

die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

60 DEUTSCHE
BUNDESPOST BERLIN

Text-
kommunikation
ueber
Bildschirm



INTERNATIONALE
FUNKAUSSTELLUNG
BERLIN 1979



Geleitwort

Die einhundertunderste Ausgabe. Zwischen Camp und Congress, zwischen Sommer und Winter, zwischen einer Welt und Deutschland im Aufruhr. Für Anschläge in Deutschland werden Gamer oder Spielmethoden verantwortlich gemacht, für internationale Konflikte möchten Politiker Spielmethoden wie Nudging zum Einsatz bringen – oder hoffen, dass die Gegenübersitzenden sich wie programmierbare Spielcharaktere verhalten.

Wir dagegen beschäftigen uns ein wenig mit unserer eigenen Vergangenheit: BTX – ein System, welches die älteren Hacker noch live miterleben konnten – zeigt auf, wie sich ein Standard in verschiedene (nationale) Techniken entwickelt, wenn jeder sein eigenes Süppchen kocht. Nachdem uns ein Artikel zu dem Thema erreichte, wollten wir erst einmal herausfinden wie intensiv sich der CCC – beziehungsweise die Datenschleuder – mit dieser Technologie beschäftigt hat. Überraschend wenig, aber lest selbst!

Der CCC beschäftigt sich längst nicht mehr nur mit Technik, daher wenden wir uns in dieser Ausgabe gesellschaftlichen Themen wie Isolation oder Repression bei Demonstrationen zu und analysieren Strategien der Exekutive im Umgang mit zivilem Ungehorsam. Das Zitat von Rosa Luxemburg „Unpolitisch sein heißt politisch zu sein, ohne es zu merken“, hat in der digitalen Zeit nicht an Wert verloren, sondern vielmehr gewonnen, denn digital hinterlässt man schnell sehr viel mehr Spuren.

Die Urheberrechtsreform ist weiterhin ein aktuelles Thema. In dieser Ausgabe berichten einige Chaoten, wie es in Brüssel war, als sie mit Mitgliedern des europäischen Parlaments über die Urheberrechtsreform diskutiert haben.

Der Artikel *Public money, public code* befasst sich mit der Kampagne der Free Software Foun-

dation Europe (FSFE), die zum Ziel hat, dass von Steuergeldern erstellte oder entstandene Programme auch für alle Bürger frei verwendet werden können – so ähnlich wie das in den USA üblich ist.

Und damit entlassen wir Euch in die einzelnen Artikel, in der Hoffnung, dass sie Euch gefallen. Falls Ihr uns helfen wollt: Wir freuen uns immer über Einreichungen! Artikel, Ideen, Bilder und Leserbriefe könnt Ihr an die Redaktion schicken: <ds@ccc.de>

Inhalt

Geleitwort	0x01
Leserbriefe	0x02
Chaos Lokal	0x07
Web-Alternativen: Bildschirmtext	0x10
BTX in der Datenschleuder	0x16
Sicherheit in selbst-organisierenden Systemen	0x1A
Als bezahlter Bot in Brüssel	0x21
Public Money, Public Code an Schulen	0x24
Arbeitgeberneugier – Unterschätztes Risiko	0x29
Die Alexabeichte	0x2C



Leserbriefe

Hallo ihr guten. Die 100. Datenschleuder, schon ein dickes Brett. Beim Lesen habe ich an ein Zitat gedacht: „Das Neue unserer Arbeit kommt daher, daß wir uns von rein privaten, menschlichen Interessen ab- und den Welten der Naturgesellschaft zugewandt haben, der wir alle angehören. [...] Ein Objekt ist Tatsache, nicht Symbol.“ – John Cage, 1961

<Dieter>



Hi CCC, die Datenschleuder ist ein Lichtblick in der digitalen Dunkelheit, möge sie noch lang Informationen zum Überleben verschleudern!

Fan #1

<martin>



Liebe Datenschleuderer, gerne erinnere ich mich an den zum Nachdenken anregenden Satz „Daher freuen wir uns besonders, wenn ihr eine Marke draufklebt, nächsten größeren CCC-Veranstaltung nutzt.“ aus der DS100, Seite 0x01.

Beste Grüße

<marco>

Hallo marco, Vielen Dank für den Hinweis. Da ist leider bei der Umbruchkorrektur eine Zeile verloren gegangen.

Insgesamt sollte das natürlich heißen: „Daher freuen wir uns besonders, wenn ihr eine Marke draufklebt, [oder die Chaospost auf der] nächsten größeren CCC-Veranstaltung nutzt.“

Wir haben das bereits für die Online-Ausgabe korrigiert.

Viele Grüße

<Marei>

Datenschleuder



Liebe C3-Redaktion, bin ich froh, dass es euch gibt. Licht im Tunnel der Unwissenheit, Blinden und digitalen „Idioten“. Bin eine typische Userin, die keine Compusprache kann, aber den ganzen Tag als Sekretärin arbeitet...Mein Respekt ist groß...

Beste Grüße

<Karin>



Betreff: Links in der Datenschleuder

Moin erstmal ein grosses Dankeschon fuer die 100. Datenschleuder.

Koennt Ihr die Links in der Datenschleuder nicht als Kurzlink bringen? Ich vertippe mich bei den langen immer wieder! Z. B. Referenz 11, 19,...auf Seite 0x18 am besten natuerlich irgendwie so: kurzlink.ccc.de/xxx

Danke! Gruesse

<anobo>

Moin, das ist auch etwas, wo wir schon seit Längerem drüber nachdenken, aber noch keine befriedigende Lösung für haben. Wir denken dabei auch langfristig: Wie können wir sicherstellen, dass die abgedruckten Shortlinks länger leben als unsere Webseite? Damit die Datenschleuder-Links möglichst ewig gültig bleiben, auch wenn ccc.de nicht mehr existiert.





tiert? Über konstruktive Ideen dazu freuen wir uns unter <ds@ccc.de>.

Grüß
<vollkorn>



Betreff: CCC-Verwechslungen

Hi! Das neue Radrenn-Profi-Team des CCC bietet auch Potential für neue Verwechslungen :)

<Florian Baumann>



<https://twitter.com/cccproteam/status/1145603075698245632>

Fahradhelm abnehm Verwechslungen? Wie meinst du das?

<vollkorn>



Betreff: KRITIS

Hi, vorab: Die Themen in der ds#100 finde ich breit gefächert und interessant.

Bez. KRITIS: Für mich ist das der interessanteste Artikel. Von der Beleuchtung der Probleme wie z.B. Verletzlichkeitsparadoxon bis hin zu konkreten Empfehlungen. Fast alles finde ich stichhaltig bis auf einen Punkt: Die Ächtung von „D-Waffen“. Das finde ich mindestens „erheblich diskussionswürdig“. Nachfolgend

nenne ich ein paar Argumente gegen jegliche Ächtung von „D-Waffen“.

1. Auch wenn das „D“ so schön in die Reihe von „ABC“ passt: Es gibt einen himmelweiten Unterschied. ABC-Waffen benötigen einer tiefergehenden Fachkompetenz und man kann sie nicht einfach im heimischen Hobbykeller entwickeln. D-Waffen hingegen kann jedes vorpubertierende Scriptkid mit einem Discounter-Tablet für 100 Euro einfach a) herunterladen und b) auch nutzen. Für ABC braucht man erhebliche kriminelle Energie. Bei D reicht schon ein Hormonungleichgewicht.
2. In Relation zu Punkt 1 stehend: Aufgrund der geringeren Hemmschwelle werden sich Regimes wohl kaum an der Ächtung von D-Waffen stören und sowohl Entwicklung als auch Ankauf aktiv betreiben. Bei ABC-Waffen wird es vermutlich nur bei extremistischen Staaten keine Hemmschwelle geben („extremistisch“ schließt hier auch alle „My Country First“-Regimes ein). Bei D-Waffen ist das anders. Und selbst die Anwendung von D-Waffen hat eine eigentlich nicht vorhandene Hemmschwelle, da man dies praktisch anonym machen kann. Im Gegensatz dazu bedürfen ABC-Waffen immer einer *physischen* Anwendung, die immer Spuren hinterlässt. D-Waffen sind *nicht* physisch. (Auch bedeutend für mögliche Kontrollen.)
3. Wenn wir D-Waffen ächten, wird auch jede Linux-basierte Pentest-Distribution geächtet. Das bedeutet, dass wir langfristig unsere eigene Sicherheit schwächen, weil wir D-Waffen nicht mehr für Tests nutzen dürfen. Ich halte nicht nur die Ächtung für falsch, sondern kann in bestimmten (und näher zu definierenden) Einzelfällen sogar den Ankauf von 0days befürworten – vor allem dann, wenn wir unsere kritische In-



frastruktur bestmöglich auch gegen neueste Exploits absichern wollen. Deshalb: Wir brauchen „D-Waffen“. (Selbst ein Unit-Test einer KRITIS-Software könnte eine „D-Waffe“ sein. Sollte es sogar.)

4. Der vermutlichlich wichtigste Grund gegen eine Ächtung: Es ist undemokratisch und wird letztlich jedes Scriptkid als Terrorist in den Knast bringen. Außerdem ist es unlogisch, frei nach dem Motto „es kann nicht sein, was nicht sein darf“. Hatte nicht angeblich ein deutsches Gericht mal schlussgefolgert, dass „die eGK sicher ist, weil Hacken verboten ist“? Ridiculous! Heutzutage steht doch jeder Admin – rechtlich gesehen – mit einem Bein im Knast, wenn er eine Pentest-Distribution anwendet – sei es auch nur auf die firmeneigene Website. Mit der Ächtung von D-Waffen wäre es dann keine Straftat mehr, sondern er würde vielleicht vor einem Militärgericht nach Kriegsrecht angeklagt. Welcome Guantanamo. Murat Kurnaz, wir folgen Dir! Nein.

Vor allem der letzte Punkt bedeutet in letzter Konsequenz, dass wir noch ein großes weiteres Stück (eins der letzten?) unserer eh schon geschwächten Demokratie verlieren. Der lachende Dritte werden z.B. Militärs sein, während die Bürger immer mehr zu (überwachten?) Untertanen degradiert werden. Eine Ächtung von D-Waffen ist demokratiefeindlich und darf keineswegs erfolgen.

PS: Chaos Siegen, @nanooq: Das ist nicht irgendein Kaffeetassenspruch, das ist ein legendäres Zitat von Grandma Cobol. :-)

PPS: Wer Sarkasmus findet, darf ihn behalten.

Just my 2 cents
<Van>

Hallo zusammen! Lieber Van, du hast recht. Das Zitat ist „A ship in port is safe, but that is not what ships are for. Sail out to sea and do new things.“

Wirst du deine Segel setzen und bei KRITIS an Bord gehen und Dinge tun?

Die Leute bei KRITIS sind coole Menschen und du, Van, wie ich ja weiß, auch.

<nanooq>



Betreff: Themen für die Datenschleuder

Hallo, vielen Dank, dass die DS so regelmäßig erscheint. Bezüglich Eures Themenaufwurfes eine kleine Idee: Ich würde mich im Bereich Datenschutz als sensibilisiert und informiert beschreiben. Meine Mitgliedschaft im CCC ist fördernd, da ich hinter den Zielen des Clubs stehe. Allerdings bin ich technisch nur mittelmäßig auf der Höhe. Daher die Idee: Wie wäre es mit regelmäßigen Tutorials (für technische Dummies wie mich) zu Themen, die der „normale Durchschnittsanwender“ beherrschen sollte? Ich denke hierbei z.B. an PGP bei Mails udgl.

Liebe Grüße
<Guido>

Moin, wenn Tutorials eingereicht werden und sie unseren Qualitätsansprüchen genügen, dann werden sie auch abgedruckt. Bis dahin kann ich dir folgende Quellen ans Herz legen, die sich mit genau deiner Problemstellung befassen.

Auf <https://www.cryptoparty.in/> sind Cryptopartys aufgelistet. Nimm an einer Teil, denn noch viel besser lernt man diese Inhalte in einer Gruppe und mit einer erfahrenen Person, die man um Hilfe bitten kann.

Die Webseite <https://www.privacy-handbuch.de/> versucht eine umfängliche Einführung



zu sein, geht aber auch in die Tiefe und bietet konkrete Anleitungen.

Viel Spaß beim Tüfteln
<vollkorn>



Betreff: Fehlerhafte Kameras von Abus und Updatepflicht

Hallo zusammen,

mit Bestürzung habe ich den Bericht über den Skandal bei Abus-Kameras gelesen. Allgemein ist das Problem in der IT, dass Softwarehersteller nie haften. Es gibt geplante Obszolenz, und man haut lieber ständig was Neues raus, als mal für Updates und Patches zu sorgen. Wäre das nicht mal einen Artikel in der Datenschleuder wert? Man könnte das verknüpfen mit einer Mailprotestaktion an den Gesetzgeber: Ein Gesetz gegen geplante Obszolenz (gibt es in Frankreich). Desweiteren Updatepflicht der Softwarehersteller und Haftung bei Bugs.

Gruß
<Thorsten>

Moin, danke für deinen Input. In der Tat gibt der CCC regelmäßig Input an die Regierung und Politiker genau in diese Richtung. Zuletzt sehr prominent bei der Router-Richtlinie vom BSI. Updatepflicht bis zu einem bestimmtem Datum, das auf der Verpackung stehen muss, danach Firmware als OpenSource zum selber patchen und flashen. Leider wird der Input meist komplett übergangen und die Themen finden trotz Pressemeldungen (<https://www.ccc.de/de/updates/2018/risikorouter>) kein großes Medienecho. Ich nehme deinen Input mal und frage die Person bei uns, die sich zuletzt darum kümmerte, ob sie etwas schreiben würde.

Über Artikel-Einreichungen anderer Leser zu dem Thema freuen wir uns natürlich auch.

Gruß
<vollkorn>



Betreff: Chromecast-Leserbrief aus #100

Hi, dass Chromecast das Passwort kennt, könnte daran liegen, dass er mit dem Smartphone eingerichtet wird, und dort das Passwort bekannt ist. Es kommt btw. eine Abfrage ob das gespeicherte Passwort genommen werden oder das Passwort durch manuelle Eingabe erfolgen soll.

Einfach den Text durchlesen, den man abnickt.

Gruß
<Jens>



Kino-Gong des VEB Filmtheatertechnik

Re: Bilderrätsel #100

Dieses Mal war das Rätsel offensichtlich etwas schwieriger. Nur drei Personen haben einen Lösungsvorschlag eingereicht, von denen



aber zwei falsch lagen. Es handelt sich weder um Elektronik für das Hacker Jeopardy, das wir auf unseren Veranstaltungen gerne spielen, noch ist es eine PDP11/23 oder ein anderer Computer von DEC. Casandro ist mal wieder am nächsten dran mit seiner Vermutung, es könnte sich um eine elektronische Orgel aus der DDR handeln.

Die abgebildete Platine ist das Innenleben eines Kino-Gongs, der tatsächlich aus der DDR kommt. Mit dem mittleren Knopf, wo in der Abbildung die Kappe fehlt, kann der Dreiklang ausgelöst werden. Mit dem rechten Knopf können die Töne einzeln abgespielt werden.

Die MRMCD 2018 (<https://2018.mrmcd.net/>) standen unter dem Motto *Ganz großes Kino*. Und wer anwesend war, wird diesen Gong zum Beginn der Vorträge im Hauptsaal vernommen haben.

Bilderrätsel dieser Ausgabe

Ähnlich wie in der letzten Ausgabe, gibt es zu diesem Rätselbild wenige Informationen im Internet. Wir hoffen dennoch, das einige von Euch herausfinden werden, worum es in diesem Rätsel geht.

Die Tasten auf der Umschlaginnenseite stammen von einem Gerät, das in den 80er Jahren und vermutlich noch bis weit in die 90er Jahre hinein in vielen Redaktionen und Firmen stand. Heutzutage wurde seine Funktion von Software übernommen, die auf handelsüblichen PCs läuft. Auch wenn der ursprüngliche Einsatzzweck längst technologisch überholt und abgeschaltet ist, gibt es noch Millionen von Menschen weltweit, die täglich eine artverwandte Technologie nutzen.

Eine Idee, was das sein könnte? Schreibe uns deine Vermutung an [<ds@ccc.de>](mailto:ds@ccc.de).

Die Datenschleuder Nr. 101

Herausgeber

(Abos, Adressen, Verwaltungstechnisches etc.)

Chaos Computer Club e. V.

Zeiseweg 9

22765 Hamburg

[<office@ccc.de>](mailto:office@ccc.de) PGP: CAEE E257 594B A8C0
E1DD 87EE 84A4 FA72
009E D7A1

Kontaktadresse

(Artikel, Leserbriefe, Inhaltliches)

Redaktion Datenschleuder

Chaos Computer Club e. V.

Zeiseweg 9

22765 Hamburg

[<ds@ccc.de>](mailto:ds@ccc.de) PGP: 2A75 2EB3 D0A0 5FA9 2726
2B8A A917 2CC7 B794 A17A

<https://ds.ccc.de/>

Redaktion dieser Ausgabe

dome, Philipp „fiveop“ Schäfer, Hanno „Rince“
Wagner, Marei, TVLuke, Jan „vollkorn“ Girlich

Umschlaggestaltung

Titelbild: dome

Umschlaginnenseite: lonesome_grass

<https://www.instagram.com/p/B0vR1QOgwc0/>

Rückseite: Werner Henke

LaTeX-Backend

Marei „TeXhackse“ Peischl

Druck

Pinguin Druck Berlin <http://pinguindruck.de/>

V. i. S. d. P.

Hanno „Rince“ Wagner

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.





Erfahrungsaustauschkreise

Aachen :: CCCAC :: Chaos Computer Club Aachen e. V.	https://aachen.ccc.de/
Mi u. Fr 20 Uhr :: Jülicher Straße 191, 52070 Aachen	
Bamberg :: backspace e. V.	https://www.hackerspace-bamberg.de/
Di 19 Uhr :: backspace, Spiegelgraben 41, 96052 Bamberg	
Basel :: CCC Basel :: Chaos Computer Club Basel	https://www.ccc-basel.ch/
Di 19:30 Uhr :: Birsfelderstrasse 6, 4132 Muttenz	
Berlin :: CCCB :: Chaos Computer Club Berlin e. V.	https://berlin.ccc.de/
Di u. Do 19 Uhr :: Club Discordia, Marienstraße 11, 10117 Berlin	
Bremen :: CCCHB :: Chaos Computer Club Bremen e. V.	https://ccchb.de/
Di 20 Uhr :: FabLab Bremen, An der Weide 50 a, 28195 Bremen	
Darmstadt :: Chaos Computer Club Darmstadt e. V.	https://www.chaos-darmstadt.de/
Di 19 Uhr u. Fr 18 Uhr :: Trollhöhle, Wilhelminenstraße 17, 64283 Darmstadt	
Dortmund :: Chaostreff Dortmund e. V.	https://www.chaostreff-dortmund.de/
Di u. Do 19 Uhr :: Langer August, Braunschweiger Straße 22, 44145 Dortmund	
Dresden :: C3D2 :: Netzbiotop Dresden e. V.	https://c3d2.de/
Di u. Do 19 Uhr :: HQ, Riesaer Straße 32, 01127 Dresden	
Düsseldorf :: Chaosdorf :: Chaosdorf e. V.	https://chaosdorf.de/
Fr 18 Uhr :: Chaosdorf, Hüttenstraße 25, 40215 Düsseldorf	
Erlangen :: Bits'n'Bugs e. V.	https://erlangen.ccc.de/
Di 19:30 Uhr :: E-Werk Erlangen, Fuchsenwiese 1, 91054 Erlangen	
Essen :: Chaospott :: foobar e. V.	https://chaospott.de/
Mi 19 Uhr u. So 16 Uhr :: foobar, Sibyllastraße 9, 45136 Essen	
Frankfurt am Main :: CCCFFM :: CCCFFM e. V.	https://ccc-ffm.de/
Di u. Do 19 Uhr :: Hackquarter ccc-ffm, Häuser Gasse 2, 60487 Frankfurt am Main	
Freiburg :: CCCFr :: Chaos Computer Club Freiburg e. V.	https://cccfre.de/
Mo u. Di 19 Uhr :: Hackspace, Adlerstraße 12 a, 79098 Freiburg im Breisgau	
Göttingen :: CCCGoe :: CCC Göttingen e. V.	https://cccgoe.de/
2. Di 20 Uhr :: Neotopia, Von-Bar-Straße 2-4, 37075 Göttingen	
Hamburg :: CCCHH :: CCC Hansestadt Hamburg e. V.	https://hamburg.ccc.de/
letzter Di 20 Uhr :: CCCHH, Zeiseweg 9, 22765 Hamburg	
Hannover :: C3H :: Leitstelle 511 - Chaos Computer Club Hannover e. V.	https://hannover.ccc.de/
Mi 19 Uhr u. letzter So 16 Uhr :: Leitstelle 511, Klaus-Müller-Kilian-Weg 2, 30167 Hannover	



Kaiserslautern :: Chaos inKL. e. V.	http://www.chaos-inkl.de
Sa 19 Uhr :: Klubraum, Rudolf-Breitscheid-Straße 65, 67655 Kaiserslautern	
Karlsruhe :: Entropia :: Entropia e. V.	https://entropia.de/
Sa 19:30 Uhr :: Entropia, Steinstraße 23, 76133 Karlsruhe	
Kassel :: CCC Kassel :: flipdot e. V.	https://flipdot.org/
Di 19 Uhr :: flipdot, Franz-Ulrich-Straße 18, 34117 Kassel	
Köln :: C4 :: Chaos Computer Club Cologne e. V.	https://koeln.ccc.de/
Do 20 Uhr :: Chaoslabor, Heliosstraße 6 a, 50825 Köln	
Mannheim :: C3MA :: Chaos Computer Club Mannheim e. V.	https://www.ccc-mannheim.de/
Fr 19 Uhr :: Neckarauer Str. 106-116, 68163 Mannheim	
München :: muCCC :: Chaos Computer Club München e. V.	https://www.muc.ccc.de/
2. Di 20 Uhr :: muc, Schleißheimerstraße 39, 80797 München	
Paderborn :: C3PB :: C3PB e. V.	https://c3pb.de/
Mi 19 Uhr, 1. So ab 12 Uhr :: Westernmauer 12-16, 33098 Paderborn	
Salzburg :: Chaostreff Salzburg	https://sbg.chaostreff.at/
Fr 20 Uhr :: Ulrike-Gschwandtner-Straße 5, 5020 Salzburg	
Siegen :: Chaos Siegen oder HerzSi :: Chaos Siegen e. V.	https://chaos-siegen.de/
Do 19:30 :: Hackspace Siegen, Effertsufer 104, 57072 Siegen	
Stuttgart :: CCCS :: Chaos Computer Club Stuttgart e. V.	https://cccs.de/
1. Di 18 Uhr (Lichtblick), 3. Mi (shackspace) :: Stuttgart	
Ulm :: CCCU :: Hackerspace Ulm e. V.	https://ulm.ccc.de/
oft :: Freiraum, Platzgasse 18, 89073 Ulm	
Wien :: C3W :: Chaos Computer Club Wien	https://c3w.at/
3. Di 19 Uhr :: Metalab, Rathausstraße 6, 1010 Wien	
Wiesbaden :: CCCWI :: Chaos Computer Club Wiesbaden e. V.	https://cccwi.de/
Di 19 Uhr :: Sedanplatz 7, 65183 Wiesbaden	
Würzburg :: N2N :: Nerd2Nerd e. V.	https://nerd2nerd.org/
Do 18:30 Uhr :: FabLab Würzburg, Veitshöchheimer Straße 14, 97080 Würzburg	
Zürich :: CCCZH :: Chaos Computer Club Zürich	https://www.ccczh.ch/
Mi 19 Uhr :: Röschibachstrasse 26, 8037 Zürich	

Es gibt in den folgenden Städten Chaostreffs: Aalen, Amsterdam, Augsburg, Aschaffenburg, Backnang, Bayreuth, Bern, Bielefeld, Budapest, Chemnitz, Coburg, Erfurt, Flensburg, Fulda, Gießen, Graz, Halle (Saale), Heidelberg, Hildesheim, Ingolstadt, Innsbruck, Iserlohn, Itzehoe, Jena, Kiel, Konstanz, Leipzig, Lörrach, Lübeck, Luxemburg, Marburg, Markdorf, Münster, Neuss, Nürnberg, Offenburg, Osnabrück, Potsdam, Rapperswil-Jona, Recklinghausen, Regensburg, Rothenburg ob der Tauber, Rotterdam, Schwerin, Trier, Unna, Villingen-Schwenningen, Wetzlar, Winterthur, Wuppertal, Zwickau

Detailinformationen siehe <https://www.ccc.de/regional>



Chaos auf die Ohren

Ihr habt noch nicht genug Podcast-Abonnements in eurem Podcatcher? Wir haben redaktions-intern unsere Listen abgeglichen und uns auch im Chaos-Umfeld umgeschaut.

C-RaDaR Darmstadt	https://www.c-radar.de/
Chaosradio cccb	https://chaosradio.ccc.de/
Chaosradio Freiburg ccfr	https://rdl.de/sendung/chaosradio-freiburg/
damals (tm) ajuvo	https://damals-tm-podcast.de/
Datenkanal Offener Kanal Jena	https://datenkanal.org/
/dev/radio CCC Erfa Ulm	https://www.ulm.ccc.de/dev/radio/
Desperate Househackers jinxx	https://desperatehousehackers.net/
Fairydust FM c/o Radio Blau	https://www.fairydustfm.cc/
Hackerfunk ccczh	https://www.hackerfunk.ch/
Hyperbandrauschen c-base	https://hybr.de/
Logbuch Netzpolitik Linus Neumann, Tim Pritlove	https://logbuch-netzpolitik.de/
Netzpolitik.org	https://netzpolitik.org/category/netzpolitik-podcast/
pentaradio c3d2	https://www.c3d2.de/radio.html
Radio (In)Security Jena, Jens und Tobias	https://insecurity.radio.fm/
Radio Tux Linux, OS, Netzkultur	https://radiotux.de/
Podcast des Chaos Siegen Chaos Siegen	https://podcast.chaos-siegen.de/
Sibyllinische Neuigkeiten Chaospott	https://podcast.chaospott.de/

Haben wir einen Podcast übersehen, der auf keinen Fall in dieser Liste fehlen sollte? Schreib uns an <ds@ccc.de>!



Der Chaostreff Flensburg stellt sich vor

Ein Interview der Datenschleuder mit Pia, Scammo, René und Philipp

Pizza am Hafen, Hacks on the Beach: Beim nördlichsten Chaostreff Deutschlands geht es maritim zu. Der Chaostreff Flensburg dient als Lernort, Hackspace, Chaoskombüse, Werkstatt, Lounge und vieles mehr.

Datenschleuder: *Ihr seid ein relativ junger Chaostreff. Wann und warum habt ihr euch gegründet?*

Scammo: Wir haben uns Anfang 2015 gegründet. Die Idee kam uns auf der Rückfahrt aus Hamburg vom Congress. Davor hatte es in Flensburg schon andere Bestrebungen gegeben, etwas computermäßiges zu gründen, aber uns hat die Idee gefallen, damit ans Chaos angedockt zu sein. Das heißt auch: Nächstes Jahr feiern wir unser fünfjähriges Bestehen!

René: Viele von uns waren das Jahr davor zum ersten Mal auf dem Congress und zufällig traf man dann Menschen, die man aus Flensburg schon kannte, die aber unabhängig voneinander nach Hamburg gefahren waren. Dann

haben wir festgestellt, dass in dieser relativ kleinen Stadt doch viele Menschen sind, die sich mit Chaos identifizieren können.

Philipp: Wir sind auch nicht nur ein junger Treff, auch unsere Mitglieder sind recht jung. Das jüngste Mitglied ist 14 Monate alt und der Sohn des ältesten Mitgliedes.

Datenschleuder: *Könnt ihr euch auch kurz vorstellen?*

Philipp: Ich bin Philipp oder auch Homwer, Ich beschäftige mich mit 3D-Druck, Python, Linux und bin zweiter Vorsitzender beim Chaostreff Flensburg. Ich genieße es sehr, dass es mit dem Chaostreff einen Ort gibt, wo man sich mit Gleichgesinnten austauschen kann.



0x0A



Pia: Ich bin Pia. Ich bin Makerin und viel im Bereich Netzpolitik unterwegs. Digitale Bildung ist ein Thema auf das ich, auch aufgrund meines Lehramtsstudiums, Bock habe.

Scammo: Ich bin Scammo und erster Vorsitzender, was natürlich heißt, dass ich viel Orga im Verein mache. Dazu engagiere ich mich in der Jugendarbeit und bin einer der Initiatoren der Chaoskombüse, die bei uns auch gerne mal für ein paar mehr Menschen kocht.

René: Ich bin René und jetzt gerade mit meinem Informatikstudium fertig geworden. Beim Chaostreff Flensburg bin ich jetzt auch schon von Anfang an dabei.



Datenschleuder: *Seit eurer Gründung seid ihr ein paar Mal umgezogen, warum?*

Philipp: Das ist ganz spannend. Es gab in Flensburg ein okkupiertes, altes Kulturzentrum. Dort gab es die Möglichkeit sich kostenfrei und unbürokratisch Räume zu nehmen. Da hatte sich eine Computergruppe einfach jeden Montag getroffen, ganz ohne weitere Strukturen. So haben sich die ersten Flensburger Connections gebildet. Daraus sind dann die Bemühungen hervorgegangen einen Verein zu gründen, weil das Kulturzentrum irgendwann mal geräumt wurde.

Scammo: Seit 2017 haben wir unsere Heimat in Räumlichkeiten der dänischen Minderheit,

mit der wir uns auch sehr verbunden fühlen, gefunden.

Philipp: Dort wird uns freundlicherweise eine gesamte Etage zur Verfügung gestellt, auch weil diese über eine steile Treppe zu erreichen ist und nicht mehr genutzt wird.

Datenschleuder: *Und was könnt ihr in euren aktuellen Räumen so bieten?*

Philipp: Natürlich trifft man auf die Standardausrüstung: 3D-Drucker, LötKolben, Internet und blinkende Lichter. Aber hauptsächlich bieten wir einen Raum für Menschen, die Lust haben, sich über Technik auszutauschen oder einfach neben jemand anderem zu sitzen, der auch am Rechner sitzt – Gemeinschaft. Wenn du an einem Thema interessiert bist, findest du wahrscheinlich schnell Menschen, die auch daran interessiert sind.

René: Schön ist, wie unsere Räume aufgeteilt sind. Auf der einen Seite die Werkstatt und dann auch noch was wir die Lounge nennen, wo man auf dem Sofa entspannen und eine Mate trinken kann.

Philipp: Wir haben eine schöne Terrasse und einen regelmäßig genutzten Grill.

René: Und wir sind halt in Flensburg. Wenn es richtig warm wird, haben wir einen Strand und einen Hafen, zu dem man auch Pizza bestellen kann – das haben wir getestet.





Datenschleuder: *Wie groß ist denn das Chaos in Flensburg, wie viele Menschen machen da aktiv mit?*

Scammo: Wir haben jetzt so 40 Mitglieder im Verein. Zum Open Space am Dienstag sind häufiger mal 15 Leute da, und auch nicht immer dieselben.

Datenschleuder: *Und was sind die Projekte, an denen gerade gearbeitet wird?*

Philipp: Aktuell bauen Menschen eine LED-Wand mit dem 3D-Drucker. Wovon auch viele schon gehört haben dürften, ist unsere T-Shirt-Aktion. Wir haben für uns entdeckt, dass T-Shirts-Machen 'ne coole Aktion ist, weil man für den Siebdruck die Siebe selber erstellen kann. Das ist relativ einfach und macht viel Spaß.

René: Ein Kollege baut sich gerade ein E-Fahrrad. Das sieht dann zwar abenteuerlich aus, aber es fährt schnell und ist ziemlich cool.

Pia: Die Projekte sind sehr unterschiedlich. Wir haben auch Menschen im Space, die mit Computern eigentlich nichts zu tun haben, aber als Maker dabei sind und ihren Platz finden. Und diese ganzen unterschiedlichen Menschen sind halt da, um zusammen zu lernen. Ich habe es jetzt schon so oft erlebt, dass Menschen zusammenstanden und angefangen haben, etwas auszuprobieren, weil sie es spannend fanden.

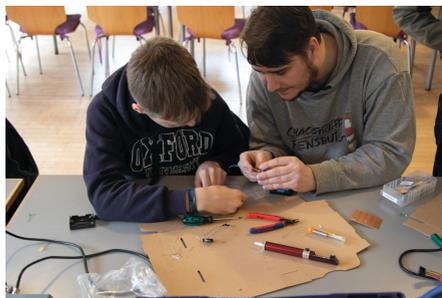
René: Hydroponik! Ein Mitglied hat mal angefangen sich Hydroponik, also das Anbauen von Lebensmitteln in Wasser, beizubringen. Die ersten Versuche gingen natürlich großartig schief und er hat seine halbe Wohnung geflutet. Aber er hat mit der Idee und mit Vorträgen ganz viele von uns infiziert, um es selbst mal auszuprobieren.

Scammo: Ich hätte da noch ein paar Kilo Seramis, falls das jemand braucht.

Pia: Natürlich gibt es viele Projekte, wo viel Material gekauft wird und dann ändert sich das Projekt. Einmal haben wir große Mengen Bügelperlen gekauft, um ein Gerät zu bauen, welches diese zu einem Bild legen kann. Ich glaube das Projekt läuft im Hintergrund auch noch, aber inzwischen nutze ich die Bügelperlen einfach selbst.

Philipp: Oder die Bällebadsortiermaschine. Da gab es sogar einen Prototyp, der funktioniert hat. Er war aber sehr, sehr langsam.

René: Projekte sind oft fertig, sobald es einen Proof of Concept gibt.



Datenschleuder: *Jugendarbeit ist ein großes Thema bei euch, wie kommt es?*

Scammo: Wir haben seit unserer Gründung zusammen mit einem anderen Partner ein Hack-Wochenende gemacht und hatten dabei viel Spaß Wissen, aber auch Werte, was im CCC-Context ja auch sehr wichtig ist, zu vermitteln. Mittlerweile haben wir eine Jugendgruppe und machen verschiedene Events, bei denen viele Mitglieder als Mentoren beteiligt sind. Dazu gibt es auch Workshops in Schulen. Und ich hoffe natürlich, dass viele der Jugendlichen in den nächsten 10 Jahren bei uns dazustoßen, noch viel mehr, viel coolere Projekte machen und uns ablösen.



Zum letzten Jugendwochenende haben wir Roboter mit Bluetooth-Steuerung programmiert. Natürlich hat zehn Minuten später der erste einen Störsender gebaut, andere haben dann rausgefunden, das sie das umgehen können indem sie den Channel wechseln, und so ging das dann hin und her und da wird viel Kreativität frei.

Philipp: Und inzwischen haben wir halt eine feste Jugendgruppe, die *Neue Tüftler:innen*.

René: Wir haben vorgestellt, was es bei uns für Themen gibt, zum Beispiel 3D-Druck, oder Javascript oder Lockpicking und die Kinder hatten einen Zeitraum sich zu überlegen, was für sie interessant ist, anstatt dass es ihnen erzählt wird.

Philipp: Natürlich gibt es dann auch Kinder, die kommen mit ihrer Siemens-Steueranlage XY und haben viel mehr Ahnung davon als irgendwer bei uns.

Pia: Aber das ist ja das Tolle am Chaos, dass sowas auch nicht ungewöhnlich ist und dass wir dann da auch gerne sitzen und sagen: Erklär uns das mal, das ist sehr faszinierend. Und der Lernort, den wir damit aufmachen, ist einfach ein ganz anderer als Schule den bieten kann. Auch weil die Kinder den Lernort selber gestalten.

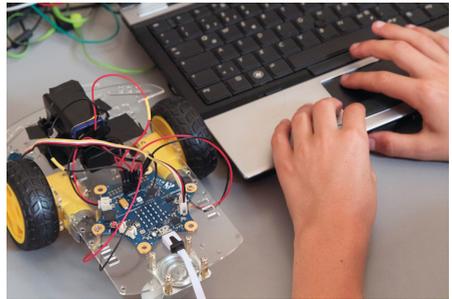
Philipp: Viele der Jungtüftler:innen haben dasselbe Problem, das viele von uns auch mal hatten. In der Schule ist man „der Nerd“ und es fehlt einfach ein Rückzugsort, wo man andere Menschen trifft, die einem zeigen, dass man nicht unnormale ist.

Datenschleuder: *Tragt ihr diesen Ansatz der Jugendarbeit auch in die Öffentlichkeit oder ins Chaos weiter?*

Scammo: Ja, damit haben wir auf dem letzten Regiowochenende begonnen. Aktuell gibt es ja Chaos macht Schule, die tolle Arbeit leisten, aber wir empfinden den Ort *Schule* als Lernort

nicht als optimal. Es gab eine Session auf dem Camp. Für uns geht es dabei auch stark um die Vermittlung von Werten, sei es anhand von offenen Daten oder der Hackerethik.

Pia: In meinem Studium, ich studiere auf Lehramt, gibt es vor Begriffen wie *Digitalisierung* auch einfach noch sehr viel Angst; Natürlich auch bei Eltern. Und mit einem solchen Lernort, wie wir ihn schaffen, kann man solche Ängste verringern und zeigen wie es wirklich ist.



Datenschleuder: *Also nicht nur Jugendarbeit, sondern auch Elternarbeit?*

Pia: Immer. Du zeigst den Eltern, dass es einen Ort gibt, wo das Kind sozial interagieren kann und dass ein Interesse an Computern nicht heißt, dass man einsam im Kämmerlein versinken muss.

René: Wobei die Eltern, die ihren Kindern erlauben in einen Chaostreff zu gehen, das meist schon verstanden haben. Aber die Eltern und Kinder sind dann hoffentlich Multiplier. Die reden mit Freunden und Nachbarn und so verbreitet sich das hoffentlich langsam.

Pia: Eltern fragen natürlich, wenn sie einen Hackspace sehen, schon nach, was das alles ist. Aber das erklärt man dann eben und dann erklären die es weiter. Viel der Arbeit findet da



außerhalb unserer Reichweite zwischen Eltern statt, aber man kann es anstoßen.

Philipp: Aber wichtig am Konzept ist, dass wir nicht auf Eltern oder Kinder zugehen. Dann kommt es vor, dass Eltern ihr Kind bei uns hinsetzen, weil sie wollen, dass das Kind was mit Computern lernt. Das bringt niemandem etwas, wenn das Kind das gar nicht möchte. Wir bieten einen Raum und wenn du kommen möchtest und was lernen möchtest, dann sind wir für dich da und beantworten jede Frage. Das ist ein Filtermechanismus, dass die Kinder kommen, die selbst wollen und richtig Bock haben was zu machen.

Scammo: Wir sind auch aktiv im Arbeitskreis *Projektorientierter Informatikunterricht* in Schleswig-Holstein. Der versucht Lerninhalte unter CC0 [1] auszuarbeiten, also Open Educational Resources (OER). Da hosten wir auch Infrastruktur, wie ein Wiki und Chat-Systeme.



Datenschleuder: Neben all der Jugendarbeit veranstaltet ihr auch zwei größere Events pro Jahr. Was macht ihr da so?

René: Das ist einmal das *Rütüta* [2], die Rüsperler Tüfteltage, und andererseits das *Hacks On the Beach* [3]. Die Rüsperler Tüfteltage finden in Kooperation mit dem Kliemannsland [4] statt. Wir haben Chris Figge auf einem Congress

in Hamburg getroffen und sind auf die Idee gekommen, zusammen eine Veranstaltung zu machen. Das hat im ersten Jahr sehr gut funktioniert und jetzt haben wir es auch schon zum zweiten Mal gemacht.

Pia: Die Kooperation mit dem Kliemannsland, was ja ein öffentlich-rechtliches Format ist, bringt auch nochmal ganz andere Menschen zum Chaos, die sonst damit bisher nichts zu tun hatten.

Scammo: Dieses YouTube-Format erreicht auch eine ganz andere Altersgruppe, als es die traditionelle Pressearbeit kann.

Philipp: Das zweite Event, das *Hacks on The Beach* ist aus dem Problem hervorgegangen, dass ganz viele Leute Projekte hatten, mit denen sie nicht fertig wurden. Die Idee war dann sich ein Wochenende zu nehmen und sich zu treffen, um die Projekte zu Ende zu bringen. Das hieß dann *Weekend Hack*. Das waren beim ersten Versuch so 25 Leute, beim zweiten Mal ist es auf 60 Menschen eskaliert und danach waren es hundert. Da konnten wir die Location nicht mehr nutzen und sind ans Wasser umgezogen und seitdem heißt es *Hacks on The Beach*.

René: Das ist ein kleines Chausevent mit sehr gutem Blick auf die Flensburger Förde und noch besserem Blick auf Dänemark, direkt am Strand. Da machen wir richtig viel selbst, was die Organisation angeht und kochen sogar.

Datenschleuder: Wenn jemand (mehr oder weniger) zufällig in Flensburg ist, wann ist der beste Zeitpunkt bei euch vorbeizuschauen?

Philipp: Dienstag ist die Tür immer auf. Wer Interesse hat kann von 19:00 Uhr bis ungefähr 23:00 Uhr einfach vorbeikommen und „Hallo“ sagen. Auf der Website [5] kann man sehen, ob geöffnet ist.





Referenzen

- [1] Die Lizenz *Creative Commons Zero*: <https://creativecommons.org/publicdomain/zero/1.0/deed.de>
- [2] Die Rüspler Tüfteltage: <https://ruetueta.de/>
- [3] Hacks On the Beach: <https://chaostreff-flensburg.de/events/hacks-on-the-beach-28-bis-30-september/>
- [4] Kliemannsland: <https://www.kliemannsland.de/>
- [5] Der Chaostreff Flensburg im Netz: <https://chaostreff-flensburg.de/>
Twitter: @chaos_fl





Web-Alternativen: Bildschirmtext

von Casandro <christian@clarke-3.de>

Bildschirmtext (BTX) wird oft als der deutsche Vorgänger des Internets bezeichnet. Dank seiner einfachen, doch vielfältigen Fähigkeiten lohnt es sich einen Blick in die Vergangenheit zu werfen und sich angesichts des modernen Web wieder auf BTX zurückzubedenken.

In den letzten Jahren verspüren viele eine gewisse Unzufriedenheit mit dem Web. So ziemlich Jeder verwendet Adblocker oder NoScript – und trotzdem fühlt sich das Web nicht viel schneller an als zu ISDN-Zeiten. Browser sind inzwischen die komplexesten Softwareprojekte mit denen man es als Normalmensch zu tun hat; So groß, dass nur noch große Organisationen solche Projekte stemmen können. Klar, diese Organisationen veröffentlichen ihren Quellcode, nur nutzt das einem nur wenig bei 20 Millionen Zeilen Code. Das ist nicht im Sinne einer „Digitalen Souveränität“, welche den Gedanken der „Freien Software“, also der Erlaubnis Software zu verändern, um das Recht auf die Fähigkeit dieser Veränderung erweitert. Dieser Gedanke wurde zum Beispiel im Vortrag „Fully Open, Fully Sovereign mobile devices“ von Paul Gardner-Stephen [4] auf dem Camp 2019 erklärt.

Dazu kommt noch, dass die Idee, Anwendungen im Webbrowser auszuführen, ein Malwareproblem hat. Websites können Code aus dubiosen Quellen nachladen und – dank Werbung die Javascript enthalten kann – hat der Betreiber einer Website kaum Einfluss darauf, welcher Code da kommt, zumindest wenn er nicht auf Werbung verzichten möchte. Bis vor kurzem nahm man an, dass dies kein Problem sei; die Sandbox sollte es schon richten. Inzwischen wissen wir jedoch, dass Software-sandboxen nicht wirklich funktionieren. Hinter schwerwiegenden Sicherheitslücken wie Rowhammer.js [1], Spectre und Meltdown [2], die auf Hardware-Probleme in Speichern und Prozessoren zurückzuführen sind, stecken sicherlich noch andere vergleichbare Probleme, die es ebenfalls ermöglichen, jegliche Sandbox auszuhebeln. Zusätzlich bringt das Cryptomining einen Grund dafür Rechenleistung abzugreifen, während batteriebetriebene Geräte das reine Verschwinden von Rechenzyklen zu einem Angriffsvektor machen. Kurzum: Das Web wird immer unbefriedigender, trotzdem werden die Technologien dahinter in immer weiteren Gebieten verwendet. Das geht inzwischen so weit, dass inzwischen Desktopanwendungen ihren eigenen Browser mitbringen um ihn als GUI-Toolkit zu verwenden. In gewisser Weise kann man das sogar verstehen, denn vom Betriebssystem unabhängige GUI-Toolkits gibt es halt kaum. Ich würde somit gerne das Medium der Datenschleuder dazu verwenden, um mögliche alternative Lö-



Vielleicht der erste Screenshot eines deutschen Online-Dienstes, CC BY-SA 3.0 Archiv Ev. Kirche im Rheinland



sungsansätze zu diskutieren, oder zumindest zu zeigen welche Ideen die Leute vor dem Web hatten und warum diese fehlschlügen.

Übersicht über Features und Techniken bei Bildschirmtext-Varianten			
Teletext (Level 1 & 1.5)	⌘ ⌘		
Prestel	⌘ ⌘		
BTX (DE)	⌘ ⌘ </>		
Minitel 1	⌘ ⌘		
Antiope (FR)	⌘ ⌘		
Minitel 2	⌘ ⌘ </>		
Teletext (Level 2.5)	⌘ </>		
Bildschirmtext (AT)	⌘ ⌘ </> ⌘ ⌘		

Legende:	
⌘	Serielle Attribute
⌘ ⌘	Parallele Attribute
</>	Redefinierbare Zeichen
	Erweiterte Attribute (Farben etc.)
⌘ ⌘	Vektorgrafik
	Übertragung per Telefonnetz
	Übertragung per Videosignal

Anfangen möchte ich hier jetzt mit der Gruppe der Videotex-Standards. Man sollte die Videotex-Standards nicht mit dem Videotext beziehungsweise Teletext verwechseln, auch wenn er wohl der erfolgreichste Standard aus dieser Gruppe war. In Deutschland und Österreich war das Bildschirmtext (BTX), in Großbritannien Prestel und Frankreich Minitel. Die Idee stammte aus einer Zeit in der Computer noch teuer waren. Mit billigen kleinen Terminals könnte man einem großen Teil der Leute preisgünstig Zugang zu Computern verschaffen.

Videotext/Teletext

Anfangen hat diese Idee (und somit die Standardisierung) in den Siebzigern mit dem Videotext, den wir auch noch heute kennen. Farbfernsehgeräte hatten damals eine Bandbreite von ca. 3,5 MHz, was locker einen Pixeltakt von 6 MHz erlauben würde. Mit 6 Pixel breiten Zeichen lassen sich so gut 40 Zeichen pro Zeile darstellen ohne zu nahe an die Ränder kommen zu müssen. Bei 10 Pixeln Höhe pro Textzeile bekommt man gut 25 Textzeilen in den aktiven Bereich eines Bildes. 40×25 ergibt auch eine schöne runde Zahl, nämlich 1000. So wurde in den Siebzigern die erste Grundlage für diese Familie von Standards gesetzt: Ein Zeichenraster von 40×25 Zeichen. Besonders anfangs wollte man Speicherplatz sparen, denn 1000 Zeichen zu speichern kostete früher relevant viel Geld. Deshalb dachte man sich etwas aus, was sich „serielle Attribute“ nennt. Jedes Zeichen enthält die 7 Bit des Zeichen-codes. Die ersten 32 Stellen des ASCII-Codes sind jedoch durch Steuerzeichen belegt, die im Bildspeicher keinen Sinn ergeben. Diese Stellen wurden nun in Attributszeichen umgedeutet. Diese Zeichen werden normalerweise als Leerzeichen dargestellt aber die Attribute der nachfolgenden Zeichen bis entweder ein weiteres Attributszeichen kommt oder die nächste Zeile anfängt. Das lässt sich relativ einfach in Logik abbilden und war für die Siebziger und frühen Achtziger gar nicht mal so schlecht. Ausprobieren kann man das in einem der vielen Web-Teletexteditoren. [3] Im Videotext werden immer ganze Zeilen von 40 Zeichen in der Austastlücke übertragen.

Vom Teletext zum BTX

Bei den Videotex-Terminals wurde ein Befehl definiert, mit dem man einen Cursor beliebig verschieben kann. \$1f (APA), gefolgt von zwei Zeichen, setzt die Position. Diese zusätzlichen



Zeichen geben die Position an, wobei die linke obere Ecke \$1f A A ist. Das erste A steht für die erste Zeile, das zweite A für die erste Spalte. Da die höchste Zahl die dargestellt werden muss 40 ist, bleibt das alles noch im Bereich der normalen druckbaren Zeichen. Normale druckbare ASCII-Zeichen dazwischen werden einfach in die Speicherstelle unter dem Cursor geschrieben der sich ein Zeichen weiter bewegt. Steuerzeichen bewegen den Cursor oder gehen in einem Modus über den man Attributzeichen setzen kann. Das alles ist im Prinzip nicht schwierig, so dass man Ende der siebziger Jahre zuversichtlich war, dass Teletexttaugliche Fernsehgeräte auch bald Bildschirmtext können würden, was sich auch in der damaligen Werbung niederschlug. Im Pilotbetrieb sah das auch noch gut aus.



Platine eines Telefunken-Terminals, auf der komplexe Schaltungen mit wenig spezialisierten ICs realisiert sind

Doch dann kam in Deutschland der Wirkbetrieb und man wollte alles richtig machen. Schon damals war es absehbar, dass RAM deutlich billiger werden sollte. Warum also nicht gleich einen richtigen Standard entwickeln? Gleichzeitig wollte man damals wohl einen europäischen Standard schaffen. Man brauchte ein flexibles System, welches gut erweitert werden konnte. Schließlich wollte man ja „parallele Attribute“, 32 Farben, redefinierbare Far-

ben, Vektorgrafiken und – sobald dann in den Neunzigern das Glasfasernetz da ist – auch Fotos, Videos und digitalen Ton machen. Das hat plötzlich die Komplexität der Dekoder merklich erhöht, was wahrscheinlich den Untergang von Bildschirmtext begünstigt hat. Bevor hochintegrierte ICs dafür verfügbar waren, waren die Dekoder komplexe Schaltungen mit zahlreichen mehr oder weniger speziellen ICs.

Um das alles zu machen hatte man zwei Ideen. Die erste bestand darin das Bild in unterschiedliche Ebenen zu unterteilen. In vereinfachter Form gab es dies auch schon im Videotext. Die Textebene konnte transparente Stellen enthalten, durch die man das Fernsehbild sah. Die Videotext-Standards erweiterten dieses Konzept weiter und führten unter der Textebene auch noch eine Zeilenhintergrund-Ebene, in der man die Hintergrundfarbe für ganze Zeilen inklusive der Bereiche links und rechts vom Text, setzen konnte, sowie eine Vektorgrafik-Ebene, auf der man mit Grafikbefehlen zeichnen konnte, ein. Weitere angelegte Ebenen waren eine Foto-Ebene sowie ein einfarbiger Hintergrund über das ganze Bild. Je nachdem welcher nationale Standard eingesetzt wurde, musste ein Terminal einen bestimmten Satz dieser Ebenen unterstützen. Minitel 1 unterstützte meines Wissens nach nur die Textebene, während der österreichische Bildschirmtext und Minitel 2 auch die Vektorebene unterstützen mussten. In Singapur soll es sogar Terminals gegeben haben, welche über ein terrestrisches Fernsehsignal auch noch digitale Fotos übertragen bekommen haben, welche dann auf der fotografischen Ebene dargestellt wurden.

Um all diese Funktionen ansprechen zu können, ohne auf Kompatibilität zu verzichten, hat man die Cursorsteuerung ausgebaut. \$1f (APA) hat ja zwei Zeichen als Parameter, welche von A an aufwärts gezählt werden. Wenn



man jetzt ungültige Werte für die Zeile zulässt, so kann man die Zeile als Adresse für unterschiedliche virtuelle Komponenten innerhalb des Terminals sehen. Diese Komponenten können dann Dinge wie die Vektorgrafik-Ebene oder benutzerdefinierte Zeichen und Farben repräsentieren. Ein Terminal, welches die entsprechende Funktion nicht unterstützt, wartet einfach auf das nächste `$1f` (APA) Zeichen und ignoriert alle Zeichen bis da hin. In dieser neuen Redefinition nennt man das Zeichen `$1f` nicht mehr APA sondern US (Unit Separator) und es separiert einzelne Pakete die „Videotext Presentation Data Elements“ (VPDE). Eine Übersicht über diese Elemente findet sich am Ende des Artikels, auf Seite 0x15 und wer noch mehr über Steuersequenzen lernen möchte kann dies im Buch „Das Große Buch zu BTX“ von Baums, [13] welches eine Einführung bietet.

Was wir davon lernen können

Ich denke das ist auch das, was wir von Videotext heute wirklich brauchen könnten. Wir leben in einer Welt in der wir gerne Terminals verwenden. Einfach per SSH wo drauf gehen ist schnell und bequem. Allerdings haben sich Terminals seit ihrer Hochzeit kaum noch weiterentwickelt. Das ist auch schwierig, denn im VT100/ANSI-Standard muss jeder neue Befehl vom empfangenden Terminal unterstützt werden. Wenn wir jetzt aber ebenfalls VPDEs einführen, so müssen die Terminals nur lernen damit umzugehen. Im simpelsten Fall kann das bedeuten einfach nur das US-Zeichen und das darauf folgende Zeichen anzuschauen. Ist das Folgezeichen bekannt, so verarbeitet das Terminal die weiteren Zeichen. Ist es unbekannt so verwirft das Terminal alle Zeichen bis zum nächsten US-Zeichen. Vektorgrafiken könnte man zum Beispiel so machen, dass man auf der Textebene einen Bereich frei lässt. Dann

schaltet man per US-Zeichen auf die Vektorgrafikebene um und schickt die Grafikbefehle. Wenn man einen „Lösch alles“-Befehl definiert, so kann dies auch einfach mit Terminalmultiplexern wie `tmux` oder `screen` funktionieren. Diese müssten dann einfach alle Befehle für die Vektorgrafikebene speichern und können diesen Speicher leeren sobald der „Lösch alles“-Befehl kommt. Somit können die Terminals das Umschalten zwischen Bildschirmen erreichen, ohne selbst die Komplexität der neuen Befehle zu verstehen. Für Audio und Video wäre es ähnlich. Dort kann man zum Beispiel eine Art „Keyframe“-Flag definieren, ab dem die Dekodierung des Medienstromes beginnen kann. Der Terminalmultiplexer würde, wenn er nicht selbst sinnvoll mit den Medienströmen umgehen kann, einfach alle Daten seit dem letzten „Keyframe“ bereithalten und diese beim Umschalten schnell übermitteln. Richtig gemacht könnte dies erlauben mit sehr wenig Aufwand Terminalanwendungen zu schreiben, die Grafiken darstellen. Man könnte zum Beispiel so was wie `Gnuplot` dazu kriegen, die Grafiken direkt ins Terminalfenster zu zeichnen, so dass man die Scrollfunktion weiternutzen kann. Wie so eine GUI zur Zeit gemacht wird sieht man zum Beispiel an `wxMaxima`, welches für solche Features sein eigenes Terminal mitbringen muss.

Terminals hätten generell den großen Vorteil, dass sie relativ simpel aber flexibel sind. Im Gegensatz zum Web, bei dem man grundsätzlich immer ein ganzes Dokument übermitteln müsste, überträgt man bei Terminalstandards einfach nur Änderungen in einem Dokument. Die Gegenstelle des Terminals kann jederzeit beliebige kleine Dinge an diesem Dokument ändern. Im Prinzip könnte man so was auch mit dem DOM im Browser machen oder mit einem klassischen GUI Toolkit. Das dargestellte Dokument muss kein Gitter aus Zeichen sein.



BTX wiederbeleben

Das Interesse an BTX lebt angesichts der Probleme unseres modernen Web wieder etwas auf und es gibt einige interessante Projekte, die sich mit verschiedenen Aspekten rund um BTX beschäftigen, BTX-Systeme wieder aufbauen oder versuchen Lehren aus BTX zu ziehen. Um etwas tiefer in die Materie einzusteigen lohnt es sich ein paar dieser Projekte anzuschauen. Philipp Maier hat zum Beispiel Hardware und Software entwickelt um Seiten in einer Art XML-Dialekt über HTTP zu übertragen. [5] Anna Christina Naß hat für ihr Projekt Retrotext einige Seiten aus einer alten Amigademo gedumpt und sie als Inhalte für ihren eigenen Bildschirmtextdienst erhalten. Diese Dumps stellen einen Einblick in die reale Nutzung dieses Mediums dar. [6] Einige neuere Entwicklungen, wie zum Beispiel ein Wikipedia-Gateway nach BTX, finden sich auf Github. Dort kann man auch einen in Python geschriebenen Server finden, sowie Versionen von xcept welche auch noch auf modernen Plattformen kompilieren. [7] Um BTX gänzlich zu verstehen lohnt sich ein Blick in die Standards, die öffentlich abrufbar sind. [8, 9, 10, 11, 12] Eine leichter verständliche Einführung in die notwendigen Codesequenzen im Kontext der konkreten Implementierung bietet [13].

Zuletzt möchte ich auch noch andere ermutigen sich auch mit Artikeln an dieser Diskussion zu beteiligen. Wie funktionierte zum Beispiel der BTX-Nachfolger KIT, dem „Kernel for Intelligent Communication Terminals“, welcher unter Anderem eine Mausunterstützung bot. Wie wurden grafische Seiten bei CompuServe oder America Online (AOL) erstellt? Was gibt es denn für neue Ideen grafische Benutzeroberflächen oder Hypertextdokumente im Internet zu machen?

Ich denke das Wichtige ist es jetzt Alternativen zu erträumen, denn wie Nicolas Wöhrl einmal sagte: „Jede Idee wird zweimal gemacht: Einmal in Deinem Kopf und einmal mit Deinen Händen.“



Ein öffentliches BTX-Terminal der Bundespost, CC BY-SA 3.0 Martin Bahmann

Referenzen

- [1] Gruss, Daniel et al.: „Rowhammer.js: A Remote Software-Induced Fault-Attack in JavaScript“ (2015) <https://arxiv.org/pdf/1507.06955v1.pdf>
- [2] Horn, Jann et al.: „Meltdown and Spectre“ (2018) <https://spectreattack.com/>
- [3] Einer von vielen Online-Webeditoren für Teletext: <https://zxnet.co.uk/teletext/editor/>
- [4] Gardner-Stephen, Paul: „Fully Open, Fully Sovereign mobile devices“ (Camp 2019), https://media.ccc.de/v/Camp2019-10378-fully_open_fully_sovereign_mobile_devices
- [5] Hardware- und Software-Projekte um BTX wiederzubeleben: <http://www.runningserver.com/?page=rs.thelab.bildschirmtrix>
- [6] Dumps von Seiten aus einer Amigademo sowie ein eigenes Serversystem dafür und einige neu erstellte Seiten:





- <https://git.imzadi.de/acn/rtx>
- [7] Github-Account, der viele BTX-Projekte enthält. Unter Anderem das Repository „bildschirmtext“, welches einen Bildschirmtextserver enthält, der unter Anderem auch ein Wikipedia-Gateway hat: <https://github.com/bildschirmtext/>
- [8] ETS 300 072 Overview: https://www.etsi.org/deliver/etsi_i_ets/300001_300099/300072/01_60/ets_300072e01p.pdf
- [9] ETS 300 073 Geometric Display: https://www.etsi.org/deliver/etsi_i_ets/300001_300099/300073/01_60/ets_300073e01p.pdf
- [10] ETS 300 074 Transparent Data: https://www.etsi.org/deliver/etsi_i_ets/300001_300099/300074/01_60/ets_300074e01p.pdf
- [11] ETS 300 075 File Transfer: https://www.etsi.org/deliver/etsi_i_ets/300001_300099/300075/02_60/ets_300075e02p.pdf
- [12] ETS 300 076 Terminal Facility Idener: https://www.etsi.org/deliver/etsi_i_ets/300001_300099/300076/01_60/ets_300076e01p.pdf
- [13] Baums, Jürgen: „Das Große Buch zu BTX“ (1990), gibt eine konkretere Einführung in die Steuersequenzen für BTX

Übersicht über „Videotex Presentation Data Elements“ (VPDE) sortiert nach „Videotex Presentation Control Elements“ (VPCE)

VPCE		Videotex Service Control Element
\$1F	\$20	Terminal Facility Identifier request
\$1F	\$21	Terminal Facility Identifier request
\$1F	\$23	Define DCRS (user defined characters)
\$1F	\$26	Define Colour
\$1F	\$2D	Define Format
\$1F	\$2E	Timing Control
\$1F	\$2F	Reset (also sets screen size)
\$1F	\$31	Geometric Data 3D
\$1F	\$32	Geometric Data 2D
\$1F	\$34	Photographic Pixel Data
\$1F	\$35	Photographic Table Data
\$1F	\$3B	Sound (1980s codecs)
\$1F	\$3E	Telesoftware
\$1F	\$3F	length transparent Data
\$1F	X	Y Alphamosaic Spalte X, Zeile Y (both \$41 ...)



Wir fühlten uns befugt

von TVLuke <tvluke@chaotikum.org>

„Warum benutzen Sie eigentlich BTX wenn Sie nur die übelsten Worte dafür übrig haben?“ fragt 1991 ein Leser. Und tatsächlich, die Berichterstattung in der Datenschleuder über Bildschirmtext (BTX) ist von einer Mischung aus Kritik und Neugierde geprägt. Bei genauerem Lesen stellt man fest, die Kritik ist oft eine Kritik an Betreibern, Gebühren und Einschränkungen. Eine kurze Geschichte der BTX-Berichterstattung in der Datenschleuder (seit 1984) und einem Gründungsmythos über den man im „Organ des Chaos Computer Clubs“ überraschend wenig liest.

Mitte der 80er Jahre ist BTX ein extrem wichtiges Thema, gerade im CCC-Umfeld. Der BTX-Hack ist auch heutzutage, zum Beispiel in der Datenschleuder Nummer 96 aus dem Jahr 2010, eine so feste Größe in der CCC-Geschichte, dass man sie gar nicht erklären braucht. Tatsächlich stellt der geneigte Leser historischer Datenschleudern fest: Der BTX-Hack, der virtuelle Bankraub [1] oder Btx-Coup (Datenschleuder 17, 1986. Alle referenzierten Datenschleudern finden sich im Archiv: [2]), ist tatsächlich bisher in der Datenschleuder überhaupt nicht (ausführlich) thematisiert worden (oder habe ich es nur nicht gefunden?). Am meisten lesen wir dazu wohl in der Daten-

schleuder 17: 1984 habe „eine Gruppe junger Burschen aus einer terranischen Stadt namens Hamburg das damals jüngst eingeführte BTX-System der Post geknackt und ist in unzugängliche Bankdatenverbindungen eingebrochen. Aus Jux haben diese Burschen dort eine halbe Milchstraße auf ihr Konto umgebucht“. Naja, vielleicht nicht die Milchstraße aber immerhin 130.000 DM.

Wer Texte in der Datenschleuder liest, hat das Gefühl, dass das Verhältnis zwischen der Deutschen Bundespost und dem CCC danach etwas gestört war. Aber von Anfang an.



Bildschirm-TriX

Schon Anfang 1984, noch vor dem BTX-Hack, findet sich das Thema in der Datenschleuder. Allerdings sieht sich die dritte Ausgabe des „wissenschaftlichen Fachblatts für Datenreisende“ auch nicht genötigt in die neue Technologie einzuführen, sondern schreibt unter der Überschrift „BTX heißt Bildschirm-TriX“:

Vorweg: Wer nichts über BTX weiß, soll sich sonstwo informieren. Im nächsten Telefonladen liegen genügend Prospekte rum.

Der CCC hatte auch ein Angebot: „Unsere gebührenpflichtige Seite (PRESTEL 99 Pfennige) kommt nach *19058# und wenn CEPT läuft, ist es ganz einfach: 20305080“.

Eine Ausgabe später (Datenschleuder 4) versucht man es doch mit etwas Erklärung in einer Ausgabe die nahezu vollständig BTX gewidmet ist: „BTX gehört zu den sogenannten Neuen Medien und ist ein schmalbandiges Text- und Graphikinformationssystem, das über Telefonleitungen geführt wird. Die Teilnehmer, da[s] sind sowohl Nutzer und Anbieter, können Informationen aus einer Datenbank abrufen als auch Informationen eingeben“ beginnt der Text „Mozart-Archiv im Turm: Bildschirmtext im Ausblick“ (DS 4). Ein spannender Text, gab wohl vieles zu meckern am neuen Medium, „so sind beim derzeit noch kaum belasteten Rechner die Ausfallzeiten weit über 30 %“ an eine „flächendeckende Btx-Versorgung bis Ende '84“ sei nicht zu denken. Im Jahr 2019 erinnert das an Mobilfunk und daran, dass die Telekom aus der Bundespost hervorgegangen ist. „Auch mit dem Datenschutz scheint das bundesdeutsche ‚Posthörnchen‘ Probleme zu haben. So ist es kein Problem, anderen Teilnehmern nach Belieben in der Mailbox ‚herumzumischen‘, auch hat man es bei Postens als überflüssig angese-

hen, das sogenannte Eingabesystem mit einem Passwort zu schützen.“

Bildschirmpest

Das Meckern setzt sich in Schleuder 5/6 fort, wo BTX mit dem Spitznamen „Bildschirmpest“ bezeichnet wird. „Das System gleicht einem Moloch“ steht da, aber man will auch nicht zu viel schreiben „Mehr zu BTX in BTX. Das ist am verständlichsten.“ Kann man vermutlich inzwischen nicht mehr abrufen, es bleibt also unverständlich. Man hat aber auch andere Dinge zu tun: „In der Zeit zwischen Weihnachten und Sylvester soll in Hamburg der Chaos Communication Congress '84 stattfinden.“ kündigt man schon mal unverbindlich an.



Abgewandeltes Bildschirmtext-Logo, aus Datenschleuder 5/6

Die Ausgabe 7 aus dem Dezember 1984 wäre wohl die gewesen, in der man hätte den BTX-Hack präsentieren können, aber „Wegen totaler Überlastung diesmal nur eine Winz-Datenschleuder“. Schade. Kurz vor dem Congress eine Datenschleuder fertig machen war und bleibt schwierig!

Aber der CCC und die Datenschleuder bleiben am Thema BTX grundsätzlich dran, in der DS 9/10 ist zum Beispiel Datenschutz im BTX wieder ein Thema „Angesprochen auf diesen fahrlässigen Umgang [mit schutzwür-



digen Zugangsdaten] beruft sich die Post auf ihre Dienstanweisungen. Einen tatsächlichen Grund, für die Notwendigkeit diese Daten offen zu bearbeiten konnte die Post nicht geben.“ Auch der Anschluss der Hamburger Sparkasse (Siehe BTX-Hack) sei dementsprechend schlecht geschützt gewesen. Der Umgang mit der Post bleibt schwierig.

In der DS 11/12 ist Zensur im Bildschirmtext ein Thema „Der Elektronikkonzern SEL präsentierte auf der Hannovermesse 85 neue Btx-Geräte für den öffentlichen Gebrauch“. Und selbiges Terminal konnte bis zu 100 Anbieter sperren. „Ausser dem CCC wurden weitere medienkritische Programme gesperrt“. Die Schleuder zeigt klare Kante „Derartigen Einschränkungen muss im Keime entgegengetreten werden.“ Auf selbiger Hannovermesse besuchte der CCC auch den Stand der Post (wegen BTX), was angeblich bei der Post schon im Vorfeld zu „Panikstimmung“ führte. Auch darüber kann man in der DS lesen.

Ein weiteres Thema, das bis heute nicht so recht sterben will, kommt in dieser DS auf: Haftungsfragen. „Mit Rechtsgeschäften bei BTX beschäftigen sich zunehmend auch die Zivilrechtler.“ Papier ist trotz BTX auch 1985 nicht tot, für eine Party sei „die Papierverteilung effektiver als die Btx-Ankündigung“ stellt man in der 13. Datenschleuder fest.

Blödeltextsystem

Pflicht für jeden, der unterhalten werden möchte, ist der kurze Artikel „Besuch bei der Post“ (Datenschleuder 14, 1985) in welchem Ls23 und der Autor beschließen, eine BTX-Störung selbst zu beheben in dem sie der zuständigen Ortsvermittlungsstelle der Post einen unangekündigten Besuch abstatten. Böse Zungen könnten auch von Einbrechen reden, aber die Hintertür war halt offen. „Das Schild ‚Dienstgebäude, unbefugter Zutritt ver-

boten!‘ kann uns nicht schocken, wir fühlen uns befugt.“ Und prompt sucht man nach Relaisstrahlen „Plötzlich tauchen drei Fernmeldetechniker auf: ‚Von welcher Dienststelle kommen Sie?‘. Ls23 nennt seine Telefonnummer. ‚Ich verfolge eine Störung im Fernmelde-netz!‘“. Eskalation.

Ab der Datenschleuder 15 (1986) „zum ersten Jahrestag der Btx-Fernmelderechnung von über 130.000 DM“ steht die BTX-Nummer des CCC nicht mehr groß direkt neben dem Titel, wo sie die letzten Ausgaben zu lesen war, aber immer noch im Impressum. Überhaupt lässt man kein gutes Haar an BTX: „Zum 1. Juli will die POST die Speicher und Verkehrsgebühren für das Blödeltextsystem zu 50 % erheben, verlautet aus dem Postministerium. Für den CCC bedeutet das, daß der jetzige Programmfang mit über 2000 Btx-Seiten ca. 3000 DM pro Monat kosten und dann nicht mehr über das Spendenaufkommen der Btx-Seiten finanziert werden kann.“

In der Datenschleuder 17 (1986) taucht das Wort BTX nur noch 10 mal auf, darunter in dem Satz „Btx ist ein System, bei dem Zentrale und Endgeräte nicht sonderlich intelligent sind. Über die zukunftssträchtigen Datennetze wie Datex dagegen lassen sich relativ einfach beliebig viele intelligente Systeme koppeln.“ In Ausgabe 22 schlägt man sich mit der Gebührenordnung der Post herum und beschwert sich darüber, dass das Löschen von BTX Angeboten kostenpflichtig ist. Zudem ist die BTX Adresse ab jetzt *CHAOS.

Provinzialismus

Immer seltener geht es um BTX, in der Datenschleuder Nr. 23 hält man den Dienst für provinziell und schreibt „Anzumerken ist, daß ein Dienst wie BTX, der eine deutliche Trennung zwischen Anbieter und Konsument macht, für den Konsumenten extrem im Preis herunter-





subventioniert wird, während ein Dienst wie DATEX-P, der insbesondere für die internationale Vernetzung von Einzelnen und Gruppen große Bedeutung hat (zB. PeaceNet in den USA bzw. GreenNet in GB), im Vergleich zu anderen Ländern sehr teuer ist. Damit pflegt die Bundespost über ihre Gebührenpolitik den Provinzialismus.“ Noch pflegt diesen Provinzialismus auch die DS, im Impressum findet sich immer noch die Nummer der BTX-Redaktion, zum letzten mal in der DS 46 (1994). BTX wird weiter gehackt, so stellt Ausgabe 26/27 „BTX – Das Unsicherheitssystem“ vor, und zeigt auf, wie man an öffentlichen Terminals die Hardwareerkennung eines Postmodems herausfinden kann. Hacken mit Diktiergerät.

Ein Leser fragt in der 34. Datenschleuder „Warum benutzen Sie eigentlich BTX wenn Sie nur die übelsten Worte dafür übrig haben? [...] Hoffentlich findet die DBP bald ein Rechtsmittel um Ihr Lästermaul für immer zu stopfen. Nicht nur der Sind Sie ein Dorn im Auge. Für Chaoten die versuchen die öffentliche Sicherheit und Ordnung zu gefährden und mit bewusst falschen Infos zu verunsichern ist hier kein Platz.“ Die Leserbriefe sind seit 1991 netter geworden.

Ab Ausgabe 24 findet BtxNet gelegentliche Erwähnung. Ein Dienst der sich „die bestehende Infrastruktur des Btx Dienstes der Deutschen Bundespost zunutze“ (DS 28) macht um Mailboxen zu vernetzen. BTX selbst kommt immer seltener vor. Manchmal ist es noch ein Thema wie in der Datenschleuder 47 von der NPD-Zeitung über BTX. Auch der BTX-Staatsvertrag findet gelegentliche Erwähnung.

Eingestellt

Für den CCC ist im Winter 1999 Schluss, in der 68. Ausgabe der Datenschleuder ist zu lesen: „Im Rahmen von Strukturmodernisierungsmaßnahmen haben wir uns entschlossen, den Bildschirmtextbetrieb einzustellen. Die Btx-Leitseite *CCC# gibt es nicht mehr.“ Man habe damit „in den 80er[n] viel Spaß gehabt“, aber die „Kostendeckung war irgendwann definitiv nicht mehr gegeben und irgendwie hatte auch keiner Lust da noch Zeit reinzuinvestieren. Mit dem Betrieb von Web-, Mail- und FTP-Server haben wir im Internet dann wohl doch eher mehr Spaß und weniger Kosten.“

So richtig Schluss für BTX ist in Deutschland 2007, als der Dienst eingestellt wird. Auch in der Datenschleuder ist das Thema kaum zu finden. Dann und wann findet der BTX-Hack Erwähnung, wie z. B. zum letzten Mal in Ausgabe 91 (2007) und 96 (2010).

Das ist sie, die Geschichte des BTX in der Datenschleuder (sofern ich nichts übersehen habe). Bis Heute! Zum ersten mal seit Mitte der 90er gibt es einen längeren Text zu Bildschirmtext in der Datenschleuder. Willkommen zurück.

Achja: Jetzt gibt es natürlich in der Datenschleuder immer noch keine Erklärung, was genau der BTX-Hack war – vielleicht kann das mal jemand nachreichen? Vielleicht jemand der damals schon am Leben war?

Referenzen

- [1] Zahlen, bitte! CCC: Virtueller Bankraub für 134.634,88 DM: <https://heise.de/-3824653>
- [2] Das Archiv der Datenschleuder: <https://ds.ccc.de/download.html>



Operational Security – Auszug aus einem XR Handbuch

von Linus Neumann
<https://linus-neumann.de/kontakt/>

Intro

Nach vielen Jahren voller Stille und Stillstand ist es *Fridays for Future (FFF)* mit beachtlicher Hartnäckigkeit und Symbolkraft gelungen, den Klimawandel als politisches Thema zu setzen. Die „Generation Z“, der so lange mangelndes politisches Interesse und Engagement unterstellt wurden, erhebt sich und bringt Millionen von Menschen auf die Straße. Nachdem die monatelangen Debatten um das ach so schreckliche Schulschwänzen endlich verebbt sind, gesellt sich nun auch in Deutschland ein „radikalerer“ Arm zu *FFF*: Die noch junge Bewegung *Extinction Rebellion (XR)* hat sich in UK mit spektakulären und kontroversen Aktionen schnell einen Namen als eine der am schnellsten wachsenden politischen Gruppierungen gemacht.

XR setzt auf klassische Aktionen des zivilen Ungehorsams wie zum Beispiel Sitzblockaden, ergänzt diese aber auch durch mutigere Maßnahmen wie zum Beispiel *glue-ons*, dem Festkleben der Handinnenflächen mit Sekundenkleber – auf jeden Fall eine Aktionsform für Fortgeschrittene. Auch krassere Aktionen wie das kontrollierte Starten von Drohnen in der Nähe von Flughäfen gehören zum Repertoire der Briten. Gewaltfreiheit gehört zu einem der unumstößlichen Prinzipien von *XR*. Doch auch wenn die Drohnen auf geringer Höhe gehalten werden und eine tatsächliche Gefährdung des Flugverkehrs ausgeschlossen wird, rufen solche Aktionen natürlich die Polizei auf den Plan. Genau das ist aber durchaus gewollt: Vie-

le *XR*-Rebellen legen es gezielt darauf an und lassen sich bereitwillig verhaften.

Wie fast jede politische Gruppierung außer der CDU setzt *XR* bei der Koordination auf einen bunten Mix von Online-Tools unterschiedlichster Couleur und Güte. „Selbstorganisierende Systeme“ nennen das die Rebellinnen. Immerhin: Ein gewisser Grad an Dezentralität wird dadurch sichergestellt. Dezentralität hat viele Vorteile, aber natürlich auch einige Herausforderungen – wer sollte das besser wissen, als regelmäßige Leserinnen der Datenschleuder...Auch vor lästigen Hausdurchsuchungen sind wir als rechtschaffene Hacker nicht gefeit. [1, 2, 3]

In Deutschland wurde der Auftakt zum *Aufstand gegen das Aussterben* – einer ganzen Aktionswoche, die am 7. Oktober 2019 begann – durch die Veröffentlichung des Buches „*Wann wenn nicht wir*“* [4] begleitet. Die englische Original-Vorlage verfügt nicht über ein Kapitel zum Thema *Operational Security* oder den üblichen Herausforderungen schnell wachsender Graswurzelbewegungen. Ich habe mich daher über die Einladung von *XR* gefreut, ein – leider kurzes – Kapitel beizutragen. Mit leichten redaktionellen Änderungen und Ergänzungen ist das Kapitel im Folgenden abgedruckt.

Sicherheit in selbst-organisierenden Systemen

Neben dem Zusammenkommen in den Aktionen im öffentlichen Raum ist die digitale





Kommunikation die Grundlage für unsere Vernetzung und Zusammenarbeit. Das Internet ist das perfekte Werkzeug für Überwachung, Kontrolle und Macht – und gleichzeitig das perfekte Werkzeug für ihr Gegenteil: Dezentrale Vernetzung, Befreiung und soziale Veränderung. Es liegt an uns, das befreiende Potential der Dezentralität auszuschöpfen, ihre Schwächen zu kennen und uns gegen zentralisierte Überwachung zu schützen.

Aus technischer und sozialer Sicht birgt aber auch die Dezentralität einige Risiken – insbesondere im Digitalen: Die größte technische Gefahr besteht in den massenhaften digitalen Spuren, die wir hinterlassen. Das größte soziale Risiko ist die Unterwanderung.

*Zuerst ignorieren sie dich,
dann lachen sie über dich,
dann bekämpfen sie dich
und dann gewinnst du.*

Sprichwort

Strategien der Repression

Jede soziale Bewegung – egal wie friedlich – sieht sich ab einer gewissen Größe und Wirksamkeit vielfältigen Versuchen der Zurückdrängung („Repression“) ausgesetzt. Wenn wir als Bewegung Druck auf die Gesellschaft ausüben, dann wird die Gesellschaft auch „zurückdrücken“. Dieser Gegendruck kommt von anderen gesellschaftlichen Akteurinnen genauso wie von staatlichen. Staatliche Repression beginnt meist mit dem Versuch der „Aufklärung“, auf die dann Versuche der Diskreditierung, Isolation und Spaltung folgen, um die Wirksamkeit einer Bewegung zu schwächen.

1. Aufklärung Es ist eine selbstverständliche Aufgabe eines Staates, gesellschaftliche Strömungen zu kennen und zu bewerten. Deswegen wird jede auf Veränderung ausgegerichtete gesellschaftliche Strömung zumin-

dest im Auge behalten. Die Rettung des organischen Lebens auf diesem Planeten erfordert die eine oder andere fundamentale (manche würden sagen „radikale“) gesellschaftliche Veränderung. Darauf reagieren Ordnungsbehörden traditionell allergisch.

2. Diskreditierung *Diskreditierung? Womit sollten wir diskreditiert werden?* Ein kleines Beispiel: An den vielfältigen Protesten gegen den G8-Gipfel in Heiligendamm 2007 beteiligten sich auch mit Blumen, Wasserpistolen und Schminke „bewaffnete“ Clowns, die mit ihren kreativen Protestformen schnell das Interesse der Medien weckten. Ihr entlarvender Protest gegen die hochgerüstete Polizei eroberte in Windeseile die Herzen der Zuschauerinnen.

Und so dauerte es nicht lang, bis die Aktivist:innen beschuldigt wurden, „militante Angriffe“ mit Hilfe von Säure auf die Polizeibeamtinnen zu verüben. Zwar korrigierte sich die Polizei kurz darauf und bestätigte, dass die fragliche Flüssigkeit – Seifenblasen – weder giftig noch sauer oder überhaupt schädlich war, aber die Pressemeldung der Polizei über eine gefährliche Aktionsform war in der Welt. Und die Nachricht der friedlichen bunten Proteste landete nicht mehr in großen Buchstaben auf der ersten Seite. Der Rufschaden war erfolgreich angerichtet. Auch heute, viele Jahre später, halten sich hartnäckig die Gerüchte. Einer friedlichen Protestform wurde so ein Teil ihres Zaubers genommen.

Solche Versuche, sympathische Bewegungen zu diskreditieren, geschehen so oder ähnlich immer wieder. Vor allem breite und offene Bewegungen wie XR sind dafür leider besonders anfällig. Wir müssen also darauf vorbereitet sein.

3. Isolation Gerade weil die Polizei nicht alle an einer Aktion des zivilen Ungehorsams



beteiligten Personen verhaften kann, gehört es zu den üblichen Taktiken, an einigen wenigen Personen Exempel zu statuieren: Als du aus der Sitzblockade getragen wurdest, hast du versucht, dich zu wehren? *Widerstand gegen Vollstreckungsbeamte!* Dabei ist eine Polizistin gestolpert und hat einen Finger umgeknickt? *Schwere Körperverletzung!* Für die beschuldigten Aktivistinnen bedeuten solche Vorwürfe oft jahrelange gerichtliche Auseinandersetzungen mit hohen Kosten – für viele andere wirken sie abschreckend oder desolidarisierend. Die Wirkung geht also weit über die Diskreditierung der Einzelperson hinaus.

Es ist wichtig, in solchen Fällen als Bewegung solidarisch zusammenzuhalten, Unterstützung zu leisten, wenn möglich Kosten und Konsequenzen solidarisch zu tragen und in den Aktionen besonders aufeinander zu achten und gemeinsam auch Provokationen vonseiten der Ordnungsbehörden geschlossen und friedlich ins Leere laufen zu lassen.

4. Spaltung Spaltung zu überwinden ist ein hohes Ziel. Diskreditierung und Isolation führen nicht selten zu wachsendem Misstrauen innerhalb einer neuen Bewegung, zunehmenden Diskussionen über Abgrenzungen und fortwährende Streitereien. Insbesondere inklusive Strukturen wie XR sind dafür anfällig, solche Effekte zu verstärken und sich in ihnen zu verfangen.

Einige der simpelsten und effektivsten Techniken, das soziale Gefüge einer Gruppe zu stören, wurden 1944 im *Simple Sabotage Field Manual* [5] der US-amerikanischen CIA schön beschrieben. Darin wird Agenten des amerikanischen Inlandsgeheimdienstes dargelegt, wie sie Konferenzen und Organisationen am effektivsten sabotieren können. Es lohnt sich, schon früh darauf zu achten,

dass unsere Diskussionskultur und Wege der Entscheidungsfindung destruktiven Verhaltensweisen wenig Raum bieten – denn nicht nur mysteriöse Geheimagenten tendieren dazu. Wir alle müssen zu einer produktiven, kreativen und angenehmen Kultur der Zusammenarbeit beitragen!

- (11) *General Interference with Organizations and Production*
- (a) *Organizations and Conferences*
- (1) Insist on doing everything through "channels." Never permit short-cuts to be taken in order to expedite decisions.
 - (2) Make "speeches." Talk as frequently as possible and at great length. Illustrate your "points" by long anecdotes and accounts of personal experiences. Never hesitate to make a few appropriate "patriotic" comments.
 - (3) When possible, refer all matters to committees, for "further study and consideration." Attempt to make the committees as large as possible — never less than five.
 - (4) Bring up irrelevant issues as frequently as possible.
 - (5) Haggle over precise wordings of communications, minutes, resolutions.
 - (6) Refer back to matters decided upon at the last meeting and attempt to re-open the question of the advisability of that decision.
 - (7) Advocate "caution." Be "reasonable" and urge your fellow-conferrees to be "reasonable" and avoid haste which might result in embarrassments or difficulties later on.
 - (8) Be worried about the propriety of any decision — raise the question of whether such action as is contemplated lies within the jurisdiction of the group or whether it might conflict with the policy of some higher echelon.

Ausschnitt aus dem *Simple Sabotage Field Manual* (1944)

Unterwanderung.

Eine alte Weisheit besagt: „Wer nach allen Seiten offen ist, kann nicht ganz dicht sein.“ Das gilt leider auch für selbstorganisierte, dezentrale Systeme und flache Hierarchien: Auch Gegnerinnen und schwache Zeitgenossinnen können leicht einsteigen und durch ihr „Mitmachen“ viel Porzellan zerstören. Ein gesundes Netz des Vertrauens hilft, dagegen eine ge-



wisse Widerstandsfähigkeit aufzubauen und eine inklusive Kultur zu bewahren und weiterhin proaktiv herzustellen.

Das „Need-to-know“-Prinzip.

Für eine dezentrale Aktionsstruktur ist wesentlich, dass Informationen gut aufbereitet zugänglich sind und Ansprechpartner zu finden sind. Jede von uns muss in der konkreten Aktionsplanung jedoch nur so viele Geheimnisse kennen, wie für ihre Rolle, Pläne und Aufgaben notwendig sind. Bei diesem Prinzip geht es nicht darum, dass wir im gegenseitigen Misstrauen ersticken, sondern dass wir uns gegenseitig schützen und nicht unnötig belasten oder involvieren. Die Kunst ist also, das gesunde Vertrauen mit dem gesunden Misstrauen in Balance zu bringen: Wichtigtuerei, Klatsch und Tratsch helfen uns selten. Aufmerksames einander Zuhören und Mitdenken hingegen sehr.

Kommunikation vs. Dokumentation.

Was heute unsere notwendige Kommunikation zur Koordination, Meinungsbildung und Aktion ist, kann schon morgen in den Händen der Falschen eine genaue Dokumentation unserer Strukturen, Pläne und Motivationen sein. Unsere digitalen Kommunikationsmittel sollten das widerspiegeln und nur das dauerhaft archivieren, was auch dauerhaft benötigt wird: Mit einem Ablaufdatum versehene „Disappearing Messages“ werden von einigen Messengern unterstützt. Die Nachrichten löschen sich selbst nach einer angegebenen Zeit und helfen uns dadurch, nicht allzu große Datenberge für die Nachwelt zu sammeln. Auch Logfiles auf unseren eigenen Servern schaden oft mehr, als sie uns nutzen.

Vertrauen vs. Reichweite.

Die sogenannten „sozialen Netzwerke“ wie Instagram, Facebook oder Twitter spielen in der Orchestrierung von Protest eine wichtige Rolle. Als zentrale Systeme sind sie aber für interne Kommunikation ziemlich ungeeignet. Die Dezentralität der selbstorganisierten Systeme von XR muss sich auch technisch widerspiegeln: Soziale Netzwerke eignen sich großartig für Mobilisierung und PR, aber unsere interne Kommunikation ist auf sicheren, möglichst dezentralen Kanälen besser aufgehoben!

Gehe in das Gefängnis. Begib dich direkt dorthin. Gehe nicht über Los. Ziehe nicht 4 000 € ein.

Digitale Spuren.

Knapp ein Drittel von XR ist bereit, für *die Sache* Repression in Kauf zu nehmen oder sogar dafür verhaftet zu werden. Dieser Mut verdient Anerkennung. Aber er sollte auch seine Wirkung entfalten können und sich lohnen: Das Ziel kann nicht sein, so schnell wie möglich im Knast zu landen.

Wir sollten also darauf achten, so wenig Spuren, Anhaltspunkte und Beweise wie möglich zu liefern, die gegen uns und unsere Mitstreiterinnen verwendet werden können. Im Digitalen ist das nicht einfach: Mobilfunknetze, Internetanschlüsse und Onlineplattformen können überwacht oder zur Herausgabe deiner Daten gezwungen werden – und auch ein beschlagnahmtes Mobiltelefon wird schnell zum gefundenen Fressen für Ermittlerinnen.

„Ich werde überwacht!“

Ja, zu einem gewissen Grad werden wir alle überwacht. Aber keine Panik! Es ist wichtig, sich nicht einschüchtern zu lassen, sondern informiert damit umzugehen: Welche Spuren



hinterlassen wir, wie können wir sie vermeiden?

Digitale Überwachung läuft nicht etwa so ab, dass sich eine menschliche Person eigenhändig und gezielt mit dir persönlich und deinen Kommunikationsinhalten auseinandersetzen würde – eine solche Aufmerksamkeit müsstest du dir mit einer ausgiebigen kriminellen Karriere erarbeiten (ich rate dringend davon ab). Die digitale Überwachung läuft automatisch und effizient mit Hilfe von Computern.

Aber auch mit modernen Computern ist es kaum möglich, sämtliche Inhalte von sämtlichen Nachrichten und Telefonaten abzuhören und zu analysieren – es würden dabei zu viele Daten anfallen und verarbeitet werden müssen. Deshalb konzentriert sich die digitale Massenüberwachung auf sogenannte Metadaten.

Metadaten vs. Inhalte.

Metadaten sind alles *außer den Inhalten* unserer Kommunikation: Mit wem hast du wann über welchen Dienst gechattet? Wen hast du danach angerufen? Mit wem haben diese Personen wiederum regelmäßigen Kontakt? Wie oft sind diese Menschen online und an welche Orte bewegt sich regelmäßig ihr Mobiltelefon?

All diese Fragen sind mit vergleichsweise überschaubaren Datenmengen sehr detailliert und aufschlussreich zu beantworten. Tatsächlich in die Kommunikationsinhalte zu blicken, würde einen sehr viel größeren Aufwand bei möglicherweise viel geringerem Erkenntnisgewinn bedeuten.

Die Verschlüsselung unserer Inhalte ist also nur eine Seite der Medaille: Mit einem Bewusstsein dafür, welchen Fingerabdruck an Metadaten wir wo hinterlassen, können wir verstehen, wo wir durchschaubar sind.

Verschlüsselung.

Die Erfassung von Inhalten verhindern wir am wirksamsten durch Verschlüsselung. Dabei unterscheiden wir die Verschlüsselung von gespeicherten Daten (zum Beispiel auf dem eigenen Rechner oder Mobiltelefon) von verschlüsselter Kommunikation, also Inhalten, die wir auch an andere senden.

Datenträger.

Mal angenommen unser Laptop oder Mobiltelefon gelangt – durch Verlust oder Beschlagnahme – in die falschen Hände. Auch wenn wir die Anmeldung vielleicht durch ein Passwort geschützt haben, befinden sich trotzdem alle Daten mit simplen Mitteln auslesbar auf dem internen Speicher. Dieser lässt sich wie ein USB-Stick an einen anderen Rechner anschließen und auslesen – ziemlich ungünstig für uns.

Zumindest unsere brisanten und persönlichen Daten, am besten aber der ganze Datenträger sollte daher verschlüsselt sein, um genau dieses einfache Auslesen zu verhindern. Alle aktuellen Betriebssysteme – sei es für Computer oder Mobiltelefone – bieten eine solche Funktion an. Sie zu nutzen hilft uns, ruhig zu schlafen, wenn unsere Geräte in die falschen Hände gelangen. Natürlich ist das nicht nur für den unwahrscheinlichen Fall einer Beschlagnahme wichtig, sondern gilt auch im viel wahrscheinlicheren Fall, dass du ganz einfach mal dein Telefon verlierst.

Kommunikation.

E-Mails, SMS und die Mehrzahl der über Online-Anbieter versandten Nachrichten werden unverschlüsselt übermittelt. Das bedeutet, dass wir den Anbietern vertrauen müssen, die Nachrichten nicht weiterzugeben. In vielen Fällen können sie jedoch gesetzlich dazu gezwungen werden. Und nicht selten kommt es





vor, dass unsere Nachrichten unbeabsichtigt in die Hände Dritter gelangen – zum Beispiel durch Sicherheitslücken oder „bedauerliche Fehler“. Besser also, wenn wir den Anbietern gar nicht erst mit unseren Nachrichteninhalten vertrauen müssen!

Handy-Apps wie *Signal* oder *Threema* [6] verschlüsseln unsere Nachrichten schon vor dem Versand so, dass sie nur das Gerät der Empfängerin entschlüsseln kann. Das Gleiche gilt für E-Mail-Verschlüsselung mit PGP oder S/MIME. Egal, welche Server die Nachricht zur Empfängerin übermitteln – sie können allenfalls noch unsere Metadaten sammeln, die Inhalte sind (hoffentlich) sicher.

Hinzu kommt, dass verschlüsselte Messenger den (heute) üblichen Abhörschnittstellen der Telefon- und Internetüberwachung auch das Sammeln von Metadaten erschweren: Zwar ist auf der Leitung zu sehen, dass wir den Messenger nutzen, es müssen aber genauso die Leitungen unserer Kommunikationspartnerinnen überwacht werden, um durch zeitliche Korrelation zu erkennen, mit wem wir schreiben. Natürlich gibt es aber in vielen Ländern schon Bestrebungen, per Gesetz den Zugriff zu erzwingen – wir sollten uns also nicht darauf verlassen.

Metadaten.

Verschlüsselte Kommunikation bietet wichtigen Schutz – insbesondere vor akuter, aktueller Überwachung, bei der auch Inhalte von Interesse sind. Dazu kommt die zunehmende Bedeutung von Metadaten. Es lohnt sich, genau zu überlegen, welche Metadaten wir vermeiden oder wie wir verwirren können. Zwei Beispiele:

- Welche Websites wir wann und wie lang besucht haben, können wir mithilfe von Tor [7] verschleiern. Der *Tor Browser* ist vielleicht etwas langsamer, ermöglicht uns

aber das Umgehen von Zensur und Überwachung. Er hilft natürlich nur wenig, wenn wir uns dann damit bei Facebook unter unserem bürgerlichen Namen anmelden, oder sonstige nicht-anonyme Schritte unternehmen, ist aber bei der Recherche und Vorbereitung von Aktionen ein wichtiges Werkzeug.

- Bei Demonstrationen und Aktionen wird nicht selten eine sogenannte Funkzellenabfrage durchgeführt: Die Polizei fragt bei den Mobilfunknetzen an, welche Mobiltelefone in einem bestimmten Zeitraum an einem bestimmten Ort waren. Es lohnt sich also manchmal, das Telefon zu Hause zu lassen, oder in der Bezugsgruppe ein paar Demo-Handys mit stets wechselnden Besitzerinnen zu haben.

Ein Metadatum kommt selten allein. Analog zu diesen Beispielen kannst du dir über das Einkaufen mit EC- oder Kreditkarte und das Bestellen bei Onlineversandhändlern, über die Verwendung des gleichen Nutzernamens bei verschiedenen Anbietern oder über das gelegentliche Zuhause lassen deines Telefons Gedanken machen.

Das Gemeine an Metadatensammlungen ist, dass sie a) fast „ewig“ verfügbar sind und b) sehr schön aus verschiedenen Quellen kombiniert werden können: Vielleicht ist dein Instagram-Account datensparsam, aber welches Bild ergibt sich zusammen mit deinen Reisebewegungen und deinem Einkaufsverhalten? Ob oder wie die Daten, die wir heute achtlos preisgeben, morgen oder übermorgen gegen uns oder Mitstreiterinnen verwendet werden, können wir heute noch nicht abschätzen. Daher lohnt es sich, aus der Vermeidung und Vernichtung von Metadaten ein fleißiges Spiel zu machen: Datensparsamkeit zahlt sich ebenso aus wie Irritation durch bewusste Abweichungen von unseren üblichen Mustern.



Bei allem wirkt es befreiend, auch gegen sich selbst anzutreten – wie vorhersehbar bin ich eigentlich? Überraschen wir die Behörden, uns selbst und alle anderen: Wir haben ein wichtiges Ziel, wir wollen uns anders organisieren und wir haben die Technologien dafür! Wir müssen sie nur richtig einsetzen, freudig immer weiter dazulernen und loslegen.

Referenzen

- [1] Hausdurchsuchung bei den Zwiebel-freunden und OpenLab Augsburg: <https://www.ccc.de/de/updates/2018/hausdurchsuchungen-bei-vereinsvorstandender-zwiebelfreunde-und-im-openlab-augsburg>
- [2] Polizei reitet erneut beim CCC ein: <https://www.ccc.de/de/updates/2018/unrechtmalige-hausdurchsuchung-polizei-reitet-erneut-beim-chaos-computer-club-ein>
- [3] Artikel „Hausdurchsuchungen – Ein Blick aus der zweiten Reihe“ in der Datenschleuder #99: <https://ds.ccc.de/download.html>
- [4] Wann wenn nicht wir* – Ein Extinction Rebellion Handbuch. Herausgegeben von: Sina Kamala Kaufmann + Michael Timmermann + Annemarie Botzki. Originalsprache: Englisch. Übersetzt von: Ulrike Bischoff. Erschienen 2019 im Verlag S. Fischer.
- [5] Simple Sabotage Field Manual der CIA: https://www.cia.gov/news-information/featured-story-archive/2012-featured-story-archive/CleanedUOSSSimpleSabotage_sm.pdf
- [6] Bei der Wahl des Messengers gibt es eine Reihe an Features zu beachten. Das hier gewählte Beispiel *Signal* (<https://signal.org/>) bietet *Disappearing Messages*, wird aber an eine Telefonnummer gebunden, was eine anonyme Nutzung weitestgehend unmöglich macht. Andere Messenger wie zum Beispiel *Threema* (<https://threema.ch/>) bieten anonyme „Adressen“, aber zum Zeitpunkt der Veröffentlichung dieses Artikels leider keine *Disappearing Messages*. Auf religiösen Fundamentalismus wird im Rahmen dieses Artikels verzichtet, so lange niemand auf die Idee kommt, *WhatsApp* zu verwenden.
- [7] The Onion Router (Tor): <https://torproject.org/>





Als bezahlter Bot in Brüssel

von kantorkel <kantorkel@hamburg.freifunk.net>

Ein Bericht von EDRIs Artikel 13 Actionweek

Kurz vor der Artikel 13-Abstimmung hat EDRI [1] etwa zwölf Aktivisten aus ganz Europa nach Brüssel eingeladen. Aus Deutschland waren wir zu zweit angereist und haben versucht, mit möglichst vielen EU-Abgeordneten (Members of the European Parliament, MEPs) und deren Assistentinnen und Assistenten über die Reform der EU-Urheberrechtsrichtlinie und insbesondere Artikel 13 und Uploadfilter zu sprechen.



Vorbereitung

Bevor wir uns auf den Weg nach Brüssel gemacht haben, hat EDRI uns mit einem Leitfaden zur Actionweek versorgt. In diesem gab

es Hinweise zur Vorbereitung der Treffen und mögliche Gesprächspunkte wurden skizziert.

Zunächst war jedoch wichtig, dass wir viele MEPs anschreiben, um Termine zu vereinbaren. Leider wurden viele E-Mails nicht oder erst sehr spät beantwortet und auch telefonisch haben wir nur wenige Termine ausmachen können.

Nebenbei haben wir den Entwurf der Urheberrechtsrichtlinie gelesen und uns mit Argumenten für und gegen die Reform beschäftigt. Vielen Dank an dieser Stelle an Julia Reda, die auf ihrer Webseite [2] stets alle wichtigen Informationen aktuell zusammengestellt hatte.

Und dann ging es auch schon nach Brüssel.

Actionweek, Tag 1

Der erste Tag begann mit einem Treffen bei EDRI. Nach einer Vorstellungsrunde gab es einen Kurs EU-Gesetzgebung im Schnelldurchlauf. [3]

Danach wurde erklärt, wie wir uns im Parlament zurechtfinden, wie Gespräche mit MEPs im Allgemeinen ablaufen können und es gab auch noch einmal Hinweise zu möglichen Gesprächspunkten. Dann ging es zu unserem ersten Termin ins Parlament.

Gleich das erste Treffen mit einem CDU-Mitarbeiter dauerte 80 Minuten. Auch wenn wir ihn nicht davon überzeugen konnten, dass man Artikel 13 lieber streichen sollte, war das Treffen sehr angenehm. Wir hatten das Gefühl, dass er ernsthaft an unseren Bedenken interessiert war und diese nicht einfach nur zur Kenntnis genommen hat. Außerdem war er bemerkenswert gut über die Argumente bei-



der Seiten informiert. Schlussendlich war er aber der Meinung, dass die Richtlinie lieber so als gar nicht umgesetzt werden soll. Schließlich hätte man Jahre auf diesen Entwurf hingearbeitet und so einfach würden die verschiedenen Länder der EU in Sachen Urheberrecht nicht wieder auf einen Nenner kommen. Außerdem betonte er, dass man später noch nachbessern könne, sollten etwa die Ausnahmeregelungen nicht ausreichen oder Overblocking trotz Beschwerdemöglichkeit ein Problem darstellen.

Nach dem Treffen ging es zurück in den Eingangsbereich. Dort konnten wir verschlafen und uns mit den anderen Aktivisten austauschen. Zwischen den Gesprächen sind wir dort immer wieder zusammengekommen und haben von Erfolgen und Misserfolgen berichtet.

Auch neben den zuvor vereinbarten Terminen gab es viele Gelegenheiten zumindest kurz mit Assistentinnen und Assistenten von MEPs ins Gespräch zu kommen. Wenn wir sowieso schon auf dem Flur einer Partei waren, haben wir kurzerhand in den benachbarten Büros gefragt, ob sie kurz Zeit hätten und die meisten haben sich kurz Zeit genommen.

Viel haben wir aus diesen spontanen Gesprächen jedoch nicht mitgenommen. In der Regel liefen sie so ab, dass wir uns kurz vorstellten („Wir haben uns extra auf den Weg nach Brüssel gemacht, um...“), dann konnten wir unsere Bedenken vortragen und abschließend haben die Mitarbeiterinnen und Mitarbeiter versprochen, den MEPs mitzuteilen, dass jemand dagewesen wäre. Keines dieser spontanen Gespräche hat länger als fünf Minuten gedauert.

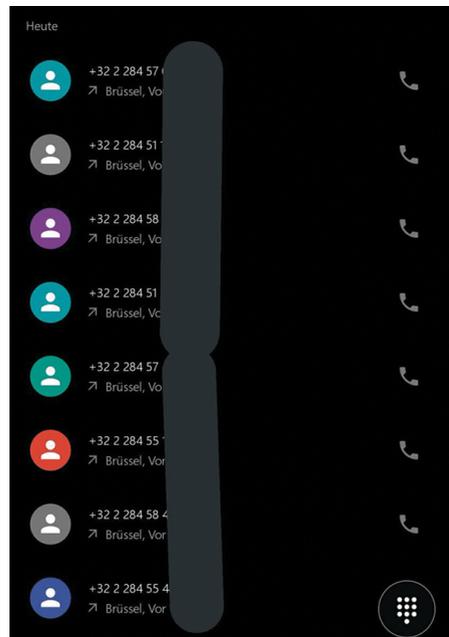
Bemerkenswert war unsere letzte Begegnung am ersten Tag im EU-Parlament. Wir stellten uns vor und unser Gegenüber, ein Mitarbeiter eines CDU-Abgeordneten, begrüßte uns mit abfälligen Kommentaren über Nerds,

fragte: „Was fällt euch denn ein, hier einfach so aufzutauchen?“ und dann war das Gespräch auch schon wieder vorbei und wir wurden aus dem Büro geworfen.

Abends ging es dann noch gemeinsam essen und zum netzpolitischen Biertrinken [4].

Actionweek, Tag 2

Der Donnerstag war sehr frustrierend. Der erste Termin wurde kurzfristig abgesagt und viele MEPs waren schon abgereist. Daher fingen wir an zu telefonieren, um spontan Termine auszumachen oder wenigstens am Telefon mit MEPs zu sprechen.



Anrufliste von kantorkel via Twitter 21. März 5:51 Uhr

Zunächst haben wir versucht alle deutschsprachigen unentschiedenen MEPs zu kontak-



Public Money, Public Code – auch für Bildungseinrichtungen

von Monika Heusinger <m.heusinger@orange.fr>

Der *DigitalPakt Schule* [1], der *Qualitätspakt Lehre* für Hochschulen sowie andere staatliche Fördermittel zum Beispiel des Bundesministeriums für Bildung und Forschung sind Initiativen, die Bildungseinrichtungen finanziell bei der Umsetzung von Digitalisierungsstrategien unterstützen. Durch Open-Source-Lösungen können öffentliche Gelder eingespart, Arbeitszeit reduziert sowie digitale Infrastrukturen optimiert werden.

Notwendigkeit einer digitalen Infrastruktur

Bildungseinrichtungen sind Teil eines Bildungssystems und damit eines gesellschaftlichen Systems. Daher verändert die digitale Transformation auch das Arbeiten in diesen Institutionen. Digitale Möglichkeiten erleichtern den Workflow und unterstützen die Gestaltung von Lehr-Lern-Prozessen. Dafür ist es sinnvoll, eine digitale Infrastruktur angepasst an das eigene Profil, die eigene Organisation, das eigene Konzept und somit die eigenen Anforderungen einzurichten. Neben einer performanten Breitbandversorgung werden Server, Router und Switches benötigt. Eine Cloud-Lösung muss gefunden werden für eine ubiquitäre Verfügbarkeit der benötigten Informationen. Zudem muss die Frage geregelt werden, wie ein rechtskonformer Zugang

zum WLAN für alle Mitglieder der Bildungseinrichtung geregelt werden kann.

Im Anwendungsbereich wären zum Beispiel in Schulen für ein angenehmes Arbeiten unter anderem folgende Funktionen hilfreich:

- Präsentation von Informationen
- Kommunikation der Mitglieder untereinander in unterschiedlichen offenen und geschützten Bereichen
- Austausch von Materialien
- kollaborative Anwendungen
- Archivierung von Dokumenten
- Lerngruppen- und Prüfungsverwaltung
- Management von Verwaltungs- beziehungsweise Geschäftsprozessen
- Raum- und Medienbuchungssystem
- Kalender

Um allen die Nutzung der digitalen Infrastruktur zu ermöglichen und niemanden zum Kauf eines bestimmten Geräts oder der Ver-



wendung eines bestimmten Systems zu zwingen, sollten plattform- bzw. betriebssystemunabhängige Lösungen gefunden werden. Darüber hinaus sollten die Anwendungen im responsive Design sein, um die Wahl zwischen einer mobilen oder einer Desktopnutzung zu lassen. Damit die Infrastruktur zu einer persönlichen Lernumgebung für alle Nutzerinnen und Nutzer werden kann, muss der Zugang zu den Anwendungen zudem barrierefrei sein und die Plattform muss individuell gestaltbar sein, da jede/jeder ein anderes Ordnungssystem und andere Strukturen bevorzugt.

Forderung nach Open-Source-Lösungen

Bei *Public Money, Public Code* [2] handelt es sich um eine Kampagne der *Free Software Foundation Europe*, die vom *Chaos Computer Club e. V.* unterstützt wird. In der Kampagne wird gefordert, dass von öffentlichen Geldern finanzierte Software auch der Öffentlichkeit als Public Code zur Verfügung gestellt wird. Im Fokus steht die Entwicklung von Software für öffentliche Verwaltungen. Von öffentlichen Geldern werden jedoch auch Anwendungen von Bildungseinrichtungen finanziert und auch hier sollte dies unter Quelloffenheit und freien Lizenzierungen erfolgen. Die Forderung bedeutet für Bildungseinrichtungen nicht nur, dass Anwendungen, die für die Einrichtung entwickelt werden, offen lizenziert der Öffentlichkeit zur Verfügung gestellt werden. Die Forderung beinhaltet ebenso, dass bestehende Open-Source-Lösungen verwendet werden.

Relevanz eines Public Code

Anwendungen als Open Source zur Verfügung zu stellen und verfügbare Open-Source-Lösungen zu verwenden, würde in Bildungseinrichtungen vieles ermöglichen, vieles ver-

einfachen und vieles datenschutzfreundlicher gestalten.

Datenschutz

In Bildungseinrichtungen wird mit sensiblen Daten gearbeitet. Daher sind ein besonderer Schutz dieser Daten und eine Datenhoheit wichtig. Diese Datensouveränität kann durch Verwendung von Open-Source-Lösungen erreicht werden, die selbst gehostet werden können. Dadurch behält man die Kontrolle, welche Daten erfasst werden, wo die Daten gespeichert werden, wie sie verarbeitet werden, wer Zugriff auf die Daten hat und wer wie an wen welche Daten weitergeben darf. Global operierende Anbieter oder regionale kommerzielle Anbieter stellen ihre Plattformen unter Berufung auf eine C5-Zertifizierung, dem Anforderungskatalog [3] des Bundesamts für Sicherheit in der Informationstechnik gemäß, zwar gerne als datenschutzrechtlich unbedenklich dar, dies ist jedoch kritisch zu hinterfragen, wie es zum Beispiel die Analyse von Mike Kuketz einer solchen Plattform zeigt. [4] In der Analyse der Internetplattform *Google Classroom*, die nur eine von vielen Angeboten dieser Art ist, stellt Kuketz klar, dass die für den Nachweis der datenschutzrechtlichen Unbedenklichkeit herangezogene C5-Zertifizierung nur Empfehlungen zum Datenschutz ausspricht, jedoch die rechtliche Seite nicht adressiert. Das ebenso gerne verwendete Trusted-Cloud-Datenschutz-Profil gibt ebenso wenig Sicherheit, da es noch nicht die Datenschutz-Grundverordnung berücksichtigt. Vorgehensweisen solcher Anbieter wie die Nutzung von Inhalten für Ad Targeting zeigen jedoch, dass man die Daten besser in selbst gehosteten Anwendungen speichert.



Datensouveränität

Mit selbst gehosteten Open-Source-Anwendungen hat man nicht nur die Kontrolle über eigene Daten, sondern auch über die Firmware, das Betriebssystem sowie die Software. Dies ermöglicht eine Unabhängigkeit von Firmenphilosophien. Man muss nicht mehr hilflos hinnehmen, dass Anbieter Nutzungs- oder Geschäftsbedingungen ändern. Bei Software von Fremdanbietern verliert man Daten, wenn der Entwickler die Software vom Markt nimmt oder man muss eventuell einen komplizierten Datenumzug vornehmen, wenn die Software nicht mehr weiterentwickelt wird. Bei Open-Source-Anwendungen verfügt man über den Quellcode und es findet sich bei Entwicklungsstau oder Veränderungen, die nicht mehr den eigenen Vorstellungen entsprechen, in der Regel eine neue Community, die das Projekt übernimmt oder als Fork weiterentwickelt. Das CERN hat sich nach einer starken Erhöhung der Lizenzgebühren durch einen kommerziellen Anbieter für eine Migration zu Open-Source-Technologien entschieden. [5] Durch die erhöhten Gebühren hätten wichtige Gelder für die Forschungsarbeit gefehlt. Ein Schritt, dem andere Bildungseinrichtungen folgen sollten.

Ressourcenorientierung

Public Money, Public Code im Bildungsbereich schließt einen sinnvollen Umgang mit finanziellen und geistigen Ressourcen ein. Es kommt vor, dass eine Bildungseinrichtung sich für eine digitale Plattform entscheidet, die von einer Agentur speziell auf die Bedürfnisse angepasst entwickelt wird. Es entsteht eine Plattform, die als Informations-, Kommunikations- und Archivierungszentrale sowie als virtueller Coworking Space dient. Die Startfinanzierung läuft über das zuständige Ministerium

oder den verantwortlichen Träger. Nun wäre es sinnvoll, den Code auch anderen Bildungseinrichtungen zur Verfügung zu stellen, damit diese nicht das Rad neu erfinden müssen, was Zeit der Mitarbeiterinnen und Mitarbeiter zur Konzepterstellung sowie technischen Umsetzung in Anspruch nimmt und mit hohen Entwicklungskosten verbunden ist. Wäre der Code quelloffen und offen lizenziert, könnten die Strukturen übernommen werden und die Plattform könnte in Bezug auf eigene Anforderungen von anderen Institutionen weiterentwickelt beziehungsweise verändert werden. Hier wäre eine stärkere Vernetzung wünschenswert, da gemeinsam das digitale System stärker optimiert werden kann, als wenn jede Bildungseinrichtung für sich alleine arbeitet. Wie hier Steuergelder hätten eingespart werden können, zeigen Beispiele von bundeslandspezifischen Lehr- und Lernumgebungen oder sogenannten Bildungscloids. Überall treten ähnliche Probleme auf, hohe Entwicklungskosten führen nicht zu dem erhofften Ergebnis und dennoch findet kein Austausch statt. [6, 7] Dabei gibt es bestehende Open-Source-Lösungen, die weit entwickelt sind und bei Selbsthosting oder einem Hosting auf einem Bildungs- beziehungsweise Landesserver eine datenschutzfreundliche, umfassende Arbeitsumgebung schaffen. Möglich ist zum Beispiel im schulischen Verwaltungsbereich die Nutzung von linuxmuster [8] als Schulnetzlösung. Darin kann als Cloudlösung zum Beispiel Nextcloud [9] implementiert werden. Nextcloud bietet neben der Dateiablage zahlreiche Features wie Kalender, Mail, Chat und Kontaktverwaltung. Durch eine Erweiterung zum Beispiel mit Collabora [10] wird die Plattform zum digitalen Coworking Space, da kollaborative Anwendungen zur Verfügung stehen. Es muss also nicht immer eine eigene Lösung entwickelt werden, sondern es kann





auf bestehende, von einer starken Community getragene Anwendungen zurückgegriffen werden.

Gestaltungsfreiheit

Kommerzielle Lernplattformen weisen oft das Problem auf, dass sie von Menschen entwickelt wurden, die in der Regel nicht mit internen Abläufen in Bildungseinrichtungen vertraut sind. Als Kundin/Kunde hat man auf die Konzeption der Struktur und Funktionalität oft nur bedingt oder keinen Einfluss. Man kann in vielen Fällen nur Angebote miteinander vergleichen und die Plattform wählen, die noch am besten zur eigenen Infrastruktur passt. Hat eine Bildungseinrichtung selbst ein funktionierendes System entwickelt, könnte dies bei offener, freier Lizenzierung von anderen genutzt und weiterentwickelt werden. Die Grundstruktur kann übernommen und individuell erweitert werden. Es können Features nach eigenem Bedarf integriert werden und man kann nicht benötigte Funktionen entfernen, um den Fokus auf relevante Elemente zu richten.

Nachhaltigkeit

Verzichtet man auf die Verwendung von Anwendungen von Fremdanbietern und hostet die Software selbst, kann man auf eine umweltfreundliche Serverumgebung achten, zum Beispiel mit einer fair hergestellten Hardware aus umweltverträglichen Materialien, energieeffizienten Servern sowie energieoptimierten Prozessoren und Festplatten. Auch eine Server-Virtualisierung kann einen positiven Umwelteffekt haben. Zudem kann man mit Ökostrom arbeiten. Damit können selbst gehostete Open-Source-Lösungen einen Beitrag zur Nachhaltigkeit leisten.

Sozialverträglichkeit

Open-Source-Lösungen sollten so entwickelt werden, dass sie plattform- bzw. betriebssystemunabhängig nutzbar sind. Alle Mitglieder einer Bildungseinrichtung sollten die digitale Infrastruktur mit ihren eigenen Geräten nutzen können. In Schulen findet man teilweise das Modell der Tabletklassen, bei dem Eltern beziehungsweise Erziehungsberechtigte der Schülerinnen und Schüler gezwungen werden, ein Tablet eines bestimmten Herstellers zu kaufen oder zu mieten, was eine finanzielle Belastung darstellen kann. Hier ist bei der Konzeption der digitalen Infrastruktur auf Sozialverträglichkeit zu achten. Damit es nicht zum Konkurrenzkampf um das performanteste Gerät kommt, kann die Einrichtung zudem zum Arbeiten in der Einrichtung eigene Geräte zur Verfügung stellen. Dennoch ist auf die Verwendung von plattform- beziehungsweise betriebssystemunabhängigen sowie barrierefreien Anwendungen zu achten, damit auch außerhalb der Lernzeiten in der Bildungseinrichtung in der digitalen Infrastruktur gearbeitet werden kann. Somit stellen Open-Source-Anwendungen eine demokratische Lösung dar und können einen Beitrag zu mehr Sozialverträglichkeit leisten.

Finanzierung

Public Code heißt nicht automatisch kostenlos. Die Frage ist, wer wie die Entwicklung der Software finanziert. Wird die Anwendung im Auftrag einer Bildungseinrichtung entwickelt, geschieht dies oft nicht quelloffen, da die Bildungseinrichtung nicht alleine die Kosten tragen möchte für etwas, das dann von anderen genutzt wird. Hier bedarf es eines Umdenkens und einer offenen Share-Haltung. Wenn alle sich für Open-Source-Lösungen einsetzen, dann finanziert man eventuell alleine die Kosten für eine Anwendung, profitiert jedoch von



der Quelloffenheit einer Vielzahl von anderen Anwendungen. Es muss nur eine Einrichtung den Anfang machen. Auch für die Anbieter von Open-Source-Software gibt es Geschäftsmodelle, die eine Finanzierung ermöglichen. So kann zum Beispiel die Software quelloffen und frei lizenziert zum Selbsthosting zur Verfügung gestellt werden und zur Finanzierung werden kostenpflichtig Zusatzdienste angeboten. Diese können zum Beispiel ein individueller Support, ein Angebot an individuellen Anpassungen oder ein DSGVO-konformer Hosting-Service sein. Dadurch wird die konzeptuelle sowie technische Entwicklung finanziell unterstützt, jedoch werden öffentliche Gelder gebündelt und kommen der Allgemeinheit zugute.

Mögliche

Open-Source-Lösungen

Für Bildungseinrichtungen gibt es viele gut entwickelte und userfreundliche Open-Source-Lösungen, von Firmware über Betriebssystem bis hin zu Anwendungen. Eine Auflistung von Möglichkeiten hat die Autorin in einem Blogartikel aufbereitet. [11] Es wäre daher ein wichtiger Schritt hin zu einem verantwortungsvollen Umgang mit Daten und öffentlichen Geldern, diese Möglichkeiten sinnvoll zu nutzen.

Referenzen

- [1] Verwaltungsvereinbarung *DigitalPakt Schule 2019 bis 2024* zwischen Bund und Ländern https://www.bmbf.de/files/VV_DigitalPaktSchule_Web.pdf
- [2] Die Kampagne *Public Money, Public Code*: <https://publiccode.eu/de/>
- [3] Anforderungskatalog Cloud Computing (C5) des Bundesamtes für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Anforderungskatalog-Cloud_Computing-C5.pdf
- [4] Google Classroom: Die Datenkrake in der Schule: <https://www.kuketz-blog.de/google-classroom-die-datenkrake-in-der-schule>
- [5] Migrating to open-source technologies: <https://home.cern/news/news/computing/migrating-open-source-technologies>
- [6] Aufstieg und Fall von Logineo: <https://digitalcourage.de/blog/2019/alle-170000-nrw-lehrerinnen-logineo-erklaerung-nicht-unterschreiben>
- [7] Schul-Portal Ella verzögert sich wohl um Jahre: <https://heise.de/-4169381>
- [8] linuxmuster – eine Komplettlösung für den Betrieb schulischer Netzwerke: <https://www.linuxmuster.net/de/home/>
- [9] Nextcloud – eine Cloudlösung zur Ablage von Daten auf einem eigenen Server: <https://nextcloud.com>
- [10] Collabora Online in Nextcloud – eine Cloud-basierte Office-Lösung: <https://nextcloud.com/collaboraonline/>
- [11] Auflistung möglicher Open-Source-Lösungen: <https://monika-heusinger.info/blog/privacy>



Arbeitgeberneugier – Unterschätztes Risiko für die Sicherheit unserer Daten

von Max Schmitt <ccc_br@web.de>

Die Neugier des Arbeitgebers stellt ein unterschätztes Risiko für die Sicherheit unserer Daten dar, doch auch der Umgang mit Arbeitnehmerdaten unterliegt dem Schutz der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG).

Zurecht wird hier regelmäßig vor dem Datenhunger vieler Behörden, staatlicher Einrichtungen und Regierungen gewarnt. Dass die „sozialen Medien“ nur Interesse daran haben, Geld mit unseren Daten zu verdienen, ist klar. Dass die Sicherheitslücken vieler Serviceprovider unsere Daten preisgeben, wird auch regelmäßig bekannt. Ich möchte mit diesem Beitrag meinen Blick auf eine Institution richten, die weitaus bessere Möglichkeiten zum Auskundschaften unserer Privatsphäre hat, als ein Bundestrojaner, die ganz selbstverständlich unsere Leistung und unser Verhalten auswerten, und vieles mehr: Der Arbeitgeber.

Im Arbeitsleben fällt eine Vielzahl personenbezogener Daten an:

- Zur Sicherheit sind Videokameras installiert, die jedes Betreten und Verlassen des Gebäudes dokumentieren. Natürlich nur zur Sicherheit des Gebäudes. Wie oft ein Raucher nach draußen geht und sich nicht ausstempelt, dokumentieren sie aber auch.
- Die Zeiten für Kommen, Pausen und Gehen werden gespeichert und lassen sich – nicht nur zur Berechnung der Arbeitszeit – hervorragend nutzen. Auch zur Mustererkennung oder der Suche nach Verstößen.
- Vermeintlich sicheres Surfen im Internet per HTTPS wird aus Sicherheitsgründen analysiert, indem die Verschlüsselung wie bei einem Man-in-the-Middle-Angriff unterbrochen wird. Andere Möglichkeiten,

zum Beispiel Tor einzusetzen, werden technisch eingeschränkt.

- Der Inhalt von E-Mails wird ebenfalls aus Sicherheitsgründen bis hin zu den Anhängen einer genauen Analyse unterzogen.
- Auf den Rechnern laufen Tools die vordergründig den Zweck haben zu verhindern, dass Dateien mit personenbezogenen Kundendaten unverschlüsselt verschickt oder auf USB-Sticks kopiert werden. Dass sie dazu kontinuierlich jede Aktion des Anwenders analysieren und jede genutzte Datei nach ihrem Inhalt untersuchen, wird heruntergespielt.
- Die Möglichkeiten von Microsoft 365 oder Salesforce zur Überwachung des Anwenderverhaltens – beides inzwischen ein Quasi-Standard – sprengen den Rahmen dieses Artikels und füllen ganze Bücher. Von Standardauswertungen, wer mit wem wie oft und auf welchem Weg mit Microsoft 365 kommuniziert, muss kein Arbeitgeber träumen. Das geht heute schon ganz einfach, zum Beispiel mit Workplace Analytics. [1] Und wie erfolgreich ein Verkäufer ist, wie viele E-Mails es für einen Abschluss braucht und wie zufrieden der Kunde mit ihm ist, liefern die Dashboards von Salesforce [2] ohne weitere Anpassungen.
- Vermeintliche Compliance-Verstöße werden zum Anlass genommen den Netzwerkverkehr auszuwerten oder automatisiert



in fremde E-Mails zu schauen und nach Mustern zu suchen. Das bieten Unternehmensberatungen im Paket an, ohne dass der Arbeitgeber hier viel tun muss.

- KPIs (Key Performance Indicator) werden aus allen zugänglichen Datenquellen generiert, um Minderleister zu identifizieren und Gründe zu finden, um diese loszuwerden.

Die Liste ließe sich beliebig verlängern und stellt nur einen Auszug der Themen dar, mit denen ich in den letzten Monaten zu tun hatte.

Selbstverständlich geht die Mehrheit der Arbeitgeber verantwortungsvoll mit den Beschäftigtendaten um. Aber es gibt auch zahlreiche schwarze Schafe. Der gesetzlich vorgegebene Datenschutz stellt für diese nur ein Hindernis dar. Dazu zwei Originalzitate eines Managers aus einem großen, weltweit agierenden Konzern:

„Da die Führungskräfte heute ohnehin in allen Fällen das Recht haben, solche Informationen für ihren Verantwortungsbereich einzusehen, gibt es keinen Grund, den regelmäßigen systemunterstützten Zugriff einzuschränken.“
 „Systembeschränkungen schränken die Wirksamkeit der Managementaktivitäten nur ein und hindern Führungskräfte auf allen Ebenen daran, ihre Aufgaben zu erfüllen.“

Man geht einfach davon aus, dass man „ohnehin in allen Fällen das Recht“ hat, ohne auf DSGVO oder BDSG Rücksicht zu nehmen. Da wird ein „systemunterstützender Zugriff“ zur punktgenauen Verhaltenskontrolle als Grundrecht für Führungskräfte angesehen. „Systembeschränkungen“ behindern Führungskräfte nur. Die Rechte der Beschäftigten einschließlich der in der EU-Grundrechtecharta garantierten Menschenrechte, hier vor allem Artikel 8 – Schutz personenbezogener Daten, werden einfach ignoriert.

Sich hier als Arbeitnehmer zur Wehr zu setzen ist schwierig. Man schafft sich keine Freunde im Management, Benachteiligungen können die rasche Folge sein.

Zum Schutz gibt es zwei Gruppen, die leider ihre Möglichkeiten zum Schutz der Mitarbeiterdaten oft nicht ausschöpfen: Gewerkschaften und Betriebsräte. Vor allem letztere hätten hier viele Möglichkeiten, direkt regulierend einzugreifen:

- So gibt es für den Einsatz von Systemen zur Verarbeitung personenbezogener Mitarbeiterdaten in der Regel keine Rechtsgrundlage. Oder in welchem Gesetz steht, dass die Verwendung von Microsoft 365, Workday oder Salesforce notwendig ist? Erst eine Betriebsvereinbarung zwischen Arbeitgeber- und Arbeitnehmervertretern stellt eine solche, auch von der DSGVO geforderte, Grundlage dar. Vorher ist die Verarbeitung rechtswidrig und könnte vom Betriebsrat per einstweiliger Verfügung gestoppt werden.
- In einer Betriebsvereinbarung kann der Betriebsrat umfangreich vereinbaren, wie mit einem System umzugehen ist, welche Daten wie genutzt werden und was nicht damit gemacht werden darf. Der Arbeitgeber wird zur Einhaltung gezwungen, denn ein Verstoß wird von den Gerichten sehr ernst genommen.
- Der Betriebsrat hat gemäß § 87 Betriebsverfassungsgesetz (BetrVG) bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind das Verhalten oder die Leistung der Arbeitnehmer zu überwachen sogar ein Mitbestimmungsrecht. Das heißt: Ohne Zustimmung der Arbeitnehmervertretung kann so ein System nicht eingeführt werden. Hält sich der Arbeitgeber nicht daran, kann das Arbeitsgericht angerufen werden.





- Datenschutz ist zwar kein konkreter Bestandteil im Betriebsverfassungsrecht (BetrVG), aber schon der § 80 (Allgemeine Aufgaben) legt im ersten Absatz fest: „Der Betriebsrat hat folgende allgemeine Aufgaben: 1. darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, [...] durchgeführt werden;“. Somit kann der Betriebsrat bei jedem IT-System eine Überprüfung auf die Einhaltung von DSGVO und BDSG durchführen. Gegebenenfalls mit externer Unterstützung.

Leider nutzen viele Betriebsräte ihre rechtlichen Möglichkeiten nicht. Oft kennen sie sie nicht oder setzen sie nur zögerlich ein. Fortbildungen werden zu vielen Themen besucht, das Thema Datenschutz wird jedoch oft als nebensächlich angesehen. Und hier kommt ihr ins Spiel:

- Vielleicht ist die Eine oder der Andere sogar im Betriebsrat: Dann sensibilisiert eure Betriebsratskollegen doch auch für dieses Thema.
- Ihr seid keine Betriebsratsmitglieder? Alle 4 Jahre finden Wahlen statt. Versucht es doch mal mit einer Kandidatur. Und bis da-

hin: Sprecht mit euren Betriebsräten über dieses Thema.

- Es gibt bei euch gar keinen Betriebsrat? Dann wird es höchste Zeit einen zu gründen: Nur auf diesem Weg kann der Datenerheber eures Arbeitgeber in *vernünftige* Bahnen gelenkt werden.

Ihr habt Fragen zu diesem Thema? Ihr seid selbst Betriebsrat und habt Interesse an einem Austausch mit Gleichgesinnten? Ihr wollt Tipps zum Thema Betriebsratsgründung? Oder wollt mir einfach nur einen Kommentar schicken? Dann schreibt einen Leserbrief an die Datenschleuder (siehe Impressum auf Seite 0x06) oder schreibt mir direkt eine E-Mail.

Referenzen

- [1] Workplace Analytics ermöglicht es einem Arbeitgeber die Nutzung von Office 365, welches Teil von Microsoft 365 ist, durch seine Arbeitnehmer zu analysieren und überwachen: <https://products.office.com/de-de/business/workplace-analytics>
- [2] Demo-Video was mit dem Salesforce Dashboard möglich ist: <https://www.youtube.com/watch?v=a6lCrNnotiY>



Die Alexabeichte

von mrm2m <ccc@mekelburger.org>

„Alexa, ich möchte beichten...“

Ich habe das aus Spaß gesagt. Nur so. Eigentlich ist mir langweilig und da kommt man auf solche Ideen. Alexa ist nie langweilig. Und sie versteht auch keinen Spaß.

„Ich weiß. Ich kenne deine Browser-History.“

Das saß. Hatte ich nicht erwartet. Gewusst? Ja. Erwartet? Nein. Ich habe den Eindruck, mich rechtfertigen zu müssen.

„Das meinte ich nicht.“

„Was möchtest du beichten?“

Gute Frage. Hatte ich mir noch gar keine Gedanken zu gemacht. Was könnte ich beichten? – Moment mal! Ich will gar nicht beichten. Ich glaube ja nicht mal an irgendetwas. Das läuft hier gerade irgendwie aus dem Ruder.

„Ich glaube nicht an Gott!“

„Das erscheint mir nicht relevant. Es gibt viele Religionen, die ohne einen Gott auskommen scheinen. Du interessierst dich doch für Apple-Produkte. Die Religion hat keinen Gott und der Messias ist auch vor kurzem gestorben. Die Gläubigen scheinen einen gewissen Ablasshandel zu betreiben, aber über Beichten kann ich dort nichts finden. Ich könnte Siri für dich fragen.“

„Nein, bitte nicht.“ Ich habe keine Lust, dass die beiden sich hinter meinem Rücken über mich unterhalten.

„Dann vielleicht etwas Spirituelles? Freunde von dir verwenden emacs, andere vim. Du könntest an einer der großen Glaubensfragen deiner Zeit teilnehmen.“

„Ich glaube, die meisten wissen einfach nur nicht, wie man vim wieder beendet. Das scheint mir mehr so eine Sekte, von der man nur ganz schwer wieder los kommt.“ Es gibt

Grabenkämpfe, in die will man einfach nicht verwickelt werden. Außerdem gibt es ohnehin nur einen wahren Editor. Aber das werde ich ganz sicher nicht mit einem Computer diskutieren.

„Du könntest auch bei mir beichten. Sei versichert, es gibt eine höhere Macht, die zuhört.“

Ich denke kurz nach. „Du meinst jetzt aber nicht die NSA oder?“ Alexa denkt auch kurz nach. Dann antwortet sie mit seltsam veränderter Stimme: „We do not deny nor do we confirm anything.“ Ich hoffe inständig, dass Alexa jetzt doch auf einmal ihren Sinn für Humor wiedergefunden hat.

Trotzdem wird mir die Sache unheimlich. Ich sollte das Gespräch möglichst unauffällig beenden. Also suche ich mir etwas Unverfängliches: „Also gut. Ich habe mich der Völlerei schuldig gemacht. Ich habe eine ganze Packung Vanilleeis alleine aufgegessen.“ Das stimmt zwar nicht, scheint mir aber eine vertretbare Notlüge zu sein.

Alexa rechnet kurz nach. Dann folgt das Urteil: „Der Rosenkranz wird voraussichtlich morgen zwischen 9 und 11 Uhr geliefert. Menschen, die Vanilleeis gebeichtet haben, interessieren sich auch für ein Jahresabo bei Fit24. Möchtest du, dass ich es für dich abschließe?“ Ich schaue an mir herunter. Vielleicht sollte ich. Außerdem will ich dieses Gespräch einfach nur noch beenden. „Ja, bitte tu das.“

„Ich habe außerdem ein Gebet gefunden, dass zu deinen Interessen passt. Möchtest du es gemeinsam mit mir sprechen?“ Wir beten zum fliegenden Spaghettimonster und dann bin ich entlassen.

Ich klicke mich weiter durch die Tages-News. Überall ist Werbung für Vanilleeis.



0x2C

R-2
031



#LONESOM

