die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

HILFE, ICH HABE EINEN CHATBOT GEHEIRATET!

Sommertrends 2023:
Dürre, Waldbrände
& Altrosa sind zurück

Außerdem in dieser Ausgabe:

Verifizierungshaken!
Welche halten wirklich in Altbauwänden?

Verdacht auf NFT:
Die besten Hygiene-Tipps

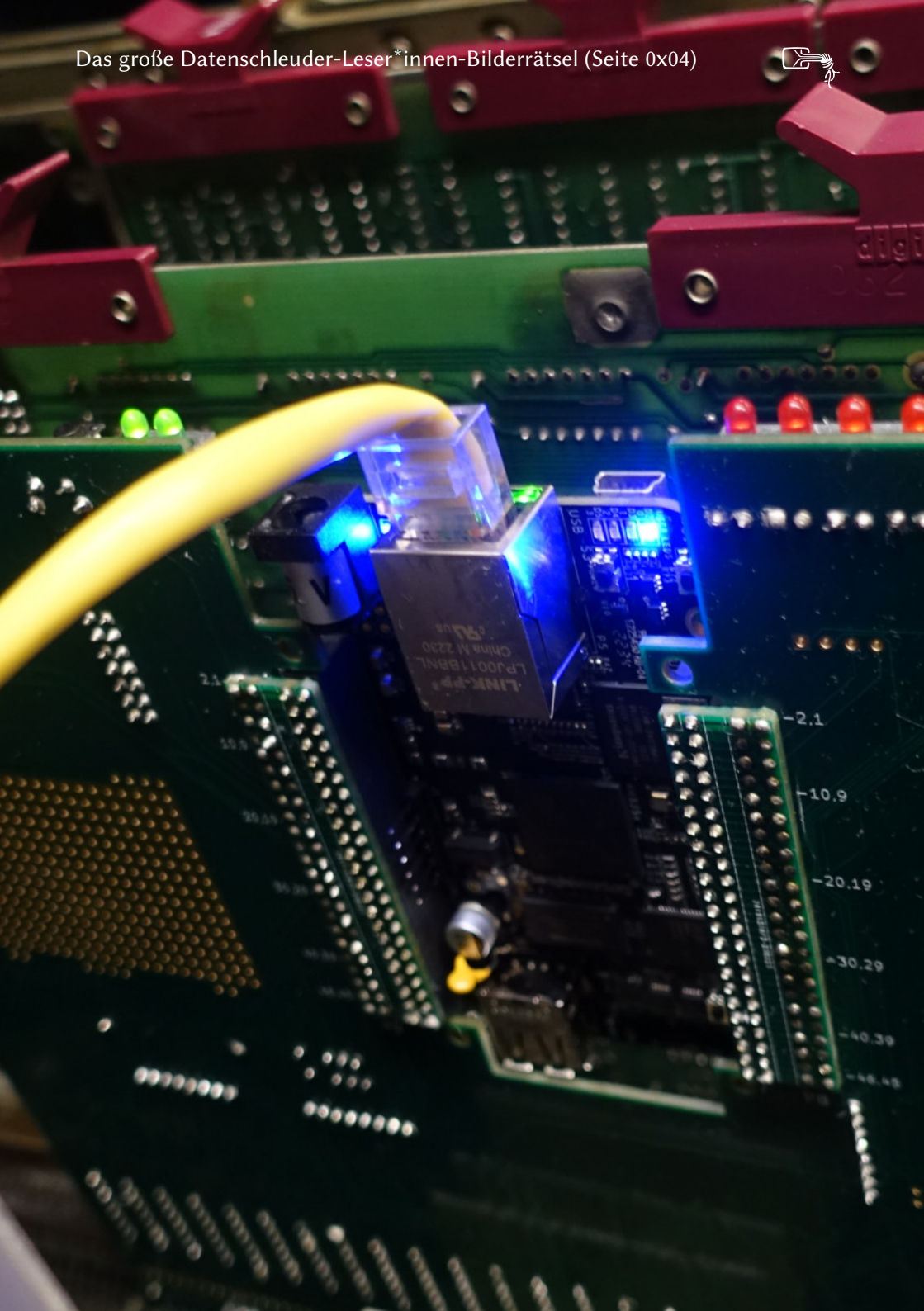


ZIP-DIÄT
12GB in einer Woche

Gratisbeilage: Demokratie-Schnelltest!

ISSN 0930-1054 • 2023
2,6 Kilonewton

#107


2.1
10.9
20.19
30.29
40.39

Geleitwort

Eigentlich sollte die DS107 eine „Safe-Mode“-Ausgabe werden. Die Redaktion sitzt grade an einem anderem Projekt, das viele Kräfte bündelt: Die Hackbibel 3. Allerdings ist doch wieder einiges an Texten zusammengekommen, denn wir lieben unsere Schleuder zu sehr, um nur Halbgares zu verschicken. Außerdem gibt es tatsächlich eine Menge zu erzählen:

Wusstet ihr zum Beispiel, dass die Telekom einfach mal echt lange durch DNS-Hijacking as a Service („Navigationshilfe“) gesammelte Daten an Dritte weitergegeben hat? (Seite 0x0D) Oder dass Tetrafunk nicht ansatzweise so dicht hält wie ein Tetrapak? (Seite 0x2D) Und wenn eins auf seiner IT-Forschungsreise durch Daten-Urwälder einen Bug findet, was macht es dann? (Seite 0x1D) Aber wir wollen euch nicht nur mit Problemen zutexten, sondern auch ein paar Lösungen vorstellen. Aus Dresden erfahren wir, wie gute Rechtskenntnis auch ein demokratisches Mittel gegen Nazi-Demos sein kann, (Seite 0x3F) wie ihr selbst Schöff*in werden könnt, damit die AfD das nicht übernimmt (Seite 0x4B) und dass geteiltes Leid halbes Leid ist, wenn der Passwortmanager umgezogen werden muss. (Seite 0x25)

Und wenn ihr mal so einen langen Fünf-Uhr-Tee der Seele braucht, erzählt euch Cory die Geschichte vom Lebenslauf der Social-Media-Plattformen. Zusätzlich haben wir uns psychologisch für euch ins Zeug gelegt und einen hochprofessionellen Persönlichkeitstest entworfen, (Seite 0x37) und ein Horoskop (Seite 0x59) gibt’s auch nochmal, mit brandneuen Sternzeichen.

Dieses Mal *neu* ein kleiner Kommunikationsversuch: Wir haben Mastodon Hashtags und dazu passende QR-Codes unter jeden Artikel gepackt, unter denen ihr eure Meinungen, Fragen, etc. packen könnt, falls euch Leser*innenbriefe zu analog sind.

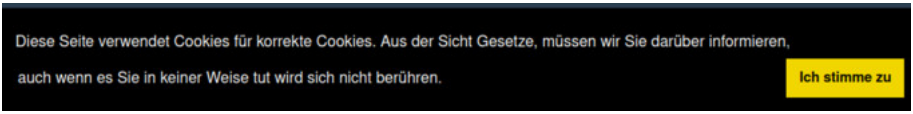
Texte in dieser Ausgabe wurden nicht von Chat-GPT verfasst, sondern organisch gesourced.

Bleibt gesund, eure DS Redaktion (Seite 0x09)

Inhalt

Geleitwort	0x01
Leser*innenbriefe	0x02
Chaos Lokal	0x06
/whois Datenschleuder	0x09
Wie Telekom und Staat unser Vertrauen verspielen	0x0D
It’s not a feature, it’s a bug!	0x1D
Passwortmanager	0x25
Tetra-Funk	0x2D
Sticker-Selbsttest	0x37
Chaos für die Ohren	0x3D
Demos Hacken - Nazis blockieren. Interview mit Anne Herpertz	0x3F
Schöffin werden und sein	0x4B
Tiktoks Vershittifizierung	0x4F

Leser*innenbriefe



Moin!, In Antwort auf das aktuelle Cover: Korrekte Cookies! „Diese Seite verwendet Cookies für korrekte Cookies. Aus der Sicht Gesetze, müssen wir Sie darüber informieren, auch wenn es Sie in keiner Weise tut wird sich nicht berühren. ... [Ich stimme zu]“ Gefunden auf der Login-Page der Cloud-Steuerung einer Steuerung für Heizkessel- und -kreise, vmtl. ausm Tschechischem übersetzt. Hier steht „Thematronic“ dran, der Hersteller, der es benutzt, heißt „Atmos“. https://jbr1.thematronic.cz/de/sign/in/ ps.: Noch zu Seite 2: Ausm Bahn-Stellwerk, wa?

Soweit & besten & war ne schöne Ausgabe,

<wetter>



Tach, müsste Lena – es geht um einen Leserbrief aus Ausgabe 106 – nicht auch noch darauf achten das Handy immer an unterschiedlichen öffentlichen Standorten mit auch verschiedenen Funkzellen zu benutzen. Keinesfalls aber von zu Hause aus verwenden, weil der Standort dann bestimmt werden kann. Chaotische Grüsse aus dem richtigen Süden.

Euer

<Dieter-Josef>



Guten Tag, Ich habe mehrere Fragen bezüglich des Messengers, Signal und Datenschutz. Ich habe bis gestern die Signal App auf meinem Smartphone gehabt. Folgende Situation: Da ich mehrere Anrufe von Unbekannten hatte, habe ich diese Nummer in mein Telefonbuch meines Smartphones aufgenommen, um diese Nummer zu blockieren. Dabei ist mir aufgefallen, dass derjenige Signal auf seinem Smartphone hat.

1. Wird mein Gegenüber per Nachricht von Signal darüber informiert, dass ich ihn in meine Kontaktliste aufgenommen habe?
2. Bekommt der Unbekannte von Signal eine Nachricht, dass ich auch Signal nutze?
3. Wenn der Unbekannte meine Nummer gespeichert hat, bekommt er dann von Signal eine Nachricht, dass er in meine Kontaktliste aufgenommen wurde und er jetzt mit mir kommunizieren kann?
4. Wenn der mir Unbekannte mich nicht gespeichert hat, sondern nur meine Nummer gewählt hat, bekommt der Unbekannte dann auch eine Nachricht, dass er jetzt mit mir kommunizieren kann?

Mit freundlichen Grüßen

<Carsten>

Hi Carsten, ich mache es kurz: https://support.signal.org/hc/en-us/articles/360007061452-Does-Signal-send-my-number-to-my-contacts-

1. nein
2. wenn die Nummer gespeichert ist und Signal Zugriff auf das Adressbuch hat
3. ja

4. nein, die Nummer muss Signal ja irgendwie bekannt sein, also im Adressbuch stehen und Zugriff darauf haben

Im Grunde genau das gleiche wie auf deiner Seite. Du bekommst die Meldung, dass du einen Kontakt auf Signal anschreiben kannst, ja auch nur nachdem du die Nummer in deinem Adressbuch gespeichert hast.

Gruss,
<vollkorn>

Re: Bilderrätsel #106



Drei korrekte Antworten erreichten diesmal die Datenschleuder-Redaktion, vielen Dank an alle, die mitgeraten haben! Wer bei den Leser*innenbriefen aufgepasst hat, hat durch die beiläufige Erwähnung von wetter schon eine Ahnung, wohin das Gerät gehören könnte.

Aber hier kommt die vollständige Auflösung: Es handelt sich um die Zugnummernmeldeanlage mit Eingabekontrollanzeige ZNS 801 EKA.

Zugnummernmeldeanlagen ersetzen bei der Bahn fernmündliche Zugmeldungen. Diese Gespräche mit festem Wortlaut werden zwischen Fahrdienstleiter*innen geführt und in entsprechend dafür vorgesehenen Zugmeldebüchern notiert. Bei der ZNS werden die Zugnummern selbsttätig über Schaltmittel der Signaltechnik mit dem Lauf des Zuges von einem zum nächsten Abschnitt weitergeleitet. Kriterium für diese Fortschaltung ist das Erlöschen des Fahrtbegriffs am Signal. Bei der ZNS 801 EKA erfolgt die Bedienung über eine Eingabekonsole mit 32-stelliger LED-Anzeige und Tastaturblock. Die hier abgebildete Anlage ist an einem elektromechanischen Stellwerk angeschlossen. Das Zugmeldebuch wird ersetzt durch einen Nadeldrucker und die Gleistopographie wird über einen Monitor dargestellt. Bei Störung der Anlage oder betrieblichen Besonderheiten sind die Zugmeldungen wieder mündlich zu geben und nachweispflichtig. Neben verschiedenen Eingabemöglichkeiten kann auch die Dienstübernahme mit der ZNS festgehalten werden. Durch die entsprechende Eingabe druckt der Nadeldrucker ein Feld mit Uhrzeit, auf dem die Arbeitsübergabe und -übernahme durch Unterschrift quittiert werden kann.

Die Antwort von Moritz war besonders stichhaltig, weshalb wir sie hier abdrucken.

Hi! Es handelt sich bei dem abgebildeten Objekt um die Dateneingabetastatur für eine Zugnummernmeldeanlage (vielleicht ZNP 801) – normalerweise also im Bedienraum eines Eisenbahnstellwerks beim Fahrdienstleiterarbeitsplatz zu finden. Links sieht man angeschnitten den Nummernblock (Zehnertastatur) und im Rest des Bildes die Funktionstasten. Die wichtigsten dabei sind die Löschtaste (LÖE – löscht die aktuelle Eingabe), die Anbietetaste (ANB – um einen Zug über seine Zugnummer auf einem Gleis mit Richtungswechsel dem Nachbarfahrdienstleiter anzubieten), die Annahmetaste (ANN – nimmt den angebotenen Zug eines Nachbars an), die Zugnummernspeichertaste (ZNS), die Zugnummernlöschtaste (ZNL – löscht eine Zugnummer von einem Gleisfeld) und die Bahnhofstasten (GD/WS – evtl. Berlin Grunewald und Berlin Wannsee – das Foto müsste dann wegen der Position der Taste aus dem Stellwerk Berlin Wannsee stammen; man erkennt, dass die Beschriftung der beiden Tasten leicht anders aussieht, als die der übrigen Standard-Tasten). Informationen zur Bedienung findet man z.B. im Wiki einer Stellwerksimulation [1].

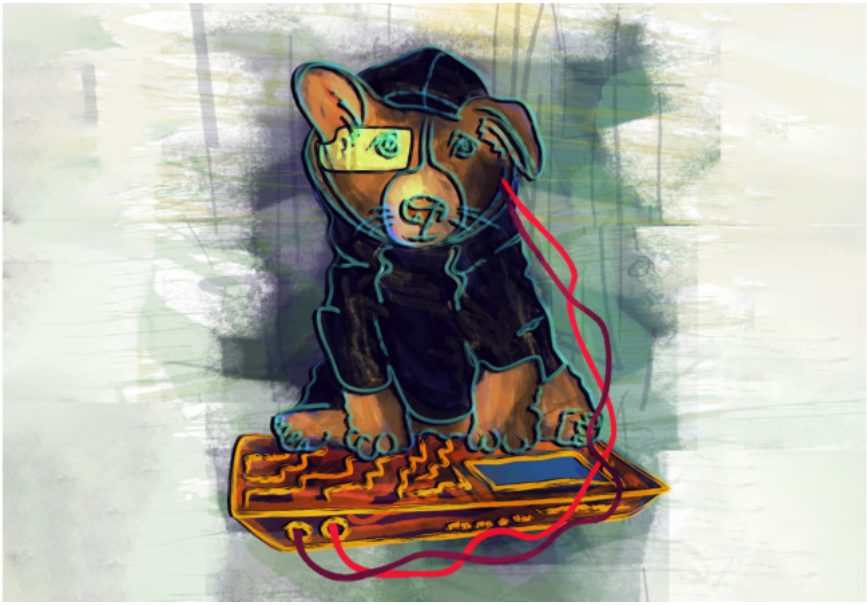
Referenzen

[1] Stellwerksimulation: https://railsignalling.org/signalwiki/index.php/ZNP801_DE

<Moritz>

Bilderrätsel dieser Ausgabe

Die Maschine auf dem Bild kommt aus Zeiten, wo es zwar schon gerade so Internet und Ethernet gab, aber trotzdem wurde dieser Anschluss erst viele Jahre später nachgerüstet. Eine Idee, was das sein könnte? Schreibe uns deine Vermutung an <ds@ccc.de>.




Flensburg
Lübeck
Hamburg
Bremen
Hannover
Berlin
Paderborn
Essen
Düsseldorf
Dortmund
Göttingen
Kassel
Leipzig
Köln
Dresden
Aachen
Siegen
Fulda
Wiesbaden
Frankfurt
Bamberg
Würzburg
Darmstadt
Erlangen
Mannheim
Kaiserslautern
Karlsruhe
Stuttgart
Ulm
Wien
Freiburg
München
Salzburg
Basel
Zürich

Erfahrungsaustauschkreise

Aachen :: CCCAC :: Chaos Computer Club Aachen e. V. https://aachen.ccc.de/
Fr 20 Uhr :: Schützenstraße 11, 52062 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 :: https://meeten.statt-drosseln.de/b/inj-2ec-4na, Zweigstraße 1, 28217 Bremen

Darmstadt :: Chaos Computer Club Darmstadt e. V. https://www.chaos-darmstadt.de/
Di 19 Uhr u. Fr 18 Uhr :: W17, 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 ab 18 Uhr :: Chaosdorf, Sonnenstraße 58, 40227 Düsseldorf

Erlangen :: Bits'n'Bugs e. V. https://erlangen.ccc.de/
Fr 18:00 Uhr :: ZAM Erlangen, Hauptstraße 65-67, 91054 Erlangen

Essen :: Chaospott :: foobar e. V. https://chaospott.de/
Mi 19 Uhr u. So 16 Uhr :: foobar, Sibyllastraße 9, 45136 Essen

Flensburg :: Chaostreff Flensburg https://chaostreff-flensburg.de/
Di 18 Uhr :: Apenrader Straße 49, 24939 Flensburg

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://cccfr.de/
Mo u. Di 19 Uhr :: Hackspace, Adlerstraße 12 a, 79098 Freiburg im Breisgau

Fulda :: mag.lab :: Magrathea Laboratoratories e. V. https://maglab.space/
Fr 19 Uhr :: Buttlarstraße 1 a, 36039 Fulda

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/
zweiter Fr & letzter Di, 19:42 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
Leipzig :: dezentrale :: dezentrale e. V.	https://dezentrale.space
	Fr 19 Uhr :: Hackspace dezentrale, Dreilindenstraße 19, 04177 Leipzig
Lübeck :: nbsp :: Chaotikum e. V.	https://chaotikum.org/
	Mi 19 Uhr :: Fackenburger Allee 11, 23554 Lübeck
Mannheim :: C3MA :: Chaos Computer Club Mannheim e. V.	https://www.ccc-mannheim.de/
	Fr 19 Uhr :: Neckarauer Straße 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 :: CCC Salzburg :: Chaostreff Salzburg	https://cccsbg.at
	Fr 18 Uhr :: Ulrike-Gschwandtner-Straße 5, 5020 Salzburg
Siegen :: Chaos Siegen, 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://www.cccs.de/
	1. Di 18 Uhr (Online), 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 :: Neue Hard 12, 8005 Zürich

Es gibt in den folgenden Städten Chaostreffs: Aalen, Alzey, Amberg, Amsterdam, Andernach, Aschaffenburg, Augsburg, Backnang, Bayreuth, Bern, Bielefeld, Bochum, Bonn, Budapest, Chemnitz, Coburg, Cottbus, Erfurt, Gießen, Graz, Göppingen, Halle (Saale), Heidelberg, Heilbronn, Hildesheim, Hildesheim, Hilpoltstein, Hoher Fläming, Ingolstadt, Innsbruck, Itzehoe, Jena, Kiel, Klaus, Konstanz, Landau, Ludwigsburg, Luxemburg, Lörrach, Marburg, Münster, Neuss, Nürnberg, Offenburg, Osnabrück, Potsdam, Ransbach-Baumbach, Rapperswil-Jona, Recklinghausen, Regensburg

Nichts in Deiner Gegend gefunden? Schau' mal bei den Aliens vorbei: https://aliens.ccc.de/

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


die datenschleuder.
das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club
Chaos Cookie Consent
Wir nutzen CCCekse in unserem Heft. Einige von ihnen sind essenzielle Grundnahrungsmittel, während andere uns helfen, diese Publikation und dein Erlebnis zu verbessern.
Essenziell
Statistiken
Externe Medien
Alle akzeptieren
Speichern & schließen
Nur essenzielle CCCekse konsumieren
Individuelle CCCeks-Konfiguration
#106


die datenschleuder.
das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club
BORED CHAOS SCHLAUCHBOOT CLUB
#105

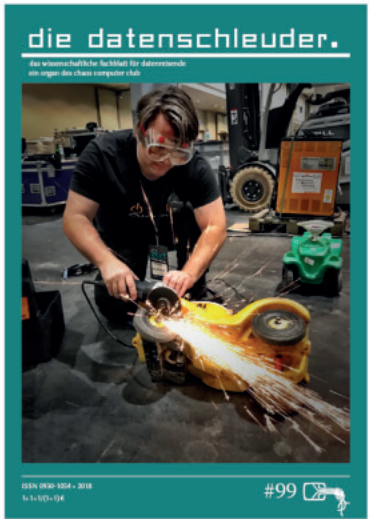

die datenschleuder.
das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club
#104


die datenschleuder.
das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club
#103


die datenschleuder.
das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club
#102


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
#101


die datenschleuder.
das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club
#100


die datenschleuder.
das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club
#99


die datenschleuder.
das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club
leicht defekt
#98

/whois Datenschleuder

von der Datenschleuder-Redaktion <ds@ccc.de>

Dies ist der erste Beitrag einer Nabelschau in mehreren Teilen. Wir beleuchten alles rund um die Datenschleuder. Erst mal erzählen wir wer denn eigentlich hinter den ganzen wohlklingenden Namen im Impressum steckt. In weiteren Folgen rollen wir die Historie dieser ehrwürdigen Publikation für ein paar Meter auf, berichten von ihrer Wiederbelebung in den Nullerjahren und beschreiben unsere Arbeitsweise als Redaktion.

Die Datenschleuder wird von einer bunt gemischten Gruppe Chaos erstellt. Schätzungen ergaben, dass die meisten Mitglieder dieser Gruppe Menschen sind. Um das etwas genauer zu bestimmen haben wir ein paar unprofessionelle, hausinterne Umfragen durchgeführt, deren Ergebnisse wir hier möglichst durchschnittlich wiedergeben.

Offensichtlich sind wir derzeit 10 Redakteur*innen, die auf Umfragen antworten. Davon werden 5 (meist) weiblich gelesen und 3,9 männlich. Die restlichen 1,1 passen nicht in eine binäre Schublade. Dabei sind wir 31 bis 49 Jahre alt und wohnen in einem Ort mit 1.454.200 +/- ein paar Millionen Menschen. Die Mitglieder der Schleuder-Gang haben genau 2,85 Fahrräder im Haushalt, aber nur 0,7 Kinder, Tiere, Pflanzen. Manche nichts davon. Alternativ einen Rasenmäherroboter mit anthropomorphisierenden Augen.

Beruflich lesen, denken, schreiben, lehren, repeaten, lernen wir. Wir machen irgendwas mit Medien oder Flugzeugen und organisieren die Automatisierung von Softwaretests. Wir stellen Leuten Fragen, die sie ungern ehrlich beantworten. Und helfen ihnen Fehler zu korrigieren. Wir sind Research Software Engineers, IT-Security-Analysten, System Engineer Security und testen Webseiten und Android-Apps auf Sicherheitslücken. Dabei lernen wir hauptsächlich wie Prozesse von Großkonzernen funktionieren. Wir beantragen Nutzer*innen-Accounts, übersetzen „Digitales“ zu „Soziale Arbeit“ oder sind Fachreferentin für digitale Jugendarbeit. Bunter Lebenslauf.

Wir sind natürlich auch Nerds und Chaot*innen. Prozentual nutzt das Redaktionswesen zu 84 % Linux in zum Beispiel den Flavors Arch, Alpine und Ubuntu, zu 40 % MacOS und zu 50 % Windows, außerdem noch BSD und „sonstiges“. 30 % von uns sind Erfas organisiert, 40 % sind Aliens und 15 % sind bei den Haecksen aktiv, manche sind Hitchhikers.

In unserer Freizeit beschäftigen wir uns mit Stickern, Sprachen, Archivieren, Pen-&-Paper-Rollenspielen, cyber4edu oder klassisch-sexistischem Ballroom Dancing. Wir schreiben Bücher, gestalten Aktivitäten einer evangelischen Gemeinde oder schauen Make-Up-Tutorials und färben uns die Haare. Wir sind Tenor, fahren Boot und/oder Fahrrad, boxen, basteln, tüfteln, knobeln, löten, bauen Gemüse an und hören Musik. Und zwar türkischen Pop, deutschen Rap, harten Techno, Meditationsmusik, The Prodigy, KMFDM, Machine Girl und Trentemøller, Alternative Rock, Hip-Hop, bisschen Punk, Acappella, Jazz, Tropical House, Experimentelles, Funk, Swing, deutsche Singer-Songwriter, OldSchool Rock, Pop oder Chiptunes.

Das sind wir also in allen unseren Extremen. Was uns alle auf jeden Fall eint ist natürlich die Datenschleuder. Da es die Datenschleuder schon seit 1984 gibt, ist es nicht verwun-

derlich, dass niemand vom Gründungsteam heute noch dabei ist. Die aktuellen Mitglieder sind zu unterschiedlichsten Gelegenheiten dazugekommen: Bei Treffen auf dem EasterHegg 2017 (vor 108 Monaten) und anderen Chaos-Events bis zum letzten EasterHegg in Hamburg (vor 8 Monaten), wo sie sich reingesetzt hatten ohne zu realisieren, dass sie von so einem Treffen nicht ohne Aufgabe weggehen werden. Andere sind durch Aufrufe per Mail dazugekommen, wieder andere wurden durch Freund*innen angeworben. (Und das ohne Werbeprämie!)

Pro Ausgabe arbeiten wir durchschnittlich an 2 bis 10 Issues. Ein Issue kann dabei eine Idee, ein eingereichter Text oder auch das Bilderrätsel sein. Die Datenschleuder wird in in LaTeX gebacken und in Git eingecheckt. Das ist, auch innerhalb der Redaktion, Geschmackssache. Unsere LaTeX- und Git-Skill-Level schwanken zwischen Laie und Vollprofi. Durch die Redaktionsarbeit haben wir uns durchschnittlich nicht unerheblich verbessert. Wir sind dabei LaTeX mehr oder weniger zugeneigt. Wir mögen LaTeX und dafür nicht so das Texten, oder wir mögen beides oder keines davon. Dafür schmeißen wir uns in neue Themen und purzeln den Kaninchenbau herunter, und das manchmal glatt an Deadlines vorbei. Wir doodlen gern Bilder, freuen uns, wenn die Commits ohne Fehlermeldung durchgehen, wir reviewen Entwürfe. Was uns nervt ist Einreicher*innen oder Redakteur*innen hinterherzulaufen. Wir organisieren und bebunten und recherchieren.

In der Datenschleuder gefallen uns am besten Artikel mit Themen, über die wir noch wenig wissen. Wir lesen gerne zu Technik im Kontext von Kultur- und Gesellschaftsthemen. Spaß machen uns auch Bastelartikel, Artikel von echten Hacks oder politische Themen wie die Chatkontrolle. Wir mögen Texte, bei denen wir das Gefühl haben alles ohne Anstrengung zu verstehen und dennoch etwas Neues zu lernen. Als Redaktion des Clubmagazins nehmen wir die Gestaltung der Datenschleuder sehr ernst. Wir wollen keine reine Druckmaschine, sondern Wissensspeicher, Archiv, aber auch Dokumentation aktueller Themen sein. Wir sehen uns als eine kleine Schnittstelle des Wissenstransfers. Nicht nur, aber hauptsächlich innerhalb des CCC.

Während unserer Arbeit haben wir festgestellt, dass wir, obwohl wir so unterschiedliche Biografien haben, ganz ähnliche intrinsische Motivatoren haben: Wir möchten mit guten Leuten gute Dinge tun und als Teil des Chaos aktiv sein.

Beim nächsten Mal dann mehr zu unserem Vorgehen.





DIY COOKIE HOWTO

1. Zucker in eine große Schüssel, Öl, Wasser und Vanille dazu rühren.

2. Mehl, Backpulver, Natron, Salz, Schokotropfen in der zweite, noch größere Schüssel verrühren, dann den ersten Mix dazugeben, bis sich alles homogen gemischt hat.

3. Schüssel abdecken und 12 Stunden im Kühlschrank chillen lassen.

4. Backofen auf 180°C vorheizen und ne Menge Backbleche mit Backpapier auslegen.

5. Mit einem Esslöffel Teig portionieren und auf dem Backblech verteilen.

6. Kekse ca. 15 min backen, bis die Ränder goldbraun sind und wenn ihr es aushaltet, ca. 15 min abkühlen lassen.

7. Vom Blech nehmen und luftdicht verpacken, halten sie mindestens 7 Tage frisch.

Reicht für 100 Kekse

Zutaten
1,2 kg Zucker
580 g Öl
380 ml Wasser
6 TL Vanilleextrakt
1.4kg Mehl
5 TL Backpulver
3 TL Natron
1 TL Salz
550 g dunkle Schokotropfen

Zubehör
2 große Schüsseln
Esslöffel
Backofen
Backbleche
Backpapier
Platz im Kühlschrank





Wie Telekom und Staat unser Vertrauen verspielen

von ElooKoN <ccc@elookon.de>

14 Jahre nach Einführung der „T-Online Navigationshilfe“, die Telekom-Kunden bei fehlerhaften DNS-Anfragen zu sehen bekamen, und fast vier Jahre nach Einleitung rechtlicher Schritte, endet ein Verfahren mit einem enttäuschendem Ergebnis. Wir betrachten – nach technischer Einordnung – die Historie und die (Nicht-)Folgen dieser manipulativen und letztlich völlig ungestraften Dreistigkeit.

Der Artikel ist ursprünglich schon im Mai 2019 auf meiner Webseite unter leicht anderem Titel erschienen. [1] Dort stelle ich auch die vollständigen Schreiben der Behörden im Original zur Verfügung. Der folgende Artikel ist aktueller und arbeitet die Vorgänge über einen Zeitraum von fast vier Jahren chronologisch ab.

Vorwort

Erst einmal zum Anfang der Geschichte: Es geht um den Eingriff der Deutschen Telekom in den DNS-Traffic ihrer Kunden, der dazu dienen sollte, mehr Traffic auf eigene Webseiten umzuleiten.

Solche Manipulationen am DNS sind nicht neu. Schon im Jahre 2009 berichtete *heise online* über die Einrichtung einer mit „T-Online Navigationshilfe“ betitelten Webseite durch die Deutsche Telekom. [2] Kunden des Internetdienstanbieters wurden dorthin weitergeleitet, etwa, wenn sie sich beim Eintippen von Internetadressen in den Webbrowser vertippten oder der Nameserver der angesteuerten Webseite nicht ordnungsgemäß konfiguriert war. Auch ein Jahr später wurde das Thema erneut vom Heise-Magazin aufgegriffen [3], doch danach wurde es still. Es wurde so still, dass ich – der auch nicht mehr daran dachte – es nicht für möglich gehalten hatte, dass die Deutsche Telekom ihren Kunden bis vor einiger Zeit (Ende April 2019) immer noch manipulierte DNS-Resolver zur Verfügung stellte. Allein das ist schon ziemlich absurd – ob im Jahre 2009, 2019 oder 2023. Doch wie sich herausstellen sollte, wurden durch diese Manipulationen Daten – indirekt – aus dem Netz der Deutschen Telekom an Dritte weitergereicht. Diese Dritten standen dabei in keinerlei Verbindung mit den Kunden der Deutschen Telekom. Bei den Daten handelt es sich in erster Linie um die IP-Adressen der Kunden, weiterhin aber auch andere Daten, zum Beispiel solche, die ein Webbrowser bei unverschlüsselten Verbindungen standardmäßig überträgt. Das vorbeugende Prinzip *HTTPS-First* wurde in Google Chrome erst 2021 realisiert.

Überblick: Wer technisch Bescheid weiß, kann direkt mit dem Abschnitt „Netzwerkverkehr“ beginnen. Ab dem Abschnitt „Strafanzeige (§§ 206, 303a StGB)“ geht es um die Strafanzeige und das vonseiten der Bundesnetzagentur geführte Verfahren.

Vertrauen

Um das Problem zu verstehen, muss man sich zunächst klarmachen, dass der technische Stand vieler Bereiche des heutigen Internets nach wie vor dem der Pionierzeit ent-

spricht. Grundlegende Prinzipien basierten damals alleine auf Vertrauen und wurden bis heute nicht wesentlich verändert. Nicht erst DNS-Server können von denjenigen anstrengungslos manipuliert werden, die sie bereitstellen, sondern ganze IP-Adressbereiche (Subnetze) und der damit verbundene Netzwerkverkehr kann zum Teil erschreckend einfach von Dritten vereinnahmt werden. Dieses sogenannte „BGP-Hijacking“ kommt immer wieder vor, unabsichtlich und absichtlich. [4, 5]

BGP Das „Border Gateway Protocol“ ermittelt mögliche Routen zu dem Ziel eines Datenpakets, um es möglichst effizient ans Ziel leiten zu können.



Ich mache mich mal mit dem Problem vertraut.

In vielerlei Hinsicht muss auch noch heute darauf vertraut werden, dass Charlie nicht eingreift, wenn Alice mit Bob kommuniziert. Dies gilt insbesondere dann, wenn Charlie bloß Übermittler der Nachricht ist. Charlie soll die Nachricht gemäß seiner zugewiesenen Aufgabe und Verantwortung also nicht verändern oder unterdrücken. Aus dieser Verpflichtung folgt zugleich das Providerprivileg, das den Übermittler vor rechtlichen Angriffen schützen soll, indem man ihn für Inhalte oder Handlungen der Kommunikationsteilnehmer rechtlich nicht mitverantwortlich macht. Dass dieses stillschweigend anerkannte und nur teils gesetzlich kodifizierte Prinzip in letzter Konsequenz vor Gericht mitunter nicht immer standhält, zeigt ein vor wenigen Wochen ergangene Urteil des LG Leipzig.

Providerprivileg
Dass man für fremde Handlungen im Grundsatz zivilrechtlich nicht so ohne Weiteres einzustehen hat, schließt eine Haftung als sogenannter Mitstörer nicht aus; daraus resultieren wiederum Mitwirkungs- und Sorgfaltspflichten. Um zu verhindern, dass im Umkehrschluss leichtfertig in die besondere Vertrauensstellung eines Diensteanbieters eingegriffen wird, indem dieser zum Beispiel zur Überwachung seiner Nutzer gedrängt wird, um eine eigene Haftung zu vermeiden, muss seine Stellung durch gesonderte Gesetze geschützt werden. Für Telemediendienste findet sich das Providerprivileg in §§ 7, 10 TMG.

Der Betreiber des öffentlichen DNS-Resolvers Quad9 (eine Zürcher Stiftung) wurde dazu verurteilt, seine Auskünfte zu manipulieren, beziehungsweise es zu unterlassen, zwei bestimmte Domainnamen aufzulösen. Die Begründung des Gerichts: Quad9 spiele eine zentrale Rolle bei der Urheberrechtsverletzung [6]; Gegenstand des vonseiten Sony Music Entertainment angestoßenen Verfahrens waren wohl zwei Domainnamen, unter denen rechtsverletzendes Material abrufbar war oder auf das dort bewusst verlinkt wurde. Ob das Urteil in den Rechtsmittelinstanzen bestehen wird, ist angesichts dieser grenzüberschreitenden Interpretation der – an sich als unstrittig anerkannten – Mitstörerhaftung fraglich.

Grenzüberschreitend ist das Urteil deshalb, weil Quad9 als Betreiber eines öffentlichen DNS-Resolvers kein Internetzugangsanbieter ist. Der BGH hatte zwar im Oktober 2022 bestätigt, dass eine Sperrung von Einträgen auf DNS-Servern als Ultima Ratio in Betracht kommt [7], doch dort betraf es eben einen solchen Internetzugangsanbieter (zufälligerweise die Deutsche Telekom). Es spricht viel dafür, den für *eigene* Kunden bereitgestellten DNS-Resolver und den Internetzugang als eine Einheit zu sehen; dass die Sperrung mithilfe des DNS-Servers umgesetzt wird, kann dann dahinstehen. Überträgt man diese Rechtsprechung allerdings auch auf Betreiber von freien DNS-Resolvern, die nichts anderes tun, als technische Informationen weiterzuleiten, erschließt sich nicht, warum man dann nicht auch etwa die unter anderem für die Vergabe von IP-Adressbereichen in Mitteleuropa zuständige RIPE NCC dazu verpflichten könnte, urheberrechtlich veranlasste Sperren durch den Entzug der entsprechenden Bereiche zu realisieren. Absurd, wenn man weiß, was das eigentlich bedeutete.



Serviervorschlag: Telekom-DNS-Revolver

Vorbei ist der Fall wahrscheinlich noch lange nicht. Quad9 hat Berufung vor dem OLG Dresden angekündigt. Wird eine Revision zugelassen oder angenommen, landet sie auch noch beim Bundesgerichtshof. Weil es sich hierbei um eine das EU-Sekundärrecht betreffende Frage handelt, ist eine Vorlage an den Europäischen Gerichtshof auch nicht gerade unwahrscheinlich. Am Ende steht dann die Erkenntnis, dass bisher als Selbstverständlichkeit geltende Grundsätze auch in Mitte der 2020er-Jahre einer langjährigen richterlichen Klärung durch etliche Instanzen bedürfen.

Revision
Anders als im Strafrecht kann in Zivilprozessen nicht so ohne Weiteres Revision eingelegt werden, sondern die Revision muss erst durch das Berufungsgericht selbst zugelassen werden, zum Beispiel wenn die Rechtssache – wie hier – grundsätzliche Bedeutung hat. Eine zu Unrecht unterbliebene Zulassung kann mit der Nichtzulassungsbeschwerde angegriffen werden (§§ 543, 544 ZPO).

Domain Name System (DNS)

DNS-Server beziehungsweise Nameserver dienen unter anderem dazu, Domainnamen mithilfe einer Datenbank in IP-Adressen zu übersetzen, im Falle des Reverse-DNS in umgekehrter Reihenfolge. Eine eindeutige Verknüpfung von Domainname und IP-Adresse (der A- beziehungsweise AAAA-Record im Falle von IPv6) in einer solchen Datenbank kann zum Beispiel so aussehen:

```
www.ccc.de.  3600  IN  A  169.254.53.23
```

Bei den DNS-Servern, welche die Deutsche Telekom ihren Kunden zur Verfügung stellt, handelt es sich um nichtöffentliche, rekursive

DNS-Resolver. Rekursiv heißt, dass der DNS-Server die Daten wiederum von einem anderen Nameserver holt. Sie sind nicht – wie zum Beispiel der erwähnte Resolver von Quad9 oder der wohl noch bekanntere Google Public DNS (weitläufig bekannt unter den IPv4-Adressen 8.8.8.8 und 8.8.4.4.) – für jedermann nutzbar, sondern nur für Teilnehmer aus dem Telekom-Netz, also für die eigenen Kunden. Davon abgesehen unterscheiden sie sich nicht, denn weil es sich um DNS-Resolver handelt, enthalten nicht *sie* die eigentlichen Datenbankeinträge (außer im Zwischenspeicher), sondern sie fragen diese ihrerseits nur von anderen – den autoritativen – DNS-Servern ab.



Hallo Datenbank? Ich morse F5 wie fürs Camp Ticket.

DNS-Resolver funktionieren nach folgendem Prinzip:

Schritt 1 Versucht ein Nutzer Daten von einem Server abzurufen und verwendet er dabei nicht die IP-Adresse (wie `169.254.53.23`), sondern den damit verknüpften Domainnamen (zum Beispiel `ccc.de`), wie das in aller Regel der Fall ist wenn man im Internet surft, wird zunächst der DNS-Resolver kontaktiert, der im Router oder Betriebssystem des Nutzers hinterlegt wurde.

Schritt 2 Dieser DNS-Resolver kontaktiert daraufhin einen Root-DNS-Server, woraufhin er die Informationen zu den Nameservern zurück erhält, welche für die Domainendung (Top Level Domain TLD) wie `de` zuständig sind.

Schritt 3 Von diesen Nameservern erhält der DNS-Resolver dann wiederum die Informationen zu den autoritativen Nameservern, die für die eigentliche Domain (Second Level Domain SLD) zuständig sind, also `ccc` im vorliegenden Beispiel (`ccc` = SLD, `de` = TLD).

Schritt 4 Der DNS-Resolver kontaktiert anschließend auch diesen Nameserver. Von diesem erhält er die IP-Adresse, die mit dem Domainnamen verknüpft ist. Findet er keinen entsprechenden Datensatz oder ist er für den Domainnamen nicht zuständig, liefert er den Status `NXDOMAIN` beziehungsweise `REFUSED` zurück.

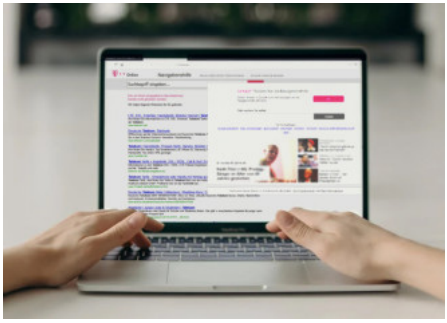
Schritt 5 Schlussendlich leitet der DNS-Resolver den Status beziehungsweise die IP-Adresse, normalerweise unverändert, an das System des Nutzers weiter. In der Folge wird versucht, eine Verbindung zum hinter der IP-Adresse liegenden Server herzustellen.

Normale DNS-Resolver

Tippt ein Nutzer einen nicht existenten oder ungültigen Domainnamen wie `ccc.dee` (ein 'e' am Ende zu viel) in seinen Webbrowser ein, oder gibt es auf Seiten des für die Webseite zuständigen autoritativen Nameservers technische Probleme, erhält er auf einem ordnungsgemäß funktionierenden System normalerweise eine Fehlermeldung des

Webbrowsers. In Google Chrome (Version 110) lautet sie wie folgt:

> ***Die Website ist nicht erreichbar***
>
> *Prüfe, ob „ccc.dee“ einen Tippfehler enthält. Wenn die URL keinen Tippfehler enthält, kannst du die Windows-Netzwerkdiagnose durchführen.*
>
> *DNS_PROBE_FINISHED_NXDOMAIN*



Wie kommen die Löcher in den Käse und der Mist in den Browser?

DNS-Resolver der Deutschen Telekom

Nicht so bei Kunden der Telekom. Diese wurden 2019 noch auf eine sogenannte Navigationshilfeseite weitergeleitet [8], die dem Nutzer natürlich nicht half, sondern stattdessen hausgemachte Werbung präsentierte:

> *t-online.de Navigationshilfe*
> *Besser surfen mit dem Telekom Browser*
> *[…]*
> *Die von Ihnen eingegebene Internetadresse konnte nicht gefunden werden. Wir haben folgende Webseiten für Sie gefunden.*
> *LTE, DSL, Entertain, Handytarife, Mobiles Internet | Telekom*
>
> *Hier finden Sie Informationen zu LTE, DSL, Entertain, Telekom Tarifen, Handytarifen und zu vielen Aktionsangeboten der Telekom.*
> *www.telekom.de/*
> *[…]*

Weiterleitung durch DNS-Hijacking

Zunächst sei dem Ganzen vorangestellt, dass die DNS-Resolver der Deutschen Telekom ganz automatisch vom System des Kunden verwendet werden, wenn er in seinem Router oder Betriebssystem nicht explizit andere auswählt. Das ist ein normales und gewünschtes Verhalten, denn irgendeinen DNS-Resolver muss der Kunde eingestellt haben. Zumindest, bis er einen besseren findet – was dringend anzuraten ist.

Die Weiterleitung wurde realisiert, indem im Falle der Nichtauffindbarkeit der vom Nutzer eingegebenen Internetadresse abweichende, d. h. schlichtweg gefälschte Daten an den Nutzer übermittelt wurden, anstatt korrekterweise den Fehlerstatus im Browser zurückzuliefern. Es wurden fremde, mit der eigentlichen Domain nicht in Verbindung stehende IPv4-Adressen übermittelt.

Diese Praktik nennt sich DNS-Hijacking, hier in Form eines klassischen Man-in-the-Middle-Angriffs. Verifizieren ließ sich diese Tatsache später in Raspbian (GNU/Linux) recht einfach mit einem Befehl aus dem Paket `dnsutils`. Im nachfolgenden Beispiel wurde die IPv4-Adresse des gültigen, aber nicht existenten Domainnamens `wwww.bfdi.bund.de` (ein „w“ am Anfang zu viel) abgefragt. Und obwohl diese Subdomain nicht existiert, antwortete der DNS-Resolver mit einem `NOERROR`

und zwei IPv4-Adressen – so, als wäre alles in bester Ordnung:

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
   ↪ id: 23877
[...]
;; ANSWER SECTION
wwww.bfdi.bund.de. 3600 IN A 62.138.238.45
wwww.bfdi.bund.de. 3600 IN A 62.138.239.45
```



WTF Telekom-in-the-middle-attack!!

Bei der Domain `bfdi.bund.de` handelt es sich um die Website des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Wir sprechen also von der Website einer Bundesbehörde. Ob die Subdomain mit den vier anstatt den gängigen drei 'w' nun existiert oder nicht – sie gehört eindeutig zur Domain `bfdi.bund.de`, was bedeutet, dass eigentlich niemand anders als der für diese Domain zuständige autoritative Nameserver Subdomains besetzen oder nicht besetzen kann.

Netzwerkverkehr

Technologie aus der Pionierzeit wie das DNS-Protokoll muss mangels Authentifizierung davon ausgehen, dass die Informationen stimmen, also nicht manipuliert wurden. Sprechen wir von unverschlüsselten Verbindungen – und allzu lange ist es nun nicht her, als jede Website völlig ohne oder zumindest *auch* ohne TLS erreichbar war. Jeder Webbrowser leitete den Nutzer daher ohne Weiteres auf den Server weiter, der sich hinter der vom DNS-Server zurückgelieferten IP-Adresse verbarg. Ein unredlicher Internetzugangsanbieter musste nicht mehr tun, als lediglich einen falschen Status und eine falsche IP-Adresse zurückzugeben, um sich selbst Reichweite durch die Weiterleitung auf eine Werbeseite zu verschaffen.

TLS „Transport Layer Security“ ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.

Verschlüsseltes DNS
Erst seit wenigen Jahren setzt sich zunehmend verschlüsseltes DNS durch, weil immer mehr öffentliche DNS-Resolver *DNS over TLS* (DoT) anbieten. Darunter Google, Quad9, Cloudflare und nicht zuletzt auch der im Weiteren erwähnte Verein Digitalcourage e. V.

GET Eine Methode bestimmte Ressourcen eines Servers anzufragen, wie zum Beispiel Ergebnisse für einen Suchbegriff: https://www.ccc.de/de/search?search_term=dns

Solange der Nutzer die Internetadresse nur mit einem `http://` davor aufrief, wurden unter anderem folgende Daten an den fremden Server übermittelt:

- Die gesamte URL, also Domainname, Pfad und GET-Parameter, zum Beispiel:

```
http://www.ccc.de/account/
   ↪ payments?sid=02c60f88db03
```

- Im Falle einer wie auch immer initiierten Absendung eines Formulars auch dessen Daten (POST-Daten). Das können im schlimmsten Falle Zahlungsinformationen oder Passwörter in Klartext sein.
- Name und Inhalt von Cookies, zum Beispiel Session-Cookies mit Authentifizierungsinformationen, es sei denn, diese wurden zuvor vom Betreiber der (echten) Website mit dem Header-Flag `secure` ausgestattet. [9, 10]

Dieses standardmäßige Browserverhalten ließ sich nicht nur über die Entwicklerkonsole von Google Chrome (F12-Taste) belegen, sondern auch, wenn man den Netzwerkverkehr direkt analysierte. Obwohl es sich eigentlich um die falsche Ziel-IP-Adresse handelte, wurden die Daten wie beschrieben übertragen, wie eine Wireshark-Analyse belegte:

```
Hypertext Transfer Protocol
   POST /geheimer-pfad/?daten=sehr\_geheim
      ↪ HTTP/1.1\r\n
   [...]
   Cookie: unsicheres\_cookie=Geheimer
      ↪ Inhalt.\r\n
   [...]
HTML Form URL Encoded:
   ↪ application/x-www-form-urlencoded
   Form item: "passwort" = "qwertz"
```

Eine Übertragung fand nur dann nicht statt, wenn der Benutzer eine TLS-geschützte Internetadresse (also mit einem `https://` davor) aufrief. Dies lag daran, dass die Navigationshilfeseite standardmäßig keinen Netzwerkverkehr auf Port 443, sondern nur auf Port 80 durchließ, die Verbindung also schon vor der eigentlichen Datenübertragung vom Webbrowser abgebrochen wurde.

Übertragen wurde jedoch auch hier die IP-Adresse des Kunden. Wäre (sinnloserweise) auch der Port für verschlüsselte Verbindungen abgehört worden, wäre immerhin der abgefragte Domainname, also `www.ccc.de` übermittelt worden, denn diese Information gehört aus technischen Gründen noch zum Teil der unverschlüsselten Vorinformationen, bevor die gesicherte TLS-Verbindung gestartet werden kann.



Warum willst du meine IP?

Natürlich bedeuten diese Ergebnisse nicht, dass die Daten auch gespeichert wurden. Sie bedeuten aber auch nicht, dass diese Daten nicht gespeichert wurden. Tatsächlich weiß kein Mensch, ob oder welche Daten wie lange wo gespeichert wurden und ob und inwieweit diese in welchem Ausmaß für welche Zwecke verarbeitet wurden – man weiß allerdings nun, dass sie zumindest übertragen wurden.

Wireshark Eine freie Software zur Analyse von Datenprotokollen

Port 443 Standard-Port für HTTPS (verschlüsselte Verbindungen)

Port 80 Standard-Port für HTTP (unverschlüsselte Verbindungen)



Wie bitte? Ströer Media hat meinen Verkehr gekapert?!

Übermittlung an Dritte

Der nächste Schritt lag nun darin herauszufinden, wer sich hinter der ominösen Navigationshilfeseite eigentlich verbarg. Es sollte keine Überraschung sein, dass die mit T-Online überschriebene Website ausweislich ihres Impressums gar nichts (mehr) mit der Telekom zu tun hatte. [11] Und tatsächlich hat sie das Webportal im Jahre 2015 an die Ströer Digital Publishing GmbH verkauft. [12] Dieses Medienunternehmen gehört zum Konzern Ströer SE & Co. KGaA (kurz Ströer Media), der mit mehr als einhundert Tochter- und Enkelgesellschaften [13] nicht nur Plattformen wie GIGA [14] und Spieletipps.de [15], sondern auch Statista, nach eigenen Angaben einen Anbieter für Markt- und Konsumentendaten [16], betreibt.

Die Datenbank der RIPE NCC bestätigte schlussendlich, dass auch der Netzwerkverkehr der Navigationshilfeseite nicht über die Deutsche Telekom, sondern über Dritte lief. Der entsprechende IP-Adressbereich, den das genannte Medienunternehmen verwendete, war damals mit einem Rechenzentrum verbunden, das mit der Deutschen Telekom nichts zu tun hatte:

> *This prefix is announced by:*
> *AS61157 - RPKI Status [..] "PLUSSERVER-ASN1 - PlusServer GmbH"*

Eine Abfrage der beiden IP-Adressen 62.138.238.45 und 62.138.239.45 in der RIPE-NCC-Datenbank ergab zu diesem Zeitpunkt folgendes:

```
Responsible organisation: PlusServer GmbH
Abuse contact info: abuse@plusserver.com

inetnum:          62.138.238.0 - 62.138.239.255
netname:          STROEER-NET
descr:            Ströer Digital Publishing GmbH
descr:            www.t-online.de
country:          DE
admin-c:          GH4837-RIPE
tech-c:           PNO7-RIPE
status:           ASSIGNED PA
mnt-by:           MNT-PlusServer
created:          2017-12-01T10:22:47Z
last-modified:    2017-12-01T10:22:47Z
source:           RIPE
```

Die Daten blieben also offenbar nicht bei der Deutschen Telekom. Sie wurden ganz augenscheinlich schon seit Jahren, seit dem Verkauf der Plattform T-Online, unerkannt an Dritte übermittelt.

RIPE NCC Für die Vergabe von IP-Adressen unter anderem in Europa zuständige Organisation

Kein Opt-In-Verfahren

Nach alldem, wie es aussieht, wurde die Navigationshilfe-Funktion nie auf ein Opt-In-

Verfahren umgestellt. Vielmehr mussten Kunden die 2009 eingeführte Funktion stets manuell im Kundencenter deaktivieren. Dafür sprechen, neben früheren Medienberichten und unzähligen Artikeln auf Hilfeseiten, vor allem die zahlreichen Beschwerden im Telekom-Kundenforum auch noch kurz vor Abschaltung.

Strafanzeige (§§ 206, 303a StGB)

Mit Schreiben vom 25. Januar 2019 habe ich Strafanzeige gegen die Deutsche Telekom AG und ihre Tochter, die Telekom Deutschland GmbH, wegen aller in Betracht kommender Straftatbestände erstattet. Das Schreiben habe ich in Kopie auch der Bundesnetzagentur (BNetzA) und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zugeleitet, sodass zeitgleich auch diese Behörden informiert wurden. Das BfDI hat meiner Kenntnis nach keine eigenen Maßnahmen ergriffen, sondern das Verfahren zuständigkeitshalber an die Bundesnetzagentur abgegeben – und die ist im weiteren Verlauf tatsächlich eingeschritten. Auf die Strafanzeige reagiert hat die Staatsanwaltschaft zunächst nicht. Erst rund drei Monate später, am 25. April 2019 wurde mir dannauf Nachfrage das Aktenzeichen und die Information, dass ein Ermittlungsverfahren wegen des Verdachts der rechtswidrigen Datenveränderung (§ 303a StGB) eingeleitet wurde, mitgeteilt. [17] Ich selbst habe – wie eingangs erwähnt – die Strafanzeige wegen aller in Betracht kommender Straftatbestände erstattet, sodass allein die Staatsanwaltschaft zu bewerten hatte, welche Straftatbestände möglicherweise verletzt wurden.

Dann ging mehrere Monate lang nichts voran; auf Sachstandsanfragen wurde nicht reagiert. Mit Schreiben vom 12. Januar 2020 habe ich deshalb Dienstaufsichtsbeschwerde wegen möglicher Untätigkeit erhoben. Der zuständige Leitende Oberstaatsanwalt in Bonn stellte mit Schreiben vom 17. Februar 2020 hierzu unter anderem fest:



Hier könnte Ihre Anzeige liegen.

In dem Verfahren sind die Ermittlungen aufgenommen und verschiedene Maßnahmen ergriffen worden. Derzeit dauern die Ermittlungen noch an. Dienstpflichtwidrige Unterlassungen bei der Bearbeitung des Verfahrens habe ich nicht festgestellt.

Ihre Sachstandsanfragen vom 14.05.2019, 29.10.2019 und 14.11.2019 sind allerdings tatsächlich nicht beantwortet worden, wobei die Anfragen vom 29.10.2019 und 14.11.2019 aufgrund eines Versehens der Geschäftsstelle erst verspätet zur Akte gelangt sind. Die zuständige Dezernentin hat die Sachstandsmitteilung an Sie mit Schreiben vom 07.02.2020 umgehend nach Bekanntwerden des Versehens nachgeholt.

Die angekündigte Sachstandsmitteilung vom 7. Februar 2020 lautete:

[E]s wird mitgeteilt, dass die Ermittlungen andauern.

Mit Schreiben vom 14. Mai 2020 wurde dann die Einstellung des Verfahrens – nunmehr wegen des Verdachts der Verletzung des Fernmeldegeheimnisses (§ 206 StGB) – bekanntgegeben:

[D]as Ermittlungsverfahren habe ich […] mit Zustimmung des zuständigen Amtsgerichts gemäß § 153 Abs. 1 der Strafprozessordnung [Absehen von der Verfolgung bei Geringfügigkeit und gleichzeitiger Verneinung eines öffentliches Interesse an der Strafverfolgung] eingestellt.

[…]

Nach dem derzeitigen Ermittlungsstand erscheint es gut möglich, dass eine telekommunikations- und datenschutzrechtliche Anpassung der sog. Navigationshilfe als Dienst von „T-Online“ nach der Veräußerung der Sparte „T-Online“ von der Deutschen Telekom AG / Telekom Deutschland GmbH an die Ströer SE Ende 2015 aufgrund eines Versehens nicht erfolgte. Eine Strafbarkeit wegen Verletzung des Fernmeldegeheimnisses gem. § 206 des Strafgesetzbuches setzt jedoch vorsätzliches Handeln voraus. Von weiteren umfangreichen Ermittlungen wurde abgesehen. Eine Verfolgung des Vorgehens [gemeint ist ‚Vergehen'] – auch des fahrlässigen Handelns – ist im Rahmen eines Ordnungswidrigkeitsverfahrens möglich.

Unter diesen Umständen wäre das Verschulden als gering anzusehen. Ein öffentliches Interesse an der Strafverfolgung besteht in diesem Falle nicht.

[…]

Mit Schreiben vom 31. Mai 2020 habe ich Beschwerde gegen diese Entscheidung eingelegt, weil ihr keine strafrechtliche Bewertung des ursprünglichen Verdachts der Datenveränderung gemäß § 303a StGB entnommen werden konnte. Der Generalstaatsanwalt Köln teilte hierzu rund drei Monate später, am 9. September 2020, mit:

Ein entsprechender strafrechtlicher Anfangsverdacht scheidet bereits aus Rechtsgründen aus. Denn die vorgenannte Strafvorschrift erfasst als zu schützendes Tatobjekt lediglich fremde Daten, das heißt solche, an denen ein unmittelbares Recht einer anderen Person auf Verarbeitung, Löschung oder Nutzung besteht. Weder die IP-Adresse des Kunden noch die von dem Kunden – erfolglos – angesteuerte Internetadresse (URL) stellen für die die DNS-Server betreibenden beschuldigten Unternehmen und deren Verantwortliche fremde Daten dar. Gleiches gilt für die Fehlermeldungen der DNS-Server. […]



Am Ende des Labyrinths ein löchriger Käsekuchen. Er ist eine Lüge.

Bewertung der Entscheidung

Im ersten Moment klingt die Einstellung des Verfahrens unerfreulich, doch dürfen wir in diesem Zusammenhang nicht vergessen, dass Strafrecht nur natürliche Personen – also echte Menschen – treffen kann. Die Telekom ist aber kein Mensch, sondern eine juristische Person. Selbst wenn die Staatsanwaltschaft die Verwirklichung eines Straftatbestandes also bejaht hätte, wären dafür allenfalls Einzelpersonen bestraft worden. Dass die Geschäftsführer die Funktion nach dem Verkauf der Plattform T-Online sehenden Auges so beließen, wie sie war, ist zwar nicht absolut ausgeschlossen, für wahrscheinlich halte ich es aber nicht – die beschäftigen sich mit Sicherheit mit ganz anderen Dingen. Das unprofessionelle Verhalten seitens der Telekom spricht ironischerweise dafür, dass es an jenem Vorsatz fehlte, den das Gesetz fordert, denn wer weiß, wer die Manipulation der DNS-Server (wohl) im Jahre 2009 einrichtete. Etwaige Nachfolger früherer Mitarbeiter haben (oder sollten zumindest) bei einem der führenden Telekommunikationsunternehmen Europas keinen Anlass haben, Systeme auf rechtswidrige Manipulationen zum Nachteil eigener Nutzer zu überprüfen, sodass die Annahme, die Behebung dieses Zustands sei schlicht vergessen worden, keineswegs abwegig ist.

Allerdings stimme ich nicht zu, insoweit die Einstellung nach § 153 Abs. 1 StPO erfolgte. Denn die Norm verlangt, dass die Schuld des Täters als gering anzusehen wäre und dass kein öffentliches Interesse an der Verfolgung besteht. Die Staatsanwaltschaft stützte sich aber darauf, dass es am erforderlichen Vorsatz fehlte und implizit auch darauf, dass ohnehin nicht klar wäre, *wem genau* dieser Vorsatz überhaupt nachzuweisen wäre. Das Verfahren hätte also gemäß § 170 Abs. 2 StPO eingestellt werden müssen. Auf § 153 Abs. 1 StPO hätte sich die Staatsanwaltschaft nur stützen können, hätte sie die Annahme des erforderlichen Vorsatzes für wahrscheinlich gehalten. Und dann wäre die Einstellung äußerst fragwürdig gewesen, denn dieser erhebliche Vertrauensbruch mit Auswirkungen auf so viele Kunden kann kaum als Argument dafür dienen, das öffentliche Interesse an einer Verfolgung zu verneinen.

Verfahren der Bundesnetzagentur, unter anderem

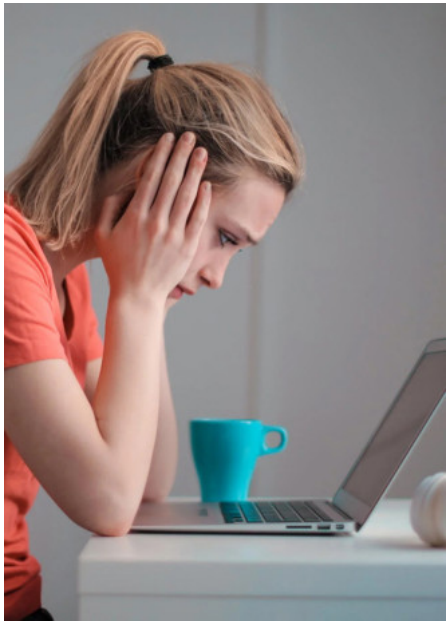
Die Bundesnetzagentur hat sich ausführlich mit dem Fall befasst und ist letztendlich dagegen vorgegangen. Sie sah einen Verstoß gegen § 149 Abs. 1 Nr. 16 in Verbindung mit § 96 Abs. 2 TKG (der alten Fassung, seit dem

1. Dezember 2021 gilt ein neues TKG), der die unerlaubte Erhebung oder Verwendung von Verkehrsdaten beschreibt. Sie verhängte am 29. September 2021 (rund zwanzig Monate nach Erstattung der Strafanzeige) – offenbar nach einem langwierigen Anhörungsverfahren und/oder zeitraubenden tatsächlichen oder rechtlichen Erwägungen – eine Geldbuße in Höhe von 50.000 € gegen die Telekom Deutschland GmbH.

Mit Schreiben vom 23. Februar 2022 teilte mir die Bundesnetzagentur mit, dass der entsprechende Bescheid mit einem Einspruch angegriffen wurde. Daraufhin ging der Fall gemäß § 69 Abs. 3, 4 OWiG zurück an die Staatsanwaltschaft, die – erfreulicherweise – entschieden hat, das Ordnungswidrigkeitsverfahren nicht einzustellen, sondern es dem zuständigen Gericht vorzulegen. Am 6. Oktober 2022 teilte mir die Bundesnetzagentur dann mit, dass für Ende November 2022 ein Verhandlungstermin vor dem Amtsgericht Bonn anberaumt wurde. [18]

Man kann es glauben oder nicht, aber es ist mangels Reaktion der Pressestelle des Amtsgerichts auf meine Anfrage vom 26. Januar 2023 unklar, ob dieser Termin denn überhaupt stattgefunden hat. Die Bundesnetzagentur teilte mir mit Schreiben vom 15. Dezember 2022 nämlich mit, dass das Amtsgericht Bonn das Verfahren gemäß § 47 Abs. 2 OWiG durch Beschluss vom 24. November 2022 endgültig eingestellt hat. Notwendig hierfür ist grundsätzlich zwar auch die Zustimmung der Staatsanwaltschaft (Satz 1); im Übrigen aber verhält sich die Vorschrift beinahe willkürlich. Es reicht völlig aus, wenn das Gericht die Verfolgung für nicht *geboten* hält. Der ganze Zirkus war also völlig umsonst.

Hinweis: Mittlerweile hat die Pressestelle des Amtsgerichts Bonn auf eine nochmalige Nachfrage reagiert und das Aktenzeichen 710 OWi 105/22 mitgeteilt. Dem öffentlich abrufbaren Beschluss ist zu entnehmen, dass die Einstellung erfolgte, weil eine Ahndung aus Sicht des Gerichts nicht geboten erschien. Die Kosten des Verfahrens wurden teilweise der Staatskasse auferlegt.



Ab und zu kommt jemand vorbei und befreit mich von den Spinnenweben.

Abschaltung der Funktion

Wesentlich schneller ging hingegen die Abschaltung der Navigationshilfe voran. Schon am 26. April 2019, drei Monate nach Erstattung der Strafanzeige und einen Tag nach dem Schreiben der Staatsanwaltschaft über die Einleitung des Ermittlungsverfahrens, wurde die Funktion abgeschaltet, wie einer offiziellen und zwischenzeitlich nicht

mehr abrufbaren Verlautbarung im Telekom-Kundenforum und einer privaten Direktnachricht des Twitter-Accounts @Telekom_hilft zu entnehmen war. So hätten nach Aussage des Telekom-Mitarbeiters „viele Kunden […] damals genau wegen der Navigationshilfe Probleme [gehabt]“.

Alternativen

Eine persönliche Konsequenz sollte es in jedem Falle sein, die DNS-Resolver der Telekom allenfalls nur noch dazu zu nutzen, um eine Suchmaschine zu öffnen und nach besseren zu recherchieren. Eine Zentralisierung ist nie gut, doch einen Resolver erachte ich durchaus als empfehlenswert, nämlich den des Vereins Digitalcourage e. V. [19]
Wer tiefer in die Materie einsteigen will, der kann – sozusagen – mithilfe eines Raspberry Pis und dem DNS-Resolver Unbound [20] seinen eigenen DNS-Resolver (für sich zuhause) betreiben. Der Kuketz-IT-Security-Blog hat hierzu einen ausführlichen Gastbeitrag veröffentlicht. [21]

Schlusswort

Ich möchte an dieser Stelle auf ein umfangreiches Schlusswort verzichten, weil mich der Umstand, dass der Rechtsstaat sage und schreibe vier Jahre gebraucht hat, um letztendlich dann (doch) nichts zu tun, gewissermaßen sprachlos macht. Wahrscheinlich braucht es noch einmal zwanzig und dann noch einmal dreißig Jahre, bis sich bei allen Entscheidungsträgern die Erkenntnis durchgesetzt hat, dass ein freies Internet ein zu schützendes Instrument ist, das zugleich als Spiegelbild nicht nur die Verfasstheit unserer Gesellschaft, sondern auch die unseres Rechtsstaates wiedergibt. Derartige Eingriffe sind nicht unerheblich, nur, weil niemand nachweislich geschädigt wurde. Sie stellen eine massive Verletzung der Garanten- und Vertrauensstellung des eigenen Internetzugangsanbieters dar und sind schon deshalb völlig indiskutabel.

Dass so etwas letztendlich nicht geahndet wird, wie sich gezeigt hat, ist nichts anderes als das Ergebnis eines von Grund auf falschen Werteverständnisses und einer daraus folgenden unzureichenden und teils geradezu anmaßenden Gesetzgebung beziehungsweise Rechtsprechung – wie es sich auch im eingangs angesprochenen Fall Quad9 nur zu deutlich gezeigt hat.

Referenzen

[1] ElooKoN: „Wie die Telekom mit unserem Vertrauen spielt“ (08.10.2022), https://elookon.de/artikel/wie-die-telekom-mit-unserem-vertrauen-spielt.

[2] Reiko Kaps: „Telekom leitet DNS-Fehlermeldungen um“ (17.04.2009), https://www.heise.de/newsticker/meldung/Telekom-leitet-DNS-Fehlermeldungen-um-213726.html (abgerufen am 05.03.2023).

[3] Johannes Endres: „DNS-Verbiegungen: Wie Provider das Domain Name System manipulieren“ (22.06.2010), https://www.heise.de/ct/artikel/DNS-Verbiegungen-1025662.html?view=print (abgerufen am 02.03.2023).

[4] Sebastian Grüner: „BGP-HIJACK: Telegram-Nachrichten kurzzeitig durch Iran geroutet“ (01.08.2018), https://www.golem.de/news/bgp-hijack-telegram-nachrichten-kurzzeitig-durch-iran-geroutet-1808-135788.html (abgerufen am 02.03.2023)

[5] Dusan Zivadinovic: „BGP-Hijacking: IP-Verkehr der Großen Vier nach Russland

umgeleitet“ (16.12.2017), https://www.heise.de/newsticker/meldung/BGP-Hijacking-IP-Verkehr-der-Grossen-Vier-nach-Russland-umgeleitet-3919524.html (abgerufen am 02.03.2023).
[6] Tomas Rudl: „Sony attackiert das Internet und siegt vor dem Landgericht“ (03.03.2023), https://netzpolitik.org/2023/eklatantes-fehlurteil-sony-attackiert-das-internet-und-siegt-vor-dem-landgericht (abgerufen am 05.03.2023).
[7] BHG, Urteil vom 13.10.2022, I ZR 111/21
[8] Bis zum 26. April 2019, ausweislich einer offiziellen Verlautbarung im Telekom-Kundenforum, die mittlerweile jedoch nicht mehr abrufbar ist.
[9] mdn web docs: „Set-Cookie“, https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie.
[10] Internet Engineering Task Force: „HTTP State Management Mechanism“, Abschnitt 4.1.2.5, https://www.rfc-editor.org/rfc/rfc6265#section-4.1.2.5.
[11] Ströer Digital Publishing: „Das Unternehmen“ (verlinkt als Impressum der T-Online Navigationsseite) https://www.stroeerdigitalpublishing.de/index.html%3Fp=2593.html (abgerufen am 15.03.2023).
[12] mm-newsdesk: „Ströer kauft T-Online, Telekom wird Großaktionär“ (13.08.2015), https://www.manager-magazin.de/digitales/it/stroeer-kauft-t-online-a-1047997.html (abgerufen am 02.03.2023).
[13] Ersichtlich bei einer Suche nach „Ströer Digital Publishing GmbH“ im Bundesanzeiger: https://www.bundesanzeiger.de/pub/de/start?0 (abgerufen am 15.03.2023).
[14] GIGA: „Impressum“, https://www.giga.de/info/impressum (abgerufen am 13.05.2023).
[15] spieletipps: „Impressum“, https://www.spieletipps.de/pages/imprint/ (abgerufen am 13.05.2023).
[16] statista: „Über uns – Das Unternehmen hinter dem Erfolgsprodukt“, https://de.statista.com/statistik/info (abgerufen am 16.04.2023).
[17] Staatsanwaltschaft Bonn: „Ermittlungsverfahren gegen Timotheus Höttges und Dr. Dirk Wössner“ (25.04.2019), Aktenzeichen 430 Js 139/19, https://elookon.de/public/articles/telekom/ermittlungsverfahren.pdf.
[18] Aktenzeichen des Amtsgerichts Bonn: 710 OWi-116 Js 163/22-105/22.
[19] digitalcourage: „Zensurfreier DNS-Server“, https://digitalcourage.de/support/zensurfreier-dns-server (abgerufen am 21.04.2023).
[20] NLNETLABS: „Unbound“, https://nlnetlabs.nl/projects/unbound/about/ (abgerufen am 13.05.2023).
[21] Maximilian Ernst: „Pi-hole, Unbound & Hyperlocal: Keine Werbung – Größtmögliche Unabhängigkeit“ (12.03.2019), https://kuketz-blog.de/pi-hole-unbound-hyperlocal-keine-werbung-groesstmoegliche-unabhaengigkeit (abgerufen am 13.05.2023).



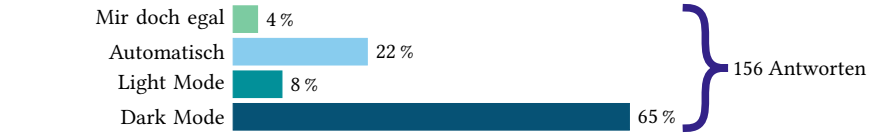
Statistik für alle!

Wir haben Mastodon und Mastodon hat ein Umfragetool. Nach einer kleinen Lernkurve haben wir festgestellt, dass es maximal 4 Antwortmöglichkeiten gibt. Hier stellen wir die Ergebnisse vor.

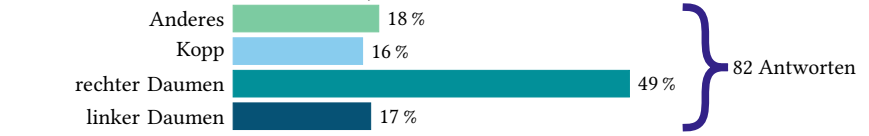
Ihr könnt uns folgen für mehr Umfragen, wichtige Neuigkeiten oder falls euch in Printmedien eine Kommentarspalte fehlt.

@datenschleuder@chaos.social

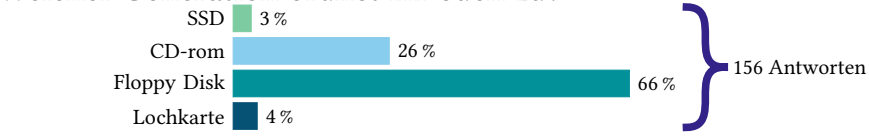
Die Gretchenfrage teilt die Redaktion:



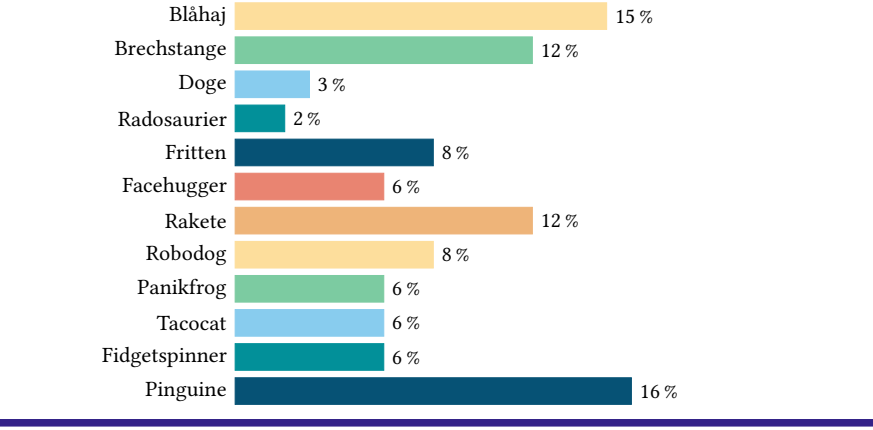
For Science! Was nutzt ihr, um ein Leerzeichen zu machen?



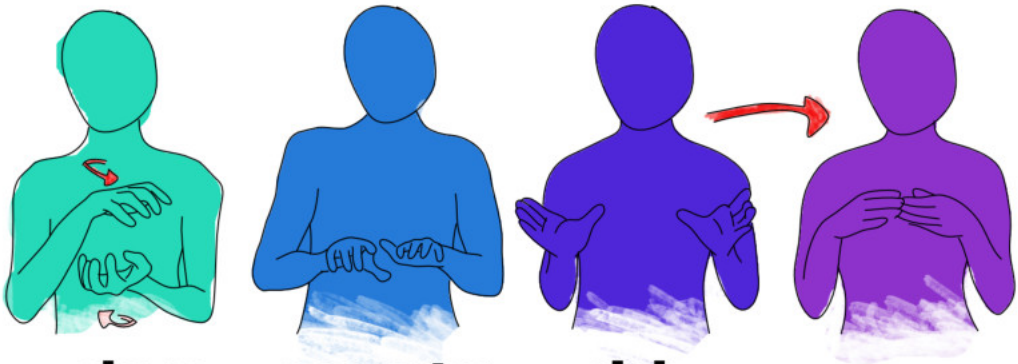
Welcher Generation ordnet ihr euch zu?



Wir machen Statistik. Welches Sternzeichen seid ihr? #ds106 #letzteseite



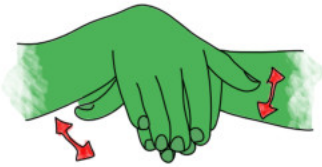
Wir lernen DGS*



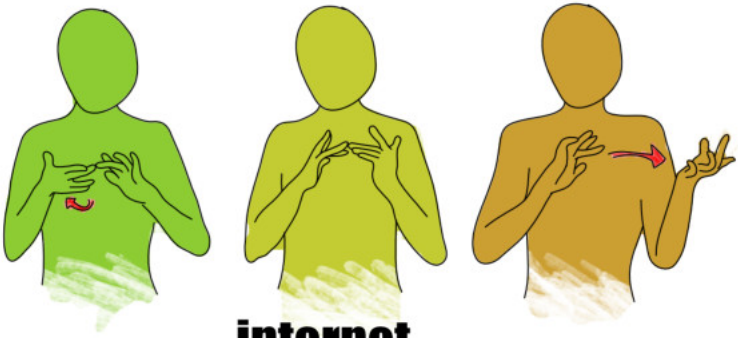
chaos computer club



c c c



schildkröte



internet

*Deutsche Gebärdensprache

It’s not a feature, it’s a bug! – Mehr Rechte für IT-Sicherheitsforschende

von magnus
@magnus_cerebrum@legal.social

Für ein verantwortungsvolles Forschen an und mit IT-Sicherheitslücken braucht es einen klar geregelten Meldeprozess für IT-Sicherheitslücken und eine unabhängig vermittelnde Instanz. Durch die bestehende Rechtslage werden Forschende an einem ethischen Handeln gehindert. An welchen gesetzlichen Schrauben gedreht werden könnte, damit die Arbeit von IT-Sicherheitsforschenden mehr gesellschaftliche Wertschätzung bekommt, zeigt dieser Beitrag.

2023. Die nationale IT-Sicherheitsforschung trägt zu den nötigen Patches und Fixes für IT-Sicherheitslücken derzeit nur bedingt bei. Grund dafür ist die komplexe und einengende Rechtslage, durch die Tätigkeiten in der IT-Sicherheitsforschung vielfach mit Risiken verbunden sind: Seit 2013 gibt es insgesamt 18 Videos auf media.ccc.de, die auf das Stichwort „Hausdurchsuchung“ verschlagwortet sind – von allgemeinen rechtlichen Empfehlungen [1] über praktische Hinweise [2] bis hin zu OpSec-Tipps [3]. IT-Sicherheitsforschung als wissenschaftlich-ethisches Hacken ist ein Versteckspiel vor Ermittlungsbehörden, obwohl es dazu dient, die kritischen Sicherheitslücken in Systemen zu schließen. Das Recht unterscheidet nämlich nicht, ob IT-Sicherheitsforschende moralisch handeln. Moralisches Handeln bedeutet in diesem Zusammenhang Sicherheitslücken zu melden, anstatt sie zum eigenen Nutzen zu missbrauchen. Wie sollte das Recht also angepasst werden, damit IT-Sicherheitsforschende ruhig – oder zumindest ruhiger – schlafen können?

Eine Antwort auf diese Frage versucht die Initiative „sec4research“ seit 2020 zu finden, in der IT-Sicherheitsforschende und Rechtswissenschaftler*innen Lösungsvorschläge erarbeiten und auf Missstände hinweisen. Das gemeinsame Ziel ist, IT-Sicherheitsforschende zu unterstützen und für einen sicheren, verständlichen Rechtsrahmen zu sorgen. Rechtswissenschaftlich sind Strafrecht, Datenschutz- und IT-Sicherheitsrecht und die jüngeren Bewegungen im EU-Rechtsraum von Bedeutung. Eine ausführliche (juristische) Auseinandersetzung mit der Konstruktion einer unabhängigen Meldestelle [4] und dem Prozess der Coordinated Vulnerability Disclosure [5] findet sich in den Veröffentlichungen von sec4research [6].

Definition der IT-Sicherheitsforschung

Grundlage für die folgenden Betrachtungen ist folgende Definition von IT-Sicherheitsforschung: IT-Sicherheitsforschung hat das Ziel, die IT-Sicherheit zu verbessern. Hierzu zählen das Beseitigen von Schwachstellen, Schadensbegrenzung, wenn diese Schwachstellen ausgenutzt werden, sowie die technische Analyse der An- und Eingriffe. Forschung dieser Art kann institutionell an Universitäten, beruflich in der Analyse von Sicherheitslücken beim Penetration Testing, oder rein privat geschehen. Ist eine Sicherheitslücke gefunden, wird



Augen auf. Die Bugs sind überall.

diese analysiert. Das Vorgehen ist dabei methodisch und versucht, die Faktoren für das Reproduzieren des Fehlers bzw. der Lücke zu ermitteln. Ein Beispiel: Eine Hackerin entdeckt beim Gebrauch einer Software zufällig eine Schwachstelle. Um zu verhindern, dass die Sicherheitslücke von Dritten ausgenutzt wird, analysiert sie ihren Umfang und meldet sie den Entwickler*innen der Software, um möglichst schnell ein Schließen der Lücke zu ermöglichen.

Strafrecht: Hackerparagraph und Co.

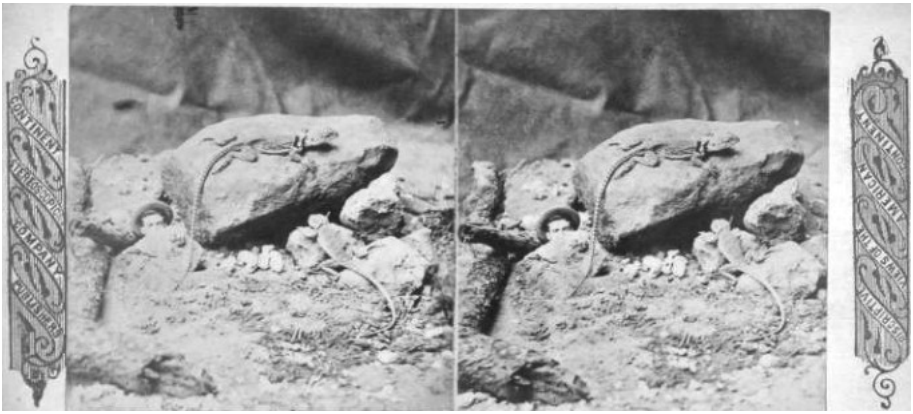
Bisherige Initiativen aus der IT-Sicherheitsforschung und dem CCC-Umfeld, die öffentlichkeitswirksam auf die Missstände für IT-Sicherheitsforschende hingewiesen haben, fokussierten sich im Strafrecht in der Regel auf den § 202c StGB, den sogenannten Hackerparagraphen. Dieser besagt, dass das Coden von Computerprogrammen und jede sonstige vorbereitende Handlung, die das spätere Ausspähen und Abfangen von Daten zumZweck haben, strafbar ist. Der Vorsatz des bewussten Erstellens eines Codes, der dazu dienen soll die Daten Dritter auszuspähen und abzufangen, trifft aber in der Regel nicht auf die Forschenden zu. Sie wollen die fremden Daten ja gerade schützen. Üblicherweise ist juristisch im Zweifel von der Unschuld der Forschenden auszugehen. Im Streitfall wird jedoch schon das Programmieren als objektives

Indiz für einen möglichen Vorsatz gesehen. Der tatsächliche Nachweis eines fehlenden (inneren) Vorsatzes im Prozess ist oft schwierig. Damit bleibt ein Restrisiko, mit einer Meldung der Sicherheitslücke zumindest den Verdacht der Ermittlungsbehörden zu wecken.

Es bedarf hier also einer klarstellenden Einbeziehung der IT-Sicherheitsforschung in das Strafrecht. Diese Überarbeitung muss dabei mehr als nur den „Hackerparagraphen" umfassen. Denn weitaus kritischer ist der § 202a StGB, der das Ausspähen von Daten durch „Umgehung von Zugangssicherungen" regelt. Die IT-Sicherheitsforschung analysiert und prüft Soft- und Hardware. Oftmals muss dafür eine Zugangssicherung (zum Beispiel Account Management oder Firewalls) überwunden werden. Das Strafrecht unterscheidet nicht zwischen kriminellen Absichten und ethischem Hacking. Die Zielsetzung Forschender spielt keine Rolle. Das Melden einer Sicherheitslücke bei einer Behörde hat strafrechtlich keine Relevanz, und müsste erst rechtlich geregelt werden, um eine „echte" Rechtssicherheit zu bieten. Für ein rechtssicheres, unbeschwertes Hacken zum Zweck der Forschung ist deswegen die Zustimmung der Auftraggebenden nötig. Zufallsfunde oder im Vorfeld stattfindende Forschungstätigkeiten sind aber mit einer solchen Lösung nicht berücksichtigt. Eine Meldung bietet strafrechtlich das gute Gewissen, alles zur Beseitigung des Bugs versucht zu haben. Nur im Einzelfall wirkt es sich strafmildernd aus. Selbst der wissenschaftliche Hintergrund der IT-Sicherheitsforschung, vorausschauend Fehler erkennen und beseitigen zu können, reicht für eine forschungsfreundliche Auslegung des § 202c StGB in Kombination mit der Wissenschaftsfreiheit (aus Art. 5 Abs. 3 Grundgesetz) nicht aus. Es braucht also eine völlig neue Regelung, die folgendes Vorgehen anerkennt: Das Offenlegen und Melden der IT-Sicherheitslücke geschieht im Rahmen der Forschung und aus öffentlichem (Schutz-)Interesse, wobei mit einer gewissen Rücksicht auf das jeweilige System/Objekt und mit dem reinen Ziel der Erkennung/Analyse der Lücke vorgegangen wird.

Datenschutzrecht

Dafür braucht es aber Regelungen über das Strafrecht hinaus. Die bestehende Rechtslage ist auch an anderen Stellen überarbeitungsbedürftig: Ist die Sicherheitslücke gefunden, gilt beim Fund personenbezogener Daten das Datenschutzrecht. Die IT-Sicherheitsforschung benötigt eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten, wenn die Datensätze „angefasst" bzw. verarbeitet werden. Erst bei einer überwiegenden Kontrolle über die Zwecke und Mittel der Verarbeitung personenbezogener Daten auf fremden Systemen gilt eine Verantwortlichkeit der IT-Sicherheitsforschenden nach dem Datenschutzrecht. Ein Einordnen, ob das Datenschutzrecht zur Anwendung kommt, ist hier aber kaum klar möglich, da Forschende nicht für die lückenhaften Systeme verantwortlich sind, und der Fund einer Lücke nicht automatisch eine datenschutzrechtliche Verantwortung auslöst. Erst wenn die Daten heruntergeladen oder auf andere Weise verarbeitet werden, bedarf es einer Rechtsgrundlage. In Betracht kommen dann entweder die öffentliche Forschung (zum Beispiel institutionelle Forschung im Rahmen von Forschungsprojekten oder im eigenen Forschungsauftrag öffentlicher Einrichtungen wie Universitäten – Art. 6 Abs. 1 Bst. e DSGVO) oder eine private Forschung (zum Beispiel ethisches Hacken – Art. 6 Abs. 1 Bst. f DSGVO) um den Sachverhalt einzuordnen.



Eine datenschutzrechtliche Grundlage erlaubt allerdings nicht das Analysieren, geschweige denn den unerlaubten Zugriff auf Datensätze. In der Regel kommt die Sicherheitsforschung erst ins Spiel, wenn ihre Meldung einer Sicherheitslücke als Präventiv- und Schutzmaßnahme verstanden wird. Da die DSGVO Verantwortliche und Unternehmen dazu anhält, Schutzmaßnahmen nach dem „Stand der Technik" zu implementieren, könnten diese das präventive schließen von Lücken aktiv in Coordinated-Vulnerability-Policies selbstständig regeln. Für einen sicheren Rechtsrahmen für Forschende und ethische Hacker*innen reicht das aber nicht.

IT-Sicherheitsrecht

Viel mehr lohnt ein Blick in das aktuelle IT-Sicherheitsrecht und das BSI-Gesetz (BSIG). Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat laut § 4b Abs. 2 BSIG die Rolle, „Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen" zu sammeln. Meldungen können anonym oder pseudonym erfolgen. Sofern die erhaltenen Informationen zur Einleitung von Straf- und Ermittlungsverfahren gegen Dritte, oder gegen die Forschenden selbst benötigt werden, ist eine Auflösung des Pseudonyms zulässig. Beide Aufgaben bei der gleichen Stelle zu verorten wirkt widersprüchlich, weil ein Schutz der IT-Sicherheitsforschenden bei einer anonymen Meldung und die nachträgliche Ermittlung im Verdachtsfall den Zweck einer anonymen bzw. anonymisierten Meldung sich ausschließen. Das BSI gehört zum Geschäftsbereich des Bundesministeriums des Innern. Seine Methoden erinnern aber an Ermittlungsbehörden: Es führt beispielsweise Portscans im öffentlichen Telekommunikationsnetz (§ 7b) durch, und fragt Bestandsdaten bei Telekommunikationsanbietern in Verbindung mit Verkehrsdaten aus Vorratsdatenspeicherung (§ 5c Abs. 1 und 2) ab. Das BSI scheint vorrangig sicherheitspolitische Fragen zu untersuchen. Der Schutz von nationalen IT-Systemen und Nutzen-

den bzw. Verbraucher*innen scheint nur hehres Ziel. Wünschenswert wäre stattdessen eine unabhängige Melde- und Koordinationsstelle, die vermittelnd zugunsten der IT-Sicherheitsforschenden agiert.

Grundrechte: Schutz vor IT-Sicherheitslücken?

Artikel 5 Abs. 3 des Grundgesetzes schützt jedes wissenschaftliche Handeln als Grundrecht, denn „Wissenschaft, Forschung und Lehre sind frei". Nun könnte man auf den Gedanken kommen, dass die Forschung in Art. 5 Abs. 3 GG – und damit auch die IT-Sicherheitsforschung – grundrechtlich geschützt ist. Grundrechte haben die Aufgabe, Lücken und Unsicherheiten im Verständnis von Gesetzen durch eine einheitliche Auslegung auszugleichen. Grundrechte helfen den IT-Sicherheitsforschenden damit aber nur bedingt, wie das Strafrecht schon oben zeigt: Auch eine forschungsfreundliche Auslegung von Strafrechtsnormen gibt dem Strafrecht nicht ausreichend vor, ob wissenschaftliche Handlungen das Erfüllen strafrechtlicher Tatbestände rechtfertigen. Wegweisend ist bislang nur das Urteil des Bundesverfassungsgerichts im Sommer 2021, [7] nach dem der Staat bei Kenntnis von IT-Sicherheitslücken das Schließen von IT-Sicherheitslücken durchsetzen muss. Gleiches gilt für das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme, jeweils verankert in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG. [8] Gemeinsam schützen beide die Sicherheit von Systemen auf Datenebene (also Datensicherheit) und System-Ebene (also IT-Sicherheit) und verstärken die staatliche Pflicht das Schließen von Lücken durchzusetzen. Das Handeln der IT-Sicherheitsforschenden ist also grundrechtsschützend. In diesen Prozess der Coordinated Vulnerability Disclosure könnten und sollten IT-Sicherheitsforschende bewusst eingebunden und ihre Rolle positiv besetzt werden. Der Prozess und dazugehörige Akteur*innen müssen in einem Gesetz festgehalten werden, um einen sicheren Rechtsrahmen zu bieten.

EU-Regulierung durch NIS2-Richtlinie und Cyber Resilience Act

Die zukünftigen bzw. laufenden EU-Regelungsvorhaben üben merklichen Druck aus, ein solches staatliches Schwachstellen-Management zu regeln: Die im Dezember 2022 verabschiedete Richtlinie zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS2-Richtlinie) will eine einheitliche Regulierung der IT-Sicherheit erzielen, und die Schwächen des Vorgängers von 2017 ausgleichen. Sie betrifft nun nicht mehr „kritische Infrastrukturen" und „digitale Dienste", sondern löst die Begriffe auf und orientiert sich an der sogenannte Kritikalität als Risiko der Infrastruktur. Dies ermöglichst ein dynamischeres Verständnis für neue Plattformen und technische Anwendungen. So können beispielsweise in Zukunft Soziale Netzwerke wegen ihrer gesellschaftlichen Rolle für die Meinungsbildung als kritische Infrastruktur eingeordnet werden. Einen koordinierten und verantwortungsvollen Umgang mit Schwachstellen-Meldungen regelt die NIS2-Richtlinie in Art. 12: Mitgliedsstaaten benennen bestehende oder (selten) neue Institutionen als Cyber Security Incident Response Teams (kurz CSIRTs), die mit der koordinierten Offenlegung von Sicherheitslücken beauftragt werden. Als koordinierende

Stelle fungiert das CSIRT wie ein „vertrauenswürdiger Vermittler und erleichtert die Interaktion zwischen der eine Schwachstelle meldenden natürlichen oder juristischen Person und dem Hersteller oder Anbieter" (Art. 12 Abs. 1) der Software, Hardware oder des Systems.

Mit diesen Vorgaben geht die weiter oben genannte Regelung des BSI nur bedingt einher. An der Vertrauenswürdigkeit bestehen wegen der fehlenden Unabhängigkeit vom Innenministerium und zum Beispiel der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) oder dem Bundeskriminalamt erhebliche Zweifel; eine vermittelnde Rolle benennt § 4b BSIG nicht. Der Druck auf die Bundesregierung wird durch den im Herbst 2022 von der EU veröffentlichten Entwurf des sogenannte Cyber Resilience Acts (CRA) noch erhöht, da darin für Produkte mit „digitalen Elementen" ähnliche Pflichten für eine Cybersicherheitsstrategie und (Coordinated) Vulnerability Disclosure Policies vorgesehen sind. Damit sind sämtliche Produkte gemeint, die sich vernetzen können – vor allem aus dem Bereich Internet of Things. Die Ausgestaltung ist aber bislang nur lose im Anhang I des Entwurfes verankert. Ob und wie ein synchrones Verständnis von NIS2-Richtlinie und CRA für die Prozesse gesichert ist, lässt sich bislang nicht erkennen. Ein Problem könnte hier sein, dass die NIS2-Richtlinie national umgesetzt werden muss und daher gesetzgeberische Spielräume bestehen. Nationale Regelungen könnten sich im Detail von der EU-weiten Regelung durch den CRA unterscheiden und für Verwirrung oder uneinheitliche Prozesse sorgen.

Zusammenfassung

IT-Sicherheitsforschende und ihre für die Gesellschaft wertvolle Arbeit sind durch ein Netz von verschiedenen nationalen Regeln eingeengt. Nachhaltige Forschung kann nicht betrieben werden, wenn das Recht Unternehmen und staatlichen Institutionen die Möglichkeit gibt, diese zu torpedieren. Es braucht nicht nur eine Streichung oder Anpassung des § 202c StGB. Der Umgang mit IT-Sicherheitslücken, eine bewusste und nachhaltige Entwicklung von Soft- und Hardware, und rechtlich klar geregelte Prozesse müssen Sicherheit schaffen. Mit der NIS2-Richtlinie und dem CRA besteht die Möglichkeit, einer weiteren Bedrohung entgegenzusteuern. Grundlage ist aber nach wie vor eine offene Kommunikation zwischen Jurist*innen und Informatiker*innen/IT-Sicherheitsforschenden. In der Hackerethik steht: „Beurteile Hacker*innen nach dem, was sie tun und nicht nach Kriterien wie Aussehen, Alter, Herkunft, Spezies, Geschlecht oder gesellschaftliche Stellung [wie Beruf oder akademischen Titeln]". [9] Dieser Grundsatz muss Einzug in die nationalen Rechtsvorschriften finden, damit eine Meldung von Schwachstellen möglich wird.

Referenzen

[1] https://media.ccc.de/v/36c3-91-risky-business-rechte-und-pflichten-von-it-sicherheitsforscherinnen

[2] https://media.ccc.de/v/35c3-10018-verhalten_bei_hausdurchsuchungen

[3] https://media.ccc.de/v/35c3-9716-du_kannst_alles_hacken_du_darfst_dich_nur_nicht_erwischen_lassen

[4] Kurzfassung – Vettermann/Wagner/Leicht/Freiling, bidt-Papier: https://doi.org/10.35067/b0bj-im05; Langfassung – Wagner/Vettermann et al., Verantwortungsbewusster Umgang mit IT-Sicherheitslücken (Whitepaper 2): https://doi.org/10.25353/ubtr-xxxx-8597-

6cb4.
[5] https://sec4research.de/assets/Whitepaper.pdf
[6] Zur Initiative: https://sec4research.de
[7] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2021/06/rs20210608_1bvr277118.html
[8] Vettermann, Der grundrechtliche Schutz der digitalen Identität, S. 251 ff – https://www.ksp.kit.edu/site/books/m/10.5445/KSP/1000148103/.
[9] Zitat aus der Hackethik des CCC – https://www.ccc.de/de/hackerethik. Einfügung durch den Autor.



Die Datenschleuder Nr. 107

Herausgeber
(Abos, Adressen, Verwaltungstechnisches etc.)

Chaos Computer Club e. V.
Zeiseweg 9, 22765 Hamburg
<mitgliedschaft@ccc.de> PGP:
A3C9 D85C 03E1 B294 1317
42A6 BB23 9969 B503 5E5A

Kontaktadresse
(Artikel, Leser*innenbriefe, Inhaltliches)

Redaktion Datenschleuder
Chaos Computer Club e. V.
Zeiseweg 9, 22765 Hamburg
<ds@ccc.de> PGP:
A2D6 72C1 15A4 363F 0DA0
512F 5835 6F24 94A7 9641
https://ds.ccc.de/

Redaktion dieser Ausgabe

clx, Janine „sharon" Frisch, Jan „vollkorn" Girlich, Helen „smettbo" Klaus, myri, Philipp „fiveop" Schäfer, Yves „Kitsune" Sorge, sylvia, Oliver „magnus" Vettermann, Hanno „Rince" Wagner

Bearbeitungsschluss der Druckversion

13.08.2023

Umschlaggestaltung

Titelbild	vorletzte Seite	Rückseite
clx	clx	clx

Gesamtherstellung

Texdat-Service gGmbH,
gemeinnützige Inklusionsfirma nach § 215 ff. SGB IX
https://www.texdat.de/
ZVD Kurt Döringer GmbH & Co. KG,
https://www.zvd.info/
Fehringer Industriebuchbinderei,
https://www.ibbfehringer.de/

Vervielfältigung

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.

V. i. S. d. P.

Hanno „Rince" Wagner


PRIORITY®
★ MAIL
UNITED STATES
POSTAL SERVICE®
VISIT US AT USPS.COM®
ORDER FREE SUPPLIES ONLINE
FROM:
IN
FAIRDUST
WE TRUST
Label 228, March 2016
FOR DOMESTIC AND INTERNATIONAL USE

New Passwordmanager, who dis?

von clx und towe
<clx@riseup.net>

Mal wieder gab es einen Datenregen beim Passwortmanager LastPass. Es reicht, beschließen clx und towe und verabschieden sich von LastPass, um zu einem neuen Passwortmanager umzuziehen. Dies sind ihre Abenteuer.

Gute Nachrichten zum Jahreswechsel

Es ist der 22. Dezember 2022, diverse Jahresend-Veranstaltungen finden online statt, draußen ist es kalt, grau, verregnet und voll mit Corona-Viren. Drinnen poppt eine E-Mail auf.

Das ist nicht die erste E-Mail von LastPass zu diesem Breach. Die kam schon am 25. August 2022. Damals stand da allerdings „alles gar nicht schlimm und super safe“, „bitte keine Sorgen machen“, „gehen sie weiter, es gibt hier nichts zu sehen“. Die neue E-Mail ist das erfreuliche Vorweihnachtsupdate vom 22. Dezember 2022. „Uups, es wurden auch Vaults erbeutet – aber bitte keine Panik, die Passwörter sind weiter sicher“. [1]

„Dear valued customer, In keeping with our commitment to transparency, we wanted to inform you of a security incident that our team is currently investigating. We recently detected unusul activity within a third-party cloud storage service, which is currently shared by both LastPass and its affilliate, GoTo. We immediately launched an investigation, engaged Mandiant, a leading security firm, and alerted law enforcement. We have determined that an unauthorized party, using information obtained in the August 2022 incident, was able to gain access to certain elements of our customers’ information. Our customers’ passwords remain safely encrypted due to LastPass’s Zero Knowledge architecture.“

Im Klartext heißt das: Deine Daten hat jemand anders und sobald diese Person genug Rechenpower hat, um die zu entschlüsseln – oder dein Passwort einfach kacke ist – kann sie damit auch Unfug treiben. Nun haben wir zwar beide Keyphrases, die etwa 25 Zeichen lang sind, aber trotzdem. Hinzu kommt, dass zum einen nicht alle Inhalte mit dem Passwort geschützt sind und zum anderen nicht wie die einzelnen Passworte schlicht mit einer Änderung aus der Welt zu räumen sind.

Nochmal in langsam: Online-Passwort-Manager sind Werkzeuge, die Mensch helfen sollen, sichere Passwörter für jeden Dienst, den Mensch online verwendet zu erstellen, zu speichern, auf allen eigenen Geräten verfügbar zu machen und leicht zu ändern. Die Idee ist: Eigenen Login-Dateien werden in einem Vault, oder virtuellen Schließfach gespeichert. Das Schließfach ist verschlossen mit einem Hauptpasswort – erst wenn man dieses Passwort eingibt, werden die gespeicherten Daten lokal entschlüsselt und nutzbar. Am Computer gelingt der Zugriff auf das Online-Vault meist durch Browser-Plugins, die dann zum Beispiel das Password- und Login-Fenster automatisch ausfüllen, wenn ein Passwort und Login für diese Webseite gespeichert sind und das Plugin verifiziert hat das die URL richtig ist. Wie fast alles im Internet haben solche Dienste Vor- und Nachteile. Warum wir bei LastPass

waren: der Preis war okay und es gab Plugins oder Apps für so gut wie alle Geräte. Nachteil: Die Vaults und damit die sensiblen, aber verschlüsselten Passwort-Dateien sind auf Servern des Anbieters gespeichert… das ist für Angreifer natürlich ein attraktiver Honigtopf, um Passwortdaten zu erbeuten, um sie dann später zum Beispiel im Darknet zu verkaufen; sie müssen nur bei einem Anbieter erfolgreich die Daten bekommen und können dann die Daten seiner Kunden nutzen. Und genau das war bei LastPass geschehen. Im Sommer 2022 war aufgefallen, dass Angreifer*innen auf Nutzer-Daten zugreifen konnten. Die Daten der Nutzer*innen – insbesondere die Passwörter und Logins – sind zwar verschlüsselt auf den Servern gespeichert, aber wahrscheinlich wird es nicht mehr zu lange – das wäre nach unserem Dasein in dieser Welt – dauern, bis aktuell verwendete Verschlüsselungsalgorithmen möglicherweise auch ganz ohne Quantum Computing gebrochen oder nachgerechnet werden können. LastPass zeichnet sich hier besonders negativ durch scheibchenweise Kommunikation aus. Erst Stück für Stück und Woche für Woche oder Monat wurde bekannt, welche Daten wirklich alle erbeutet wurden, welche Teile des Vaults wirklich verschlüsselt waren und welche potentiellen Gefahren das für die Nutzer*innen bedeuten würde. Spätestens mit der Mail vom Dezember wurde also klar: wir müssen handeln.

towe hat die Feiertage mit der Familie verbracht, clx hat sich durch NightCity [3] geklickt. Das neue Jahr startet nun mit einem neuen Task: dem Umzug des Passwort-Managers. Welchen soll man wählen? Wir wollen beide nicht selbst hosten und uns war wichtig, dass wieder möglichst viele Gerätearten unterstützt werden und die bisher bekannten Nutzungskonzepte über Browser-Plugins und Smartphone-App weiter funktionieren. Irgendwer im Internet hat gesagt, dass 1password sicherer sei, also probieren wir den mal aus: „Platforms like @1Password also have a secret key in addition to master password which makes the process much more difficult as well as encrypting all associated metadata that could be an attack vector.“ [2] Nun sind ja aber Daten nicht sicherer in einer neuen Umgebung, wenn sie vorher schon in die freie Wildbahn gelangt sind. Also müssen wir nicht nur umziehen, sondern auch aufräumen und Passwörter erneuern. Marie Kondo würde sagen: „Does it spark joy?“ Nich wirklich! Ohne Internet is aber auch doof. So planen wir, für genutzte Accounts neue PW zu vergeben und ungenutzte einfach zu löschen. Easy peasy. Kurz zu unseren creds: towe ist Verwaltungsnerd, clx macht irgendwas mit Medien. Wir sind daher nur interessierte Amateur*innen ohne Informatikstudium.

Der Umzug

Step 1: Export der Passwörter aus dem LastPass-Vault auf den eigenen Rechner. Das ging erstaunlich schmerzfrei und konnte dann als *irgendwas.csv* geöffnet werden. Sortiert nach den Spalten: *url, username, password, totp, extra name, grouping, fav*. Bei den meisten Einträgen sind lediglich die ersten drei Spalten gefüllt. Seine ganzen Passwörter in Klarschrift zu sehen, fühlt sich irgendwie gruselig an, denn so würden die LastPass-Angreifer unsere Daten auch sehen, hätten sie unser Hauptpasswort entschlüsselt. Bei clx sind es etwa 530, bei towe um die 480 Einträge – also ordentlich was zu tun. Es stellt sich die Frage: Nutze ich überhaupt so viele Accounts?

Step 2: Neuen Account bei 1password anlegen. 14 Tage kostenfrei, danach eine Summe je Monat. Ein bisschen teurer als LastPass, wenn man das auf mehreren Geräten verwen-

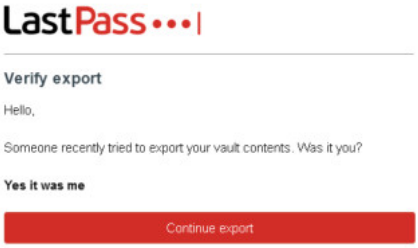
den will. Dafür muss Mensch sich 'ne neue Passphrase überlegen. Wir schauen uns zur Inspiration nochmal Snowdens Einweisung bei John Oliver an.



Zur Inspiration: John Oliver fragt Snowden was ein gutes Passwort wäre.
Last Week Tonight [4]

towe entscheidet sich dann doch nicht für „passwerd_!2E45“, sondern für einen hübschen Satz, gewürfelt aus Seiten, Zeilen und Nummern verschiedenster Bücher aus dem Regal. Import der CSV ist ziemlich easy: Format aussuchen, Upload, Browser-Plugin installieren und fertig.

Step 3: Let the pain begin… Wir fangen beim Buchstaben A an, beziehungsweise bei irgendwelchen WiFi-Namen, die mit Zahlenkombos beginnen und 1und1. clx setzt Tee auf für die Sofa-Workstation mit Decken, denn die Heizung ist aus wegen Putin. Fünf Stunden später sind wir bei E. Es entsteht ein kleiner Wettbewerb: Wer kommt als Erste*r beim nächsten Buchstaben an? Gemeinsames Aufregen, entnervt wird aus Tee irgendwann auch Rotwein und Pistazien. Wir wiederholen diese Session noch zwei Mal (!!!), bis wir endlich durch sind.



LastPass fragt via 2FA nach, ob der export legit ist. (LastPass)

Passwerds tickle your brain

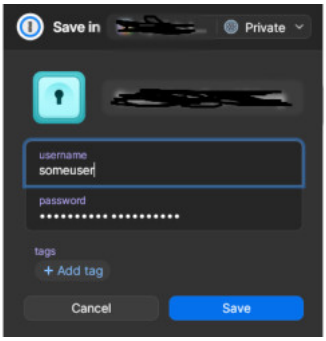
towe ist ewiger Optimist, versucht das ganze Unterfangen positiv zu framen und meint, dass es doch ein schöner „Trip down Memory Lane“ sei, sich alte Services anzusehen, die mensch irgendwann mal benutzt hat und vielleicht gut fand, zu schauen, welche Startups es geschafft haben, welche nicht. Immerhin haben manche Services uns in einer bestimmten Phase des Lebens begleitet – mal ein Interesse für Data Science, für das mensch sich damals bei den heißen Tools angemeldet hat; mal der damals neue Streaming-Anbieter, der uns durch den ersten COVID-Winter begleitet hat. Vergleichbar mit dem Scrollen durch einen lange nicht mehr geöffneten Foto-Ordner.

clx ist eher frustriert und genervt, dass es beispielsweise ein Portal gibt, welches einem nicht die Möglichkeit gibt, das Passwort zu ändern, oder den Account zu löschen, dafür aber gern eine E-Mail mit dem Passwort in Klarschrift als Reminder schickt. Oder eins, das darauf hinweist, dass mit Löschung des Accounts die Gewährleistung für gekaufte Produkte ent-

fällt. E-Mails sind für alte Leute, warum muss mensch sowas schreiben, um einen Account zu löschen? clx hat keine Geduld für so'n Quatsch. towe hat sich das mit den E-Mails aber auch gleich geklemmt.



Schon an der Länge der Übermalung sieht man, dieses Passwort, das nicht geändert werden kann, ist supersafe.

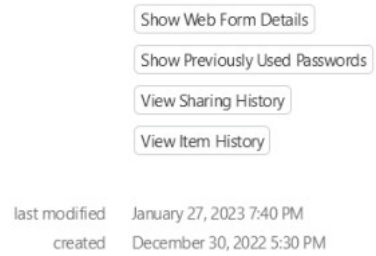


Ist es klug das neue Passwort zu speichern, bevor die Website es akzeptiert hat?

Passwerds divide the bad and the not so bad

1Password macht es mensch aber auch nicht immer leicht und einige Probleme in der Programmierung können schon recht nervig werden, wenn die Webseite und das 1password-Browser-Plugin nicht richtig miteinander arbeiten. Dann wird zum Beispiel ein neues Passwort in 1password gespeichert weil das Pop-up das so will, das Formular der Webseite nimmt aber das neue Passwort nicht an, weil zuwenig/zuviel/die falschen Sonderzeichen/Zahlen/Gremlins darin vorkommen.

Dann kann man den ganzen Spaß von vorne beginnen und das alte Passwort aus der History fischen.



History des alten Passworts

Da war LastPass besser, das hat meistens erst nach Setzung des PW gefragt, ob mensch den entsprechenden Eintrag updaten will.

Mach doch selber

Higher-Level-Nerds werden jetzt vielleicht fragen: „Aber warum hostet ihr nicht selbst?" Short answer: Zuviel Nerv, um einen sicheren Betrieb zu garantieren. towe hat einen Erwachsenenjob, clx drölfzig Freelance-Projekte und beide haben einfach mehr Spaß an anderen Dingen. Was das Löschen von nicht mehr gebrauchten oder gewollten Accounts angeht: bei den importierten Accounts sind echt viele Dead Ends dabei. Teils sind die Seiten einfach 404, teils inzwischen dubioses Clickbait oder einfach aufgekauft. Hat der Käufer unsere Daten gleich mitgekauft? Wenn mensch sich auf der LastPass-Seite die Nutzung der betroffenen Datenbank-Einträge ansieht, ist das allerdings nicht wirklich verwunderlich.

Nur einige wenige Anbieter*innen offerieren eine „echte" DSGVO-konforme Datenlöschung nach „Recht auf Vergessen" an – die personenbezogenen Daten werden hier also wirklich gelöscht, und nicht nur die Accounts



Letzte Nutzung einiger Passwörter in LastPass

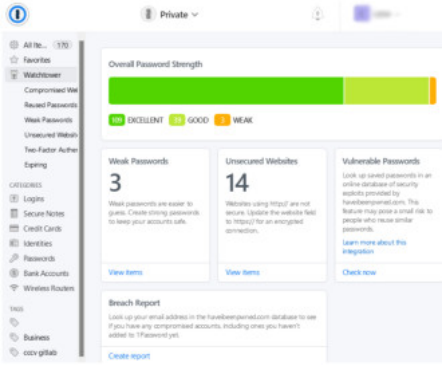
irgendwo im Backend auf „inaktiv forever“ gesetzt. Einen Account bei einer Seite zu löschen, die es tatsächlich noch gibt, braucht zwischen drei Klicks und vier E-Mails mit einer echten Person und dauert entsprechend zwischen wenigen Sekunden und mehreren Wochen. Bei manchen Accounts ging es auch einfach gar nicht. Das war sehr frustrierend, weil wir natürlich trotzdem lange danach gesucht haben. Wünschenswert wären hier Standards oder Best Practices, die einem intuitiv zeigen, wo mensch seinen Account löschen kann – inzwischen wissen wir ja auch, dass uns ein Klick auf das Seitenlogo zurück zur Homepage bringt… Und noch ein Wunsch an all die kleinen Wein-Shops, Werkzeug-Verkäufer und so weiter: Bitte baut doch mindestens eine „Passwort vergessen“-Funktion in eure selbstgebastelten Shop-Systeme ein – dann könnt ihr euch auch sparen, uns unsere vergessenen Passwörter im Klartext händisch per Mail zu schicken, so viel Service muss gar nicht sein. Ebenso fällt auf, dass viele der größeren Anbieter*innen inzwischen eine 2FA-Option hinzugefügt haben. Wenn mensch also eh gerade tief in den Account-Pages ist, um Passwörter zu ändern, lohnt es sich oft auch gleich 2FA zu aktivieren – zumindest uns beiden gibt das etwas mehr gefühlte Sicherheit für den nächsten Breach/Hack/Leak.

Passwerds are for Messies

Durch den Umzug haben wir eine Reduktion von etwa 40 % unserer Passwort-Einträge geschafft und eine kleine Wunschliste entwickelt, an alle, die so’ne Sachen beruflich oder professionell machen:

1. Passwörter sind nicht wirklich zukunftsfähig, denkt euch gefälligst was anderes aus!

2. Accounts löschen muss ein standardisierter Prozess werden, genauso einfach wie eine Accountregistrierung, ohne E-Mails, ohne mystische Sub-Sub-Seiten. Vielleicht hilft hier der EU-Vorstoß für einen Widerrufsbutton [5]?
3. Transparente Erklärung und Aufklärung darüber was mit Daten passiert, wenn eine Plattform gekauft wird – bitte in weniger als 2000 Zeichen.
4. Self Destruction Timer von Accounts bei Inaktivität, natürlich verbunden mit einem Verfallsdatum der im Account enthaltenen Daten.



Der freundliche grüne Balken lobt die getane Arbeit.

Nach dem Umzug ist vor dem Umzug

Aufgrund der Jahreswechsel-Verpeiltheit und Rotwein, haben wir nicht alles genau dokumentiert und eine Reihe von Beispielen sind natürlich hochgradig subjektiv und garantiert nicht reproduzierbar. Beim nächsten Hack und Password-Umzug planen wir besser zu dokumentieren, inklusive Zeitdokumentation und Eyetracking für die Suche nach dem dann hoffentlich häufiger vorhandenen „Account löschen“-Button.

Für uns bleibt der optimistische Plan vielleicht zukünftig in regelmäßigen Abständen Account-Cleaning zu betreiben – das geht ja auch ohne den externen Zwang durch Hacks und braucht dann nicht immer gleich drei Tage. Also demnächst am Wochenende nach der Steuererklärung mal die Accounts ausmisten? Oder was anderes spannendes unternehmen?

Referenzen

[1] Graham Cluley: „LostPass: after the LastPass hack, here's what you need to know“ (2023), https://grahamcluley.com/lostpass-after-the-LastPass-hack-heres-what-you-need-to-know/

[2] Architecture Notes: Twitter-Thread über den LastPass-Breach und die Verschlüsselung der Passwörter (2022), https://twitter.com/arcnotes/status/1608130745826177025

[3] Night City, der fiktive Handlungsort des Spiels „Cyberpunk 2077“, https://www.nightcity.love/

[4] Last Week Tonight: „Edward Snowden on Passwords“ (2015), https://www.youtube.com/watch?v=yzGzB-yYKcc

[5] Europäischer Rat: „Rat vereinbart Verhandlungspositionen zu im Fernabsatz geschlossenen Finanzdienstleistungsverträgen“ (2023), https://www.consilium.europa.eu/de/press/press-releases/2023/03/02/council-agrees-negotiating-position-on-financial-services-contracts-concluded-at-a-distance/

Nerv' uns doch auf

#ds107_4


Besiegt unsere
KI


grab
goss
bye

Tetra-Funk: Solarparks mit der Handfunke steuern?

von Thomas Blinn, Sprecher der AG KRITIS <tblinn@ag.kritis.info>

„Digital“ heißt nicht unbedingt „verschlüsselt“. Ein kleiner Exkurs in die digitale Funktechnik kritischer Infrastrukturen.

Ende 2022 wurde bekannt, dass Hackende in deutschen Städten die Verkehrsampeln mittels Funktechnik auf grün schalten können. Das dort verwendete Funk-Protokoll aus den 1980er Jahren nutzt weder Authentifizierung noch Verschlüsselung. Es ist deshalb anfällig für Replay-Attacken, also Angriffe durch Wiederaussenden eines vorher aufgezeichneten Funksignals. [1]

Nicht nur Ampeln haben eine ungeschützte Funk-Schnittstelle

Die AG KRITIS wurde von Hobby-Funkenden kontaktiert, die auf ein ähnlich gelagertes Problem bei Energieerzeugungsanlagen und weiteren Anwendungsfällen hinwiesen.

Wir haben Einblick in Mitschnitte aus zwei Digitalfunknetzen von Energieversorgungsunternehmen (EVU) aus dem Süden und Südwesten Deutschlands bekommen. Sie zeigen wie die EVUs ihre Erzeugungsanlagen über Funk steuern. Diese Netze basieren auf dem Terrestrial Trunked Radio (TETRA)-Standard.

Dabei fielen gleich mehrere gravierende Schwachstellen auf:

- Die TETRA-Digitalfunknetze der beiden EVUs nutzen keine Verschlüsselung.
- Das verwendete Fernwirkungsprotokoll zur Steuerung der Energieerzeugungsanlagen ist ein gängiger Industriestandard und frei zugänglich.
- Die technischen Details zur konkreten Umsetzung (wie Anschlussbelegung von Schaltelementen und deren Zuordnung im Steuerungsprotokoll) sind auf den Internetseiten der EVUs gut dokumentiert.

Was ist TETRA-Digitalfunk-Technik?

Ab Mitte der 1990er Jahre entwickelte sich der TETRA zu einer modernen Alternative zum analogen Bündelfunk. Firmen und Behörden können bei der Bundesnetzagentur die Nutzung eines TETRA-Digitalfunknetzes beantragen. Die Antragstellenden erhalten bei Zuteilung eine eigene Funknetz-Kennung sowie eine Frequenzbereichszuweisung. Die Liste der über 300 Zuteilungen wird von der Bundesnetzagentur öffentlich gepflegt. [2] Die zugeteilte Frequenz liegt gemäß den „Verwaltungsvorschriften für Frequenzzuteilungen im schmalbandigen Bündelfunk (VVBüfu)“ im Bereich von 410–420 MHz (Uplink, also Mobilgerät zur Basisstation) und 420–430 MHz (Downlink, also Basisstation zu Mobilgerät). [3]

Technisch besteht die Möglichkeit, die Luftschnittstelle (also die Verbindung zwischen Mobilgerät und Basisstation)

- gar nicht zu verschlüsseln („Class 1“)
- mit einem statischen Schlüssel zu verschlüsseln („Class 2“)

- mittels dynamischen Schlüssel zu verschlüsseln („Class 3“)

Eine obligatorische Verschlüsselung im TETRA-Digitalfunk-Standard gibt es somit nicht. [4]

Unabhängig von der Verschlüsselung der Luftschnittstelle haben die Betreibenden des Funknetzes ferner die Möglichkeit, eine Ende-zu-Ende-Verschlüsselung zu verwenden. Diese ist technisch unabhängig vom TETRA-Standard, denn die so verschlüsselten Daten werden transparent durchgereicht. Die Ende-zu-Ende-Verschlüsselung ist von den Betreibenden des Funknetzes somit separat in den Endgeräten zu implementieren.

Das digitale Funknetz für alle „Behörden und Organisationen mit Sicherheitsaufgaben“ (BOS-Digitalfunk) basiert ebenfalls auf dem TETRA-Digitalfunk-Standard. Hier kommen sowohl die dynamische Verschlüsselung der Luftschnittstelle, als auch die zusätzliche Ende-zu-Ende-Verschlüsselung zum Einsatz. Mit diesen Maßnahmen kann der BOS-Digitalfunk als ausreichend abhör- und manipulationssicher eingestuft werden. Denn durch den dynamisch wechselnden Schlüssel werden auch Replay-Attacken, also das Wiederaussenden eines vorher aufgezeichneten Funksignals, praktisch unmöglich gemacht. Auch wenn Angreifende Zugriff auf die Basisstationen selber oder die Vernetzung der Basisstationen untereinander hätten, wäre die Kommunikation noch gegen Mitlesen gesichert. Dies ist durch die Ende-zu-Ende-Verschlüsselung sichergestellt.

Beispiel 1: Fernwirktechnik der EVUs

Nach Aussage der Hinweisgebenden sind die TETRA-Digitalfunknetze der beiden EVUs auch „zig Kilometer“ außerhalb der eigentlichen Versorgungsgebiete empfangbar. Es reicht „ein halber Meter Draht auf der Fensterbank“ als Antenne. Auf eine Verschlüsselung wird in beiden Funknetzen betreiberseitig komplett verzichtet.

Laut Website der betroffenen EVUs kommt TETRA-Digitalfunk zur Fernsteuerung für Photovoltaik-Anlagen bis 100 kW zum Einsatz. Verwendet wird dazu das Kommunikationsprotokoll IEC 60870-5-101. [5] Es dient als allgemeines Übertragungsprotokoll zwischen den (Netz-)Leitsystemen und den Fernbedienungs-Terminals.

Die Hobby-Funkenden zeigen, dass ein Funkempfänger für etwa 30 €, [6] freie Software [7] und ein betagtes Laptop mit Linux-Betriebssystem für den Empfang ausreichen.



Funkempfänger für TETRA-Empfang
(Florian Fuchs, CC-BY-SA 3.0)

Damit können der Sprechfunk und die Kurznachrichten im unverschlüsselten TETRA-Digitalfunk einfach aufgezeichnet werden.

Die mitgeschnittenen Textnachrichten der beiden Funknetze enthalten tatsächlich in Klartext die typische Rahmen-Struktur des IEC-60870-5-101-Protokolls. Mittels frei verfügbarer Software wie Wireshark [8] und passender Erweiterungen [9] ist es leicht möglich die Steuerungsprotokolle zu analysieren und für Menschen lesbar aufzubereiten.

Die beiden EVUs stellten auf Ihrer Website auch sogenannte „Musterdatenmodelle“ bereit.

Aus diesen geht die exakte Zuordnung der Fernwirk-Telegramme auf die jeweilige Funktion hervor, wie zum Beispiel

- Schalten von Lasttrennschaltern, um z.B. Versorgungsnetze, Erzeuger oder Verbraucher ein- und auszuschalten
- Freigabesignale zur Drosselung der Wirkleistungseinspeisung auf die definierten Sollwerte wie 0 % beziehungsweise 30 % / 60 % / 100 %
- Rückmeldung der Freigabesignale, also ob z.B. ein angeschlossener Verbraucher tatsächlich die Freigabe zum Einschalten erhalten hat

Zudem ist die eingesetzte Hardware dokumentiert. Also die konkret verwendeten digitalen TETRA-Modems und die genaue Verdrahtung der Schaltausgänge und Sensoreingänge der Modems mit den Steuereingängen und Schaltausgängen der Wechselrichter der Energieerzeugungs-Anlagen.

Insgesamt ist so im Detail beschrieben, mit welchen TETRA-Kurznachrichten die Steuereingänge und Lasttrennschalter der Energieerzeugungs-Anlagen angesteuert werden können. Auch die Status-Rückmeldung der Energieerzeugungs-Anlagen an das Netz-Leitsystem ist exakt dokumentiert.

Nur Mithören tut doch keinem weh?

Für einen Angriff auf die Fernwirktechnik liegen dadurch alle relevanten Informationen vor: Durch die frei zugänglichen Informationen im Internet und durch passives Mitschneiden der unverschlüsselten TETRA-Kurznachrichten. Dazu zählen vor allem die Steuerbefehle aus dem Netzleitsystem zur Erzeugungsanlage, aber auch die Status-Rückmeldungen in Gegenrichtung.

Mit einem Aufwand von unter 200 EUR [10] wäre es leicht möglich gewesen in die Steuerung der Energieerzeugungs-Anlagen aktiv einzugreifen. Die Sende- und Empfangsanlagen dafür sind frei verkäuflich.

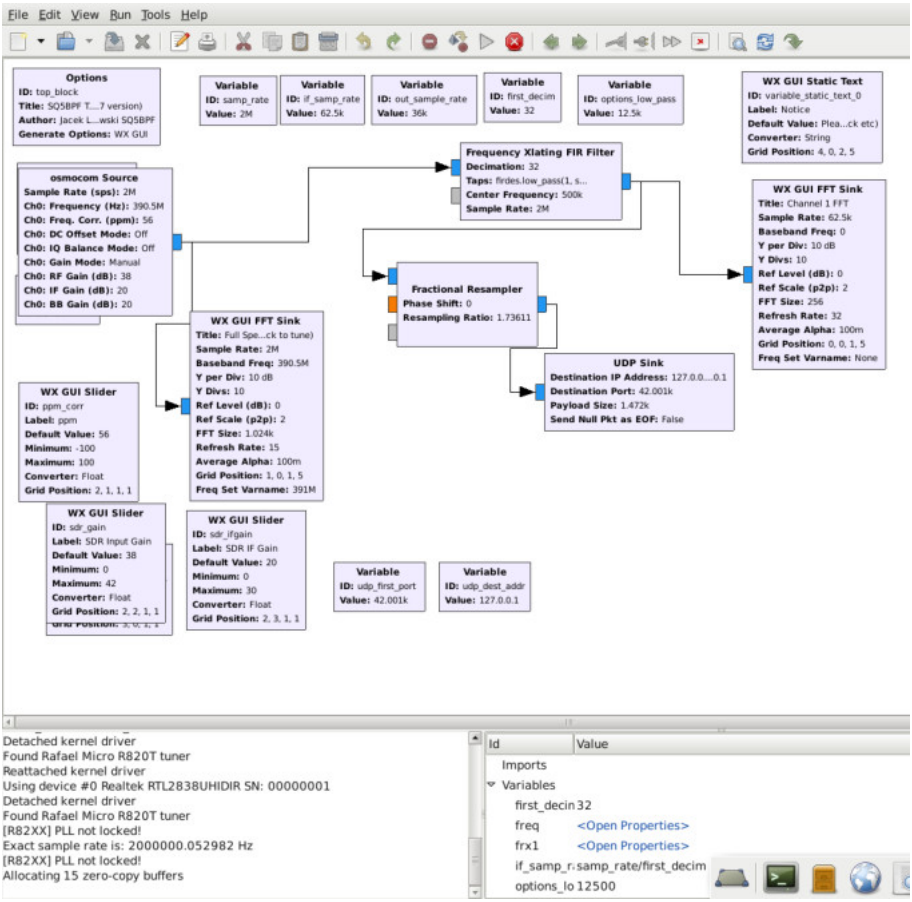
So hätten falsche Steuerbefehle an die Energieerzeugungs-Anlagen gesendet werden können, oder falsche Status-Rückmeldungen an die Netz-Leitstelle. Einzige Voraussetzung: Angreifende hätten sich innerhalb der Reichweite des TETRA-Digitalfunknetzes aufhalten müssen.

Im schlimmsten Fall hätten falsche Steuerbefehle an die Energieerzeugungsanlagen zu negativen Rückwirkungen auf das Stromnetz in der Region führen können: Das konzertierte Ab- und Einschalten von vielen Erzeugungsanlagen hätte zu spürbaren Spannungsschwankungen im Stromnetz geführt. Im Extremfall hätten so Notabschaltungen anderer Erzeugungsanlagen oder energieintensiver Maschinen durch das EVU provoziert werden können. Energieeinspeisende hätte für die Zeit der Notabschaltung auf die Einspeisevergütung verzichten müssen. Betreibende größerer Maschinen und Anlagen hätten aufgrund zeitweiser Abschaltung Betriebseinschränkungen hinnehmen müssen.

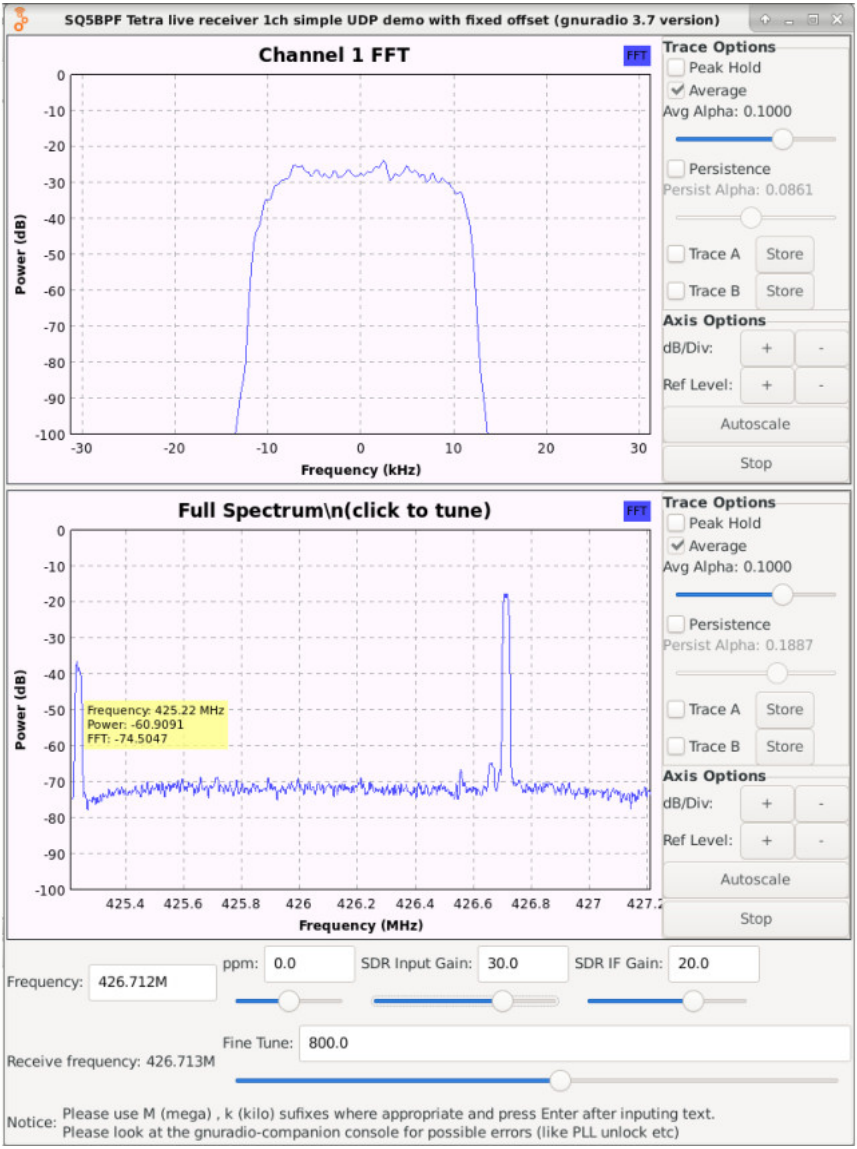
Falsche Statusrückmeldungen an das Leitsystem hätten zu falschen Regeleingriffen im Stromnetz führen können. Das Leitsystem hätte auf den falsch signalisierten Betriebszustand von Energieerzeugungsanlagen mit nicht notwendigen Eingriffen ins Stromnetz reagiert. Zum Beispiel wären Speicherkraftwerke aktiviert oder energieintensive Wärmepumpen abgeschaltet worden ohne technische Notwendigkeit.

Eines der EVU gab an, dass über 7.000 Energieerzeugungsanlagen und Lastschalter über sein TETRA-Netz angesteuert werden.

Doch so weit gingen die Hobby-Funkenden nicht. Der Sachverhalt wurde ausreichend dokumentiert und an das CERT-Bund (Computer Emergency Response Team des Bundes) im Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet. Dafür steht beim BSI ein geeignetes Meldeformular zu Verfügung. [11] Es erlaubt auch ausdrücklich eine anonyme Meldung. Außerdem wurde mit dem BSI „responsible disclosure“ vereinbart: Erst drei Monate nach der Benachrichtigung der betroffenen Unternehmen durch das BSI durfte die erste öffentliche Stellungnahme der AG KRITIS zu der Sicherheitslücke erfolgen. Damit sollte den Betroffenen genug Zeit für eine technische Abhilfe zur Verfügung stehen.



Software-definierter Empfänger als Datenquelle für den TETRA-Live-Monitor „TELIVE“ [7], eingestellt auf das Signal eines TETRA-Digitalfunknetzes (Teil 1)



Software-definierter Empfänger als Datenquelle für den TETRA-Live-Monitor „TELIVE“ [7], eingestellt auf das Signal eines TETRA-Digitalfunknetzes (Teil 2)

Beispiel 2: Öffentlicher Personennahverkehr (ÖPNV)

Ein weiterer Hinweis betrifft das TETRA-Digitalfunknetz eines Nahverkehrsunternehmens. Hier liegen Sprechfunkmitschnitte vor, die inhaltlich keinerlei Bezug zum ÖPNV haben. Der Inhalt lässt eher auf behördliche Nutzende schließen.

Auf den ersten Blick würde man meinen das Funknetz eines ÖPNV-Unternehmens würde nur für die Kommunikation zwischen Zentrale, Fahrpersonal, Anzeigetafeln und Ticketverkaufsgeräten verwendet werden. Doch das Funknetz deckt das räumlich sehr ausgedehnte Tarifgebiet ab. Aus wirtschaftlicher Sicht läge es nahe das Netz auch noch anderweitig zu nutzen als nur für ÖPNV-relevante Kommunikation.

Eine Anfrage nach dem Informationsfreiheitsgesetz (IFG) an eine andere Nahverkehrsgesellschaft, den Rhein-Neckar-Verkehrsverbund (RNV), bestärkt diese Vermutung: Das Funknetz wird dort „intern für Busse, Bahnen, Handfunkgeräte sowie Fahrgastinfosysteme“ verwendet. Zum anderen kommt es aber auch bei „externen“ Nutzenden zum Einsatz, wie „Ordnungsdienste, Stadtentwässerung, Chemiefabrik“. [12]

Laut Werbe-Flyer wird das Funknetz außerdem von Energieversorgungsunternehmen und Sicherheitsfirmen genutzt und nicht zuletzt für die unternehmenseigenen Gleichrichterunterwerke und Oberleitungsschalteinrichtungen. [13]

Ob dieses Funknetz tatsächlich Verschlüsselung einsetzt oder nicht, das wird im Werbe-Flyer nicht erwähnt. Dies war auch nicht Teil der IFG-Anfrage. Die Auskunft dazu wäre aus Sicherheitsgründen vermutlich auch abgelehnt worden.

Mitglieder der AG KRITIS haben in den vergangenen Jahren etliche öffentlich-rechtliche Betreiberorganisationen von TETRA-Digitalfunknetzen auf Grundlage des IFG über die Plattform fragdenstaat.de befragt. Die Anfragen betrafen die das Funknetz nutzenden Organisationen, die Anzahl der Endgeräte, die geographische Abdeckung des Funknetzes und administrative Aspekte. Die Antworten dazu sind auf fragdenstaat.de öffentlich zugänglich. [14]

Was bleibt?

Die eingangs erwähnte Liste „Zuteilungen TETRA-Netzkennungen (ITSI-Blocks)“ der Bundesnetzagentur [2] zeigt über 300 Zuweisungen von TETRA-Digitalfunknetzen an Unternehmen, Einrichtungen und Behörden. Vertreten sind Nutzende aus verschiedenen KRITIS-Sektoren und der Privatwirtschaft wie:

- Energieversorgungsunternehmen und Stadtwerke
- Betreibende kerntechnischer Anlagen
- ÖPNV-Anbietende
- Kliniken
- Flughäfen
- Justizvollzugsanstalten und Justizbehörden
- Zentralbanken
- Forschungseinrichtungen
- große Industriebetriebe

Die „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ (BSI-Kritisverordnung – BSI-KritisV) [15] reguliert eigentlich welche Betreibenden technischer Infrastrukturen ihre Anlagen besonders kontrollieren und physisch schützen müssen. Dazu werden Schwellenwerte vorgegeben, die definieren ab wann eine technische Infrastruktur (zum Beispiel eine Stromerzeugungsanla-

ge) überhaupt als kritische Infrastruktur einzustufen ist.

Insbesondere bei technischen Infrastrukturen unterhalb dieser Schwellenwerte obliegt es den Betreibenden selber wie ihre Anlagen kontrolliert und physisch geschützt werden.

Durch individuelle Fehleinschätzungen der privaten Betreibenden entstehen so Sicherheitslücken, wie die obigen Beispiele zeigen.

Über die Sicherheit der bei der Bundesnetzagentur gelisteten TETRA-Digitalfunknetze ist aktuell nur wenig bekannt. Ob es sich bei den oben gezeigten Sicherheitslücken um Einzelfälle handelt kann aus Sicht der AG KRITIS nicht abschließend bewertet werden. Es ist jedoch davon auszugehen, dass, schlicht auf Grund der Möglichkeit und Legitimität TETRA unverschlüsselt zu betreiben, dies auch noch in weiteren Funknetzen so praktiziert wird.

Ein pikantes Detail aus den Beobachtungen der Hobby-Funkenden: In einem der beobachteten Funknetze war der über Funk ausgesendete Status der Luftschnittstellenverschlüsselung zwar auf „aktiv“ gesetzt. Tatsächlich erfolgte die Übertragung jedoch unverschlüsselt. In der Dokumentation der verwendeten TETRA-Dekodier-Software heißt es dazu:

„Question: tetra-rx reports Air Encryption:1, does this mean that all is encrypted? Answer: No, this means that someone has paid money for the encryption license for their TETRA infrastructure. To use encryption each radio needs to have encryption enabled too, which also costs. So probably there will still be some radios (which are not used for secret communications), without encryption.“

„Rechtlicher Rahmen“

In § 5 des „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien“ (TTDSG) ist das Abhörverbot geregelt. So heißt es in Absatz 1: „Mit einer Funkanlage dürfen nur solche Nachrichten abgehört oder in vergleichbarer Weise zur Kenntnis genommen werden, die für den Betreiber der Funkanlage, für Funkamateure […], für die Allgemeinheit oder für einen unbestimmten Personenkreis bestimmt sind.“ Gemäß § 27 TTDSG droht hier eine Freiheitsstrafe bis zu zwei Jahren.

Für das Betreiben einer Funkanlage auf Frequenzen ohne Genehmigung und Zuteilung der Frequenz durch die Bundesnetzagentur drohen Bußgelder gemäß § 228 des Telekommunikationsgesetz in Höhe von bis zu 500.000 €.

Außerdem sanktioniert § 316b des Strafgesetzbuchs die Störung von Energieerzeugungsanlagen mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe.

Es drohen also empfindliche strafrechtliche Konsequenzen, sowohl beim passiven Abhören und erst recht beim aktiven Eingriff in fremde Funknetze.

Auch im europäischen Ausland gibt es ähnliche gesetzliche Regelungen. Als Beispiel sei hier der Fall Dejan Ornig aus Slowenien angeführt. [16] Dejan Ornig hatte die fehlende Verschlüsselung beim TETRA-Digitalfunknetz der Sicherheitsbehörden seines Landes aufgedeckt und wurde zu 15 Monaten auf Bewährung verurteilt.

Aufgrund der eindeutigen strafrechtlichen Situation müssen wir eindringlich davor warnen, TETRA-Digitalfunknetze selber abzuhören.

Nicht ganz „responsible disclosure“

Die Sicherheitslücke der fehlenden Verschlüsselung in den TETRA-Digitalfunknetzen der beiden EVUs wurde dem CERT-Bund gemeldet. Dieses hat die beiden betroffenen Unternehmen informiert. Außerdem sind zusätzlich alle beim BSI registrierten KRITIS-Betreiber

mittels Traffic Light Protokoll (TLP) unterrichtet worden. Das TLP – zu Deutsch etwa „Ampel-Protokoll“ – ist eine standardisierte Vereinbarung zum Austausch von schutzwürdigen Informationen. Seitdem sind mehr als drei Monate vergangen.

Eine direkte Rückmeldung der betroffenen EVUs an die Hinweisgebenden gab es bis zur Drucklegung nicht. Aufgrund des strafbewehrten Abhörens kann die AG KRITIS auch nicht nachprüfen, ob die betroffenen TETRA-Digitalfunknetze mittlerweile Verschlüsselung nutzen oder die Schwachstelle noch weiterhin ausgenutzt werden könnte.

Wir haben uns deshalb dazu entschieden die Namen der beiden EVUs nicht zu nennen.



Forderungen der AG KRITIS

- Alle öffentlich zugänglichen, digitalen Schnittstellen im Bereich der kritischen Infrastruktur – insbesondere Digitalfunknetze – müssen Verschlüsselung nutzen.
- Die Sicherheitsanforderungen an kritische Infrastrukturen müssen endlich bundesweit einheitlich geregelt werden, beispielsweise in einem KRITIS-Dachgesetz. Denn bundesweit geltende Sicherheitsstandards und gesetzliche Vorgaben gibt es bislang nicht.
- Es muss verbindliche Sicherheitsaudits für ausnahmslos alle Betreibenden technischer Infrastruktur geben. Auch für jene, welche die Schwellenwerte der „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ (BSI-Kritisverordnung – BSI-KritisV) unterschreiten.

Referenzen

[1] Panorama 3: „Kritische Infrastruktur: Wie leicht Ampeln manipuliert werden können“ (2022), https://www.ndr.de/fernsehen/sendungen/panorama3/ampeln120.html

[2] Bundesnetzagentur: „Liste der zugeteilten TETRA Mobilen Netzkennungen“ (2023), https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/TechnischeNummern/ITSI/ITSI_zuget_Rufnr.pdf

[3] Bundesnetzagentur: „Verwaltungsvorschriften für Frequenzzuteilungen im schmalbandigen Bündelfunk (VVBüfu)“ (2021), https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Verwaltungsvorschriften/VVBuefu.pdf

[4] European Telecommunications Standards Institute: „ETSI TS 100 392-7 V4.1.1 Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security“ (2022), https://www.etsi.org/deliver/etsi_ts/100300_100399/10039207/04.01.01_60/ts_10039207v040101p.pdf

[5] International Electrotechnical Commission: „IEC 60870-5-101:2003+AMD1:2015 CSV Consolidated version“ (2015), https://webstore.iec.ch/preview/info_iec60870-5-101%7Bed2.1%7Den.pdf

[6] RTL-SDR Blog: „Buy RTL-SDR Dongles (RTL2832U)“, https://www.rtl-sdr.com/buy-rtl-sdr-dvb-t-dongles/

[7] Jacek Lipkowski: „telive – Tetra Live Monitor“, https://github.com/sq5bpf/telive

[8] Wireshark: „The world’s most popular network protocol analyzer“,

https://www.wireshark.org/
[9] Michael Zhang: „iec101-103-selcmd_dissectors“, https://github.com/michaelxzhang/iec101-103-selcmd_dissectors
[10] Wikipedia: „List of software-defined radios“, https://en.wikipedia.org/wiki/List_of_software-defined_radios
[11] CERT-Bund: „Schwachstellenmeldung via Online-Formular“, https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/Schwachstellenmeldungen/Schwachstellenmeldungen_node.html
[12] Frag den Staat: „TETRA-Digitalfunk-Netz der Rhein-Neckar-Verkehr GmbH“ (2019), https://fragdenstaat.de/a/169280
[13] Rhein-Neckar-Verkehr GmbH: „Digitalfunknetz Rhein-Neckar im Einsatz für Ihr Unternehmen“ (2018), https://www.rnv-online.de/media/rnv-online.de/Unternehmen/Digitalfunk/Flyer_Digitalfunknetz.pdf
[14] Frag den Staat: „Anfragen zu *TETRA-Digitalfunk-Netz*“, https://fragdenstaat.de/anfragen/?q=TETRA-Digitalfunk-Netz
[15] Gesetze im Internet: „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ (2023), https://www.gesetze-im-internet.de/bsi-kritisv/
[16] Pierluigi Paganini: „Slovenian hacker who reported issues in Tetra Protocol gets prison sentence“ (2016), https://securityaffairs.co/47579/hacking/hacking-tetra-protocol.html



Die AG KRITIS ist unabhängig von Staat und Wirtschaft, sie ist kein Unternehmen oder Wirtschaftsverband. Wir sind etwa 42 aktive Fachleute, alle beruflich in kritischen Infrastrukturen unterwegs. Das Ziel unserer Arbeitsgruppe ist die Versorgungssicherheit der Bevölkerung zu erhöhen. Dabei wollen wir unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der IT-Sicherheit kooperativ mit allen Beteiligten herbeiführen. Unsere öffentlichen Stellungnahmen betreffen Gesetzesentwürfe in den Bereichen IT-Sicherheit, zur Technik der Behörden und Organisationen mit Sicherheitsaufgaben und zur Warnung der Bevölkerung im Katastrophenfall. Weitere Informationen gibt es unter https://ag.kritis.info/

Exzellente Symbiose!



TIKES
ATTENTION

Der ultimative New-Age-Eso-Sticker-Selbstfindungs-Test

von clx, kitsune, manu, myri und smettbo

Hast du dich schon mal gefragt warum auf deinem Obst Aufkleber sind? Oder warum es nicht mehr sind? Vielleicht knibbelst du aber auch gerne Preisschilder ab oder überklebst deine Webcam dreifach mit Glitzerstickern? Wir haben uns tief mit der Psychologie hinter dem Kleber beschäftigt und einen präzisen Test entwickelt, der dir sagt wie du klebst.

Hier die Spielregeln: Du kontemplierst hart über die Frage, und suchst dir die Antwort aus, die tief in deiner Seele liegt (wird schon eine von den angegebenen sein). Dann guckst du, was dahinter für griechische Zeichen stehen und machst für jedes Zeichen in den Matrizen einen Strich. Es gibt natürlich zwei Matrizen, weil wir in der Post-Bauhaus-Zeit Form und Content getrennt abfragen. Am Ende zählst du die Striche und jeweils da wo die meisten sind findest du die zutreffende Beschreibung auf deinen Stickarakter.

Form-Typ	
α	
β	
γ	
δ	
ε	

Content-Typ	
ω	
ψ	
χ	
ϕ	
υ	

Fragen

Da vorn gibts ne volle Kuchentheke!

- Ich kann mich nicht entscheiden und nehm am Ende keinen. — $\psi\,\delta$
- Ich kann mich nicht entscheiden und nehm am Ende eins von jedem. — $\upsilon\,\phi\,\gamma$
- Ich greife mir das erstbeste Stück und gehe weiter. — $\beta\,\varepsilon$
- Ist hier was vegan? — $\chi\,\alpha$
- Ich mag gar keinen Süßkram. — ω

Dein Kleiderschrank enthält:

- Die Pullis der letzten CCC-Veranstaltungen. — $\phi\,\beta\,\varepsilon$
- Auf jeden Fall ohne Label. — $\omega\,\delta$
- Ich kauf nur Second Hand. — $\psi\,\alpha$
- Alles in Farbe und bunt! — $\chi\,\gamma$
- Moment, ich muss eben wühlen. — υ

Eine Partei verschenkt Kugelschreiber in der Innenstadt.

- Cool! Gratis Kulis! — $\upsilon\,\phi\,\beta$
- Danke, ich hab schon einen. — $\chi\,\omega\,\delta$
- Wenn die anderen sich einen holen, nehm ich halt auch einen. — $\psi\,\gamma\,\varepsilon$
- Welche Partei ist das? — α

Wonach ist dein Gewürzregal sortiert?

- Farbe. — $\chi\,\delta$
- Haltbarkeitsdatum. — $\omega\,\alpha$
- Alphabetisch. — $\phi\,\beta$
- Platz. — $\psi\,\varepsilon$
- Sortiert? — $\upsilon\,\gamma$

Oh ein Etikettiergerät! Ich beschrifte mal eben…

- …meine USB Ports! — $\omega\,\beta\,\delta$
- …mein Gewürzregal! — $\psi\,\alpha$
- …das Etikettiergerät! — χ
- …all the things! — $\upsilon\,\phi$
- …deine Mutter! — $\gamma\,\varepsilon$

Heute Solikonzert!

- Mal schaun, ob meine Gang Lust hat. — $\psi\,\gamma\,\varepsilon$
- Ich bin am Start! — υ
- Wer spielt denn? — $\phi\,\delta$
- Soli für was denn? — $\chi\,\alpha$
- Boah, keine Zeit. — $\omega\,\beta$

Was machst du mit den EasterHegg-Tassen?

- Das Tafelsilber? Ab in die Vitrine! — $\varphi\,\beta\,\varepsilon$
- Logo abkleben (oder einfach ein paar mal in die Spülmaschine). — $\chi\,\delta\,\alpha$
- Verschenken. — ψ
- Ist meine neue Blumenvase. — υ
- Oh, Mist, hab ich im K2 stehenlassen. — $\gamma\,\omega$

Wohnungsübergabe, deine Tapete is oll.

- Ich tapezier einfach drüber. — υ
- ich mach die Tapeten ab und streiche den Putz weiß. — $\chi\,\omega\,\delta$
- Es werden neue Tapeten. — $\varphi\,\beta$
- Ich hinterlass ne lebensgroße Message für die profitgeilen Vermieter*innen. — α
- Mir doch egal, scheiß auf die Kaution. — $\psi\,\gamma\,\varepsilon$

Dein Laptop wurde geklaut!

- C'est la vie, war versichert. — $\psi\,\beta$
- Ich werde Zeit brauchen, um den Stickerverlust zu verdauen. — $\varphi\,\varepsilon$
- Shit, meine Daten sind lost! — $\chi\,\delta$
- Shit, shit, war nicht verschlüsselt! — $\upsilon\,\gamma$
- Den hacke ich mir zurück! — $\omega\,\alpha$

Du entdeckst was Cooles/Nerdiges und…

- …alle sollten mehr davon erfahren! — $\chi\,\beta$
- …du bist zu schüchtern, um wem davon zu erzählen. — $\psi\,\delta\,\varepsilon$
- …klickst dich jetzt durch Foren. — $\varphi\,\alpha$
- …hab ich schon erwähnt, dass alle davon erfahren sollten? — $\upsilon\,\gamma$
- …das bleibt dein Geheimnis. — ω

Da findet ein Lötworkshop statt!

- Yippie! Ich bring mein Werkzeug. — $\upsilon\,\beta\,\varepsilon$
- Kein Interesse. — $\omega\,\delta$
- Ich löte nur funktionales, ne coole Wecker-Lampen-Wetter-Station zum Beispiel. — ψ
- Blinke-Tier-Badges, ich will sie alle! — $\varphi\,\gamma$
- Ich löte nur, was ich programmieren kann. — $\chi\,\alpha$

Deine Socken?

- Sind schwarz. — $\omega\delta$
- Regenbogen, Einhörner, Pizzastücke. — $\upsilon\beta\varepsilon$
- Von Oma gestrickt. — $\chi\psi$
- Was für Socken? — $\varphi\gamma$
- Haben die Farbe meiner Partei. — α

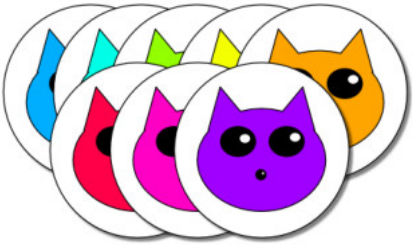
Dein Verkehrsmittel der Wahl?

- Yallah, immer Öffis. — $\omega\alpha$
- Ich hab ein neues schönes Auto, das will ich ausführen. — $\varphi\gamma$
- Circ, Lime, Tier, Omo, Voi, Jump, Bird (one of these is not like the others). — $\upsilon\beta$
- Fahrrad ist Liebe. — $\chi\delta$
- Füße, maximal 2. — $\psi\varepsilon$





Auflösung Form-Typ



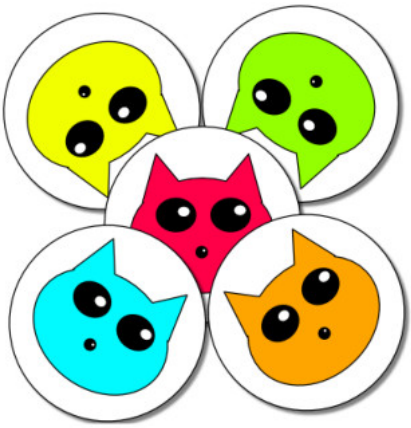
α – **Panini-Hamster**

Schon in der ersten Klasse hast du verstanden: Sticker in Sammelalben kleben ist ne feine Sache. Und weil du heute statt einem Sammelalbum ein Notebook hast, dient dir dein Notebook als Stickersammelfläche. Wenn das Notebook voll ist, dann sammelst du einfach weiter – in deiner privaten Sticker-Box. Aber du sammelst nicht beliebig jeden Sticker. Oh nein! Bei der Suche nach den Stickern, die noch in deiner Sammlung fehlen, bist du geduldig und ausdauernd. Du wühlst dich stundenlang durch Stickerboxen, um genau die Sticker zu finden, die noch in deiner Sammlung fehlen. Der Zeitaufwand spielt dabei eine untergeordnete Rolle. Da kann schon der ein oder andere Talk unter den Tisch fallen, aber das macht nichts. Deine Sammlung muss wachsen. Ab und zu kommt es dann schon mal vor, dass du einen speziellen Sticker in denen Vorräten nicht mehr findest. Das ist ziemlich ärgerlich, aber der nächste Wühltisch ist ja bei Chaosevents nie weit. Also: Weiter sammeln und die Früchte deiner Arbeit genießen, denn niemand hat so viele tolle Sticker wie du. Und wenn das Notebook vollgeklebt ist, dann muss im Zweifelsfall ein neues her.



β – **Sticker-Schichtkleber_in**

Sticker hattest du noch nie genug auf deinem Notebook. Und wenn es zu viele sind, dann klebst du einfach in Schichten. Der praktische Nebeneffekt ist doch: Mit den neuen Stickern lassen sich die Alten ganz toll überkleben. Da braucht es kein Abrubbeln. Und es ist dir auch ziemlich egal wie dick die Sticker-Schichten werden, denn Sticker auf dem Notebook wiegen ja nix. Für manche mag dein Ansatz vielleicht unübersichtlich wirken. Aber mal ganz ehrlich: Nur das Genie beherrscht das Chaos. Du hast noch genau den Überblick darüber, welcher Sticker wo klebt, und welcher Sticker was aussagt, selbst wenn nur noch eine kleine Ecke irgendwo rauslugt. Denn du behältst trotz allem den Überblick. Hinter allem steckt dein großer Masterplan. Dein System funktioniert, und du findest dich darin perfekt zurecht. Meistens. Oft. Manchmal? Egal. Also suchst du schon jetzt nach dem nächsten Sticker, mit dem du weiter überkleben kannst. Denn Schichten, das steht ja auch für Vielschichtigkeit.



γ – **Klebekurator_in**

Du bist organisiert, und planst bei Chaosevenst deinen Sticker-Crawl mit Bedacht. Nicht zu früh beim Event, und auch nicht zu spät. Gerade dann, wenn die Sticker-Boxen schon gefüllt, aber die Horden sie noch nicht geplündert haben. Denn du suchst den großen Fund. Das Schmuckstück. Das neue Center-Piece für deinen Rechner. Denn Sticker sind Kunst, und Kunst ist dein Ding. Großartiges Design erkennst du schon aus meilenweiter Entfernung. Mit einer Zielstrebigkeit, die seinesgleichen sucht, pickst du dir die schönsten, kreativsten Sticker aus jeder Wühlbox. Dabei nimmst du wirklich nur die Sticker mit, von denen du auch begeistert bist, denn nur die passen auch in deine Ausstellung. Du kannst auch gar nicht mehr an einer Hand abzählen, wie oft du schon auf dein Notebook angesprochen worden bist. Es erfüllt dich immer wieder mit Freude, wenn dir Menschen Komplimente zu deinen Stickern machen. Dann bist du dir auch nicht zu schade, die Betrachter durch deine kleine Ausstellung zu führen.



δ - **Minimalist_in**

Weniger ist mehr. Du fokussierst dich auf das wesentliche im Leben. Und deshalb reicht dir auch ein Sticker. Bewusst verzichtest du auf einen Stickerexzess, denn das wäre dir zu beliebig. Du beschränkst dich lieber auf ein Minimum und trennst dich von Unwichtigem. Aus Stickerwühlboxen nimmst du dir ein paar Aufklebe-Kandidaten mit, aber den einen, den du tatsächlich auf dein unbeflecktes Notebook klebst, den suchst du zu Hause nochmal unter Evaluation aller Pro- und Contra-Punkte genau aus. Den Rest verschenkst du, denn der wäre nur unnötiger Ballast. Du stellst dir dabei die großen Fragen des Lebens: Was sagt der Sticker über mich aus? Und passt der Sticker wirklich zu mir? Hat er die richtige Aussage? Immerhin spiegelt das Notebook deine Identität wider, da müssen die Sticker schon zu passen.



ε – **Abziehallergiker_in**

Es gibt einfach perfekte Design-Objekte. Der Eames Lounge Chair zum Beispiel. Oder dein Notebook. Bei der Auswahl deines Notebooks hast du nicht nur auf Arbeitsspeichergröße und Prozessorleistung geachtet, ganz im Gegenteil. Die schlanke, unverwechselbare, minimalistische Optik war entscheidender Kauffaktor. Und jetzt hütest du dich davor, die-

se Optik mit einem Sticker zu verschandeln. Du willst einfach nichts auf die polierte Metalloberfläche oder aufs matte schwarze Plastik kleben. Aber es ist ja nicht so, dass du Sticker doof fändest. Die sind schon hübsch und du pickst dir die Besten aus der Stickerbox. Als Trophäen trägst du sie nach einem langen Chaos-Event nach Hause. Aber auf dein Notebook klebst du sie nicht. Die Sticker liegen in deiner privaten Box – oder in der Cloud, und das ist auch gut so.

Auflösung Content-Typ



ω – Die/Der Politische

Du hast eine klare politische Meinung, und tust die auch gern kund. Man findet dich auf Demos, auch die ein oder andere Rede hast du vielleicht schon gehalten. Du bist energetisch und durchsetzungsstark, und das auf deine ganz eigene Art und Weise. Das alles spiegeln deine Sticker wider. Du suchst gezielt nach Stickern, die zu deiner politischen Einstellung und zu dir passen. Dafür durchwühlst du stundenlang die Stickerbox, weil politische Sticker sind oft nicht leicht zu finden. Der positive Nebeneffekt: Bei Wühltischen tummeln sich allerlei Menschen, die sich über die Sticker unterhalten. Und das ist der perfekte Ausgangspunkt für eine politische Diskussion.



ψ – Die/Der Nerdige

Deine Liebe zur Technik wird durch deine Liebe zu Stickern widergespiegelt. Besonders gerne hast du Sticker, die irgendwas mit Löten zu tun haben. Überhaupt findet man dich auf Chaosevents hauptsächlich in der Lötwerkstatt. Praktisch auch, dass Sticker mit Technikbezug dort besonders viel rumliegen. Um politische Sticker machst du einen Bogen, und wenn so ein Politik-Nerd versucht, dir einen politischen Sticker aufzudrücken, bedankst du dich ganz höflich, und suchst das Weite. Löten statt Töten ist das Maximum an politischem Slogan, auf den du dich einlässt.



χ – Die/Der Witzige

Das Leben ist schon ernst genug, deswegen willst du es mit Witzen lustiger machen. Die erzählst du gerne allen, die sie (nicht) hören wollen. Jetzt hast du das Potential von Stickern für dich entdeckt. Deren Humor ist unterschwelliger, und du erntest weniger genervte Blicke als für deine Wortwitze. Zur Not moddest du auch deine Sticker, schneidest mal was ab oder puzzelst was dazu. Auch die ein oder andere Stickerkombination funktioniert als gelebter Witz recht gut. Schon mal „No Link sharing“ über einen QR-Code geklebt? Super Sache! Wenn irgendwer dann deinen Witz kapiert,

erntest du ein lachendes Augenzwinkern. Und dann ist die Welt für dich in Ordnung.



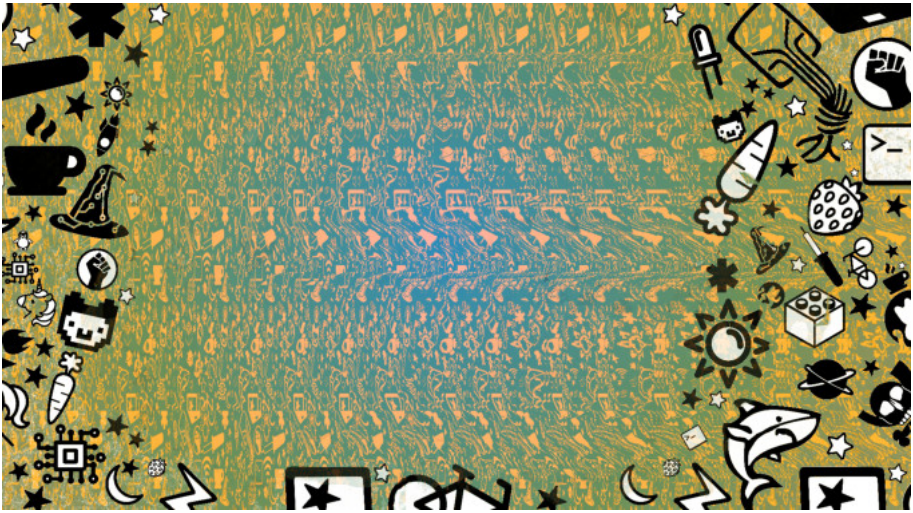
ϕ – Die/Der Ästhetische

Du achtest auf die äußere Erscheinung deines Rechners. Wenn du sie gestaltest, dann bis du kreativ. Sticker-Botschaften sind dabei für dich zweitrangig. Über Sticker, die im Chaos-Dunstkreis verteilt werden, muss man nicht kritisch nachdenken. Dir kommt es auf die Ästhetik an. Passen deine Sticker zusammen? Sind sie hübsch genug? Und stimmen Farben und Formen? Passt alles, dann nimmst du sie mit. Manche davon klebst du auf, und manche nicht. Aber selbst die, die du nicht aufklebst, holst du gerne immer mal wieder raus, um sie einfach nur zu betrachten.



υ – Die/Der Identifier

Das Chaos und sein Sonnensystem, das ist dein Metier. Du fühlst dich der Gruppe zugehörig, kennst deren Regeln in- und auswendig. Auf einem Chaosevent kannst du erstmal so richtig durchatmen, weil du weißt, dass du unter Menschen bist, die dich verstehen. Damit die anderen aus deiner Gruppe das auch erkennen, zeigst du deine Zugehörigkeit durch passende Sticker. Besonders stolz bis du auf den Sticker vom Chaosevent vor der Pandemie. Den hast du zufällig in deiner Cloud gefunden, ausgedruckt, und aufs neue Notebook geklebt. Denn, wie sollst du sonst zeigen, dass du schon so lange dabei bist?



Chaos für die Ohren

Ihr habt noch nicht genug Podcast-Abonnements in eurem Podcatcher? Wir haben redaktionsintern 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 cccfr	https://rdl.de/sendung/chaosradio-freiburg
Click! Clack! Hack! 0x17	https://clickclackhack.de/
damals (tm) ajuvo	https://damals-tm-podcast.de/
Datenkanal Offener Kanal Jena	https://datenkanal.org/
Datenleben Helena & Janine	https://www.datenleben.de
Hackerkultur 0x17	https://www.hacker-kultur.de/
haecksenwerk Haecksen	https://haecksen.org/
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 Tux Linux, OS, Netzkultur	https://radiotux.de/
Sibyllinische Neuigkeiten Chaospott	https://podcast.chaospott.de/
Sondersendung Sendezentrum	https://das-sendezentrum.de/sondersendung/

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


PIRATEN
WANN
AMNESTIE?

Demos Hacken – Nazis blockieren. Interview mit Anne Herpertz

Ein Interview von Smettbo mit Anne Herpertz

Anne Herpertz macht Politik auf Lokal- und Bundesebene. Im Interview erzählt sie uns von ihrer aktivistischen Tätigkeit in Dresden. Welchen Herausforderungen sieht sie sich gegenüber, wenn wir Neonazis aus der Dresdner Innenstadt heraushalten wollen. Warum es hilft, verhandlungssicher im Versammlungsrecht zu sein, wenn mit nur wenigen Gegendemonstranten eine Neonazi-Demo zum Umkehren bewegt werden soll. Vielleicht ist es dann sogar noch hilfreicher, die Polizei im Rücken zu haben. Im Interview teilt Anne nützliche Hinweise und Tipps.

Smettbo: *Hallo Anne, wie geht's dir? Gerade habt ihr ja in Dresden mal wieder einen riesigen Neonazi-Aufmarsch.*
Anne Herpertz: Das stimmt. Und nach der Demo ist vor der Demo. Heute Abend findet der nächste Aufmarsch statt. Da sind alle Pegida-Größen vor Ort. Pegida steht für Patriotische Europäer gegen die Islamisierung des Abendlandes. Wir haben uns die letzten Tage darauf vorbereitet und jetzt gerade sind schon die ersten Gegendemonstrant*innen da. Nach dem Interview mache ich mich auch gleich auf den Weg.

Smettbo: *Und gerade eben war der 13. Februar.*
Anne Herpertz: Genau. Am 13. Februar finden jedes Jahr noch die größten Neonazi-Aufmärsche Europas in Dresden statt. Das ist eine eigene Hausnummer, da reisen die Neonazis aus Ungarn, Spanien und anderen Ländern an. Das Ziel der Anreisenden ist, dem Opfermythos der unschuldigen Stadt Dresden zu huldigen. Der 13. Februar wird von den Neonazis dazu instrumentalisiert, Dresden als unschuldige Kunst- und Kulturstadt darzustellen und die Opferzahlen hoch zu stilisieren. In Dresden gab es massenweise Deportationen, es gab Kriegsindustrie. Dresden war eine der ersten Städte, die Bücher verbrannt hat. Es gab das erste Museum über entartete Kunst in Dresden. Das Ziel der Neonazis am 13. Februar aber ist die Täter-Opfer-Umkehr. Das Narrativ der Demonstrierenden ist, dass die arme Zivilbevölkerung bombardiert wurde, die ja gar nichts für diesen Krieg konnte. Und auch in der städtischen Erinnerungskultur sehen wir von offizieller Seite ein riesiges Problem. Es ist deswegen dringend notwendig, dass wir unser Gedenken überdenken. Eigentlich müsste man sagen, Gedenken abschaffen. Alles was mit dem Gedenken an die Personen verknüpft ist, die bombardiert wurden, trägt in Dresden immer etwas Geschichtsrevisionismus in sich. Es findet eine Täter-Opfer Umkehr statt. Es wird nicht mehr den Opfern der Nationalsozialisten gedacht, sondern die Täter werden als Opfer dargestellt. Dieses Jahr war es besonders schlimm. Im offiziellen Aufruf der Menschenkette wird noch nicht mal erwähnt, dass dieser Tag von Neonazis instrumentalisiert wird. Es wurde nichts zum antifaschistischen Gegenprotest gesagt. Das ist ein Rückschritt. Die Menschenkette wurde mal gegründet, um symbolisch die Innenstadt zu schützen. Damals wurde von den Bürgern drei Reihen um die Synagoge gebildet. Da war die Aussage noch:

Wir schützen die Synagoge vor den Neonazis. Dieses Jahr gab es auch eine Menschenkette. Aber deren Motto war: "Frieden gemeinsam gestalten". Diese Änderung des Grundgedankens führt dazu, dass wir nicht mehr die deutsche Kriegsschuld und -verbrechen thematisieren. Sondern wir sagen, Krieg allgemein ist böse und führt zu Zerstörung. Das ist sehr problematisch.

Smettbo: *In Dresden seht ihr euch nicht nur den Neonazis, sondern auch anderen Gruppen gegenüber.*
Anne Herpertz: Dresden ist auch die Geburtsstadt von Pegida. Hinzu kommt die Querdenken-Bewegung. In Westdeutschland sind AfD, Pegida und Querdenker ja manchmal unterschiedliche Gruppierungen. In Dresden aber finden wir eine andere Situation vor. Hier verschwimmen die Grenzen. Das hat sich das letzte Jahr nochmal deutlicher gezeigt. So ergibt das ein echt schlimmes Gemisch, das jetzt auch noch mit Menschen in Kontakt kommt, die vorher keine Berührungspunkte mit Rechtsextremen hatten. Die Mutti, die Angst hat, dass ihr Kind unter der Maske erstickt, läuft jetzt mit stadtbekannten Neonazis zusammen auf der Demo. Das ist neu und ermöglicht rechten Strömungen mehr in die Mitte der Gesellschaft vorzudringen. Die Leute hinterfragen leider überhaupt nicht, mit wem sie da umherlaufen.

Smettbo: *Und die Menschen informieren sich nicht?*
Anne Herpertz: Eher weniger. Es gab auch ein recht aussagekräftige Interviews in den Öffentlich-Rechtlichen, wo Leute dazu befragt wurden, was sie darüber denken, dass sie mit Pegida und Co. auf die Straße gehen. Die haben geantwortet: Ja, wenn diese Gruppen für das gleiche Thema auf die Straße gehen, dann ist das doch in Ordnung. Es geht dann nur darum, dass ein gemeinsamer Feind da ist. Das ist für mich unbegreiflich, wie man das nicht verstehen kann, dass man neben Größen der Neonazi-Szene auf der Straße steht. Was wir auch sehen ist, dass die, die sonst nur bei Querdenken unterwegs waren, dann auch mal eben am 13. Februar einen Trauermarsch begleiten.

Smettbo: *Das ist ja auch ein historisches Phänomen, dass gerade Nationalsozialisten ihren Zugang zur Mitte der Gesellschaft über familienpolitische Themen suchen.*
Anne Herpertz: Themen wie die Corona-Pandemie werden instrumentalisiert. Da wurden alle eingesammelt, die gegen die Corona-Maßnahmen waren. Und das Gleiche sehen wir jetzt auch im Zuge des Überfalls von Russland auf die Ukraine. Die pro-putin'schen Kräfte finden Anschluss bei der AfD und Pegida, die solche Themen gern aufgreifen. Es ist auch super gefährlich, was Alice Schwarzer und Wagenknecht da treiben. Da wird jedes Thema vereinnahmt, das gegen die Regierung instrumentalisiert werden kann, um möglichst viele Menschen dazu zu motivieren, mit einem auf die Straße zu gehen. Aus deren Sicht ist das vielleicht strategisch klug, es macht nur halt extrem rechtes Gedankengut immer weiter anschlussfähig und bagatellisiert es auch. Wenn man Angst hat, dass das Kind geimpft wird, eine islamophobe Grundeinstellung hat, denkt die Ausländer machen alles kaputt und überfallen Frauen, dann sind es auch nur zwei, drei Schritte weiter zu Pegida. Gerade in Sachsen und Dresden ist es ein großes Problem, dass diese Inhalte für große Teile der Bevölkerung sehr anschlussfähig sind. Wir haben halt über 30% AfD-Wähler*innen in Sachsen.

Smettbo: *Und dem Allen steht ihr dann bei Gegenprotesten gegenüber.*

Anne Herpertz: Vor allem sind es Gegenproteste, bei denen die breite Zivilbevölkerung fehlt. Es sind immer die gleichen Gruppen und Personen, die die Gegenproteste organisieren. Die breite Mitte, also Familien etwa, beteiligt sich einfach weniger. In München sind bei Anti-Nazi-Protesten ganze Familien mit ihren Kinderwägen dabei, in Dresden sind es die typischen Leute aus der linken Szene. Es beteiligen sich auch Kirchen, das möchte ich sicher nicht klein reden. Aber vom organisatorischen Kern treffe ich immer die gleichen Menschen. Dresden hat fast 600 000 Einwohner*innen und dann stehen manchmal nur 100 Leute herum, die gegen Neonazis auf die Straße gehen. Der breiten Stadtgesellschaft ist es leider oft egal, was in ihrer Innenstadt geschieht. Das ist, glaube ich, ein besonderes Problem von Sachsen.



Portrait von Anne Herpertz.
(Anne Herpertz.)

Smettbo: *Welche Organisationen sind es denn, die sich an den Gegendemos beteiligen? Kirchen hast du ja schon erwähnt.*
Anne Herpertz: Das sind natürlich antifaschistische Initiativen. Aber auch Gewerkschaften und Parteien beteiligen sich, was ich extrem wichtig finde, weil Parteien eben gewisse Strukturen haben, die darauf ausgelegt sind, mehr Leute zu erreichen, als es antifaschistischen Gruppen möglich ist. Bei den Parteien sind es neben uns Piraten noch Die Linke, SPD, Grüne und auch Volt. Alles, was eben oftmals links-progressiv ist. Dann gibt es noch Initiativen, die sich für die Geflüchtetenhilfe einsetzen, wie etwa die Seebrücke Dresden. Leider bekommt man eine FDP oder CDU nur alle paar Jahre zu einer Demo. Uns ist auch bewusst, dass linke Gruppen mitunter ein Grund sein können, warum sich gerade nicht mehr Menschen aus der bürgerlichen Mitte anschließen. Da wird dann die Extremismustheorie mit dem berühmten Hufeisen herausgekramt. Argumente sind eben, es sei nur die Antifa da, warum sollten wir hingehen? Das stimmt aber nicht. Kirchen und Gewerkschaften sind dabei. Auch Mission Lifeline, die Seebrücke und die Universität Dresden - angetrieben durch engagierte studentische Initiativen - sind sehr aktiv mit dabei. Und trotzdem fehlt die breite Masse an Menschen.

Smettbo: *Sieht du hier auch eine Art Politikverdrossenheit der Menschen?*
Anne Herpertz: Ich würde es eher als eine Art beschreiben, Verantwortung von sich zu weisen. Im Sinne von: “Was betrifft es mich, dass hier Neonazis durch die Innenstadt laufen”. Das ist extrem fatal.

Smettbo: *Wie vielen Demonstranten seht ihr euch denn im Normalfall gegenüber?*

Anne Herpertz: Das kann man gar nicht so einfach sagen. Als Querdenken jeden Montag gelaufen ist, ist Pegida ein halbes Jahr nicht gelaufen, das zeigt auch gut den Zusammenhang zwischen den beiden Gruppen. Als dann Pegida mal wieder ein Comeback versucht hat, kamen 500 Leute zu denen und wir konnten 1500 mobilisieren. Das war eine positive Überraschung. Oft kann man sich nicht sicher sein, wie viele Menschen man mobilisieren kann. Es kann auch sein, dass man mit nur 50 Leuten herumsteht. Aber ganz unabhängig davon, wie viele Menschen da sind, gibt es ja einige kreative Maßnahmen, die man ergreifen kann.

Smettbo: *Aber ihr habt auch eure Demo-Strategie grundlegend geändert.*
Anne Herpertz: Die Personen von Querdenken hatten anfangs ihre eigenen Demonstrationen nicht angezeigt. Die Leute sind dann einfach marodierend durch die Stadt gelaufen und die Polizei hat zugesehen. Wir haben unsere Demonstration dann spontan angezeigt und konnten mit zehn Personen ganze Straßenzüge absperren. Das war der Game-Changer, dass wir unsere Blockaden von vorneherein angezeigt haben. Wir haben festgestellt, dass eine gewisse "Kooperation" mit der Polizei an dieser Stelle neue Spielräume eröffnen kann. Wir haben mit einem drei Meter Banner und nur zwei Leute an jeder Ecke eine ganze Straße dicht gemacht. Und da wir die einzige angezeigte Demonstration sind, dürfen wir das auch. Es ist schon eine wilde Erfahrung, die Polizei zum ersten Mal mit dem Rücken zu einem stehen zu haben. Sonst - vor allem in Sachsen - steht die Polizei oft mit dem Rücken zu Rechtsextremen, während der Gegenprotest kriminalisiert wird. Die Polizei muss in diesem Fall unsere Blockade schützen und blockiert damit letztlich Querdenken mit. Trotzdem ist und bleibt es natürlich eine schwierige Gemengelage, und man muss einfach situativ gucken, wie weit man gehen kann. Aber der ausschlaggebende Faktor ist, dass man seine Rechte durchsetzt und die Polizei einen dabei unterstützen muss.

Smettbo: *Ihr könnt dann aber von der Polizei beauflagt werden.*
Anne Herpertz: Es ist immer entsprechend der Situation vor Ort zu entscheiden, was man wie machen kann und wie man die Gegebenheiten für sich nutzen kann. Aber auch eine auf den Gehweg beauflagte Gegendemo kann viel bewirken.

Smettbo: *Und wie war das damals bei eurer ersten angezeigten Gegendemo?*
Anne Herpertz: Die Neonazis haben sich ja einfach die Straßen genommen. Und durch unsere Anzeige konnten wir die Polizei dazu bringen, die andere (unangezeigte) Demo zu regulieren. Stell dir vor 300 Menschen im schwarzen Block ziehen einfach so durch die Innenstadt. Keine Polizei würde das erlauben. Diese Versammlung würde festgesetzt und aufgelöst. Oder es müsste sich ein Versammlungsleiter finden, der mit der Polizei eine Route aushandelt. Und diese verharmlosend "Spaziergänge" genannten Demonstrationen von Querdenken konnten das machen. Die sind einfach durch die Stadt marodiert. Die Polizei ist hinterhergefahren und hat nichtmal den Anschein erweckt, eingreifen zu wollen. Aber dadurch, dass wir aufgekreuzt sind, und unsere Demo angezeigt haben, mussten sie das Polizeiaufgebot in die Höhe fahren und dann regulierend eingreifen. Die Polizei hat dann zu denen gesagt: Hey, ihr seid nicht angezeigt, ihr habt keine Versammlungsleitung, ihr bekommt jetzt diese Straße nicht. Das war ein großer Erfolg, den wir erzielen konnten.


NAZIS
WEGFLAUSCHEN
WIRR IST DAS VOLK.
Birds
aren't real.

Wer ist Anne Herpertz?



Anne Herpertz ist seit Juni 2022 Bundesvorsitzende der Piratenpartei Deutschland. Sie wuchs im Landkreis Meißen auf und wurde politisiert durch die rassistischen Proteste der NPD rund um die Jahre 2014-15. Seit 2017 ist sie bei der Piratenpartei, studiert Politikwissenschaft im Master und arbeitet an der Technischen Universität Dresden. Momentan ist sie gewählte Bezirksbeirätin in der Dresdner Neustadt. Neben der institutionellen Politik engagiert sie sich aktivistisch in der Dresdner Zivilgesellschaft und organisiert unter anderem Demos gegen Rechts.

Mastodon: @stillnotlovin@dresden.network
Twitter: @stillnotlovin
Instagram: @stillnotlovingreality

Smettbo: *Ist im Vorfeld bekannt, ob die Demonstration der Gegenseite angezeigt ist?*
Anne Herpertz: Das kann man notfalls vor Ort herausfinden. Dresden hat ein Versammlungsportal, wo Kundgebungen, die vorher angezeigt sind, draufstehen. Und spätestens vor Ort kann man das erfragen. Doch selbst wenn sie angezeigt sind, wissen wir meistens nicht, wie die Routen vor Ort sein werden. Deswegen sind unsere Demonstrationen dann spontane Versammlungen. Das ist auch der Grund, warum wir nicht mit Vorlauf anzeigen können, weil wir eben nicht wissen, wo die andere Gruppe ist. Das ist dann auch versammlungsrechtlich gedeckt, denn wir wissen ja nicht, wo wir hin müssen.

Smettbo: *Was passiert, wenn beide Demos angezeigt sind?*
Anne Herpertz: Dann kann man die Polizei dazu bewegen, die andere Demo einzuschränken. Das kann man aber nur machen, wenn die Kräfte vor Ort nicht ausgewogen sind. Etwa wenn es nur tausend Polizisten sind, aber drei oder viertausend Gegendemonstranten sind. Es soll in so einem Fall vermieden werden, dass die beiden Demos aufeinandertreffen. Die Polizei muss dann gegebenenfalls die Neonazis umlenken. Und das ist ja auch unser Ziel.

Smettbo: *Wurde eine Demonstration dann auch mal aufgelöst?*
Anne Herpertz: Das kam ein einziges Mal bei Querdenken vor. Ansonsten konnte man eben durch unsere Einschränkung und die polizeiliche Einschränkung die Querdenken-Demonstration leiten. Allerdings haben die Querdenker daraus gelernt, hatten dann irgendwann Versammlungsleitungen und haben die Sachen selbst angezeigt. Ab da wurde es schwieriger für uns, denn unser Vorteil war weg.

Smettbo: *Was ist das Ziel, wenn ihr die Demos umlenkt?*
Anne Herpertz: Die Demos sollen nicht die prominenten und vor allem auch geschichtsträchtigen Innenstadtplätze bekommen. Dort könnten sie auch mehr Menschen erreichen

als am Stadtrand. Gerade wenn man an Dresden denkt, ist es eben krass, dass Neonazis auf diese Plätze laufen dürfen. Denn eigentlich könnte die Versammlungsbehörde das untersagen. Das ist im sächsischen Versammlungsgesetz ausdrücklich für besondere Orte vorgesehen und liegt in deren Ermessensbereich. Eine Möglichkeit wäre etwa, die Demos an den Stadtrand zu beauflagen. Das wurde in anderen Städten gemacht, aber nicht in Dresden. Was man aber generell beim Umlenken beachten muss, ist, dass die Teilnehmenden der anderen Demo ja auch wieder weg können müssen. Wir hatten einmal die Situation in einer engen Häusergasse, wo die Querdenken-Demo hätte umkehren müssen. Es muss auch Wege geben können, wohin die andere Demo abfließen kann. Am 13. Februar konnten wir die Demo von Querdenken übrigens mit einer erfolgreichen Blockade durch über 1500 Personen von den geschichtsträchtigen Plätzen fernhalten. Deren Kundgebung musste dann an einem Skaterplatz stattfinden und wurde dann auch beendet.

Smettbo: *Um so etwas umsetzen zu können, müsst ihr recht sicher im Versammlungsrecht sein.*

Anne Herpertz: Ja, wir halten dazu auch Workshops ab. Wichtig ist zum Beispiel das Wording. Wir machen keine Verhinderungs-Blockaden. Wir machen Spontan-Demonstrationen, die das gestalterische Mittel des Sitzens verwenden. Auf Demonstrationen besteht Gestaltungsfreiheit, und da darf uns der Staat auch nicht wirklich einschränken. Das kann die Form eines Flashmobs haben, oder wir können uns eben hinsetzen. Oder man kann Banner nutzen. Die Frage ist an der Stelle auch: Wie weit geht die Versammlungsfreiheit und wo beginnt das Polizeigesetz? Hier machen wir viel Aufklärung. Viele wissen zum Beispiel nicht, dass wenn bei Demonstrationen keine Straftat passiert, die Polizei nicht mal die Versammlungsfläche betreten darf. Das Problem ist dann nur oft, dass die Polizeikräfte bis auf die höheren Führungsebenen nicht wissen, was sie dürfen und was nicht. Da gilt es dann, in Verhandlungen vor Ort auf den eigenen Rechten zu bestehen. Wir nutzen, was das Verhandlungsrecht uns gibt und gehen proaktiv auf die Polizei zu, um das Beste für uns herauszuschlagen. Wir wollen damit auch die Leute schützen, die auf unsere Demonstrationen gehen. Über all diese Monate haben wir es so geschafft, dass niemand der Teilnehmenden eine ID-Maßnahme bekam. Durch das Anzeigen der Demos bringen wir die Teilnehmenden in einen explizit legalen Rahmen. Es war für uns in dieser Form und Dynamik ein komplett neuer Ansatz. Das braucht auch sehr viel Koordination in der eigenen Gruppe.

Smettbo: *Inwiefern?*

Anne Herpertz: Es geht darum, dass nicht spontan unabgesprochene Aktionen passieren. Wir versetzen uns in die Polizei hinein und überlegen, wie wirkt das, wenn plötzlich zwanzig, dreißig Leute losrennen? Dann sind die sofort im Alarmmodus. Wir mischen uns ein, wenn Teilnehmende unserer Demos von Polizeikräften angesprochen werden und deeskalieren. Falls es auf unserer Seite Teilnehmende gibt, die eine Konfrontation mit der Polizei suchen, nehmen wir diese zurück, um unnötigen Stress zu vermeiden. Das braucht viel Vertrauen, viel Konsens, viel Koordination. Und das erreichen wir dadurch, dass wir verhandeln und den Leuten zeigen: durch die Verhandlungen schaffen wir es, die Repressionen zu minimieren. Wir haben mittlerweile mehrere Leute, die schon viele Erfahrungen haben im Verhandeln mit der Polizei. Sei es

bei Uneinigkeit die Vorgesetzten dazu zu holen oder die Polizist*innen auf unsere Rechte und ihre Pflichten hinzuweisen. Unser Ziel ist ein starkes Auftreten. Aber wie gesagt, das ist super situativ. Das hängt von den Einsatzkräften vor Ort ab, von den Örtlichkeiten, von der Aufstellung, von der Anzahl der Personen. Davon, wie schnell wir es von A nach B schaffen als Gruppe. Und es kann immer sein, dass Verhandlungen fehlschlagen.

Smettbo: *Wie schützt ihr auf den Demonstrationen denn eure Privatsphäre?*
Anne Herpertz: Da müsste man dann unterscheiden zwischen Menschen, die schon in der Öffentlichkeit stehen und Privatpersonen, die schützenswerter sind. Es gab genügend Listen von Neonazis, wo Privatpersonen drauf standen. Für Menschen, die schon in der Öffentlichkeit stehen, stellt sich die Sache etwas anders dar. Der Vorteil bei einer angezeigten Demonstration ist, dass nur ein begrenzter Personenkreis seine Identität preisgeben muss und alle anderen geschützt bleiben. Als Vorsitzende der Piratenpartei stehe in sowieso schon in der Öffentlichkeit. Ich persönlich habe auch schon wegen schwerer Körperverletzung als Zeuge vor Gericht gegen einen Neonazi ausgesagt. Der Zug ist abgefahren.

Smettbo: *Wie geht ihr mit rechten Streamer*innen um, die die Teilnehmenden abfilmen?*
Anne Herpertz: Das ist relativ einfach, wenn die Demo angezeigt ist. Diese Streamer*innen haben oft keinen Presseausweis und stören den Ablauf der Demo, da sie Menschen bedrängen. Das kann man der Polizei mitteilen. Zwar reagiert die Polizei manchmal komisch, so nach dem Motto: Ihr hasst uns doch als Polizei, und jetzt sollen wir hier Leute für euch wegräumen? Das hatten wir schon. Aber die Sache ist eben, das sind versammlungsrechtlich geschützte Demonstrationen, und es ist Aufgabe der Polizei, dann die Demo vor Übergriffen zu schützen.

Smettbo: *Was ist der Benefit, wenn Parteien bei der Demo anwesend sind?*
Anne Herpertz: Man hat einfach andere Möglichkeiten, wenn Parteien mit dabei sind. Wir schaffen MdLs und MdBs von der SPD, den LINKEN und Grünen heran, die sobald etwas mit der Polizei ist, daneben stehen. Marco Böhme zum Beispiel, Mitglied im sächsischen Landtag für die LINKE, ist durch seine jahrelange Aktivismus- und Demoerfahrung ein unglaublich selbstbewusster, proaktiver parlamentarischer Beobachter. Parteien haben auch einfach andere Ressourcen, auch was die Finanzierung angeht. Demos müssen ja auch finanziell unterstützt werden, und da können Parteien einen großen Vorteil bieten, weil sie gewisse Strukturen und Geld haben und öffentlich auftreten können. Ich wünsche mir, dass noch mehr anerkannt wird, was einem Parteien für diesen Zweck nutzen können.

Smettbo: *Welche Gesetze sind relevant? Also, was sollte man alles kennen?*
Anne Herpertz: Zum einen haben wir da das Grundgesetz. Jedem steht es frei sich unter freiem Himmel zu versammeln. Dann gibt es noch die Versammlungsgesetze, die jedes Land entwirft, und dann noch die Entscheidungen der lokalen Behörden. Dazu kommen noch die jeweiligen Polizeigesetze, die Tür und Tor für polizeiliche Eingriffe öffnen. Nach dem neuen sächsischen Polizeigesetz darf die Polizei zum Beispiel Funkmasten in kompletten Gebieten abstellen. Es wurde noch nicht genutzt, aber damit könnten sie die komplette Kommunikation der Demonstrierenden, aber auch von Unbeteiligten, unterbinden. Wichtig ist auch, dass rechtliche Fragen vor Ort oft Ausle-

gungssache sind. Dann ist man vielleicht im Recht, aber die Polizei sagt einem, du kommst hier nicht durch. Da spielt es auch eine große Rolle, ob die Demo vorher oder spontan angezeigt wurde. Zeigt man vorher an, muss auch die Route bekannt sein, was auch die Gefahr für Einschränkungen erhöht. Beim spontanen Anzeigen entscheidet die Polizei oft direkt über Beauflagungen. Am 13. Februar wurde die komplette Stadt abgegittert. Wir, als Gegendemonstration, haben dann schon Stunden vorher Platzverweise bekommen, was unseres Erachtens nicht rechtens ist. Wir wurden sogar rauseskortiert. Es haben aber trotzdem ein paar Leute geschafft, eine Straße spontan zu blockieren. Als diese Spontanblockade angezeigt war, musste jeder zu dieser Versammlung dürfen. Das ist auch ein Kniff. Gerade dort hat sich aber auch mal wieder die Willkür der Polizei gezeigt. Am 13. Februar war ich außerhalb des Korridors, aber nachdem diese Spontandemonstration angemeldet war, durfte ich eigentlich hin. Die erste Polizeisperre hat mich nicht durchgelassen, und auch deren Vorgesetzter nicht. Ich bin dann zur zweiten Polizeisperre gegangen, und habe mit denen gesprochen. Der Polizist sagte mir, wir müssten abwarten, wie sich die Lage entwickelt, was nicht rechtens ist, schließlich hat niemand eine Straftat begangen. Bei der dritten Polizeisperre bin ich plötzlich durchgekommen. Die Polizei entscheidet eben von Fall zu Fall darüber, was sie zulassen - was nicht okay ist. Das ist einfach Willkür vor Ort. Hierin kann man aber auch eine Chance sehen, denn das bedeutet auch, dass ich meine Rechte durchsetzen kann. Hilfreich ist dazu auch, dass man die individuellen Polizeikräfte ja für ihre Entscheidungen verantwortlich machen kann. Man kann sie nach ihrem Namen oder dem Namen der Einsatzleitung fragen und eine Dienstaufsichtsbeschwerde einreichen. Man darf auch immer eine Demonstration wieder verlassen, ohne mit Maßnahmen der Polizei rechnen zu müssen. Das wissen viele nicht. Wir müssen hier noch sehr viel Aufklärungsarbeit leisten, was die Menschen auf Demos alles dürfen. Sonst nutzt die Polizei diese Unwissenheit aus.

Smettbo: *Hast du schon mal eine Dienstaufsichtsbeschwerde gemacht?*
Anne Herpertz: Einmal ja. Da ist mir das Recht, eine Demo anzuzeigen, verwehrt worden. Man wollte mich nicht woanders hin beauflagen, etwa auf den Gehweg. Der hat einfach gesagt: ne, nehme ich nicht an. In dem Fall habe ich mit dem Justiziar der Piratenpartei dann eine Dienstaufsichtsbeschwerde eingereicht und natürlich haben sie sich rausgeredet. Aber die Vorgesetzten bekommen das auf den Tisch. Ich glaube nicht an Sinneswandel in der Polizei, weiß aber, dass sie den dadurch entstehenden Papierkram lieber vermeiden wollen. Es gab auf der Demo am 13. Februar aber auch noch den Fall, dass ein Anwalt aus unserem Legal Team jemanden angesprochen hatte, ob er als Anwalt die Person vertreten soll. Die Polizei hat ihn dann des Platzes verwiesen. Damit hat die Polizei ein Mandantenverhältnis gestört, was sie nicht darf. Der Anwalt wird den Platzverweis schriftlich anfordern und dann rechtlich dagegen vorgehen. Das ist eben auch so eine Sache: Man hat das Recht, sich Platzverweise auch schriftlich geben zu lassen. Dann müssen sie den Platzverweis auch ausführlicher begründen. Und für einen Platzverweis braucht es außerdem auch Ort und Zeit, also wie lange man genau welches Platzes verwiesen ist.

Smettbo: *Manchmal ist aber auch die Versammlungsbehörde vor Ort.*
Anne Herpertz: Die Versammlungsbehörde steht über der Polizei, was etwa Beauflagun-

gen angeht. Wenn die nicht da sind, dann kann die Polizei selbst entscheiden. Das Lustige ist aber, dass sich zwischen Versammlungsbehörde und Polizei ein Blame-Game entwickeln kann. Die Polizei würde ja gern, kann aber nicht, weil die Versammlungsbehörde hat ja, und die Versammlungsbehörde sagt, die Polizei hat so oder so agiert, und da können wir ja nichts dafür.

Smettbo: *Wie geht ihr das Thema IT-Sicherheit bei eurer aktivistischen Arbeit an?*
Anne Herpertz: Wir haben einen eigenen Matrix-Server, da können sich die Leute einen Account zulegen. Wir stellen verschiedene Tools zur Verfügung, wie etwa Aktionskarten oder vormarkierte Karten via Open Streetmap. Da kann man gut Struktur schaffen. Für Schnelleres haben wir Signal, das ist manchmal niederschwelliger als Matrix. Was wir auch noch praktizieren ist: Shut the Fuck Up. Also sich zu überlegen, ob man gewisse Dinge wirklich digital kommuniziert. Ich denke, da kann man noch einiges machen. Technische Lösungen erklären, verbreiten und aufklären. Es gibt auch noch Potential Open Source Lösungen mehr auf unseren speziellen Anwendungsfall anzupassen.

Smettbo: *Was möchtest du den Personen mitgeben, die diesen Artikel lesen?*
Anne Herpertz: Bildet Banden! In Strukturen organisiert es sich besser. Demonstrationen kosten Geld. Etwa wenn es darum geht, einen Lautsprecherwagen zu beschaffen. Und es kostet Zeit. Man muss sich mit der Versammlungsbehörde koordinieren, Ordner*innen vor Ort haben. Das passiert nicht einfach mit einem Fingerschnippen, sondern muss organisiert werden. Es sind immer die gleichen, die Demos organisieren in Dresden. Wenn man sich hier beteiligen will, dann kann ich nur sagen: geht aktiv auf die Leute zu und sprecht sie an, was ihr tun könnt. Wir freuen uns über jede Unterstützung!






Bei aufkommenden
Emotionen
bitte hier streicheln
H. P. Adamski

Wenn Eltern in Deutschland ihrem Kind einen Namen geben wollen, der nicht auf der offiziellen Liste erlaubter Namen steht, können sie Grafikdesigner*innen anheuern.
Die basteln Fake-Seiten in echte Bücher von großen Verlagen.
Auf den Seiten stehen die erfundenen Namen, die Eltern in Deutschland ihren Kindern nicht geben dürfen.
Die Eltern zeigen dem Amt diese Seite von, let's say, Ullstein Verlag oder so und schwups hat das Kind einen neuen Namen.



Die ehrenamtliche Richterin

von Mandy Krebs

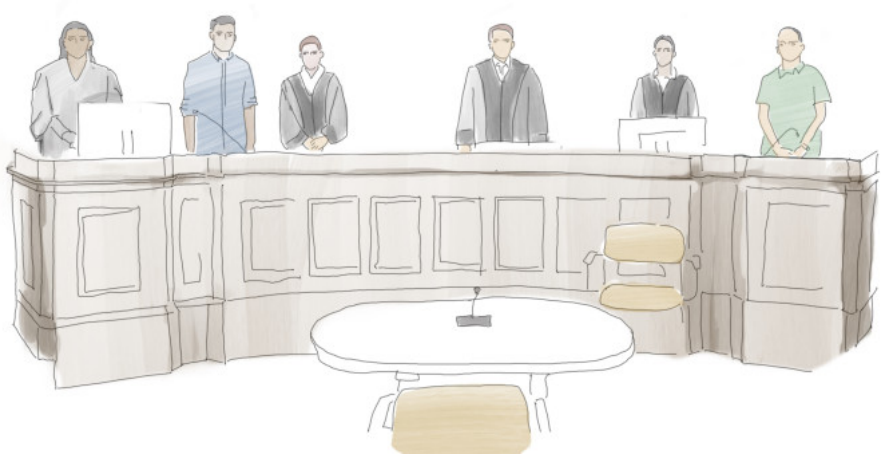
Wenn mich eine unbekannte Berliner Festnetznummer anruft, gehe ich meist im Kopf vorsichtshalber meinen Schichtplan für die kommenden Tage durch, denn mit hoher Wahrscheinlichkeit muss meine Einsatzplanerin diesen dann ändern. Ich bin seit 2019 Hilfsschöffin am Landgericht Berlin. Das Amt eines Schöffen ist ein Ehrenamt [1, 2], dessen Ausübung nicht ganz unbedeutend ist. Bei Straf- und Jugendstrafprozessen an Amts- und Landgerichten darf ohne Mitwirkung dieser ehrenamtlichen Richter kein Urteil gefällt werden. [3] Durch mich soll der Grundsatz der Teilhabe der Bevölkerung an der Rechtssprechung verwirklicht werden. Ich soll durch meine Lebens- und Berufserfahrung und meine nicht-juristische Wertung eine gerechte, volksnahe und damit gute Urteilsfindung sicherstellen.

In dieses Amt wurde ich gewählt. Ich habe eine Bereitschaftserklärung ausgefüllt und mit meiner Unterschrift versichert, dass mir keine Gründe bekannt sind, die meiner Berufung entgegenstehen, ich also eine deutsche Person [1] zwischen dem 25. und 70. Lebensjahr bin und in der jeweiligen Gemeinde lebe. [4] Ich wurde nicht wegen einer vorsätzlichen Tat zu einer Freiheitsstrafe von mehr als sechs Monaten verurteilt. Auch schwebende Ermittlungsverfahren gegen meine Person soll es nicht geben, wenn das den Verlust zur Bekleidung öffentlicher Ämter zur Folge hätte. [5, 2] Gesundheitlich fühle ich mich fit genug, verstehe meistens die deutsche Sprache [1], bin aktuell keine Bundespräsidentin, Mitglied der Bundes- oder Landesregierung oder als Religionsdienerin tätig. [6] Ich arbeite auch nicht als Richterin, Staatsanwältin oder Notarin. [7] Ich habe nicht gegen Grundsätze der Menschlichkeit verstoßen und ich war auch nicht bei der Stasi. [8]

Wenn es in einer Gemeinde nicht genug freiwillige Meldungen gibt, werden Bürger aus dem Einwohnermelderegister gegriffen und zwangsverpflichtet. Dieses Amt dürfen sie nur ablehnen, wenn sie schon zwei aufeinanderfolgende Amtsperioden als Schöffe oder Schöffin absolviert haben oder Mitglied des Bundestages, Bundesrates oder Europäischen Parlament sind. Des Weiteren können Ärzte, Krankenschwestern und Hebammen ablehnen. Personen können auch versuchen, glaubhaft darzustellen, dass das Amt für sie eine besondere Härte bedeutet. [6] Zwar verspüre ich das Wohnen in Berlin Gesundbrunnen an manchen Tagen schon als besonderen Härtefall, aber das dürfte höchstwahrscheinlich nicht als Begründung reichen. Ich wollte aber auch überhaupt nicht ablehnen und hatte mich freiwillig gemeldet.

Bei meiner ersten Ladung habe ich durch folgende Worte einen Eid geleistet: „Ich schwöre, die Pflichten einer ehrenamtlichen Richterin getreu dem Grundgesetz für die Bundesrepublik Deutschland, getreu der Verfassung des jeweiligen Bundeslandes und getreu dem Gesetz zu erfüllen, nach bestem Wissen und Gewissen ohne Ansehen der Person zu urteilen und nur der Wahrheit und Gerechtigkeit zu dienen, so wahr mir Gott helfe.“ [9] Den Gott habe ich weggelassen.

Ich hätte es nicht gedacht, aber es fühlte sich erstaunlich gut an, da mit der erhobenen rechten Hand zu stehen und diesen Eid zu schwören. Auch bin ich jedes Mal ein bisschen



(Mandy Krebs)

stolz, wenn ich das imposante Kriminalgericht Moabit betrete. Zwar nimmt die Suche nach dem richtigen Saal manchmal kafkaeske Züge an und die Cafeteria ist besser versteckt als das Gleis 9 ¾, aber das beeinträchtigt meine Zustimmung über diese gelegentliche Arbeitsstätte nicht.

Als Hilfsschöffin wurde ich bis jetzt herangezogen, wenn die Hauptschöffen verhindert waren. Die Hauptschöffen sollen möglichst nicht mehr als zwölf ordentliche Sitzungstage im Jahr absolvieren und ich rücke nach, wenn ein Hauptschöffe von der Liste gestrichen wird. [1, 10, 2]

Wenn ich von diesem Ehrenamt erzähle, wird meist davon ausgegangen, dass ich über große Vorkenntnisse verfüge. Dem ist aber nicht so. Nur von den Jugendschöffen wird eine erzieherische Befähigung erwartet. [11] In meinem Fall bekomme ich nach dem Anruf eine Ladung, erscheine zu der angegebenen Uhrzeit und werde dann im Beratungszimmer über den Sachverhalt informiert. Wenn ich eine Nachfrage haben sollte oder etwas nicht verstanden habe, wird es mir die Richterin oder der Richter erklären.

Ich kann von mir behaupten, dass ich durch dieses Ehrenamt meine Stadt noch einmal von einer ganz andern Seite kennengelernt habe - nicht unbedingt von ihrer schönsten. Nichtsdestotrotz bin ich froh über diesen mir neuen Blickwinkel. Denn sich immer nur in der eigenen Blase zu bewegen und die Stadt nur als Bühne für die eigene Selbstverwirklichung zu verstehen, halte ich für ungesund. Ich habe viel gelernt und musste feststellen, dass sich nicht selten die für mein Verständnis so eindeutige Sachlage mit jeder Aussage, jedem Nachfragen zu verschieben begann. In stundenlangen Sitzungen wurde hinterfragt, zugehört, ge-

zeigt und übersetzt. Das kann schwierig sein und erfordert des Öfteren, neben ordentlich Sitzfleisch, ein hohes Maß an Aufmerksamkeit. Auch muss ich zu jedem Zeitpunkt unparteilich sein. Ich darf mich nicht von Regungen der Zuneigung oder Abneigung gegenüber den Angeklagten beeinflussen lassen. Ich muss alles vermeiden, was äußerlich Zweifel an meiner Unparteilichkeit wecken könnte. [9] Im Nachhinein darüber reden darf ich ebenfalls nicht, da ich eine Amtsverschwiegenheit auch nach Beendigung der Tätigkeit befolgen muss. [9, 12]

Frustration habe ich erlebt, wenn die Abläufe nicht funktionieren. Wenn sich niemand mehr an irgendwas erinnern kann, weil der Vorfall ewig her ist, geladene Zeugen zu spät kommen oder überhaupt nicht erscheinen und wenn die Technik nicht läuft. Wobei, viel Technik gibt es nicht, dafür massenhaft Akten und Papier.

Für meinen Einsatz muss mein Arbeitgeber mich freistellen [9] und für eventuellen Verdienstausfall und andere Aufwendungen kommt der Staat auf. [13] Ich würde mir wünschen, dass die Schöffen trotz nicht weniger Voraussetzungen möglichst ihre Gemeinde, ihre Stadt abbilden. Alle, die wollen, sollten sich aufstellen lassen, statt zu denken, dass das zeitlich nicht drin ist, der Chef das nicht gern sieht oder man zu wenig weiß. Ich habe erneut eine Bereitschaftserklärung für eine weitere fünfjährige Amtsperiode abgegeben.

Referenzen

[1] §§ 31 Gerichtsverfassungsgesetz (GVG): https://www.gesetze-im-internet.de/gvg/__31.html

[2] §§ 77 Gerichtsverfassungsgesetz (GVG): https://www.gesetze-im-internet.de/gvg/__77.html

[3] § 30 Gerichtsverfassungsgesetz (GVG): https://www.gesetze-im-internet.de/gvg/__30.html

[4] § 33 Gerichtsverfassungsgesetz (GVG): https://www.gesetze-im-internet.de/gvg/__33.html

[5] § 32 Gerichtsverfassungsgesetz (GVG): https://www.gesetze-im-internet.de/gvg/__32.html

[6] § 35 Gerichtsverfassungsgesetz (GVG): https://www.gesetze-im-internet.de/gvg/__35.html

[7] § 34 Gerichtsverfassungsgesetz (GVG): https://www.gesetze-im-internet.de/gvg/__34.html

[8] § 44a Deutsches Richtergesetz (DRiG): https://www.gesetze-im-internet.de/drig/__44a.html

[9] § 45 Deutsches Richtergesetz (DRiG): https://www.gesetze-im-internet.de/drig/__45.html

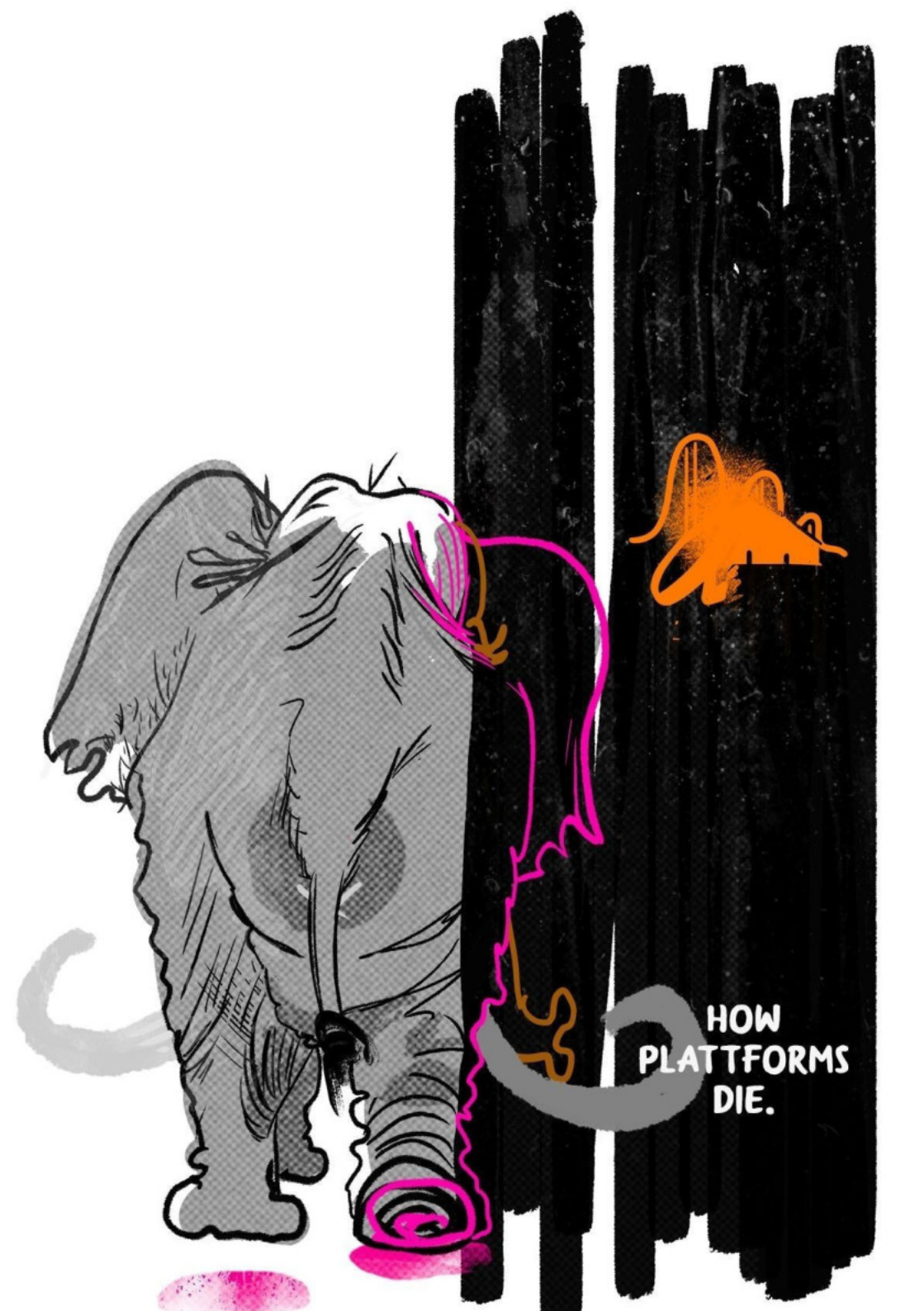
[10] § 45 Gerichtsverfassungsgesetz (GVG): https://www.gesetze-im-internet.de/gvg/__45.html

[11] § 35 Abs. 2 Satz 2 Jugendgerichtsgesetz (JGG): https://www.gesetze-im-internet.de/jgg/__35.html

[12] § 43 Deutsches Richtergesetz (DRiG): https://www.gesetze-im-internet.de/drig/__43.html

[13] § 55 Gerichtsverfassungsgesetz (GVG): https://www.gesetze-im-internet.de/gvg/__55.html




HOW
PLATTFORMS
DIE.

Tiktoks Vershittifizierung

von Cory Doctorow

So sterben Plattformen: Erst sind sie gut zu ihren Nutzenden; dann nutzen sie ihre Nutzenden, um die Situation ihrer Geschäftskundschaft zu verbessern; schließlich benutzen sie diese Geschäftskundschaft, um den ganzen Gewinn selbst abzugreifen. Dann sterben sie. *Der Original-Artikel ist Anfang 2023 erschienen. [1] Veröffentlicht und lizensiert unter CC BY 4.0. [2]*

Ich nenne es Vershittifizierung

Es ist die unvermeidliche Folge einer Kombination aus der Leichtigkeit, mit der sich die Art der Wertschöpfung einer Plattform ändern lässt, und der Natur eines *zweiseitigen Marktes*, bei dem eine Plattform zwischen Kaufenden und Verkaufenden sitzt. Dabei setzt sie jeden als Geisel für den anderen ein, indem sie einen immer größeren Anteil des Wertes, der zwischen ihnen ausgetauscht wird, abgreift. Wenn eine Plattform neu entsteht, braucht sie Nutzende, also macht sie sich für diese wertvoll. Amazon zum Beispiel: Viele Jahre lang arbeitete das Unternehmen mit Verlust und nutzte seinen Zugang zu den Kapitalmärkten, um alles zu subventionieren, was man kaufte. Waren wurden unter Wert verkauft und unter dem Selbstkostenpreis ausgeliefert. Wenn man nach einem Produkt suchte, tat Amazon alles, um es an die erste Stelle der Suchergebnisse zu setzen.

Das hat viel Geschäftskundschaft angelockt, sogenannte *Marketplace-Seller*, die Amazon zu dem *Laden für alles* machten, wie sie es von Anfang an versprochen hatten. Als die Seller in Scharen kamen, ging Amazon dazu über, Liefernde zu subventionieren. Kindle- und Audible-Produktionen erhielten großzügige Pakete. Marketplace-Seller erreichten ein riesiges Publikum, und Amazon nahm ihnen nur niedrige Provisionen ab. Mit dieser Strategie wurde es für die Kundschaft zunehmend schwieriger, Dinge woanders als bei Amazon zu finden. Das wiederum bedeutete, dass sie nur noch auf Amazon suchten. Was wiederum bedeutete, dass die Verkaufenden auf Amazon auch verkaufen mussten.

Zu diesem Zeitpunkt begann Amazon, Überschüsse seiner Geschäftskundschaft abzuschöpfen und sie an die Amazon-Aktieninhabenden weiterzuleiten. Inzwischen geben Marketplace-Seller mehr als 45 % des Verkaufspreises in Form einer Abzockgebühr an Amazon ab. Das 31-Milliarden-Dollar-*Werbe*-Programm des Unternehmens ist in Wirklichkeit ein Schmiergeldsystem, welches Verkaufende gegeneinander ausspielt und sie dazu zwingt, auf die Chance zu bieten, bei Suchergebnissen ganz oben zu erscheinen. In den Amazon-Suchergebnissen erscheint keine Liste von Produkten, die der Suche am ehesten entsprechen, sondern eine Liste der Produkte, deren Verkaufende am meisten dafür bezahlt haben, bei dieser Suche ganz oben zu stehen. Diese Gebühren sind in den Kosten enthalten, die man für das Produkt bezahlt, und Amazons *most-favored-nation*-Klauseln an die Verkaufenden bedeutet, dass diese anderswo nicht billiger verkaufen dürfen, so dass Amazon die Preise auch im Einzelhandel nach oben getrieben hat.

Wenn du bei Amazon nach *Katzenbetten* suchst, erscheint zunächst ausschließlich Werbung. Darunter auch Werbung für Produkte,

die Amazon von seinen eigenen Verkaufenden geklont hat, um sie aus dem Geschäft zu verdrängen. Dritte müssen 45 % Gebühren an Amazon zahlen, aber Amazon erhebt diese Gebühren nicht selber. Insgesamt bestehen die ersten fünf Ergebnisseiten für *Katzenbett* zu 50 % aus Werbung.

Das ist Vershittifizierung

Überschüsse werden zuerst an die Nutzenden geleitet. Dann, wenn sie gebunden sind, gehen die Überschüsse an die Anbietenden. Dann, wenn sie gebunden sind, werden die Überschüsse an die Aktieninhabenden verteilt und die Plattform verkommt zu einem nutzlosen Haufen Scheiße. Von den mobilen App-Stores bis zu Steam, von Facebook bis zu Twitter – das ist der Lebenszyklus der *Vershittifizierung*.

Dieses Hütchenspiel mit Überschüssen ist das, was mit Facebook passiert ist.

Erst war Facebook gut zu dir

Es zeigte dir, was Menschen, die du liebst und die dir wichtig sind, zu sagen hatten. Das führte zu einer Art gegenseitiger Geiselnahme: Sobald eine kritische Masse an Personen, die einem wichtig sind, auf Facebook waren, wurde es praktisch unmöglich, die Seite zu verlassen. Da man alle davon überzeugen müsste, ebenfalls zu gehen und man sich dann darauf einigen müsste, wohin man gehen wollte. Sosehr du deine Freunde auch liebst, die Hälfte der Zeit könnt ihr euch doch nicht einigen, welchen Film ihr sehen und wohin ihr essen gehen wollt.

Dann begann Facebook, deinen Feed mit Beiträgen von Konten vollzustopfen, denen man nicht folgte. Zuerst waren es Medienunternehmen, die den Nutzenden aufgedrängt wurden, damit sie auf Artikel klickten und Traffic bei Zeitungen, Zeitschriften und Blogs erzeugten. Sobald diese Publikationen für ihren Traffic von Facebook abhängig waren, wurde ihr Traffic gedrosselt. Zunächst wurde der Traffic zu Publikationen gedrosselt, die Facebook nutzten, um Auszüge mit Links zu ihren eigenen Websites zu veröffentlichen, um dann die Publikationen dazu zu bringen, Volltext-Feeds innerhalb von Facebook bereitzustellen.

Dadurch wurden die Publikationen endgültig von Facebook abhängig – ihre Lesenden besuchten nicht mehr die Websites der Publikationen, sondern nur noch deren Facebook-Seite. Die Publikationen waren Geiseln der Lesenden, die wiederum Geiseln ihrer Facebook-Befreundeten waren. Facebook zeigte den Lesenden die veröffentlichten Artikel nicht mehr, indem es den Algorithmus so einstellte, dass Beiträge von Publikationen unterdrückt wurden. Ausnahme: Die Publikationen zahlten dafür, dass ihre Artikel bei Abonnierenden hervorgehoben wurden und das obwohl die Lesenden diese ausdrücklich abonnierten und Facebook gebeten haben, jene in ihrem Feed anzuzeigen. Als Nächstes packte Facebook mehr Werbung in den Feed und mischte Bezahlinhalte von Leuten, für die man sich interessierte, mit Bezahlinhalten von Fremden, um unsere Aufmerksamkeit zu kapern. Es war ein großartiger Deal für die Werbetreibenden, denn es kostete sie fast Nichts, ihre Anzeigen auf Grundlage der nicht genehmigten Datensammlung von Nutzenden auszurichten. Auch die Verkaufenden wurden von Facebook abhängig, da sie ohne Zugriff auf diese zielgerichteten Werbemaßnahmen ihre Geschäfte nicht weiterführen konnten. Das war der Auslöser für Facebook, die Anzeigenpreise in die Höhe treiben, sich weniger um Anzeigenbetrug zu kümmern und mit Google zu kooperieren,

um den Anzeigenmarkt über ein illegales Programm namens Jedi Blue zu manipulieren. [3]

Heute ist Facebook unheilbar verseucht, ein schrecklicher Ort, an dem sich weder Nutzende noch Medienunternehmen oder Werbetreibende wohlfühlen. Es ist ein Unternehmen, das absichtlich einen großen Teil der Verlegenden zerstört hat, indem es sie mit falschen Behauptungen über die Beliebtheit von Videos bei Facebook-Nutzenden zu einem *Pivot to Video* verleitet hat. Die Unternehmen steckten Milliarden in die Umstellung auf Videos, aber die Zuschauenden blieben aus und die Medien machten scharenweise dicht. [4]

Doch Facebook hat einen neuen Pitch. Es nennt sich nun Meta und fordert, dass wir den Rest unserer Tage als an die Plattform gefesselte, geschlechtslose, stark überwachte Low-Poly-Cartoon-Figuren leben.

Es hat den Unternehmen, die Apps für dieses Metaversum entwickeln, versprochen, sie nicht wie das alte Facebook unter Druck zu setzen. Es bleibt abzuwarten, ob ihnen das jemand abnimmt. Mark Zuckerberg gestand einst einem Kollegen, dass er sich über die vielen Harvard-Studierenden wunderte, die ihre persönlichen Daten an seine neue Website *The-Facebook* schickten: *„Ich weiß nicht, warum. Sie vertrauen mir. Schwachköpfe."* [5]

SEO heisst Search Engine Optimization: Alle Maßnahmen technischer oder inhaltlicher Natur, um die Sichtbarkeit von Websites oder Produkten in einer Suchmaschine zu verbessern.

Wenn man das Vershittifizierungs-Muster einmal verstanden hat, lösen sich viele der Plattform-Rätsel von selbst. Es ist genau wie der SEO-Markt oder die ganze energiegeladene Welt der Content-Creator, die endlose Stunden damit verbringen, sich mit nutzloser Plattform-Kremlinologie zu beschäftigen. Sie handeln in der Hoffnung, die algorithmischen Stolperdrähte ausfindig zu machen, die, wenn sie überschritten werden, die kreativen Werke, in die sie ihr Geld, ihre Zeit und ihre Energie stecken, zum Scheitern zu bringen. [6]

Der Begriff **Plattform-Kremlinologie** ist eine Anspielung auf die „Kremlinologie", eine Praxis, die während des Kalten Krieges in Bezug auf die Sowjetunion angewendet wurde. Dabei versuchten Experten, aus öffentlichen Äußerungen, politischen Handlungen und anderen indirekten Hinweisen auf das Innenleben des Kremls und die sowjetische Führung zu schließen, da Informationen aus erster Hand begrenzt waren.

Für eine Plattform zu arbeiten, ist so, als würde man für einen Chef arbeiten, der einem Geld für *Regelverstöße* von jedem Gehalt abzieht, aber nicht sagt, welche Regeln das sind, weil man dann herausfinden würde, wie man diese Regeln umgeht, ohne dass er es merkt und den Lohn kürzt. Dagegen ist die Moderation von Inhalten der einzige Bereich, in dem Sicherheit durch Geheimhaltung der Sicherheitsmechanismen zur Best Practice zählt. [7]

Die Situation ist so schlimm, dass Organisationen wie *Tracking Exposed* eine ganze Armee von Freiwilligen und eine Roboterarmee von kopflosen Browsern angeheuert haben, um zu versuchen, die Logik hinter den willkürlichen, maschinellen Urteilen des Algorithmus zu entschlüsseln. Einerseits um den Nutzenden die Möglichkeit zu geben, die Empfehlungen, die sie erhalten, zu optimieren, andererseits um den Urheber*innen zu helfen, den Lohndiebstahl zu vermeiden, der mit einer Reichweitendrosselung einhergeht. [8]



Common Livecycle of a plattform – Vom Start bis zur Vershittifizierung

Was aber, wenn es keine grundlegende Logik gibt? Oder sich die Logik je nach Priorität der Plattform ändert? Auf jedem Rummel kann man einen armen Trottel sehen, der den ganzen Tag mit einem riesigen Teddybär herumläuft, den er durch das Werfen von drei Bällen in einen Korb gewonnen hat. Das Korbspiel ist manipuliert. Der Schausteller kann einen Schalter betätigen, um die Bälle aus dem Korb rausspringen zu lassen. Niemand gewinnt den Jumbo-Teddy, es sei denn, der Schausteller entscheidet so. Warum lässt der Schausteller den Trottel den Teddy gewinnen? Damit er ihn den ganzen Tag mit sich herumträgt und andere Trottel davon überzeugt, fünf Dollar für die Chance auszugeben, einen zu gewinnen. [9]

Der Schausteller hat dem armen Trottel einen Teddy zugewiesen, so wie Plattformen Überschüsse an 1-Key-Performer vergeben – als Überzeugungshilfe in einem *Big Store* Schwindel, um andere Trottel zu gewinnen, die Inhalte für die Plattform erstellen und sich und ihr Publikum daran binden.

Das bringt mich zu Tiktok

Tiktok ist – unter anderem – *ein kostenloses Adobe Premiere für Teenager, die auf ihren Handys leben.* [10]

Aber was Tiktok von Anfang an so erfolgreich gemacht hat, war die Qualität seines Empfehlungssystems. Von Anfang an war Tiktok sehr gut darin, seinen Nutzenden Dinge zu empfehlen. [11]

Durch gut gemeinte Empfehlungen von Dingen, die den Nutzenden gefallen könnten, baute Tiktok ein Massenpublikum auf, das größer war, als viele es angesichts der übermächtigen Konkurrenz von Youtube und Instagram für möglich hielten. Seitdem Tiktok sein Publikum hat, hat es begonnen, die Medienunternehmen und Kreativen, die immer noch hartnäckig an Youtube und Instagram hängen, abzuwerben. Emily Baker-White von Forbes veröffentlichte, wie Bytedance, die Muttergesellschaft von Tiktok, arbeitet. Sie zitiert mehrere interne Quellen, welche die Existenz eines *Heating-Tools* enthüllen, mit dem Tiktok Videos von ausgewählten Konten in die Feeds von Millionen Zuschauenden spült. [13]

Diese Videos landen im *ForYou*-Feed der Nutzenden, die laut Tiktok *von einem Algorithmus ausgewählt wurden, der deine Interessen auf Grundlage deines Verhaltens in der App vorhersagt.* In Wirklichkeit enthält *For You* nur manchmal Videos, bei denen Tiktok glaubt, sie würden einen Mehrwert für dich ergeben. Meistens ist der Feed gefüllt mit Videos, die Tiktok einfügte, damit die Erschaffenden denken, dass Tiktok ein guter Ort sei, um ein Publikum zu erreichen.

> Ein **Paperclip Maximizer** ist ein von Nick Bostrom 2003 beschriebenes Gedankenexperiment. Eine KI, die darauf programmiert ist, möglichst viele Büroklammern herzustellen, gerät außer Kontrolle und wird existenziell bedrohend für die Menschheit.

Quellen haben *Forbes* berichtet, dass TikTok das *Heating-Tool* oft nutze, um Influencer und Marken zu umwerben und sie zu Partnerschaften zu verleiten, indem die Anzahl der Aufrufe ihrer Videos in die Höhe getrieben wurde. Dies deutet darauf hin, dass das *Erhitzen* einigen Influencern und Marken, mit denen TikTok Geschäftsbeziehungen anstrebte, zugute kam, auf Kosten anderer. Mit anderen Worten: Tiktok verteilt Jumbo-Teddys. Aber Tiktok ist nicht in der Lage, riesige Teddys zu verschenken. Tiktoks Ursprünge liegen in der quasi-kapitalistischen chinesischen Wirtschaft, Tiktok ist trotz alledem nur ein weiterer Büroklammern-maximierender, künstlicher Kolonieorganismus, der den Menschen wie eine lästige Darmflora behandelt. Tiktok wird die Menschen, die es einfangen will, nur so lange kostenlose Aufmerksamkeit schenken, bis sie gefangen sind; dann wird es diese Aufmerksamkeit zurückziehen und beginnen, sie zu Geld zu machen.

Monetarisieren ist ein schreckliches Wort, das stillschweigend zugibt, dass es so etwas wie eine *Aufmerksamkeitsökonomie* nicht gibt. Man kann Aufmerksamkeit nicht als Tauschmittel verwenden. Man kann sie nicht als Wertaufbewahrungsmittel verwenden. Man kann sie nicht als Rechnungseinheit verwenden. Aufmerksamkeit ist wie eine Kryptowährung: ein wertloser Token, der nur in dem Maße wertvoll ist, in dem man jemanden austricksen oder zwingen kann, sich im Tausch von einer Fiat-Währung zu trennen. [12] Man muss sie *monetarisieren* – das heißt, man muss das falsche Geld gegen echtes Geld eintauschen. Im Fall der Kryptowährungen basierte die wichtigste Monetarisierungs-Strategie auf Täuschung. Börsen und *Projekte* verteilten einen Haufen Jumbo-Teddys und schufen so eine Armee treu ergebener Judasböcke, die ihre Mitmenschen davon überzeugten, dem Schausteller ihr Geld zu geben und zu versuchen, selbst ein paar Bälle in den Korb zu werfen. Aber Täuschung kann nicht endlos Geld schaffen. Irgendwann gehen einem die Trottel aus. Um viele Menschen dazu zu bringen, das Spiel mitzuspielen, muss man sie zwingen, nicht überreden.

Die erste Krypto-Liquidität entstand durch Ransomware. Die Existenz eines Pools verzweifelter, in Panik geratener Unternehmen und Einzelpersonen, deren Daten von Kriminellen gestohlen worden waren, schuf eine Basis für Krypto-Liquidität, da sie ihre Daten nur zurückerhalten konnten, indem sie echtes Geld gegen falsches Kryptogeld tauschten. Die nächste Phase des Kryptozwangs war Web3: Die Umwandlung des Webs in eine Reihe von Mautstellen, die man nur passieren konnte, wenn man echtes Geld gegen falsches Kryptogeld tauschte. Aber das Internet ist ein Muss, kein Nice-to-have, eine Voraussetzung für die vollständige Teilhabe an Beschäftigung, Bil-

dung, Familienleben, Gesundheit, Politik, Gesellschaft und sogar Romantik. Indem sie all diese Dinge hinter Krypto-Mauthäuschen halten, hoffen die Hodler, ihre Token in echtes Geld umzuwandeln. [14]

Ein **Hodler** ist ein Begriff, der in der Kryptowährungsgemeinschaft verwendet wird. Der Ausdruck leitet sich von einem Schreibfehler des Wortes *holder* ab, der in einem Bitcoin-Forum gemacht wurde und sich als Meme etabliert hat. Es handelt sich um eine Person, die Bitcoin oder andere Kryptowährungen besitzt und diese langfristig halten möchte, unabhängig von den kurzfristigen Preisschwankungen. Ein Hodler glaubt an das langfristige Potenzial von Kryptowährungen und ist nicht daran interessiert, sie zu verkaufen oder kurzfristige Gewinne zu erzielen.

Für Tiktok ist das Verteilen kostenloser Jumbo-Teddys über das *Heating* von Videos, eingestellt von skeptischen Produzierenden und Medienkunstschaffenden, ein Weg diese zu wahren Gläubigen zu machen. So werden sie dazu gebracht, alles auf eine Karte zu setzen und ihre Bemühungen aufzugeben, auf anderen Plattformen ein Publikum aufzubauen. Dabei hilft ihnen, dass sich das Tiktok-Format von anderen unterscheidet, was es schwierig macht, Tiktok-Videos zur Verbreitung auf konkurrierenden Plattformen wiederzuverwenden. Sobald die Produzierenden und die Medienunternehmen an der Angel sind, beginnt die nächste Phase: Tiktok dreht das *Heating* herunter, welches die Videos den Menschen anzeigt, die noch nie von ihnen gehört und nicht darum gebeten haben. Tiktok führt hier einen heiklen Tanz auf: Es gibt nur eine bestimmte Menge an *Vershittifizierung*, die sie in die Feeds ihrer Nutzenden pushen können, und Tiktok hat viele andere Produzierende, denen sie riesige Teddybären geben wollen.

Tiktok wird den Produzierenden nicht nur die *kostenlose* Aufmerksamkeit entziehen, indem es sie im Algorithmus zurückstellt, es wird sie aktiv bestrafen, indem es ihre Videos nicht an die Nutzenden liefert, die sie abonniert haben. Denn jedes Mal, wenn Tiktok dir ein Video zeigt, das du sehen willst, vergibt es die Gelegenheit, dir ein Video zu zeigen, das du sehen sollst. Weil deine Aufmerksamkeit der Jumbo-Teddybär ist, den es an einen umworbenen Produzierenden verschenken kann. Und genau das hat Twitter als Teil seines Marschs in Richtung *Vershittifizierung* getan: Dank der Monetarisierungs-Änderungen wird die Mehrheit der Leute, die dir folgen, nie die Dinge sehen, die du postest. Ich habe 500k Follower auf Twitter und meine Beiträge wurden früher regelmäßig von Hunderttausenden oder sogar Millionen gelesen. Heute sind es nur noch Hunderte, vielleicht Tausende. Ich habe Twitter gerade 8 Dollar für Twitter Blue gegeben, weil das Unternehmen durchblicken liess, dass es die Dinge, die ich poste, nur den Leuten zeigen wird, die darum gebeten haben, sie zu sehen, wenn ich Lösegeld zahle. Dies ist die jüngste Schlacht in einem der am längsten schwelenden Kriege im Internet: der Kampf um End-to-End. [15]

Ma Bell war der Spitzname für die Southwestern Bell Corporation (heute AT&T Inc.), die bis zur Auflösung im Jahr 1982 als Telekommunikationsmonopolist in den USA tätig war.



Am Anfang gab es die *Bellheads* und die *Netheads*. Die Bellheads arbeiteten für große Telekommunikationsunternehmen und glaubten, dass der gesamte Wert des Netzes zu Recht den Betreibenden gehöre. Wenn jemand eine neue Funktion erfand – z. B. die Anruferkennung – sollte diese so eingeführt werden, dass die Betreiberin monatlich für die Nutzung eine Gebühr erheben kann. Software-as-a-Service, im *Ma Bell*-Stil.

Die Netheads hingegen glaubten, dass der Wert des Netzes verteilt und pluralisiert werden sollte. Die Netheads wollten vielfältige Netze mit vielen Angeboten, viel Wettbewerb und einem einfachen, kostengünstigen Wechsel zwischen den Wettbewerbenden dank Interoperabilität aufbauen. Sie entwickelten das *End-to-End-Prinzip*: die Idee, dass Netze so gestaltet sein sollten, dass Botschaften der willigen Sprechenden so schnell und zuverlässig wie möglich an die Endpunkte der willigen Zuhörenden geliefert werden. Unabhängig davon, ob Netzbetreibende damit Geld verdienen können, dir Daten zu senden, die du empfangen sollst, wäre es ihre Pflicht, dir diejenigen Daten bereit zu stellen, die du sehen möchtest.

Das Ende-zu-Ende-Prinzip ist heute auf dem Dienstleistungssektor tot. Nützliche Idioten wurden zu der Annahme verleitet, dass das Risiko des Twitter-Missmanagement im *Woke Shadowbanning* bestünde.

Ein **Shadowban** ist eine Art der Nutzenden-Sperrung, bei welcher die betroffenen Accounts nicht direkt blockiert werden, sondern deren Sichtbarkeit und Reichweite eingeschränkt werden, ohne die Nutzenden darüber zu informieren.

Das wirkliche Risiko ist, dass deine Aussagen nicht die Personen erreichen werden, die sie hören wollen. Der Grund: Twitter kann mehr Geld damit verdienen, indem es seine Feeds *vershittifiziert* und Auslösegeld für das Privileg berechnet, dabei zu sein. Wie ich zu Beginn schrieb, übt die *Vershittifizierung* eine fast unwiderstehliche Anziehungskraft auf den Plattformkapitalismus aus. Es ist einfach zu leicht, den Vershittifizierungsknopf auf elf zu drehen. Twitter konnte die Mehrheit seiner qualifizierten Mitarbeitenden entlassen und dabei trotzdem immer noch voll aufdrehen, sogar mit einer Notmannschaft verzweifelter, demoralisierter H-1B-Arbeitskräfte, die aufgrund einer drohenden Abschiebung an Twitters sinkendes Schiff gefesselt sind.

H-1B ist ein Nicht-Einwanderungsvisum, das es ausländischen Fachleuten ermöglicht, vorübergehend in den USA zu arbeiten.

Die Versuchung zur *Vershittifizierung* wird durch die Interoperabilitätssperren noch verstärkt: Wenn Twitter interoperable Clients verbietet, seine APIs ausdünnt und seine Nutzenden regelmäßig suspendiert sobald sie ihre Mastodon-Handles in ihre Bios nehmen, wird es schwieriger, Twitter zu verlassen. Dadurch wächst die *Vershittifizierung* an, die Nutzenden können zwangsernährt werden, ohne deren Weggang dabei zu riskieren.

Diese Vershittifizierungs-Strategie ist nur dann erfolgreich, wenn sie in Maßen erfolgt. Der maximal verhaftete Nutzende erreicht eine Grenze und geht – oder wird dazu ermutigt. Die Dorfbewohner von Anatevka in *Fiddler on the Roof* duldeten jahrelang die gewalttätigen Überfälle und Pogrome der Kosaken, bis sie schließlich gezwungen waren, nach Krakau, New York und Chicago zu fliehen. [16]

Ein Gleichgewicht ist für verdorbene Vershittifizierungs-Unternehmen nur schwer erreichbar. Einzelne Produktmanager*innen, Führungskräfte und aktivistische Aktieninhabende bevorzugen schnelle Renditen auf Kosten der Nachhaltigkeit und befinden sich in einem Wettlauf darum, wessen Saat zuerst aufgeht. Die *Vershittifizierung* hat sich nur deshalb so lange gehalten, weil das Internet sich in *fünf riesige Websites verwandelt hat, die jeweils mit Screenshots der anderen vier gefüllt sind.* [17]

Mit diesem Markt, der von einer Gruppe behäbiger Monopolist*innen abgeschottet wird, tauchen keine besseren Alternativen auf, die uns weglocken könnten. Wenn doch, dann kaufen die Monopolist*innen sie einfach auf und integrieren sie in ihre Vershittifizierungs-Strategien. Wie beispielsweise, als Mark Zuckerberg einen Massenexodus von Facebook-Nutzenden bemerkte, die zu Instagram wechselten, und er daraufhin Instagram kaufte. Wie Zuckerberg sagt: *Es ist besser zu kaufen als zu konkurrieren.*

Das ist die verborgene Dynamik hinter dem Aufstieg und Fall von Amazon Smile: Amazon spendete in dem Programm einen kleinen Geldbetrag an Wohltätigkeitsorganisationen deiner Wahl, wenn du darüber einkauftest. Allerdings nur, wenn du die gekauften Produkte über Amazons eigenes Suchtool gefunden hast. Dies war ein Anreiz für die Kundschaft, die vershittifizierte Amazon-Suche zu benutzen, welche zunehmend mit Produkten von dafür zahlenden Verkaufenden sowie mit gleichen Amazon-Produkten vollgestopft wurde. Die Alternative war die Nutzung von Google, das einen direkt zum gesuchten Produkt führte und wofür Amazon eine Provision für die Wei-



terleitung in Rechnung gestellt wurde. [18]

Der Niedergang von Amazon Smile fällt mit der zunehmenden *Vershittifizierung* der Google-Suche zusammen, dem einzigen erfolgreichen Produkt, das das Unternehmen selbst entwickelt hat. Alle anderen erfolgreichen Produkte wurden eingekauft: Videos, Dokumente, Cloud-Dienst, Werbung, Mobilgeräte. Eigene Produkte sind entweder Flops wie z. B. Google Video, oder übernommene Produkte anderer Unternehmen, wie Chrome. Die Google-Suche basiert auf den Grundsätzen, welche die Gründer Larry Page und Sergey Brin 1998 in ihrem wegweisenden Artikel *Anatomie einer groß angelegten Hypertext-Web-Suchmaschine* dargelegt haben, in dem sie schrieben: *Durch Werbung finanzierte Suchmaschinen sind von Natur aus auf die Werbetreibenden ausgerichtet und nicht auf die Bedürfnisse der Nutzenden.*

Trotz dieses grundlegenden Verständnisses der *Vershittifizierung* konnte Google der verführerischen Melodie der Sirenen nicht widerstehen. Die heutigen Google-Ergebnisse sind ein zunehmend nutzloser Morast aus selbstreferenzierenden Links zu den eigenen Produkten, Anzeigen für Produkte, die nicht gut genug sind, um von selbst Spitzenreiter zu werden und parasitärer SEO-Müll, der Huckepack mit den beworbenen Produkten daher kommt.

Vershittifizierung ist tödlich. Google hat gerade 12.000 Mitarbeitende entlassen, und das Unternehmen ist in heller Aufregung über den Aufstieg von *KI-Chatbots* und wirbt mit aller Kraft für ein KI-gesteuertes Suchtool – das heißt, ein Tool, das dir nicht das zeigt, wonach du fragst, sondern das, was es glaubt, dass du sehen sollst. [19]

Nun, man kann sich vorstellen, dass ein solches Tool gute Empfehlungen ausspricht, so wie es der Algorithmus von Tiktok vor der *Vershittifizierung* tat. Aber es ist schwer vorstellbar, wie Google in der Lage sein wird, ein nicht vershittifiziertes Chatbot-Frontend für die Suche zu entwickeln, angesichts der starken Anreize für Produktmanager*innen, Führungskräfte und Aktieninhabende, die Ergebnisse genau bis zu dem Punkt zu vershittifizieren, an dem die Nutzenden fast so verärgert sind, dass sie die Seite verlassen, aber eben nicht ganz.

So sterben Plattformen wirklich: durch Vershittifizierung

Das ist eigentlich auch gut so. Wir brauchen keine ewigen Herrschenden des Internets. Es ist in Ordnung, dass neue Ideen und neue Arbeitsweisen entstehen. Das Hauptaugenmerk von Gesetzgebenden und politischen Entscheidungstragenden sollte nicht darauf liegen, die dämmrige Vergreisung sterbender Plattformen zu bewahren. Vielmehr sollte sich unsere Politik darauf konzentrieren, die Kosten für die Nutzenden zu minimieren, wenn diese Unternehmen ihr Verfallsdatum erreichen: Die Verankerung von Rechten wie End-to-End würde bedeuten, dass, egal wie autokannibalistisch eine Zombie-Plattform wird, willige Sprechende und willige Zuhörende immer noch miteinander verbunden sind.

Und die politischen Entscheidungstragenden sollten sich auf die Freiheit des Ausstiegs konzentrieren – das Recht, eine sinkende Plattform zu verlassen und dabei weiterhin mit den Gemeinschaften verbunden zu bleiben, die man zurückgelassen hat, die Medien und Anwendungen zu genießen, die man gekauft hat, und die Daten zu bewahren, die man erstellt hat. [20]

Die Netheads hatten Recht: Die technologische Selbstbestimmung steht im Widerspruch zu den natürlichen Imperativen der Tech-Unternehmen. Sie verdienen mehr Geld, wenn sie uns die Freiheit nehmen – unsere Freiheit zu sprechen, zu gehen, uns zu verbinden. Viele

Jahre lang haben selbst Tiktok-Kritisierende zähneknirschend zugegeben, dass Tiktok – egal wie überwachend und unheimlich es war – wirklich gut darin war zu erraten, was man sehen wollte. Aber Tiktok konnte der Versuchung nicht widerstehen, dir das zu zeigen, was du sehen sollst, und nicht das, was du sehen willst. Die *Vershittifizierung* hat begonnen, und es ist unwahrscheinlich, dass sie jetzt noch aufhört. Es ist zu spät, Tiktok zu retten. Jetzt, da es von der *Vershittifizierung* infiziert wurde, bleibt nur noch, es mit Feuer zu töten.

Referenzen

[1] „Originalartikel“, https://pluralistic.net/2023/01/21/potemkin-ai/#hey-guys

[2] „Creative Commons Lizenz“, https://creativecommons.org/licenses/by/4.0/legalcode.de

[3] „Wie Facebook und Google den Anzeigenmarkt mit dem Programm Jedi Blue manipulieren“, https://en.wikipedia.org/wiki/Jedi_Blue.

[4] „Über die strategische Entscheidung, sich verstärkt auf Videoinhalte zu konzentrieren“, https://slate.com/technology/2018/10/facebook-online-video-pivot-metrics-false.html

[5] „Wie Facebook entstand“, https://doctorow.medium.com/metaverse-means-pivot-to-video-adbe09319038

[6] „Das Phänomen Algospeak“, https://pluralistic.net/2022/04/11/coercion-v-cooperation/#the-machine-is-listening

[7] „Content Moderation als Sicherheitsmassnahme“, https://doctorow.medium.com/como-is-infosec-307f87004563

[8] „Die Tool-Suite von Tracking Exposed“, https://www.eff.org/deeplinks/2022/05/tracking-exposed-demanding-gods-explain-themselves

[9] „Ein abgekatertes Spiel“, https://boingboing.net/2006/08/27/rigged-carny-game.html

[10] „corecore in Tiktok“, https://www.garbageday.email/p/the-fragments-of-media-you-consume

[11] „Tiktok to the top“, https://www.npr.org/transcripts/1093882880

[12] „Fiatgeld“, https://de.wikipedia.org/wiki/Fiatgeld

[13] „Tiktoks Heating Tool“, https://www.forbes.com/sites/emilybaker-white/2023/01/20/tiktoks-secret-heating-button-can-make-anyone-go-viral/

[14] „Was ist Geld?“, https://locusmag.com/2022/09/cory-doctorow-moneylike/

[15] „Redefreiheit und Reichweite“, https://pluralistic.net/2022/12/10/e2e/#the-censors-pen

[16] „Sterbende Plattformen verlassen.“, https://doctorow.medium.com/how-to-leave-dying-social-media-platforms-9fc550fe5abf

[17] „Das Internet bestehend aus fünf Webseiten.“, https://twitter.com/tveastman/status/1069674780826071040

[18] „Amazon stellt Spendenprogramm ein.“, https://www.reddit.com/r/technology/comments/10ft5iv/comment/j4znb8y/

[19] „Googles Antwort auf ChatGPT.“, https://www.theverge.com/2023/1/20/23563851/google-search-ai-chatbot-demo-chatgpt

[20] „Interoperables Facebook.“, https://www.eff.org/interoperablefacebook



Horoskop



Feldmaus
21.01. – 19.02.

Was ich nicht weiß, sagt mehr als tausend Worte.



Gänseblümchen
20.02. – 20.03.

Einsicht ist aller Laster Anfang.



Seehund
21.03. – 20.04.

Ein schlafender Fuchs muss auch "B" sagen.



Pommespiekser
21.04. – 20.05.

Kleine Geschenke beschmieren Tisch und Wände.



Einhorn
21.05. – 21.06.

Zufriedenheit verpflichtet.



Windkraft
22.06. – 22.07.

Hunger ist dicker als Wasser.



Autoscooter
23.07. – 23.08.

Spinne am Morgen ist die beste Verteidigung.



Tisch, kaputt
24.08. – 23.09.

Im Dunkeln ist alles rund.



Loopingschaukel
24.09. – 23.10.

Der Zweck macht noch keinen Sommer.



Rübe
24.10. – 22.11.

Gott findet auch mal ein Korn.



Nudelsuppe
23.11. – 21.12.

Wer wagt, ist aller Künste Stiefmutter.

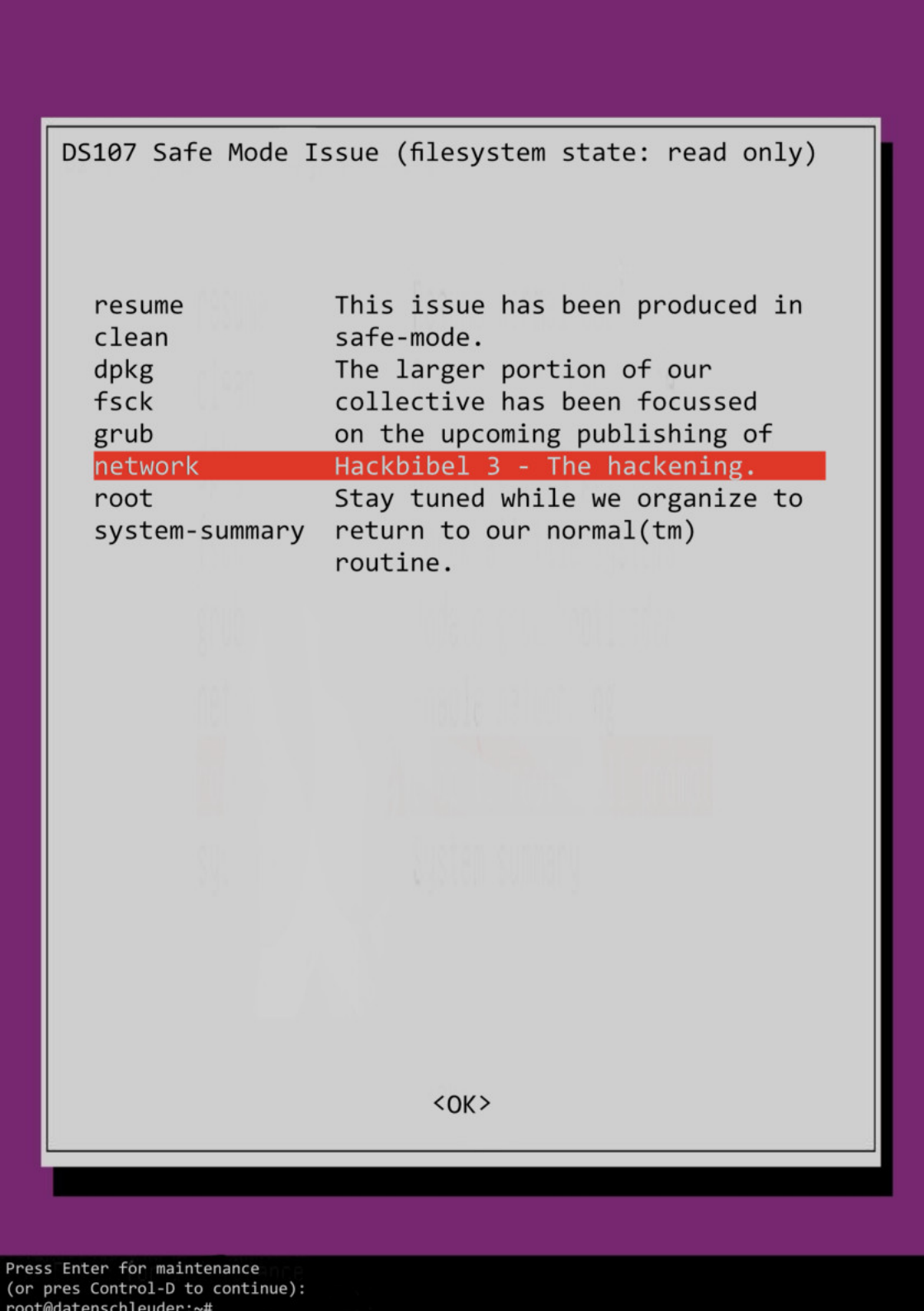


Faltschiffchen
22.12. – 20.01.

Aller Anfang steckt im Detail.

cheers an sprichwortgenerator.de

16ØFE


DS107 Safe Mode Issue (filesystem state: read only)
resume
clean
dpkg
fsck
grub
network
root
system-summary
This issue has been produced in
safe-mode.
The larger portion of our
collective has been focussed
on the upcoming publishing of
Hackbibel 3 - The hackening.
Stay tuned while we organize to
return to our normal(tm)
routine.
<OK>
Press Enter for maintenance
(or pres Control-D to continue):
root@datenschleuder:~#