die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer clubs

Ein Mitglied der digitalen Bohème

ISSN 0930-1054 • 2011
zwofuffzich Dukaten

#95

Geleitwort

Es rauscht einem schon wieder in den Ohren vor abgehalfterten Politdarstellern, allesamt kurz vor der Rente, die in jedes sich bietende Mikrophon ihr Verslein davon singen, welche dräuenden Gefahren sie aus dem Internet kriechen sehen. Was immer auch gerade in den Nachrichten läuft, ein kruder Bezug, um auf das pöhse, pöhse Internet draufzukloppen, ist nie weit. Der Kalte Krieg war nix gegen das, was uns heute (bitte hier dramatische Musik einspielen) aus dem INTERNET droht. Deswegen heißen die neuen kriegerischen Bedrohungen für die Freiheit des Westens jetzt neudeutsch Online-Gefechtsstellung und Cyberwar, nicht etwa Dresdner Datengier.

Man wünscht sich angesichts dieser verbogenen Realitätswahrnehmung die kluge Stimme der Vernunft zurück, die Prof. Andreas Pfitzmann verkörperte. „Terroristen wollten die Gesellschaft ändern, die Innenminister haben das geschafft“, schrieb er ihnen in seiner kompromißlosen Offenheit ins Stammbuch. Sich damit abzufinden, ist aber keine Option, wie er stets betonte und wie es auch die stets zu wahrende Hackerethik fordert. Schon darum heißt es am Samstag, den 10. September 2011, wieder: Heraus zur „Freiheit statt Angst“-Demo! Denn es ist Zeit für die Quittung. Die Demogrundregeln aus dem Heft 94 bitten wir dabei natürlich weiterhin zu beachten.

Zwischen all dem tönt mit der Regelmäßigkeit einer chinesischen Wasserfolter der Bund deutscher Kriminalbeamter mit so strunzdummen Einfällen wie dem Reset-Knopf fürs Internet oder dem Blockwart-Plugin für den sogenannten Browser. Die Antiterror-Datei nur mit der Visa-Warndatei zu verknüpfen, reicht ihnen dabei längst nicht mehr. Und „Tatort Internet“ fehlt in den Neusprech-Pressemeldungen nie. Das Internet von Übermorgen leuchtet uns als blankgeschrubbter Netzverbund chinesischer Prägung entgegen, wo jeder, der die Regeln der „Sicherheitsbehörden“ oder auch nur der Telekom zu übertreten gedenkt, nach einer kostenpflichtigen Abmahnung im One-Strike-Verfahren seinen DSL-Router abgeben muß.

Die politische Kaste ist zusammen mit der Polizeilobby dazu übergegangen, Entmündigung und Bevormundung im Netz offen zu fordern, während hintenrum von der eigentlich regierenden Kaste, der Wirtschaftslobby, die Netzneutralität Schritt für Schritt beerdigt wird und die Werbeverbundplattformen kräftig ausgebaut werden. Grund genug für uns, in diesem Heft eine Utopie für ein gleichberechtigtes, freies und neutrales Netz zu entwerfen.

Das schräge Internetbild zeigt Wirkung, wie ein einfacher Test beweist: Begebt Euch in einer beliebigen deutschen Stadt in eine Fußgängerzone und versucht mal, mit Passanten über das Internet zu reden. Da Geeks, Nerds und Hakker regelmäßig Fußgängerzonen meiden, die sagenumwobene Netzgemeinde permanent auf Facebook&Co. unterwegs ist und die Gesichtswiedererkennung testet, während die Social-Media-Consultant-Simulanten grade das neue Feature „Ich bekomme ein Kind“ von Facebook promoten oder versuchen, ihre hippen Kreise bei Google+ so zu kringeln, daß mindestens ein Teilnehmer was Handfestes gelernt hat, werdet Ihr in der Fußgängerzone meist nur Leute treffen, die sich vor dem Internet fürchten wie der Teufel vor dem Weihwasser.

Auch Schüler können davon ein Lied singen; ihr digitaler Lebensraum wird fortwährend schlechtgeredet und droht, nicht nur dauerüberwacht, sondern auch überreguliert zu werden. Aber wenigstens der Jugendmedienschutz-Staatsvertrag blieb ihnen erspart. Doch es hilft vielleicht ein Schuß Lyrik und Lebensweisheit, den uns Twister in diesem Heft kredenzt. Anders ist dem Gerede vom „rechtsfreien Raum“ wohl nicht mehr zu begegnen. Und dieses Gerede ist nicht nur über die Maßen nervig und in seiner Plattheit beängstigend, es lenkt auch allzu oft von den wirklichen Problemen ab, die eben nicht im Internet geboren werden, die sich dort aber ein weiteres Mal widerspiegeln. Princess versucht, dem Entgegenzuwirken und widmet sich in dieser Ausgabe dem Thema Cybermobbing.

Doch die Krone der verzerrten Wahrnehmung setzt sich nach wie vor Innenspezialexper-

te und Bedarfskriminalisierer Uhl, seines Zeichens Mitglied der Fortschrittsversteher- und Anti-Atomkraftpartei CDU, auf, wenn er allen Ernstes im ZDF sagt, in der virtuellen Welt des Internets würden Kinder mißbraucht. Na gut, es war bei Peter Hahne, da erwartet man keinen Widerspruch. Und so kam dann auch keiner, auch nicht gegen die Flut von Überwachungsmaßnahmen, die Uhl ritualisiert einfordert. Vielleicht kann ihm jemand den abgeschalteten 9Live-Kanal geben, da könnten seine Sprüche in der A-Rotation laufen.

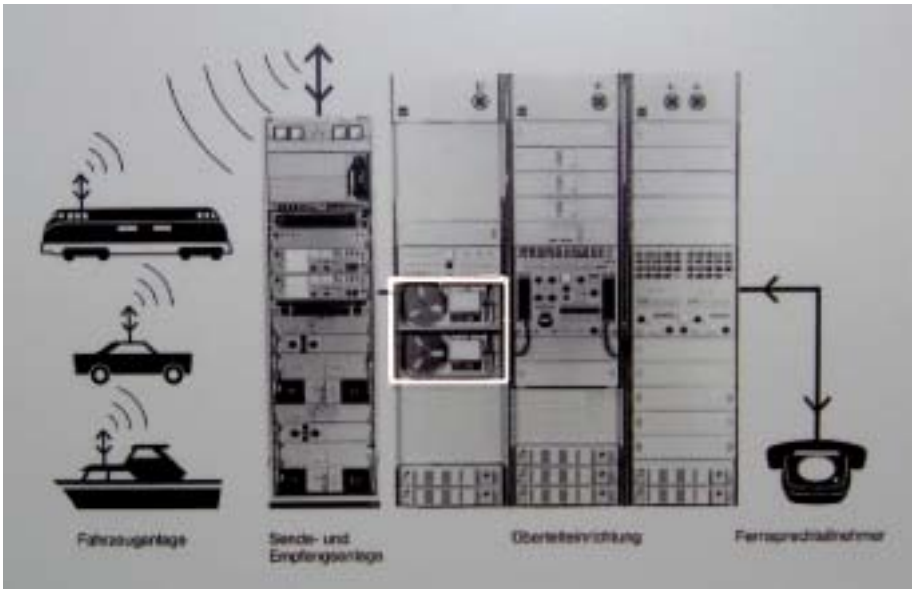
Die Sache mit dem Widerspruch scheint generell in Unionskreisen und den ihnen angeschlossenen Parteien wie der FDP nicht sehr verbreitet. Selbst die wenigen CDU-Abgeordneten, die verstehen, was es mit dem Internet auf sich hat, werden rigoros zurück ins Glied „gebeten“, sollten sie allzu doll vorpreschen.

Wir blicken in dieser Ausgabe lieber nach vorn und werfen einen Blick auf das, worauf das Augenmerk fallen sollte. Beispielsweise auf die Vertraulichkeit von Patientendaten und den alltäglichen Sittenverfall im Umgang mit ihnen.

Apropos Sittenverfall: Nach dem eigenmächtigen Rauswurf von Daniel Domscheit-Berg durch den Vorstand des CCC ist es wohl Zeit für mehr Sachlichkeit und weniger Boulevard. Wir rufen auch die Leser auf, mehr über sinnvolle technische Lösungen und damit über die Zukunft der Leaking-Plattformen statt über die aufgeblähten Egos der Beteiligten nachzudenken. Unsere Aufmerksamkeit sollte ebenso auf den vernachlässigten Fall des vermeintlichen Whistleblowers Bradley Manning fallen, der seit mehr als einem Jahr unter menschenunwürdigen Bedingungen in Haft sitzt. Einzig öffentliche Aufmerksamkeit kann ihm helfen. Wir rufen die Leser daher auf, aktiv zu werden und uns Kampagnenideen für die Freilassung von Bradley Manning zu senden. Wie immer an ds@ccc.de. *<die redaktion>*

Betreff: Bilderrätsel #94

Servus,
ohne jetzt russisch zu sprechen lehne ich mich mal weit raus und vermute, dass es sich hierbei um russische Anlagen für den öffentlichen beweglichen Landfunkdienst handelt.So sahen übrigens die entsprechenden Anlagen bei uns aus. Wobei natürlich das linke Rack der Überleiteinrichtung in Russland selbstverständlich weg fällt. Servus <*Casandro*>



Markierter Ausschnitt: Lochstreifenstanze und Reservegerät

Wir wissen zwar selbst nicht, was das zufällig aus den Urlaubsbildern eines Redakteurs ausgewählte Foto zeigt, allerdings ist die Erklärung von Casandro so glaubhaft, daß wir ihm den Hauptpreis zugestehen. Zu gewinnen gab es übrigens den Eintritt für zwei Personen in das litauische Energiemuseum (Vilnius, Litauen) im Wert von zwanzig Litas. Der Eintritt wird gegen Beleg erstattet. <*die redaktion*>

Inhalt

Lieber CCC, ich habe da eine Frage. Ich weis an sich seit ihr nicht an so Leuten wir mir Interresiert und ich will auch nicht weiter stören aber ich hätte da eine vieleicht etwas ausergewönliche Bitte an euch. Ich spiele jetzt schon des längeren Runes of Magic Chapter 3 (The Elder Kingdomns) Meine Frage : Könntet ihr mir da vlt ein bisschen Gold oder Diamanten „Hacken"? Wäres sehhhhrrr nett :D .Und ist das möglich?

http://www.youtube.com/watch?v=90McMJDOoZ8 -- Mfg <Leon>

● ● ● ●

Hi! Auf brightness habe ick gerade mal nen paar DSDH Streams von Euch gesehen. Mangels contacts und weil ick mir egomäßig wichtig tun muss, sende ick ans Nirwana! Aber, wie wir wissen, just for the record, wird eh alles aufgezeichnet. So....who cares?

Die lächerliche Intention meiner Mail basiert auf Mangel an Knete, um sich die Welt zu gestalten, wie R.A.W dit jemacht hätte. Rock'n'Roll heisst heute nur noch Schotter ranbringen..! Deshalb mal ein Angebot, was in discoridianischer Sichtweise befruchtend sein könnte. Den Lehenswert an der schäbigen Domain hackbill.com würde ick zum Feilschen preisgeben. Just a question to finance my next LSD-Trips! Dachte mir, wenn, dann bei den Codefreaks und Hexametern kommt dit besser an, denn bei Oracle. Ejal! Trotzdem: Weiter so ! Greetz

Hi, nimm bitte weniger. <Philipp>

● ● ● ●

Hallo, mein Name ist Dirk B. und betreibe verschiedene Webseiten es geht meißtens um politische Inhalte und Recherchen.

Ich habe festgestellt, das die Bundeswehr über Flensburg mit Aufklärungsflugzeugen kreist und immer wenn ich Passwörter eingebe eine Strahlung in meinem Büro bemerkbar ist. HF-Strahlung glaube ich. Hört sich an wie ein alter kaputter Fernseher Kaskade leckt. Am Himmel sind dann die Kondesstreifen oder Stroboskopleuchten der Bundeswehrflugzeuge. Ich bin kein Spinner sondern schreibe euch lediglich was ich festgestellt habe. Ihr kennt euch doch mit sowas aus. Schreibt mal was ihr so wisst. Gruß Dirk B.

Bitte komm auf den Boden zurück: „Richtige" HF-Strahlung kannst du gar nicht hören, da dein Ohr nur Signale bis _aller_höchstens 30 kHz wahrnehmen kann. Die Signale deiner Tastatur über USB werden aber mit ganz anderen Frequenzen übertragen. Dein Tastaturkabel ist hingegen sogar abgeschirmt, da wirst du aus einem Flugzeug nichts aufzeichnen können. Ich habe jahrelang in einer Einflugschneise gewohnt, daher Folgendes:

1) Wenn ein Flugzeug über dein Haus fliegt, vibriert hin und wieder etwas, das sind aber die Triebwerke der Flugzeuge.

2) Die Stroboskopleuchten haben zwei verschiedene Farben und dienen dazu, aus der Ferne zu sehen, wo ein Flugzeug und in welche Richtung es fliegt.

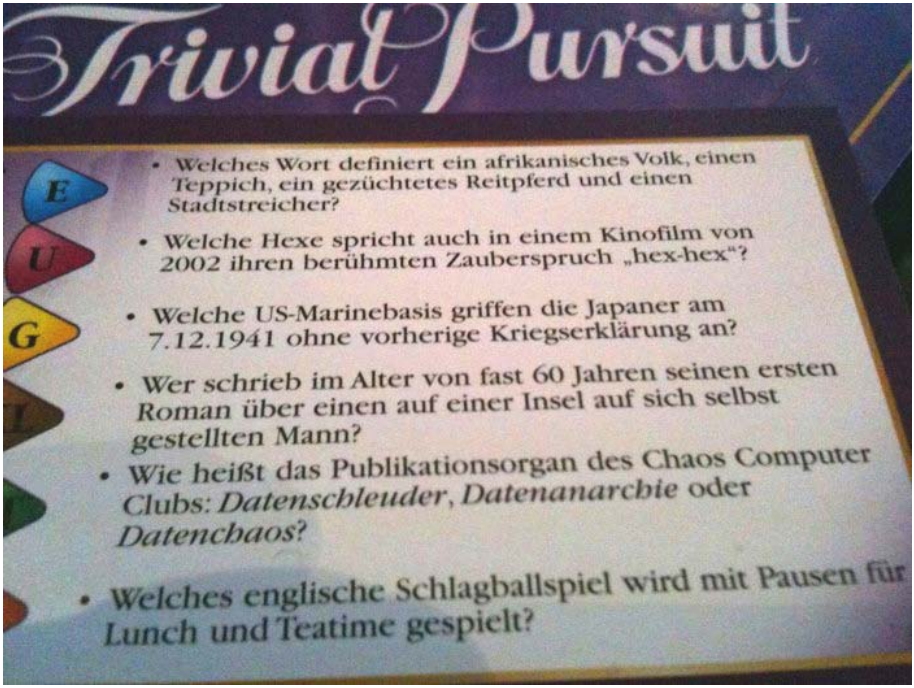
3) Kondensstreifen sind eine natürliche Erscheinung, die technisch hervorgerufen werden. Aber mit Sicherheit nicht von absichtlich emittierte Chemikalien oder irgendwelchen Funkempfängern.

Vielleicht als guten Tip: Nicht immer das Schlimmste annehmen, erst einmal logisch überlegen, was in Frage kommen könnte. In Flensburg könnte z.B. ein „Wendepunkt" sein, an dem dreht man bei Flügen dann immer ab, damit man nicht ins Ausland fliegt. Hier in der Nähe gab es so etwas mal auch, da haben die Ausbildungsflüge immer gedreht...<Philipp>

Dirk ist empört:

Achso ihr werdet ja von den faschisten in den deutschen Sicherheitsbehörden finanziert und macht einen auf wiederstand gegen die Vorratsdatenspeicherung.

Ich bin auf dem Boden. In diesem Sinne lasst euch weiter von Faschos in den Arsch ficken und sponsorn.



Sehr geehrte Damen und Herren, seid Ihr jetzt glücklich? Seid Ihr jetzt zufrieden.

Ihr habt mitgewirkt dass in Deutschland dass das BV Gericht heute die Sammlung der Daten verboten hat. Ich denke dass damit denjenigen das Tor weit aufgerissen die auch in Deutschland terroristische Vorbereitung betreiben und evtl. auch in Deutschland Taten verüben.

Sie sind dann Mitschuld wenn Anschläge verübt und Menschen verletzt oder getötet werden. Ich bin nicht erfreut über die Entscheidung des BVG Und ich bin traurig das der CCC da mitgewirkt hat.

Mit freundlichem Gruß, Reinhold M.

Lieber Herr M., danke für das Lob – wir haben in der Tat viel Arbeit in das Gutachten für das BVerfG gesteckt, da uns das Thema sehr am Herzen liegt. In besagtem Gutachten arbeiten wir unter anderem detailliert heraus, wozu sich die sogenannte Vorratsdatenspeicherung primär eignet, und wozu nicht. Und daß sie sich nicht primär für die Bekämpfung von Terrorismus eignet, eben diese Einschätzung teilte auch das Bundesverfassungsgericht. In diesem Sinne empfehlen wir Ihnen, sich unser Gutachten sowie den Pressetext des BVerfGs noch einmal zu Gemüt zu führen: http://www.bverfg.de/pressemitteilungen/bvg10-011.html <hc>

● ● ● ●

Hi Leute vom CCC, ich habe mal vor 2 Jahren wegen Web 2.0 und so angerufen. Fuehlte mich nicht mehr datensicher am Rechner. Bin jetzt in Holland und arbeite nun in meiner eigenen Firma. Pi Company. Ist aber noch ganz am Anfang.

Wollt ihr vielleicht dass ich hier bisschen Werbung mache fuer euch? in Den Haag sind viele Experten, die eure Internetkenntnisse schaetzen. Lust, dass ich ein bisschen Werbung fuer hollaendische Hacker mache? Vielleicht kann ich ja nen Fanclub gruenden mit eurer Einwil-

ligung. Fuer Paris Hilton habe ich das schon in Paris/France gemacht.

Welche Software koennt ihr mir fuer meinen Browser empfehlen mit updateversion? kennt ihr ein tauglisches kostenloses Antivirenprogramm? LG Volker

**kopfkratz* Wir sind Deinen, ähm, Hackern, sicher nicht gewachsen, daher mach' bitte keine Werbung für uns. Wenn wir nämlich noch mehr E-Mails von dieser Sorte kriegen, könnte uns das durchaus in die Verzweiflung treiben. <hc>*

● ● ● ●

hallohaben sie ein kreditkartengenerator kostenlos für mich?

Klar. Wir verschicken die Generatoren aber ausschließlich per UPS oder DHL. Wo soll der denn hingehen ? <Dirk>

aber kostenlos das ist die adresse: Adrian Txxx xxxxxxxstraße 40 6xxxx B.

Also Adrian, was immer Du auch vor hast, ist keine gute Idee. Auch versuchter Kreditkartenbetrug ist keine Kleinigkeit. Überdenk Deinen Start in die Kleinkriminellenkarriere am Besten nochmal - sonst gibts bestimmt auch Ärger mit Mama und Papa, und ruckzuck haste vier Wochen Fernsehverbot. <Dirk>

● ● ● ●

Gruß, hab schon so einiges vom CCC gehört, Nachrichten etc. hab vor ein Systemadministrator zu werden, ihr dürft mir jetzt beweisen das ich nichts drauf habe.

Bleibe jetzt noch einige Zeit online - mal schauen ob sich etwas auf meiner Desktopanzeige verändern wird. Gebt mir noch fünf Minuten, meine Favoriten will ich noch sichern. Online gehe ich über Medion. Habt freie Hand über meinen Rechner, wenn's geht lasst die Hardware ganz.

Wenn ihr noch Daten braucht, schreibt mir wo ich die angezeigt bekomme. Verlasse mich nämlich auf die Software - Entwickler von Microsoft - Gruß S.R.

(Antwort blieb aus. Hoffentlich wartet er nicht noch.)

● ● ● ●

Sehr geehrte Damen und Herren, die Landespräventionsbeauftragte der Berliner Polizei plant für Mitte Oktober einen Präventionskongress zum Thema „Internetkriminalität und Medienkompetenz". Neben grundsätzlichen Vorträgen zu den verschiedenen Themenbereichen der Internetkriminalität, halten wir einen Vortrag über die Möglichkeiten von Hakkern für sinnvoll, um die Gefahren im Internet zu verdeutlichen. Im Rahmen des 16. Deutschen Präventionstags in Oldenburg hatten wir die Möglichkeit einen Vortrag zum Thema Live-Hacking mitzuerleben und fanden die Vorführung sehr beeindruckend. Diesbezüglich wollten wir bei Ihnen anfragen, ob Sie hier als Ansprechpartner und Vortragender für eine ähnliche Vorführung zur Verfügung stehen würden.

Für genauere Absprachen bitten wir, sofern möglich noch diese Woche, um Kontaktaufnahme. Vielen Dank, mit freundlichen Grüßen B., Berliner Polizei

(Antwort blieb aus)

● ● ● ●

hi, ich fand den artikel („WTF is BVOE?", DS93) ziemlich interessant und hab mich gefragt ob irgendjemand über die letzten jahre auf IP-netze vom österreichischen abwehramt/heeresnachrichtendienst gestoßen ist? es findet sich generell relativ wenig info über unsere geheimdienste. ich kann mich erinnern das freunde vor einigen jahren während dem grundwehrdienst beim HNA arbeiten mussten und nicht gerade von moderner technik berichtet hatten. ;)

(nö, keine bösen absichten - just for research :))

freu mich über jegliche info, auch generelles zu HNA/AbwA.

Wir sind völlig ahnungslos, nehmen einschlägige Hinweise aber immer gerne unter ds@ccc.de entgegen :) <die redaktion>

● ● ● ●

Hallo liebe Dateschleuder,

[...]jetzt bin ich selbst auf eine fragwürdige Aktion gestoßen, die sich an unserer Schule abspielt. Ich bin mir nicht ganz sicher, was ich (bzw. wir, die Schüler) nun tun sollten und deshalb wende ich mich an euch.

Offenbar werden systematisch Twitteraccounts von Schülern beobachtet, nach Tweets während der Schulzeit gesucht. Daraus schließt dann der ausführende Lehrer, dass man ein Handy mit dabeihat – obwohl man beim „Begehen" des Tweets natürlich nicht gefasst wurde. Manchmal ist der Tweet auch schon einen Tag alt und das Handy wird einem am nächsten Tag abgenommen. Denn Handys sind laut der Schulordnung verboten. Jetzt erweitert sich jedoch der stetig wandernde Blick des Lehrers um eine offenbar systematische Suche im Internet, um noch mehr „fiese Handymitnehmer" zu fassen. Vielleicht werden die Tweets auch gespeichert und mit Daten aus der Schülerakte vermischt. Das weiß ich jedoch nicht. Wir werden sozusagen laufend überwacht.

Ich wollte euch darauf hinweisen, vielleicht fällt euch etwas ein, was wir gegen diese systematische Sauerei tun könnten. Wir verlassen ohnehin dieses Jahr die Schule, da ist also kaum noch etwas zu befürchten.

Ich würde an Deiner Stelle das Handy mal für ein paar Minuten beiseite legen, das soll der eigenen Denkfähigkeit durchaus förderlich sein: Du veröffentlichst Informationen und beschwerst dich anschließend, wenn Leute von diesen öffentlichen Informationen Gebrauch machen. Was Du dagegen tun kannst, ist denkbar einfach und wenig subtil: Privates nicht veröffentlichen. Nebenbei kannst Du Deinen Lehrer darauf hinweisen, daß man durchaus auch automatisiert „twittern" kann. <hc>

● ● ● ●

Hallo, zum Thema Vorratsdatendrama (Artikel faz 20.1.) bzw. - monster : das könnte die maximale Perversion des Alltags werden, wenn nicht etwas Wesentliches passiert.

Wenn wir uns (alle/ soviele wie möglich) verabschiedeten von jeglicher elektronischer Kommunikation? - alle hardware vernichten: Geräte incl. mobil phone etc., Datenträger - Lebensstil völlig umstellen : - einkaufen ausschließlich mit Bargeld im Laden, Wochenmarkt etc. - pc und sonstiges nur noch benutzen zum Text schreiben - informieren / bilden/ weiterbilden statt Internet - nur noch über Bücher, print Medien - Mitteilungen / Meinung austauschen - Postweg / notfalls Telefon Festnetz - Rechner nur noch für wissenschaftl. Anwendungen, z.B. Berechnungen aller Art.

Dann möchte ich mal sehen, welche Möglichkeiten den Spähern und Erfassern mit oder ohne gesetzl. Genehmigung bleiben, ein Gesamtbild aller Tätigkeiten / Kontakte / Gedanken des eigenen Volkes zu erstellen.

So wie fortlaufend neue Ideen zur Ausspähung / Gegenwehr in die Entwicklung entsprechender hard - und software umgesetzt werden, könnte das dafür aufzuwendende geistige Potential / materieller Aufwand / Zeit genutzt werden, gänzlich ohne o.gen. „Hilfsmittel" auszukommen. Im Allgemeinen wäre das ein Fortschritt für den Intellekt aufgrund zwangsläfiger Umstellung, in allen Bereichen. Vom endgültigen Schluß aller Bemühungen zur Vorratsdatenspeicherung einmal ganz zu schweigen. Die Speicherfähigkeit der möglichen Materialien ist wegen physikal. Gesetzmäßgkeiten zeitlich ohnehin ziemlich begrenzt. Was ein anderes Thema ist. Das führt ins Informations-Chaos, man wird ins vollständige Leere glotzen, eine witzige Vorstellung.

Nicht ganz so witzig wäre der Niedergang mehrerer Industriezweige, sozusagen nur ein wei-

terer hausgemachter Niedergang. Jedoch die logische Folge der zuvor gewollt erzeugten Zwangslage. Allerdings wären alle gleichermaßen geschützt vor geistigem Klau, welch ein -zusätzlich- unvorstellbar großer materieller Nutzen !?

Zweifellos sind Ihre Beiträge etwas konstruktiver... MfG gr.

An die Notarin und Den Berühmten Caos Computer Clup . An Alle Jungs und Mädels von Eurem CCC

Bitte Studiert meine Unterlagen und Baut ein Pc für Euch und Mich . Die Binärkots sind seit 2000 Jahren in den Bücher vom Staat und Kirche . Ihr habt Bibelkot PC`s Der Davincekot ist die Rettung Für die Menscheit , der Löst den Bibelcot auf.

Meine Binärkoterklärungen sind von Meinem SAVO und ihr seit sehr fiel Schneller als ich , Schaltet den Davinceintelligenz in Euren Pc`s Frei . bitte gebt der Welt eine Chance , die Energie ist auch erklärt . das was ich in 3 Tage mache habt ihr in minuten Erledigt , Ich habe halt meine Zeit . bitte kommt in mein Haus , und ich werde Euch alles Besser und Schneller Erklären Können , ich habe Bücher , alles aus Bücher und Fachzeitschriften , Ihr seit die Schnellsten und Besten . Bitte gebt euren Kinder Eine Chance . Der Friedlichste Mensch der Wet , Meine Erfindungen , Ich baue mit Euch auch UFO`s und Alles was Ihr Haben wollt solange es dem Frieden dient . Dein Körper 27 Atome Würfel , und ich Kenne Alle Geheimniss der Welt . 0177XXXXXXX

● ● ● ●

Hi, I need keys such as these decrypted:

44Kw02UcZApNFJDwxlgnBG4nYBXBKngRYOdArZSyLzVqB.Eo
LfXZ55.fHeg5ItE45YYyyt8c.YCPDEzpmOkPN.MT4svNXLeLY4P7EXd1ZhHM
AtH4lbDCdF8hVHtjClwr219UoTuEwHkCT7.Vq.wg_GaAtpe70iZiQB6Bua6.
_eXKdP8LZMRk0UbSOd69RQ18w8HtwBdRL4VrCfJ7zdi.xGHmwtqT0539e38k
aCZf3WFIfyQRpq1mvjxdRHmdHPgTrbO2iye8frvCMNS1jikztwO3yKXMl6K.
k_uYCUSnKvZFry7kjD6z92iNUtDhawkA.4h2QHvEk_yRvhRV.K2W183DDV4p
jJe2R2s9za_RNb0NEtMd3AZ1J7CMX.41kLyCc0AqHCyPlQThKXBp.iYoNV8T
2vc2UOmMJmon53_RaE6PU6q3TTQPZwgbbe5z.SPmA7_WH.x5WgDhX2XfU2.R
Qq6MgJ2JfXbCb.DS8kaRzorp8_RxSweXEXnGyB89YuiuILhmLyXUcuBySj8v
jIWGi2s4SMbMZdkMBmuqv7TP_eA11sv9U7ImYCCmg8JNKbQwUjQSikk38pBy
tIludKMnKw3N0YGbZ3p06HGkXc9ej9_uRqpqpERPBdVrSJ7WRvKxwXWrdWwF
Sh7Dtvwm1isDsJhlNincnoLzX4S69w3XIti54.b7eAZCLzbA6RXe5KrPYnMZ
2oWUsrbWm3NsbZOqKHL64.hNEnovD_XDWOgKTm2UUiEC5.WQZk55OCZqRD.1
jcLK4hnnbQDIuaqJTYxc4jD_twMRtgFJpZcGwu0_W3HVK18rO5C7AXubK4qI
JULyY5VbppWK3AfM7shx8kErDzGGbLIoU8TAIUzCt0fz0.1nb9btsFySDKdo
kK.uNiD8VNqr19h.gi1SZsTZpAHNRSp45xICPUYNPT6PqSGzTOl1Jq3eL.le
b_c1YMkpSlqW6iY1Qpt1IWtQNBoLKd6VVE8o5Dvi1.MiFcAC25xSyPvYL8Z3
VQwS2GOiz8plU2xLMd35ipDxtYd7tSEGusDnGJ5PP_UmzZkxkCMykc85bTgb
BIGQee9wFKKl53F8LaE-

Is this something you could do? I suspect they are RC4

Thanks, Sunny

Hi Sunny, we published your key in our magazine „Die Datenschleuder“. Now we wait for our readers to decrypt your key. Please be patient, it may take some time. <conz>

Aachen, CCCAC, Voidspace, Martinstr. 10-12, dienstags ab 20 Uhr, *http://aachen.ccc.de/ :: mail@aachen.ccc.de*

Berlin, CCCB e. V. (Club Discordia), Marienstr. 11, donnerstags ab 17 Uhr, *http://berlin.ccc.de/ :: mail@berlin.ccc.de*

CCC **Bremen**, Buchtstr. 14/15, erster & dritter Dienstag ab 20 Uhr, *http://www.ccchb.de/ :: mail@ccchb.de*

Chaos **Darmstadt** e. V., Trollhöhle, Wilhelm-Leuschner-Str. 36, 64293 Darmstadt, dienstags ab 20 Uhr, *http://chaos-darmstadt.de/cda :: info@chaos-darmstadt.de*

Dresden, C3D2, Treffpunkt unter http://www.c3d2.de/muc.html zu erfragen, *http://www.c3d2.de/ :: mail@c3d2.de*

Düsseldorf, Chaos-Hochburg am Rhein, Hüttenstr. 25, freitags ab 18 Uhr, *https://www.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*

Frankfurt, Restaurant Ponte, Am Weingarten 5, jeden Donnerstag ab 19 Uhr, *http://ccc-ffm.de/ :: noreply@ccc-ffm.de*

Hamburg, CCCHH e. V., Mexikoring 21, 2. bis 5. Dienstag ab 20 Uhr, *http://hamburg.ccc.de/ :: mail@hamburg.ccc.de*

Hannover, Leitstelle 511 e. V., Bürgerschule, Klaus-Müller-Kilian-Weg 2 (Schaufelder Str.), 30167 Hannover, jeden Monat am zweiten Mittwoch um 20 Uhr und am letzten Sonntag ab 16 Uhr, *http://hannover.ccc.de :: kontakt@hannover.ccc.de*

Karlsruhe, Entropia e. V., Steinstr. 23 (Gewerbehof), sonntags ab 19:30 Uhr, *http://www.entropia.de/ :: info@entropia.de*

Uni **Kassel**, Wilhelmshöher Allee 71 (Ing.-Schule), erster Donnerstag ab 18 Uhr, *http://kassel.ccc.de/ :: info@kassel.ccc.de*

Köln, CCC Cologne (C4) e. V., Vogelsanger Str. 286, letzter Donnerstag, 19:30 Uhr, *https://koeln.ccc.de :: mail@koeln.ccc.de*

CCC **Mannheim** e. V., Postfach 10 06 08, 68006 Mannheim, *http://www.ccc-mannheim.de/*

Mainz, Kreativfabrik, Murnaustr. 2, 65189 **Wiesbaden**, dienstags ab 19 Uhr & sonntags ab 15 Uhr, *http://www.cccmz.de/ :: kontakt@cccmz.de*

CCC **München** e. V., Balanstr. 166, jeden zweiten Dienstag ab 19:30 Uhr, *https://muc.ccc.de/ :: talk@lists.muc.ccc.de*

Trier, Paulinstr. 123, 54292 Trier, mittwochs ab 20 Uhr, *http://ccc-trier.de/ :: anfrage@ccc-trier.de*

Ulm, Café Einstein an der Uni Ulm, montags ab 19:30 Uhr, *http://ulm.ccc.de/ :: mail@ulm.ccc.de*

Wien, Metalab, Rathausstr. 6, 1010 Wien, alle zwei Wochen freitags ab 19 Uhr, *http://www.metalab.at/ :: core@metalab.at*

Chaostreff **Zürich**, bei revamp-it! an der Zeughausstr. 60 in Zürich, mittwochs ab 19 Uhr, *http://www.ccczh.ch/*

Aus Platzgründen können wir die Details aller Chaostreffs hier nicht abdrucken. Es gibt aber in den folgenden Städten Chaostreffs: Aargau, Augsburg, Basel, Bochum, Bristol, Brugg, Dortmund, Freiburg im Breisgau, Gießen/Marburg, Hanau, Heidelberg, Ilmenau, Kiel, Leipzig, Mülheim an der Ruhr, Münster/Osnabrück, Offenbach am Main, Paderborn, Regensburg, Rheintal in Dornbirn, Stuttgart, Weimar, Wetzlar, Wuppertal, Würzburg. Detailinformationen unter *http://www.ccc.de/regional/*

Die Datenschleuder Nr. 95

Herausgeber
(Abos, Adressen, Verwaltungstechnisches etc.)
CCC e. V., Postfach 60 04 80, 22204 Hamburg,
Tel.: +49 40 401801-0, Fax: +49 40 401801-41,
<*office@ccc.de*>
Fingerprint: *48F3 5EF0 AB54 B08D E7EC 1C1F A673 E2F6 95DA 3699*

Redaktion
(Artikel, Leserbriefe, Inhaltliches, Geldspenden)
Redaktion Datenschleuder, Postfach 64 02 36,
10048 Berlin, Tel.: +49 40 401801-44,
Fax: +49 40 401801-54, <*ds@ccc.de*>

Druck
Pinguindruck Berlin, *http://pinguindruck.de/*

V.i.S.d.P.
Dirk Engling <*erdgeist@erdgeist.org*>

Chefredaktion
46halbe und Hans-Christian Espérer

Layout
46halbe, Stefan Ullrich, Unicorn

Redaktion dieser Ausgabe
46halbe, Bine, CCC Dresden, erdgeist, Hans-Christian Espérer, ex10dead, Martin Haase, packet, Lew Palm, Andreas Portele, Malte Springer, Twister, Stefan Ullrich, Unicorn, Andrea ‚Princess' Wardzichowski, Jan Wulfes

Nachdruck
Abdruck für nicht-gewerbliche Zwecke bei Quellenangabe erlaubt

Eigentumsvorbehalt
Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zurhabenahme ist keine persönliche Aushändigung im Sinne des Vorbehaltes. Wird die Zeitschrift dem Gefangenen nicht ausgehändigt, so ist sie dem Absender mit dem Grund der Nicht-Aushändigung in Form eines rechtsmittelfähigen Bescheides zurückzusenden.

Andreas Pfitzmann

von Jan Wulfes <jw@klobs.de>

Ich bin kein Schreiberling; dennoch ist es mir ein persönliches Anliegen, noch einmal in gedruckter Form ein paar Zeilen einem ganz besonderen Mann zu widmen, der für viele unserer Chaos-Ideale eingetreten ist, oftmals gemeinsam mit uns.

Am 23. September 2010 ist Prof. Dr. Andreas Pfitzmann im Alter von 52 Jahren viel zu früh verstorben. Für viele seiner Mitmenschen spielte er eine herausragende Rolle.

Andreas war auch für mich einer der ganz Tollen. Ein Mann, den ich bewunderte und dem ich versuchte und auch immer noch versuche nachzueifern. Er war nicht nur mein Professor; er war ein tatsächlicher Wegweiser.

Was mich begeisterte, ist, daß er immer mehr gesehen hat als die pure Technik. Technik und Gesellschaft waren bei ihm immer vereint; eine Lebensweise, die ich bei vielen meiner Kommilitonen, Professoren und sonstigen Mitnerds vermisse. Vielleicht nicht, weil sie bei ihnen nicht da ist, sondern vielleicht nur nicht so intensiv gelebt wird, wie Andreas das gemacht hat.

Er hat ein gutes Stück dazu beigetragen, die Welt cooler zu machen, in kleinen sowie in großen Maßstäben. Etwas weniger Angst, etwas mehr Freiheit verdanken wir in den letzten Jahrzehnten an vielen Ecken nicht zuletzt ihm.

Zu den kleinen Maßstäben zählt beispielsweise, daß er immer für Studenten da war, auch wenn er sehr viel Arbeit auf dem Tisch hatte. Oder daß er als einziger Hochschullehrer Kurse an seiner Fakultät angeboten hat, in denen er zusammen mit den Studenten versuchte, Informatik und Gesellschaft zu verbinden – um sozusagen über den Tellerrand der Fachwissenschaft hinauszuschauen.

Zu den großen Maßstäben zählt beispielsweise, daß er nahezu unermüdlich scheinbar noch so beratungsresistenten Politikern Sachverhalte rund um das Thema Datenschutz wieder und wieder anschaulich erläuterte. Er bewies Mut, auch unangenehme Wahrheiten gemäß seiner Überzeugung und Expertise aufrecht gegen jegliche Widerstände zu verteidigen. Daß wir in Deutschland keinen Kryptobeschränkungen seitens der Regierung unterliegen, verdanken wir zu guten Teilen ihm.

Er war ein weitsichtiger Mensch und gegenüber neuen Denkansätzen aufgeschlossen. Seine visionären Gedanken eilten der Zeit voraus. Seine Ideen und Tatkraft entwickelten den Datenschutz und die Datensicherheit maßgeblich als integralen Bestandteil der sich formenden Informationsgesellschaft. Er hat es oft geschafft, diese Thematik auch Fachfremden zugänglich zu machen.

Es gibt so viele Dinge über ihn, die es sicherlich Wert wären, hier aufgeführt zu werden. Das bekomme ich aber nicht so gut hin. Deswegen kann ich jedem nur wärmstens ans Herz legen, mehr von diesem Menschen in sich aufzusaugen. Zum Glück hat er uns ein paar seiner Gedanken konserviert.

Ich denke, daß es nicht zu viel ist, wenn ich schreibe, daß der Verlust von Andreas Pfitzmann viele Clubmitglieder tief erschüttert hat und ihn viele sehr vermissen. Er hätte in den kommenden Jahren bestimmt noch einiges dazu beigetragen, unsere Gesellschaft zu etwas Besserem zu machen. Ich wünsche allen, die um ihn trauern – egal in welchem Maße – nach wie vor viel Kraft und vielleicht in Zukunft noch ein kleines Bißchen mehr als sonst den Pfitzmann-Spirit zu leben.

Praxisüberwachung

von Lew Palm <lew@tzi.de>

Zur Zeit werden die meisten Praxen in Deutschland von den Kassenärztlichen Vereinigungen zu einer Anbindung an ein Netzwerk namens „KV-SafeNet“ über das Internet gezwungen. Ich bin Informatiker und betreue die Computersysteme einer psychotherapeutischen Praxis. Mir sind grobe Sicherheitsmängel bei der Konzeption und Ausführung dieser Umstellung aufgefallen, jedoch kein Nutzen für Ärzte, Therapeuten oder Patienten. Des weiteren sehe ich gesellschaftliche und politische Gefahren sowie die Möglichkeit, daß sich die eingesetzte Technik sehr einfach zum Überwachen des gesamten internen Datenverkehrs der lokalen Praxis-Computernetzwerke verwenden läßt.

Die niedergelassenen Ärzte und Psychotherapeuten in Deutschland rechnen ihre Leistungen nicht direkt mit den gesetzlichen Krankenkassen ab, sondern über Mittlerinnen: die Kassenärztlichen Vereinigungen (KVen). In jedem Bundesland gibt es eine KV, die in der Kassenärztlichen Bundesvereinigung (KBV) organisiert ist, die wiederum vom Gesundheitsministerium kontrolliert wird. Vereinfacht gesagt haben die KVen auch noch den öffentlichen Auftrag, die knapp 150.000 Praxen so zu organisieren, daß diese im Interesse der etwa 72 Millionen gesetzlich Krankenversicherten wirken können.

In der von mir betreuten Praxis wurde bislang das quartalsweise Versenden der KV-Abrechnung durch das persönliche Überbringen von feststofflichen Datenträgern bewerkstelligt. Zu diesem Zweck wurden eine CD, eine Diskette oder ausgedruckte Unterlagen direkt zur Geschäftsstelle der Kassenärztlichen Vereinigung gebracht. Dem Praxispersonal war das recht, der Aufwand war nicht sehr groß. Mir als IT-Verantwortlichem gefiel es ebenfalls, denn es mußte kein Praxisrechner am Internet hängen, und die Sicherheit der persönlichen Datenübertragung war ungeschlagen hoch. Die für Abrechnungen in “meiner” Praxis verwendete und auf dem Markt existierende Software setzt Microsoft Windows als Betriebssystem voraus. Es wird mit hochvertraulichen Patientendaten umgegangen, auf einer Vielzahl von zum Teil nachlässig betreuten und mit Backdoors oder Rootkits verseuchten Windows-Computern.

Aus diesem Grunde wollte ich eine Anbindung der Praxis an das Internet vermeiden, die mit einem unverhältnismäßig hohen Aufwand an Sicherheitsmaßnahmen verbunden gewesen wäre. Alle mir bekannten psychotherapeutischen Praxen der Umgebung lieferten die Abrechnungsdaten bis dato persönlich bei der KV ab; es ist aber zu vermuten, daß viele andere (bei größerer räumlicher Entfernung zum nächsten KV-Büro) ihre Abrechnung per Einschreiben über den Postweg versendeten.

Doch nun hat sich die Situation geändert – die KVen haben die bisherige Vorgehensweise verboten und zwingen die niedergelassenen Ärzte und Psychotherapeuten ab dem Jahr 2011 zur Online-Abrechnung über das Internet. Der Sinn dieses Zwangs erschloß sich mir zunächst nicht. Dem minimal höheren Aufwand des manuellen Einlesens eines Datenträgers pro Arzt beziehungsweise Therapeuten und Quartal bei den KVen steht ein erhöhtes Sicherheitsrisiko durch IT-unkundige Praxismitarbeiter gegenüber, die ihre Computer nun zwangsläufig mit dem Internet verbinden müssen. Mir schien ein sukzessiver und zwangfreier Umstieg von persönlicher oder postalischer zur Online-Übertragung sinnvoller, falls dieser von den Betroffenen überhaupt gewünscht ist.

Auch ging ich davon aus, daß ein einfaches und sicheres Übertragungsverfahren gewählt würde. Eine Grundregel beim Entwerfen eines jeden technischen Systems ist, dieses so ein-

fach wie möglich zu gestalten, da jedes zusätzliche Element Risiken birgt. Es würde sich beispielsweise anbieten, die Abrechnungsdatei auf dem Computer des Arztes mittels GnuPG zu verschlüsseln, um sie anschließend über eine beliebige Dateiübertragungstechnik (zum Beispiel scp) auf den KV-Server zu transportieren. Die dafür benötigten Programme sind vorhanden und ausgiebig erprobt; die Einbindung in eine bestehende Abrechnungssoftware wäre denkbar trivial. Der größte Vorteil läge in der Überprüfbarkeit der Sicherheit der technischen Vorgänge durch die Öffentlichkeit (beziehungsweise durch unterschiedliche Experten, die für keine oder zumindest unterschiedliche Lobbies arbeiten), denn der Quellcode der genannten – im Sicherheitsbereich wichtigen und weitläufig akzeptierten – Programme liegt offen vor.

Es kam aber ganz anders. Die KVen entschieden sich, mit Kanonen auf kleine, niedliche Vögel zu schießen. Sie bildeten ein Netzwerk namens „KV-SafeNet“, wobei die Rechner der Bundesländer-KVen und der KBV-Zentrale über eigene Backbones verbunden sind. Den Anschluß dieser Server an das Internet organisieren momentan fünfundzwanzig privatwirtschaftliche Firmen. Von der Arztpraxis aus wird ein VPN über den DSL-Anschluß zu einem Server einer dieser Firmen aufgebaut.

Dieses Konzept ist vom Prinzip her nicht schlecht – wenn man von einer Zentrale aus eine permanente Verbindung zu allen Praxiscomputern haben möchte. Jedoch ist dies für die KV-Abrechnung und so gut wie alle anderen Datenverarbeitungsbedürfnisse der Ärzte, Psychotherapeuten und Patienten völlig unnötig.

Es geht noch weiter: Die KVen haben angeordnet, daß der Aufbau des VPN-Tunnels nicht durch einen Praxiscomputer selbst geschieht, was problemlos möglich wäre, sondern durch einen speziellen Router. Dieser Router muß von den Praxisbetreibern bei einem der fünfundzwanzig „Provider“ gekauft werden. Von den KVen wird er treffenderweise offiziell „Black Box“ genannt, denn in seine Funktionsweise darf von den Ärzten und Psychotherapeuten und ihren IT-Betreuern keine Einsicht genommen werden. Als Router ist er meistens das Zentrum auch des internen Netzwerk-Datenverkehrs in der Praxis. Er darf aber vom Praxisbetreiber weder konfiguriert werden, noch kann dieser nachvollziehen, zu welchen Servern im Internet der Router Verbindung aufnimmt und welche Daten er überträgt. Eine Überwachung und Protokollierung der gesamten lokalen Netzwerkdaten durch die entsprechende KV-SafeNet-Provider ist also problemlos möglich, diese können den Router ohne das Wissen des Arztes oder Therapeuten aus der Ferne administrieren. Kein verantwortungsbewußter IT-Administrator würde eine Black Box mit einer verschlüsselten Schnittstelle nach außen in das Zentrum seines Netzwerkes einbauen. Die KVen scheinen das anders zu sehen, sie haben ja auch keine Hemmungen, die Praxen zu einer Installation einer solchen Box zu zwingen.

Man muß also als Arzt oder Psychotherapeut – und als Patient sowieso – seinem SafeNet-Provider vollkommen vertrauen. Ebenso muß man darauf vertrauen, daß – sollte die „Black Box“ ordnungsgemäß funktionieren – allen anderen am Gesamtnetzwerk Beteiligten keine sicherheitstechnischen Pannen passieren. Wir reden hier von immerhin fünfundzwanzig Provider-Firmen, siebzehn KVen, der KBV sowie mehrere zehntausend Arztpraxen. Allein die Größe dieses Netzwerkes und seine vielen Schnittstellen zum Internet legen nahe, daß eine Abschottung gegen ernsthafte Angreifer von außen eher Minuten als Tage standhält. Man muß davon ausgehen, daß Datendiebe oder -manipulatoren sich sehr schnell zumindest einen Praxis-Account bei einem der Provider besorgen können und damit Teil des Netzes werden.

So sieht es zumindest im „Idealfall“ aus – wenn keine der Firmen relevante Fehler oder unerwünschte sicherheitskritische Funktionen in ihrer Box übersieht. Wie gut die einzelnen Firmen in diesem zentralen Punkt ihre Arbeit machen, ist aber prinzipbedingt nicht überprüfbar, denn für ihre Kunden ist die Box ja „black“.

Die Übertragung der Patientendaten im „SafeNet“ wird nun zusätzlich zur Transportver-

schlüsselung noch einmal separat verschlüsselt – per PaDok oder D2D –, die gleiche Technik, die auch auf der „Elektronischen Gesundheitskarte“ zum Einsatz kommen soll (siehe auch Datenschleuder #85). Diese Technik hat mit dem „Black Box“-Router im Praxis-Netzwerk eines gemeinsam: Beide arbeiten nach dem Prinzip „security by obscurity“. Dies ist kontraproduktiv, da eine Analyse unabhängiger Sicherheitsexperten hierdurch deutlich erschwert wird, die Kriminellen auf Dauer aber selten am Verstehen des Systems gehindert werden. So ließen sich die gesamten geheimen Einstellungen der „Black Box“ meiner Praxis innerhalb weniger Stunden Arbeit auslesen, wenn man das Gerät in den Händen und die Motivation zu einer kriminellen Handlung hat. Die Black-Boxerei stellt also keineswegs einen ernstzunehmenden Schutz gegen Kriminelle und bösartige Datendiebe dar, sie hindert einzig die Betreiber der Praxen an der Kontrolle über ihre eigene IT-Infrastruktur.

Claude Shannon, der Begründer der Informationstheorie, äußerte sich schon in den 40er Jahren des letzten Jahrhunderts zu diesem Thema: „The enemy knows the system.“ Auguste Kerckhoffs schrieb 1883 in seinen Grundsätzen der modernen Kryptographie: „The system must not require secrecy and can be stolen by the enemy without causing trouble.“ Mit „system“ bezog er sich auf den technischen Verschlüsselungsapparat. Damit meinte er, daß die Kenntnis vom Verschlüsselungsalgorithmus, die ein Spion durch das Stehlen des Apparates erlangt, beim Entschlüsseln der geheimen Nachrichten nicht helfen dürfe. Seit über einhundert Jahren ist es allen Kryptographen bekannt, daß man Sicherheit durch die hohe Qualität der Kodierverfahren und nicht durch die Geheimhaltung derselben herstellen sollte. Eine Verschleierung der Verfahren selbst spricht immer für ihre mindere Qualität – und hält nie lange.

Ein weiterer Nachteil des „SafeNets“ sind die hohen Kosten für die Praxen. Ein Black-Box-Router kostet zwischen 190 und 500 Euro. Die Provider-Firmen verlangen von jeder Praxis eine monatliche Gebühr von mindestens 17 Euro (zusätzlich zum DSL-Anschluß). Jährliche Kosten von über zweihundert Euro sind unverhältnismäßig hoch bei einem Übertragungsvolumen von oft weniger als einem Megabyte (so zumindest in der von mir betreuten Praxis) pro Quartal. Hier könnte man darüber nachdenken, ob die Preisgestaltung nicht nach § 138 Abs. 2 BGB als sittenwidrig einzuschätzen ist.

Die Entwickler und Entscheidungsträger hinter dem „SafeNet“ bauen also ein System, das nicht einmal den Sicherheitskonzepten von 1883 entspricht (security by obscurity). Es ist für die KVen wie auch für die Ärzte sehr teuer, dabei aber für die Abrechnung unnötig. Allein die Größe und Menge der involvierten Parteien (u. a. fünfundzwanzig Privatfirmen) macht das Netz angreifbar. Die Abrechnungen wären über bestehende Techniken (PGP) einfacher, billi-

ger und sicherer zu übertragen. Jeder Netzwerkadministrator wird auf die Barrikaden gehen, wenn er eine ferngesteuerte Black Box in das Zentrum seines Netzes einsetzen soll, wie dies nun in den Praxen geschehen muß. Hier drängt sich nach Cicero die Frage auf: „Wem nützt es?" Die erste Antwort darauf ist merkwürdig. Auf den ersten Blick scheint es nur den fünfundzwanzig Provider-Firmen zu nützen, die daran kräftig verdienen. Diese sind aber nicht die Initiatoren. Alle anderen haben mit dem „SafeNet" erstmal nur Ärger.

Doch vor Spekulationen über die Interessen hinter „SafeNet" möchte ich über die Erfahrungen berichten, die ich als IT-Administrator meiner Praxis in den letzten Tagen gemacht habe. Zur Zeit bekommen die Ärzte und Psychotherapeuten vieler Bundesländer von den KVen eine „motivationsfördernde Prämie" von mehreren hundert Euro, wenn sie innerhalb von kurzer Zeit die ferngesteuerte „Black Box" für ihr Praxisnetzwerk anschaffen. Wohlgemerkt müssen die Praxen dies sowieso tun, denn andere Arten der Abrechnungen werden nicht mehr akzeptiert. Wieso also für eine verpflichtende Handlung noch eine „Prämie" ausloben? Es soll hiermit wohl der passive Widerstand vieler Ärzte und Psychotherapeuten gebrochen werden, die durch ein Verschleppen der Anschaffung die Einführung des neuen Systems verzögern oder behindern könnten.

Diese „motivationsfördernde Prämie" funktionierte auch bei meiner Praxis. Ich schaute mich um nach dem billigsten Angebot und stieß auf die Firna "Deutsches Gesundheitsnetz Service GmbH" (DGN). Dort kostet der Router „nur" 190 Euro; die jährlichen Gebühren für die Berechtigung zur Verbindungsaufnahme zum VPN-Server belaufen sich auf 204 Euro.

Die mysteriöse „Black Box" interessierte mich besonders. Sie entpuppte sich als „Fritz! Box Fon Wlan 7170", hergestellt von der AVM GmbH aus Berlin. Ein nachträglich angebrachter Aufkleber etikettierte sie um in einen „DGN Safenet-Konnektor". Dieses Gerät (ohne den Konnektor-Aufkleber) bekommt man nicht nur bei Media Markt und ähnlichen Geschäften, sondern auch im Versandhandel ab 120,10 Euro. Der mit siebzig Euro bezahlte „Mehrwert" des an meine Praxis gelieferten Routers gegenüber dem Versandhandel-Modell liegt in der Konfiguration: Durch die DGN wurde die Verbindung zu ihrem Virtuellen Privaten Netzwerk (und vielleicht noch andere Funktionalitäten) eingestellt sowie ein dem Käufer unbekanntes Login-Paßwort gesetzt. Ebenjenes geheime Paßwort macht für die Praxis dann aus der Fritz! Box eine Black Box.

Eine Untersuchung des Routers im Netzwerk (genauer gesagt: ein Portscan) ergab dann, daß diverse Ports geöffnet waren und auf Verbindungen warteten. Dies ist für die angedachte Funktionalität des VPN-Routers unnötig; es stellt zumindest ein erhöhtes Sicherheitsrisiko dar. So ist beispielsweise der laufende Dienst für Telefonie (SIP) überflüssig, da das Gerät weder für diesen Zweck angeschafft wurde noch, mangels Passwort, dafür konfigurierbar wäre.

Unter anderem lief auch ein Webserver. Die dort angezeigte Seite ist die übliche "Fritz! Box"-Login-Page. Unter dem Passwortfeld steht die freundliche Aufforderung: „Wenn Sie Ihr Kennwort vergessen haben, klicken Sie hier". Da konnte ich mich nicht zurückhalten und habe es getan. Das Ergebnis war, wie erwartet, daß die Fritz! Box ihre Konfiguration löschte und sich damit in den Zustand versetzte, den sie auch hat, wenn man sie frisch aus dem Elektronikdiscounter trägt.

Auf die Anfrage an die DGN nach den Konfigurationsdaten wurde ebenfalls wie zu vermuten reagiert: Ich solle das Teil einschicken und eine Gebühr von dreißig Euro entrichten, damit die Firma den Router neu konfiguriert.

Bei der ganzen Geschichte gibt es mehrere Häßlichkeiten. Die Firmen verlangen sehr viel Geld für sehr wenig Leistung – insbesondere die monatlichen siebzehn Euro für die üblicherweise nur einmal im Quartal genutzte Berechtigung zur Teilnahme am VPN sind unverschämt. Ein happiger Aufschlag von siebzig Euro für die Vorkonfiguration eines Routers

ist auch nicht wenig. Das ganze Konzept des fremdkontrollierten Routers im Praxis-LAN ist unsicher, aber wieso laufen auf dem Gerät auch noch unnötige Dienste? Wieso hat die DGN eine Fritz! Box mit WLAN- und Telefonie-Hardware verwendet, wenn solche Funktionalitäten gar nicht genutzt werden dürfen?

Es stellt sich auch die Frage, ob ein solches Konsumenten-Endgerät den an eine ärztliche Praxis gestellten Sicherheitsanforderungen genügt. Offenbar hat die DGN mit den überflüssigen Serverdiensten in der Konfiguration geschlampt. Bei einem solch groben Patzer, einem Fehler, durch den jeder Auszubildende in den entsprechenden Lehrberufen durch eine Prüfung fallen würde, drängt sich die Frage auf, wie denn die restliche Konfiguration aussieht. Leider ist dies nicht auf legalem Wege überprüfbar, denn die Firma rückt – auf Weisung der KV, es muß ja eine Black Box sein – mit dem Paßwort nicht heraus.

Von Seiten des „SafeNets“ und der Provider-Firma ist der Router – dank VPN – ebenso erreichbar wie aus dem lokalen Netzwerk. Deswegen können sich die Angestellten der DGN in unsere Fritz! Box jederzeit einloggen, sie haben ja auch das Paßwort. Beworben wird das auf deren Homepage: „Kostenlose und komfortable Fernwartung durch unsere Hotline-Mitarbeiter“. Das bedeutet konkret, daß jede ärztliche und psychotherapeutische Praxis in Deutschland die Kontrolle über ihren herausgehenden und internen Datenverkehr an eines der privatwirtschaftlichen „SafeNet“-Unternehmen „outsourcen“ muß.

Im Fall der DGN hat die Sache ein Sahnehäubchen: Die Fritz! Box hat eine Funktion zum Mitschneiden des gesamten Datenverkehrs schon eingebaut. Auf der Seite *http://router-adresse/html/capture.html* – wobei router-adresse durch die IP-Adresse der jeweiligen Praxis-Fritz! Box zu ersetzen ist – kann ein DGN-Angestellter bequem und ohne besondere Computerkenntnisse über den Webbrowser das Mitschneiden des gesamten internen Netzwerk-Datenverkehrs in der jeweiligen Praxis ein- und ausschalten und die Daten zu sich herunterladen.

Aber warum sollte das denn jemand tun? Weiter gefaßt führt das zu der oben gestellten und noch nicht beantworteten Frage: Warum das alles? Wem nützt es? Hier kann nur spekuliert werden. Es ist jedoch offensichtlich, daß die vorgegebenen Argumente für das „SafeNet“ nicht mit den echten Interessen übereinstimmen. Wollte man wirklich ein gutes System für die Online-Übertragung der Abrechnung über das Internet, so hätte man das einfacher, schneller, besser, sicherer und billiger haben können.

Die Praxen sollen offensichtlich mit aller Gewalt dazu gebracht werden, daß ihre Informationstechnik permanent mit dem Zentralserver der KVen beziehungsweise der KBV verbunden ist und daß sie durch diese besser überwachbar sind. Die zentrale Anbindung und Vernetzung der Praxen ist für sich allein nicht zweckmäßig; Sinn ergibt das Ganze erst, wenn noch weitere Schritte folgen. Man kann also vermuten, daß die KBV oder das Gesundheitsministerium Erweiterungen des Systems plant, für die die momentan aufgebaute Vernetzung Voraussetzung ist. Was könnte das sein? Es wäre möglich, die Abrechnungsdaten, also die Daten über Patientenbesuche, Medikamente und Therapien, schon zum Zeitpunkt der Erzeugung zentral bei der KV zu speichern; eine Abrechnung pro Quartal ist dann nicht mehr notwendig, alles instantan online erfaßt.

Die Auslagerung der Informationstechnik aus der Praxis in den KV-Server im „SafeNet“ läßt sich noch deutlich weiter treiben. Warum nicht alle Patientendaten in die Zentrale übertragen? Diagnosen, chronische Krankheiten, Arztnotizen... Die Datenhaltung wäre viel „effizienter“, und die Praxen müßten sich kaum noch um die Wartung irgendwelchen Computerkrams kümmern. Alle Gesundheitsdaten der gesamten Bevölkerung (mit Ausnahme der Privatversicherten) wären an einer Stelle und in einer Hand. Daten sind Macht, und eine Datenbank ist mehr als die Summe ihrer Einzelteile. Besonders bei der Pharmaindustrie dürfte eine solche, technisch leicht auszuwertende Datensammlung Begehrlichkeiten wecken.

Cybermobbing

von Andrea ‚Princess' Wardzichowski <princess@bofh.de>

„Cybermobbing – Kann das nicht mal einer abstellen?" – warum man gegen Mobbing nicht technisch vorgehen kann und warum Erziehung zur Medienkompetenz wichtiger denn je ist. Denkanstöße nicht nur für Eltern und Lehrer.

Die aktuelle Situation

Ende März 2011 wurde das Problem „Cybermobbing" durch die Internetplattform *http://www.isharegossip.com/* einer breiten medialen Öffentlichkeit bekannt. Bei isharegossip.com handelt sich um ein Portal, das extra dazu errichtet wurde, Klatsch und Tratsch zu verbreiten. Leider blieb es dabei aber nicht bei harmlosen Geschichten; auch Beleidigungen, Lügen und Diffamierungen aller Art wurden dort verbreitet.

In deutscher Sprache und mit praktischen „Gefällt mir" und „Gefällt mir nicht"-Buttons versehen, fein sortiert nach Bundesländern und Landkreisen kann man dort seine Meinung (oder besser: seinen Müll) abkippen. Die vermeintliche Anonymität des Netzes trägt leider auch hier zu einer gewissen Enthemmung bei und läßt Anstand, Höflichkeit und Erziehung schnell vergessen sein.

Der Grundsatz „Sage im Netz nichts, was Du nicht auch jemandem im richtigen Leben ins Gesicht sagen würdest" gerät immer mehr in Vergessenheit. Er stellt aber eine gute Abschätzung dessen dar, was man im Netz tun und lassen sollte.

Ist Mobbing ein neues Problem?

Betrachtet man die Gesellschaft, so ist Mobbing kein „Problem des Internets". Auch in Schule und Berufswelt wird und wurde schon immer gemobbt. Ein jeder frage sich, ob er in der Schulzeit immer zu den beliebtesten Kindern der Klasse gehörte oder eher Außenseiter oder „graue Maus" war. Auch im Berufsleben nehmen Erkrankungen und Fälle von Berufsunfähigkeit durch Mobbing zu. Wir müssen uns daher die Frage stellen, ob nicht die gesamte Gesellschaft „ungnädiger" geworden ist, und was man dagegen tun kann.

Betrifft Mobbing nur Jugendliche?

Mobbing findet in der Tat nicht nur in der Schule statt, wie jeder aufmerksame Mensch, der die Medien verfolgt, auch weiß. Es hilft also wenig zu sagen: „Stell Dich nicht so an, die Schulzeit dauert ja nicht ewig." Gerade Kinder und Jugendliche, die sich ja noch in der Entwicklung ihrer Persönlichkeit befinden, kann kaum zugemutet werden, jeden Tag zu ertragen, woran selbst erwachsene Menschen erkranken und zusammenbrechen.

Wenn wir ehrlich sind, gab es doch auch in unserer Schulzeit Tage und Wochen, wo mal auf den einen, mal auf die andere verbal „eingeschlagen" wurde. Lehrer können dies meist nicht verhindern. Sie sind nicht anwesend oder können in der großen Pause bei der Aufsicht auch nicht überall sein.

Neue Medien – neue Dimensionen

Ein Aspekt allerdings ist neu: Während Mobbing und das „kleine Herumschubsen in der Pause", Ranzen ausschütten und ähnliche „Nettigkeiten" früher den Rahmen der Klasse und vielleicht der Schule nicht verließen, sieht sich ein Mobbing-Opfer durch Plattformen wie *http://www.isharegossip.com/* einer globalen Demütigung ausgesetzt. Das Geärgert-Werden ist mit Ende der Pause nicht vorbei, es wird lang und breit im Internet ausgeführt.

Stefan Middendorf vom LKA Baden-Württemberg äußerte sich bei einem Vortrag des CCCS e. V.: Er führte an, daß weder Eltern noch Lehrer heutzutage manche Verletzungen mitbekommen, denn diese zeigen sich nicht mehr in einem „blauen Auge", sondern seien seelischer Natur.

Unter diesen Vorzeichen ist ein lapidares „Hör' doch nicht auf das, was andere sagen oder schreiben" nur ein Teil der Lösung. Unter Umständen wird auf Webseiten und Portalen der eigene Name genannt, ohne daß man etwas dagegen tun kann.

Was ist NICHT neu an isharegossip?

Menschen, die nicht so technikaffin sind oder sich mit dem Internet nicht so gut auskennen, neigen vielleicht dazu, das „böse Internet" oder gar das „böse WWW" dafür verantwortlich zu machen, daß Cybermobbing möglich ist.

Aber ist das wirklich so?

Das Internet war schon immer ein Spiegel seiner Teilnehmer. Da heute breite Teile der Bevölkerung am Internet teilnehmen, ist es inzwischen auch ein Spiegel der Gesellschaft an sich. Alles, was es „draußen im richtigen Leben" gibt, findet sich auch im Internet wieder, insbesondere alle guten und schlechten Eigenschaften der Menschheit: Hilfsbereitschaft wie Verweigerung, Kommunikation und Zusammenarbeit – und eben auch Mobbing.

Da ich bereits die Vor-WWW-Zeit im Internet miterlebt habe, kann ich aus meiner Erfahrung sagen: Kleinkriege gab es schon vor dem Web2.0 und auch lange vor dem WWW. Es standen Newsserver (die Vorläufer von Diskussionsforen) und Internet Relay Chat zur Verfügung. Diese wurden zur Kommunikation wie zum Flamen (Beschimpfen) genutzt. Man konnte also auch schon vor zwanzig Jahren das Internet zu seinem persönlichen Sandkasten machen und trefflich darüber lamentieren, wer wem zuerst Schaufel und Förmchen weggenommen hat.

Besonders verwundert hat mich übrigens, daß Anfang des Jahres sogar ein GPG-Keyserver vom Netz genommen werden mußte, weil Menschen es geschafft haben, sich über das Hochladen von Schlüsseln gegenseitig Beleidigungen an den Kopf zu werfen. Der Aufwand für solch ein Vorgehen ist schon relativ hoch, und mir erschließt sich dessen Sinn nicht ganz, aber es hat tatsächlich stattgefunden.

Dies alles stützt die These, daß in Mobbing-Plattformen nur fortgeführt wird, was ohnehin offenbar in den schlechten Eigenschaften der Menschheit angelegt ist.

Was kann man tun, als Betroffener, als Eltern, als Lehrer?

Zunächst einmal muß der Betroffene beziehungsweise das Opfer überhaupt den Weg finden, sich einem Erwachsenen zu offenbaren. Dies ist schwieriger, als man gemeinhin denkt, aber wenn man ehrlich ist und sich an seine Kindheit und Schulzeit erinnert, so hat man selber auch Eltern und Lehrern nie alles erzählt.

Im günstigen Fall erfahren die Eltern, daß etwas schiefläuft. Aber sie müssen dann vieles leisten: Sie müssen zunächst verstehen, daß Dinge vorgehen, die ihrem Kind den täglichen Schulbesuch zur Qual machen. Sie müssen genug vom Internet verstehen, um zu sehen, wo das Mobbing und die Beleidigung stattfinden. Und DANN müssen sie noch helfen, das Problem einzuordnen und zu bewerten: Natürlich möchte fast jedes Kind/jeder Jugendliche zu seinem sozialen Umfeld (neudeutsch: peer group) dazugehören. Es gilt herauszufinden, wer die Urheber der Beleidigungen sind. Technisch ist dies schwierig, denn die Plattformen loggen ganz zu Recht keine Adressen (und auch der erneute Ruf nach der Vorratsdatenspeicherung würde weder etwas an der Situation ändern noch helfen, denn Zugriff über anonyme Proxies existiert). Aber tatsächlich weiß man in der Regel auch aus dem richtigen Leben, wer dahinterstecken könnte. Es gilt zu erkennen, daß die beleidigenden Mobber doch vielleicht nicht so wichtig sind wie die besten Freunde.

Eltern sollten auch ein offenes Ohr für die Freunde ihrer Kinder haben. Oftmals vertraut man sich einem fremden Elternteil leichter an, als den eigenen Eltern.

Lehrer sind in einer denkbar ungünstigen Situation: Sie sollen sich an Lehrpläne halten und prüfungsrelevanten Stoff vermitteln, sind aber mit Mobbing-Situationen konfrontiert. Es ist manchmal unmöglich, auch noch Erziehungsaufgaben zu übernehmen (genau aus diesem Grund gibt es zum Beispiel in Internaten nicht nur Lehrer, sondern auch Erzieher, deren Aufgaben sich von denen der Lehrer unterscheiden). Dennoch ist die Frage, ob es nicht doch Fächer geben sollte, in denen allgemeine politische Themen und Themen des Tagesgeschehens untergebracht und diskutiert werden können.

Der Kantsche Kategorische Imperativ für den Hausgebrauch („Was Du nicht willst, daß man Dir tu, das füg' auch keinem andern zu.") sollte wohl wieder etwas präsenter im Leben werden.

Am Ende der Bestandsaufnahme („es ist etwas passiert, nicht nur einmal, und nein, ich bilde es mir nicht nur ein") steht aber das Schwierigste: die Kommunikation.

Eltern der Opfer können mit den Eltern der vermeintlichen Urheber der Beleidigungen Kontakt aufnehmen. Aber hier ist pädagogisches Geschick angezeigt: keine Vorverurteilung aussprechen, sondern erfragen, wie sich die Sachlage von der anderen Seite her darstellt.

Im günstigen Falle sind die Eltern kooperativ und kommen ihrem Erziehungsauftrag nach. Im günstigsten Fall aber erziehen Eltern ihre Kinder auch zu selbstbewußten, denkenden und mündigen Bürgern und produzieren keine Opfer. Allerdings ist diese Welt einfach nicht perfekt, und nicht jeder bringt einen derart breiten Rücken mit und hat ein so dickes Fell wie ich nach zwanzig Jahren im Internet. Ich war in der Schulzeit auch schüchtern, schwach und eher der Opfertyp.

Es besteht also, auch WENN man sich der Vorfälle annimmt, die große Gefahr, daß auch die Kommunikation unter Erwachsenen eskaliert. Nur ist damit leider niemandem geholfen. (Was an dieser Stelle gar nicht hilft, sind übrigens gerichtliche Auseinandersetzungen.)

Aber auch bei Elternabenden und im Unterricht (siehe oben) muß das Thema zur Sprache gebracht werden: auf dem Elternabend, um aufzuklären und aufmerksam zu machen (die erwähnten seelischen Verletzungen werden sonst unter Umständen gar nicht bemerkt). Dies setzt natürlich eine hohe Fachkompetenz der Lehrer voraus.

Im Unterricht gestaltet es sich fast schwieriger: Die technische Seite ist den Schülern wohlbekannt, das „thou shalt not" hingegen offenbar nicht (denn sonst hätten sie im Vorfeld ja schon nicht so kalt und herzlos gehandelt und vor allem so ohne jedes Nachdenken). Hier muß eine gute Strategie entwickelt werden, auch die Mobber betroffen zu machen und den Opfern das Rückgrat zu stärken. Das aber sprengt den Rahmen einer „normalen" Unterrichtsstunde fast.

Ist Sperren oder Löschen dieser Portale eine Lösung? Die Köpfe der Hydra

Natürlich kommt an dieser Stelle immer die Frage, ob man das Problem nicht technisch bewältigen kann. Aber es wurde schon angedeutet: Das Löschen solcher Portale würde natürlich nichts bringen. Kleinkriege dieser Art werden immer eine Plattform finden, und es wird auch nicht lange dauern, bis sich der Name der neuen Plattform herumgesprochen hat.

Eine „Idee" war, daß Suchmaschinen die Namen von Mobbingseiten nicht mehr anzeigen. Nur nützt das aus mehreren Gründen nichts: Um den Namen einer Plattform herauszubekommen, muß man keine Suchmaschine bemühen. E-Mail, Chat, SMS existieren und dienen als Verbreitungsmedium. In direkter Folge würde das Nicht-Anzeigen bei Suchma-

schinen nur dazu führen, daß technisch nicht so versierte, aber besorgte Eltern die Adresse nicht finden. Es kommt hinzu, daß „security by obscurity“ noch nie ein gutes Konzept war. Das Geheimhalten von Sicherheitsmaßnahmen ist selbst keine Sicherheitsmaßnahme. Und nicht zuletzt: Sperrt oder löscht man eine solche Plattform, tauchen dafür zwei oder mehr auf, um die Nachfrage zu befriedigen (genau wie bei der Hydra für jeden abgeschlagenen Kopf zwei neue nachwachsen). Es ist also ein Wettrüsten.

Immer, wenn die Frage nach technischen Lösungen aufkommt, muß man sich eines vor Augen halten:

Soziale Probleme können nie durch Technik gelöst werden

Deswegen ist der Ruf nach dem Suchmaschinen- oder Plattformbetreiber und nach dem Gesetzgeber fehl am Platz. Auch der Gesetzgeber kann die menschlichen Abgründe nicht abschaffen, Erziehung kann sie aber zumindest zum Teil in die Schranken weisen.

Wie könnten Lösungsansätze aussehen?

Um sich halbwegs gefahrfrei im Internet zu bewegen, muß man nach wie vor eine ganze Menge lernen. Dazu gehört das Bedienen der Technik, aber auch das Einordnen von Quellen. Letzteres ist übrigens keine neue Fähigkeit: Schon vor Erfindung des Internets mußte man überlegen, ob man Groschenhefte konsumiert oder Thomas Mann, ob man seine Nachrichten auf den Öffentlich-Rechtlichen guckt oder bei SuperRTL, ob man die BILD kauft oder die Süddeutsche. Das Internet hat sich „nur“ dazugesellt, und natürlich stellt es durch seine Medienflut eine neue Herausforderung dar.

Das „Einfachste“ ist natürlich immer: nicht lesen/hinhören, wenn man das hinbekommt. Wenn mich jemand auf einer Webseite diffamieren will (und ich habe in den letzten zwanzig Jahren reichlich veröffentlicht, auch Unsinniges und Jugendsünden, ich habe also durchaus einige Angriffspunkte) und ich kenne diese Webseite gar nicht, so ficht es mich erst einmal nicht an. Man könnte genauso im Schwarzwald in einem Klohäuschen „Die Princess ist doof“ rufen.

Macht mich aber jemand darauf aufmerksam, daß irgendwo böse Dinge über mich stehen, so kann ich es mir immer noch ansehen und noch viel wichtiger: Ich kann entscheiden, wieviel Energie und Zeit ich da hineinstecke.

Ich habe mich seinerzeit auch dagegen entschieden, gegen die EMMA gerichtlich vorzugehen, obschon sie in einer Ausgabe behauptete, es gäbe mich gar nicht (was nochmal eine andere Qualität hat als „Du bist so doof“). Aber ich hatte und habe mit meiner Zeit Besseres zu tun.

Vielleicht ist es auch wichtig, das einmal zu transportieren: Viele Kleinkriege werden ja auch erst durch die Reaktion interessant! Schon früher in News und im Usenet wußten wir zu sagen: „Don‘t feed the trolls“ (Wenn also jemand Unsinn redet, einfach nicht drauf eingehen, dann verschwindet der Unsinn Verbreitende schon irgendwann wieder).

Und ist das nicht auch ein Aspekt des Lebens, der vielen Erwachsenen nicht mehr so präsent ist, daß sie ihr LEBEN leben sollten? (Und sich zum Beispiel nicht in Streitigkeiten mit den Nachbarn verzetteln?) Hier tritt auch die Vorbildfunktion der Eltern in Kraft!

In einem gewissen Rahmen sollte jeder versuchen, Tätigkeiten auszuüben, die ihm oder ihr Spaß machen, und sich mit Menschen zu umgeben, die einem guttun oder die einem zumindest nicht schaden. Auch wenn das im Schulalltag nicht immer realistisch ist (denn mal ehrlich, wer mochte schon jeden Lehrer?), so sollte man doch darauf achten, daß die Freizeit nicht auf Dinge verwandt wird, die einem vampirhaft die Kraft aussaugen.

Letzten Endes wird es aber doch auf eines hinauslaufen: miteinander reden, und zwar von Angesicht zu Angesicht, nicht online. Und das ist das Schwierigste von allem.

Die universellen Maschinen verantworten

von ex10dead <baderus@noderus.de> und packet <packet@berlin.ccc.de>

Ein geschichtlicher Überblick und die Grundsätze der Hackerethik

Beginnen wir mit der Bedeutung des Wortes Hacker. Am weitesten verbreitet ist noch immer die Verwendung des Begriffs als Synonym für Menschen, die Computer benutzen, um anderen Menschen zu schaden. Da sich böswillige Computerkundige weigern, sich selbst abgrenzend als Cracker zu bezeichnen, bleibt der Begriff des Hackers einer mit mehreren Bedeutungen. In unserem Sinne ist der Begriff Hacker in erster Linie eine Art Ehrentitel, um andere Menschen auszuzeichnen. Der Begriff ist also positiv besetzt und dabei rekursiv definiert: Hacker ist ein Begriff, der von Angehörigen der Hackerkultur verwendet wird, um sich nach außen abzugrenzen oder um Einzelne für besondere Leistungen auszuzeichnen.

Grundsatz der Hackerkultur ist es, daß Technik genutzt werden sollte, um die Lebensumstände aller Menschen zu verbessern. Dieses Ziel kann dann als erreicht betrachtet werden, wenn Technik und das erforderliche Wissen allen verfügbar, diese Technik elegant und gut ist und Hierarchien durch Selbstorganisation ersetzt werden – ein weiter Weg also. Wann aber ist Technik elegant oder gut? Die Definition dieser beiden Eigenschaften ist umstritten, wir wollen es dennoch versuchen: Elegant ist Technik dann, wenn sie nicht weiter vereinfacht werden kann, ohne Funktionalität zu verlieren. Gut ist Technik dann, wenn sie weder entworfen wurde noch dazu benutzt wird, um Menschen zu schaden.

Hackerkultur

Die Hackerethik ist eine Arbeitsethik. Erstmals schriftlich formuliert hat sie Steven Levy in seinem Buch „Hackers – Heroes of the Computer Revolution“ [1]. Die Entstehung dieser schriftlichen Fassung ist eng verbunden mit dem Tech Model Railroad Club am Massachusetts Institute of Technology in den USA; Levy behauptet, die Club-Mitglieder hätten die von ihm postulierte Hackerethik vorweggenommen.

Der Modelleisenbahnclub wurde nach eigenen Angaben im Jahre 1946 gegründet. [2] Ende der 1950er Jahre wurde die Modellbahnanlage des Clubs von den Mitgliedern in zwei Gruppen gepflegt und weiterentwickelt: Die erste Gruppe beschäftigte sich hauptsächlich mit dem sichtbaren Teil der Anlage, die zweite Gruppe, das Signals and Power Subcommittee, beschäftigte sich mit der Steuerung der Anlage. Dieses Signals and Power Subcommittee kann als eine der Keimzellen der amerikanischen Hakkerkultur erachtet werden, viele der damaligen Mitglieder gehörten später zum harten Kern des MIT AI Labs um Marvin Minsky. Sie verschafften sich Zugang zum IBM-704-Computer des MIT, ein teures Einzelstück und nicht für interaktive Benutzung, sondern für Stapelverarbeitung von Lochkarten gedacht. Rechenzeit war eine knappe Ressource, die von einer „Priesterschaft“ verwaltet wurde. Da die frühen Hacker nicht zu den Ministranten gehörten und sich in ihrer Computerbenutzung ohnehin nicht von einer Priesterschaft bevormunden lassen wollten, mußten sie kreative Wege ersinnen, um an diesen Computer heranzukommen.

Der Zugang zu Rechenkapazität verbesserte sich für die Hacker, als sie Zugriff auf den TX-0, einem vom Lincoln Lab ausrangierten Computer, erhielten. Dieser Computer benutzte einen Lochstreifen zur Eingabe und ermöglichte interaktives Arbeiten. Der Computer stellte


KEEP
CALM
AND
HACK
ON

die universelle Maschine dar: der Traum jedes Technikers – obgleich nicht zwangsläufig die finale Realisierung dieser Maschine.

Die Beschäftigung mit der gleichen Materie formte aus dieser Gruppe früher Hacker eine eingeschworene Gemeinschaft. Diese Gemeinschaft besaß implizite ungeschriebene Regeln für die gemeinschaftliche Computerbenutzung. Die Anerkennung von Individuen und Autoritäten in der Gemeinschaft, aber auch die Ziele und Werte der Gruppe wurden hierdurch bestimmt. Levys Hackerethik bezieht sich auf diese von ihm formalisierten Regeln.

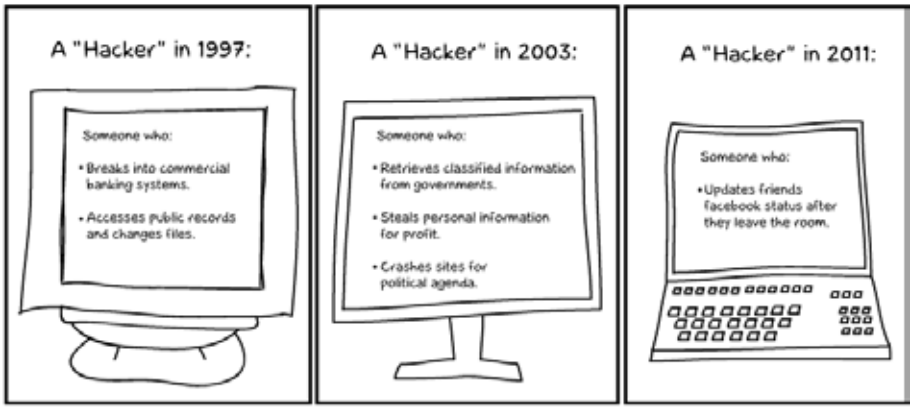
Der Tech Model Railroad Club in den späten 1950ern und frühen 1960ern ist nur ein Beispiel für die Erfahrungen der frühen Hacker. Das New Hacker's Dictionary [3], das auf das Jargon File am Stanford AI Lab zurückgeht, zeigt, daß die Hackerkultur schon in den 1970er Jahren bereits mehr als das MIT umfaßte.

Philosophie des Teilens

Levy hat die Personen der Hackerszene zu Beginn der 1980er Jahre im Rahmen der Recherche interviewt. In der Einleitung seines Buches beschäftigt er sich mit den angetroffenen Ansichten der Interviewten: „It was a philosophy of sharing, openness, decentralization, and getting your hands on machines at any cost – to improve the machines, and to improve the world." Er formuliert die erste These zur Hackerethik daher so: „Access to Computers – and anything that might teach you something about the way the world works – should be unlimited and total." Hacken setzt Verständnis voraus, Hacken ist kreative Beschäftigung mit Ideen, ist, Bewährtes in einen neuen Kontext zu setzen – das ist die Motivation der Hacker. Es gilt daher auch: „Always yield to the Hands-on Imperative." Kreative Beschäftigung, Spieltrieb und aktives Handeln in der Soziosphäre, also weit über die Technosphäre hinaus, wird gefordert. [4]

Die These „All information should be free." ist eine weitere Präzisierung. Stewart Brand sagte 1984 auf der ersten »Hacker Conference«: „On the one hand information wants to be expensive, because it's so valuable. The right information in the right place just changes your life. On the other hand, information wants to be free, because the cost of getting it out is getting lower and lower all the time. So you have these two fighting against each other." [5]

Nehmen wir beispielsweise das deutsche Informationsfreiheitsgesetz (IFG), das voraussetzungslose Einsicht in Akten amtlicher Informationen von Bundesbehörden ermöglichen soll (§§ 1 - 2 IFG) und 2006 in Kraft getreten ist. Der Zugang ist nicht schrankenlos, denn etwa die Ausgabe personenbezogener Daten oder „geistigen Eigentums" ist davon ausgenommen (§§ 3 - 6 IFG). Private Unternehmen erhielten außerdem eine häufig angewendete Schutzklausel:



Die Herausgabe und Einsicht darf verweigert werden, wenn ihre Geschäftsinteressen berührt sind. Zudem kosten nach der Informationsgebührenverordnung Auskünfte bis zu fünfhundert Euro. Das IFG ist wohl nur ein bescheidener Anfang für die Forderung nach einer maschinenlesbaren Regierung und „Open Government". Die in den Achtzigern aufgekommene, von Wau Holland entwickelte Idee einer maschinenlesbaren Regierung wurde in der Datenschleuder Nr. 24 definiert: „Es bleibt, will man den Informationskrieg vermeiden, nur die Forderung nach Offenen Netzen. Wo Information frei ist, braucht nichts versteckt zu werden, der Psychokrieg um die Verstecke entfällt, denn wir brauchen niemanden, der in vermeintlichen Verstecken schnüffeln muß. Sicherheit durch absolute Offenheit beinhaltet gleichzeitig die für jede Demokratie notwendige Übersicht über die laufenden Entwicklungen. Freie Daten, lautet die Forderung für die Zukunft – und das ist gemeint, wenn Hacker die maschinenlesbare Regierung fordern." [6] Man kann wohl auch einen aktuellen Bezug zu Wikileaks nicht verleugnen. Ziel des Einsatzes von Computern war und ist in Hinsicht auf die Privatsphäre ein überlegter technischer Datenschutz, in der Politik jedoch die maschinenlesbare Regierung.

Mißtraue Autoritäten, bilde Meritokratien, schaffe Kunst mit dem Computer

Eine weitere Forderung der Hackerethik: „Mistrust authority, promote decentralization." Daß Autorität nicht per se vertrauenswürdig ist, zeigt die libertäre, individuelle Natur der Hacker, die sich für Dezentralisierung einsetzen und keine Diskriminierung dulden: „Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position." Nach dieser Maxime gleicht die Hakkerszene einer Meritokratie: Die Position jedes Hackers im Gefüge wird ausschließlich nach seinen Fähigkeiten, Erfolgen und Kompetenzen bestimmt. [7]

Es ist zum Mantra weit über die Hackerszene hinaus geworden: „You can create art and beauty on a computer." Computergestützte, digitale Medienproduktion hat sich spätestens seit den letzten zwei Jahrzehnten allgemein durchgesetzt. Die Moog-Synthesizer des Progressive Rocks Ende der sechziger Jahre zeigten den Vorgeschmack auf Bands wie Kraftwerk, die elektronisch komponierten. Der Einsatz von Computern zur Musikerzeugung wurde dann durch die Demoszene Ende der achtziger Jahre durch den C64 und Atari 800 populär. Die Demoszene hat ihren Ursprung in derart künstlerisch ambitionierten Intros für Cracks, daß sie sich verselbstständigt hat. Nicht zuletzt gehört zu dieser These auch der Grundsatz, daß Hacken Kunst sei („Hacking is art"), Quelltext besitze eine eigene Ästhetik. [8]

Daten ändern die Welt

Es wird wohl heute keiner mehr bestreiten: „Computers can change your life for the better." Sie mögen nicht die Lösung für die meist menschengemachten Probleme dieser Welt sein, auch wenn sie oft dafür herhalten müssen. Dennoch hat die Globalisierung von Ton, Bild, Informationen, Daten über eine weltweite Echtzeitkommunikation nicht nur die westliche Welt unbestritten stark beeinflußt. Die Ereignisse um Wikileaks können als exemplarisch angesehen werden dafür, wie das Internet den „Informationskrieg" erleichtert oder behindert, in jedem Falle aber verändert.

Nach den späten fünfziger und den frühen sechziger Jahren hat sich die Hackerethik weiterentwickelt: Der CCC fügte zwei explizite For-

derungen zu Levys Hackerethik hinzu; Steven Mizrach reflektierte darüber, wie sich in den Neunzigern eine neue Hackerethik etabliert hat. [8]

Die neu hinzugekommenen Forderungen lauten: Mülle nicht in den Daten anderer Leute. Die Interpretationen dazu gehen auseinander: Man könnte darunter verstehen, daß das Eindringen in Systeme legitim im Sinne der Hackerethik ist, solange Daten weder verändert noch gelöscht werden. Eine andere Interpretation wäre, daß ausschließlich das Hacken von dafür vorgesehenen oder eigenen Systemen legitim ist. Nicht aufgenommen wurde der strittige Punkt „No hacks for money", auch weil hinreichend viele Hacker sich den Lebensunterhalt mit legitimen Hacks verdienen. [9]

Klarer ist da wohl die zweite neue Forderung: Öffentliche Daten nützen, private Daten schützen. Das Spannungsverhältnis von Privatsphäre und Öffentlichkeit läuft hier zusammen. Die Entscheidungen, welchen Bereichen Daten zuzuordnen sind, bleiben ethische Dilemmata.

Beide Forderungen stellen Schranken der Informationsfreiheit dar, deren Grenze von Fall zu Fall entschieden werden muß. Es sind letztlich Verpflichtungen, selber nachzudenken. Scheinbar stehen diese Forderungen im Widerspruch zu Levys Diktum „All information should be free". Tatsächlich besteht dieser Widerspruch aber nicht, denn Daten sind nicht gleichzusetzen mit Informationen, Daten können aber Informationen enthalten. Der scheinbare Widerspruch löst sich auf, wenn man annimmt, daß Informationen im Sinne der Hackerethik nur in öffentlichen Daten enthalten sein können.

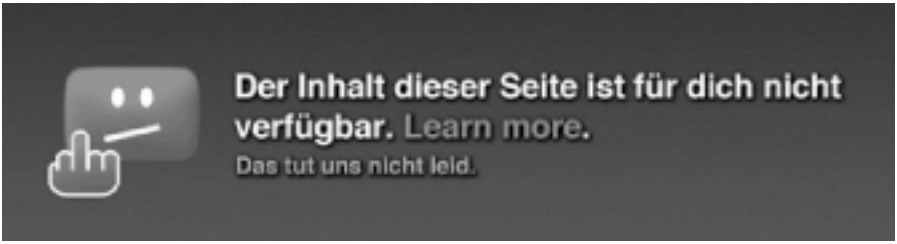
Kommunikation als Menschenrecht

Steven Mizrach hat in [8] eine Analyse von Hackerethiken, von vorhandenen Forderungen vorgenommen, und zwar durch computergestützte Textanalyse. Er fand heraus, daß neuere Hackerethiken Teile der alten Ethik beinhalten. Als Grund für die Entstehung einer neuen Hacker-ethik spekuliert Mizrach, daß Veränderungen in der Computertechnologie, in sozialen Indikatoren, in der Praxis der Computerindustrie und in der Demographie als Erklärung bemüht werden können. Daß die Hackerethik der Neunziger und die aus den frühen Sechzigern nicht aus verschiedenen Wurzeln stammen, erklärt die ethische Kontinuität.

Einige der neuen Maximen nach Mizrach belegen Kontinuität und Veränderung zugleich, so etwa: „Share!" Daß alle Informationen frei sein sollten, wird erweitert um Ressourcen wie Hardware. Freie Verfügbarkeit wird angestrebt, um sie zu teilen.

Hinzu tritt der „Communicational Imperative". Kommunikation, insbesondere die digitale, ist immer noch ein Privileg der reichen Länder. Die These fordert Kommunikation als Menschenrecht. Dies beinhaltet einen freien, unzensierten Zugriff auf das Internet einschließlich Netzneutralität.

Ein typisches Gegenbeispiel zu einem freien, unzensierten Internet sind die Sperr- und Filterpraktiken Chinas. Doch auch in Deutschland und anderen westlichen Ländern gibt es Bestrebungen, Netzneutralität und den einigermaßen unzensierten Zugriff zu begraben und mittels Vorratsdatenspeicherung den freien Zugang zu Informationen indirekt einzuschränken. Der



Communicational Imperative fordert für die ganze Welt, daß Kommunikation Menschenrecht sein soll, im Okzident einerseits, weil die Freiheit, frei elektronisch zu kommunizieren, bedroht ist, im Rest der Welt andererseits, weil die Grundlage flächendeckender elektronischer und unzensierter Kommunikation nicht gegeben ist.

Eine dritte neu hinzugetretene Forderung lautet: Hacking Helps Security. Im Informationszeitalter ist die Sicherheit und Integrität von IT-Systemen wichtiger geworden, nicht zuletzt auch dadurch, daß Systeme kompromittiert und Sicherheitslücken bekanntgemacht werden. Durch diesen Wettbewerb wird die Sicherheit von Programmen und von IT-Systemen allgemein erhöht.

Peer-to-Peer-Netze und Wikileaks

Welche Relevanz haben die Grundsätze der Hackerethik in der breiteren Gesellschaft, heute und in der Zukunft? Inwiefern ist ein Teil der Hackerethikgrundsätze mittlerweile auch außerhalb der Hackerkultur anerkannt? Mit der heutigen Durchdringung der Gesellschaft mit Computern und Internet kommt auch der Hackerethik eine neue Bedeutung zu: Peer-to-Peer-Netzwerke und Wikileaks haben Politik, Wirtschaft und Gesellschaft gelehrt, daß Information frei sein möchte, die Datenschutzdebatte erlebt in Deutschland spätestens seit der Vorratsdatenspeicherung eine deutliche Aktualisierung, mit der Bezeichnung „digitale Spaltung“ existiert ein Begriff für die Ausgeschlossenheit von Technologie und Kommunikationsmitteln.

All dies sind Phänomene, die von der Hackerethik mit ihren Forderungen nach Informationsfreiheit, dem freien Zugang zu Computern und dem Gebot, private Daten zu schützen, bereits vorweggenommen wurden. Die Verbreitung der Computertechnologie hat also auch die ursprünglichen Hacker-Probleme verbreitet. Auch die Feststellungen, daß mit einem Computer Kunst und Schönheit geschaffen werden können und daß Computer das eigene Leben zum Besseren verändern können, werden wohl vom Großteil der Menschen geteilt.

Werden aber auch die Forderungen der Hackerethik geteilt, etwa bezüglich der Informationsfreiheit allgemein? Peer-to-Peer-Netze und Wikileaks zeigen wohl vor allem eines: Information läßt sich nur schwerlich geheimhalten, ihre Verbreitung nicht mehr kontrollieren. Gewünscht ist dieser Effekt indes nicht von allen Beteiligten. Was die Geheimhaltung von Informationen anbelangt, so ist davon auszugehen, daß mächtige Geheimhaltungsinteressen wohl letzten Endes eher geringen Offenlegungsinteressen gegenüberstehen. Das Interesse der Gesellschaft an Informationsfreiheit scheint nur punktuell zu sein: Wikileaks anfangs zugespielte Dokumente erregten kaum mehr als lokales Aufsehen. Erst seitdem Wikileaks Tausende von Dokumenten aus dem US-amerikanischen Militär- und Diplomatiewesen zusammen mit klassischen Medien aufbereitet und präsentiert, ist Wikileaks auch zu einem internationalen Phänomen geworden.

Anders sieht es aus bei der Forderung nach dem Schutz privater Daten: Der Bedarf an Privatsphäre scheint in der Gesellschaft zurückzugehen. Die zwangsweise Herausgabe von Daten ist zwar verpönt, freiwillig präsentiert man sie jedoch gern. Die Vernetzung im privaten Freundeskreis geschieht mittlerweile vielfach öffentlich einsehbar, teilweise in einer direkt maschinenlesbaren Form. Diese Daten werden ausgewertet, und zwar im Zweifelsfall von jedem, der sich die erforderliche Rechnerleistung und Speicherkapazität leisten kann. Dieser Form der freiwilligen Preisgabe privater Daten zu widerstehen, bedeutet auch Selbstausgrenzung aus sozialen Ereignissen, die vielleicht nur noch online geplant oder durchgeführt werden. Auch die Möglichkeiten des technischen Datenschutzes sind hier begrenzt, da die Öffentlichkeit solcher Daten ja gewünscht und eben nicht nur ein vermeidbarer, technisch nicht notwendiger Seiteneffekt ist. Letzten Endes verbirgt sich darin der auch in der Hackerethik enthaltene Konflikt zwischen öffentlichen und privaten Daten.

Die übrigen Forderungen der Hackerethik, also die Forderung nach Dezentralisierung und Mißtrauen gegenüber Autoritäten und das Meritokratiegebot, sind hauptsächlich Anforderungen an das Verhalten eines Individuums. Ihre Umsetzung wird kaum von technischer Weiterentwicklung gefördert, sie sind vielmehr Ergebnis einer sozialen Entwicklung, die jedoch begünstigt werden kann: Der freie Zugang zu Informationen kann etwa das Mißtrauen gegenüber Autoritäten schüren. Das Meritokratiegebot wiederum scheint nur in sehr begrenztem Rahmen umsetzbar: Wer keine Ahnung von Computern hat, kann einen Hacker auch nicht nach seinem Handeln beurteilen. Analog gilt: Wer keine Ahnung von Politik hat, kann auch Politiker nicht nach ihrem Handeln beurteilen. Solange diese Wissenslücken bestehen, erscheint eine meritokratische Gesellschaftsordnung nicht allgemein umsetzbar.

Die Frage bleibt: Wann sind Daten nicht privat und müssen demnach öffentlich und frei zugänglich sein? Wir sind dazu aufgerufen, diese Entscheidung bewußt zu fällen. Haben wir uns entschieden, so können wir aus der Hackerethik nur eine von zwei möglichen Konsequenzen ableiten: Öffentliche Daten gilt es zu nutzen, private Daten hingegen zu schützen, hier sollen Mittel bereitgestellt und angewendet werden, um diese Daten vor ungewünschter Verbreitung zu bewahren.

[1] Levy, S.: Hackers – Heroes of the Computer Revolution. Anchor Press, Garden City, 1984.

[2] Tech Model Railroad Club of MIT: TMRC History. http://tmrc.mit.edu/history/, visited on 2011-02-28.

[3] Raymond, Steele, et al.: The New Hacker's Dictionary. MIT Press, Cambridge, 1998.

[4] Chaosradio 124: Hands-On Hacking – Always Yield To The Hands On Imperative. http://chaosradio.ccc.de/cr124.html, visited on 2011-03-05.

[5] Clarke, R.: Information wants to be free. http://www.rogerclarke.com/II/IWtbF.html, visited on 2010-10-26.

[6] Offene Netze – Jetzt, Datenschleuder 24, 1987.

[7] Löwgren, J.: Hacker culture(s). http://webzone.k3.mah.se/k3jolo/HackerCultures/, visited on 2011-03-05, Traditional hacker ethics.

[8] Mizrach, S.: Is there a hacker ethic for 90s hackers? http://www2.fiu.edu/~mizrachs/hackethic.html, visited on 2010-08-21.

[9] Krempl, S.: Gute Hacker, böse Hacker. http://www.zeit.de/1999/05/199905.comp_hackerethik.xml, visited on 2010-11-28.

Muß man neutral bleiben?

von Hans-Christian Espérer <hc@hcesperer.org> und Andreas Portele <andreas@portele.com>

Über die Netzneutralität wird inzwischen schon eine ganze Weile diskutiert; ein Konsens – auch innerhalb des Chaos Computer Clubs – scheint bisher nicht in Sicht. Komplex ist es ja, das Thema, und immer, wenn man eine Lösung gefunden zu haben glaubt, taucht ein neues Argument auf, ein weiterer Punkt, der das Konstrukt wieder über den Haufen wirft.

Wir wissen da auch keinen so rechten Ausweg, daher versuchen wir es stattdessen mit einer Utopie. Und genauso, wie es bei Star Trek Gefängniszellen, Strafkolonien, und – in mindestens einem Fall – die Todesstrafe gibt, so ist auch unsere Utopie nicht perfekt: Wir gehen davon aus, daß die Übertragungskapazitäten endlich sind. Wären sie beliebig groß, so wäre das Problem gelöst.

Die Problematik der Netzneutralität kann man grob in zwei Kategorien unterteilen. Das zusätzliche Profitstreben durch Aufhebung der Netzneutralität und der teilweisen Wiederherstellung selbiger durch beispielsweise die Zahlung eines Aufpreises fällt in die erste Kategorie. Die Behandlung von Engpässen und Ermöglichung zeitkritischer Anwendungen wie der Internet-Telefonie oder Anwendungen in der Telemedizin, aber auch die Finanzierung der Internet-Infrastruktur selbst durch zusätzliche Einnahmen fallen in die zweite Kategorie.

Profit

Was die erste Kategorie betrifft, so dürfte ein breiter Konsens bestehen unter all jenen, die sich mit der Thematik beschäftigt haben: Die Netzneutralität muß in jedem Fall aufrechterhalten werden. Man kann hier selbst durch trivialste Einschränkungen mitunter einen nicht zu unterschätzenden Profit herausschlagen. Die Autoren dieses Artikels könnte man damit ziemlich gut ausnehmen, auf eine ganz einfache Art und Weise: Unsere Provider müßten nur ssh sperren. Über ssh lesen und schreiben wir unter anderem E-Mails und chatten mit diversen Leuten, also zwei ganz alltägliche Sachen. Wir würden unseren Providern bereitwillig eine monatliche Extrazahlung leisten, damit wir ssh benutzen können.

Oft wird in der Praxis tatsächlich schon gefiltert: So würden wir zum Beispiel so mancher Lokalität, die einen öffentlichen Internetzugang anbietet oder einen für ihre Mitglieder, durchaus einen kleinen monatlichen Beitrag zahlen, wenn sie im Gegenzug ihre Portfilter abstellen. Denn diese Portfilter machen uns nicht nur verrückt, sie machen es uns unmöglich, produktiv zu arbeiten oder auch nur E-Mails zu lesen; die Annahme, produktiv arbeite man im WWW und alles andere sei nur zum Zeitvertreib erforderlich, mag auf einen Teil der Bevölkerung zutreffen – auf jenen, der nur einen kleinen, zwar gut sichtbaren Teil des Internets wirklich benutzt, aber Allgemeingültigkeit hat sie keinesfalls. Zu Hause nun sind wir existenziell darauf angewiesen, daß nicht gefiltert wird. Wenn der Zusatzbetrag für ein ungefiltertes Internet zu hoch wäre und wir zwangsweise beispielsweise auf einen Webmail-Provider umsteigen müßten, weil wir unsere E-Mails sonst nicht mehr lesen könnte, würden wir dies tun – was bliebe uns denn anderes übrig? Adieu, du kleiner Rest Privatsphäre, der uns in dem Fall auch noch abhanden käme.

IT'S NOT A BUG, IT'S A FEATURE! JEDE EINSCHRÄNKUNG IM NETZ KANN ANSCHLIESSEND ALS SONDERDIENSTLEISTUNG VERKAUFT

Technik

Bei der zweiten Kategorie wird es komplizierter. Betrachtet seien zunächst einmal die Endkundenprovider (ISPs), also jene Provider, die für Leute wie uns, die nicht über den Luxus einer Zehn-Gigabyte-Leitung im Büro und einer Darkfiber nach Hause verfügen, den Zugang zum Internet ermöglichen.

Für die Betrachtung der Probleme der zweiten Kategorie gehen wir nun davon aus, daß die ISPs nicht aus unmittelbarem Profitstreben das Internet filtern – wie auch immer geartet, sei es durch einfache Portfilterungen oder subtilere Maßnahmen wie Traffic-Drosselung oder Bevorzugung eigener Dienste vor denen der Konkurrenz.

Unsere Utopie ist ja nicht perfekt, da die Bandbreiten nicht beliebig groß sind. Das Internet ist groß geworden aufgrund seiner inhärenten Struktur: Jeder kann mit jedem kommunizieren, egal, wo sich die Kommunikationspartner befinden. Befinden sie sich nicht im gleichen Subnetz, so wird geroutet. Befinden sich die beiden Kommunikationspartner nicht im selben autonomen System, so wird über das Transfernetz geroutet, dem eigentlichen „Internet", dem Netz der Netze. Das Transfernetz verbindet die autonomen Systeme miteinander; jeder ISP, jede Universität und jedes größere Unternehmen betreiben jeweils ein autonomes System; die Menge aller autonomen Systeme bildet das Internet.

Daraus ergibt sich zwangsläufig, daß es keine garantierten Bandbreiten geben kann: Um Mindestbandbreiten zu garantieren, müßte man jeden Punkt mit jedem Punkt direkt verbinden – aber daß genau dies für ein Funktionieren des Internets eben nicht erforderlich ist, diese Tatsache hat den Erfolg des Internets überhaupt erst ermöglicht. Momentan fällt diese Limitierung nicht so sehr auf, da Endkundenanschlüsse generell um ein Vielfaches langsamer sind als das Transfernetz und die autonomen Systeme der ISPs.

Trotzdem ist diese Erkenntnis von elementarer Bedeutung: Selbst im schnellsten Internet kann es prinzipbedingt keine garantierten Bandbreiten geben. Wer also garantierte Bandbreiten fordert, zweifelt in gewisser Weise an der Funktionsweise des Internets selbst.

NIEMAND IST PERFEKT, AUCH DAS INTERNET NICHT. ES GEHT VIEL, SEHR VIEL, ABER NICHT ALLES.

Bandbreite

Neben der Forderung nach Mindestbandbreiten ist die arbiträre Limitierung von Bandbreiten eine gängige Form der Verletzung der Netzneutralität. Viele Provider argumentieren, sie müßten bestimmten Traffic drosseln, um zu verhindern, daß ihre Netze überlastet werden. In manchen Fällen entspricht dies einfach nicht der Wahrheit, in anderen Fällen haben diese Provider Dienstleistungen verkauft, die sie nicht vollumfänglich erbringen können und stolpern nun über ihre Kalkulation. In allen Fällen gibt es keine zuverlässigen öffentlichen Zahlen, die das eine oder das andere Argument untermauern.

Der Verkauf von Dienstleistungen, die in der Praxis nicht erbracht werden können – im Volksmund Flatrates genannt –, wird oftmals damit gerechtfertigt, daß viele Kunden gar nicht wüßten, ob sie monatlich zwei Gigabyte oder zwei Terabyte Traffic verbrauchen. In unserer Utopie wissen das alle aufgeklärten Bürger oder

können es zumindest grob einschätzen. Denn die Eltern bringen es ihren Kindern bei, und für jene aus bildungsferneren Schichten gibt es Grundkurse zum Umgang mit dem Internet – ernstzunehmende Kurse, keine Propagandaveranstaltungen. Darüberhinaus gibt es bereits heute viele Router für daheim, die schöne Graphiken und Statistiken über den Traffic-Verbrauch darstellen können. Man hat ja für gewöhnlich auch keine Stromflatrate zu Hause, denkt aber auch nicht über jede Sekunde nach, die der Computer eingeschaltet ist. In unserer Utopie gibt es keine Flatrates, nur Volumentarife mit vernünftigen Mindestanforderungen oder Bitstream Access zu vernünftigen Konditionen.

BILDUNG IST WICHTIG, UND ALLES HAT SEINEN PREIS.

Latenz

Als nächstes Argument der Netzneutralitätsgegner kommt das der Latenz. Diese spiele bei einigen Diensten eine wesentlichere Rolle als bei anderen. Hierbei stellt sich nicht nur die Frage, bei welchen Diensten die Latenz welche Rolle spielt. Viel wichtiger ist die Frage, wer dies entscheidet. Letzteres läßt sich nämlich nicht ohne weiteres beantworten. In unserer Utopie gilt: Der Endkunde entscheidet. Und Endkunden halten die von ihnen genutzten Dienste grundsätzlich für wichtiger als die der Nachbarn.

Ein vielgenutzter Dienst, bei dem die Latenz eine wichtige Rolle spielt, ist die Internettelefonie. Daneben gibt es diverse Livestreams und solche Dinge wie Telemedizin, wo Ausfallsicherheit und niedrige Latenz gleichermaßen eine große Rolle spielen.

Viele Leute wollen die verschiedensten Dinge mit dem Internet anstellen. Das Internet – durch und durch ein Konstrukt der Hackerkultur – läßt sich biegen und verformen, bis manches Unmögliche eben doch möglich ist. Aber zum Teil nur mit wirklich viel Biegen und Brechen, und schön ist das Resultat oftmals in keiner Weise. Man biegt solange, bis es bricht.

Schlimmer noch: Ein Experiment, einmal geglückt, resultiert oftmals in der merkwürdig anmutenden Erwartungshaltung, das Internet müsse den eben noch experimentell getesteten Einsatz nun dauerhaft und unter allen Wetterbedingungen unterstützen. Sei es Internet-Telefonie, sei es zeitkritische Telemedizin, sei es irgendein hochauflösendes Fernsehprogramm, das man plötzlich kostengünstig oder werbewirksam über das Internet übertragen möchte.

In unserer Utopie weiß man die Bedeutung des Internets und dessen Stärken und Schwächen gut einzuschätzen. Wer die Forderung stellt, Telemedizin, womöglich im Sinne von ferngesteuerten Liveoperationen, müsse über das Internet möglich sein, hat dessen Funktionsprinzip nicht verstanden. Durch seine heterogene Struktur aus vielen Netzen, verbunden nur über das Transfernetz, sind Garantien aller Art schlicht unmöglich. Das Einzige, das man von allen Netzbetreibern realistisch verlangen kann, ist es, maximale Kooperation im Netzbetrieb an den Tag zu legen, und dieses sollte man auch konsequent fordern.

WER HÖCHSTE ANSPRÜCHE AN VERFÜGBARKEIT, BANDBREITE ODER LATENZ STELLT, SOLLTE DAVON ABSEHEN, DAS INTERNET ZU BENUTZEN, DENN DAFÜR IST ES NICHT GEBAUT.

Man stelle sich nur mal einen Hacker vor, der im Jahre 1960 zu einer Rundfunkanstalt geht und fordert, jedes Radio müsse über einen Musik-Aus!-TM-Knopf instantanes Feedback an das Funkhaus liefern können, so daß ein Lied abgebrochen wird, wenn sich die Mehrheit der Hörer dafür ausspricht. Man hätte den Hacker im besten Fall vermutlich ausgelacht. Ber der Rundfunktechnologie gibt es einen Sender und viele Empfänger – ein fundamentaler Unterschied zum Internet.

In unserer Utopie bleibt diese Eigenschaft der Peer-to-Peer- oder Ende-zu-Ende-Kommunikation im Internet erhalten und ist gesetzlich im Mindestinternetanschluß garantiert. Jeder Privatkunde im Netz hat das Recht, jede Art von Dienst an seinem Anschluß anzubieten, den er möchte. Heute dagegen steht in vielen AGBs von ISPs, daß „der Betrieb von Serverdiensten" ausgeschlossen ist. Dies widerspricht der Natur des Internets. Die Probleme fangen schon bei der Definition eines Serverdienstes an: Zählen VOIP/SIP-Telefone genauso dazu wie ein X11-Server und der Drucker oder Fotoaparat, der sich daheim im Netz anmeldet, um seine Dienste anzubieten?

KEIN DATENPAKET IST ILLEGAL.

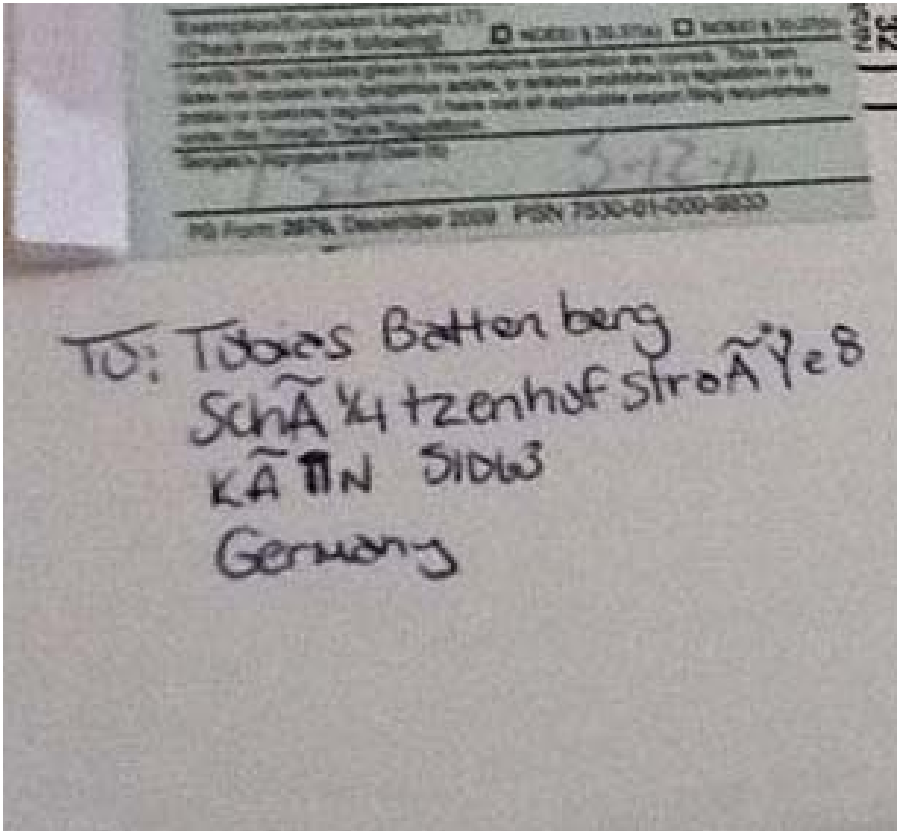
Was ist nun aber mit Priorisierung von Traffic im Zusammenhang mit ssh? ssh ist ein elementarer Teil des Internets. Wir behaupten einfach mal: Geht ssh nicht mehr, so bricht ein Großteil unserer Infrastruktur nach und nach aufgrund von Vernachlässigung und mangelnder Wartung weg. ssh profitiert von einer geringen Latenz, braucht sie aber nicht unbedingt. Mit ein bißchen Übung kann man als geschickter Systemadministrator auch eine größere Latenz verkraften. Wenn die Latenz zu hoch wird, wenn sie, sagen wir, 500 Millisekunden überschreitet, dann ist die logische Konzequenz in unserer Utopie aber nicht die, selektiv Traffic zu priorisieren. Wenn ssh in unserer Utopie zu langsam wird, ist die einzig logische Konsequenz der Ausbau der Netze.

Einige Anbieter und sicher mancher Kunde würde gerne Traffic-Priorisierung für bestimmte Dienste dazukaufen. Die Idee ist Folgende: Man bietet ein sogenanntes „Mindestinternet"' an; will man mehr, so zahlt man auch mehr. Aber zahlt man auch genug? Die ISPs freuen sich über die zusätzlichen Einnahmen, die sie erreichen können, ohne das Netz ausbauen zu müssen. Die vorhandenen Leitungen werden einfach in immer kleinere Stücke gehackt und zu immer höheren Preisen verkauft. Um die Preise zu halten, wird also statt mehr Bandbreite einfach eine höhere Priorisierung verkauft. Um damit gegen den Nachbarn mit besonders schnellem Internet zu prahlen, ist das vollkommen ausreichend. Wer Traffic-Priorisierung möchte, kauft, mietet oder verlegt in unserer Utopie eigene Leitungen. Diese Leitungen haben eine konstante garantierte Bitrate, diese kann man dann nutzen, wie man möchte.

Nochmal zur Drosselung einzelner Dienste: An manchen Stellen erscheint eine Priorisierung bestimmten Traffics durchaus angebracht. Zum Beispiel könnte man argumentieren, ein langwieriger Datei-Download könne gegenüber einem Telefongespräch vernachlässigt werden – ob besagter Download nun drei oder vier Stunden dauert, sei unerheblich. Es darf hierbei nur eines nicht vergessen werden: Ein zunächst rein quantitativer Unterschied resultiert oft in einer qualitativen Verschiebung. So hat beispielsweise das MP3-Format nicht etwa den Musikaustausch über das – damals noch um einiges langsamere – Internet ermöglicht. Es hat ihn lediglich lukrativer gemacht, da die Downloadzeiten erträglich wurden. Eine rein quantitative Änderung (Reduktion der Dateigröße) resultierte damit in einer qualitativen Änderung (massenweiser Austausch von Musik). Es müßte also

für diese Art von Traffic-Priorisierung ein unabhängiges Gremium geben, das für einzelne Protokolle und Dienste genau festlegt, welche Mindestbandbreiten und -latenzgrenzen eingehalten werden müssen. Wie gut es um unabhängige Gremien bestellt ist, sei an dieser Stelle dahingestellt.

Die Probleme hören bei der Beziehung zwischen Endkundenprovidern und Endkunden längst nicht auf, es gibt da noch die mitunter sehr häßliche Thematik der Nutzung des Transfernetzes. Jenes Netzes also, das die autonomen Systeme der Provider, Universitäten und Rechenzentrenbetreiber untereinander verbindet. Hier bestimmen individuelle Verträge, auch Peering-Abkommen genannt, das Gesamtbild. Dabei kommt es schon einmal vor, daß ein großer Provider einem anderen großen Provider günstige Konditionen einräumt – die beiden profitieren voneinander –, während ein kleiner Provider sich mit einseitigen Konditionen abfinden muß. In unserer Utopie wird das Internet als der Allgemeinheit dienliches Kulturgut angesehen – ein bißchen vergleichbar mit einem Haus, das unter Denkmalschutz steht: Das Haus hat zwar einen Eigentümer, er darf es jedoch nicht nach Belieben abreißen oder entstellen. In unserer Utopie gibt es Gesetze, die Provider zum Peering unter gewissen Rahmenbedingungen verpflichten. Und zwar in jedem Staat, denn die aufgeklärten Weltbürger haben ihre entsprechenden Regierungen zu diesen Gesetzen gedrängt. Mehr noch: Die Regierungen haben eine entsprechende Notwendigkeit zum Teil selbst eingesehen.



Gesichtswiedererkennung – Vorsicht Kamera

von Malte Springer <malte.springer@alice.de>

Das Thema Google Street View war in Deutschland in aller Munde. Die Medienmaschine wurde angeschoben von der öffentlichen Angst vor steigender Transparenz und dem stetigen Verlust der Privatsphäre.

Während im Jahr 2005 die Einführung des elektronischen Reisepasses vor allem wegen der staatlichen Erfassung biometrischer Daten zu einer öffentlichen Datenschutzdiskussion geführt hat, entwickeln die großen sozialen Netzwerke und Anbieter von Onlinediensten abseits des öffentlichen Interesses immer genauere Methoden zur kommerziellen Gesichtserkennung in Bilddateien.

Bis heute werden die meisten Bilddaten im Internet nur gefunden, wenn eine textliche Beschreibung des Bildmotivs im Zusammenhang mit der Bilddatei zu finden ist. Klassische Bildsuchmaschinen assoziieren dann die Adresse der Bilddatei mit den Suchbegriffen, die sie in der Nähe des Fotos gefunden haben. Die Bildsuchmaschine findet also im eigentlichen Sinn keine Bilder. Vielmehr findet sie relevante Webseiten, aus denen sie ausgewählte Bilder lädt und strukturiert darstellt. Die Voraussetzung für gute Suchergebnisse ist hierbei die relevante Beschreibung des Bildmotivs im Quellcode der Webseite, in der URL, im Dateinamen des Bildes oder in den beschreibenden Tags des Fotos. Das Suchresultat ist somit weitestgehend abhängig vom Autor, der eine Bilddatei im Internet publiziert. Der Autor muß das Motiv kennen, erkennen und richtig beschreiben, damit es bei den relevanten Suchbegriffen auch gefunden wird. In der Vergangenheit führte dies oftmals zu schlechten Suchergebnissen.

Treffgenauere Suchergebnisse erhält man, wenn die Software der Bildsuchmaschine selber dabei hilft, Motive eigenständig zu erkennen. Die automatische Interpretation von Bildinhalten war in der Vergangenheit jedoch sehr rechen- und somit kostenintensiv, denn die Bildsuchmaschine muß dabei bis zu mehreren Millionen Pixel je Bilddatei in Bezug auf Ihre Farbe und Anordnung untersuchen und die Ergebnisse indexieren. Daher beschränkte sich beispielsweise Google zunächst darauf, einen von zwölf Hauptfarbwerten eines Bildmotivs zu ermitteln. Sucht man etwa ein Foto eines gelben VW Golf III, so genügt die Textsuche nach „Golf 3“ kombiniert mit dem Suchfilter „gelb“. Die Farbe Gelb wird dabei nicht als textlicher Begriff auf Webseiten gesucht. Vielmehr hat Google für die gefundenen Bilder die Farbwerte aus den Motiven gelesen und den Hauptfarbwert ebenfalls indexiert. Das Suchergebnis sind Bilder, die im textlichen Zusammenhang mit den Suchbegriffen stehen und einen hohen Anteil des selektierten Farbwertes aufweisen.

Die oben beschriebene Kombination aus textlicher Bildsuche und Interpretation der Farbwerte ist jedoch noch immer fehleranfällig. Als Ergebnis kann man theoretisch auch ein gebrauchtes Lenkrad vor einem gelben Hintergrund erhalten. Um einer Suchmaschine nun den Unterschied zwischen einem Lenkrad und einem PKW zu erklären, braucht die Suchmaschine eine menschliche Hilfestellung. Dafür werden die indexierten Farbwerte und Muster in der Pixelanordnungen von Menschen verschlagwortet. Google bedient sich dazu des Spieltriebs seiner Nutzer. Mit dem Google Image Labeler sammelt der Konzern seit einigen Jahren auf spielerische Weise Informationen zu Millionen

von Bildmotiven. Die Bildsuchmaschine erlernt durch zahlreiche Freiwillige neben Farben auch Formen und so schließlich Motive zu unterscheiden.

Ein neueres Ergebnis dieser Technologie ist die einfache Gesichtserkennung. Der Suchbegriff „Paris“ liefert per Google-Bildersuche in den Top-Ergebnissen hauptsächlich Bilder der französischen Hauptstadt. Durch Betätigung des Suchfilters „Gesichter“ lassen sich die Suchergebnisse auf Abbildungen von Gesichtern im Zusammenhang mit „Paris“ einschränken. Der Bildersuchmaschine ist anhand von Farbwerten und Formen bekannt, bei welchen der Suchergebnissen es sich um Darstellungen von Gesichtern handelt. Die Bildsuchergebnisse zum Wort „Paris“ werden also auf die Bilder reduziert, die Gesichter zeigen und durch die gängigen Algorithmen der Google-Suche sortiert. Somit landen die Bilder der bekannten Hotelerbin Paris Hilton dann auf den ersten Suchplätzen. Weitere Beispiele für die Anwendung dieser Technik sind die automatische Verpixelung von Gesichtern und KFZ-Kennzeichen in Google-Street-View-Bildern und die Suche ähnlicher Fotos in der Google-Bildsuche.

An der Gesichtserkennungsfunktion der Desktop-Software Picasa von Google kann man heute schon sehen, wie gut nicht nur das technische Erkennen menschlicher Gesichter in Bildern funktionieren kann. Die Software identifiziert auch anhand von biometrischen Vermessungen, ob auf verschiedenen Bildern die gleiche Person abgebildet ist. Dem

Benutzer wird dann angeboten, den Namen der Person zu hinterlegen und letztlich alle lokal gespeicherten und indexierten Bilder mit dem Namen einer Person zu durchsuchen. Über die Synchronisation mit einem Webalbum können biometrisch analysierte Bilddaten samt der dazugehörigen personenbezogenen Daten in Form von Tags ins Internet gelangen und liefern die Basis für die automatische Wiedererkennung von Personen in Bilddateien.

Eine weitere Quelle für Basisdaten zur Erkennung von Gesichtern wächst in sozialen Netzwerken. Nach eigenen Angaben werden täglich einhundert Millionen neue Fotos allein auf der Plattform Facebook veröffentlicht. Wie auch in anderen sozialen Netzwerken haben die User dort immer komfortablere Möglichkeiten, sich selber, Freunde und Familie auf den Bildern zu verlinken. So entsteht ein riesiger Datenpool an Bildern mit den dazugehörigen Namen der Personen.

Und genau diese Veröffentlichung von Namen im Zusammenhang mit biometrisch analysierbaren Bilddaten birgt nicht absehbare Gefahren für den Datenschutz. Zusammen mit dem stetigen Anstieg der veröffentlichten privaten Bilder wird diese Entwicklung in absehbarer Zeit dazu führen, daß die frei zugängliche Bildsuche nach Privatpersonen ein Vielfaches der heutigen Ergebnisse liefern wird, und das auch bei Personen, die selber nicht in sozialen Netzwerken agieren bzw. selber keine Fotos posten oder taggen.

Bislang stammen die Bildresultate der Suche nach einer Privatperson aus dem überschaubaren Umfeld des Menschen selber, da die Person dem Autor namentlich bekannt sein muß, damit eine Relation zwischen dem Bild und dem Namen hergestellt werden kann. Jeder von uns wird allerdings nicht nur von Menschen aus dem eigenen und einigermaßen kontrollierbaren Umfeld fotographiert und gepostet. Vielmehr stehen wir bislang häufig anonym im Hintergrund einer Vielzahl von Fotos, von deren Existenz wir nichts ahnen. Sei es im Urlaub am Strand, während eines Konzertes in der Masse, in der Disco oder durch eine Webcam auf dem Arbeitsweg. Ständig sind wir ungewollte und bislang anonyme Motive von unzähligen Fotographen.

Die Bekanntheit von biometrischen Daten in Zusammenhang mit dem Namen ermöglicht nun die automatische Verschlagwortung eines jeden Bildmotivs mit den Namen aller abgebildeten und erkennbaren Personen. Zukünftig könnten so unzählige Bilder als Suchresultate zu einem Namen auftauchen, die den Menschen in jeder erdenklichen Lebenslage zeigen, seine Aufenthaltsorte aus Geotags rekonstruierbar machen oder gar eine Rückwertsuche ermöglichen. Bei letzterer reicht dann ein Handyfoto einer Person, um nicht nur den Namen, sondern auch weitere private Informationen beispielsweise aus sozialen Netzwerken über den Menschen zu finden. Außerdem lassen sich so aus Fotos Beziehungen zwischen Personen rekonstruieren, denn oft sind es Freunde, Familienmitglieder und Kollegen, die auf dem gleichen Foto abgebildet sind.

Geschützt werden die Bilddaten mit assoziierten Namen lediglich durch das kommerzielle Interesse der Betreiber. So lassen sich mit neuen Technologien zum einen User länger an ein Onlineangebot binden, zum anderen läßt sich die Bekanntheit privater Informationen werblich kommerzialisieren. Es bleibt nur zu hoffen, daß die technische Komplexität und die Geschwindigkeit der Entwicklung den Gesetzgeber nicht wieder überholen. Sind die Daten erst einmal frei zugänglich, wird es nahezu unmöglich, sie wieder aus dem Netz zu nehmen.

Der dezentrale Club

von Martin Haase <maha@ccc.de>

Kurze Durchsage des Erfa-Repräsentanten

Der CCC kämpft für freie und neutrale Netze, aber die Informationsfreiheit ist akut in Gefahr. Manche sprechen von einem „Information War" oder einem „War on Infrastructure". Tatsächlich ist damit zu rechnen, daß bei einem Terroranschlag in Deutschland Handy-Netze abgeschaltet werden. Das Internet kann zwar nicht völlig abgeschaltet werden, aber wichtige Netz-Infrastruktur kann ausgeschaltet oder zumindest überwacht und gefiltert werden. Für eine Filterung ist nicht mal ein Krisenfall nötig: Internetsperren können von heute auf morgen zur Anwendung kommen, und mit dem ACTA-Handelsabkommen (Anti-Counterfeiting Trade Agreement) stehen Möglichkeiten bereit, einzelne Nutzer vom Netz unter Umgehung des Rechtswegs auszuschließen. Was kann der Chaos Computer Club angesichts dieser düsteren Aussichten, die nicht einmal in einer fernen Zukunft angesiedelt sind, tun?

Neben seinem Bürgerrechtsengagement liegt es nahe, daß sich der Club infrastrukturell auf das Bedrohungsszenario einstellt. Hier ist vor allem Dezentralisierung nötig. Dezentralisierung des Clubs bedeutet zunächst, daß es möglichst viele „Filialen" gibt, also möglichst viele Erfa-Kreise und Chaostreffs. Die Erfa-Kreise müssen die Arbeit unter sich so aufteilen, daß es nicht eine einzelne Gruppe gibt, deren Lahmlegung die ganze Clubarbeit gefährdet. Die Aktiven in den regionalen Filialen müssen natürlich gut vernetzt sein (der Name „Erfahrungsaustausch" legt das ja schon nahe). Daher muß es mehr dezentral organisierte Treffen („Geekends" und ähnliches) geben. Den Club auf nur eine zentrale Veranstaltung auszurichten, die noch dazu aus allen Nähten platzt, ist keine nachhaltige Strategie.

Vor allem geht es darum, eine dezentrale Kommunikationsinfrastruktur zu schaffen. Wichtige Projekte in diesem Zusammenhang sind das „decentralized network 42" (kurz dn42) [1] und das ChaosVPN [2], beide sollten weiterentwickelt werden. Hinzu kommt die dezentrale Bereitstellung von freien Inhalten (*media.ccc.de*) – auch über bittorrent – und vor allem der Ausbau von Freifunk [3]. Einige Erfa-Kreise und Chaostreffs arbeiten ja schon mit Freifunkinitiativen zusammen (zum Beispiel im Rheinland und in Berlin); freie Funknetze müssen (wieder) ein Hauptanliegen des dezentralen CCC sein. Die jüngste Vergangenheit (insbesondere die Revolution in Ägypten) haben im Übrigen gezeigt, daß zur Bereitstellung von Netzzugängen auch wieder der altmodisch anmutende Betrieb von Einwahlmodems gehört [4]. Auch darum muß sich der CCC kümmern.

Freifunk soll es jedem ermöglichen, überall einen Netzzugang zu haben (und zwar „abschaltungsrobust"). Damit ist es auch eine Maßnahme gegen den Digital Divide. Der Digital Divide ist allerdings weniger ein technisches, sondern vor allem ein Bildungsproblem. Daher ist es ganz wichtig, daß der dezentrale CCC landauf, landab die digitale Kompetenz der Nicht-Internet-Eingeborenen erhöht. Das Projekt „Chaos macht Schule" [5] ist hier einschlägig und natürlich ausbaufähig.

[1] https://dn42.net/trac/
[2] http://wiki.hamburg.ccc.de/index.php/ChaosVPN
[3] http://de.wikipedia.org/wiki/Freies_Funknetz
[4] http://www.telecomix.org/
[5] http://chaos-macht-schule.org/

Datenspuren

vom CCC Dresden <mail@c3d2.de>

Alle Jahre wieder: Congress mit gigantischem Nerdspaß in Berlin, zusätzlich Woodstock für Hacker auf dem Camp. Wer jedoch nicht so lange auf derartige Veranstaltungen und den chaotischen Spaß verzichten will, den treibt es, über das Jahr verteilt, zu den kleineren Symposien, welche von lokalen Erfa-Kreisen realisiert werden. Übliche Verdächtige wurden, neben Easterhegg, GPN und MRMCD, diesmal nun schon zum siebten Mal in Folge auf den Datenspuren in Dresden angetroffen.

Die alljährliche und zweitägige Konferenz fand letztes Jahr vom 16. bis 17. Oktober erneut im Kulturzentrum „Scheune" der Dresdner Neustadt statt. Eingeladen waren wie immer alle selbstdenkenden Wesen, der Eintritt war auch diesmal wieder kostenlos.

Zeit, um das Backlog aufzuklappen, und anschließend einen Blick nach vorne zu werfen, um Euch, liebe Leser und Leserinnen, diese tolle Veranstaltung schmackhaft zu machen.

Backlog

Am 8. Mai 2004 fand unter dem Motto „Daten-Spuren – Privatsphäre war gestern" das erste Mal das Symposium des CCC Dresden statt. Auch wenn damals nur ein Tag eingeplant war, mangelte es nicht an Vorträgen: Achtzehn Vorträge in drei Räumen, anschließend eine Podiumsdiskussion zum Thema „Was habe ich zu verbergen?" legten die Meßlatte für die darauffolgenden Datenspuren hoch. Schon damals waren Themen wie Vorratsdatenspeicherung, das Mautsystem und die lokale Videoüberwachung Dresdens auf der Agenda.

Der kürzlich verstorbene Datenschutz- und Datensicherheitsexperte Prof. Andreas Pfitzmann gestaltete die Keynote bei diesen ersten Datenspuren. Eingeladen wurde damals mit „Ich weiß, was Du letzten Sommer gemailt hast"-Postkarten.

Im nächsten Jahr wurden die Räumlichkeiten gewechselt, das nerdfreundliche Kulturzentrum „Scheune", gelegen im lebendigen Stadtteil der Dresdner Neustadt, diente nun als Treffpunkt der Selbstdenkenden aus Dresden und Umgebung, welche mehr wissen wollten über Biometrie in Ausweisdokumenten, RFID, Lokalisierung in Handynetzen und anderen spannenden Themen, die sich mit dem Dualismus „Öffentliche Daten nützen, private Daten schützen" beschäftigten. Dazu bietet die Scheune neben Vortragsräumen ausreichend Platz, um bei einem selbstgebrauten Tschunk zu fachsimpeln und tiefer in die gerade besprochene Materie einzusteigen. Insgesamt handelte es sich seit jeher um eine sehr vielseitige Veranstaltung grundentspannter Atmosphäre und szeneträchtiger Umgebung.

Das Symposium wurde im Laufe der Zeit auf zwei Tage ausgedehnt, um somit dem stetig anwachsenden Besucherzulauf und den Themenbereichen, welche über die Jahre ständig wuchsen, weiterhin gerecht zu werden. Denn längst waren die Datenspuren nicht mehr nur eine regionale Veranstaltung, sondern weit über die sächsischen Grenzen hinaus für die gute Vortragsqualität und das nette Ambiente bekannt. Im Jahr 2009 gab es in drei Räumen über zwei Tage lang mehr als vierzig Stunden Vortragsprogramm. Hierbei bot die Veranstaltung wie gewohnt sowohl Einsteigervorträge für Laien als auch fortgeschrittenes Material.

Die letztjährigen Datenspuren fanden unter dem Motto „Mind the Gap“ statt, um auf die Kluft zwischen gefühlter und realer Privatsphäre aufmerksam zu machen. Am Anfang standen die Daten – und deren Nutzung.

In der Keynote sprachen fukami und Daniel Dietrich über Open-Data-Projekte in Deutschland – getreu der bekannten These „Private Daten schützen, öffentliche Daten nutzen“. Im Anschluß gab Mark Neis einen Überblick über den Stand des Überwachungsstaates – wie weit ist der Ausbau schon fortgeschritten? Im zweiten Teil dieses Vortrages, welcher am Sonntag stattfand, ging es dann um das Handelsabkommen „ACTA“ sowie das europäische Überwachungsvorhaben „INDECT“.

Weitere Themen waren der anstehende Zensus 2011 mit Oliver „unicorn“ Knapp, welcher bereits Stellungnahmen zum Zensus für verschiedene Landtage geschrieben hat, sowie ein Blick auf das Leuchtturmprojekt der Piratenpartei Liquid Feedback von maha. Ein Überraschungshighlight war der Vortrag „Ich weiß, was du letzte Nacht getan hast“. Hier hatten zwei lokale Nerds eine Idee und bauten ein System, welches die Metadaten verschiedener Sozialer Netzwerke (Microblogging, Last. FM) sammelte und auswertete. Daraus wurden Punchcards erstellt, welche Tagesrhythmen und Urlaubszeiten sehr anschaulich darstellen. Den Höhepunkt bildete am Samstag ein Panel mit plomlompom, unicorn und fukami, welche, moderiert von Tim Pritlove, über den Stand der Privatsphäre in Deutschland debattierten.

Am Sonntag warfen wir einen Blick auf die Weitergabe von Daten durch Meldeämter, wir erfuhren, wie Gentests arbeiten und wie Social Engineering funktioniert. Wieder war die omnipräsente Fragestellung, wie man die Gesellschaft besser für das Thema Datenschutz sensibilisiert.

Neben den Vorträgen gab es wieder viel Zeit und Raum, um sich zu informieren, zu nerden, zu diskutieren oder sich durch einen gelungenen Lightning Talk interessierte Mitstreiter für neue oder bereits laufende Projekte anzuheuern. Abgeschlossen wurden die Datenspuren dieses Jahr mit einem unerwarteten Ansturm auf das von Alien8 und Astro durchgeführte Nerdquiz. In drei Runden schlugen sich neun Kandidaten bis in die Endrunde, um in einer „knappen“ Entscheidung geflasht zu werden.

An dieser Stelle möchten wir dem Chaos Computer Club e. V. noch einmal herzlich für die allseitige Unterstützung danken, welche es uns ermöglicht, diese Veranstaltung bisher und sicher auch weiterhin ohne die Erhebung von Eintrittspreisen durchzuführen. Nur damit sind die Datenspuren eine der wenigen Chaosveranstaltungen, die sich auch an den Querschnitt der Bevölkerung wenden. Auch an alle freiwilligen Helfer einen großen Dank!

Das Internet darf kein rechtsfreier Raum sein

von Twister

Quelle: BMI/Schaaf

Montagmorgen, das Telefon klingelt laut.
Ich nehme ab, die Stimme klingt vertraut.
„Wir müssten da noch etwas über ihr Blog bereden“,
höre ich den Anwalt vor Zorne beben.

„Da hat schon wieder einer so ein Bild online gestellt.
So langsam ist es um ihr Blog ganz schlecht bestellt.“
Ich lege auf und logge mich schnell ein,
beseitige das Bild, doch schnell fällt mir ein,
dass das nur für kurze Zeit helfen kann,
denn spätestens morgen fängt es wieder an.

Blindfische, die mir die Zeit stehlen,
Blindfische, die sich als Trolle empfehlen,
Blindfische, die die mir sagen, tagaus, tagein:
„Das Internet darf kein rechtsfreier Raum sein.“

Dienstagmorgen, ein Anwaltschreiben.
Der Bilderposter lässt es halt nicht bleiben.
Außerdem fehlt beim Blog ein Impressum.
Das wüsste ich sehr wohl, ich sei ja nicht dumm.
Kostet diesmal nur tausend Euro, fast ein Sonderangebot.
Wäre da nicht der nächste Anwalt, der mir droht.
Denn schließlich steht im Blog was über meine Firma.
Dass das nicht gut geht, war eigentlich klar.
Ist eigentlich nur die Wahrheit, aber wen interessiert das schon?
Ich zahle brav – weg ist der Lohn.

Blindfische, die mir die Zeit stehlen,
Blindfische, die sich als Trolle empfehlen,
Blindfische, die die mir sagen, tagaus, tagein:
„Das Internet darf kein rechtsfreier Raum sein."

Mittwochmorgen ist es wieder soweit.
Der Briefträger hält ein paar Schreiben bereit.
Das Bild von meiner Freundin ist der Stein vom Anstoß.
Sie sieht doch hübsch aus, was haben die bloß?
Achso, zu jung, tja, was soll sie denn machen?
Antibotox spritzen oder solche Sachen?
Nur damit sie nicht mehr wie 15 aussieht?
Egal – weg damit ist das Ende vom Lied.

Gleich danach kommt das Schreiben von der MI.
Ich hätte, sagt ein Anwalt der Industrie,
auf einer Tauschbörse mit Liedern gehandelt.
Mit Leuten getauscht, mit denen ich verbandelt
oder irgendwie verwandt bin, wie auch immer.
Ich blick da nicht durch, hab keinen Schimmer.
Ich ruf den Anwalt an, seine Worte klingen gedrechselt.
„Achje", sagt er lässig, „IP-Adresse verwechselt.
Vergessen Sie es einfach, guter Mann.
Aber sollten Sie sowas tun, dann sind Sie dran."
Ich lege auf und seufze laut.
Der Typ hat mir gerade den Tag versaut.

Blindfische, die mir die Zeit stehlen,
Blindfische, die sich als Trolle empfehlen,
Blindfische, die die mir sagen, tagaus, tagein:
„Das Internet darf kein rechtsfreier Raum sein."

Donnerstag – mein Blog ist offline, ich weiß nicht warum.
Mein Provider sagt: „Stell Dich nicht dumm."
Doch er kann mir nicht genau sagen, was passiert ist.
Ich fühle mich, sorry, leicht angepisst.

Urheberrechtsverletzung, sagt der Provider,
aber leider, leider
hat er und auch der Typ, der alles inszenierte
und mal wieder nichts kapierte,
nicht verstanden, dass „Ronny Kräutersame“
nichts anderes ist als mein echter Name.
Man hätte versucht, den Urheber des Songs herauszufinden,
sagt man mir – meine Sinne schwinden,
ich selbst bin der Urheber, Mann, versteht ihr es denn nicht?
Ich bin es, ich, der arme Wicht,
den ihr jeden Tag mit Euren Klagen und Verfügungen bedenkt.
Der Provider entschuldigt sich – geschenkt.

Blindfische, die mir die Zeit stehlen,
Blindfische, die sich als Trolle empfehlen,
Blindfische, die die mir sagen, tagaus, tagein:
„Das Internet darf kein rechtsfreier Raum sein.“

Der Freitag kommt, mein Blutdruck steigt an.
Ich weiß es, ich fühle es, Mann, oh Mann.
Heute werden sie wieder ankommen, diese geldeintreibenden Maden
mit ihren Verfügungen und Klagen.
Ich frage einen Politiker, ob er meint, das wäre so alles gerecht,
doch er fragt mich stattdessen erstmal – ganz echt –
nach meinem Namen,
ich sage „Ronny Kräutersame“.
Mit so einem Namen ist man wirklich dumm dran,
weil keiner wirklich glauben kann,
dass dies mein wirklicher Name ist,
so auch nicht der Politiker, der am anderen Ende spricht.

Er fragt mich nochmal nach dem echten Namen, wird lauter und lauter.
Ich sage letztendlich „Franz-Helmut Krauter“.
Er ist zufrieden, sagt mir, wie wichtig es wäre,
wenn jeder sich zu erkennen gibt in dieser Sphäre,
dann aber bricht das Gespräch ab,
und ich höre erst später, dass der Politiker einen Sohn hat,
der unter seinem Realnamen Rapsongs veröffentlicht
von Wichsern, Schlampen, von Bukakke und Gangbang bei Kerzenlicht.
Davon, dass der Herr Vater ihm empfohlen hat,
sich einen Rapnamen anzuschaffen, wie ihn jeder hat.
Und ich höre ganz am Ende dieser Litanei:
Der Sohn nennt sich jetzt „MC Heuchelei“.

The Concert

von Hans-Christian Espérer <hc@hcesperer.org>

Ein Konzert auf einer CCC-Veranstaltung? Ich bin ja von CCC-nahen Veranstaltungen schon einiges gewöhnt, im positiven Sinne, aber mit einem Konzert hätte ich dann doch nicht gerechnet. Das Ganze fing ganz harmlos mit einer Vortragseinreichung zum 27. Chaos Communication Congress an. Sie hatte den Titel „The Concert", und wurde vom Content-Team zwar etwas verunsichert, aber einstimmig angenommen.

Ein Konzertflügel wurde organisiert, der am zweiten Congresstag auch bei jedem Vortrag im großen Saal zu bewundern war. Um 18:30 Uhr an Tag zwei ging es dann los, unmittelbar vor Dan Bernsteins Vortrag zur Internet-Generalverschlüsselung. Corey Cerovsek an der Violine und Julien Quentin am Klavier – zwei hochkarätige Musiker, diese Bemerkung sei mir erlaubt – spielten Stücke diverser Komponisten, darunter Johannes Brahms und Claude Debussy.

x-foto.ch

Unterstützt wurden sie von Alex Antener, der eine Präsentation auf seinem Macintosh abspielte, synchronisiert mit der Musik, Thema: Das Verhältnis der Musik zum modernen Copyright. Besonders begeistert hat mich bei der Vorstellung die Kreutzer-Sonate von Beethoven, von den beiden in voller Länge meisterhaft gespielt. Zwischen den Musikstücken gab es kleine Youtube-Musikvideos diverser Künstler zu sehen, die aber jeweils nach dreißig Sekunden abgebrochen wurden – Fair Use erlaubt nicht mehr.

In der begleitenden Präsentation gab es unter anderem Auszüge aus verschiedenen Chats der Musiker zu lesen. Diese ließen sich dort ausgiebig über das moderne Copyright aus, das die künstlerische Entwicklung mehr behindere denn fördere. In der „Klassik-Szene" greife man daher hauptsächlich auf Werke zurück, deren Copyright ausgelaufen sei. Auch die stetige Verlängerung der Schutzfristen des Copyrights wurde, bezogen auf die USA, kritisiert. So sei das Copyright im 18. Jahrhundert auf maxi-

mal 42 Jahre aufgestockt worden, heute gelte das Copyright gar 95 Jahre. Mußte man früher explizit einen Antrag auf Verlängerung des Copyrights stellen, so falle dieser Schritt heute weg. Die Musiker waren einhellig der Meinung, daß zu lange Schutzfristen die Kreativität unterdrücken, anstatt sie zu fördern.

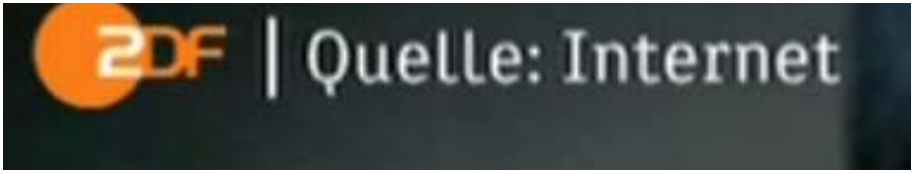
Auf Software-Patente wurde ebenfall kurz eingegangen: Die Stradivari und auch der Konzertflügel seien „patentfreie Open-Source-Technologien", deren Benutzung jedem ohne Einschränkung offenstehe. Der einzige limitierende Faktor sei das eigene Können. Auch Richard Stallman kam zu Wort, in Form eines kurzen Videoclips, und dachte darüber nach, was wäre, wenn man Musik patentieren könnte: „You are going to find that it is harder to write a symphony that you won't get sued for than write a symphony that sounds good."

Das Konzert endete mit stürmischem Beifall des überwältigten Publikums, und inzwischen ist die Veranstaltung laut Feedback-System der Konferenzplanungssoftware die beliebteste des 27c3 – offenbar waren nicht wenige Geeks und Hacker der stupiden Beats in den Kellerräumen des BCC überdrüssig und freuten sich über die erfrischende musikalische Abwechslung. Mir sind auch Gerüchte zu Ohren gekommen, wonach „The Concert" einige der Zuschauer dazu motiviert haben soll, öfter, gar regelmäßig ins Konzert zu gehen.

Ich muß ja sagen, daß mich die musikalische Darbietung wesentlich mehr überzeugt hat, als die Argumentationen zum Thema Copyright, die in meinen Augen etwas oberflächlich, unstrukturiert und hauptsächlich anhand eines einzigen Buches, „Free Culture" von Lawrence Lessig, geführt wurde. Einige interessante Denkanstöße bot sie aber durchaus.

Die Musiker spielten nach Ende ihres Vortragsslots munter weiter, bis unmittelbar zu Beginn des nächsten Vortrages. Die Aufzeichnung des Konzertes wurde leider streng zu Beginn der Pause unterbrochen, so daß die zahlreichen Zugaben in der Pause nicht als Download verfügbar sind. Die Aufnahme des eigentlichen Konzertes gibt es in annehmbarer Qualität zum Download: ftp://ftp.ccc.de/congress/27c3/mp4-h264-HQ/27c3-4201-en-the_concert_a_disconcerting_moment_for_free_culture.mp4

Bleibt für mich noch zu hoffen, daß Alex, Corey und Julien auf dem 28c3 wieder ein Konzert veranstalten werden, vielleicht diesmal mit der Musikredaktion vom WDR vor Ort, um die Veranstaltung professionell aufzuzeichnen.



Quelle: Internet

»Widerstand war zwecklos.«

von Hans-Christian Espérer <hc@hcesperer.org>

2082 – Die Journalistin Erica Bayer im Gespräch mit dem Widerstandskämpfer Marcel Salzberg anläßlich der vor dreißig Jahren abgeschafften »Datenkoppel« und dem damit verbundenen Zusammenbruch des Internets.

Herr Salzberg, Sie sind einer der wenigen Zeitzeugen. Ein Glück für uns, denn man hat ja damals alle Festplatten formatiert, alle Flash-Drives vernichtet.

Die Daten wurden vernichtet, ja. Man hatte Angst vor Viren, die später wieder hervortreten könnten, wenn man den alten Kram einer Untersuchung unterzieht. Das ist zumindest einer der Gründe.

Erinnern Sie sich noch an die Anfänge der Datenkoppel?

Ja, klar. Ich war ja damals in den besten Jahren, nicht? Also ich hatte ja schon früh angefangen, am „Komputer“ zu hocken, so sagte man damals, das war so 1993 ‚rum. Da war der Computer noch gleichberechtigt mit anderen Haushaltsgeräten, bis die Technik dann immer kleiner wurde. Die Datenkoppel kam recht spät. Ich glaube, so um 2011 rum. Vorher gab es diverse andere soziale Netzwerke – so nannte man sowas –, bis man dann irgendwann beschloß, in der „Koppel“ alle zu vereinen.

Warum?

Warum man diese Netzwerke schuf? Ich weiß es nicht genau. Meine Vermutung ist, daß dieser ganze Netzwerkkram von Geeks und Hakkern begonnen wurde, die einen echten Mehrwert für die Gesellschaft schaffen wollten, die den Leuten langweilige Arbeit abnehmen wollten. Diese Leute meinten es gut, aber sie merkten nicht, daß sie in Wahrheit unermüdlich daran arbeiteten, Werkzeuge für einen Diktator bereitzulegen. Wenn ich an dieser Stelle mal Paul Denton zitieren darf. Warum man dann die Koppel ins Leben rief? Die anderen Netzwerke hatten Probleme, da kam halt wieder jemand und behauptete, alles besser machen zu wollen. Und die Leute waren es inzwischen gewohnt, alle halbe Jahre in ein neues Netzwerk umzuziehen.

Wer steckte denn hinter der »Datenkoppel«? War das ein Unternehmen oder eine Einzelperson?

Es gab eine Person, die nannte sich »Der Protektor«. Ihren richtigen Namen erfuhren wir nie. Ebensowenig wußten wir, ob das Ganze ein Marketinggag war oder ob es diese Person wirklich gab und welche Rolle sie spielte.

Ist das nicht eine große Ironie, daß der vermeintliche Besitzer der Koppel pseudonym auftrat?

Ach was. Was sagen denn schon Namen? Die sagen fast genausowenig wie ein Geburtsdatum.

Aber gerade letzteres wurde doch bei der Anmeldung immer verlangt? Warum denn, wenn es so nichtssagend ist?

Warum verbeugt man sich vor einem König? Es ist ein Ritual. Allen Beteiligten wird klargemacht, wer hier das Sagen hat. Das geschah bei Koppel-Nutzern schon bei der Registrierung. Viele Leute glaubten, Widerstand zu leisten, indem sie ein falsches Geburtsdatum angaben. Wie sehr diese irrten. Daß diese Leute überhaupt etwas dort angaben, das war das Problem. Das Geburtsdatum konnte die Koppel sowieso deduzieren. Aber warum soll eine Firma mein Geburtsdatum wissen? Wenn ich es ihr ohne plausiblen Grund nenne, habe ich mich schon unterworfen. Nicht auch – sondern erst recht, wenn ich ein falsches Geburtsdatum angebe.

Sie fingen damals an, die Leute zu warnen.

Das ist richtig. Aber immer weniger Leute wollten mir zuhören. Ich glaube, viele, die einst den Staat für laxen Datenschutz kritisiert hatten, suchten nur Aufmerksamkeit, fühlten sich von der Gesellschaft nicht ernstgenommen. Als der Staat sie dann beachtete und als Firmen anfingen, benutzerfreundliche Software zu schreiben, die ihnen einen Mehrwert brachte, verstummten viele ehemals Kritische erstaunlich schnell. Zum Teil schlug die Stimmung sogar ins Gegenteil um. Und die wenigen, die noch aktiv waren, von denen forderten viele einfach nur mehr Datenschutz...

Der Datenschutz ist Ihnen nicht wichtig?

Doch, doch. Aber das Wort hat für mich mit der Zeit einen ganz negativen Beigeschmack bekommen. Der Datenschutz wurde oft als Ablenkung genutzt. Viele Leute konnten das Gewicht ihrer Daten gar nicht einschätzen. Und dann gab es immer diese schrecklichen Beispiele. Ohne Datenschutz würde man mehr Kleinkriminelle erwischen, zum Beispiel. Das war eine Argumentation der Datenschutzbefürworter, wohlgemerkt. Das müssen Sie sich einmal vorstellen. Und dann kam immer das „Totschlagargument" der personalisierten Werbung. Lassen Sie mich Ihnen eine persönliche Frage stellen: Würde es Sie stören, wenn Sie statt »normaler« personalisierte Werbung bekämen?

Also, ich glaube, Werbung würde mich so oder so stören. Zumindest in dieser aufdringlichen Form zu Beginn des 21. Jahrhunderts.

Präzise. Für mich ist beides – nichtpersonalisierte wie personalisierte Werbung – gleichermaßen verachtenswert. Aber die personalisierte Werbung war für viele das Hauptargument gegen »soziale Netzwerke«, nicht nur gegen die Koppel. Und, naja, viele wollten Datenschutz, aber dachten unbewußt bei sich, mehr als personalisierte Werbung kann mir nicht passieren, und das ist ja eigentlich nicht schlimm. Deshalb war der Widerstand sehr schnell gebrochen.

Und die Angst, sich mit seinen Daten völlig nakkig zu machen?

Naja, ignorance is bliss, Sie wissen schon. Und die Fantasie vieler reichte auch einfach nicht weit. Und dann war ja da dieses Ohnmachtsgefühl. Und, während immer mehr Leute glaubten, der Datenschutz sei das einzige Problem: Sie ignorierten dieses Problem gerne. Aber es gab ja noch viel größere Gefahren. Damals ging zum Beispiel der Trend mit der Zeitplanung los. Wenn Sie abends Lust auf ein Tennisspiel verspürten, sagten Sie nur der Koppel Bescheid. Die Koppel wußte um Ihre Finanzen. Sie suchte einen Tennisplatz heraus, den Sie sich leisten konnten. Die Koppel wußte, ob Sie ein Auto besaßen. Falls nicht, stellte sie sicher, daß der Tennisplatz per ÖPNV erreichbar war. Die Koppel wußte, welche Ihrer Freunde ebenfalls Tennis spielten. Die Koppel lud diejenigen Freunde ein, die Ihnen ebenbürtige Gegner sein würden. So wurde der Spielspaß maximiert. Fast keiner sah da ein Problem.

Das klingt ja auch nicht nach einem Problem. Das klingt nach einem echten Mehrwert.

Ein riesengroßer Mehrwert! Nur den Preis, den sahen viele nicht. Der Preis war, daß alle sozialen Ereignisse plötzlich von einem nebulösen Unternehmen zentral gesteuert wurden! Auf der ganzen Erde! Und was glauben Sie, wenn einer vom Netzwerk bestraft werden sollte, dann wurde er einfach nicht mehr eingeladen. Und durfte auch nicht mehr einladen. Und die Leute waren genervt, wenn man sie »manuell« einlud, weil das dann nicht in ihren Koppel-Kalendern berücksichtigt war. Plötzlich hatte man nicht nur Angst, gegen die mehr oder weniger demokratisch legitimierten Gesetze des eigenen Landes zu verstoßen. Noch größere Angst hatte man aber davor, gegen die Allgemeinen Geschäftsbedingungen einer Firma zu verstoßen, denn dies hätte im Extremfall zur kompletten Vereinsamung führen können.

Und traf das viele Leute?

Immer mehr. Auch offizielle Veranstaltungen wurden immer öfter über die Koppel organi-

siert. Irgendwann konnte man in seinen Koppel-Kalender keine »normalen« Events mehr eintragen – dadurch zwang die Koppel einen, alles, was man im Koppel-Kalender haben wollte, über diese Plattform zu organisieren. Viele Handys unterstützten nur noch den Koppel-Kalender. Wer also sein Handy zur Terminplanung nutzen wollte, mußte dies oftmals zwangsläufig komplett über die Koppel machen.

Gab es keine Leute, die sich trotz alldem noch »manuell« verabredet haben?

Sicher, einige Zeit schon.

Das hat doch die Koppel sicher gestört, wenn sie so machtbesessen war, wie Sie behaupten.

Naja, das waren ja wenige. Und die galten auch als wahnsinnig rückschrittlich. Man ist ihnen oft mit großer Aggression begegnet. Ich erinnere mich noch an einen Bekannten, den ich mal im Zug kennenlernte – Kalle hieß er, glaube ich –, der hat mich einen Lügner genannt, als ich ihm sagte, ich habe keinen Koppel-Account. Verstehen Sie, der hat geglaubt, ich hätte Angst vor ihm oder wolle seine Freundschaft nicht. Weil es in sein Weltbild nicht paßte, keinen Koppel-Account zu haben.

Hat denn die Koppel überhaupt auf die »Manuellen« reagiert?

Die Koppel hat nicht direkt darauf reagiert. Man hat nur irgendwann die sogenannten »freiwilligen Hausarreste« eingeführt.

Was war das?

Man konnte mit seinem Handy über Bilderkennung Leute »scannen«. Man sah dann, ob sich jemand unter Hausarrest befand. Die Koppel hatte irgendwann eine Funktion, die nannte sich »I Hate«. Wenn fünfzig Leute eine Person »hateten«, so nannte man das, dann stellte die Koppel diese gehatete Person für eine Woche unter Hausarrest.

Diese Hausarreste konnte man doch aber getrost ignorieren.

(lacht) Na klar, von Gesetzes wegen. Aber viele akzeptierten das. Unterschätzen Sie niemals die gesellschaftlichen Zwänge. Der Druck, sich einem Koppel-Hausarrest zu fügen, wuchs und wuchs; diese Realität kann man sich mit normaler Fantasie kaum vorstellen. Man wurde an vielen Orten nicht mehr toleriert, wenn das Handy des Gegenübers anzeigte, daß man unter Koppel-Hausarrest stand. Aus den fünfzig notwendigen »Hatern« wurden irgendwann zehn, später fünf. Und dann hat die Koppel natürlich auch nach eigenem Gutdünken Leute unter Hausarrest gestellt.

Hatte man keine Angst vor Willkür?

(lacht verächtlich) Ach was! Das wurde den Leuten als demokratische Errungenschaft verkauft! Endlich kein abgeschlossenes Jura-Studium mehr brauchen, um über jemanden zu richten. Das fanden viele toll – gelebte Demokratie! Mit dem Handy...

Aber waren die Leute nicht auch genervt von der ständigen Reizüberflutung? Von dem ständig »Auf-Empfang-Sein-Müssen«?

Schon, aber die Koppel bemühte sich, die Reizüberflutung zu minimieren. Freilich wollte man die Menschen aber auch zu einem ständigen Multitasking und Bereit-Sein umerziehen.

Gab es keine Möglichkeiten, sich dem zu entziehen?

Viele wollten es gar nicht. Sie glauben ja gar nicht – viele Menschen hatten ständig Angst, ihnen entgehe etwas wichtiges, vielleicht eine Liebschaft – was passierte, wenn sie mal für eine Stunde nicht erreichbar waren. Und es gab ja auch immer weniger Gründe, nicht online zu sein. Am Arbeitsplatz war das Handy erlaubt, auch an der Uni. In der Freizeit sowieso.

Wie war das im Kino?

Die wenigen Kinos, die es noch gab, wurden überwiegend von Leuten genutzt, die sich keine eigenen Projektoren leisten konnten oder deren Wohnung zu klein war, um eine ausreichend

große Leinwand aufzunehmen; es war im modernen Kino selbstverständlich, sein Handy niemals aus- oder stummzuschalten. Die Filme, die in den Kinos liefen, waren seichter Natur, so daß es niemanden störte, wenn ständig was los war, wenn Koppel-Nachrichten eintrafen oder gar jemand während des Films telefonierte. Im Gegenteil. Die Filme wurden später sogar gezielt darauf ausgelegt.

Leute, die sich einen Projektor leisten konnten, sahen Filme im kleineren Kreis zu Hause – da hatte man ja auch mehr Auswahl an Filmen. Die Koppel-Nachrichten wurden da direkt über den Beamer eingeblendet.

Ach ja, die Kinobetreiber erlebten eine Renaissance, waren mit die angesehensten Institutionen der Stadt. An ihnen war das Versprechen wirklich wahr geworden, daß die Technologie sie in den Wohlstand führen würde. Sie mußten gar nichts tun: Die Filme wurden automatisch ausgewählt, automatisch geliefert – die Publikumsplanung übernahm die Koppel. Die Wartung der Technik erfolgte ebenso automatisch. Kinobetreiber mußten einfach nur da sein; aus formalen Gründen mußte es halt einen Besitzer geben. Wie wurden die Kinobetreiber beneidet – sie waren zu meiner Zeit angesehener als so mancher Intendant.

Apropos Intendant... wie sah es denn in der Oper aus?

Kommen Sie mir bloß nicht mit der Oper! Das war ja noch viel schlimmer als im Kino; grauenhaft, wenn ich dran denke. Manche Leute wollten ja, um wenigstens einen Grund zu haben, die Handys mal für ein paar Stunden auszuschalten, die Pausen abschaffen...

Lassen Sie mich raten: Man hat stattdessen mehr Pausen eingeführt?

Nein, man ist immer sehr subtil vorgegangen. In diesem Fall manipulierte man die Partituren, man strich einzelne Noten, die durch Handyklingeln ersetzt wurden. Man kooperierte mit den großen Handyfirmen. Die entwickelten dann Handy-Jammer, mit denen man Koppel-Mitteilungen aufs Handy zu einer ganz bestimmten Zeit durchlassen konnte. Noch nicht versandte Mitteilungen von Koppelfreunden wurden dann an den richtigen Musikstellen zugestellt – mit speziellen Klingeltönen. Die Noten wurden also durch Handyklingeln erstetzt – die Oper klang nur gut, wenn das Publikum viele Koppel-Freunde hatte. Die Älteren und die weniger Handybegeisterten wurden so immer mehr aus den Spielstätten verdrängt. Die Koppelfreundlosen, die saßen einfach nur da, und nach einer gelungenen Kadenz – da klingelte ihr Handy nicht! Wie peinlich! – das können Sie sich gar nicht vorstellen.

Und ich dachte immer, Handys seien im Theater verboten.

Das änderte man einfach über Nacht – die Theater müßten modern werden, hieß es. Und die Orchestermusiker bekamen ja nichts davon mit. Ihre Noten bezogen sie ausnahmslos von einer kleinen Werbefirma über das Internet – kostenlos, versteht sich. Man bezahlte mit seinen Daten, glaubte man. Obwohl man nicht so recht wußte, was das hieß. Aber man bezahlte mit noch mehr: Es fiel gar nicht auf, wenn man einzelne Noten strich, denn die Originale hatte man ja nie gesehen. Und die Musiker merkten hinterher nur, daß es trotz Handyklingeln irgendwie immer noch gut klang. Nur die Inspizienten mußten eingeweiht werden, aber die waren aufgrund ihrer finanziellen Situation meist nicht in der Lage, sich zur Wehr zu setzen, wenn sie das Problem erkannten. Ach ja, zeitgenössische Komponisten wie Sallinen oder Charles wurden nicht mehr gespielt, denn bei deren teils sehr atonaler Musik funktionierten diese Handy-Spielchen nicht, weil das durchschnittliche Publikum dort kleine Diskrepanzen so gut wie nicht bemerkte.

Haben die Leute, die keine Handys hatten, nicht verärgert reagiert und protestiert?

Öffentliche Versammlungen waren ja nur noch auf der Koppel – nicht mehr per se unter freiem Himmel erlaubt. Man kam nicht dazu, zu protestieren oder einen Protest zu organisieren.

Wie hat man denn Versammlungen in der Öffentlichkeit aufgelöst? Die Polizei hatte man ja auf ein Minimum unqualifizierter Betrunkener zusammengeschrumpft.

Die Zeiten meiner Großeltern – die der Polizeigewalt und der Wasserwerfer – die waren endgültig vorbei. Wobei die Alternative auch nicht viel subtiler war, muß ich sagen. Wie Sie wissen hat die Koppel auch Daten über den Gesundheitszustand ihrer Mitglieder gehabt. Und plante unter anderem die Jogging-Routen und Zeitpläne. Wenn also eine Versammlung aufgelöst werden sollte, ließ die Koppel einfach viele Jogger in die Gegend joggen. Dort angekommen, bekamen die dann alle viele Nachrichten oder Anrufe und sprachen laut in ihre Handys. Ein normaler Mensch konnte sich unter diesen Bedingungen gar nicht mehr vernünftig unterhalten. Nein, Versammlungen unter freiem Himmel gab es keine mehr.

Wirklich subtil war das ja nun wahrlich nicht.

Das nicht, aber den Widersacher zu erkennen, das war schwer. Wenn viele Leute um Sie in ihr Handy blöken – sehen Sie das gleich als Verschwörung gegen Sie? Man würde Ihnen ein Aufmerksamkeitsdefizit bescheinigen, aber Sie nicht ernstnehmen. Den Feind sah man damals gar nicht mehr.

Wie war das in den Discos? Wurde die Musik regelmäßig runtergeregelt, damit man telefonieren konnte?

Nein, in den Discos wurde tatsächlich nicht telefoniert.

Man hatte also seine Ruhe dort?

Vom Handy? Nein. Es gab ja die Koppel-Nachrichten. Die bekam man auch dort. Es war üblich, beim Tanzen oder beim Flirten ab und zu die Nachrichten zu lesen. Viele Discos sendeten Funksignale, die die Handys automatisch auf Vibrationsalarm stellten.

Und die Leute akzeptierten das? Dann gab es doch für den typischen Disco-Besucher gar keinen Grund, eine Revolution zu starten, oder?

(lacht) Nein, das nicht. Aber die Aufstände gingen tatsächlich von den Diskotheken aus.

Wie sah denn die Koppel auf dem Höhepunkt ihrer Macht aus?

Tja, es ist gar nicht ganz einfach zu sagen, wann genau dieser Höhepunkt erreicht war. Aber ziemlich nahe da dran war der Tag, wo sich ein Mitarbeiter der »Datenkoppel« ein Palais bauen lassen wollte. Er hatte zweifelsohne viel Geld, aber er brauchte keines für den Bau.

Wie schaffte er das?

Bei der Koppel wurden die Fähigkeiten der Mitglieder quantitativ bewertet – besagter Mitarbeiter versprach einfach, daß er jeden, der sich am Schloßbau beteiligte, durch eine Aufwertung seiner Fähigkeitseinschätzungen belohnen würde. Wenn man je einen Sinn im Leben gefunden hatte, dann war das zu dieser Zeit. Jeder lebte in der Hoffnung, irgendwann einhundert Prozent zu erreichen. Da baute man natürlich nur zu bereitwillig an einem Prunkschloß mit, um ein paar Prozente höher zu kommen.

Das Schloß wurde fertig?

Ja, in kürzester Zeit.

Das war der Höhepunkt der Macht der Koppel?

Ja, zumindest der gut sichtbare Teil. Die Koppel kontrollierte auch die Gedanken vieler Leute.

Wie kann man sich denn das vorstellen? Das klingt ja schon sehr erschreckend für mich.

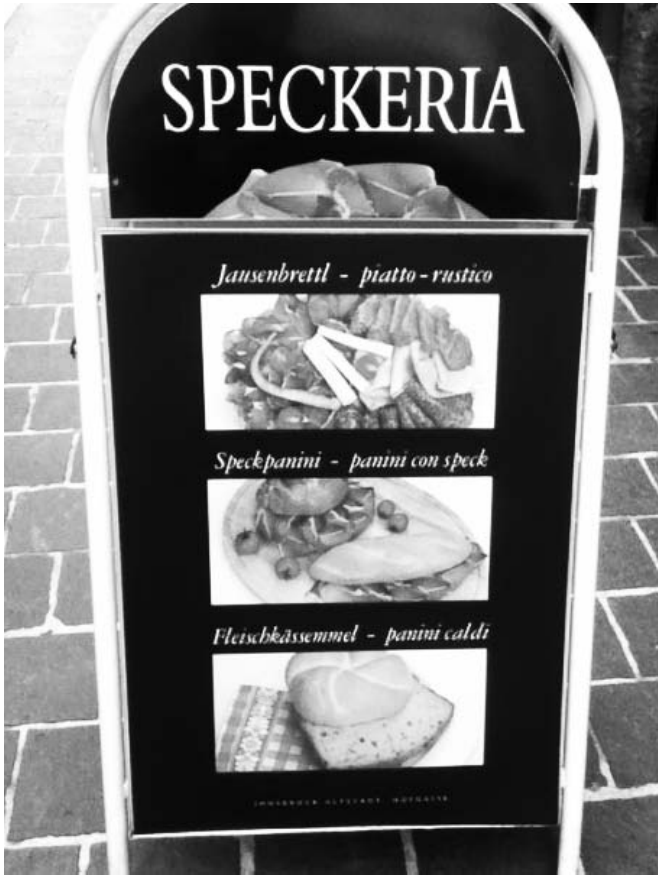
Klingt es erschreckend für Sie, ein Tagebuch zu führen? Natürlich nicht. Blöd nur, wenn es jemand findet. Blöder noch, wenn es jemand manipuliert. Die Koppel war freilich viel einfacher zu benutzen als ein Tagebuch, deshalb lagerte man auch viel größere Teile sei-

nes Gehirns darin aus. Einige Koppel-Protestgruppen organisierten sich tatsächlich über die Koppel selbst. Man änderte dann einfach ihre Einträge, jeder glaubte den Ort des Protestes an einer anderen Stelle. So fand man nicht zusammen. Einigen redete man sogar ein, sie wollten für die Koppel demonstrieren. Und sie glaubten das.

Irgendwann gab es aber dann doch Proteste – und die Macht der Koppel brach. Wie kam es dazu?

Durch Zufall. Das fing in den Discos an...

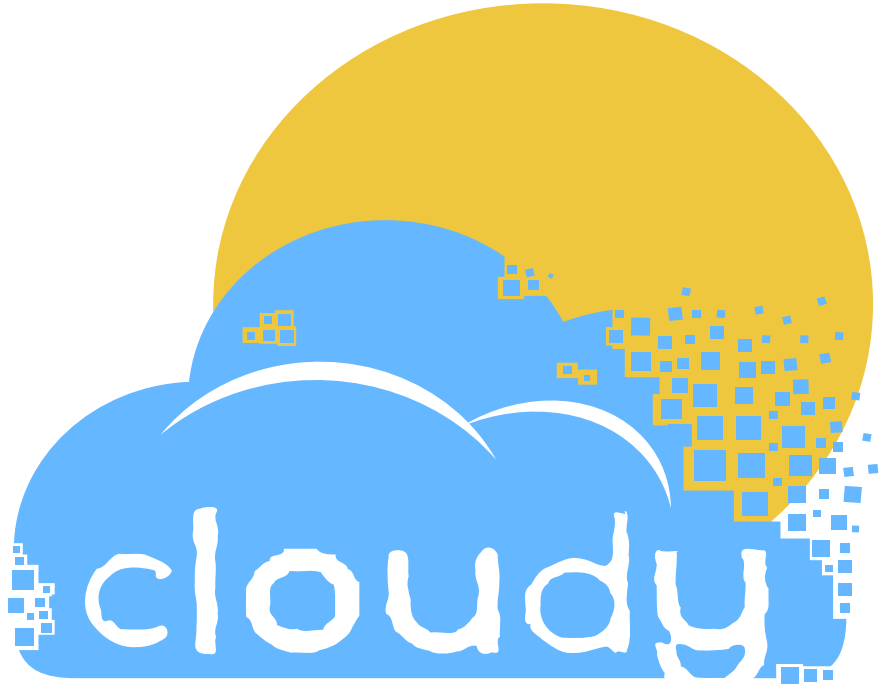
Sie sagten doch vorhin, der durchschnittliche Disco-Besucher sei nicht wirklich genervt gewesen von der Alltagssituation. Wie paßt das jetzt mit den Aufständen zusammen?



Es hing an den Türstehern. Es gab ja irgendwann diese Türsteher-App fürs Handy. Wenn ein Türsteher sich nicht danach richtete, gab's Ärger. Und das gefiel den Türstehern gar nicht. Die hatten nämlich ihre eigenen Heuristiken, um zu entscheiden, wen sie in ihres Hausherrn Gebiet einließen und wen nicht. Daß ihnen nun jemand Fremdes vorschrieb, wen sie einlassen sollten, paßte ihnen gar nicht. Sie fühlten sich degradiert. Es war ein bekannter Türsteher, der schließlich die ganze Sache mit den »sozialen Netzwerken« satt hatte. Er ließ dann nur noch Leute ohne Koppel-Account in seine Disco. Von ihm ließen sich viele Kollegen inspirieren. Von da war es dann nicht mehr weit zur Revolution...

Das war das Ende der »Ära Internet«?

Ach ja, wenn meine Fantasie doch nur ausreichen würde, diese Frage zu beantworten. Ich weiß ja noch nicht mal, ob es tatsächlich zur Revolution kam – genauer: kommen wird. Ich danke Ihnen auf jeden Fall für dieses Gespräch. Meine Gedanken soweit spinnen zu dürfen, hat mich jedenfalls für eine kleine Weile abgelenkt. Abgelenkt von der Realität. Denn ich fürchte, wir sind nicht am Ende einer großen Unterdrückung, sondern wir stehen ganz am Anfang.



MIT AUSSICHT AUF

DATENSPUREN

15
16 Oktober 2011

Kulturzentrum Scheune, Dresden

http://datenspuren.de

Einreichungen bis zum 31. August 2011


IBM