom Nutzer heruntergeladen werden und schleust dabei die Schadsoftware ein. Dies ist ein denkbarer Infektionsweg für den „Staatstrojaner", von dem sich Dreamlab im September 2013 noch im Rahmen eines Statements auf seiner Webseite scharf distanziert.

Erst nach und nach wurden die Karten seitens des Auftraggebers offener ausgespielt. Es ist nicht ganz klar, ob Gamma hier eine systematische Desensibilisierung betrieb oder einfach annahm, alle Beteiligten wüßten ohnehin Bescheid. Vermutlich war dies teilweise sogar der Fall, dieser Teil hatte jedoch noch nichts zu sagen. Gamma-Kataloge, die man zwischenzeitlich auch bei Wikileaks finden konnte, priesen längst Waren an, die einem James-Bond-Fan das Herz höher schlagen lassen. Doch Simon erinnert sich auch noch genau an die immer plumper werdenden, selbstbetrügerischen Schönrederein wie: „Man kann einen Infection Proxy auch für friedliche Zwecke benutzen, zum Beispiel um Viren unschädlich zu machen".

„Erkenntnis kommt langsam und schleichend", erklärt Simon, „man hinterfragt in der Regel erst dann, wenn einem etwas merkwürdig vorkommt. Die räumliche Distanz zwischen Bern und Winterthur führte letztlich auch dazu, daß uns einiges nicht oder erst sehr spät merkwürdig vorkam", beschreibt er den Prozeß, der sich etablierte, die Dinge und Tätigkeiten innerhalb der Firma mit einem kritischen Auge zu betrachten. Er sagt von sich, sehr gutgläubig und naiv gewesen zu sein – aber auch froh, mit seiner Arbeit eine gewisse Anerkennung gefunden zu haben – nur zwei der Gründe, warum sich die finale Erkenntnis spät, dafür aber heftig eingestellt habe.

In der Konsequenz beschlossen die beiden, allmählich Abstand von den immer eindeutiger werdenden Anfragen seitens Gamma gewinnen zu wollen und begannen, negativ auf Projektanfragen zu reagieren, wenn klar war, wo die Reise hingehen soll. Irgendwann drückte Mayencourt dem Team einen extrem fragwürdigen Job „auf's Auge", über deren Details aber noch immer eine Verschwiegenheitsvereinbarung schwebt. Eine firmeninterne Differenz brachte dann das Faß zum Überlaufen, und Simon und Bernd kündigten während eines Team-Meetings mit den Schweizer Kollegen im zwei Monate zuvor eröffneten Büro in Berlin.

Akt 3 – Gewissensentscheidungen

Obwohl am nächsten Morgen auch noch die erst frisch angestellten anderen Berliner Kollegen aufgrund der Kündigung fristlos vor die Tür gesetzt wurden, beschlossen die beiden, sich professionell zu verhalten und die Projekte ordentlich zu beenden. Zeitgleich kamen natürlich Sorgen um die Zukunft auf, und Simon und Bernd skizzierten zahlreiche Modelle, um gemeinsam weiter zusammenarbeiten zu können. Sie verhandelten mit einigen potentiellen Investoren und anderen Firmen aus der Branche weltweit.

In der Gründungsphase nahm Gamma auch gleich die Chance wahr, sich der Firmen-Neugründung anzubiedern. Alle wissen – oder nehmen zumindest an –, daß eine Existenzgründung auch mit Tiefs einhergeht, in denen man Unterstützung von Freunden und Partnern benötigt. Simon sagt, auch Mayencourt bot großzügig an, sich an der Firma mit diversen Mitteln zu beteiligen und auch gleich noch Bekannte in den Aufsichtsrat zu setzen.

Wer spielt da nicht gleich noch mit den Ängsten zweier Familienväter, die im Grunde eine Menge zu verlieren haben? Gamma bot an, jederzeit für die Gründer da zu sein, wenn die neue Firma in einen finanziellen Engpaß geraten sollte; es gäbe genug zu tun. Und im Zweifelsfall gäbe es natürlich auch immer wieder Bedarf an Offensive-Security-Schulungen, an denen man in der Regel die größte Gewinnmarge abschöpfen kann.

Am Ende entschlossen sich Simon und Bernd jedoch, das hohe Risiko zu akzeptieren und zu einhundert Prozent unabhängig von Geldgebern und deren politischen und technischen Motiven zu sein: Sie beschlossen, eine Schweizer Aktiengesellschaft zu gründen, die sich vollständig in ihrer Hand befindet.

Die Firma Gamma rückte nun bereits in das negative Licht der Öffentlichkeit, und sie wollten primär eine Distanz zu der Firma aufbauen, nicht zu den Menschen, die dort arbeiteten. Doch trotz Distanz und Konsequenzen im beruflichen Leben gerieten die beiden Abtrünnigen allmählich unter Druck, da sich auf der Webseite der alten Hackergruppe noch Münchs Name und Foto befand. Er wurde aus der Gruppe ausgeschlossen, sein Name und das Foto entfernt. Damit beendete zumindest Bernd eine langjährige Freundschaft, wofür ihm Simon „höchsten Respekt und Anerkennung" zollt.

Bei Gamma arbeiten normale, nette Menschen – Simon konnte Kritik üben, ohne sofort abzublitzen. Im Gespräch über die moralischen Bedenken stellte er fest, daß er es dort auch nur mit Menschen zu tun habe, denen er persönlich auch nichts vorwerfen möchte. Auch Münch sei ein netter und sehr umgänglicher Mensch, aber im Grunde bestätigte er mit einer Aussage das, was Simon bereits bei Zusammentreffen auf polizeilastigen Veranstaltungen in den Raucherpausen mitbekommen haben will: „Man stumpft einfach ab. Und das muß man auch." Dennoch ist sich jeder seines Handelns dort bewußt, spätestens nach all den öffentlichen Debatten um die verkauften Technologien.

Man merkt Simon an, wie schwer das Zusammenfassen der diversen unbequemen Wahrheiten fällt, ab und zu fallen viele relativierende Worte, doch immer wieder fokussiert sich die Erzählung. Es ist ihm wichtig, die Mechanismen aufzudecken, wie einfach enthusiastische Hakker entlang der Grauzone gelockt werden: Da die SIGINT-Industrie dank der zahlreichen Gesetzesänderungen in der jüngsten Vergangenheit der EU und Deutschland einen äußerst lukrativen Markt vor die Nase gesetzt bekommen hat,

spielt Geld oft eine untergeordnete Rolle bei der Rekrutierung.

So besteht die Herausforderung primär darin, die mit Geld noch nicht beseitigte Rest-Moral zu besänftigen, indem gezielt mit den Wünschen und „Sehnsüchten" der Hacker gearbeitet wird. Die Zutaten kennt Simon genau: Viel Lob und Anerkennung für bereits geleistete Arbeiten und Veröffentlichungen; Spiele mit der Neugier eines Hackers, Versicherungen, daß es nichts Besseres gäbe, als für das Spielen (Forschen) überdurchschnittlich gut bezahlt zu werden; Beseitigung restlicher moralischer Bedenken, indem dem Hacker eingeräumt wird, über die ethisch-moralischen Aspekte später nachdenken zu können.

Er kann schließlich nach einem Jahr einfach mal gucken, wie es war – und dann gehen, wenn er möchte. Tätigkeiten werden soweit es geht mit dem positiven Teil der Dual-Use-Geschichte beschrieben und beworben: Ein ehrgeiziger Hakker und Programmierer wird sein Projekt immer so perfekt wie möglich abschließen wollen, egal was passiert, er tut das für sein Ego und seine Reputation.

Vorbildfunktion

Nun kann man sein Schicksal akzeptieren und zum Überwachungsfachidioten „abstumpfen", man kann aus Angst, die Familie nicht mehr ernähren zu können, einfach weitermachen. Und es lauert die Angst im Hinterkopf, auf dem anderen Markt zu versagen.

Man kann sich einreden, nirgendwo anders eine gleichbedeutend interessante Forschungstätigkeit für gleiches Geld und gleiche Anerkennung zu bekommen, man kann auch strategisch denken und sehen, welche Sicherheiten und Chancen es auf dem Markt der Überwachungstechnik derzeit und in Zukunft gibt. Der Großteil aller Gruppen hat vermutlich eines gemeinsam: die Angst vor dem unbequemen Weg, aus dieser Angelegenheit wieder herauszukommen.

Im Grunde genommen hätte sich eine „Zusammenarbeit" mit Gamma auch auf anderem Wege anbahnen können, ohne daß Simon oder Bernd über einen Freund Kontakt zur fragwürdigen Firma gehabt haben müßten – schließlich bewegen sich Gamma und ähnliche Firmen auch auf einschlägigen Hacker-Konferenzen und kommen so mit technisch versierten Leuten leicht in Kontakt. Dreamlab selbst gibt sich deutlich ziviler und unterstützt Open-Source-Projekte und Ausstellungen, wie zum Beispiel die OpenExpo, wo sie 2009 die Organisation des Security-Tracks übernommen hat.

Alternativlos

Auf die Frage, ob es denn wirtschaftlich alternativlos ist, sich an die einschlägigen Regimes zu verkaufen, holt Simon kurz aus: Auf dem IT-Security-Markt gibt es keine höheren Tagessätze, es gibt nur viele verkaufbare Berater-Tage. Als ehemaliger Arbeitnehmer in der Branche und Geschäftsführer einer eigenen Firma mit mittlerweile fünf Angestellten kann Simon konstatieren, daß es sich finanziell überhaupt nicht lohnt, als Firma oder Dienstleister für die schattigen Seiten tätig zu werden.

Der zivile Markt ist voll mit spannenden Projekten und Forschungsthemen – und am Ende kann man sich sogar auf einen Chaos Communication Congress stellen und öffentlich darüber diskutieren. Wenn man das möchte, um sich die notwendige Anerkennung zu holen. Es gibt keinen Grund, auf Aufträge einer Firma

wie Gamma oder DigiTask angewiesen zu sein – auch nicht als Subunternehmer. Das ist alles eine Frage des eigenen Mutes und des Aufwandes. Simon rät jedem Hacker dazu, sich einmal Gedanken über das eigene Tun und Handeln zu machen und den einen großen Schritt für das eigene Selbstbewußtsein zu wagen.

Simon findet, das Argument „wenn ich es nicht mache, macht es halt ein anderer", welches man allerorten hört, sei ein Trugschluß. Denn dieser Andere muß sich erstmal finden, und findet er sich nicht, macht es eben keiner. Allein die öffentlichen und vergeblichen Bemühungen des BKA, diese Expertise im eigenen Haus anzusiedeln, sind Beweis genug. In der Regel müssen sie jedoch bei Bedarf immernoch externe Dienstleister hinzuzuziehen, wie eben Simon. Das ist auch bei den meisten deutschen Behörden wunderbar öffentlich dokumentiert. Von denen wurde er bislang noch nicht bewußt angesprochen und glaubt vorerst auch nicht, daß dies passiert. Die passive Suche des finanziell überraschend schlecht ausgestatteten BKA nach Schadsoftware-Autoren für den neuen „Staatstrojaner" läuft quasi öffentlich vor unserer aller Augen. Es ist ein Spaß, sich über einen längeren Zeitraum die entsprechenden Stellenausschreibungen anzusehen. Simon meint, die Behörden werden sich noch einen sehr langen Zeitraum mit Unternehmen aus dem privaten Umfeld auseinandersetzen müssen, wenn sie an ihren fragwürdigen Werkzeugen weiter festhalten wollen.

Wie eifrig Firmen auf der Suche nach neuen fähigen Kräften sind, läßt sich auch an Gamma beobachten. Die Firma schien in eine neue sehr aktive Rekrutierungsphase einzusteigen, um weniger auf externe Dienstleister angewiesen zu sein. Gamma-Mitarbeiter suchen aktiv nach neuen Kontakten und schauen sorgfältig allen Aktivitäten auf der Business-Plattform XING hinterher: Ein „Reverse Engineer", der für eine Firma im süddeutschen Raum tätig war, suchte Kontakte zu Personen mit ähnlichen Fähigkeiten und Interessen und sendete eine Kontaktanfrage an Simon. Der akzeptierte den Kontakt, und sie tauschten ein paar Nachrichten per E-Mail aus. Prompt erhielt Simon einen Anruf von Gamma, ob er ebenjene Person denn kennen würde, offensichtlich war die Firma an seinem Profil sehr interessiert. Wenig später änderten sich zahlreiche Datenfreigabe-Einstellungen des Kontaktes und der Name der Firma wurde unterdrückt – wie bei allen anderen Gamma-Mitarbeitern auch.

Aber es zeigt sich auch immer wieder, daß fähige Köpfe fehlen und deswegen selbst vermeintlich hochprofessionelle Firmen wie Gamma an den einfachsten Sicherheitstechniken scheitern. Hier verweist Simon auf die von Aktivisten beschriebenen Anfängerfehler beim Einsatz der AES-Verschlüsselung von Gammas „Trojaner" mit dem Namen FinFisher. Es scheint eben nicht der Fall zu sein, daß sich sofort ein neuer guter Mitarbeiter findet, sofern es um komplexe Randthemen geht, also überläßt man das Feld den Stümpern oder kann es eben nicht besetzen. Das gleiche Problem kann man übrigens auch bei den anderen Herstellern solcher Software begutachten: Ob HackingTeam, Gamma oder DigiTask – sie alle scheinen auch minderbegabtes Personal zu beschäftigen, frei nach dem Motto „Sell now, patch later".

Anders jedoch die Situation in den USA: Dort gibt es ein großes Budget für die Forschung in dieser und anderen Richtungen. Neusprech-Stichwort hier wäre zum Beispiel **„Defense"**. Die DARPA und IARPA bezuschussen dort teilweise Open-Source-Projekte und Hackerspaces – das Geld wird gern genommen. Simon findet das bedenklich, wenn solche Militär-Institutionen immer ein Feigenblatt vorweisen können, um schleichend in die zivile Gesellschaft einzusikkern und dort als Normalität oder gar Notwendigkeit wahrgenommen werden. Vielleicht profitieren sogar Menschen von dem Geldsegen, die in der Lage sind, kritisch mit der Motivation ihrer Sponsoren umzugehen und diese zu reflektieren – allerdings ist zu befürchten, daß auch bei kritischer Akzeptanz eine Schere im Kopf schlummert, die sich irgendwann bemerkbar macht – und sei es bei der Erziehung der eigenen Kinder in zehn Jahren.

Simon und Bernd wurden ebenfalls von einem vermeintlichen Mitarbeiter der IARPA per E-Mail angeschrieben, der mit bezahlter For-

schung im Rahmen der IARPA „gedroht“ hatte – auch hier ging es um ein von ihnen zuvor auf Sicherheitskonferenzen vorgestelltes Verfahren zum Belauschen und Kompromittieren funkbasierter Systeme. Simon nimmt an, hier herrscht grundsätzlich eine Mischung aus sorglosem Umgang mit dem eigenen Wissen und einer Art Domino-Effekt unter Hacker-Kollegen, die vermutlich fast alle schon mal für die Regierung oder ihre Zulieferer umgekippt sind.

Man kann sich seine Hacker auch züchten, indem man moralisch weniger gefestigte Jugendliche in der Uni abholt. So arbeitet die Armee auch an US-Universitäten, und diese Verhältnisse werden wir vermutlich ebenfalls bald hierzulande beobachten. Die Armee wirbt auch nicht mit dem Töten von Zivilisten um Rekruten, sie wirbt mit Sport & Spiel, mit Freiheit & Gerechtigkeit, mit High-Tech und modernster Ausrüstung. Diese jungen Menschen an den Unis müssen heute gut aufpassen, daß man sie nicht um den Finger wickelt – nicht, daß sie sich dann Jahre später durch Lieferanten digitaler Waffensysteme zu ent-moralisierten Hacker-Schergen haben erziehen lassen.

Epilog

2011 begann die Enthüllungsplattform Wikileaks mit der Veröffentlichung der sog. „Spy Files“. Gegenwärtig gibt es bereits die dritte Runde, die interne Dokumente von Zulieferern und Kunden veröffentlichen und somit technische Details sowie weitere Zusammenhänge bloßstellen. Die jüngste Veröffentlichung offenbarte einige Dokumente der Firma „Dreamlab Technologies AG“ in Bern, welche eine partnerschaftliche Kooperation mit Gamma zum Inhalt hatte, sowie zahlreiche Angebote und Preislisten für Dienstleistungen und Komponenten aus dem eigenen Hause: „Lawful Interception“-Hardware, -Software und dazugehörige Wartungsverträge. In einer Stellungnahme auf der eigenen Webseite *http://www.dreamlab.net/stellungnahme-zu-spy-files/* erklärte Geschäftsführer Nicolas Mayencourt in der üblichen, passiven Salami-Taktik-Manier, daß es eine Erleichterung sei, daß die Verträge nun (endlich) geleakt wurden. Die „Schuld“ an einer angeblich so negativen Partnerschaft mit Gamma wird nach der Einleitung unmittelbar auf Bernd geschoben, da dieser ja den Kontakt zu Gamma anfangs herstellte. Simon merkt an, daß er seine These später noch mit der – wie er sagt – Lüge bekräftigt, „betreffender Mitarbeiter“ hätte ihm dazu geraten und ihm unproblematische Praktiken attestiert.

Noch interessanter findet er Mayencourts anschließendes Statement, die neugegründete Firma seines ehemaligen Angestellten hätte seine technische und geschäftliche Beziehung zu Gamma weiter ausgebaut. Dies seien Weasle-Words und interessante These eines Menschen, der die ganz gegenläufigen Meinungen seiner alten Kollegen zum Thema Überwachung und Überwachungstechnik offenbar geschickt ausblendet, um seine Weste reinzuwaschen.

Geschickt beschreibt Mayencourt, daß Dreamlab niemals „Staatstrojaner“ selbst entwickeln würde, weil diese nicht rechtsstaatlich seien und es keine legitimen Anwendungsfälle für staatliche Trojaner gäbe. Währendessen haben, wie aus den letzten Wikileaks-„Spy Files“ zu entnehmen ist, im Jahr 2013 er und seine Firma Dreamlab offenbar den Vertrieb der Gamma-Produktpalette inklusive Trojaner in bestimmten Regionen übernommen.

Simon bekundet sein Mitleid mit dem Geschäftsführer der Dreamlab Technologies in Bern, der berufsbedingt offenbar streng gegen seine persönlichen Ideale und dem Selbstbild des Unternehmens verstoßen muß: Einige, über einen TV-Beitrag veröffentlichte Dokumente zeigen, daß Dreamlab den oben erwähnten „Infection proxy“ vermutlich für sehr hohe Summen verkaufte. Sollte dies wahr sein, widersprächen das dem Statement auf der Webseite genauso wie die im Rahmen der „Spy Files“ Serie 3 auf Wikileaks veröffentlichten Dokumente. Die erwähnten Dokumente sind auf einen Zeitpunkt datiert, zu dem Simon und seine Kollegen schon nicht mehr für Dreamlab tätig waren oder bereits an einer Alternative planten: *http://www.wikileaks.org/spyfiles/docs/DREAMLAB-2010-OMQuotMoni-en.pdf* Abschnitt 3.1.1

*** Namen wurden von der Redaktion geändert**

Alles nur Fake?

Pseudohumanität, Pseudotransparenz, Pseudoidentität

von Andrea <andrea@renderland.de> & Constanze <constanze@ccc.de>

In Deutschland gibt es eine Regelung, die mit Residenzpflicht bezeichnet wird. Sie gilt für Geduldete und Asylsuchende: Diese dürfen das Bundesland (in Bayern und Sachsen kleinere Gebiete), in dem sie auf eine sogenannte Aufnahmeeinrichtung zugeteilt werden, nur mit Erlaubnis der zuständigen Ausländerbehörde verlassen. [1] Verstoßen sie dagegen, machen sie sich strafbar.

Als eine der Autorinnen vor vielen Jahren eine Sachbearbeiterin der Eberswalder Ausländerbehörde wegen der durch die Residenzpflicht bei einer Freundin aufgetretenen Probleme fragte, ob sie diese Regelung nicht auch für inhuman und als eine Beschränkung des Rechts auf Bewegungsfreiheit hielte, bekam sie eine unerwartete Antwort: „Aber nein, die Residenzpflicht dient dem Schutz der Asylsuchenden! Das sind politisch Verfolgte, hochgefährdete Leute – wir müssen immer wissen, wo sie sich aufhalten." Das machte sprachlos, denn die Frau war ganz überzeugt, daß die in den letzten Jahren noch erweiterte Residenzpflicht und die Pflicht zum Verbleib beim „Aufnahmeplatz" eine gute Sache seien. Hallo Welt? Willkommen in der Sprache der versicherheitlichten Ethik, des Neusprech, der Euphemismen.

So heißt es etwa zu der seit 2003 regulär vorgenommenen erkennungsdienstlichen Behandlung von Flüchtlingen:

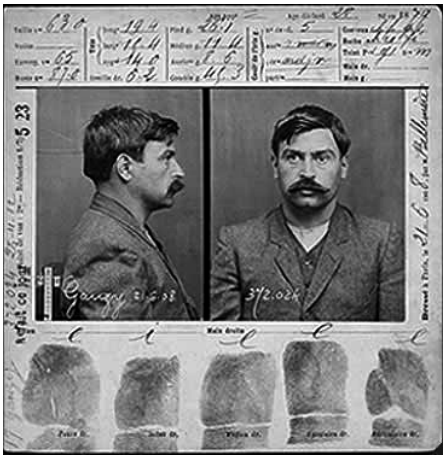
„Des Weiteren sind die Mitgliedstaaten zu verpflichten, allen Personen, die internationalen Schutz beantragen, und allen Drittstaatsangehörigen oder Staatenlosen, die mindestens 14 Jahre alt sind und beim illegalen Überschreiten einer Außengrenze eines Mitgliedstaats aufgegriffen wurden, unverzüglich die Fingerabdrücke abzunehmen und die Daten dem Zentralsystem zu übermitteln." (Erw 17, VO (EU) 603/2013) „Das Verfahren zur Erfassung von Fingerabdruckdaten wird gemäß der nationalen Praxis des betreffenden Mitgliedstaats und unter Beachtung der in der Charta der Grundrechte der Europäischen Union, in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten und im Übereinkommen der Vereinten Nationen über die Rechte des Kindes verankerten Schutzklauseln festgelegt und angewandt." (Artikel 3, Abs. 5 VO (EU) 603/2013)

Landet also ein Asylsuchender heute beispielsweise in Frankfurt am Flughafen, ist ihm die erkennungsdienstliche Prozedur sicher. Der elektronische Abgleich von Fingerabdrücken mit erkennungsdienstlichen Dateien der Polizeivollzugsbehörden ist mit der Novellierung der oben zitierten „Eurodac"-Verordnung zum Normalfall geworden. Eurodac, ein Fingerabdruckidentifizierungssystem nur für die eben genannten Gruppen, wurde im Jahr 2000 beschlossen und 2003 in Betrieb genommen, um das Dubliner Übereinkommen besser umsetzen zu können. Das Dubliner Übereinkommen der 1990er und die genaueren Verfahrensregelungen von 2003 (EG-Verordnung 343/2003, auch „Dublin II" genannt, sowie EU-Verordnung 604/2013, „Dublin III") regeln die Zuständigkeit eines europäischen Landes für ein Asylverfahren. „Dublin II" läuft im Grunde der Genfer Flüchtlingskonvention zuwider, der sich sämtliche EU-Mitgliedsstaaten verpflichtet sehen. Denn es führt zu der dort explizit als sogenanntes Non-Refoulement-Prinzip ausgeschlossenen Rückschiebepraxis, die Flüchtlinge zwingt, nur in dem Staat Asyl beantragen zu können, der ihre Einreise durch Visumserteilung oder Nichtverhinderung des Grenzübertritts „verursacht" hat.

Eurodac ist ein Kernstück der Asylverweigerungspraxis in Europa. In Deutschland erledigt die damit verbundene erkennungsdienstliche Behandlung zur Aufzeichnung von möglichst eindeutigen physiologischen Merkmalen der Individuen die sogenannte Erstaufnahmeeinrichtung oder die Polizei. Die Fingerabdrücke werden jeweils zum Bundeskriminalamt (BKA) übermittelt, um sie mit der Eurodac-Datenbank abzugleichen.

Sind die aufgenommenen Abdrücke nicht von ausreichender Qualität, um sie mit Eurodac-Daten zu vergleichen, muß sich die Betroffene erneut erkennungsdienstlich behandeln lassen. Asylsuchende und illegalisierte Migrantinnen sind damit seit Jahren die am intensivsten registrierte und kontrollierte Bevölkerungsgruppe. Ein Vertreter einer Gruppe von eritreischen Flüchtlingen im Oberurseler Containerlager bringt es so auf den Punkt:

„Der Fingerabdruck ist ein verstecktes Gefängnis für uns. Aber die Leute sehen diese Wahrheit nicht. Ich klage alle Europäer an. Sie sehen nur Dublin, Dublin, Dublin,... Wenn du Kriminelle kontrollieren willst, dafür gibt es Interpol. Aber wozu wollen sie uns kontrollieren? Wir haben nichts gemacht. Wir haben keine Bombenanschläge verübt. Sie bringen uns dazu, Kriminelle zu werden, weißt du?“ [2]



Innerhalb der Eurodac-Regelungen werden Rechte der Betroffenen integriert, zum Beispiel Datenauskunfts- und Löschungsrechte. An die Betroffenen gewandt heißt es auf der Webseite des Europäischen Datenschutzbeauftragten (EDSB): „Sie können bei den zuständigen Behörden eines jeden Mitgliedstaats Zugang zu den Sie betreffenden gespeicherten Daten beantragen. Erforderlichenfalls kann die nationale Datenschutzbehörde Ihres Landes um Unterstützung ersucht werden.“ [3] Das entbehrt nicht einer gewissen Perfidie. Denn wieviele in äußerst prekären, kriminalisierten und von Demütigungen geprägten Umständen lebende Menschen nehmen derartige Rechte in Anspruch, sind so mutig wie die eritreische Gruppe, die ihre Stimme erhebt? Wieviele können auf ein menschenrechtlich engagiertes Netzwerk an Rechtsberaterinnen zurückgreifen, die im Zweifel bis vor den Europäischen Menschenrechtsgerichtshof gehen?

Die Veröffentlichungen der Kommission und des Europäischen Datenschutzbeauftragten sprechen Bände dazu: Unter den jährlich mehreren hunderttausend Zugriffen auf die Eurodac-Daten waren nur einige hundert, bei denen das Auskunftsrecht genutzt wurde. Diese aber entpuppten sich größtenteils als nicht im Auftrag der Betroffenen gestellt, sondern von den Verwaltungen für einen ganz anderen Gebrauch der Daten vorgenommen. [4] Der Rückgang auf wenige Dutzend ab dem Jahr 2008 ließ die Kommission schließen, daß es nun „keinerlei Anlass zu Besorgnis“ hinsichtlich eines Mißbrauchs mehr gebe. [5] Es wird von vornherein angenommen, daß höchstens einige Dutzend Migrantinnen ihr Auskunftsrecht in Anspruch nehmen.

Die regelmäßigen öffentlichen Berichte der durch den EDSB gestellten ‚Koordinierungsgruppe für die Aufsicht über Eurodac‘ darüber, ob alle Auflagen und Sicherheitsanforderungen eingehalten werden, nützen den Betroffenen kaum etwas, bereichern allenfalls akademische, politische und technische Debatten von Beraterinnen und Entscheidungsträgerinnen. Die Informationstiefe oder institutionelle Transparenz waren besonders in der Anfangsphase mäßig und erweckten teilweise den Eindruck,

als habe diese Kontrolle doch mehr Feigenblattfunktion als alles andere.

So wurden viele Teile eines Inspektionsberichts 2006 durch die Angestellten des EDSB über die konkreten Betriebsbedingungen und die Administration der zentralen Datenbank einfach gelöscht: „Because of the sensitivity of some information in the report, it is not publicly available." Dazu gehörten etwa Abschnitte zum Risiko- und Vorfallmanagement, die gesamten Informationen zur Sicherheitsdokumentation, über zugehörige Institutionen und Zulieferer. Das Fazit lautete denn auch: „EDPS is generally speaking satisfied with the security level of EURODAC." [6]

Auch 2007 wurde beim datenschutzbezogenen Security-Audit der Technik seitens der Koordinierungsgruppe „a fair level of protection to date" attestiert. [7] Im Inspektionsbericht von 2009 wurde die Kritik differenzierter und monierte vor allem die schlechte Informationspolitik gegenüber den Betroffenen sowie das oft kritisierte unwürdige Verfahren der Alterseinschätzung via medizinischer Untersuchung (etwa Röntgenverfahren). Gefordert wurde auch eine Anhebung der Altersgrenze zur Abnahme der Fingerabdrücke von 14 auf 18 Jahre. [8]

Die in den biometrischen Systemen verwendete Hard- und Software und deren reale Performanz unterliegen keinerlei Transparenz. Jedes biometrische System produziert Falschrückweisungen, die durch administrative Anpassungen mehr oder weniger häufig auftreten. Welche Performanzdaten die verwendete Technik hat, auf Basis welcher Datenqualität mit welchen Schwellwerten zwei Fingerabdruckmuster noch als hinreichend ähnlich gewertet werden, um als sogenannter „Treffer" zu gelten, erklärt keiner der Berichte sowohl des EDSB als auch der EU-Kommission auch nur annähernd, obwohl „Treffer" zu lebensgefährlichen Rückschiebungen von Asylsuchenden führen können.

In einer der Stellungnahmen der EU-Kommission zur Anfang 2013 abgeschlossenen Anpassung der Verfahrensregeln rund um Eurodac – zum Beispiel erweiterte Zugriffsbefugnisse für Strafverfolgungsbehörden – wird ein weiterer schwerwiegender, biometrischen Systemen inhärenter Fehler thematisiert: ‚failure to enrol', ein Problem, das immer auf einen gewissen Prozentsatz Betroffener zutrifft. Daß die Eurodac-Abschreckung einen ganz besonderen ‚failure to enrol' herbeiführt, wird fast beiläufig erwähnt:

„In anderen Fällen, deren Häufigkeit nur schwer zu bestimmen ist, kann es vorkommen, dass sich Flüchtlinge selbst verstümmeln, damit ihnen keine Fingerabdrücke abgenommen werden können." [9]

Durch den EDSB erfährt die Öffentlichkeit zwar derlei Aspekte einigermaßen gesichert. Es werden immer wieder Detailfragen des unautorisierten Zugriffs auf Einzeldaten, zur Einhaltung der Pflicht zur vorzeitigen Löschung unter bestimmten Umständen, zum Zugriffsrecht durch Betroffene, zur Speicherung der Daten von Kindern oder zur Heranziehung privater Subunternehmer für Teile des Systemmanagements oder der -entwicklung kritisch untersucht. Dennoch drängt sich die Frage auf, inwiefern die Kontrollinstanz selbst das auf Basis der Menschen- und Persönlichkeitsrechte grundsätzlich fragwürdige System noch zusätzlich legitimiert und weiter stabilisiert. Sie wirkt allzuoft wie ein institutionalisierter Don Quixote.

Deutschland hat eine führende Rolle im Vorantreiben der Dublin-Regelungen und ihrer Absicherung durch Überwachungstechnologien eingenommen. Der Bundesgrenzschutz, der heute Bundespolizei heißt, hat seit Ende der 1960er Jahre das Recht zur erkennungsdienstlichen Behandlung von Menschen. Was einmal eine kurzzeitige Regelung innerhalb der Notstandsgesetze war, kam wenige Jahre später ins Gesetz und wurde mit der Neuregelung des Asylverfahrens 1992 zur Normalität. In jener Zeit wurde auch das beim BKA geführte AFIS-A etabliert, das „Automatisierte Fingerabdruckidentifizierungssystem für die Daten der Asylbewerberinnen" , in den der damals schon 1,4 Millionen Abdrücke umfassende Altbestand überführt wurde. [10]

Zwar heißt es im deutschen Paßgesetz: „Eine bundesweite Datenbank der biometrischen

Daten nach Satz 1 wird nicht errichtet." (§ 4) Das gilt jedoch nur für Reisepaß, Dienstpaß und Diplomatenpaß, nicht jedoch für zentrale biometrische Datenbanken der Polizei oder Asylbehörden.

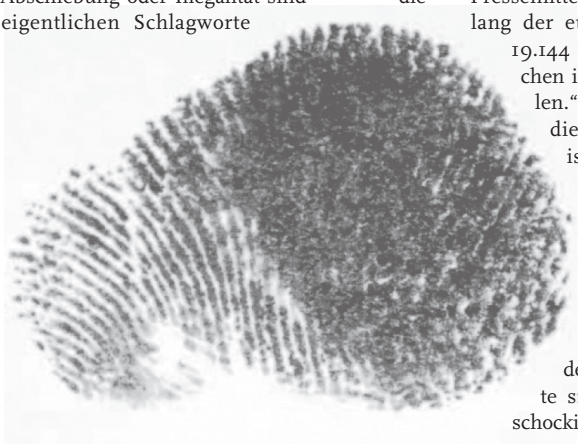
Auch die umfassende Erfassung von „Ausländerinnen" in diversen weiteren Datenbanken wird seit Jahren in Deutschland praktiziert. [11] Am prominentesten ist das Ausländerzentralregister, das insgesamt 23,9 Millionen Datensätze aller (!) „Ausländerinnen" enthält, die ein Visum beantragen oder erhalten – beziehungsweise der Asylbewerberinnen. Die zentrale Kartei gibt es seit 1953 und hat ihr Vorbild in der 1938 durch die Ausländerpolizeiverordnung eingeführten Ausländerzentralkartei.

Längst findet auch Datenaustausch über Behördengrenzen hinweg statt: Sozialamt, Arbeitsagentur und Ausländerbehörde informieren sich untereinander, oft ohne Wissen der Betroffenen. Wenn ein Antrag auf Sozialleistungen gestellt wird, benachrichtigt beispielsweise das Sozialamt die Ausländerbehörde oder die Polizei oder beide. Auch das ist Teil einer neuen Datenpolitik, die schleichend Einzug hielt.

Erfassung, medizinische Untersuchung, Anhörung, Internierung in oft abgelegenen „Lagern" oder in den Transitbereichen der Flughäfen, Abschiebung oder Illegalität sind die eigentlichen Schlagworte gegenwärtiger Migrationspolitik. Die Abschiebungen selbst verlaufen nicht selten gewaltsam. Zu großen öffentlichen Protesten führte der Erstickungstod von Aamir Agheeb 1999, der durch die gewaltsame Abschiebung und die Methoden der BGS-Beamten herbeigeführt wurde. In jenen Tagen wurde bekannt, daß es bereits Dutzende Todesfälle europaweit durch die Art der Fesselung, Knebelung und medikamentösen Ruhigstellung von abgeschobenen Flüchtlingen in verschiedenen europäischen Staaten gegeben hatte.

Bis heute wird an gewaltsamen Abschiebungen festgehalten. Die Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen FRONTEX, die seit Oktober 2004 für die Sicherung der EU-Außengrenzen zuständig ist, formuliert das so: „When Member States make the decision to return foreign nationals staying illegally, who have failed to leave voluntarily, Frontex assists those Member States in coordinating their efforts to maximise efficiency and cost effectiveness while also ensuring that respect for fundamental rights and the human dignity of returnees is maintained at every stage." [12]

Der italienische Journalist Gabriele del Grande dokumentierte die auffindbaren Presseberichte zu europäischen Grenztoten des Mittelmeers zwischen 1988 und 2010: „Folgenden Pressemitteilungen nach starben seit 1988 entlang der europäischen Grenzen mindestens 19.144 Immigranten, davon sind 8.822 Leichen immer noch im Mittelmeer verschollen." [13] Ein tragischer Bodycount, der die Menschenrechtsrhetorik europäischer Politikerinnen zu entlarven sucht. Seitdem sind Tausende hinzugekommen. [14] Als die Bilder der 366 Särge in einem Flugzeughangar auf Lampedusa mit den Leichen der am 3. Oktober 2013 mit ihrem Flüchtlingsboot verunglückten Männer, Frauen und Kinder durch die Weltpresse gingen, zeigte sich die europäische Öffentlichkeit schockiert. Doch hernach hat sich nicht viel geändert. [15]



Echt [redacted] – *Auf dem neuen Personalausweis können die Fingerabdrücke gespeichert werden. Das geschieht freiwillig, so freiwillig, wie* [redacted] *gestern seinen Daumenabdruck für unser Bild zur Verfügung gestellt hat.* Foto Matthias Lüdecke

Bilderrätsel Fingerabdruck. Um welche prominente Person der Zeitgeschichte handelt es sich?

Das Asyl- und Ausländerrecht sowohl auf europäischer als auch auf nationaler Ebene pervertieren im Grunde jeglichen Schutzanspruch. Sämtliche Maßnahmen führen nur dazu, daß die verfolgten Migrantinnen und Overstayer in leicht ausbeutbare Lebenssituationen und in immer gefährlichere Überfahrten und Fluchtmanöver getrieben werden; wirklich verhindern werden sie Migration nie. Ganz sicher aber werden immer mehr Menschen beim Versuch, nach Europa zu kommen, sterben.

Die sich rasant weiterentwickelnden Smart Borders der EU – EUROSUR, VIS, SIS II, Eurodac, die Agentur für das Betriebsmanagement von IT-Großsystemen –, die ausführlich kritisiert worden sind, [16] fixieren die migrationspolitischen Kontrollsysteme auf technologischer Ebene – milliardensubventioniert.

Wer nun glaubt, das alles ginge ihn nichts an, der liegt nicht nur moralisch daneben, sondern auch ganz praktisch. Denn das Sammeln der Fingerabdrücke der Asylsuchenden war nur das Versuchslabor für weitere Millionen Datensätze, die bereits an den Grenzen gesammelt werden. Am bekanntesten ist das US-VISIT-Programm an über zweihundert Flughäfen, Grenzübergängen und Häfen der USA, in dem seit dem Jahr 2007 mehrere hundert Millionen Menschen erfaßt wurden.

Die erkennungsdienstliche Behandlung, die Vermessung der Körper, war in demokratischen Ländern bis vor wenigen Jahren ausschließlich für Verdächtige bei Straftaten vorgesehen. Jetzt wird die Prozedur von den Asylsuchenden über die Reisenden nach und nach für die gesamte Bevölkerung möglich – zunehmend kontaktlos über Kontrollautomaten, die auch gleich die laufenden Fahndungen prüfen.

Während es über die Aufnahme biometrischer Daten in bundesdeutsche Ausweise und Reisepässe wenigstens noch eine Diskussion gab, ist die Erfassung zweier Fingerabdrücke und eines digitalen Fotos in der elektronischen Aufenthaltskarte für Ausländer öffentlich kaum wahrgenommen worden. Der Beschluß zur Vermessung von etwa 4,3 Millionen Betroffenen aus dem Nicht-EU-Ausland, die in Deutschland leben, blieb auch in weiten Teilen der Medien unkommentiert. Auch die verquere Argumentation des Bundesinnenministeriums, daß die Aufnahme biometrischer Merkmale in die Aufenthaltskarte ein Mittel gegen illegale Einwanderung und illegale Aufenthalte sei, blieb unwidersprochen.

Und blickt man auf die Frage „Cui bono?“, fällt die verdeckte Subventionierung der Biometrie-Industrie, aber auch der ganzen umtriebigen „Sicherheits“-Branche unmittelbar ins Auge. Die nutzt nicht nur die gigantischen staatlichen Biometrieprojekte weltweit zur Umsatzmaximierung, sondern auch die Forschungsgelder, die international zuhauf verteilt werden, obgleich Nutzen, Überwindungssicherheit und vor allem Zuverlässigkeit der Biometrie in Frage stehen. Nebenbei doktert sie an Bezahl- und Zutrittssystemen mit Fingerabdruck für den Bereich jenseits staatlichen Zwangs.

Die durch die Maschine bewiesene vermeintliche Identität eines Menschen soll dabei in jeder Lebenslage sicherstellen, daß keine Unberechtigte sich ihr nicht zustehende Ressourcen aneignet. Pseudohuman aber ist es, Ressourcen anzubieten und sie dann mit allerlei Technokratie an stigmatisierende und demütigende Verfahren zu binden, die den Mißbrauch selbiger von vornherein unterstellen. Pseudotransparent ist es, aufgrund sogenannter Sicherheitsinteressen immer nur die Hälfte darüber zu sagen, was genau bei diesen Verfahren eigentlich geschieht. Also, alles nur Fake?

Daß ein Paß, ein lebenslänglich und universell vorhandenes Körperteil oder die DNA, die Pseudoidentität einer Person, oder vielmehr den edelsten Teil des Menschen in anonymen, sozial vermachteten, mißtrauensdurchtränkten Gesellschaften ausmachen, wußte ja bekanntlich schon Brecht.

Quellen (abgerufen am 27. Oktober 2014)

[1] *http://www.proasyl.de/de/themen/basics/basiswissen/rechte-der-fluechtlinge/bewegungsfreiheit/residenzpflicht/*

[2] Welcome to Europe (W2EU): Dublin muss brennen! ... der Fingerabdruck in Italien ist ein verstecktes Gefängnis für uns. Gruppeninterview mit eritreischen Flüchtlingen. *http://dublin2.info/2011/10/dublin-muss-brennen-interview-mit-eritreischen-fluchtlingen/dublin-muss- brennen/*

[3] Der Europäische Datenschutzbeauftragte: Eurodac. *http://www.edps.europa.eu/EDPSWEB/edps/lang/de/Supervision/Eurodac*

[4] Eurodac Supervision Coordination Group: Report of the first coordinated inspection. Brüssel, 17. Juli 2007. *http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/07-07-17_Eurodac_report_EN.pdf*

[5] Europäische Kommission: Tätigkeitsbericht 2009 der EURODAC-Zentraleinheit zur Vorlage beim Europäischen Parlament und beim Rat. Brüssel, 2. August 2010. *http://ec.europa.eu/commission_2010-2014/malmstrom/archive/1_DE_ACT_part1_v1.pdf*

[6] European Data Protection Supervisor: Inspection report on the first phase of the EURODAC central unit. Brüssel, 20. März 2006. *http://register.consilium.europa.eu/pdf/en/06/ st07/st07514.en06.pdf*

[7] European Data Protection Supervisor: Summary report on the EURODAC Audit. Brüssel, 9. November 2007. *http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/07-11-09_Eurodac_audit_summary_EN.pdf*

[8] Eurodac Supervision Coordination Group: Second Inspection Report. Brüssel, 24. Juni 2009. *http://www.edps.europa.eu/EDPSWEB/ webdav/site/mySite/shared/Documents/Supervision/ Eurodac/09-06-24_Eurodac_report2_EN.pdf*

[9] Stellungnahme des Europäischen Datenschutzbeauftragten zum geänderten Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „Eurodac". Amtsblatt Nr. C 101 vom 1. April 2011. *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?ur i=OJ:C:2011:101:0014:01:DE:HTML*

[10] Hessischer Datenschutzbeauftragter Professor Dr. Winfried Hassemer: 21. Tätigkeitsbericht 1992. *http://www.datenschutz.hessen.de/_old_ content/tb21/k3p2.htm*

[11] Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. Drucksache 17/8887, 6. März 2012. *http://dip.bundestag.de/btd/17/088/1708887.pdf*

[12] Frontex: Mission and Tasks. 2012. *http://www.frontex.europa.eu/about/mission-and-tasks*

[13] Gabriel del Grande: Fortress Europe. Blog. *http://fortresseurope.blogspot.de/*

[14] Popp, Maximilian: Europas tödliche Grenzen. 10. September 2014. *http://www.spiegel.de/politik/ausland/fluechtlinge-europas-toedliche-grenzen-multimedia-reportage-a-989815.html*

[15] Jan-Christoph Kitzler: Ein Jahr nach Lampedusa. „Tod, Schmerz, Verzweiflung". ARD Rom, 3. Oktober 2014. *http://www.tagesschau.de/ausland/jahrestag-lampedusa-101.html*

[16] Hayes, Ben/ Vermeulen, Mathias: Borderline. EU Border Surveillance Initiatives – An Assessment of the Costs and Its Impact on Fundamental Rights. Heinrich-Böll-Stiftung: Berlin, Mai 2012. *http://www.boell.de/downloads/DRV_120523_BORDERLINE_-_Border_Surveillance.pdf*

Nationale Mobilmachung

von Uta Wagenmann

Daten und Bioproben von 200.000 Menschen sollen bundesweit in der sogenannten „nationalen Kohorte“ gesammelt werden. Eine Sammlung in dieser Form und Größe wirft nicht nur Fragen nach ihrem medizinischen Sinn oder zum Datenschutz auf, sondern auch zu ihrer biopolitischen Bedeutung.

Wie staatliche und medizinische Institutionen zusammenspielen, zeigt sich in Leipzig, wo ein auf 30.000 Menschen ausgerichtetes Projekt angelaufen ist. Während die britische „UK Biobank“ jahrelang Auseinandersetzungen in der Öffentlichkeit provozierte, ging hierzulande ein ähnliches Großprojekt trotz 200.000 zu erfassenden Menschen beinahe lautlos an den Start. Um Repräsentativität herzustellen, werden in dreizehn Bundesländern nach dem Zufallsprinzip aus dem Datenbestand der Meldeämter Adressen gezogen. [1]

Die ausgewählten Menschen bekommen einen Brief von einem der achtzehn Studienzentren der „nationalen Kohorte“, mit dem sie zur freiwilligen Teilnahme an dem Großprojekt gebeten werden. Nach Aufklärung und Zustimmung sollen sie Blutproben abgeben, sich verschiedenen Untersuchungen unterziehen und Fragen zur Ernährung, zum Lebenswandel, zu eigenen Erkrankungen, zu Krankheiten in der Familie und zu ihrem sozialen Hintergrund beantworten.

Für die folgenden Jahrzehnte sind Nachuntersuchungen geplant. Die Proben und Daten derjenigen untersuchten Menschen, die im Laufe der Zeit krank werden, sollen dann Aufschluß über Krankheitsursachen geben. Denn das Großprojekt startet – wie auch die „UK Biobank“ – vorgeblich, um „Ursachen weit verbreiteter Erkrankungen aufzuklären“ und „Risikofaktoren zu identifizieren“. Explizit genannt werden auf der Webseite der „nationalen Kohorte“ Herz-Kreislauf-, Demenzerkrankungen, Krebs, Diabetes und Infektionskrankheiten. [2]

Reduktionistische Praxis

Der Ansatz, die Entstehung komplexer Erkrankungen durch statistische Korrelationen mit biologischen und sozialen Daten erklären zu wollen, wurde in der Diskussion um die „UK Biobank“ vehement kritisiert. Allein aus zeitlichen Gründen muß sich die Erhebung bei einem so breiten Spektrum an Erkrankungen, wie es die „nationale Kohorte“ abdecken will, auf leicht quantifizierbare Informationen beschränken: Für die bisher vorgesehenen Messungen und Befragungen sind insgesamt drei Stunden veranschlagt – und das, obwohl ausnahmslos Routineuntersuchungen etwa des Blutdrucks oder des Körpergewichtes geplant sind und standardisierte Fragebögen verwendet werden. [3]

Besonders eindringlich demonstriert das Beispiel der „Umweltfaktoren“ die reduzierte Perspektive des Ansatzes: Gefragt wird nach der Häufigkeit von Röntgenuntersuchungen und nach den Adressen von Arbeitsplatz und Wohnort, so daß ein Abgleich mit verfügbaren Umweltdaten möglich ist. Aus diesen beiden Angaben wird schwerlich auf Beziehungen zwischen einzelnen Umwelteinflüssen und der Entstehung bestimmter, komplexer Erkrankungen zu schließen sein.

Realistischer als die in Aussicht gestellte Erklärung von Krankheitsursachen klingt da schon das Ziel des Projektes: Entwickelt werden sollen „Modelle zur Risikoabschätzung, um Personen mit erhöhtem Risiko für chronische Erkrankungen zu identifizieren“. Insbesondere wolle man Marker aller Art „für die Früherkennung von Krankheiten und subklinischen Phänotypen“ bewerten. [4] Mit anderen Worten: Blutpro-

ben spielen eine zentrale Rolle in der „nationalen Kohorte“.

Präventiver Wahn

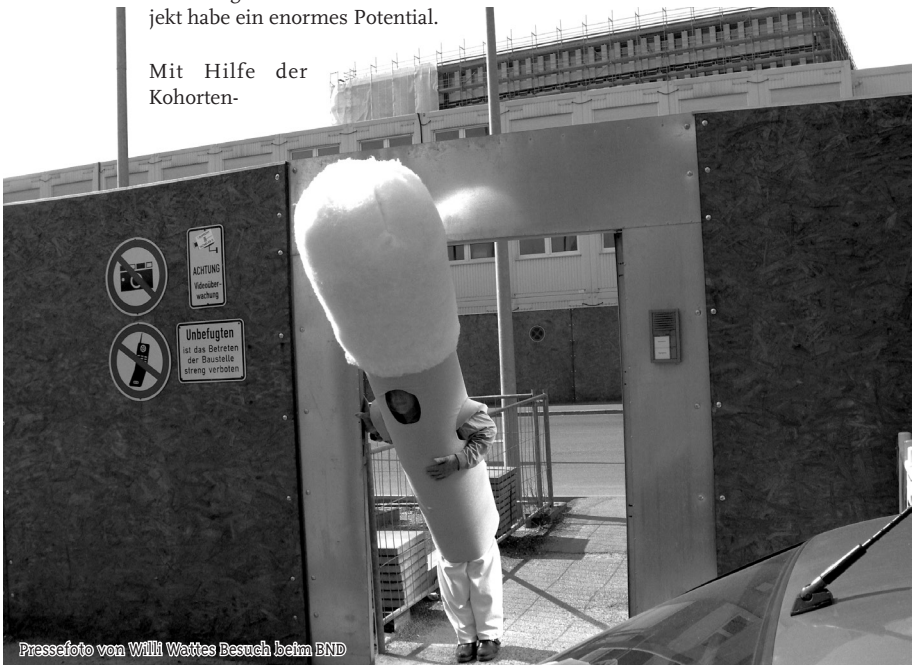
Die von der Helmholtz-Gemeinschaft mit zwanzig Millionen Euro finanzierte Vorbereitungsphase des Großprojektes hatte bereits vor Jahren begonnen. [5] Nun erhält das Projekt vom Bundesforschungsministerium (BMBF) eine Grundfinanzierung in Höhe von zweihundert Millionen Euro, und zwar verteilt auf zehn Jahre.

Der lange Förderzeitraum ist ohne Beispiel in der Forschungspolitik: In den vergangenen Jahrzehnten wurden Projekte zum Aufbau von Proben- und Datensammlungen gewöhnlich zwei bis vier Jahre gefördert. Möglicherweise zielt das BMBF bei der Finanzierung von Aufbau und Betrieb der „nationalen Kohorte“ nur in zweiter Linie auf die wirtschaftlich orientierte „Stärkung“ des „Standortes Deutschland“. „Alle sind sich einig, daß wir eine Nationale Kohorte brauchen“, sagt Andrea Lindner vom Referat Gesundheitsforschung im BMBF. Das Projekt habe ein enormes Potential.

Mit Hilfe der Kohorten-Daten sollen Fragen zur Entstehung einzelner Erkrankungen ebenso bearbeitet werden wie epidemiologische Problemstellungen und Wechselwirkungen zwischen Erbanlagen und Umwelteinflüssen oder Beziehungen zwischen Lebensalter und Krankheitsausbruch. Langfristig sei hier viel zu erwarten für eine effektive Prävention von Krankheiten. „Und wenn die Menschen gesund bleiben, hat das ja auch den angenehmen Nebeneffekt, daß das Gesundheitssystem entlastet wird“, so Lindner. „Die Nationale Kohorte ist wirklich vielseitig nutzbar. Das ist, wenn Sie so wollen, eine Art eierlegende Wollmilchsau.“

Ein Kuchen für viele

Welcher Wert der „nationalen Kohorte“ beigemessen wird, verdeutlichen die Eigentumsbestimmungen in dem fast 350 Seiten umfassenden wissenschaftlichen Konzept des Projektes. [6] Dort heißt es unmißverständlich, daß der eingetragene Trägerverein „der juristische Eigentümer aller von den Teilnehmern zur Verfügung



Pressefoto von Willi Wattes Besuch beim BND

gestellten Daten und biologischen Proben ist". Der Zugang zu der mit öffentlichen Mitteln finanzierten Sammlung soll grundsätzlich zwar für alle Forschungsprojekte gewährleistet werden, allerdings will man Gebühren zur Deckung der Kosten erheben. Von „Organisationen, die finanzielle Vorteile aus der Nutzung der Daten erwarten", können zudem höhere Gebühren verlangt werden. [7]

Auch die Liste der beteiligten „Cluster" zeugt davon, daß viele ein Stück vom Kuchen wollen: Neben diversen Helmholtz-Zentren, verschiedenen Abteilungen des Deutschen Krebsforschungszentrums, dem Berliner Max-Delbrück-Centrum für Molekulare Medizin und dem Robert-Koch-Institut sind mehrere medizinische Fakultäten großer Universitäten an Aufbau und Betrieb der regionalen Studienzentren beteiligt. Es sollen an diesen Studienzentren „Machbarkeitsstudien zur Testung verschiedener innovativer Erhebungsinstrumente" stattfinden. [8]

LIFE in Leipzig

Beteiligt ist auch die medizinische Fakultät der Universität Leipzig, wo ein Studienzentrum mit der Erfassung begonnen hat – allerdings zunächst für ein anderes Großprojekt: die aus Mitteln der Europäischen Regionalförderung und des Freistaates Sachsen finanzierte „Gesundheitsstudie LIFE". [9] Geplant ist hier, neben 10.000 bereits Erkrankten jeweils 10.000 gesunde Erwachsene und 10.000 gesunde Kinder für die Teilnahme zu gewinnen, die über einen Zeitraum von zunächst zehn Jahren regelmäßig zu Untersuchungen und Befragungen erscheinen und Urin- und Blutproben abgeben sollen. Auch 2.000 Schwangere werden gesucht, um bereits pränatal mit den Messungen beginnen zu können.

Hier werden ganz neue Methoden der Probandengewinnung erprobt. So erfreut sich das Teilprojekt „LIFE Child" der Unterstützung durch die Schulverwaltung: Zu Beginn des laufenden Schuljahres wurden staatliche Schulen in Leipzig ausführlich über das Projekt informiert, auch Elternabende fanden statt, 50.000 Flyer wurden verteilt. Ganze Klassenverbände bekommen schulfrei, um im Rahmen eines Projekttages den Untersuchungsparcours im Leipziger Studienzentrum zu durchlaufen.

Auch die sogenannte „Rekrutierung" der rund 10.000 gesunden Erwachsenen, die bei LIFE mitwirken sollen, scheint zu funktionieren. Sie werden aus dem Adreßbestand der Meldeämter per Zufallsziehung ausgewählt – ganz so wie bei der „nationalen Kohorte". Seit dem Start der Ziehungen hätten sich 35 bis 40 Prozent der Angeschriebenen zur Teilnahme gemeldet, berichtet Professor Markus Löffler, Vorstand bei LIFE und zugleich Mitglied des epidemiologischen Planungskomitees der „nationalen Kohorte". „Ein Drittel antwortet, sie wollen nicht mitmachen, und ein Drittel antwortet gar nicht, die schreiben wir ein zweites Mal an."

Die Erfahrungen bei der Probandengewinnung für LIFE sind für den Aufbau des nationalen Großprojektes sicherlich verwertbar. In jedem Fall steht die Leipziger Infrastruktur dafür zur Verfügung. „Wir werden unsere Studienambulanz einige Jahre lang für die Nationale Kohorte nutzen", kündigt Löffler an. „Dann kommen unsere LIFE-Nachuntersuchungen, und dann die Nachuntersuchungen für die Kohorte, so daß das hintereinander ineinander geschachtelt ist."

Daß auch menschliche LIFE-Datengeber in das bundesweite Großprojekt eingeschlossen werden, ist aber eher unwahrscheinlich. „Die Kohorten überlappen nicht hundert Prozent, zum Beispiel hat LIFE keine Leute zwischen 20 und 40 Jahren, und die Nationale Kohorte hat keine zwischen 70 und 80", erklärt Löffler. „Außerdem gehen eine Reihe unserer Untersuchungen über das Programm der Nationalen Kohorte hinaus. Da, wo ein Abgleich herstellbar ist, machen wir den aber."

In einem Punkt allerdings geht die „nationale Kohorte" deutlich weiter als LIFE: Geplant ist für die 200.000 Menschen umfassende Sammlung, zusätzlich zu Untersuchungsergebnissen und biologischen Proben auch Daten der Sozialversicherungen und der Krankenkassen einzubeziehen. Im wissenschaftlichen Konzept des Großprojektes heißt es, für solche sogenann-

ten sekundären Daten solle ein „Kompetenzzentrum“ eingerichtet werden, weil sie „nach besonderen Datenschutzbestimmungen verlangen“. [7]

In der Tat sind diese Informationen besonders sensibel. Verknüpft mit Bioproben, daraus gewonnenen genetischen Informationen und Angaben zu Krankheiten und Lebensgewohnheiten lassen sich Versichertendaten vielseitig nutzen – heute für Kalkulationen von Gesundheitsökonomen oder für Marktanalysen von Pharmaunternehmen, morgen dann vielleicht für Präventions- und Kontrollsysteme anderer Art.

Links

[1] Die Kriterien, denen eine für die deutsche Wohnbevölkerung repräsentative Stichprobe genügen muß, lassen sich nur schwer bestimmen. Es bestehen jedenfalls erhebliche Zweifel, daß das Zufallsprinzip diese Repräsentativität herzustellen vermag. Vgl. Fußnote 5.

[2] *http://www.nationale-kohorte.de/index.html*

[3] Zu den Fragen und Untersuchungen vgl. die Tabellen und Erläuterungen im wissenschaftlichen Konzept der „nationalen Kohorte“ (Fußnote 7), S. 68 ff., 74 ff. und 86 ff.

[4] Vgl. *http://www.nationale-kohorte.de/content/ziele.pdf* Der Begriff der „subklinischen Phänotypen“ meint Menschen, die nicht krank sind, aber es möglicherweise einmal werden. Er zeugt von dem Krankheitsmodell, das der Konzeption der „nationalen Kohorte“ zugrundeliegt und von genetisch vorprogrammierten Potentialen ausgeht, die dann im „Wechselspiel“ mit Umwelteinflüssen, Ernährung und Lebensstil aktiviert werden.

[5] GID Nr. 191, Dezember 2008, S. 45 - 47.

[6] Die wissenschaftliche Konzeption der „nationalen Kohorte“ liegt nur in englischer Sprache vor. Sie wurde zum Teil eng mit dem grenzüberschreitenden Großprojekt „Biobanking and Biomolecular Resources Research Infrastructure“ (BBMRI) abgestimmt und ist auf eine europäische Einbindung ausgerichtet. Der Aufbau des BBMRI wurde von 2008 bis 2011 durch die EU-Kommission gefördert und soll der Standardisierung und Vernetzung europäischer Biobanken dienen. Der europäischen Forschungsinfrastruktur gehörten im September 2011 225 Einrichtungen an, darunter die „UK Biobank“ oder die deutsche Sammlung „Popgen“ (Universität Kiel). Auch die „nationale Kohorte“ wird sich hier angliedern.

[7] The national cohort. A prospective epidemiologic study resource for health and disease research in Germany, Februar 2011, S. 199ff. Download unter *http://www.nationale-kohorte.de/wissenschaftliches-konzept.html*

[8] Das neue Buch von Uta Wagenmann und Susanne Schultz: Identität auf Vorrat. Zur Kritik der DNA-Sammelwut. *ISBN: 978-3-68241-439-0*

gefunden von @larafritzsche

Biometrie in polizeilichen Anwendungen

Tiberius <tiberius@cccmz.de>

Biometrie ist die Wissenschaft der Metriken von lebenden Organismen. Soweit die grobe Lexikondefinition des Begriffes. Basierend auf dieser Definition fällt es nicht schwer, sich vorzustellen, daß die Biometrie ihren Ursprung in der Systematik der Arten in der Biologie hat. Bereits Jahrhunderte vor Erscheinen eines gewissen Fingerabdrucks eines gewissen Innenministers in einem gewissen Hackerblättchen benutzten Biologen, die sich selbst noch nicht als solche bezeichneten, Biometrie, um Tier- und Pflanzenarten voneinander unterscheiden zu können.

Die Tatsache, daß verwandte Arten auch Ähnlichkeiten in ihren durchschnittlichen biometrischen Eigenschaften aufweisen, begründete die Systematik der Arten und half auch Charles Darwin auf die Sprünge bei der Formulierung seiner Evolutionstheorie. Den Begriff „Biometrie" an sich verwendete erstmals der Naturwissenschaftler und Statistiker Christoph Bernoulli in einer Veröffentlichung „Handbuch der Populationistik", in der er im Jahre 1841 eine statistische Analyse biometrischer Merkmale der (europäischen!) Bevölkerung präsentierte. So gesehen betrachtete die klassische Biometrie nicht die Metriken eines Individuums, sondern mittelte die gewonnenen Erkenntnisse, um eine Aussage über eine komplette Art treffen zu können. Heutzutage nennen wir dieses Gebiet die biometrische Statistik.

Dieser Tage versteht die breite Öffentlichkeit unter Biometrie nur noch die Biometrie des Menschen, die mit modernen Mitteln zur Identifikation von Individuen genutzt wird. Egal, ob beim Abnehmen der Fingerabdrücke eines gefaßten Straftäters oder der Gesichtserkennung zur Freischaltung eines Smartphones, es werden biometrische Merkmale von Individuen in rasender Geschwindigkeit extrahiert, mit Datensätzen bereits bekannter Individuen abgeglichen und größtenteils automatisiert Entscheidungen gefällt, ob der Mensch einer bestimmten vorher definierten Gruppe, also beispielsweise Straftäter oder Smartphone-Nutzer, angehört oder nicht. Korrekterweise müßte man hier von biometrischer Erkennung sprechen.

Wie kam es also zu dieser veränderten Bedeutung des Begriffes der Biometrie? Als treibende Kraft darf sicher der Bereich der Verfolgung von Straftätern angesehen werden. Bereits früh in unserer Geschichte war den Verfechtern unserer öffentlichen Ordnung klar, daß es nicht ausreicht, Täter in flagranti zu erwischen; daß es vielmehr nötig ist, sie auch nach der Tat ermitteln und verfolgen zu können. Die Anonymität einer Gesellschaft kam den Tätern zu Gute und ermöglichte ihnen, weitgehend unbehelligt mit ihren Taten davonzukommen.

Wanted! Dead or Alive

Zeit also für den Auftritt der Biometrie. Die erste Anwendung biometrischer Fahndungsmethoden darf in der Entwicklung der Phantombilder angesiedelt werden. Mit der Erfindung des Buchdrucks war es erstmals möglich, Fahndungsplakate massenweise zu verteilen. Daraufhin entwickelte sich der Berufsstand des Polizeizeichners. Auf Basis von Zeugenaussagen wurden von speziell geschulten Zeichnern Bilder eines Verdächtigen erstellt und in der Bevölkerung verteilt. Die anfänglich kruden Zeichnungen wurden auf

Basis der Erkenntnisse der statistischen Biometrie und der physischen Anthropologie zunächst zu standardisierten „Identkits“ erweitert, bei denen fest definierte Sätze von Gesichtsteilen auf Folien ein puzzleartiges Zusammensetzen des Phantombildes ermöglichten. Der menschliche Faktor in Form des Zeichners wurde also in dem Verfahren dezimiert.

Richtig los ging die biometrischen Erkennung jedoch mit der Erfindung der Photographie. Erstmals war es möglich, eine Datenbank bekannter Straftäter zu führen, gegen die man biometrisch die aus den Zeugenaussagen konstruierten Phantombilder abgleichen konnte. Der Franzose Alphonse Bertillon entwickelte 1880 ein standardisiertes Verfahren, um Straftäter biometrisch zu erfassen, wobei neben der Photographie (Portrait und Profil) auch die genaue Vermessung des Körpers mittels Spezialinstrumenten sowie eine schriftliche Beschreibung spezieller Merkmale enthalten waren. Mittels der sogenannten „Signalethischen Registratur“ wurden diese ersten erkennungsdienstlichen Datensätze systematisch verwaltet und waren somit erstmals auch ebenso systematisch durchsuchbar.

Wirbel, Bögen, Schleifen, Tannen

Gleichzeitig setzte sich die biologische Erkenntnis der Einzigartigkeit von Fingerabdrücken in der Polizeitechnik durch. Der britische Kolonialbeamte William James Herschel war bereits 1860 in Indien auf die Idee gekommen, mittels Fingerabdrücken die Empfänger von Pensionen der britischen Kolonialarmee zu unterscheiden und somit den Betrug zu minimieren. Erst Ende des neunzehnten Jahrhunderts allerdings wurde dieses Verfahren durch Francis Galton, einen Cousin von Charles Darwin, in wissenschaftliche Formen gegossen und als „Daktyloskopie“ (griechisch „Fingerschau“) bezeichnet. Der Mathematiker Galton entwickelte ein System zur standardisierten Beschreibung und Klassifizierung von Fingerabdrücken und berechnete erstmals die Wahrscheinlichkeit der Übereinstimmung zweier Fingerabdrücke abhängig von der Anzahl der übereinstimmenden Merkmale. Anfang des zwanzigsten Jahrhunderts setzte sich dieses System zuerst in Argentinien, dann in Großbritannien und schließlich in ganz Europa gegen die erst kurz vorher eingeführte „Bertillionage“ durch.

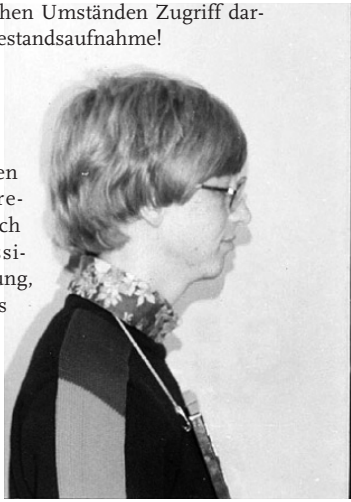
Let's do the Timewarp

Sowohl die Identifizierung mittels Gesichtsbildern als auch die Daktyloskopie haben den Übergang ins Informationszeitalter blendend bestanden. Zunächst die Daktyloskopie, dann die Gesichtserkennung etablierten sich auf den Rechenanlagen der großen Polizeien und anderer Behörden dieser Welt. Der technologische Nachzügler DNA steht in den Startlöchern zur Massenanwendung; andere Verfahren zur biometrischen Identifizierung werden erforscht.

Je nach Einsatzzweck und Behörde erreichen die Datenbanken heute Größen im zweistelligen Millionenbereich an Datensätzen. Identifizierungen, die bisher trotz Computerunterstützung letztlich von einem menschlichen Experten festgestellt wurden, werden aufgrund der Masse der Recherchen zunehmend durch vollautomatisierte Verfahren abgelöst. Biometrische Erkennung sickert in mobile Geräte ein und hat somit die Wände der Polizeistationen erfolgreich verlassen. Der Datenschutz hat Einzug gehalten, gleichzeitig nimmt die internationale Vernetzung zu und somit wird das System unübersichtlich. Welche biometrischen Daten werden wo gespeichert? Wer hat unter welchen Umständen Zugriff darauf? Zeit für eine Bestandsaufnahme!

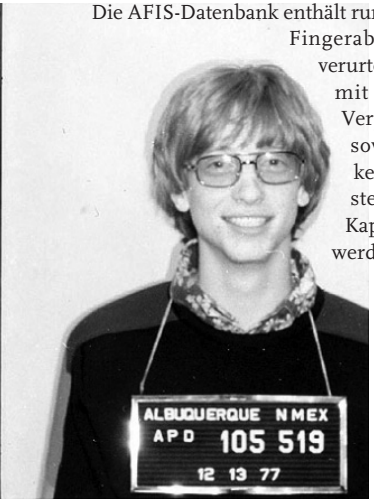
Vom BKA gefingert...

Von „der deutschen Polizei“ zu sprechen, ist eigentlich eine nicht zulässige Verallgemeinerung, schließlich gibt es in Deutschland einen unübersichtlichen Wust an Behörden, die mehr oder weniger mit Polizeigewalten ausge-



stattet sind. Jedes Bundesland hat sein eigenes Polizeigesetz und seine eigene Struktur von Polizeibehörden. Föderalismus, yay! In der vereinfachten Betrachtung besteht zumindest die deutsche Kriminalpolizei aus den Landeskriminalämtern, dem Bundeskriminalamt, der Bundespolizei und der Polizei des deutschen Bundestages. (Entgegen landläufiger Meinung zählt das Zollkriminalamt nicht zu den Polizeibehörden.) Vor allem bei LKÄ und BKA wird Biometrie in größerem Maße betrieben. Das BKA tritt hier als Dienstleister für Biometrie auf, indem es zumeist kommerziell erhältliche Systeme in die IT-Landschaft der deutschen Polizei eingliedert und für die Länderpolizeien bereitstellt.

Den verläßlichen Grundstamm biometrischer Anwendungen bildet die Daktyloskopie. Die Verarbeitung von Fingerabdrücken ist heutzutage in AFIS (Automated Fingerprint Identification System) weitgehend automatisiert. Die Codierungs- und Erkennungsalgorithmen sind soweit fortgeschritten, daß sie sogar oft die Fähigkeiten menschlicher Experten übertreffen. Anders als in vielen anderen Ländern (vor allem in den USA) existiert in Deutschland nur ein einziges polizeiliches AFIS. Es wird betrieben vom BKA in Wiesbaden und ist für die deutsche Polizei im eigenen Corporate Network als Service erreichbar.



Die AFIS-Datenbank enthält rund drei Millionen Fingerabdrucksätze von verurteilten Straftätern mit Wahrung der Verjährungsfristen sowie die Abdrücke von Asylantragstellern. Täter von Kapitalverbrechen werden bis zu ihrem Lebensende in AFIS gespeichert. Anders als viele andere AFIS dieser Welt wird im deutschen AFIS pro identifizierter Person nur ein Satz Abdrücke gespeichert. Es handelt sich um das sogenannte „Master-Set“, das aus den qualitativ besten Einzelabdrücken aller jemals durchgeführten Erfassungen einer Person zusammengesetzt ist. In anderen Ländern werden einfach alle jemals genommenen Abdrücke gespeichert, so daß nominal viel größere Datenbanken entstehen. Neben den Fingerabdrücken werden zu jedem Datensatz im deutschen AFIS das Geschlecht, das Geburtsjahr und eine Referenznummer gespeichert. Die alphanumerischen Daten einer Person werden im Polizeiverbundsystem INPOL gespeichert; AFIS als Subsystem von INPOL enthält selber keine Alphanumerik. Neben der Vermeidung von Datenredundanz ist ein anderer Grund, daß die Daktyloskopen bei ihren Entscheidungen möglichst nur die eigentlichen Fingerabdruckdaten kennen, damit andere Informationen keine Rolle spielen.

Das AFIS des BKA erfüllt im Wesentlichen folgende Aufgaben:

Das Verarbeiten von Fingerabdruckblättern für den Erkennungsdienst

Werden Verdächtige festgenommen, werden sie einer erkennungsdienstlichen Erfassung unterzogen, in deren Rahmen Fingerabdrücke abgenommen und ein Lichtbildsatz erstellt wird. „Kunde“ des BKA sind hier die einzelnen Länderpolizeien sowie die BPol, die ihre mittlerweile fast hundertprozentig digitalisierten Fingerabdruckblätter entweder per E-Mail oder über das Polizeiverbundsystem INPOL zum AFIS schikken. Die Fingerabdruckabnahme per Tinte und Papier ist weitgehend abgeschafft, es kommen optische Fingerabdruckscanner zum Einsatz. Beim Erkennungsdienst wird jedes einzelne Rechercheergebnis aus AFIS von einem ausgebildeten Daktyloskopen verifiziert, so daß die letztliche Identifizierungsentscheidung niemals ein maschineller Vorgang ist.

Daher dauern die Identifizierungen im Standardfall bis zu einer Woche, in dringenden Fällen ist eine Anwortzeit von drei Stunden durch den 24h-Dienst beim BKA garantiert. Eine Ausnahme von der menschlichen Verifizierung bil-

det das FastID-Verfahren, das seit 2005 vom BKA bereitgestellt wird. Hierbei können Mobilgeräte einen verkürzten Datensatz von vier bis sechs Fingern erfassen. Dieser Datensatz wird dann vollständig automatisiert (lights-out) mit „NO-HIT“ beantwortet, wenn kein Treffer vorliegt. Wenn AFIS allerdings einen Treffer vermutet, wird der Absender informiert, daß es womöglich einen Treffer geben könnte, und der Treffer wird, wie beim Standardverfahren auch, den Daktyloskopen des 24h-Dienstes im BKA zur Verifizierung vorgelegt und erst nach deren Beurteilung endgültig beantwortet. Dieser verschlankte Prozeß ermöglicht NO-HIT-Antworten in wenigen Minuten und HIT-Antworten in durchschnittlich zehn Minuten. Das FastID-Verfahren ersetzt allerdings nicht die erkennungsdienstliche Behandlung, da die Abdrücke nach der Verarbeitung sofort wieder gelöscht werden. Tritt ein Treffer auf oder wurde das Subjekt festgenommen, findet eine normale erkennungsdienstliche Behandlung auf der Polizeistation statt. FastID ermöglicht Polizisten auf der Straße einen schnellen Abgleich von Menschen gegen die Straftäterdatenbank, wenn diese sich nicht ausweisen können.

Das Verarbeiten von Fingerabdruckblättern für das Bundesamt zur Anerkennung Flüchtiger

Aufgegriffene Personen ohne Aufenthaltsrecht sowie Asylantragsteller werden in AFIS recherchiert. Das Asylgesetz sieht eine Ablehnung eines Asylantrages vor, wenn der Antragsteller ein Verbrechen in der BRD begangen hat. Daher werden die Abdrücke von Antragstellern gegen AFIS recherchiert um zu ermitteln, ob die antragstellende Person unter anderen Personalien eine Straftat begangen hat. Auch von der Polizei aufgegriffene Personen ohne Aufenthaltsgenehmigung werden erfaßt, bevor sie dem BAMF zur Abschiebung oder Asylantragerstellung überstellt werden. Außerdem bildet das AFIS des BKA die Schnittstelle zum europäischen Asyl-AFIS „Eurodac“. Die Datensätze von Antragstellern werden mit Eurodac abgeglichen, um festzustellen, ob bereits ein Asylantrag in einem anderen Land der EU besteht und somit per Gesetzeslage ein Asylbetrug vorliegt. Ausländer, deren Asylantrag bewilligt und deren Aufenthalt in der BRD ab dann geduldet wird, erhalten finanzielle Unterstützung für ihren Aufenthalt. Dies hat Ende der achtziger bis Anfang der neunziger Jahre nach Polizeiangaben dazu geführt, daß viele Asylberechtigte einen Antrag in gleich mehreren Staaten des Schengenraumes stellten, um Geld von mehreren Seiten zu beziehen. Das daraufhin eingerichtete Eurodac-System hätte diesen Betrug in wenigen Jahren so gut wie ausgeschaltet. Außerdem ist bei bereits bestehendem Asylantrag in einem anderen EU-Land das Land für den Antragsteller zuständig, in dem der erste Antrag abgegeben wurde. Wenn also zum Beispiel eine Person ohne Aufenthaltsgenehmigung in Deutschland aufgegriffen wird, die Eurodac-Recherche ergibt aber ein laufendes Asylverfahren in Frankreich, kann diese Person in Deutschland keinen weiteren Antrag stellen und wird an Frankreich überstellt.

Verarbeitung von Tatortspuren

Von Tatortermittlern erfaßte Fingerabdruckspuren werden in AFIS recherchiert. Die LKÄ unterhalten AFIS-Arbeitsstationen, mit denen sie Tatortspuren erfassen und gegen Straftäter und ungelöste Spuren abgleichen können. Im besten Fall trifft AFIS einen bereits bekannten Straftäter, und der Fall gilt als gelöst. Andernfalls könnte eine ungelöste Spur getroffen werden, so daß die Ermittler den Zusammenhang zweier Fälle herstellen können. Zum Schluß können die Spuren als ungelöste Spuren in AFIS eingestellt werden. Da jedes eintreffende Fingerabdruckblatt (nicht aber die FastIDs) automatisch gegen alle ungelösten Spuren recherchiert wird, kann der Täter eventuell später ermittelt werden, wenn er aus einem möglicherweise ganz anderen Grund einer erkennungsdienstlichen Erfassung unterzogen wird. Die Spurenverarbeitung ist, sowohl was die AFIS-Verarbeitung als auch die Expertise der Daktyloskopen angeht, deutlich anspruchsvoller als die Verarbeitung von Zehn-Fingerabdruck-Blättern, hauptsächlich durch die geringe Qualität von Fingerspuren. Diese Verarbeitungsart wird auch von den (freiwilligen!) Mitgliedern der Identifizierungskommission des BKAs genutzt, die bei Katastrophen in aller Welt

ausrückt, um Todesopfer zu identifizieren, wie 2004 im Falle des Tsunamis in Südost Asien.

Workflow- und Interfacesystem für angebundene Systeme

Diverse Systeme sind extern an das deutsche AFIS angebunden und tauschen auf Basis diverser Abkommen und rechtlicher Grundlagen Daten aus. Dazu gehören aktuell:

Das europäische Asylbewerbersystem Eurodac, für Recherchen des BAMF; Interpol, für die Zusammenarbeit mit den Polizeibehörden anderer Staaten; EU-Staaten, die den Vertrag von Prüm umgesetzt haben; das Workflowsystem des BAMF; das deutsche Polizeiverbundsystem INPOL; das interne Vorgangsbearbeitungssystem des BKA, sowie über den Umweg des Bundesverwaltungsamtes auch das Auswärtige Amt für den Abgleich der Fingerabdruckdaten von Visa-Antragstellern.

Mittelfristig könnten noch das FBI und das DHS in den USA auf Basis des deutsch-amerikanischen Sicherheitsabkommens dazukommen. Die Systemarchitektur wird weitgehend der des Vertrages von Prüm entsprechen, noch befindet sich das Abkommen allerdings in der Abstimmung. Nachdem ein Versuch der USA gescheitert war, über die Organe der EU einen direkten Zugriff in das Prüm-System zu bekommen und somit Fingerabdruck- und DNA-Abfragen in allen EU-Mitgliedsstaaten durchführen zu können, wurden stattdessen eine Reihe von bilateralen Abkommen mit einzelnen Staaten getroffen, Deutschland ist einer davon.

In etwas fernerer Zukunft kommt noch das europäische Visasystem VIS dazu, in dem Visa-Antragsteller abgeglichen werden, um Falschidentitäten bei der Visumserteilung aufdecken zu können.

Bitte NICHT lächeln!

Seit 2005 betreibt das BKA neben dem AFIS auch ein zentralisiertes Gesichtserkennungssystem (GES). Ein öffentlicher Feldversuch am Mainzer Hauptbahnhof hatte die Untauglichkeit von automatisierter Gesichtserkennung an Überwachungskameras gezeigt, jedoch lieferten die in Zusammenarbeit mit dem Fraunhofer-Institut getesteten Systeme eine sehr gute Erkennungsleistung für statische Portraitaufnahmen. Da das BKA ohnehin eine Datenbank mit erkennungsdienstlichen Photos unterhält, wurde beschlossen, ein Gesichtserkennungssystem zentral im BKA als Dienstleistung für die LKÄ einzurichten. Heute enthält die GES-Datenbank etwa 3,4 Mil-

Foto: Torsten Philipp, cc-by-sa

lionen Portraitaufnahmen erkennungsdienstlich behandelter Personen. Anders als bei AFIS findet hier aber keine automatische Recherche statt; ein eingetroffener Datensatz wird zunächst nur gespeichert. Recherchen werden ausschließlich manuell durchgeführt.

Da das GES nur Portraitbilder verarbeiten und nur knapp 15 Grad Abweichung von der Frontalen tolerieren kann, ist es zur Verarbeitung von Überwachungskamerabildern in der Regel nicht zu gebrauchen. Anders als bei AFIS existieren für GES auch keine wissenschaftlich bestimmten Kriterien für einen gesicherten Abgleich von Such- und Vergleichsbild. Wenn die GES-Treffer als gerichtsfestes Beweismittel zum Einsatz kommen müssen, werden sie grundsätzlich von einem Gesichtsexperten wissenschaftlich unterfüttert und in einem formalen Gutachten bestätigt. So gesehen ist GES mehr ein Hilfsmittel für die Gesichtsexperten, um die Anzahl der manuellen Vergleiche zu reduzieren.

Die Nutzer des GES sind primär die Gesichtsexperten des BKA, die Identifizierungsaufträge aus den Bundesländern ausführen. Allerdings existiert auch eine Schnittstelle für die direkte Nutzung durch die LKÄ. Diese können Rechercheaufträge über das Polizeiverbundsystem an das BKA senden und erhalten dann eine Liste mit möglichen Treffern zurück.

Sag Aaahhh....

DNA-Vergleiche sind eine relativ neue Entwicklung der biometrischen Identifizierung. Erst im Laufe des letzten Jahrzehnts wurde die Technik der DNA-Sequenzierung soweit entwickelt, daß der Laborprozeß in nutzbarer Zeit abgeschlossen werden kann. Die größten Nutzer biometrischer Erkennung via DNA-Abgleich sind die Länderpolizeien, die bei Kapitalverbrechen auch mal gerne zu „freiwilligen“ Massenabgleichen aufrufen. Es existiert auch eine zentrale DNA-Datenbank im BKA, die genutzt wird, um gefundene DNA-Profile von unaufgeklärten Verbrechen zu speichern. Da aber im Gegensatz zu Fingerabdrücken und Gesichtsbildern keine Bestandsdatenbank von identifizierten Personen zum Vergleich exisitiert, ist diese Datenbank deutlich kleiner und weniger genutzt.

Ein oft auftretendes Mißverständnis bezüglich der DNA-Recherche ist, daß die vollständig sequenzierte DNA eines Menschen gespeichert wird. Tatsächlich basiert der DNA-Vergleich auf einem Satz von Merkmalen der DNA, der von der genetischen Wissenschaft als repräsentativ für ein Individuum identifiziert wurde, also genetische Informationen, die zwar bei jedem Menschen vorhanden, aber in der Kombination der Merkmale für jedes Individuum statistisch eindeutig sind. Aus der genetischen Sequenz werden sozusagen mit einer Schablone ganz bestimmte, winzig kleine Teile ausgeschnitten, aus denen man keine „semantischen“ Informationen wie Augenfarbe oder Erbkrankheiten ersehen kann. Das führt dazu, daß digital gespeicherte DNA-Profile im Prinzip einen sehr kleinen Datensatz darstellen, der strukturell nicht variiert. Anders als ein Fingerabdruck oder Gesicht, bei deren Digitalisierung die Merkmale abhängig von der Aufnahme mal gefunden werden können und mal nicht, sind die genetischen Merkmale immer vorhanden. Somit ist die Suche eines DNA-Profils in einer Datenbank vorhandener Profile ein sehr simpler Prozeß. Die Suche ist mit normalen Datenbankalgorithmen möglich. Dementsprechend ist das DNA-System des BKA auch kein besonderes, komplexes und zugekauftes System wie AFIS oder GES, sondern eine einfache SQL-Datenbank mit maßgeschneidertem Frontend. Aus informationstechnologischer Sicht ist die DNA-Recherche also stinklangweilig.

Boring! What's next?

Natürlich gibt es noch Dutzende biometrische Verfahren, die sich technologisch weit genug entwickelt haben, um interessant für die Polizei zu werden, zunächst natürlich die Verbesserungen der bereits etablierten Verfahren. Wie alles andere Mediale im Moment auch, bewegt sich die Biometrie in die dritte Dimension. Neue Aufnahmetechniken werden aktiv erforscht, um sowohl Fingerabdruck als auch Gesichtsbild dreidimensional zu erfassen und somit noch mehr Merkmale für den Abgleich zur Verfügung zu haben.

Beim Gesichtsbild ist der Zugewinn offensichtlich: Es können Teile des Kopfes mit einbezogen werden, die bei einer Portraitaufnahme nicht zur Verfügung stehen, etwa die Ohrmuschel.

Außerdem eliminiert ein dreidimensionales Bild als Vergleichsziel auch die bisherige Winkelabhängigkeit der Gesichtserkennung. Wenn man aus dem Bild einer Überwachungskamera mittels Bildverarbeitung den Winkel errechnen kann, in dem der abgebildete Kopf zu sehen ist, so kann man aus dem vorhandenen dreidimensionalen Daten ein Vergleichsbild in genau diesem Winkel rendern und somit wieder die klassische 2D-Gesichtserkennung anwenden.

Beim Fingerabdruck besteht die Möglichkeit, mittels zusätzlicher Lichtspektren oder Ultraschall die tieferen Hautschichten des Fingers abzutasten und somit trotz Störfaktoren an der Oberhaut (wie Narben) eine Erfassung zu ermöglichen. Auch werden solche Techniken zur Echtheitsverifikation des Fingers genutzt werden können, indem man beispielsweise die Merkmale der Unterhaut mit den optisch erfaßten Oberflächenmerkmalen abgleichen und somit erkennen kann, ob sich auf dem Finger zum Beispiel der aufgeklebte Fingerabdruck eines gewissen Ex-Innenministers befindet. Generell ist die Erkennung von Falschfingern eine große Herausforderung der Hersteller von Fingerabdruckscannern. Bisher ist keine sichere Methode bekannt, einen Falschfinger als solchen zu erkennen.

Etwas „abgefahrener“ ist die Entwicklung sogenannter „Fast DNA“-Kits. Ziel dabei ist es, den Laborprozeß für die DNA-Profilbildung in ein Technologiepaket zu gießen und somit den Prozeß von derzeit mehreren Tagen auf wenige Stunden zu verkürzen. Außerdem kann der Prozeß raus aus den Laboren in die Polizeistationen gebracht werden und soll von speziell geschultem Verwaltungspersonal durchgeführt werden können. Das Erstellen eines DNA-Profils soll mit diesen Kits nicht komplizierter sein als die Bedienung und Wartung eines Kopierers.

Nicht alles, was an biometrischer Technologie entwickelt wird, ist aber auch gleichzeitig interessant für die Polizeiarbeit. So hat sich die Iris- oder Netzhauterkennung als sehr gut geeignetes Verfahren zur Identifizierung erwiesen, es findet etwa beim amerikanischen Militär breite Anwendung. Allerdings fällt es schwer, sich dafür ein sinnvolles Szenario für die polizeiliche Identifizierung auszudenken. Die Verfahren bringen einfach gegenüber Fingerabdruck- und Gesichtsbildern keinen Vorteil und werden zumindest in Deutschland nicht polizeilich betrieben oder angewendet. Anders sieht es bei der Sprechererkennung aus: Spracherkennung im Sinne der Erkennung des Sprachinhaltes ist ja nun nichts Neues mehr. Spracherkennung zur Identifikation des Sprechers ist allerdings bisher eine Aufgabe spezialisierter Experten und Algorithmen. In diesem Bereich ist technologisch Entwicklungspotential vorhanden, an dem die Polizei mächtiges Interesse hat.

Who watches the watchmen?

Die Durchdringung der Polizeiarbeit mit biometrischen Verfahren stellt ein zunehmend größeres Problem der Vereinbarkeit mit dem Datenschutz und dem Recht auf informationelle Selbstbestimmung dar. Die Gesellschaft steht vor der Herausforderung, diese Rechte der Aufklärung von Straftaten gegenüberzustellen und entscheiden zu müssen, wo die Prioritäten liegen. Ist die Wahrung des Datenschutzes wichtiger als die Aufklärung von Internetbetrug? Rechtfertigt die Aufklärung einer Vergewaltigung eine Massenerfassung von DNA der Bevölkerung? Inwieweit verlieren Straftäter die Rechte an den Daten ihres Körpers an den Staat durch ihre Taten? Welche Datenerhebung kann der Polizei überlassen werden und welche ist so sensibel, daß sie vorher juristisch geprüft werden muß?

Die Beantwortung dieser Fragen ist eine gesamtgesellschaftliche Herausforderung, die weder mit der pauschalen Ablehnung von Biometrie noch mit den totalen Überwachungsphantasien nach Law-and-Order-Manie bewältigt ist. Die dringlichere Frage allerdings lautet, ob unser gesellschaftliches und politisches System dieser Herausforderung überhaupt gewachsen ist.

Few bad apples

von Beata-K. Hubrig, Rechtsanwältin

Neun von zehn Hotpots in Island werden per Videokamera überwacht. Ich sitze in ca. 40 °C heißem Wasser, und eine dieser großen langen Kameras aus den 1990er Jahren schaut auf mich herab. Der Hotpot ist nicht leer, nein, Isländer sind dort, auch in Badegarnitur, und entspannen sich, treffen sich, tauschen sich aus. Willst Du Isländer sehen, dann gehe in die Badeanstalten, nicht in Kneipen wie in Berlin. In Island gibt es diese wunderbare Badekultur: Was macht der Mensch sonst mit soviel reinem warmen Wasser.

Aber sie tun es unter Videokameras. Ich kann mir kein rechtliches Schutzgut vorstellen, welches Bürgern in Badegarnituren, ihre Freizeit genießend, angemessen gegenübergestellt wird. Hier wird es wohl nicht um Mord und Totschlag, nicht um Raub und Erpressung und auch nicht um sexuelle Straftaten gehen. Überwacht die Kamera, daß der Besucher nicht ins Becken pinkelt? Hat die Kamera die Aufgabe, Unfälle nachvollziehbar zu machen?

Jeder Pool hat seine Bademeister, die lustig und gutgelaunt durch die Besucher stapfen. Wozu also Kameras? Ich weiß es nicht. Sie kommen mir nutzlos vor. Daß ich die Toilette statt der warmen Pools nutze, dafür sorgt die Kontrolle der anderen Besucher; falls ich ausrutsche oder dehydriere, sind andere Besucher und Angestellte zur Stelle. Da ich mich auf die soziale Kontrolle verlasse, könnte ich ohne diese Kameras leben.

Ich scheine aber ein Sonderfall zu sein, was das Vertrauen in meine Mitmenschen angeht. Und mein Mandant: auch ein Sonderfall. Wir gehen nicht davon aus, daß Kameras das sogenannte Allheilmittel sind und dafür sorgen, daß Bürger weder Ordnungswidrigkeiten noch Straftaten begehen oder allgemein durch diese diszipliniert werden. Die Aufzählung von Orten, die heutzutage nicht überwacht werden, fällt kürzer aus als die überwachten öffentlichen und privaten Räume. Aber gibt es noch Räume, in denen wir nicht überwacht werden dürfen?

Diese Frage stellte sich ganz konkret meinem Mandanten an seinem Arbeitsplatz. Er war als sogenannter „Genius“ bei der Apple Retail Germany GmbH (ab jetzt kurz „Apple“) angestellt und arbeitete teilweise im Verkaufsraum und teilweise im Büro, nämlich im „Geniusroom“, in welchem die Geräte der Kunden repariert werden. Alle Räumlichkeiten unterlagen während seiner Arbeitszeit der Videoüberwachung durch Rundkameras, die an der Decke angebracht waren.

Wenig überraschend war die außergerichtliche Auseinandersetzung mit Apple nicht nur fruchtlos, sondern stieß auf taube Ohren. Wir zogen also vor das Arbeitsgericht Frankfurt am Main. In diesem arbeitsrechtlichen Gerichtsverfahren (Az.: 22 Ca 9428/12) wurde Apple verurteilt, meinem Mandanten 3.500 Euro Schmerzensgeld wegen Verletzung seines Persönlichkeitsrechts durch unzulässige Videoüberwachung am Arbeitsplatz zu zahlen.

Der rechtliche Knackpunkt an der ganzen Auseinandersetzung ist, daß niemand mit Schlagwörtern wie Diebstahl, Sachbeschädigung oder Schutz von Bürgern wahllos Videokameras aufstellen kann. Den Betreiber einer Videokamera im öffentlichen oder privaten Raum haben die Rechte derjenigen, die seiner Videoüberwachung unterliegen, zu interessieren. Potzblitz! Wer hätte gedacht, daß im 21. Jahrhundert Bürger unterwegs sind, die das Recht auf Privatsphäre und Geheimnisse wirklich wahrnehmen.

Die Verteidigung der Gegenseite führte nicht zu schwierigen juristischen Auseinandersetzungen. Schon das Bundesarbeitsgericht hatte 2004 (BAG, B. v. 29. Juni 2004, 1 ABR 21103) geurteilt, daß das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechtes unter den Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes bedarf. Wir Arbeitnehmer können diesen Satz also leicht copy&pasten und an unsere Arbeitsplätze hängen. Das kurze zornige Aufflackern des Überwachers wird dann, wie die eingelegte Berufung von Apple, von der Bildfläche verschwinden, wenn wir unsere Grundrechte entschlossen verteidigen.

Home, Sweet Home

von Ralf Thomas Klar <ralf@entropia.de>

Gebäudeautomation gibt es schon viele Jahre, aber lange Zeit gab es in preislich erschwinglichen Bereichen für den kleinen Privateinsatz nur Bastellösungen, bevor einige Firmen den Sektor als Chance begriffen und mit eigenen, günstigen Entwicklungen begannen.

Wer sich eine aktuelle Marktübersicht im Bereich Heimautomation verschaffen und das geeignete System für sich auswählen möchte, hat viel zu tun, zumal dieser Bereich gerade sehr in Bewegung ist. Anfang 2010 wurde ich vor die Aufgabe gestellt, im Rahmen einer Kernsanierung die Heimautomation für eine Wohnung zu planen sowie den Einbau vorzunehmen. Ich hoffe, mit dieser Schilderung Tips, Anregungen und Anreize zu geben.

Systemauswahl

Aus Zeitgründen kamen Selbstbaulösungen nicht in Frage. Kabelgebundene Lösungen wie KNX, LCN oder Dali scheiterten aus zwei Gründen: Einerseits war durch einige Stahlbetondecken und -wände zu wichtigen Stellen keine (bezahlbare) nachträgliche Kabelführung möglich, andererseits überstiegen professionelle Lösungen, wie sie beispielsweise auch etablierte Schalterhersteller anbieten, den gegebenen Finanzrahmen deutlich. Als grober Richtwert für professionelle Automatisierung bei Neubauten oder Sanierungen sind fünf bis acht Prozent der Bausumme anzusetzen.

Weitere Nachforschungen führten zu Angeboten bei diversen Elektronikanbietern, exemplarisch seien Conrad und ELV genannt. Wie ausgeführt, kam nur ein Funksystem in Frage. Als weitere wichtige Randbedingung galt es, ein System zu finden, das möglichst einfach mittels eines Linux-Systems zu steuern sei.

Schlußendlich bestand die Auswahl aus zwei Systemen des Herstellers eQ-3: FS20 und HomeMatic. Beide Systeme arbeiten mit 868 MHz. Das FS20-System benutzt Amplitudenmodulation mit einer Bandbreite von 1 kHZ, hat keine Fehlerkorrektur (weswegen jeder Befehl einfach dreimal nacheinander gesendet wird), hat keinerlei Authentifizierung, keine Verschlüsselung und bietet keinen Rückkanal. Diesen Nachteilen steht eine sehr große Auswahl an Aktoren, Sensoren und Schaltern gegenüber sowie mehrere Open-Source-Projekte zur Ansteuerung.

Das HomeMatic-System benutzt Frequenzmodulation, verschlüsselte Challenge-Response-Authentifizierung und hat einen Rückkanal. Die Aktoren waren zum damaligen Zeitpunkt im Schnitt doppelt so teuer wie bei FS20, die Auswahl wesentlich kleiner, und man benötigte eine damals fünfhundert Euro teure Zentrale.

So fiel die Entscheidung recht schnell für das FS20-System. Inwieweit die ungeschützte Datenübertragung ein Problem ist, muß jeder im Einzelfall entscheiden und hängt auch von den baulichen Gegebenheiten ab. Bei dicken Wänden ist die Dämpfung so groß, daß ein potentieller Störer nur Erfolg hat, wenn er direkt vor der Wohnungstür steht. Daß man das FS20 besser nicht für das Wohnungstürschloß verwendet, versteht sich von selbst.

Die Entscheidung für das FS20 erforderte prinzipiell keine Eingriffe in die bestehende Elektroinstallation. Um einen potentiellen späteren Umstieg auf ein beliebiges anderes System zu erleichtern, wurde jedoch der vorhandene Wohnungsunterverteiler mit 2x8TE durch einen mit 3x12TE ersetzt, zwei weitere Unterverteiler (3x12TE und 1x12TE) in der Wohnung montiert und die Installation im Rahmen der Möglichkeiten auf die drei Unterverteiler zentralisiert. Jeder dieser Unterverteiler bekam noch ein Netzwerk-

kabel sowie eine universelle 24V-Gleichspannungsversorgung vom geplanten zentralen Server-/Steuerstandort spendiert, ebenso wurde die Zuleitung zur Türsprechstelle dorthin verlängert.

Systemaufbau

Die ersten Komponenten, die in der Wohnung Einzug hielten, waren Heizungssteuerungen vom Typ FHT80B/FHT8v. Letztere sind Stellregler, welche anstelle normaler Heizkörperthermostate montiert werden. FHT80B sind frei im Raum plazierbare Steuereinheiten mit bis zu vier Schaltzeiten pro Tag, drei Betriebsmodi, sowie einer Party-/Urlaubsfunktion. Damit war das Bad morgens nach dem Aufstehen gleich mal kuschelig warm, und das Wohnzimmer wurde erst gegen Abend aufgeheizt. Liegt nichts Besonderes an, ist keinerlei Aktion an den Steuereinheiten nötig, also einmal Einstellen und dann (bis zum Batteriewechsel nach circa zwei Jahren) vergessen.

Als nächstes kamen ein paar Unterputz- und Zwischendeckendimmer (DI20-3 und DU-2 für Hochvolt-Halogenlampen, DI22-3 für Niedervolt-Halogenlampen mit elektronischem Trafo). Die Unterputzdimmer haben Anschlüsse für einen Taster zur direkten Bedienung herausgeführt, bei den Zwischendeckendimmern ist nur ein versenkter Taster am Gehäuse, welcher hauptsächlich zur Programmierung verwendet werden soll, eine Bedienung über einen anschließbaren Taster ist nicht vorgesehen.

Im Klartext: Liegt der Dimmer in der Zwischendecke und es gibt Funkstörungen, geht nichts. Ich führte also die Anschlüsse des eingebauten Tasters nach außen. Da dieser direkt an einen hochohmigen Pin des Prozessors angeschlossen ist, funktioniert eine Verlängerung über ein paar Meter bis zum nächsten Wandtaster erwartungsgemäß wegen Störeinstrahlung nicht. So kam direkt neben den Funkdimmer ein Relais, an welches die herausgeführten kurzen Leitungen angeschlossen werden und das seinerseits über den Wandtaster gesteuert wird.

Nachdem noch ein paar Steckdosenschalter und -dimmer verbaut wurden (DI-3, ST-3), konnte mit den FS20-Fernbedienungen (S4, S8) sowie den direkt oder per Relais angeschlossenen Tastern fast die gesamte Lichtinstallation gesteuert werden. Alle Dimmer (bis auf den LED-Zwischendeckendimmer FS20LD) besitzen drei Timer, mit denen beispielsweise Auf- und Abblendzeiten eingestellt werden können. Alleine für das langsame Ein- und Ausfaden hat sich der Aufwand schon rentiert.

Rechneranbindung

Im nächsten Schritt kam die FHZ1000 zum Einsatz, ein per USB anzusteuerndes Funkmodul, das die Kommunikation mit den Heizungsreglern sowie anderen FS20-Komponenten ermöglicht und das ich im Vorfeld schon an anderer Stelle erfolgreich getestet hatte. In der sanierten Wohnung jedoch hing sich das Modul immer nach wenigen Sekunden auf, eine Kommunika-

tion mit den Heizungsreglern oder FS20-Schaltern/Dimmern war nicht möglich. Die Ursachensuche zog sich in die Länge. Dank eines befreundeten Funkamateurs wurde eine starke GSM-Station in der Nachbarschaft als Ursache ausgemacht. Eine Abschirmung des Funkmoduls durch Bleiakkus in Richtung der GSM-Station brachte leichte Besserung, aber keinen stabilen Betrieb.

Das Ingenieurbüro Tostmann *http://busware.de* entwickelt nette Projekte, unter anderem ein USB-Funkmodul mit einem AT90USB162-Prozessor und einem CC1101-ISM-Transceiver. Mittels einer speziellen Firmware kann dieses Modul für das FS20-System nutzbar gemacht werden – damit lief es dann.

Die Firmware ist Teil eines Open-Source-Projektes namens *fhem* *http://fhem.de*. Damit lassen sich u. a. FS20-Komponenten ansteuern und auswerten. Das Ganze ist in Perl geschrieben, hat eine funktionale Weboberfläche, erzeugt hübsche Diagramme (siehe letzte Seite) und bietet eine TCP-Schnittstelle zum Steuern und Abfragen.

Spätestens an dieser Stelle merkt man, daß es sinnvoll gewesen wäre, sich etwas früher mit der Adressierung innerhalb des FS20-Systems auseinanderzusetzen, da ein nachträgliches Ändern der vergebenen Adressen zwar möglich, aber aufwendig ist. FS20-Aktoren können mit bis zu vier Adressen versehen werden. Dadurch kann man Gruppen bilden und zum Beispiel alle Deckenlampen in der Wohnung oder alle Lampen eines Raumes in einer Gruppe zusammenfassen und die Lampen der Gruppe mittels eines Befehles ein- oder ausschalten. Eine spezielle Adresse ist fest als globale Gruppe des gesamten Systems vorgegeben. Diese ist geeignet, um beim Verlassen der Wohnung alles (was für diese Gruppe konfiguriert wurde) auszuschalten.

Gruppenbildung kann bei größeren Installationen auch deshalb notwendig werden, weil das FS20-System im SRD-Band sendet, und bei der gegebenen Frequenz ein Tastgrad von einem Prozent nicht überschritten werden darf. Die CUL/CUN-Devices überwachen die Sendezeiten und verzögern im Bedarfsfall die Signalsendung.

Erste Spielerei

Bei der Wohnungssanierung wurde versehentlich ein Kabel durchtrennt, was nicht rechtzeitig bemerkt wurde. So kam es, daß eine Unterputzdose mit zwei Tastern direkt neben der Eingangstür tot war. Mit dem S4UB aus der FS20-Serie kein Problem: Es handelt sich um eine Platine, die hinter die Schalter in eine Installationsdose paßt und an die bis zu vier Taster angeschlossen werden können. Die Batterielaufzeit soll dabei bis zu zehn Jahre betragen.

Dieser Sender wurde nun nicht direkt für Aktoren oder Gruppen konfiguriert, sondern bekam einen eigenen Code und wurde über *fhem* an ein Bash-Script gekoppelt. Beim Drücken des linken Tasters startet Bash-Script 1, bei Drücken des rechten Tasters Bash-Script 2. Zu Anfang startet Script 1 das Radio:

```
/usr/bin/sudo -u fhem -b mpg123 \
 -@http://www.friskyradio.com/frisky.m3u

/bin/echo "set Sound on" | \
/bin/nc -w1 127.0.0.1 7072
```

Script 2 schaltet dagegen alles aus:

```
/bin/echo "set Alles off" | \
/bin/nc -w1 127.0.0.1 7072

/usr/bin/killall mpg123
```

Sound ist dabei eine in fhem konfigurierte Schaltsteckdose, an der ein kleines Surroundsystem angeschlossen ist, Alles ist hierbei die oben erwähnte globale Gruppe. Die Scripte wurden bald größer. Je nach Uhrzeit wurde ein anderer Radiosender gewählt und je nach Uhrzeit und Bewölkung das Licht geschaltet. Außerdem pflegten die Scripts Statusdateien, anhand derer ein cronjob erkannte, ob Personen anwesend waren. Dieser schaltete dann – falls ja – bei beginnender Dämmerung nach und nach ein paar Lampen zur Grundbeleuchtung hinzu.

Weitere Spielereien

Recht schnell sammelten sich am zentralen Verteiler Steckdosenschalter, was zu Problemen

führte. FS20-Aktoren sollen einen Mindestabstand von fünfzehn Zentimetern zueinander haben, sonst kommt es zu Übertragungsstörungen. Abhilfe schaffte hier ein FS20SM8, eine 8-fach-Schaltplatine mit Open-Drain-Ausgängen, die die Endgeräte per Relais steuert. Da die Relais mit 24 V betrieben werden, die Ausgänge aber nur bis 12 V spezifiziert sind, wurde noch eine 74HCT540/ULN2803-Kombination eingeschleift, um auf der sicheren Seite zu sein.

Wie bei FS20-Schaltaktoren üblich, gibt es für jeden Kanal drei Timer, mit denen verschiedene Betriebsmodi programmiert werden können. Zwei der Ausgänge wurden so programmiert, daß sie bei einem Einschaltbefehl für nur vier Sekunden einschalten. An diese Ausgänge wurde zum einen der Haustüröffner und zum anderen das dritte, ungenutzte Klingeltonsignal (Dreiklanggong) der Türsprechstelle angeschlossen.

Ein auf dem gleichen Rechner laufender Asterisk wurde nun so konfiguriert, daß beim Anruf von hinterlegten Nummern ein Script gestartet wird, das den Haustüröffner schaltet. Ein cronjob schaltete – sofern gemäß Statusdatei die Wohnung belegt ist – abends zur vollen Stunde den Gong, der somit als Ersatz für eine Standuhr diente.

Bauliche Gegebenheiten erforderten es, daß in der Küche der Heizkörper hinter der Spüle montiert wurde und die warme Luft über einen Schlitz in der Arbeitsplatte nach oben strömte. Erwartungsgemäß ist die Konvektion etwas schwach. In das Schutzgitter wurden deswegen vier Papstlüfter eingebaut, die mittels eines Relais an dem FS20SM8 ein- und ausgeschaltet werden. Ein kleines, per cron gesteuertes Perlscript liest den aktuellen Wert des Heizungsstellreglers aus *fhem* aus und schaltet die Lüfter ein, sobald der Stellwert zehn Prozent überschreitet – und nun klappt das auch mit der Küchenheizung.

Die acht Ports des FS20SM8 waren belegt, aber es mußten noch drei Lüfter im Bad, eine Schrankbeleuchtung sowie zwei Kontakte geschaltet und detektiert werden. Ein uraltes ELV M232-Meßmodul fand dabei ein neues Einsatzgebiet. Das M232 hat einen RS232-Anschluß, acht GPIOs sowie sechs analoge Eingänge und läßt sich über ein rudimentäres Protokoll steuern. Vier der acht GPIOs dienen als Ausgänge zum Steuern von Relais, vier dienen als Eingang.

fhem beinhaltet auch ein Modul für das M232, jedoch kam hier ein eigener Daemon zum Einsatz: Da drei der Ausgänge die Lüfter steuern, deren Steuerung nicht ganz trivial ist, erschien es sinnvoll, die eigentliche Steuerung vom Daemon übernehmen zu lassen. An den Eingängen des M232 hängt unter anderem ein Magnetkontakt zur Wohnungseingangstür sowie ein Relais, das parallel zum Licht im Bad geschaltet wird. Der Daemon kann über einen Socket per TCP gesteuert werden. Der Begrüßungs-String liefert den aktuellen Status und wird durch ein Nagios-Script ausgewertet.

Erkennt der Daemon das Einschalten des Badlichtes, wird der aktuelle Sonnenstand berechnet und das Licht im Bad entsprechend heller oder dunkler geschaltet. Damit wird verhindert, daß zu nachtschlafender Zeit grelles Badlicht blendet oder tagsüber das Bad zu dunkel ist. Bleibt das Badlicht länger als drei Minuten an, startet der kleinste Lüfter und läuft dann bis zehn Minuten nach Ausschalten des Badlichtes.

Ein cronjob liest regelmäßig die per HMS100TF gemessene Luftfeuchtigkeit im Bad aus. Steigt diese um fünfzehn Prozent, wird das als Indiz für Duschen gewertet und die Duschlüfter laufen an, bis die Luftfeuchtigkeit wieder unter einen definierten Schwellwert sinkt.

Der Magnetschalter der Eingangstür triggert ein Perlscript. Dieses prüft zuerst Uhrzeit, Sonnenstand und Bewölkungsgrad und schaltet in Abhängigkeit davon Licht und Radio und setzt den Wohnungsstatus. Das ist nicht nur angenehm, sondern durchaus praktisch, wenn man beispielsweise Einkaufstüten hereinträgt.

Bei den anfänglich erwähnten Tastern neben der Eingangstür war nach Inbetriebnahme des Magnetkontaktes der Starttaster obsolet. Er wurde zum Schlaftaster umgecodet. Das Script

schaltet nun alles (Licht, Musik) aus, setzt den Wohnungsmodus auf „Schlaf“ und schaltet im Schlafzimmer dezentes Licht ein.

Der aktuelle Zustand des Systems ist so, daß ein Ausfall des Steuerrechners zwar keine Probleme mit sich bringt, aber schon einen deutlichen Verlust an gefühltem Komfort zur Folge hat.

Und nun? Morgendliches Wecken mit Musik und langsam ansteigender Helligkeit kann bei Bedarf schnell gescriptet werden. Komplizierter wird es mit der Einbindung der Rolläden im Rahmen einer Beschattungsautomatik. Das verwendete Zweiwege-Funkprotokoll benutzt eine 128-bittige Verschlüsselung, die Rolläden können entweder über ein sündhaft teures PC-Modul oder Funktaster, bei denen direkt die Tastkontakte z. B. per Relais manipuliert werden, bedient werden.

Der Einsatz von Bewegungsmeldern könnte das Ein- und Ausschalten von Licht in bestimmten Wohnungsbereichen triggern. Da die Grundbeleuchtung der Räume mit LEDs erfolgt und in der Summe bei unter zehn Watt liegt, ist das nicht dringlich. Interessanter ist das Überwachen der Batteriestände der FHT- und HMS-Komponenten über ein Nagios-Script. Ebenso kann man die Daten der HMS100TF für Schimmelwarnungen an schwer oder nicht zugänglichen Stellen aufbereiten.

Es gibt FS20-Komponenten für fast jeden Zweck. Neben den bisher genannten zum Beispiel ein Unterputzradio, eine Infrarot-Fernbedienung (dieser lehrt man die IR-Codes eigener Geräte wie der Hifi-Anlage, die man anschließend per FS20 steuern kann), danaben gibt es noch Komponenten zur Klingelsignalerkennung, einen Erschütterungssensor, einen Regensensor, und so weiter. Speziell für Bastler ist interessant, daß es mehrere FS20-Komponenten als Bausatz oder kleine Fertigplatinen gibt, die man schön in eigene Basteleien integrieren kann. Wenn die Grundstruktur einmal vorhanden ist, steht dem Spieltrieb kaum etwas im Weg.

Der anfänglich erwähnte fehlende Rückkanal mit der Option zur Statusabfrage von Aktoren ist unschön, ebenso die sehr störanfällige Amplitudenmodulation, aber das liegt an der Preisklasse. Da muß jeder überlegen, was er bereit ist zu zahlen, und wo die persönlichen Schwerpunkte gesetzt werden. Aber dann kann man mit Hausautomation Spaß haben. Und ja, man kann damit auch eine Kaffeemaschine einschalten und Kartoffelbrei machen.

Handliche Hacker-Hörzu

Chaosradio: CCC Berlin *https://chaosradio.ccc.de/*
jeder letzte Mittwoch, 22 Uhr - 00 Uhr, zweimonatlich auch terrestrisch auf Radio Fritz

C-RaDar: CCC Darmstadt *https://c-radar.ccc.de/*
jeder zweite Donnerstag, 21 Uhr - 00 Uhr, terrestrisch auf RadaR Darmstadt

Pentaradio: CCC Dresden *https://c3d2.de/radio.html*
jeder vierte Dienstag, terrestrisch auf coloRadio

Radio Chaotica: CCC Karlsruhe *https://entropia.de/Radio_Chaotica*
jeder dritter Montag, 16 Uhr, terrestrisch auf Radio Querfunk

Fnordfunk: CCC Mainz *https://www.cccmz.de/projekte/fnordfunk/*
jeder vierte Sonntag, terrestrisch auf Radio Rheinwelle

/dev/radio: CCC Ulm *http://ulm.ccc.de/dev/radio/index*
jeder zweite Sonntag, 13 Uhr - 15 Uhr, terrestrisch auf Radio free FM

Nerds on Air: CCC Wien *http://www.clifford.at/noa/*
jeder erste und dritte Freitag, terrestrisch auf O94

Hackerfunk: CCC Zürich *http://www.hackerfunk.ch/*
jeder erste Samstag, terrestrisch auf Radio Radius

Funksicherheitslöcher

von Mr. Phrazer

In dieser Arbeit werden Angriffe auf theoretischer und praktischer Basis gezeigt, die auf der im Standard IEEE 802.11-2007 beschriebenen Funktionsweise der Wireless Local Area Networks (WLANs) aufbauen. Eine Beschränkung erfolgt auf das 2.4-GHz-Band, wobei Operationen auf anderen Bändern identisch funktionieren.

Frames

Ein Frame besteht aus einem MAC-Header, einem Frame Body, der die Nutzdaten enthält, und einer Prüfsumme (Frame Check Sequence).

Der MAC-Header verfügt unter anderem über ein Frame Control Field, ein Feld namens Duration/ID und über maximal vier Adreßfelder.

Das erste Adreßfeld ist die Adresse des Empfängers, die Receiving STA Address (RA). Bei Adressierung innerhalb des Base-Station-Subsystems (BSS) ist dies die Adresse der empfangenden Station (STA), bei Adressierung in das Distributionssystem (DS) der Identifier BSSID. Das zweite Adreßfeld ist die Transmitteradresse, die Transmitting STA Address (TA), das heißt, die Adresse, welche das Frame überträgt. Innerhalb des BSS ist das die Adresse der sendenden STA, sonst die BSSID. Die dritte Adresse ist die fehlende Adresse, deren Angabe noch benötigt wird, entweder die Quell- oder Zieladresse oder die BSSID. Die vierte Adresse wird nur in einem Sonderfall benötigt und wird nicht näher betrachtet.

Das Feld Frame Control besteht unter anderem aus den Feldern Type, Subtype, To DS, From DS und Protected. Das Feld Protected gibt an, ob die Nutzdaten verschlüsselt sind. Gesetzt wird es unter anderem bei speziellen Data Frames und Authentication Frames. Die Felder To DS und From DS geben an, ob ein Paket aus dem oder in das DS gesendet beziehungsweise empfangen wird.

Man unterscheidet drei verschiedene Frame-Typen: Data Frames, Management Frames und Control Frames. Data Frames dienen der Übermittlung von Nutzdaten. Frames wie Acknowledgement oder Request To Send gehören zu den Control Frames, die unter anderem die Funktion der Kollisionserkennung und Sicherstellung einer fehlerfreien Übertragung haben. Management Frames sind Frames, welche die Services eines WLAN ausführen. Sie sind die grundlegenden Frames zur Verwaltung der Kommunikation in einem WLAN.

Sicherheit

Sicherheit beim pre-RSNA

Zu Beginn einer intensiveren Kommunikation zwischen der Station und dem Access Point (AP) erfolgt ein Abgleich der unterstützten Sicherheitsparameter. Bei Übereinstimmung folgt die Authentifikation.

Die Sicherheitsprotokolle für die Authentifizierung und den Austausch der dynamischen Schlüssel faßt man mit dem Begriff Robust Secure Network Association (RSNA) zusammen. Die Sicherheit in der pre-RSNA wird durch die Protokolle Wired Equivalent Privacy (WEP) oder Entity Authentication sichergestellt. Es kommen zwei Algorithmen zur Entity Authentication zum Einsatz: Die Open System Authentication besteht aus einer Anfrage und einer Bestätigung ohne jedwede Prüfung; die Shared Key Authentication aus einem Challenge-Response-Verfahren, das auf WEP basiert. Aufgrund der bekannten Unsicherheit von WEP wurde die RSNA standardisiert und die sicherheitstechnischen Verfahren aus der pre-RSNA in diese verlagert. Die RSNA wird nur mit der Open System Authentication in der pre-RSNA betrieben.

Funktionsweise der RSNA

Nach der Open System Authentication folgt die Association. Dabei übermittelt die Station die unterstützten RSN-Parameter. Auf dieser Ebene wird unter anderem festgelegt, ob ein Pre-Shared Key (PSK) oder Authentifizierungsprotokolle zum Einsatz kommen. Ebenfalls wird ausgehandelt, ob das Temporal Key Integrity Protocol (TKIP) oder das Counter-Mode/CBC-MAC Protocol (CCMP) verwendet wird. Wird eines dieser Protokolle genutzt, finden diese nach der Aushandlung, vor dem Four-Way Handshake statt. Wird PSK verwendet, findet dieser direkt statt. Im Folgenden wird nur der Fall mit PSK betrachtet.

Schlüsselableitung und Four-Way Handshake

Der verwendete PSK wird aus dem Klartextpaßwort P durch

```
PSK = PBKDF2(P, ssid, ssidLength, 4096, 256)
```

berechnet. Dabei ist PBKDF2 eine sogenannte Password-Based Key Derivation Function, deren Aufgabe eine Schlüsselableitung ist sowie key stretching, der Mechanismus der Konvertierung kurzer Schlüssel in längere, um Brute-Force-Angriffe zu erschweren. Die Berechnung erfolgt im Detail folgendermaßen:

Als Eingaben dienen das Klartextpaßwort P, das eine Länge von 8 bis 63 Zeichen hat, die SSID des Netzwerkes als Salt; die Zahl 4096, was der Anzahl der Iterationen der Pseudozufallsfunktion HMAC-SHA1 [11] entspricht, welche eine Ausgabe der Länge 160 Bit erzeugt; sowie 256, die Ausgabelänge der Funktion PBKDF2, die somit die ersten 256 Bit der Konkatenationen von T_i mit $1 \leq i \leq l$ darstellt. l ist dabei die aufgerundete Ganzzahl der Division mit der Ausgabelänge von PBKDF2 als Divident und der Pseudozufallsfunktion als Divisor. Da $\lceil \frac{256}{160} \rceil = 2$ gilt, entspricht die Ausgabe 160 von PBKDF2 den ersten 256 Bit der Konkatenation von T1 und T2.

T_i wird jeweils berechnet aus einer Addition im Zahlenring 2, wobei jeder Summand aus einem Aufruf von HMAC-SHA1 mit P sowie einem Salt besteht. Bei dem ersten Summanden ist der Salt jeweils die Konkatenation der SSID mit dem Integerwert von i; bei jedem weiteren Summanden ist der Salt der vorhergehende Summand. Die Berechnung des PSK beinhaltet folglich 8192 Aufrufe der Funktion HMAC-SHA1. Dies hat negative Auswirkungen auf die Effizienz von Brute-Force-Angriffen bei bekannter SSID. Die Verwendung der SSID als Salt verhindert die Erstellung effizienter Rainbowtables. Neben dem PSK gibt es einen Master Key, der bei Authentifizierungsprotokollen verwendet wird. Je nach RSN wird entweder der PSK oder der Master Key zum Pairwise Master Key (PMK). Dieser wird im Four-Way Handshake benötigt, das zur Association im RSN dient und Teil der RSNA ist.

1. STA ← AP : ANonce
2. STA → AP : SNonce, MIC
3. STA ← AP : GTK Encrypted, MIC
4. STA → AP : ACK, MIC

Abbildung 1: Vereinfachter Four-Way Handshake

Der AP generiert eine Nonce, ANonce, und sendet diese an die Station (Schritt 1). Die Station generiert ebenfalls eine Nonce, die SNonce. Jetzt sind alle Parameter bekannt, um den Pairwise Transient Key (PTK) abzuleiten. Dieser wird aus einer Hashfunktion berechnet, die als Eingaben unter anderem die BSSID, die Adresse der Station, die ANonce, die SNonce und den PMK hat. Aus dem PTK wiederum werden weitere Schlüssel abgeleitet: Die ersten 128 Bit bilden den EAPOL-Key Confirmation Key (KCK), die nächsten 128 Bit den EAPOL-Key Encryption Key (KEK) und die nächsten 128 Bit den Temporal Encryption Key (TEK=TK). Wird TKIP verwendet, dann sind noch 128 Bit verfügbar, von denen die ersten 64 Bit den Temporal AP Tx MIC Key (TMK1) und die letzten 64 Bit den Temporal AP Rx MIC Key (TMK2) bilden.

Der im Four-Way Handshake definierte Message Integrity Code (MIC) ist ein Message Authentication Code, welcher als MIC bezeichnet wird, um Verwechslungen mit dem Begriff MAC im 802.11-Sinne auszuschließen. Der MIC selbst wird bei verschlüsselten Paketen ebenfalls verschlüsselt übertragen. Beim TKIP wird als MIC

der Algorithmus Michael genutzt; beim CCMP wird CBC-MAC verwendet.

Der KCK dient zur Data Authentication und ist Eingabe der MIC, der KEK zur Verschlüsselung der Nachrichten im Four-Way Handshake sowie im Group Key Handshake. Der TK dient zur Verschlüsselung der Daten bei TKIP und CCMP, die TMK zur Data Authentication des MIC bei TKIP.

Parallel dazu existiert ein Group Master Key (GMK), aus dem ein Group Transient Key (GTK) abgeleitet wird. Der GEK wird zur Verschlüsselung von Paketen beim TKIP, beim CCMP zusätzlich zur Data Authentication genutzt. Dies übernimmt beim TKIP der GIK. Der Group Key Handshake dient zur Erneuerung des GTK. Dies wird nicht weiter betrachtet. Die Pairwise Keys werden zur Unicast-, die Group Keys zur Multicast-/Broadcast-Verschlüsselung genutzt.

Im zweiten Schritt sendet die Station die von ihr generierte SNonce und den generierten MIC an den AP. Dieser leitet mit Kenntnis der SNonce ebenfalls den PTK ab. Durch Verifikation der MIC hat sich die Station gegenüber dem AP authentifiziert.

Im dritten Schritt sendet der AP den mit KEK verschlüsselten GTK sowie den MIC der Nachricht an die Station. Die entschlüsselt diesen und verifiziert den MIC. Ein gültiger MIC zeigt, daß der AP den PTK berechnen konnte. Somit hat sich dieser gegenüber der Station authentifiziert. Die Station installiert den GTK bei sich.

Im vierten Schritt bestätigt die Station die Installation des Schlüssels inklusive des MIC. Dadurch hat der AP sichere Kenntnis, daß die Installation korrekt verlaufen ist. Beide Partner verfügen nun über das gleiche Schlüsselmaterial zur Verschlüsselung und Data Authentication und haben auch Gewißheit darüber, daß sie sich gegenseitig authentifiziert und frische Schlüssel generiert haben.

RSNA-Datenverschlüsselung und Data Integrity

Nachdem die Association abgeschlossen ist und alle Schlüssel zur Verfügung stehen, sind bei der weiteren Kommunikation in einem RSN Verschlüsselung und Integrität der Nutzdaten erforderlich. Dazu dienen TKIP und CCMP. Bekannt in der Praxis sind diese als Verschlüsselungsmethoden Wi-Fi Protected Access in den Varianten WPA und WPA2. Bei beiden wird zwischen Personal und Enterprise unterschieden. Personal entspricht dabei PSK, während Enterprise für die Verwendung von Authentifizierungsprotokollen steht. Anzutreffen sind auch Kombinationen wie beispielsweise WPA-PSK oder WPA2-PSK.

Temporal Key Integrity Protocol (TKIP)

Das TKIP ist der Nachfolger von WEP. Dabei verwendet es die WEP-Verschlüsselung, verfügt aber über einige Erweiterungen. So werden beispielsweise diverse Felder als Eingänge für zwei Key-Mixing-Algorithmen genutzt, es gibt eine deutlich komplexere Schlüsselableitung und der MIC gewährleistet Datenintegrität.

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

Das CCMP muß vom RSN unterstützt werden; TKIP ist dagegen optional. CCMP nutzt den Counter Mode für Blockchiffren. Dabei wird der TK als Schlüssel für die symmetrische Verschlüsselung eines Initialisierungsvektors konkateniert mit einem sukzessive erhöhten Counter genutzt. Der daraus resultierende Schlüsselstrom wird mit dem Klartext mit einer Addition im Zahlenring 2 verknüpft. Als MIC wird der CBC-MAC genutzt. CBC-MAC mit dem Counter Mode ist als CCM standardisiert. [12] Als symmetrische Verschlüsselung wird bei CCMP AES-128 verwendet. [13]

Angriffe

Einführung

Es gibt eine Vielzahl von Angriffen, die aus der allgemeinen Funktionsweise eines WLAN ableitbar sind. Aufgrund dieser Ableitungen ist eine Verhinderung dieser Angriffe oft unmöglich, ohne in den prinzipiellen Aufbau eines WLAN einzugreifen. Hier beschränkt sich die Betrach-

tung auf offene sowie auf verschlüsselte Netzwerke mit den Protokollen TKIP und CCMP mit einer PSK-Authentifizierung.

Bedeutsam sind drei verschiedene Modi, in denen ein Wireless Network Interface Controller (WNIC) betrieben werden kann. Wird ein WNIC im Modus Master beziehungsweise Infrastructure betrieben, fungiert er als AP; wird er im Modus Managed betrieben, fungiert er als Station. Der Modus Monitor ermöglicht das Empfangen sämtlicher Pakete, die über die Funkschnittstelle übertragen werden. Für die meisten Angriffe ist die Verwendung des Modus Monitor erforderlich.

Deauthentication und Disassociation

Deauthentication und Disassociation sind Benachrichtigungen. Das bedeutet, daß bei Erhalt eines Disassociation Frames die temporären Schlüssel im Extended Service Set oder bei der Station (je nachdem, von wem die Nachricht ausgeht) verworfen werden, die Kommunikation mit dem Distributionssystem verhindert wird und beim Erhalt eines Deauthentication Frames unmittelbar danach die Disassociation erfolgt.

Werden Deauthentication und Disassociation Frames an eine Station mit der BSSID des AP und an den AP mit der MAC-Adresse der Station gesendet, werden die temporären Schlüssel beidseitig verworfen und somit die Verbindung der Station unterbrochen. Diese muß sich erneut authentifizieren, danach assoziieren, dann die RSNA durchführen. Sendet der Angreifer diese Frames periodisch, kann sich die Station nicht neu verbinden. Bei Verwendung der Broadcast-Adresse ff:ff:ff:ff:ff:ff anstelle der MAC-Adresse der Station wird jede Station disassoziiert.

Beacon Flood

Ein Beacon Flood bezeichnet die kontinuierliche, kurz hintereinander ausgeführte Generierung und Aussendung generierter Beacon Frames mit gleichen oder zufälligen BSSIDs und SSIDs. Dies führt zu einem hohen Aufkommen vermeintlich verfügbarer WLANs. Eine Station kann Probleme haben, sich unter Hunderten AP mit der gleichen SSID, aber unterschiedlichen BSSIDs mit dem existierenden WLAN zu verbinden, da es den dazugehörigen AP nicht eindeutig identifizieren kann. Außerdem kann die hohe Anzahl verfügbarer WLANs bei der Software zur Suche existenter WLANs Fehler verursachen.

Rogue AP

Ein Rogue AP bezeichnet einerseits einen unautorisiert installierten, andererseits auch einen rein softwarebasiert arbeitenden AP. Hier wird der zweite Fall betrachtet. Ein Rogue AP intendiert einen direkten Angriff auf Stationen. Er kann sich als ein AP eines der Station bekannten WLANs ausgeben und diese dazu bringen, sich mit ihm anstelle des genuinen AP zu verbinden. Der Rogue AP generiert Beacon Frames und Probe-Response Frames, welche die Informationen des gesuchten WLANs der Station beinhalten. Wird die Station dazu gebracht, sich mit dem ihm zu verbinden, ist der Angriff erfolgreich.

Eine Station verbindet sich mit einem AP eines ihr bekannten WLAN. Die Information, welche WLANs und welche APs in ihrer Nähe sind, kann sowohl durch Probe-Request und Probe-Response Frames als auch durch Beacon Frames in Erfahrung gebracht werden. Eine Station kann so konfiguriert sein, daß sie sich automatisch mit einem WLAN verbindet, sobald ein Beacon Frame ein ihr bekanntes WLAN verkündet, zum anderen kann sie aktiv durch Probe-Request Frames ein solches ermitteln. Dabei kann sie die gesuchte SSID explizit setzen, oder sie setzt die Broadcast-SSID, und alle APs antworten. Zusätzlich kann die Station bereits mit einem AP assoziiert sein und muß sich aufgrund eines Verbindungsabbruches neu verbinden.

Dies alles macht sich ein Rogue AP zunutze: Setzt die Station eine explizite SSID, sendet der AP der Station eine Probe-Response mit der angefragten SSID und generiert zusätzlich Beacon Frames mit dieser. Setzt eine Station die Broadcast-SSID, und ist dem Angreifer bekannt, mit welcher SSID die Station sich verbinden würde, sendet der AP eine Probe-Response mit dieser SSID. Dabei müssen die RSN-Parameter des WLANs übereinstimmen. Ist dem Angreifer

eine SSID bekannt, mit der sich eine Station verbinden würde, kann der AP diese durch Beacon Frames verkünden, auch wenn die Station nicht in der Nähe ist. Sobald sie es ist, baut sie automatisch eine Verbindung auf. Ist eine Station bereits in Kommunikation mit einem AP, kann der Rogue AP die Verbindung zwischen beiden durch gezielte Deauthentication und Disassociation trennen und die Station dazu bringen, sich nunmehr mit ihm zu verbinden. Erwartet die Station ein unverschlüsseltes WLAN und verbindet sich mit dem Rogue AP, agiert dieser wie ein Man in the middle. Verbindet sich eine STA zufällig mit dem Rogue AP eines unverschlüsselten, ihr unbekannten WLANs, ist der Rogue AP als Honeypot zu betrachten. Verbindet sich eine STA zu dem Rogue AP, erwartet ein verschlüsseltes WLAN und der Angreifer kennt den PSK nicht, terminiert die Verbindung mit dem Rogue AP nach dem dritten Schritt des Four-Way Handshake. Dies ist ausreichend, um eine brute force attack auf den PSK auszuführen. Hat der Angreifer Kenntnis über den PSK, kann der Four-Way Handshake vollständig ausgeführt werden. Der Rogue AP kann dann den Traffic der STA in das genuine Netzwerk einspeisen.

Angriff auf den PSK

Beim Four-Way Handshake wird der PSK als PMK genutzt. Hat ein Angreifer einen Four-Way Handshake mitgeschnitten, kann er feststellen, wann er den richtigen Schlüssel geraten hat. Das Raten kann aus einem Brute-Force-Angriff zum einen auf den PSK direkt mit maximal 2256 Versuchen, zum anderen auf die Passphrase, die als Eingang der Funktion PBKDF2 dient, bestehen. Im zweiten Fall wird pro geratener Passphrase die Funktion PBKDF2 mit den 8192 Aufrufen von HMAC-SHA1 ausgeführt. Aus dem geratenen oder berechneten PMK wird mit der abgefangen ANonce und SNonce durch eine weitere Hashfunktion der PTK berechnet, aus welchem der TK und bei TKIP der TMK1 und der TMK2 abgeleitet wird. Mit diesen Schlüsseln wird in der zweiten Nachricht der MIC berechnet. Stimmt der MIC mit dem abgefangenen MIC überein, ist der PSK korrekt.

Das erfolgreiche Raten des PSK ist in der Praxis sehr unwahrscheinlich. Da zusätzlich bei jedem Durchlauf PBKDF2 aufwendig berechnet werden muß, ist diese Variante ebenfalls nahezu erfolglos. Effizienter kann ein Wörterbuchangriff ausgeführt werden, gerade bei schwachen Paßwörtern. Ein einfacher Wörterbuchangriff ist dennoch langwierig. Es gibt unterschiedlichste Methoden zur Beschleunigung, sei es die Berechnung mit FPGAs oder die Berechnung auf Graphical Processing Units (GPU) oder in der Cloud. Bei starken Paßwörtern sind diese Wege jedoch wenig erfolgreich. Der Salt durch die SSID beim PSK verhindert eine effiziente Generierung von Rainbow Tables. In dem Fall, bei dem Rainbow Tables für eine SSID existent sind, ist die Berechnung um einiges schneller. Bei schwachen Paßwörtern kann ein Angriff mit Rainbow Tables Erfolg haben [15].

Gegenmaßnahmen sind bei den meisten dieser Angriffe sehr schwer, da sie auf den Grundlagen des Standards beruhen. Dennoch sind kleine Fortschritte zu erzielen. Man kann den Standard IEEE 802.11w-2009 [16] verwenden.

Dieser integriert kryptographische Methoden in Management-Frames. Diese Frames beinhalten beispielsweise einen MIC zur Prüfung eingehender Pakete. Der Standard setzt überdies die Verwendung eines RSN voraus, ist jedoch in der Praxis bisher nicht weit verbreitet. Bei Deauthentication- und Disassociation-Angriffen kann die Firmware des WNIC so verändert werden, daß diese Frames ignoriert werden. Zum einen ist das jedoch nicht standardkonform, zum anderen muß dies im AP selbst ebenfalls angepaßt werden. Eine andere Möglichkeit ist, sich durch ein Programm benachrichtigen zu lassen, wenn derartige Frames gehäuft auftreten. Ein Ansatz dazu findet sich in. [17]

Das Abstürzen der Software bei der Suche verfügbarer WLANs vermittels Beacon Flood ist durch sicherheitsbedachte Programmierung verhinderbar. Zusätzlich kann unter Umständen die Anzahl der verfügbaren Netze bei gleicher SSID in der Anzeige eingeschränkt werden.

Bei der Detektierung eines Rogue AP kann die Gültigkeit der MAC-Adresse überprüft werden, bevor eine Verbindung aufgebaut wird. Ist dem Rogue AP eine gültige MAC-Adresse zugewiesen, ist die Detektierung ergebnislos. Wird in den Probe-Request Frames eine spezielle eindeutige SSID gesetzt, kann ein AP sich nicht mit dieser ausgeben, sofern der Angreifer nicht explizit eine setzt, deren Kenntnis der Station ihm bewußt ist. Die generelle Unterbindung eines automatisierten Aufbaus einer Verbindung sowie der Verbindung in das Netzwerk mit der SSID aus einem Beacon-Frame, ohne diese in einem Probe-Request Frame zu setzen, vermindert die Wahrscheinlichkeit einer Verbindung zu einem Rogue AP, sofern die SSID dem Angreifer nicht bekannt ist. Eine Authentifizierung durch Client-Server-Zertifikate auf Basis von Authentifizierungsprotokollen erschwert ebenso den Einsatz eines Rogue AP.

Außerdem kann zur Detektierung von Angriffen und eventueller Verhinderung allgemein ein Wireless Intrusion Detection System (WIDS) beziehungsweise ein Wireless Intrusion Prevention System (WIPS) verwendet werden. Ein Beispiel ist das freie OpenWIPS-ng. [18]

Zusammenfassung und offene Themenfelder

Wir sehen, daß die Sicherheit in WLANs ein durchwachsenes Themenfeld ist. Während die Kommunikation sehr leicht verhindert werden kann, erweisen sich gezielte Rogue-AP-Angriffe als sehr mächtig, sind jedoch sehr aufwendig in der Konfiguration und nur eingeschränkt tauglich für großflächige Angriffe. Während Angriffe auf den PSK mit schwachen Paßwörtern möglich, aber zeitaufwendig sind, sind Angriffe auf starke Paßwörter praktisch undurchführbar, sofern keine Schwächen in den Algorithmen und Protokollen gefunden werden. Diese Angriffe sind jedoch nur ein Ausschnitt aus der Vielzahl an Möglichkeiten. Nicht behandelt wurden beispielsweise die Funktionsweise der Authentifizierung und der Authentifizierungsprotokolle im RSNA vor dem Four-Way Handshake sowie Angriffe auf diese. Für eine Zusammenfassung praktischer Angriffe siehe [19].

Weitere Angriffe sind unter anderem auf kryptographischer Ebene und auf der Implementierungsebene möglich. Im Bereich der kryptographischen Angriffe gibt es bereits erste Erfolge, TKIP anzugreifen. [20], [21] Im Dezember 2011 wurde bekannt, daß ein Großteil der verbreiteten WLAN-Router über Schwachstellen in der Implementierung des WiFi Protected Setups (WPS) verfügen. WPS dient der Benutzerfreundlichkeit und ermöglicht die Anmeldung einer Station in ein mit einem PSK geschütztem WLAN mittels einer PIN, um die Eingabe und Konfiguration eines PSK für die Verwendung von TKIP/CCMP zu umgehen und dennoch diese Protokolle zu nutzen. In dem Angriff Stefan Viehböcks wird die PIN geraten, wobei der Router in seinen Antworten Hinweise gibt, wie die PIN lautet. [22]

Entwicklungen gibt es auch im Bereich der Packet-in-Packet-Injection (PIP), bei der bösartige Pakete in akzeptierten Paketen versteckt sind. [23] Ein derartiger Angriff auf WLAN nach dem Standard IEEE 802.11b-1999 findet sich in [24]. So durchwachsen und komplex das Themenfeld WLAN ist, so vielfältig sind die Angriffe, bei denen zukünftig noch sehr viel Potential vorhanden ist.

Literatur

[1] IEEE Std 802.11-1997. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standards Association. Nov. 1997.

[2] IEEE 802.11a 1999. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standards Association. Feb. 1999.

[3] IEEE 802.11b 1999. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standards Association. Feb. 1999.

[4] IIEEE 802.11g 2003. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standards Association. Okt. 2003.

[5] IEEE 802.11i 2004. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standards Association. März 2003.

[6] IEEE Std 802.11-2007. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. (2007 Revision). IEEE Standards Association. Juni 2007.

[7] S. Fluhrer, I. Mantin, A. Shamir. „Weaknesses in the key scheduling algorithm of RC4“, In: Selected areas in cryptography. Springer 2001, S. 1–24.

[8] N. Borisov, I. Goldberg, D. Wagner. „Intercepting mobile communications: The insecurity of 802.11“, In: Proceedings of the 7th annual international conference on Mobile computing and networking. ACM 2001, S. 180–189.

[9] E. Tews, R. P. Weinmann, A. Pyshkin. „Breaking 104 bit WEP in less than 60 seconds“, In: Information Security Applications, 2007, S. 188–202.

[10] B. Kaliski. PKCS #5: Password-Based Cryptography Specification Version 2.0. RFC 2898 (Informational). Internet Engineering Task Force, Sep. 2000. *http://www.ietf.org/rfc/rfc2898.txt*.

[11] H. Krawczyk, M. Bellare, R. Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104 (Informational). Updated by RFC 6151. Internet Engineering Task Force, Feb. 1997. *http://www.ietf.org/rfc/rfc2104.txt*.

[12] N. Draft. „Special Publication 800-38C“, In: „Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and confidentiality“, US Doc/NIST 2004.

[13] PUB FIPS. „197“, In: Advanced Encryption Standard (AES) 26, 2001.

[14] Aircrack-ng Team. Airmon-ng. *http://www.aircrack-ng.org/doku.php?id=airmon-ng*.

[15] Church of Wifi. WPA-PSK Rainbow Tables. *http://www.renderlab.net/ projects/WPA-tables/*.

[16] IEEE Std 802.11w 2009. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standards Association. Sep. 2009.

[17] Tinman2k. Deauthorization Attacks explained (with demo). *http://revision3.com/hak5/deauth/deauthorization-attacks-explained-with-demo-*.

[18] Thomas d'Otreppe. OpenWIPS-ng. *http://www.openwips-ng.org/*.

[19] J. Cache, J. Wright, V. Liu. Hacking Exposed Wireless. Hacking Exposed. McGraw-Hill, 2010. ISBN 9780071666619.

[20] Martin Beck, Erik Tews. „Practical attacks against WEP and WPA“, In: Second ACM Conference on Wireless Network Security, WISEC 2009.

[21] T. Ohigashi, M. Morii. „A practical message falsification attack on WPA“, In: Procedings of Joint Workshop on Information Security, Cryptography and Information Security Conference System. 2009.

[22] S. Viehböck. Brute Forcing Wi-fi Protected Setup. 2011. *http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.*

[23] T. Goodspeed et al. „Packets in Packets: Orson Welles' In-Band Signaling Attacks for Modern Radios“, In: Proceedings of the 5th USENIX conference on Offensive technologies. USENIX Association. 2011, S. 7–7.

[24] T. Goodspeed. 802.11 Packets in Packets: A Standard-Compliant Exploit of Layer 1. 2011. *http://events.ccc.de/congress/2011/Fahrplan/events/4766.en.html*.

Verräterisches Her(t)z

Audio-Analyse der Pause zwischen Tastenanschlägen

Von Bernhard Fechner <cu0815@live.de> und
Jens Christian Lisner <jens@lisner.net>

Viele Geldautomaten geben ein Audio-Feedback bei der Eingabe von PINs, das auf interessante Informationen schließen läßt. So lassen sich die Pausen zwischen einzelnen Tastaturanschlägen aufzeichnen und analysieren.

Das Aufzeichnen der Tastaturgeräusche, um die PIN herzuleiten, ist einfacher als eine Kameraüberwachung oder andere Methoden, zum Beispiel Laser oder die Power-Line-Methode. [11] Dies betrifft auch Sicherheitssysteme, die zur Zugangskontrolle numerische Tastenblöcke einsetzen. Im Folgenden soll der Versuch unternommen werden, aus den Audio-Informationen eines Automaten die Pausen zwischen gedrückten Tasten zu extrahieren und daraus Rückschlüsse auf die Eingabe zu ziehen. Solche Daten lassen sich auch im biometrischen Kontext interpretieren, um Benutzer zu authentifizieren.

Thematisch verwandte Arbeiten

Gegen Ende des 19. Jahrhunderts begann man zu beobachten, daß es charakteristische Merkmale im Rhythmus einer codierten Nachricht gab, anhand derer Telegraphierer in der Lage waren, sich gegenseitig zu erkennen. [4] Eine der ersten Arbeiten, die sich mit der Identifikation von Personen anhand der Charakteristika von Pausen zwischen gedrückten Tasten beschäftigte, wurde 1975 von Spillane veröffentlicht, [3] gefolgt von einer ganzen Biometriewelle in den 1980ern. [8] Die Identifikation mittels Tastaturanschlägen wurde sowohl von Urnphress und Williams [9] als auch von Joyce und Gupta [9] vorgeschlagen. Guven und Sogukpinar [7] benutzten einen Vektor-basierten Algorithmus, um Muster in Tastenanschlägen herauszufinden. Das Thema blieb bis heute für viele Forscher interessant. Eine Übersicht findet sich in [6]. Ein biometrisches Signatursystem für Geldautomaten wurde von Kroll [1] vorgestellt. Die Analyse von Ziffernblock-Sequenzen an Geldautomaten zur Identifikation von Benutzern wurde von Rodrigues et al. vorgeschlagen. [2] Im Unterschied zu den genannten Arbeiten, werden in dieser Arbeit Audio-Daten betrachtet.

Erhebung der Daten

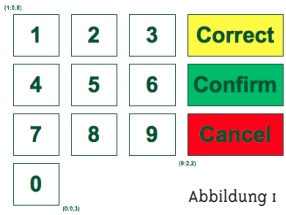
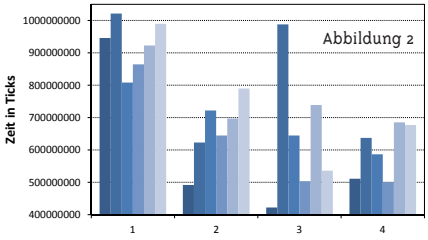


Abbildung 1

Fast jeder Geldautomat bietet eine Möglichkeit, eine PIN einzugeben. Dies kann über eine gewöhnliche Tastatur oder über einen Touchscreen geschehen. Jeder Taste wird eine bestimmte Position und ein bestimmter Wert zugeordnet. Um die Distanz zwischen zwei Tasten zu berechnen, wird der euklidische Abstand zwischen dem Mittelpunkt der Tasten berechnet. Im Beispiel (Abbildung 1) ist der Abstand von Taste „1“ zu Taste „5“ mit `sqrt(2)` gegeben. Die Notation (w: x,y) bedeutet, daß sich die Taste mit Wert w an Position (x,y) befindet, wobei die oberste Taste bei Position (0,0) liegt.

Im Experiment wird der Benutzer aufgefordert, eine Reihe von Zahlen, bestehend aus vier Ziffern, einzugeben (Quadnum). Ein Programm zeigt die einzugebenden Zahlen an. Der Benutzer liest die Zahl und gibt sie anschließend ein. Einige Benutzer lesen und memorieren zuerst die komplette Quadnum, um diese dann vollständig einzugeben, andere merken sich zunächst nur einen Teil und geben diesen ein. Dieses Verhalten unterscheidet sich vom üblichen Verhalten an einem Geldautomaten oder einer Sicherheitstür. Hier erfolgt die Einga-



be fast unterbewußt. Aus diesem Grund soll der Benutzer die gleiche Quadnum mehrfach eingeben, bevor die Sequenz geändert wird. Abbildung 2 zeigt, wie sich die durchschnittliche Zeit zwischen den Tastenanschlägen bei vierfacher Eingabe einer Quadnum entwickelt. Der dunkelste Balken stellt die zeitliche Entwicklung für die erste Quadnum dar, der hellste für die letzte (sechste) Quadnum.

Gemessen wird die Zeit in Prozessortakten, was die Genauigkeit der Zeitmessung erhöht. Dafür sind die Ergebnisse nicht direkt auf andere Systeme übertragbar. Wenn das Zielsystem bekannt ist, sollte dies kein Problem darstellen, da sich – solange die Taktfrequenz nicht von anderen Mechanismen beeinträchtigt wird – die Meßwerte leicht in absolute Timings überführen lassen. Anders verhält es sich bei der Analyse von Audio-Daten; hier ist eine absolute Zeitskala vorhanden. Jede gedrückte Taste, die Distanz zur vorhergehenden Taste auf dem numerischen Tastenblock und die Verzögerung zwischen Tastenanschlägen werden erfaßt.

Um einfach an die zeitlichen Verzögerungen zwischen den Tastenanschlägen am Geldautomaten zu kommen, werden Audio-Daten gesammelt. Bei der Analyse kann eine Fast-Fourier- oder Wavelet-Analyse eingesetzt werden, indem man zuerst das Energiespektrum der aufgenommenen Audiodaten ermittelt. Abbildung 3 zeigt die aufgenommenen Audiodaten unter realen Bedingungen (Abstand ca. 2 bis 3 m, in einer Tasche, MP3-Kodierung, 44,1 kHz Samplingfrequenz), Abbildung 4 das Ergebnis aus der diskreten FFT-Analyse (Realanteil). [12] Große Räumlichkeiten wirken sich negativ, kleine positiv auf

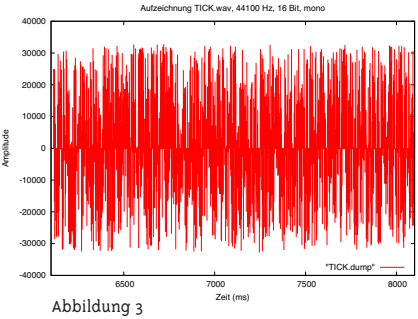
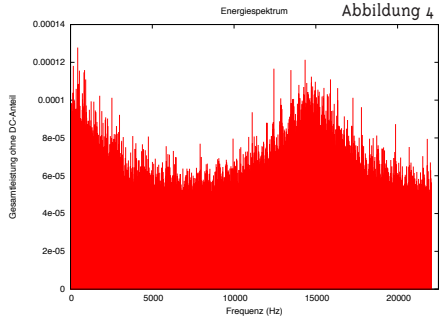
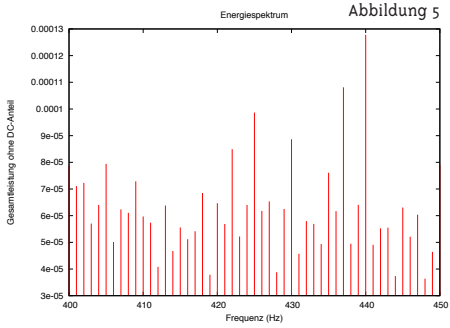


Abbildung 3

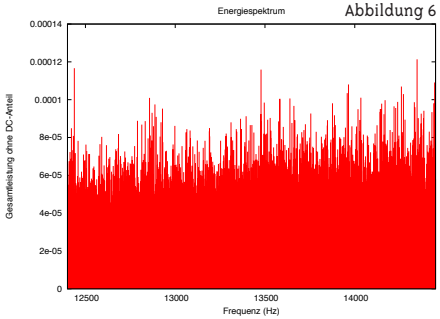


die Akustik aus. In Abbildung 4 erkennt man die interessanten Frequenzbereiche, diese sind der Bereich von 400 bis 450 Hz (Abbildung 5) und 12500 bis 14500 Hz (Abbildung 6).



Um an die Pausen zwischen gedrückten Tasten zu gelangen, sucht man die größte Merkmalsausprägung. Diese liegt im Beispiel bequemerweise bei 440 Hz (s. Abbildung 5). Allerdings kann die charakteristische Frequenz von Geldautomat zu Geldautomat variieren. Die markanteste Frequenz können wir nun als Trigger einsetzen. Die Pause zwischen einzelnen Tasten ist genau die Zeit zwischen einzelnen Triggern,

Abbildung 6



wobei mit einer höheren Samplingfrequenz die Genauigkeit erhöht werden kann. Ab wann getriggert werden soll, sollte man sich anhand der Sampling-Daten genau überlegen, damit nur zu den gewünschten Zeitpunkten getriggert wird.

Interpretation der Daten

Zur Interpretation der Daten können eine Reihe von ausgefeilten Methoden aus der Literatur, zum Beispiel Markov-Ketten, Bayes'sche oder neuronale Netze, verwendet werden. Hier soll jedoch eine einfachere Methode entwickelt werden. Zunächst werden die Daten aufbereitet. Die folgende Tabelle zeigt die Anzahl der Möglichkeiten und den Abstand für den numerischen Tastenblock eines Geldautomaten. Zusätzlich werden die Entfernungen zwischen zwei Tasten klassifiziert und mit den Buchstaben A bis I bezeichnet.

Bewegung	A	B	C	D	E	F	G	H	I
Möglichkeiten	10	26	18	14	18	6	2	2	2
Entfernung	0	1	1,41	2	2,24	2,83	3	3,16	3,61

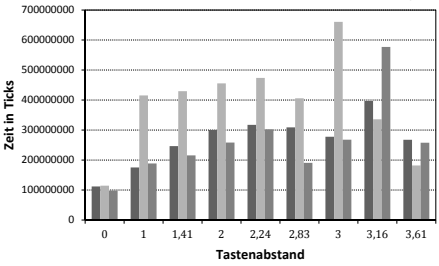
Die Beziehung zwischen Tastenabstand (x-Achse) und der Zeit zwischen Tastenanschlägen (y-Achse) ist in Abbildung 7 dargestellt. Der erste Balken zeigt die Verzögerung zwischen der ersten und zweiten Taste, der zweite Balken zwischen der zweiten und dritten Taste und der letzte Balken zwischen der dritten und der letzten Taste bezogen auf den Abstand der Tasten (x-Achse: 0 (A); 1 (B); 1,41 (C); 2 (D), ...). Die Abbildung zeigt, daß die Verzögerung zwischen der zweiten und dritten Taste unabhängig von ihrem Abstand – mit Ausnahme sehr großer Abstände (3,16 bei den Tastenkombinationen 0-2 und 3,61 bei den Tasten 0-3) – immer größer ausfiel.

Bei der Interpretation der Daten können einige Tastenkombinationen ausgeschlossen werden. Betrachtet man den Ziffernblock als eine Art Schachbrett, wird klar, daß einige Züge (Tastenkombinationen) außerhalb des Schachbretts enden. Beim Abstand d=2,24 (Klasse E) handelt es sich z. B. um einen Rösselsprung. Wir erläutern die Idee anhand einiger Beispiele.

Beispiel #1 (ohne Confirm-Taste)

AGA: Es ist bekannt, daß die zweite oder dritte Taste entweder 0 oder 1 sein muß. Deshalb ist die PIN entweder 0011 oder 1100. Wäre eine Sequenz wie AAA gegeben, gäbe es zehn Kombinationen ohne einen Hinweis, welche dies sein könnten.

Abbildung 7



Beispiel #2 (ohne Confirm-Taste)

ACE: Zur letzten Taste kommt man von allen Positionen mit einem Rösselsprung (E), dann einem diagonalen Zug (C). Auch hier muß jede Taste in Betracht gezogen werden. Anschließend wird eine Taste doppelt gedrückt (A). Dies kann ebenfalls jede Taste sein.

Wird nicht angenommen, daß die Confirm-Taste gedrückt wurde, ist die Anzahl der Möglichkeiten sehr hoch. Deshalb soll das Modell nun erweitert werden, indem zusätzliche Tasten betrachtet werden, die sich an jedem Geldautomaten finden. Im Rahmen dieser Untersuchung ist nur die Confirm-Taste relevant, da diese nor-

malerweise nach Eingabe einer PIN immer gedrückt werden muß. Falls sich der Abstand zur letzten Zifferntaste eindeutig bestimmen läßt, kann die Anzahl der Möglichkeiten stark eingegrenzt werden.

Beispiel #3 (mit Confirm-Taste)

ACE: Wir können die letzte numerische Taste anhand der Confirm-Taste ermitteln und annehmen, daß die letzte und vierte Taste „9“, die dritte Taste entweder „2“, „4“ oder „0“ ist. Mögliche Kombinationen für den diagonalen Zug sind dann entweder 2-4, 2-6, 4-2, 4-8 oder 0-8. Der letzte Zug ist eine Wiederholung der ersten Taste, so daß die folgenden Kombinationen möglich sind: {2,4,6,8}{2,4,6,8}{2,4,0}9. So reduziert sich die Anzahl der Möglichkeiten von 10.000 auf 48.

Zusammenfassung & Schlußfolgerungen

In diesem Artikel wurde die Audio-Analyse der Verzögerung zwischen einzelnen gedrückten Tasten auf einem Ziffernblock vorgestellt. Aus der Verzögerung heraus können einzelne Tasten interpretiert werden. Wir zeigten Schwierigkeiten bei der Analyse und Interpretation der Audio-Daten auf. Wenn die charakteristische Frequenz des Geldautomaten bekannt ist, könnte man die gedrückten Tasten auch in „Echtzeit“ interpretieren, also direkt bei Eingabe der PIN.

Wir schlußfolgern, daß:

- die Verzögerungen zeitlich von der letzten bis zur ersten Taste interpretiert werden sollten, da die letzte Taste (Confirm) bekannt ist und daher wahrscheinlich die zuverlässigste Interpretation zuläßt,
- alle Abstände größer gleich drei Einzelkombinationen (1-0, 0-1, 2-0, 0-2, 3-0, 0-3) sind und
- (Schach-)Verzögerungsmuster die Anzahl der Kombinationsmöglichkeiten reduzieren.

Um einen Geldautomaten gegen den beschriebenen Angriff abzusichern und damit den Diebstahl von PINs zu verhindern, gibt es folgende (mehr oder weniger kostspielige) Möglichkeiten, die auch kombiniert eingesetzt werden können:

- „stille“ Ziffernblöcke, die möglichst keine akustische Rückmeldung geben, etwa durch Einsatz anderer Materialien wie Gummi für eine geräuscharme Eingabe,

- eine zufällige Verzögerung vom Tastendruck bis zur akustischen Rückmeldung,
- eine zufällige Taste–Wertzuordnung mit Hilfe von programmierbaren (O)LEDs oder einem Touchscreen,
- die zufällige Anordnung von Tasten auf einem Touchscreen,
- eine automatische Bestätigung der PIN ohne Confirm-Taste,
- die Zuweisung der PIN zu einem Benutzer nach dessen spezifischem Verzögerungsmuster und
- die Integration eines zweiten Bildschirms, der den Zahlen Symbole zuordnet. Das Hauptdisplay funktioniert nur mit Symboleingabe. Dies stellt auch eine Abhilfe gegen Automaten mit falschem Front-End dar, da nur der Automat die Zahl-Symbol-Zuordnung kennt.

Für die Zuweisung des PIN-Eingabemusters zu einem Benutzer, kann man sich beispielsweise folgendes überlegen:

- Jeder Mensch ist kulturellen Einflüssen ausgesetzt. Wir nehmen an, daß die Geschwindigkeit der Eingabe auch davon abhängt, ob die Person Links- oder Rechtshänder ist.
- Einige – speziell ältere – Personen benötigen wesentlich mehr Zeit für die Eingabe. Wir nehmen an, daß hier eine grobe Klassifizierung getroffen werden kann.
- Die Art, wie eine Person den Ziffernblock benutzt, verrät einiges: Einige benutzen einen einzelnen Finger für die Eingabe, andere zwei oder mehr. Ein Bewegungsprofil könnte mit Hilfe mehrerer Samples erstellt werden. Ein solches Bewegungsprofil kann beispielsweise bei der Benutzung eines Handys (Stichwort: SMS) erstellt werden.

Die obengenannten Ideen im biometrischen Kontext sind im Moment weit davon entfernt, eine Eins-zu-Eins-Zuordnung von Benutzer und PIN zu ermöglichen. Eine weitere Idee ist, ein solches System für eine einfachere Eingabe von Buchstaben und Zahlen zu verwenden. Dies könnte sich zum Beispiel für Behinderte, die normale Tastaturen nicht mehr bedienen können, als sehr nützlich erweisen, da hiermit schneller eingegeben werden kann als mit vergleichbaren Lösungen wie beispielsweise einer ScanMouse.

Literatur

[1] Kroll, M. W.: ATM signature security system, US Patent number 6062474, 2000.

[2] Rodrigues, R.N. et al.: Biometric access control through numerical keyboards based on keystroke dynamics, LNCS 3832, 2005, S. 640–646, DOI: 10.1007/11608288_85.

[3] Spillane, R.: Keyboard Apparatus for Personal Identification, IBM Technical Disclosure Bulletin, Vol. 17, No. 3346, 1975.

[4] Leggett J. et al.: Dynamic Identity Verification via keystroke characteristics, Int'l J. Man-Machine Studies, Vol. 35, No. 6, 1991, S. 859–870.

[5] Chang,W.:KeystrokeBiometricSystemU sing Wavelets, Advances in Biometrics. ISSN: 0302-9743, Vol. 3832/2005, 10.1007/11608288, 2005, A. 647–653.

[6] Peacock, A., Xian Ke, Wilkerson, M.: Typing patterns: a key to user identification. IEEE Security & Privacy, Vol. 2, Issue: 5, S. 40-47, ISSN: 1540-7993, 2004, DOI: 10.1109/ MSP.2004.89.

[7] Guven, A., Sogukpinar I.: Understanding users' keystroke patterns for computer access security. Computers & Security. Vol. 22, Issue 8, 2003, S. 695-706.

[8] Gaines, R., Lisowski, W., Press, S., Shapiro, N.: Authentication by user performance time with interactive systems. Commun. ACM NSF. 1980.

[9] Urnphress, D., Williams, G.: Identity verification through keyboard characteristics. Int. J. Man-Machine Studies, Vol. 23, No. 3, 1985, S. 263-273.

[10] Joyce, R., Gupta, G.: Identity authentication based on keystroke latencies. Communications of the ACM, Vol. 33, No. 2, S. 168-176. DOI: 10.1145/75577.75582, 1990.

[11] *http://hacknmod.com/hack/two-new-methods-for-wireless-keystroke-sniffing/de/*, besucht 24.11.2009.

[12] *http://www.fftw.org/*, besucht 11.6.2012.

Globales Hackergeld

von den Jungen Linken gegen Kapital und Nation

Bitcoin (BTC) wurde von Satoshi Nakamoto im Jahre 2009 als eine neue elektronische oder, besser, virtuelle Währung vorgestellt, die ein Äquivalent zum Bargeld im Internet sein soll. [1] Anstatt Kreditkarten oder Überweisungen zum Einkaufen im Netz zu benutzen, installiert man eine Software auf seinem Computer, den Bitcoin-Client. Dieser erlaubt dann, unter einem Pseudonym Bitcoins an andere Nutzer zu senden, das heißt man gibt die Anzahl an Bitcoins und den Empfänger ein; die Transaktion wird über ein Peer-to-Peer-Netzwerk abgewickelt. [2]

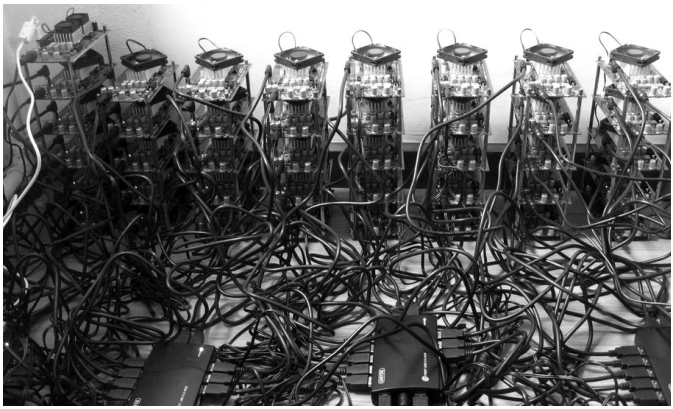
Bitcoins können zur Zeit auf ein paar hundert Webseiten zum Einkaufen verwendet werden. Zum Beispiel, um Währungen, Web Hosting, Web Space, Web Design, DVDs, Kaffee, Kleinanzeigen zu kaufen. Auch Spenden an Wikileaks sind möglich oder die Benutzung von Glücksspielseiten; letzteres kann praktisch sein, wenn diese im eigenen Land verboten sind. Was allerdings Bitcoin zumindest für kurze Zeit große öffentliche Aufmerksamkeit verschaffte, war die Möglichkeit, über eine Kleinanzeigenseite namens „Silk-Road" Drogen zu kaufen. [4]

Am 11. Februar 2012 kostete 1 BTC ungefähr $5,85 USD. Insgesamt wurden bis zu diesem Zeitpunkt 8,31 Millionen BTC ausgestellt. An besagtem 11. Februar wurden 0,3 Millionen BTC in 8.600 Transaktionen verwendet; circa 800 Bitcoin-Clients waren im Netzwerk angemeldet. Das zeigt, daß Bitcoin mehr als eine bloße Idee oder Vorschlag für ein neues Bezahlsystem ist, auch wenn dessen Umfang noch sehr deutlich hinter dem gängiger Währungen zurücksteht.

Es gibt drei Eigenschaften von Bargeld, die Bitcoin versucht nachzuahmen: Anonymität, Unmittelbarkeit und das Fehlen von Transaktionsgebühren. Diese Eigenschaften hat der aktuelle Onlinehandel mit Kreditkarten oder Bankenüberweisungen nicht. Bitcoin ist Peer-to-Peer in Reinform, genauso wie Bargeld im Gebrauch Peer-to-Peer ist.

Was das Projekt aber tatsächlich so ambitioniert macht, ist der Versuch, eine neue Währung zu etablieren. Bitcoins sollen kein Weg sein, Euros, Dollars oder Pfund zu transferieren; sie sollen selbst als neues Geld verstanden werden. Sie werden als BTC gehandelt und nicht als GBP oder EUR. Mehr noch, Bitcoins sind sogar als Geld gedacht, das auf anderen Prinzipien aufbaut als das heute übliche Geld. Am markantesten ist dabei das Fehlen von „vertrauenswürdigen Dritten", sprich: Es gibt keine Zentralbank. Weiterhin sind Bitcoins auf die Anzahl von 21 Millionen insgesamt beschränkt – mehr Bitcoins soll es nicht geben. Aus diesem Grund spricht diese neue Währung marktradikale Liberale an, die zwar den freien Markt schätzen, dem Staat und dessen Einmischung in ebendiesen Markt allerdings skeptisch gegenüberstehen. [5]

Bitcoin ist also der Versuch, etwas Bekanntes, nämlich das Geld, unter einem anderen Ansatz anzugehen und bietet dadurch einen neuen Blick auf diese alltägliche Sache. Es muß durch den Verzicht auf „vertrauenswürdige Dritte" in seiner Konstruktion einige technische Probleme oder Fragen lösen, damit es als Geld auch wirklich brauchbar ist. Damit verweist Bitcoin mit seinen technischen Probleme auf die Eigenschaften, die eine Gesellschaft hat, in der die Wirtschaft über Geld abgewickelt wird. Unter Verwendung von so wenig Fachjargon wie möglich wollen wir versuchen zu erklären, wie Bitcoin funktioniert und was uns dieses Funktionieren über eine Gesellschaft lehren kann, in



ist kooperativ." [6] Die Bitcoin-Gemeinschaft stimmt damit dem Konsens der Wirtschaftswissenschaft zu, daß Kooperation Geld richtiggehend benötige:

„Eine Gemeinschaft ist definiert durch die Kooperation ihrer Teilnehmer und effiziente Kooperation benötigt ein Mittel des Tausches (Geld)..." [7]

der freier und gleicher Tausch die vorherrschende Form von wirtschaftlicher Interaktion ist. Daraus folgt auch eine Kritik an der Ideologie von marktradikalen Liberalen.

Als erstes werden wir sehen, daß die Beschreibung des freien Marktes von Bitcoin-Anhängern genauso falsch ist, wie die der meisten anderen Leute auch. Die Behauptung nämlich, daß sich im Austausch folgendes ausdrücke:

Gegenseitiger Nutzen, Kooperation und Harmonie

Auf den ersten Blick mag eine Wirtschaft, die auf freiem und gleichberechtigtem Austausch beruht, als eine harmonische Sache erscheinen: Menschen produzieren Dinge in Arbeitsteilung, und so erhalten sowohl Kaffeebauer als auch Schuhmacher jeweils Schuhe und Kaffee. Das vermittelnde Element ist das Geld. Die Arbeit der Produzenten ist zu deren gegenseitigen Nutzen oder auch zum Nutzen der ganzen Gesellschaft. In den Worten eines Bitcoin-Anhängers:

„Wenn wir beide eigennützige rationale Wesen sind und wenn ich Dir mein X für Dein Y anbiete und Du diesem Handel zustimmst, dann bewerte ich Dein Y notwendigerweise mehr als mein X und Du bewertest mein X mehr als Dein Y. Mit diesem freiwilligen Handel haben wir beide etwas, das wir als wertvoller erachten, als das, was wir ursprünglich hatten. Wir sind beide besser dran. Das ist nicht ausbeuterisch, das

Sie stimmen also mit modernen Ökonomen darin überein, daß freier und gleicher Austausch Kooperation bedeutet und Geld ein Mittel ist, um beidseitigen Vorteil zu ermöglichen. Sie malen eine Idylle des freien Marktes, dessen negative Eigenschaften dem (wie sie meinen: falschen) Eingreifen des Staates zugeschrieben werden; manchmal auch den Banken und deren Monopolstellung. [8]

Bargeld

Einer dieser Eingriffe des Staates ist die Bereitstellung von Geld, und dagegen richtet sich Bitcoin ja auch. Denn Bitcoin basiert darauf, keine „vertrauenswürdigen Dritten" zu benötigen und damit auch keinen Staat, der Geld herausgibt und dieses verwaltet. Stattdessen ist Bitcoin nicht nur Peer-to-Peer in seinem Umgang mit Geld, sondern auch in dessen Aufrechterhaltung und Erzeugung: Ganz so, als ob es keine Europäische Zentralbank gäbe und alle Menschen in der deutschen Wirtschaft gemeinschaftlich Geld drucken und sich ebenso gemeinschaftlich um dessen Verbreitung kümmern würden. Um dies zu bewerkstelligen, müssen einige technische Hürden überwunden werden. Zum Beispiel muß Geld teilbar sein, zwei Fünf-Euronoten müssen den gleichen Wert haben wie eine Zehn-Euronote und jeder gleichwertige Teil des Geldes muß genauso gut sein wie ein anderer, so daß es keinen Unterschied macht, welchen Zehn-Euroschein ich nun in der Hand halte. Diese Eigen-

schaft läßt sich recht einfach erreichen, wenn man Zahlen auf Computern als Geld hat.

Digitale Signaturen: Garantien wechselseitigen Schadens

Wenn man mit physischem Geld, also Bargeld, hantiert, ist der Eigentumswechsel offensichtlich. Wenn zum Beispiel Anna einen Zehn-Euroschein an Bernd gibt, dann hat Bernd den Schein und nicht Anna. Nach einem Austausch (oder auch Raub) ist es offensichtlich, wer das Geld hat und wer nicht. Es gibt für Anna nach dem Bezahlen keine Möglichkeit zu behaupten, sie hätte Bernd das Geld nicht gegeben, weil sie es nunmal getan hat. Umgekehrt kann aber Bernd vor dem Händewechsel den Geldschein nicht einfach in seine Tasche stecken ohne Annas Zustimmung, außer natürlich mit Gewalt. Letzteres soll durch das Gewaltmonopol des Staates verhindert werden. Wenn man seine Zahlungen über Banken abwickelt, ist es die Bank, die dieses Verhältnis durchsetzt, in letzter Instanz aber auch wieder die Polizei.

Online in einem Peer-to-Peer-Netzwerk ist das natürlich nicht so einfach. Eine Banknote ist nun durch nichts anderes repräsentiert als durch eine Nummer oder eine Zeichenkette. Nehmen wir mal an, `0xABCD` sei eine 1 BTC-Note. [9]

Man kann diese Zeichenkette ganz einfach kopieren; es gibt erst einmal keine Möglichkeit nachzuweisen, daß jemand diese Zeichenkette nicht irgendwo gespeichert hat und weiter benutzt oder anders herum, daß jemand diese vielleicht auch gar nicht mehr besitzt, sie aber als Bezahlung weiterreicht. Weiterhin kann Bernd die Banknote von Anna einfach kopieren, wenn er sie gesehen hat. Der Eigentumswechsel ist also schwierig: Wie kann man sicherstellen, daß Anna Bernd den Bitcoin wirklich gezahlt hat? [10] Damit hat man das erste Problem an der Hand, welches virtuelle Währungen und somit auch Bitcoin lösen müssen.

Um zu beweisen, daß Anna wirklich die Zeichenkette `0xABCD` an Bernd übergeben hat, unterzeichnet sie digital einen Vertrag. Dieser gibt an, daß die Zeichenkette nicht mehr ihr selbst, sondern ab jetzt Bernd gehöre. Eine digitale Signatur ist eine große Zahl. Jedoch hat diese spezielle kryptographische und mathematische Eigenschaften, die sie – soweit man weiß – unfälschbar machen. Also ähnlich wie Menschen normalerweise Eigentum übertragen, zum Beispiel den Titel auf ein Grundstück durch die Unterzeichnung eines Vertrages verschriftlichen, wird das Eigentum am Geld im Bitcoin-Netzwerk auch über Unterschriften unter Verträgen transferiert, nur eben digital. Die Zeichenkette an sich, die unsere Geldnote darstellen sollte, zählt nicht alleine; nur der Vertrag, der anzeigt, wer die Note gerade besitzt, macht sie gültig. Dieses Verfahren der digitalen Unterschriften ist inzwischen so weit verbreitet, daß es kaum Beachtung erfährt, nicht mal im Designdokument von Bitcoin selbst. [11]

Die Frage nach dem Eigentum an Bitcoins zeigt aber schon ein Problem mit dem idyllischen Bild auf, das Menschen von der Wirtschaft mit und ohne Bitcoins haben: Es zeigt, daß es bei einem Geschäft mit Bitcoins – oder allgemeiner: bei jeglicher Art von Tausch – eben nicht damit getan ist, daß Anna, die Kaffee macht, aber Schuhe haben möchte, die wiederum Bernd hergestellt hat. Wenn es nämlich wirklich so einfach wäre, würden sie sich einigen, wie viel Kaffee und Schuhe sie benötigen und würden dies dem jeweils anderen einfach zur Verfügung stellen. Stattdessen aber tauscht Anna ihre Dinge gegen die von Bernd – über das Geld vermittelt. Sie benutzt also ihren Kaffee als einen Hebel, um an Bernds Dinge zu kommen. Ihre Waren sind ihre jeweiligen Mittel, um an die Produkte zu gelangen, die sie konsumieren möchten oder müssen. Sie erzeugen also ihre Produkte nicht für ihr eigenes Bedürfnis und auch nicht direkt für das eines anderen. Vielmehr verkaufen sie ihre Produkte, damit sie sich dann das kaufen können, das sie selbst brauchen. Bernd benutzt also Annas Abhängigkeit von Schuhen, um an ihr Geld zu gelangen und Anna macht das umgekehrt mit Bernd. Daraus ergibt sich, daß man dem jeweils anderen so viel seiner Mittel wie möglich versucht abzunehmen – was ich nicht unmittelbar brauche, ist für mich immer noch Material für künftige Tauschgeschäfte. Gleichzeitig möchte man so viel der eigenen Mittel behalten möchte wie möglich: billig kau-

fen, teuer verkaufen. Doch dies ist keine harmonische Arbeitsteilung zum gemeinschaftlichen Nutzen. Es wird vielmehr versucht, im Austausch einen Vorteil zu erlangen, weil man es eben muß. Mehr noch, der Vorteil der einen ist gleichzeitig der Nachteil des anderen: Ein geringer Preis für Bernds Schuhe bedeutet weniger Geld für Bernd und mehr Geld für Anna, das sie noch für andere Sachen ausgeben kann.

Das Geld löst diesen Interessenkonflikt nicht: Es vermittelt ihn. Damit ist es übrigens auch nicht der Grund für den Konflikt, der ist im Tausch selbst schon angelegt. Die Tauschenden müssen zu einer Einigung kommen, was aber nicht bedeutet, daß sie nicht lieber einfach das nehmen würden, was sie brauchen. Dieses gesellschaftliche Verhältnis gibt also Gründe ab zum Betrügen, Rauben und Stehlen. Unter diesen Umständen ist es schon sehr notwendig zu wissen, wer den Zehn-Euro-Schein besitzt und wer nicht, weil es eben darum geht, ob man das bekommt, was man braucht oder nicht.

Diese systematisch und damit dauernd auftretenden Situationen, in denen des einen Vorteil des anderen Nachteil ist, verlangen nach einem Gewaltmonopol des Staates. Der Tausch als das zentrale Mittel wirtschaftlicher Interaktion ist auf breiter Basis überhaupt nur möglich, wenn die Tauschpartner sich auf den ausgemachten Tausch beschränken. Nähmen sie sich einfach mit Gewalt, was sie wollten, würde das Tauschprinzip nicht mehr funktionieren. Die marktradikalen Liberalen hinter Bitcoin mögen staatliche Einmischung verabscheuen; ihre Wirtschaft jedoch setzt sie voraus.

Wei Dai beschreibt die Online-Gemeinschaft als „eine Gemeinschaft, in der die Angst vor Gewalt machtlos ist, da Gewalt unmöglich ist [...], weil ihre Teilnehmer nicht mit ihren Realnamen oder ihrem Aufenthaltsort in Verbindung gebracht werden können“.

Er erkennt damit nicht nur an, daß die Menschen in der virtuellen Wirtschaft durchaus Gründe haben, sich gegenseitig zu schaden, sondern auch, daß diese Wirtschaft nur ohne direkte Gewalt der Teilnehmer läuft, weil Menschen gar nicht richtig miteinander in Kontakt treten. Durch die Staatsgewalt in der physischen Welt geschützt, können sie im eingeschränkten Bereich des Internets miteinander in Kontakt treten, ohne Angst vor Gewalt haben zu müssen.

Online oder offline, es sind ganz schön umfangreiche Sicherheitsmaßnahmen nötig, um diesen Laden am Laufen zu halten. Bei Bitcoin sind es die „unknackbaren“ digitalen Signaturen, offline hingegen kümmert sich der Staat mit seiner Strafverfolgung beispielsweise darum, Dieben das Handwerk zu legen. Und das alles, um eine so einfache Transaktion wie den Transfer von Gütern vom Produzenten zum Verbraucher zu sichern. Das verweist auf einen grundsätzlichen Interessenkonflikt zwischen den beteiligten Tauschparteien. Wenn das liberale Bild des freien Marktes als eine harmonische Kooperation zum Nutzen aller wahr wäre, bräuchte man keine fälschungssicheren Signaturen. Die Bitcoin-Konstruktion, also das marktradikale Projekt einer Alternative zum Status Quo läßt ahnen, daß diese Theorie falsch ist.

Man könnte einwenden, es gäbe nun einmal schwarze Schafe, die sich an der gesellschaftlichen Harmonie versündigen. Dann stellt sich die Frage, in welchem Verhältnis Aufwand (Polizei, digitale Signaturen) und Nutzen (ein paar schwarze Schafe) stehen. Der Aufwand, mit dem diese schwarzen Schafe in die Schranken gewiesen werden sollen, zeigt ziemlich anschaulich, daß man davon ausgeht, daß es ganz schön viele wären, gäbe es diese Schranken nicht. Dem mögen manche prinzipieller entgegenhalten, daß die Menschen nun einmal so seien. Damit hat man schon mal den Punkt eingesehen, daß es mit der Harmonie hier nicht so weit her ist. Doch ist die Aussage „es ist halt so“ keine Erklärung.

Kaufkraft

Mit digitalen Unterschriften hat man erst einmal nur die Seite des Geldes am Wickel, die die Beziehung zwischen Anna und Bernd betrifft. Aber wenn es um Geld geht, ist auch Annas Beziehung zum Rest der Gesellschaft wichtig. Wieviel Kaufkraft hat Anna insgesamt? Physi-

sches Geld kann Anna nicht verwenden, um zwei verschiedene Leute auf einmal zu bezahlen; Mehrfachausgeben desselben Geldscheins gibt es nicht. Annas Kaufkraft ist auf das beschränkt, was sie an Geld besitzt.

Wenn es um virtuelle Währungen geht, die mit digitalen Unterschriften gesichert sind, hält Anna erstmal nichts davon ab, viele Verträge auf einmal zu unterschreiben, um ihr Eigentum mehrfach zu übertragen. In diesem Fall würde sie Verträge unterschreiben, die besagen, daß `0xABCD` nun gleichzeitig Bernd, Christian und Eva gehören. Bitcoin hat das Problem des Mehrfachausgebens als erstes dezentral gelöst. Das ist ein Fortschritt gegenüber allen früheren Ansätzen für digitales Geld, die auf irgendeiner Art von Zentralstelle aufbauten.

Das Problem wird dadurch gelöst, daß alle Transaktionen öffentlich sind. Also anstatt Annas Vertrag einfach an Bernd zu schicken, wird dieser von Annas Software im Netzwerk veröffentlicht. Anschließend unterschreibt die Software eines anderen Teilnehmers im Netzwerk, daß sie diesen Vertrag gesehen hat. Jemand fungiert bei dieser Unterschrift also als Notar, unterschreibt die Unterschrift von Anna und bezeugt damit die Transaktion. Ehrliche Zeugen unterschreiben nur das erstmalige Ausgeben eines Bitcoins: Sie bestätigen, daß Anna das Geld, das sie ausgibt, auch tatsächlich besitzt. Die Unterschrift des Zeugen wird ebenfalls veröffentlicht. All diese eben beschriebenen Vorgänge werden von der Software im Hintergrund automatisch erledigt.

Anna könnte sich nun mit Christian zusammentun und ihn bitten, all ihre Verträge zu unterschreiben, auch wenn sie ihr Geld mehrfach ausgibt. Sie würde damit also ein falsches Zeugnis von einem unehrlichen Zeugen bekommen. Dies wird dadurch verhindert, daß die Zeugen zufällig gewählt werden. Die Teilnehmer konkurrieren um das Recht, Zeuge zu werden. Als Einsatz müssen sie dafür Rechenzeit auf ihren Computern zur Verfügung stellen. Diese wird dazu verwendet, Lösungen für ein mathematisches Rätsel zu finden. Wendet man dafür mehr Rechenzeit auf, erhöht man seine Chance, ausgewählt zu werden.

Eine Nebenwirkung von diesem Ansatz ist natürlich, daß viele Computer im Bitcoin-Netzwerk Rechenzeit für das Lösen dieser Aufgaben verschwenden, nur um die Lotterie zu gewinnen. Wie dem auch sei, Anna und Christian müßten erhebliche Rechenzeit aufwenden, um diese Lotterie zu gewinnen. Zuviel, als daß es sich lohnen würde – zumindest ist das die Hoffnung.

Falschgeld

Was aber ist nun eigentlich Falschgeld und warum ist das eigentlich so schlimm? So schlimm, daß erheblicher Aufwand dafür betrieben und Rechenzeit verschwendet wird, um sein Aufkommen zu verhindern? Unmittelbar verhält sich Falschgeld nicht viel anders als echtes Geld: Man kann damit Dinge kaufen und Rechnungen bezahlen. Das ist ja genau das Problem. Es ist erst einmal von echtem Geld nicht zu unterscheiden, andernfalls würden Leute es ja auch nicht akzeptieren. Mit normalem Geld und Falschgeld

Rainer bei der Arbeit

zusammen steht allerdings mehr Geld derselben Warenmenge gegenüber, der Wert des Geldes könnte also sinken.

Was also ist dieser Wert des Geldes? Was bedeutet es, daß Geld Wert hat? Es bedeutet Kaufkraft zu haben und damit Zugriffsmacht auf den gesellschaftlichen Reichtum. Erinnern wir uns, daß Anna und Bernd beide ihr mehr oder weniger armseliges Eigentum haben. Wollen sie etwas damit anfangen, treten sie in ein Tauschverhältnis zueinander; sie geben ihre Dinge nicht einfach her, nur weil jemand anders sie braucht. Sie bestehen auf ihrem Recht, über ihr eigenes privates Eigentum zu verfügen. Unter diesen Umständen nun ist Geld die einzige Möglichkeit, um an des anderen Dinge zu kommen. Geld „überzeugt" die andere Seite, einer Transaktion zuzustimmen. Zugriff auf Privateigentum eines anderen zu erlangen, ist auf der Basis von staatlicher Privateigentumsgarantie nur möglich, indem man sein eigenes zum Tausch anbietet.

Auf wieviel Reichtum jemand in der Gesellschaft zugreifen kann, wird dabei in Geld gezählt. Damit wird Privateigentum als solches gemessen. Es wird darin ausgedrückt, von wieviel Reichtum als solchem jemand Gebrauch machen kann. Also nicht nur Kaffee oder Schuhe, sondern Kaffee, Schuhe, Gebäude, Dienstleistungen, Arbeitskraft, fast alles. Auf der anderen Seite wird in Geld aber auch angegeben, wieviel Reichtum mein Kaffee wert ist. Kaffee ist nicht nur Kaffee, sondern ein Mittel, Zugang zu all den anderen Waren auf dem Markt zu bekommen. Er wird gegen Geld eingetauscht, so daß man damit Sachen kaufen kann. Der Preis von Kaffee drückt aus, auf wieviel Kram ganz generell – und eben nicht nur Kaffee – man zugreifen kann. Ganz klar, daß unter diesen sozialen Umständen, also dem freien und gleichen Tausch, diejenigen, die nichts haben, auch nichts bekommen. Alles in allem zeigt das Geld auf meinem Konto an, wieviel ich mir leisten kann – also die Grenze meiner Zugriffsmacht. Denn es zeigt nicht nur an, was ich mir leisten kann, sondern auch, was jenseits der Macht in meinem Geldbeutel liegt. Anders ausgedrückt: Von wieviel Reichtum ich ausgeschlossen bin.

Geld ist Macht, die man in seiner Tasche tragen kann. Es drückt aus, wie viel Kontrolle über Land, Menschen, Maschinen, Produkte ich habe. Daher macht eine Fälschung den Zweck des Geldes zunichte. Es verwandelt diese Grenze, diese Größe in eine unendliche Anzahl von Möglichkeiten. Alles ist im Prinzip verfügbar – und zwar nur, weil ich es will. Wenn jeder unendliche Macht hätte, verlöre Macht ihre Bedeutung. Es würde nicht zahlungskräftige Nachfrage zählen, sondern einfach die Tatsache, daß Bedarf besteht.

Zusammengefaßt ist Geld ein Ausdruck von bestimmten sozialen Verhältnissen, in denen Privateigentum die Bedürfnisse von den Mitteln ihrer Befriedigung trennt. Damit Geld diese Qualität des Privateigentums vermitteln kann, ist es zwingend erforderlich, daß ich nur das ausgeben kann, was ich auch besitze. Diese Qualität und die damit einhergehende Ignoranz und Brutalität gegenüber den Bedürfnissen muß gewaltsam von Staat und Polizei durchgesetzt werden. Im Internet, wo es schwierig ist, jemandes habhaft zu werden, wird dies durch ein sorgfältig ausgearbeitetes Protokoll von Zeugen, Zufälligkeit und schweren mathematischen Problemen gelöst.

Der Wert von Geld

Es bleiben zwei Probleme übrig. Erstens: Wie kommt neues Bitcoin-Geld in die Welt? (Bis jetzt haben wir ja nur den Transfer behandelt.) Zweitens: Wie werden die Teilnehmer überzeugt, Rechenzeit aufzuwenden, um Transaktionszeuge zu werden? Letzteres Problem wird im Bitcoin-Protokoll durch das Erste gelöst. Um die Teilnehmer nämlich dazu zu bewegen, Rechenzeit zur Überprüfung von Transaktionen bereitzustellen, werden diese mit einer bestimmten Anzahl an Bitcoins belohnt, wenn sie als Zeuge gezogen werden. Momentan bekommen sie jedes Mal, wenn sie gezogen werden, 50 BTC und darüber hinaus noch Transaktionsgebühren für jedes Geschäft, das sie bezeugen. Das ist die Antwort auf die Frage, wie neue Bitcoins erzeugt werden: Sie werden „abgebaut", wie das Lotteriegewinnen im Bitcoin-Netzwerk heißt.

Im Bitcoin-Netzwerk „fällt“ das Geld also „einfach vom Himmel“, indem Computer ziemlich sinnlose mathematische Rätsel lösen. Entscheidend ist, daß sich das mathematische Rätsel nur mit erheblichem Aufwand lösen läßt. Worauf es letztendlich ankommt, wenn es darum geht, ob Bitcoin als Geld zählt: Händler müssen sich auf Bitcoin als Geld beziehen und es auch so benutzen. Wie es auf die Welt kam, ist dabei zweitrangig. [12]

Fazit

Ein systematischer Gegensatz von Interessen, der resultierende Ausschluß vom Reichtum, die Unterwerfung von allem unter das kapitalistische Wachstum – so sieht eine Gesellschaft aus, in der Tausch, Geld und Privateigentum die Produktion und den Konsum bestimmen. Das ändert sich auch dann nicht, wenn dieses Geld seine Substanz in Gold oder Bitcoins statt in Geldscheinen und herkömmlichen Währungen. Armut hat ihren systematischen Grund in Tausch, Geld und Wirtschaftswachstum überhaupt. Das mag die marktradikalen Liberalen nicht stören, aber das sollte durchaus auf Kritik von Linken stoßen, die sich zum Teil auch für Bitcoin begeistern.

Links

[1] Das zentrale Dokument über Bitcoin, in dem die Idee dieser digitalen Währung beschrieben wird, ist „Bitcoin: A Peer-to-Peer Electronic Cash System“ von Satoshi Nakamoto. Einige Details des Netzwerks sind jedoch nirgends in der Literatur explizit beschrieben, sondern nur im offiziellen Bitcoin-Client eingebaut. Soweit wir wissen, gibt es keine offizielle Spezifikation außer: *https://en.bitcoin.it/wiki/Protocol_specification*

[2] Als Peer-to-peer-Netzwerk wird ein Netzwerk bezeichnet, in dem die Teilnehmer sich direkt verbinden ohne die Notwendigkeit zentraler Server (wobei einige Funktionen dennoch einen Server benötigen können). Berühmte Beispiele einer solchen Technik sind Napster, BitTorrent oder auch Skype.

[3] Vermutlich auf Druck der US-Regierung haben alle großen Online-Bezahlsysteme die Zahlungen an Wikileaks eingestellt: *http://www.bbc.co.uk/news/business-11938320*. Auch das Benutzen von Kreditkarten für Online-Spielplattformen ist meist von deren Herausgebern verboten.

[4] Nach der Veröffentlichung eines Artikels auf *http://gawker.com/5805928/the-undergroundwebsite-where-you-can-buy-any-drug-imaginable* wurden zwei US-Senatoren darauf aufmerksam und baten den US-Kongreß, die Seite abzuschalten. Bis jetzt scheinen allerdings scheinen diese Versuche nicht wirklich erfolgreich gewesen zu sein.

[5] Eine Strömung, die vor allem in den USA Anhänger findet, wo sie als „Libertarians“ bekannt sind.

[6] Übersetzt von *https://forum.bitcoin.org/index.php?topic=5643.0;all*: „If we‘re both self-interested rational creatures and if I offer you my X for your Y and you accept the trade then, necessarily, I value your Y more than my X and you value my X more than your Y. By voluntarily trading we each come away with something we find more valuable, at that time, than what we originally had. We are both better off. That‘s not exploitative. That‘s cooperative.“

[7] Übersetzt von: „A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money)...“ Wei Dai, „bmoney.txt“ *http://weidai.com/bmoney.txt*. In diesem Text wird die grundsätzliche Idee, auf der Satoshi Nakamotos Bitcoin-Protokoll aufbaut, zum ersten Mal beschrieben.

[8] „The real problem with Bitcoin is not that it will enable people to avoid taxes or launder money, but that it threatens the elites' stranglehold on the creation and distribution of money. If people start using Bitcoin, it will become obvious to them how much their wage is going down every year and how much of their savings is being stolen from them to line the pockets of banksters and politicians and keep them in power by paying off with bread and circuses those who would otherwise take to

the streets."
http://undergroundeconomist.com/post/6112579823

[9] Wir sind uns bewußt, daß Bitcoin durch nichts anderes als durch die Liste der Transaktionen repräsentiert wird. Zur einfacheren Präsentation hier nehmen wir aber einfach an, daß es so ein eindeutiges Merkmal gibt wie die Seriennummer auf einem Euroschein.

[10] „Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. [...] Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. [...] With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party." Satoshi Nakomoto, „Bitcoin: A Peer-to-Peer Electronic Cash System", 2009.

[11] Für eine Einführung in das Thema kryptographisches Geld siehe Burton Rosenberg (Ed.), „Handbook of Financial Cryptography and Security", 2011.

[12] Manchen, die „Das Kapital" von Marx gelesen haben, könnte jetzt einfallen, daß dies implizieren würde, daß Bitcoin auf einem Wertkonzept aufbaue, dessen Substanz nicht vergegenständlichte abstrakt menschliche Arbeit sei. Viel eher würde es auf dem Wert von abstrakter Computerarbeit oder etwas ganz anderem beruhen. Dieser Einwand beruht jedoch auf einem Mißverständnis. Mit Rechenzeit verdient man, wenn man Glück hat, 50 BTC. Dies ist jedoch nur eine bedeutungslose Nummer. Was man mit 50 BTC anstellen kann, wieviel Verfügungsmacht oder Befehlsgewalt über sozialen Reichtum diese repräsentieren, ist eine ganz andere Sache. 50 BTC haben Wert, weil sie auf gesellschaftlichen Reichtum zugreifen und nicht, weil ein Computer zufällig die richtige Nummer ausgewählt hat. Für die Wertbestimmung ist es nicht zuerst wichtig, wie das Geld in die Gesellschaft kommt, sondern als was es in dieser gilt.

PostSpack

Post post-privacy Oder: Warum ich die Spackeria für einen Holzweg halte

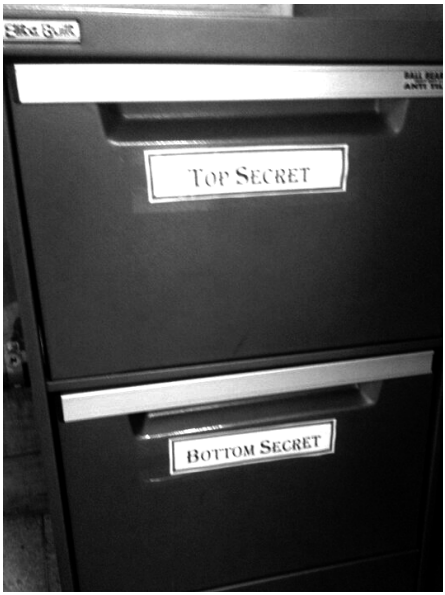
von LeV <ds@levampyre.de>

Irgendwann, vor vielen Jahren, saß ich in einer Vollmondnacht mit meinem Geliebten bei einer Tüte Heilkräuter, und er sagte: „Hach", und: „Wäre es nicht schön, wenn wir in einer Gesellschaft leben könnten, in der niemand mehr Geheimnisse zu haben bräuchte, in der sich niemand mehr seiner Vorlieben schämen, sich für sie rechtfertigen oder sie verteidigen müßte? Ich will so frei, so stark sein, mit erhobenem Kopf in der Öffentlichkeit zu stehen und zu sagen, daß ich schwul bin, daß ich Drogen konsumiere, daß ich Geliebte neben meiner Ehefrau habe, daß ich mich gerne im Bett fesseln lasse, daß ich mir für Geld einen habe blasen lassen, daß ich gestern so viel gesoffen habe, daß ich einen Blackout hatte... Ich möchte in einer Welt leben, in der niemand mehr aus Angst vor Ausgrenzung und Diskriminierung solche Geheimnisse haben muß."

Ja, das fand ich eine schöne Utopie, und das wurde unsere Lebenseinstellung: Wir schämen uns einfach nicht mehr der Dinge, von denen wir glauben, man bräuchte sich ihrer nicht zu schämen. Wer uns deswegen nicht mag, der soll sich halt andere Freunde suchen. Wir wollen uns nicht verstellen, uns nicht verbiegen oder verstecken, um gesellschaftlich akzeptiert zu werden. Dies ist für mich der ideologisch nachvollziehbare Aspekt der Post-Privacy-Bewegung, die mit Stolz den Namen „Spackeria" trägt – der einzige, denn noch leben wir selbstverständlich nicht in einer Gesellschaft, in der das uneingeschränkt möglich wäre. Der Weg dahin ist offenbar strittig. Inwieweit jeder Einzelne dem genannten Lebensentwurf erfolgreich folgen kann, hängt ganz von seiner Sozialisation, seinem Schamgefühl, seinen individuellen Geheimnissen und deren Verhältnis zu dem ab, was seine Umgebung als „gesellschaftliche Norm" betrachtet. Bin ich schwul und bin ich unabhängig von Menschen, die mit dem Schwulsein ein Problem haben, ist es leicht, mich zu outen. Lebe ich aber in einer Gemeinschaft, in der ich damit rechnen muß, im Falle meines Outings gemobbt oder gekündigt, verprügelt oder entmündigt zu werden, ist der Schritt ungleich schwerer. Meines Erachtens muß jeder für sich selbst individuell entscheiden dürfen, ob und wann er diesen Schritt gehen will; ein Zwangsouting von Privatpersonen in Privatangelegenheiten darf es nicht geben.

Wir müssen bedenken, daß derjenige, der nicht ins Bild von Recht und Ordnung paßt, in unserer Gesellschaft durchaus noch gemobbt, gekündigt, verprügelt oder entmündigt wird. Was legitim und damit legal sein sollte, ist ebenso strittig wie die Frage, was „privat" und was „öffentlich" ist. Wenn Dein Geheimnis ist, daß Du schwul bist, dann hast du heutzutage vielleicht kein so großes Problem mehr mit einem Outing wie vor dreißig Jahren, weil es inzwischen genügend Menschen gibt, die das Schwulsein offen unterstützen, und weil es nicht mehr illegal ist. Aber was ist beispielsweise, wenn du pädophil bist? Wie groß ist die gesellschaftliche Ablehnung selbst gegenüber jenen, die sich nie an einem Kind vergriffen haben oder vergreifen werden! Wie oft werden deine „kleinen Geheimnisse", Deine Verstöße gegen die Norm (z. B. Affären, Drogen, Puffbesuche, illegale Downloads) von Deinen Feinden noch gegen Dich verwendet, wenn es eigentlich um andere Dinge geht, wie etwa das Sorgerecht für Deine Kinder, Deine Tauglichkeit für ein Amt oder die Qualität Deiner Arbeit; Dinge also, die damit nichts zu tun haben?

Sicherlich, jeder hat seine kleinen Geheimnisse. Man könnte meinen, wenn die Gesellschaft



das auch endlich sähe, würde sie schon akzeptieren, was man bisher verheimlichen mußte. Sie würde sehen, daß wir alle an irgendeinem Punkt gegen irgendeine Norm verstoßen, weil sich die Norm eben nicht nach unserer individuellen Persönlichkeit richtet. Dann, so geht die Utopie weiter, könnte mir niemand mehr meinen heimlichen Drogenkonsum vorwerfen, der selbst eine heimliche Geliebte hat... Denkt man, aber so funktioniert es in der Realität nicht. Eine gleichzeitige Offenlegung aller Geheimnisse wird es nicht geben; das ist technisch und logistisch unmöglich. Jede Offenlegung geschieht sukzessive und ebenso jede Anpassung der Norm. Das heißt aber, daß, solange noch niemand von meiner heimlichen Geliebten weiß, ich sehr wohl jemandem seinen Drogenkonsum vorwerfen kann. Schlimmer noch, das könnte ich selbst dann, wenn meine Affäre bekannt wäre – falls ich Drogenkonsum für sehr viel schlimmer halte als Affären und irgendeine mir gewogene Mehrheit das auch so sieht. Wie schwer ein bestimmtes Geheimnis wiegt oder wie weit es von der Norm abweicht, ist aber selbst Gegenstand der Debatte – und somit ebenfalls in Frage zu stellen. Die Norm ist das, was bei der breiten Mehrheit konsensfähig ist, wenn wir als Gesamtgesellschaft darüber diskutieren, was ethisch korrekt ist und was nicht, was legal sein sollte und was nicht und wie hart wir dieses oder jenes Vergehen bestrafen wollen. Daß sich die Mehrheitsverhältnisse in dieser Debatte durch Outings und Tabubrüche in ständiger Bewegung befinden, ist die Grundlage für gesellschaftlichen Wandel.

Wir brauchen unsere Privatsphäre, um die Grenzen unserer gesellschaftlichen Werte für uns selbst zu reflektieren, für uns in Frage zu stellen und gegebenenfalls unseren Dissens mit der gesellschaftlichen Norm (oder sogar der Gesetzgebung) festzustellen. Unsere Privatheit ist ein Schutzraum, in dem wir von gesellschaftlichen Normen und Vorurteilen befreit existieren und uns individuell entfalten können. In ihm können wir neue Ansätze und Ideen von Identität, zwischenmenschlichem Umgang etc. entwikkeln. Ist kein solcher Schutzraum vorhanden, weil jede unserer unausgegorenen, privaten Ideen sofort öffentlich wird, ist eine gesellschaftliche Weiterentwicklung durch bewußten Tabubruch, durch Ausbruch aus der Norm, durch das Infragestellen von Gesetzen nicht mehr möglich. Jede neue Idee beginnt als zartes Pflänzchen und würde von den Fürsprechern der Mehrheitsmeinung sofort erstickt, bevor sie Verbündete finden kann, um gegen die Norm zu rebellieren. Frauen hätten nie Hosen getragen, Homosexuelle hätten nie demonstriert, Urheber hätten nie das Recht auf angemessene Entlohnung bekommen etc. Ein Schutzraum des Einzelnen gegenüber der Gesellschaft ist meines Erachtens notwendig, damit neue Ideen aufkeimen können, damit die ständige Neubewertung gesellschaftlicher Normen und Normverstöße nicht aufhört, damit die Gesellschaft sich wandeln, sich zivilisieren kann.

Selbstverständlich brauchen wir für den zivilisatorischen Prozess Vorreiter: Menschen, die sich outen und es ohne Angst und Scham tun, die ihre Werte verkünden und ihre Rechte einfordern, damit wir uns an ihnen orientieren, uns mit ihnen solidarisieren und ebenfalls stolz darauf sein können, daß wir sind, wie wir sind. Aber dazu brauchen wir ebenso Mechanismen, die uns vor dem Verlust der Privatsphäre und einem Zwangsouting schützen. Denn jeder muß

nach wie vor selbst bestimmen können, gegenüber wem er sich in welchem Umfang offenbart und outet. Nur er selbst kann entscheiden, ob er bereit ist, für seinen Tabubruch das Risiko von Mobbing, Gewalt, Entmündigung, Kündigung oder sogar Gefangenschaft einzugehen. Nur er selbst kann entscheiden, gegenüber wem er bereit ist, dieses Risiko einzugehen. Daher brauchen wir Gesetze, die den Mißbrauch von Daten, das Ausplaudern oder Verwenden von Geheimnissen zum Nachteil des Anderen oder zum eigenen (zum Beispiel wirtschaftlichen) Vorteil unter Strafe stellen. Das meint Datenschutz. Wir brauchen Datenschutz, um einen gesellschaftlichen Konsens über ethische Fragen überhaupt aushandeln zu können, um Menschen den Nährboden und den Mut für ihr Outing zu geben.

Wenn nun die Spackeria meint, wir könnten uns in einer digitalisierten Gesellschaft sowieso nicht davor schützen, daß unsere Geheimnisse ausgeplaudert würden, weil kein Computersystem sicher genug sei, um unsere Daten zu schützen, dann hat sie ohne Frage einen wahren Punkt getroffen, der dringend mal ins gesellschaftliche Bewußtsein rücken sollte. Dies bedeutet jedoch nicht im Umkehrschluß, daß es unnötig wäre, ein solches Vergehen zu sanktionieren. Wir sanktionieren ja auch Diebstahl, obwohl wir Diebstahl nicht verhindern können, weil kein Tresor der Welt absolute Sicherheit bringt. Wir müssen sicherlich diskutieren, in welcher Form wir sanktionieren und was genau, aber daß wir Datenschutz (also Sanktionen gegen Datenmißbrauch) auf der einen Seite und Aufklärung der Bevölkerung über Computersicherheit und technische Möglichkeiten der Datenverarbeitung auf der anderen Seite brauchen, steht meines Erachtens außer Frage. Alles andere liefe darauf hinaus, Zwangsoutings für ethisch korrekt zu erklären, sich zurückzulehnen und zu sagen: „Es ist doch Deine Schuld, daß du jetzt Deinen Job los bist. Was hast Du auch $Person erzählt, dass Du schwul bist? Ist doch klar, daß sich das verbreitet wie ein Lauffeuer und irgendwann auch bei Deinem heimlich homophoben Chef ankommt. Das hast Du jetzt davon, daß Du Dich $Person anvertraut hast; hättest Du Dein Geheimnis mal lieber für Dich behalten!“ Und das ist das genaue Gegenteil der anfänglichen Utopie.

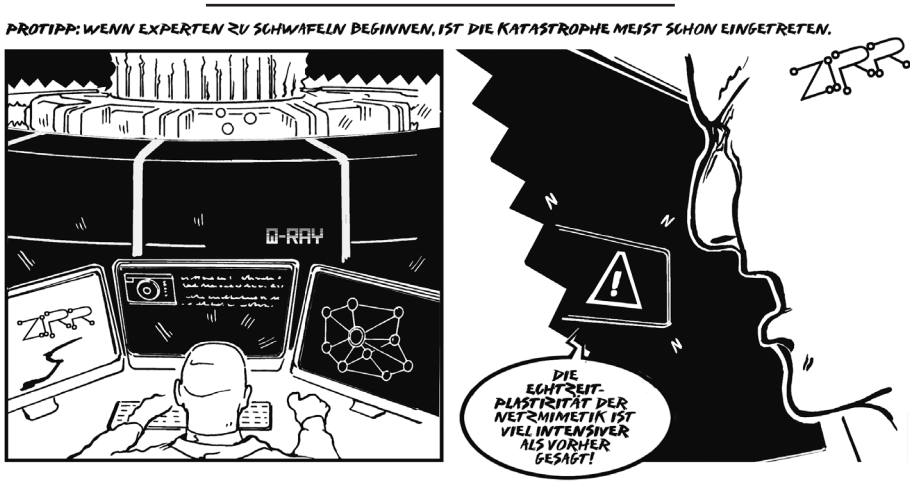
Daher verstehe ich die Position der Post-Privacy-Bewegung, die sich Spackeria nennt, bis heute nicht. Vermutlich handelt es sich, im Gegensatz zu dem, was der Gruppenname suggeriert, in Wirklichkeit um eine Ansammlung von Menschen mit sehr heterogenen Positionen, in der Träumer, die sich eine bessere Gesellschaft wünschen, neben ignoranten Facebook-Fanboys und knallharten Wirtschaftern versammelt sind. [1] Ich könnte mit den Träumern mitgehen, da auch ich es schön fände, in einer Gesellschaft zu leben, in der ich mich für meine privaten Vorlieben nicht schämen muß. Ich fazialpalmiere aber angesichts der Fanboys, die nicht über die Gefahren nachdenken, die ein unvorsichtiger Umgang mit privaten Daten mit sich bringen kann, und ich warne vor den Kapitalisten, die diese Bewegung für ihre Zwecke instrumentalisieren. Denn diese Unternehmer haben ein wirtschaftliches Interesse daran, die Gesellschaft glauben zu machen, daß es nicht sanktionswürdig ist, private Daten gewinnbringend auszuwerten oder zu verscherbeln. Genau dieses Bild erzeugt aber die Post-Privacy-Bewegung: daß Privatheit passé ist und daß das Bedürfnis nach Schutz der Privatsphäre out ist, weil jede private Information, die wir (gegenüber wem auch immer) preisgegeben haben, automatisch zu einer öffentlichen Information würde, die beliebig verscherbelt werden kann. Und das ist falsch! Nicht jede Privatangelegenheit, über die ich öffentlich spreche, wird automatisch zu einer öffentlichen Angelegenheit. Ob ich

Geliebte habe oder in den Puff gehe, ist und bleibt meine Privatangelegenheit, egal ob ich öffentlich darüber spreche oder nicht. Und wem nicht klar ist, daß er mit einer privaten Offenbarung gegenüber seiner Freundin auf Facebook eine andere Öffentlichkeit erreicht als mit einer privaten Offenbarung gegenüber seiner Freundin auf dem heimischen Sofa, der muß dringend darüber aufgeklärt werden. Das ist einfach nicht allen klar, wie auch?

Ich sehe deshalb keinen Sinn darin, daß sich eine Bewegung in expliziter Abgrenzung zum „Datenschutz“ organisiert, beziehungsweise darin, daß aktiv gegen die Werte des Datenschutzes, nämlich Sensibilisierung im Umgang mit privaten Daten und Sanktionierung von Datenmißbrauch, mobilisiert wird. Wer Interesse haben könnte an einer Aufspaltung in Datenschützer einerseits und Post-Privacy-Spackos andererseits, ist mir schleierhaft, wenn man von den wirtschaftlichen Gründen bestimmter Unternehmen absieht. Der Traum von einer besseren Gesellschaft ohne Schamgefühle scheint mir in keinerlei Widerspruch zu den Werten des Datenschutzes zu stehen, im Gegenteil. Um mich dafür entscheiden zu können, das Risiko von Gewalt, Mobbing, Inhaftierung, Entmündigung und Kündigung durch mein Outing einzugehen, muß ich das Risiko abschätzen können. Und um das Risiko abschätzen zu können, muß ich sensibel für die Interessen und Möglichkeiten derjenigen sein, die ich über mein Geheimnis informiert habe, und ich muß über eine Handhabe verfügen, die es mir gegebenenfalls erlaubt, diejenigen zu bestrafen, die mein Vertrauen mißbrauchen und meine Geheimnisse zu ihrem Vorteil oder meinem Nachteil ausplaudern. Nur das erlaubt es mir, Schild und Rüstung abzulegen, meinen Mitwölfen barbäuchig gegenüberzutreten und meinen Traum von einer besseren Gesellschaft ohne Schamgefühle durch mein eigenes mutiges Outing schrittweise zu verwirklichen.

Ich kann in der Spackeria nichts anderes als einen Holzweg sehen. Keines ihrer ehrenwerten Ziele steht im Widerspruch zum Datenschutz, weshalb es mir unsinnig erscheint, hier durch Namensgebung einen künstlichen Antagonismus aufzubauen. Die weniger ehrenwerten Ziele der Spackeria, wie Desensibilisierung für den Umgang mit privaten Daten, Verschleierung des Wirtschaftswerts von Privatheit und Datenerfassung, die Verwässerung der Grenzen zwischen Privatheit und Öffentlichkeit oder sogar die Behauptung, alles höre im Moment seiner Veröffentlichung auf, privat zu sein, haben in mir sowieso keinen Fürsprecher.

[1] Facebook ist nur ein Beispiel, das symbolisch für alle Unternehmen steht, die Wirtschaftsgewinne aus der Verarbeitung privater Daten erzielen.



Aus Gregor Sedlags Liga der Internetschurken, gezeichnet für die digiges. http://comic.digitalegesellschaft.de/

Der Richter und die Cloud

Vortrag von Ermittlungsrichter Sierk Hamann über seinen Streit mit Facebook

von Stefan Schlott <stefan@ploing.de> und
Hanno 'Rince' Wagner <rince@cccs.de>

Sierk Hamann ist Ermittlungsrichter in Reutlingen bei Stuttgart. In der Vortragsreihe des Chaos Computer Clubs Stuttgart berichtete er über seine Erfahrungen mit der Netzwelt anhand eines (inzwischen abgeschlossenen) Falles. Der Fall hatte es bundesweit unter Titeln wie „Richter beschlagnahmt Facebook-Profil" in die Presse und Blogosphäre (mit unterschiedlich korrekten Darstellungen) geschafft (siehe z. B. [0,1]).

Tathintergrund

Im Fall ging es um ein Einbruchsdelikt: Die Familie des Hauses war im Urlaub, lediglich die Tochter blieb zu Hause. Sie wurde von einem Bekannten abends zum Essen ausgeführt; der Bekannte gab dem Haupttäter einen Hinweis, daß die Luft nun rein sei, dieser beging den eigentlichen Einbruch.

Die Verhandlung beschäftigte sich mit dem Mittäter, dem Bekannten der Tochter. Der Haupttäter und der Mittäter hatten in diesem Fall über Facebook und deren Messaging-System kommuniziert. Bei beiden Handys (also Haupttäter und Mittäter) fand man die Facebook-App, beide fand man bei Facebook, wenn man nach ihnen suchte. Allerdings waren auf beiden Handys die SMS-Nachrichten der Tatnacht ab 23 Uhr gelöscht – um Mitternacht wurde der Einbruch verübt. Auf die Frage, warum diese SMS fehlten, erklärten die Beschuldigten, der Speicher sei voll gewesen.

Max Schrems zur Hilfe?

Die Vermutung von Hamann war nun, daß die Täter auch über den Facebook-Chat miteinander kommuniziert hatten; auf den Handys war von einer entsprechenden Kommunikation zwar nichts mehr zu finden, jedoch wußte der technisch interessierte Richter von den Ergebnissen Max Schrems' und dessen Initiative „Europe versus Facebook" [2], daß Facebook sehr großzügig bei der Datenspeicherung vorgeht, die Daten gar um Positionsangaben der Handys anreichert.

Analog zur Beschlagnahmung von E-Mail-Postfächern wollte er die entsprechenden Daten beschlagnahmen lassen (der Beschlagnahmebeschluß ist unter [1] verlinkt). Bei E-Mails ist dies nach seiner Aussage ein gängiges Procedere, bei deutschen E-Mail-Providern sind die Daten so innerhalb eines Tages greifbar. Wer aber war überhaupt der korrekte Ansprechpartner für sein Anliegen?

Facebook ist in Deutschland mit einer GmbH vertreten, die in Hamburg ansässig ist. An diese richtete Hamann zunächst seinen Richterbeschluß. Anstatt einer prompten Antwort erhielt er nur ein (vermutlich automatisiertes) Schreiben einer „Jana", daß seiner Anfrage eine „Record Number" zugeteilt worden wäre. Erst auf hartnäckiges Nachhaken hin versichterte Facebook Hamburg an Eides Statt per Brief, daß es in Deutschland keine Person gäbe, die Zugriff auf diese Art von Daten habe, da die Facebook GmbH in Deutschland nur für Marketing zuständig sei.

Durch den Erfolg von Max Schrems ermutigt, wollte Hamann sein Glück bei der Irischen Niederlassung Facebook Dublin Ltd. versuchen, er stellte ein entsprechendes Rechtshilfeersuchen an die irischen Behörden. Laut „Europe versus Facebook" und den Aussagen des irischen Datenschutzbeauftragten würden die Daten in Irland verarbeitet. Den irischen Ermittlungsbehörden wurde im Zuge von Hamanns Ersuchen allerdings mitgeteilt, alle Daten lägen in den USA,

der Richter solle ein entsprechendes Rechtshilfeersuchen an die USA stellen. Ein Rechtshilfeersuchen bezeichnete Hamann als den „Elefantenpfad“, ein Vorgang, der mindestens ein Jahr dauert und ungewissen Ausgang hat.

Der Widerspruch zwischen den Informationen an die Ermittler und den Aussagen, die Facebook gegenüber den Datenschutzbeauftragten machte, wurde nie aufgelöst.

Paradoxerweise wurde dem Angeklagten selbst ebenfalls die entsprechende Auskunft verwehrt: Er hatte zu seiner Entlastung ebenfalls bei Facebook die Kommunikationsdaten angefragt – vergeblich.

Randnotiz E-Mail-Beschlagnahme

Hamann erläuterte im Zuge des Beschlagnahmungs-Bescheids den Ablauf, der nach gängiger Rechtsprechung für E-Mails angewandt wird. E-Mails werden wie Postkarten betrachtet: Während der Zustellung unterliegen sie dem Fernmeldegeheimnis; sobald sie zugestellt sind, also im Briefkasten des Empfängers liegen, können sie ohne größere Hürden beschlagnahmt werden.

Analog zum Briefkasten wird das E-Mail-Postfach beim Provider betrachtet. Dies war zu Zeiten, als das POP-Protokoll noch vorherrschend verwendet wurde, eine gangbare Analogie. Da inzwischen viele Leute ihr Mailarchiv aus Bequemlichkeitsgründen auf einem IMAP-Server liegenlassen oder gar ihre gesamte Kommunikation über einen Webmail-Anbieter abwickeln, ist heute ein Zugriff auf eine große Menge an sensitiven Daten mit einer relativ geringen richterlichen Hürde möglich.

Hamann merkte hierzu an, daß er als Richter angehalten ist, sämtliche möglichen Mittel zu nutzen; hier divergieren inzwischen aber Technik und Rechtssprechung, so daß es Aufgabe des Gesetzgebers wäre, sich diesen Sachverhalt erneut anzusehen und gegebenenfalls neu zu regeln.

Mögliche technische Winkelzüge für die Zukunft

Facebook weihte im Juni 2013 ein neues Rechenzentrum in Luleå (Schweden) ein. [3] Dieses Rechenzentrum wurde von Facebook USA gebaut und wird auch von Facebook selbst betrieben. Da es sich auf europäischem Boden befindet, wird es interessant, wenn Daten in dem schwedischen Rechenzentrum liegen. Für Richter eröffnet dies eine direktere Zugriffsmöglichkeit.

Bisher völlig unbeachtet sind die Content Delivery Networks – Server in Rechenzentren rund um den Globus, die von Diensten benutzt werden, um deren Inhalte aus Gründen der Lastverteilung möglichst nah beim Kunden zu haben. Bis dato wurden solche Systeme von den Ermittlungsbehörden außer Acht gelassen; es ist eine spannende Frage, was exakt dort gespeichert wird und somit möglicherweise unter deutscher Jurisdiktion zugreifbar ist.

Die widersprüchlichen Aussagen gegenüber den Datenschützern und den Ermittlungsbehörden sind irgendwo zwischen dreist und unverschämt.

Im Interesse beider Behörden muß hier Klarheit geschaffen werden.

Hamann sieht Probleme bei der Ermittlung im Internet, da die (inter-)nationale Rechtsprechung nicht auf cloudbasierte Daten anwendbar ist. Sobald die Daten außerhalb von Deutschland oder gar Europa liegen, ist ein Zugriff schwer, da ein direkter Zugriff deutscher Behörden auf Server im Ausland eine Verletzung hoheitlicher Rechte wäre. Eine (normale) Suchanfrage in einer Suchmaschine ist möglich, da diese Daten öffentlich sind. Chat-Mitschnitte und ähnliches sind es nicht, daher muß über ein Rechtshilfeersuchen (den oben erwähnten „Elefantenpfad") angefragt werden. Da ein Richter be- und entlastende Beweise finden muß, ist es für ihn bei einigen Fällen schwierig, entsprechendes Material zu bekommen.

Soziale Netz-Anbieter speichern alles, dessen sie habhaft werden können. Geodaten sind immer gerne gesehen. Der Wunsch des Benutzers zur Löschung von Daten wird gerne ignoriert – die Daten werden zwar als gelöscht markiert, bleiben aber weiterhin gespeichert. Der (deutsche) Gesetzgeber geht davon aus, dieser Wunsch würde respektiert. Damit schafft eine Firma Fakten, die gegen geltende (deutsche) Gesetze verstoßen – und ignoriert entsprechende Anfragen.

Aus Sicht des Ermittlungsrichters schaden große Firmen der deutschen Rechtsprechung deutlich mehr als die von der Presse gerne hochstilisierten Rockergruppen, da sie einfach deutsches Recht ignorieren und entsprechende Anfragen aussitzen. Damit stellen sich Firmen über das Gesetz.

Äußerst kritisch zeigte sich Hamann sowohl gegenüber den aktuellen Snowden-Enthüllungen als auch gegenüber geheimdienstlichen Methoden wie Stammdatenabfrage, Vorratsdatenspeicherung oder Online-Durchsuchung. Die deutsche Rechtssprechung sei recht präzise und eindringlich, was das Eindringen in den privaten Bereich angeht. Heimliche Ermittlungen, bei denen die Gefahr besteht, daß der Betroffene erst spät oder gar nie von ihnen erfährt, verurteilte er genauso wie die Pauschalüberwachung, welche einem Generalverdacht gegenüber dem gesamten Volk gleichkommt. Es bestünde zwar aktuell ein Defizit, wenn es zu landesübergreifenden Ermittlungen kommt, dies müsse aber so geregelt werden, daß wie bei anderen Ermittlungsmethoden mit „offenem Visier" gearbeitet würde. Grundsätze, die bei einer Hausdurchsuchung gälten (direkte Benachrichtigung des Betroffenen, Gegenwart von Zeugen, Möglichkeit der Rechtsmittel) müßten genauso bei Ermittlungen im Internet gelten.

Fazit

Es war für uns Stuttgarter interessant, einmal die Sicht, die Möglichkeiten, aber auch die Sorgen und Nöte der „anderen Seite" zu sehen. Der Appell von Richter Hamann, Ermittlungen mit „offenem Visier" zu ermöglichen und dafür im Gegenzug auf fragliche, geheimdienstliche Methoden wie Vorratsdatenspeicherung und Online-Durchsuchung zu verzichten, stimmt nachdenklich. Seiner Aussage nach ist das „normale" Verfahren mit Quick Freeze völlig ausreichend.

Und der Fall selbst? Er wurde inzwischen abgeschlossen, da der Haupttäter ein Geständnis abgelegt hat. Das Verfahren gegen den Mittäter wurde eingestellt, da er inzwischen sozial integriert ist und eine Ausbildung macht. Richter Hamann hat bis heute die angefragten Daten von Facebook nicht bekommen.

[0] DPA: „Richter beschlagnahmt Facebook-Account" *http://www.stern.de/digital/online/internetrecht-richter-beschlagnahmt-facebook-account-1789200.html*

[1] T. Stadler: „Amtsgericht lässt Facebook-Account beschlagnahmen" *http://www.internet-law.de/2012/02/amtsgericht-lasst-facebook-account-beschlagnahmen.html*

[2] Initiative „Europe versus Facebook" *http://www.europe-v-facebook.org/*

[3] Slashdot: „Facebook Saves Datacenter Costs with Frigid Arctic Wind" *http://slashdot.org/topic/datacenter/facebook-saves-datacenter-costs-with-frigid-arctic-wind/*


INTERNET
OFF
ON
INTERNET SWITCH MUST BE ON AT ALL TIMES
11-0866-501