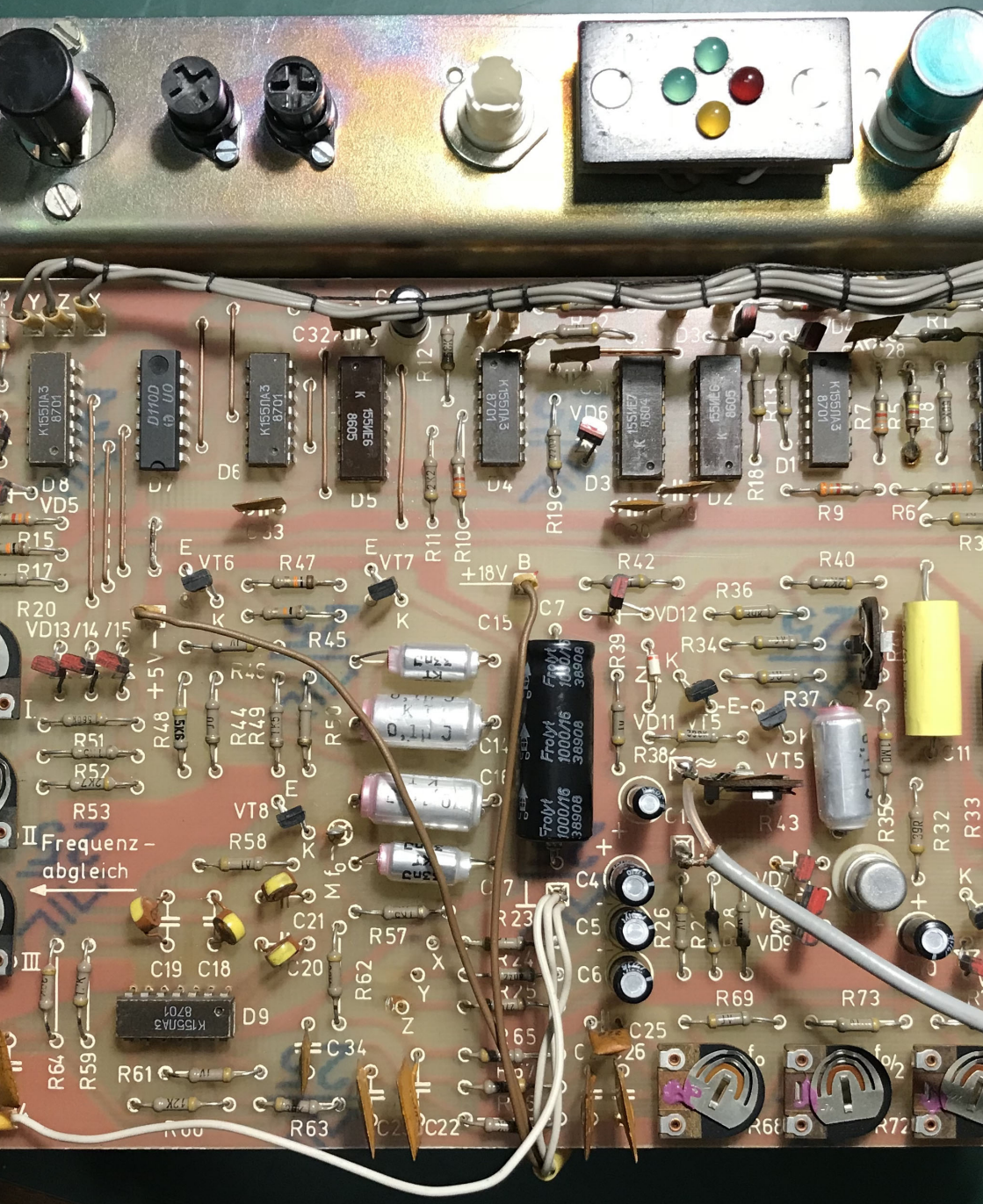
die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

ISSN 0930-1054 • 2019
250000000 µcent

#100



Das große Datenschleuder-Leser-Bilderrätsel (Seite 0x22)

```
[redaktion@zentrifuge ~/Datenschleuder]$ echo 'Endlich! ist
die erste Ausgabe der "datenschleuder" fertig. Du hälst sie
in Händen.' | sed ' s/erste/hundertste/ ; s/\"\([a-z]\+\)\"
/\\enquote\{\1\}/; s/hälst/hältst/'
```

Geleitwort

Endlich! ist die hundertste Ausgabe der „datenschleuder“ fertig.
Du hältst sie in Händen.

Das muss uns erst einmal einer nachmachen, den ersten Satz der ersten Ausgabe für die hundertste (fast) zu kopieren. Wie man sieht, ist das mit dem „Endlich“ so geblieben. Das gilt definitiv und wird wohl auch weiterhin so sein.

Wir als Datenschleuder-Redaktion haben in den letzten Monaten ganz klar gelernt, wie schwierig es ist, diese Zeitung am Leben zu erhalten. Aber so ist das mit Leidenschaften, man muss sie im Alltag pflegen, damit sie nicht untergehen. Trotzdem – oder vielleicht auch gerade deswegen – ist hier die #100. Und wir werden weiter daran arbeiten, dass die Reanimation nicht umsonst war.

Immerhin – um kurz die Eckdaten zu nennen – haben unsere Vorgänger und wir es geschafft diese Zeitschrift in 35 Jahren von einer knapp dreistelligen zu einer Auflage von 9200 Schleudern zu bringen. In der Zwischenzeit wurde mehrfach der Produktionsprozess umgestellt und mittlerweile schreiben das hier Menschen, die die erste Ausgabe nicht einmal erlebt haben.

Wir haben uns also ein bisschen umgesehen und, passend zum Motto des 35C3, „Refreshing Memories“ weitergeführt. Dabei haben wir viele neue Entdeckungen gemacht und festgestellt, dass jeder Blickwinkel andere Schätze offenbart.

Angesichts dieser Erfahrungen wollen wir euch, unsere Leser*innen, herzlichst dazu einladen, eure Erinnerungen an die ersten 100 Ausgaben mit uns zu teilen. Schreibt uns eine E-Mail an <ds@ccc.de> oder verwendet die Bastel-Postkarte am Ende des Hefts. Die Postkarte benötigt innerhalb Deutschlands keine Briefmarke. Allerdings muss dann der Club für das Porto aufkommen. Daher freuen wir uns besonders, wenn ihr eine Marke draufklebt, oder die Chaospost auf der nächsten größeren CCC-Veranstaltung nutzt. Wir freuen uns auf jede Art von Feedback, aber auch einfach darauf, unterschiedliche Wahrnehmungen zu sehen. ↪

Inhalt

Um euch auf diesen Rückblick einzustimmen, haben wir in dieser Ausgabe zwei zurückschauende Artikel für euch. Der eine bedankt sich äußerst herzlich bei der Schuhandelskette „CCC“ für die Erkenntnis der Dringlichkeit zur Behebung des Namenskonfliktes (Seite 0x23). Der zweite Artikel zu dieser Gruppe der Rückblicke befasst sich mit „groff“, ein Textsatzsystem, dass seine Arbeit heutzutage meist im Verborgenen tut. Jeder nutzt es und kaum einer weiß, dass er es tut. Ein Beitrag darüber, wieso ein Rückblick auch auf Softwareebene lohnend sein könnte (Seite 0x25).

Da der Rückblick die Welt jedoch nicht anhält, haben wir selbstverständlich auch brandaktuelle Themen im Repertoire. So haben wir einige Diskussionen vom 35C3 mitgenommen: Der C3W hat die Gelegenheit genutzt und möchte gerne einige Punkte seiner neuen Unvereinbarkeitserklärung in den Zusammenhang der Entwicklungen in Österreich stellen und erläutern (Seite 0x10). Insgesamt passt sie die Gedanken der Unvereinbarkeitserklärung des Clubs an die aktuelle örtliche Lage an: „Ideen von Rassismus, Ausgrenzung und damit verbundener struktureller und körperlicher Gewalt“ [1] haben im Club und somit auch in den Erfas keinen Platz.

Neben dieser festen Einstellung ist der Club jedoch glücklicherweise so bunt wie eh und je. Einen kleinen Einblick über die unterschiedlichen Aktivitäten haben wir ebenfalls zusammengestellt. So zeigt unsere Datenschutzbeauftragte, was bei den Strukturen im Club bezüglich der DSGVO zu beachten ist und wie sich die Umsetzung auswirkt (Seite 0x15). Neben dem Papierkram, der zur Strukturverwaltung gehört, hat sich auch eine der „tuwat“-Arbeitsgruppen nicht nehmen lassen, ihre Arbeit bei uns zu präsentieren. Die Gruppe KRITIS beschreibt den Grund für ihre Existenz und die Forderungen, die sie nach Betrachtung der Situation für kritische Infrastrukturen in Deutschland vorgefunden haben, entwickelten.

Die politische Arbeit, die im Club und den Erfas passiert, ist wertvoll und wichtig. Dennoch ist sie nur ein Teil des Chaos. Wir wollen auch einen Blick auf die lokalen Entwicklungen in den Erfas und Chaostreffs werfen. Dies ist ja meistens der Grund dafür, dass die Chaosfamilie weiterhin Zuwachs bekommt: Potsdam hat einen neuen, eigenen Chaostreff. Da haben wir natürlich direkt mal nachgefragt, um euch zu zeigen, was da so läuft (Seite 0x2C). Außerdem stellt sich das Chaos in Siegen, neuster Bewerber um den Status eines Erfa-Kreises, vor (Seite 0x31). Wenn ihr daraufhin Lust bekommen habt, in anderer Orte Chaos zu schnuppern, findet ihr wieder alle Erfas und Chaostreffs in unserer Übersicht (Seite 0x29). Neben direkten Besuchen lohnt sich natürlich auch immer die Verknüpfung mit einer lokalen Veranstaltung. Der CCC Dresden lädt beispielsweise herzlichst zu den Datenspuren zum Thema „Patch gehabt“ ein (Seite 0x2B).

Patches können tatsächlich ein nützliches Mittel sein, um Fehler zu beheben. Allerdings beschleicht uns nach der Lektüre der übrigen Artikel in dieser Aufgabe der Verdacht, dass das nicht für das Schweizer E-Voting gilt. In einem Artikel stellt der CCC-CH daher einmal grundlegend die Problematik vor und diskutiert ausführlich die Schwierigkeiten „Sicherheit“ zu garantieren (Seite 0x04). Anschließend werdet ihr jedoch feststellen, dass die Probleme in der Praxis an ganz anderen Stellen zu finden sind … (Seite 0x0B)

Wie ihr seht, haben wir wieder einmal ein vielseitiges Programm quer durch den Club und das, was ihn bewegt, zusammengestellt. Wenn ihr darüber hinaus Themen im Kopf habt, die ihr gerne einmal in der Datenschleuder finden würdet oder aber selbst etwas zu

berichten habt, gilt der obige Aufruf auch über Erinnerungen hinaus.

Wir freuen uns sehr auf den Dialog mit euch. Aber jetzt erst einmal viel Freude beim Lesen und Stöbern.

Referenzen

[1] Vorstand des CCC e. V.: „Farbe bekennen gegen Rechts“ (08.05.2005), https://www.ccc.de/de/updates/2005/unvereinbarkeitserklaerung

Wichtige Information des CCC e. V.

Seit einigen Monaten bietet der CCC e. V. seinen Mitgliedern an, aktuelle Informationen über den Verein zu erhalten. Wenn du Mitglied bist und – außer der Einladung zur Mitgliederversammlung und der Bestätigung deiner Beitragszahlung oder Datenänderung – diese Nachrichten bekommen möchtest, sende eine Mail an <office@ccc.de> und bitte darum das Informieren-Flag auf *True* zu setzen.

Die Datenschleuder Nr. 100

Herausgeber
(Abos, Adressen, Verwaltungstechnisches etc.)

Chaos Computer Club e. V., Zeiseweg 9, 22765 Hamburg
<office@ccc.de> PGP: 2A75 2EB3 D0A0 5FA9 2726 2B8A A917 2CC7 B794 A17A

Kontaktadresse
(Artikel, Leserbriefe, Inhaltliches)

Redaktion Datenschleuder, Chaos Computer Club e. V., Zeiseweg 9, 22765 Hamburg <ds@ccc.de>
https://ds.ccc.de/

Redaktion dieser Ausgabe

Jan „vollkorn“ Girlich, dome, TVLuke, Hanno „Rince“ Wagner, Marei Peischl

V. i. S. d. P.

Hanno „Rince“ Wagner

Titelbild:
Via Lewandowsky: Fazit, 2011
© VG Bild-Kunst, Bonn 2019
Rückseite:
Robert Anders

LaTeX-Backend, Satz & Layout

„TeXhackse“ Marei Peischl

Druck

Pinguin Druck Berlin http://pinguindruck.de/

Zum „Schweizer“ Cybervoting: das Vertrauensproblem bleibt ungelöst

von Claudio Luck und Hernâni Marques
Vorstände und Pressesprecher CCC Schweiz <vorstand@ccc-ch.ch>

Das Projekt mit offiziellem Namen „Vote électronique“ (auch E-Voting oder weniger positiv konnotiert Cybervoting) läuft seit dem Jahr 2000. Es handelt sich dabei um ein Projekt der Bundeskanzlei – eine Stabsstelle der Schweizer Landesregierung (bekannt als Bundesrat), ganz ähnlich wie in Deutschland das Bundeskanzleramt. [1] Das primär vorgegebene Ziel ist es, das elektronische Abstimmen und Wählen der Zeit anzupassen – eine besondere Not dafür ist nicht angezeigt; insbesondere da das Abstimmen und Wählen in der Schweiz als Urnen- und Briefwahl akzeptiert ist. Hochrechnungen liegen an Abstimmungssonntagen unmittelbar nach Urnenschluss um 12 Uhr vor und Endergebnisse sind schon nach wenigen Stunden bekannt: einzelne Kantone oder Städte benötigen immer wieder länger oder haben auch einmal Probleme, doch an den Endergebnissen insgesamt ändert das nichts. Die aktuellen Verfahren genießen Vertrauen. Daran rütteln nun der Bundesrat und die Regierungen der Kantone (wie in Deutschland Bundesländer) verstärkt.

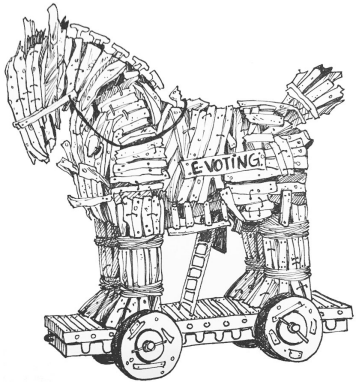
Ähnlich wie bei Wahlcomputern oder Wahlstiften [2] in Deutschland sehen wir uns in der Schweiz damit konfrontiert, dass Computerwahlen immer stärker verbreitet werden. Dabei handelt es sich bei der Form von E-Voting, die wir in der Schweiz haben, zusätzlich noch um wesentlich komplexeres E-Voting. Es wird über das Internet durchgeführt und ist somit – wie treffend im Logbuch:Netzpolitik Ausgabe 286 gesagt wurde [3] – tatsächliches Cybervoting, welches zudem „zeitsouverän“ ist, weil grundsätzlich von überall her abgestimmt werden kann. In den ersten Jahren hat die Bundeskanzlei zusammen mit interessierten Kantonen Grundlagen erarbeitet und seit 2004 finden praktische Versuche mit Cybervoting statt. Die daraus resultierenden Stimmabgaben fließen summarisch in die Endergebnisse ein. Von den ursprünglich 22 137 zugelassenen Cybervotern alleine im Kanton Genf (September 2004), waren für die Abstimmungen vom 10. Februar 2019 bereits 226 635 Credentials auf zehn Kantone verteilt, um Stimmen vollelektronisch ohne jeden Papertrail einzuspeisen.

Widerstand nötiger denn je

Der Erfakreis Zürich (CCCZH) hat sich 2013 erstmals öffentlich gegen Cybervoting geäußert – mit einem offenen Brief an das Zürcher Kantonsparlament, um den Kanal „elektronische Stimmabgabe“ aus dem Wahlgesetz streichen und Cybervoting somit verbieten zu lassen. [4] Der Antrag aus linken und rechten Kreisen scheiterte. Vordringlich wird die Lage seit April 2017 – da verkündet der Bundesrat per Medienmitteilung „[…] nächste Schritte zur Ausbreitung der elektronischen Stimmabgabe“ beschlossen zu haben. Ziel ist es, bis zu den Parlamentswahlen 2019 zwei Drittel der Kantone (Gesamtzahl Kantone: 26) mit dem Cybervoting zu beglücken [5]. Dieses Ziel konnten wir torpedieren [6].

Beginnend mit 2018 haben wir, nach längeren Mailthreads mit der Bundeskanzlei und einem Gespräch vor Ort, nicht nur die medialen Interventionen massiv verschärft [sie-

he 7], sondern auch angefangen demonstrative Hacks durchzuführen, um auf die grundsätzlichen Probleme des Cybervotings in Web-Voting-Form hinzuweisen: Danilo Bargen vom Coredump Rapperswil [8], ein Hackerspace des CCC-CH, hat beispielsweise gezeigt, wie auf den Endgeräten durch ein malignes Add-On das Stimmgeheimnis aufgehoben werden kann: abgesehen davon ist der Angriff geeignet, um Abstimmende an der Ausübung des Stimmrechts zu hindern – sollte beispielsweise die „falsche“ Wahl getroffen werden. [9]



Symbolbild „Trojanisches Pferd“ von Míka Eríksdóttir

Im November 2018 haben Volker Birk und andere Aktivisten des CCCZH [10] schließlich einen DNS-Spoofing-Angriff auf das Genfer System demonstriert, was durch den Umstand begünstigt wurde, dass weder HSTS-Preloading von Google noch DNSSEC der IETF aktiviert war [11]. Die Betreiber haben den Missstand, bekannte Angriffe dieser Art zu verteuern, auch in der Folge nicht behoben, wohingegen das System der Schweizer Post unter evoting.ch beide Technologien im Einsatz hat – DNSSEC seit Februar 2019; wenn auch die Unterstützung auf Ebene der Resolver für DNSSEC auch in der Schweiz mager (bei rund 10 %) bleibt.

Wichtiger ist aber die politische Ebene: Aktivisten des CCC-CH ist es zusammen mit ExponentInnen praktisch des gesamten Parteienspektrums gelungen, ein Initiativkomitee auf die Beine zu stellen, das ein fünfjähriges Moratorium für das Cybervoting fordert [12]. Die Diversität des Komitees, das von ganz links bis ganz rechts über das demokratische Spektrum reicht, ist auch für Schweizer Verhältnisse, wo es immer wieder parteiübergreifend *sachpolitisch* zu temporären Seilschaften kommt (vgl. beispielsweise den Kampf gegen das Überwachungsgesetz BÜPF [13]) erstaunlich. Andererseits wird damit klargemacht, dass es kein typisch parteipolitisches Thema mit Links-Rechts-Schema ist, sondern eines, wo es um alles geht: das Vertrauen in das politische System der Schweiz. Und: weil es offenkundig ist, dass die Bundeskanzlei zusammen mit einigen kantonalen Regierungen das Cybervoting verbreiten möchten, ist es unabdingbar, dass der politische Druck *schweizweit* erhöht wird, um dies zu verhindern. Die effektive Unterschriftensammlung, um eine Volksabstimmung über das Thema Cybervoting zu erzwingen, hat schließlich am Samstag, 16. März begonnen.

Nun haben wir zusammen mit den parteipolitischen und anderen Akteuren 18 Monate Zeit, um 100 000 gültige Unterschriften zu sammeln und (ironischerweise) bei der Bundeskanzlei einzureichen, die das Zustandekommen der Volksinitiative prüfen muss. Genauso ironisch ist, dass der Initiativtext von der Bundeskanzlei geprüft wurde – allerdings muss betont werden, dass es innerhalb der höchsten Stabsstelle auf Bundesebene diverse Abteilungen gibt. Das Cybervoting ist eine eigene Abteilung. Im Wesentlichen fordert die Initiative, dass Abstimmungen und Wahlen nicht nur ohne besondere Sachkenntnisse nachvollziehbar

sind – ähnlich wie beim Urteil des Deutschen Bundesverfassungsgerichts gegen Wahlcomputer, sondern auch, dass die Möglichkeit von Manipulationen nicht höher als bei Papierwahlen sein darf. Außerdem wird die Möglichkeit echter Nachzählungen gefordert – insgesamt Anforderungen, die mit heutigen uns bekannten ICT-Grundlagen äußerst schwierig zu erfüllen sein dürften, falls dies überhaupt je möglich sein sollte. Schließlich nimmt die Komplexität von ICT-Systemen tendenziell immer weiter zu und nicht etwa ab, wie dies nötig wäre, um IT-Sicherheit beherrschbar(er) zu machen.

Wie funktioniert das „Schweizer“ Cybervoting grundsätzlich?

Das Cybervoting der Schweiz soll flächendeckend als Web-Voting eingeführt werden. Abgestimmt wird mit beliebigen browserfähigen Geräten auf zentralen Webseiten der Schweizer Post oder der Genfer Staatskanzlei, wobei das Genfer System voraussichtlich zum letzten Mal im Februar 2020 zum Einsatz kommen wird.

Genf wirft – aufgrund der Notwendigkeit 2,3 Millionen Schweizer Franken zu investieren – schlichtweg das Handtuch. Und das, obwohl Genf seit mehr als zehn Jahre lang an ihrem Cybervoting-System gefeilt hat [14].

Die Schweizer Post baut unterdessen ihr System im Kern nicht selber, sondern hat dafür eine Kooperation mit der spanischen Firma Syctl, deren Motto „We Power Democracy“ lautet. Die Firma bietet elektronische Abstimmungslösungen (auch in Form von Wahlcomputern) in 42 (!) Ländern an: die Firmengeschichte ist, wie eine umfassende Recherche des Schweizer Online-Magazins Republik enthüllt hat, äußerst fragwürdig und schafft wenig Vertrauen [15]. Es ist ebenso wenig hilfreich, dass die Schweizer Post, zusätzlich zu ihrer Firmengeschichte als (Quasi-)Monopolist, in jüngerer Zeit mit Korruption aufgefallen ist: konkret wurde die Buchhaltung des Teilbetriebs PostAuto systematisch frisiert [16].

Die vorgeschlagene Spezifikation für ein „sicheres“ Cybervoting stammt von der Berner Fachhochschule (BFH), welche eng mit der Bundeskanzlei zusammenarbeitet: Es kommen Zero-Knowledge-Proofs, homomorphe Verschlüsselung und als zweiter Faktor ein Papierversand mit den Credentials (und Vergleichs- sowie Bestätigungscodes) zum Einsatz. Das Cybervoting der Schweiz kommt somit zur Zeit auch nicht ohne Papier aus [17]. Allerdings wurden bei anderen Systemen, wie in Estland, wo die Authentifikation mittels Personalausweis erfolgt, bereits erhebliche Sicherheitsprobleme durch Alex J. Halderman (akademisch spezialisiert auf Cybervoting) aufgezeigt [18, 19]. Trotzdem gehört die teilweise oder gar vollständige „Dematerialisierung“ zu den Zielen des Bundesrates, wie das aus dem Bericht der „Expertengruppe Vote électronique“ (EXVE) hervorgeht. [20]

Alleine der Umstand, dass für die elektronische Stimmabgabe weder besonders gesicherte Geräte noch ein persönlicher privater Schlüssel (z. B. im Personalausweis) zum Einsatz kommt, macht deutlich, dass skalierende Manipulationen, bei denen massenhaft Impersonation geübt wird, eine reale Gefahr sind: dies wird auch von den BFH-Forschenden nicht totgeschwiegen (vgl. S.134 der Spezifikation). Das „kryptografische Monster“ – wie das Republik-Magazin in einem weiteren Artikel treffend schreibt [21] – hängt sklavisch davon ab, dass die Credentials nicht abfließen bzw. in Kopie verkauft oder erhackt werden. Angesichts der Tatsache, dass es sich bei den Druckzentren für den Druck der Credentials um kantonale Betriebe ohne besondere elek-

tronische Abschirmung oder erhöhten Sicherheitsvorkehrungen handeln dürfte, sind das kühne Annahmen. Zumal hier quasi hundertprozentige Sicherheit unabdingbar ist. Korruption ist ebenfalls ein Problem, das nicht ausgeschlossen werden kann – schließlich kann durch das gewählte Verfahren auch massenweise für Nichtwählende abgestimmt werden (vgl. zu den grundsätzlichen Sicherheitsproblemen einschließlich der Einschätzungen einiger namhafter internationaler KryptoexpertInnen wie [22] und [23]).

Symbolbild „Abgründe“ von Míka Eríksdóttir

Zum eigentlichen Kern: Vertrauensprobleme ohne Ende

Des Pudels Problemkern beim Cybervoting ist aber nicht Sicherheit, sondern Vertrauen. Eine demokratische Abstimmung und Wahl muss dazu geeignet sein, nicht nur die Gewinnerseite, sondern auch eine Verliererpartei zufrieden zu stellen: in der Schweiz kommt es häufiger zu emotionsgeladenen Abstimmungskämpfen. Beispiele hierfür sind die Selbstbestimmungsinitiative oder die Masseneinwanderungsinitiative der SVP. Letztere wurde im Februar 2014 nur sehr knapp angenommen. Obwohl es spontan zu Protestkundgebungen linker Gruppierungen kam, hat niemand die Endergebnisse in globo angezweifelt. Solche Szenarien sind bei stärker verbreitetem Cybervoting, wie das geplant ist, sehr viel wahrscheinlicher, weil nur noch sehr wenige Akteure im Gesamtprozess involviert sind. Eine Auszählung bzw. ernstzunehmende Wahlbeobachtung wie bei der Papierwahl entfällt. Brisant ist, dass schon bei der heutigen Cybervoting-Verbreitung enge Abstimmungen und Wahlen knapp gekippt werden können. Eine wirkliche Gewissheit, dass dies nicht geschehen ist, gibt es nicht: man ist dem Prinzip Hoffnung ausgeliefert.

Beim Cybervoting besteht das grundsätzliche Problem, das die gesamte Kette im Ergebnis für einen normalen Bürger, aber auch für eine Kryptoexpertin nicht nachvollziehbar ist. Beispielsweise ist die Schweizer Post gezwungen, den Quellcode frei verfügbar zu machen, will sie ihr in Spanien eingekauftes Cybervotingsystem für 100 % des Elektorats eines Kantons zum Einsatz bringen. Dabei handelt es sich um rund 250 000 Codezeilen in der Programmiersprache Java, die von sehr hoher Komplexität geprägt sind [24]. Welcher Programmierer, welcher Kryptoexperte kann den gesamten Quellcode prüfen? Wie kann eine Bürgerin prüfen, ob dieser Code komplett unverändert läuft? Wie kann eine Bürgerin prüfen, ob die Toolchain, mit deren Hilfe der Quellcode in Bytecode übersetzt wurde, unverändert war? Wie kann ausgeschlossen werden, dass im letzten Schritt eine Hintertür eingeführt wird (Problem von „Reflections on Trusting Trust“ [25])? Baut die Schweizer Post den

Quellcode überhaupt selber oder kommt das Kompilat direkt aus Barcelona, wo Scytl den Hauptsitz hat?

Der Chaos Computer Club Schweiz (CCC-CH) ist der Ansicht, dass solcher Raum für Misstrauen und Spekulationen bei einem Abstimmungs- und Wahlsystem Gift für die Demokratie ist: Wir lehnen damit die Einführung von Cybervoting in der Schweiz resolut ab [26]. Wir machen hiermit auch klar, dass wir dezidiert sind, die Einführung von Cybervoting auf allen Ebenen zu bekämpfen und freuen uns hierbei auch um jede Unterstützung aus den CCC-Dezentralen in Deutschland und Österreich, denn: wird flächendeckendes Cybervoting in der Schweiz salonfähig, besteht akut die Gefahr, dass das auch in anderen Ländern Fuß fasst. Schließlich hat die Schweiz den Ruf einer stabilen und funktionierenden Demokratie mit umfassenden Mitbestimmungsrechten. Das Signal einer Schweiz, die Cybervoting einführt, ist für uns fatal. Wir möchten das verhindern und möchten erreichen, dass die Bundeskanzlei das Projekt nach fast 20 Jahren einstellt.

Happy Hacking!

Referenzen

[1] Bundeskanzlei BK: „Vote électronique“, https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting.html

[2] Website Kampagne gegen Wahlcomputer, https://wahlcomputer.ccc.de/

[3] Tim Pritlove (14.02.2019): „LNP286 Zeitsouveränes Cybervoting“, https://logbuch-netzpolitik.de/lnp286-zeitsouveraenes-cybervoting

[4] Fabian Vogt (11.11.2013): „E-Voting in Zürich soll verboten werden“ https://www.computerworld.ch/business/digitalisierung/e-voting-in-zuerich-verboten-1332552.html

[5] Mitteilung des Bundesrates über nächste Schritte zum E-Voting, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-66273.html

[6] https://www.watson.ch/

[7] Medienspiegel des CCC-CH: https://www.ccc-ch.ch/category_pressreview.html

[8] Website des Hackerspace Rapperswil: https://www.coredump.ch/

[9] Danilo (17.06.2018): „Verletzung Stimmgeheimnis E-Voting SG“, https://www.coredump.ch/2018/06/17/verletzung-stimmgeheimnis-e-voting-st-gallen/

[10] Website des Chaos Computer Clubs Zürich: https://www.ccczh.ch/

[11] https://www.srf.ch/news/schweiz/elektronische-abstimmungen-hacker-finden-schwachstelle-im-groessten-schweizer-e-voting-system

[12] https://e-voting-moratorium.ch/

[13] https://stopbuepf.ch/

[14] https://www.nzz.ch/schweiz/e-voting-genf-will-eigenes-system-nicht-weiterfuehren-ld.1440276

[15] Adrienne Fichter: „Das heikle Geschäft mit der Demokratie“ (31.01.2019), https://www.republik.ch/2019/01/31/das-heikle-geschaeft-mit-der-demokratie

[16] Florian Imbach: „Postauto-Skandal – So lief der Offerten-Schwindel“ (14.02.2018), https://www.srf.ch/news/schweiz/postauto-skandal-so-lief-der-offerten-schwindel

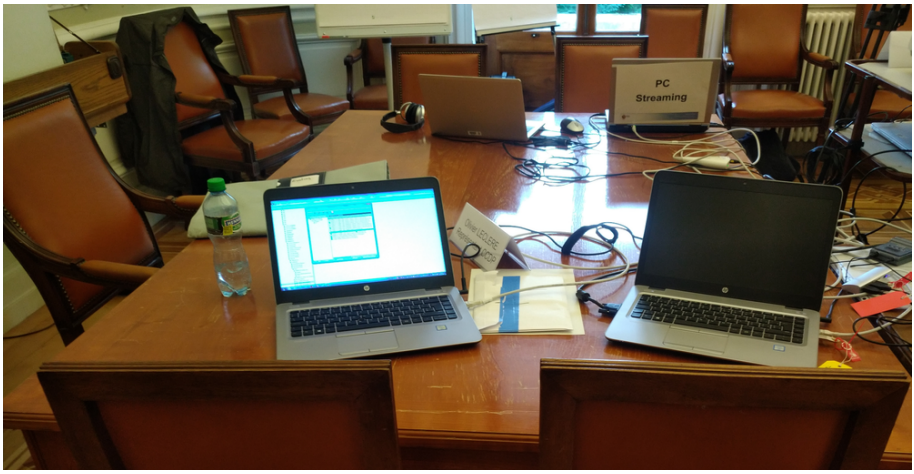
[17] „Cryptology ePrint Archive: Report 2017/325“, https://eprint.iacr.org/2017/325

[18] https://estoniaevoting.org/

[19] https://media.ccc.de/v/31c3_-_6344_-_en_-_saal_1_-_201412281400_-_security_analysis_of_estonia_s_internet_voting_system_-_j_alex_halderman

[20] https://www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/berichte-und-studien.html
[21] Patrick Recher: „Ctrl-Alt-R – 10 neue Erkenntnisse zum E-Voting der Post“ (01.03.2019), https://www.republik.ch/2019/03/01/10-neue-erkenntnisse-zum-e-voting-der-post
[22] Christoph Krummenacher: „E-Voting der Post lässt sich nicht schützen sagt Chaos Computer Club“ (19.02.2019), https://www.nau.ch/politik/bundeshaus/e-voting-der-post-lasst-sich-nicht-schutzen-sagt-chaos-computer-club-65486021
[23] Tom Sperlich: „Die Schweiz kurz vor dem Härtetest ihres E-Voting-Systems“ (23.03.2019), https://www.heise.de/newsticker/meldung/Die-Schweiz-kurz-vor-dem-Haertetest-ihres-E-Voting-Systems-4316841.html
[24] Piratenpartei Zentralschweiz: „Piratenpartei Zentralschweiz republiziert den Source Code des E-Voting“ (03.03.2019), https://ppzs.ch/2019/03/piratenpartei-zentralschweiz-republiziert-den-source-code-des-e-voting/
[25] Ken Thompson: „Reflections on trusting trust“ (1984), https://dl.acm.org/citation.cfm?id=358210
[26] CCC-CH: „CCC-CH ruft zum Boykott vom E-Voting-Stimmkanal auf und fordert statistisch kontrolliertes E-Counting“, https://www.ccc-ch.ch/ccc-ch-ruft-zum-boykott-vom-e-voting-stimmkanal-auf-und-fordert-statistisch-kontrolliertes-e-counting.html


EIN MAL KATZE IM SACK.
www.ruthe.de
Ruthe



Vertrauensverlust nach Cybervoting-Wahlbeobachtung

von Claudio Luck und Hernâni Marques
Vorstände und Pressesprecher CCC Schweiz <vorstand@ccc-ch.ch>

Die Schweizer Cybervoting-Systeme (auch E-Voting-Systeme) bauen stark auf Kryptographie auf. Die Wahlkommission – bestehend aus gewählten Politiker und Beamten – soll die Sicherheitselemente initialisieren und handhaben. Die Sicherheitsannahme der ganzen Abstimmung oder Wahl hängt vom vorsichtigen Umgang damit ab. Das verunsicherte zwei Hacker vom CCC Schweiz, die sich darauf als Wahlbeobachter beim „Genfer System“ empfahlen. Ein Erlebnisbericht.

Während unserer Wahlbeobachtung am 23. September 2018 setzten sechs (von 26) Kantone auf das „Genfer System“: Aargau (AG), Basel-Stadt (BS), Bern (BE), Luzern (LU), St. Gallen (SG) und Genf (GE) selbst. Die Kantone lagern die gesamte Abwicklung des Cybervotings an die Staatskanzlei des Kantons GE aus. Sie behalten sich das Recht vor, eigene Leute zu entsenden. Jedoch macht kein Kanton mit Ausnahme vom Kanton SG davon Gebrauch. Die Kantone AG, BS, BE und LU übten im September selbst keinerlei für uns sichtbare Kontrolle aus.

Das offizielle Setting

Wir sind mit über 20 Leuten in einem Saal, die meisten haben eine offizielle Rolle inne.

Einige hingegen überwachen offenbar uns. Auch die Notizen, die wir auf Papier kritzeln, finden diskret zugeneigte LeserInnen.

Der Überblick ist von unserem Sitz aus hervorragend. Direkt vor uns ist eine Kamera auf-

gebaut. So sehen wir drumherum direkt auf den Kabelsalat. Ein Laptop zeigt eine E-Mail mit einem Passwort in großen roten Lettern. Sowieso sind die ganzen Laptops bereits aufgebaut, wenn die Wahlkommission eintrifft. Ob sie zwischenzeitlich manipuliert wurden, kann sie also nicht ausschließen. Auch wir als Wahlbeobachter sehen uns bei rechtzeitiger Ankunft mit dem fertigen Setup konfrontiert. Im weiteren Verlauf glaubt die Wahlkommission blind den Ergebnissen, die sie von diesen Laptops, via Projektor dargestellt, sieht.

Das rote Passwort weicht später einer TeamViewer-Session, womit sich die zwei Repräsentanten vom Kanton St. Gallen zuschalten, der einzige Kanton (außer Genf selbst), der sich um etwas (virtuelle) Kontrolle bemüht.

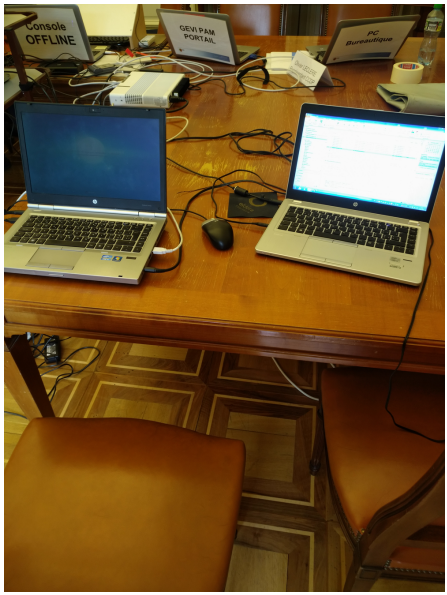
Wir erhalten noch eine Papierkopie des Sollprotokolls, der als „NON PUBLIQUE“ klassifiziert ist, und fragen uns, wer grad über TeamViewer alles mithört.

Auf den ersten Blick

Die ganze Wahlbeobachtung ist langweilig und repetitiv, weil man Systemadministratoren zuschaut, wie sie Dateien, die alle fast gleich heissen, schrittweise zwischen Remote-Desktops und lokalen Speichermedien kopieren, sie dort vor- und nachbearbeiten sowie zwischendurch auf die Offline-Arbeitsstation transferieren. Währenddessen werden Prüfsummen der verschlüsselten und entschlüsselten elektronischen Wahlurnen vom Bildschirm ins Protokoll geschrieben und später verglichen. Genau genommen nur die ersten und letzten fünf Zeichen davon, was kryptografisch 40-bittiger Schwachsinn ist.

Etwas Hektik kommt im Saal auf, sobald die Kommissäre auf der Offline-Konsole die Passwörter zum geheimen Schlüssel preisgeben müssen. Auffallend demonstrativ laufen die Systemadministratoren, die sonst alle Systeme stellvertretend für die Wahlkommission bedienen, ans andere Ende des Saals. Ganz unauffällig hingegen lesen die Kommissäre bei der Eingabe der Passwörter von ihrem Handy ab. Dies ist angesichts der zu erwartenden Angriffe auf genau diese Geheimnisträger grobfahrlässig. Dass die sichere Offline-Verwahrung des geheimen Schlüssels durch den Handyeinsatz komplett dahinfällt, lässt die beobachtende Wahlkommission kalt. Alleine dies wäre ein plausibler Grund um die Fairness und auch die Integrität der Wahl auf der Stelle zu bezweifeln.

Die Wahlbeobachtung ist also doch elektrisierend, weil dem durchschnittlich aufmerksamen Hacker bei fast jedem Handgriff gewichtige Mängel im Sicherheitskonzept auffallen.



Schwierige Schlüsselsicherung

Die Sicherheit der elektronischen Urne beruht darauf, dass die geheimen Schlüssel ab-

solut vom Internet fern gehalten werden („air-gapped“) und auch sonst nicht abfließen. Es ist aber anzunehmen, dass das „Offline“-Laptop, das mit Windows bestückt ist und aus dem normalen Beschaffungswesen des Kantons Genfs entstammt, durchaus irgendwie mit Updates aus dem Internet versorgt wird – ein Angriffspunkt, allen voran für staatliche Akteure. Auch das Gebäude ist elektronisch nicht abgeschirmt, so dass mit entsprechendenem Aufwand auch der Airgap keine wirkliche Hürde ist.

Die Passworthandhabe ist auch sonst eine Show. Dass die Kommissäre ihre Handys als Gedankenstütze einsetzen, ist bereits der GAU, wenn nicht sogar ein Super-GAU. Die Tastatur ist zwar verdeckt, aber trotzdem anfällig für „Schultersurfen“. Dafür besonders suspekt positioniert ist ein ungenutzter smarter TV-Flachbildschirm, der schräg hinten in der Ecke steht und alles spiegelt: wer weiß, ob der auch eine Webcam eingebaut hat. Im öffentlichen Bugtracker zur Genfer Cybervotingsoftware ist ein weiteres Problem dokumentiert: Die Software zeigt die Eingaben in das Passwort-Feld offenbar im Klartext an, statt – wie üblich – durch Punkte: Es gäbe dafür ein „Business Requirement“, da diese „political people“ nicht sehr geübt im Umgang mit Computern seien und es sonst wiederholt zu Eingabefehlern käme [1]. Es ist aber sowieso unklar, mit welcher Software hier wirklich gearbeitet wird und konkret die Endergebnisse erzeugt werden. Der veröffentlichte Quellcode des Genfer Systems ist weder vollständig noch auf dem neusten Stand.

Weiter in den Hash-Spielen

Da gleichzeitig Abstimmungen auf Bundesebene und eine freie Personenwahl im Kanton St. Gallen durchgeführt werden, wiederholen sich viele Schritte, die sich nur in Details unterscheiden. So fällt unter allgemeinem Gelächter plötzlich auf, dass der vorher notierte Hashcode des anderen Laufs verglichen wird – also wohl die falsche Seite des Protokolls abgearbeitet wurde.

Die Panne

Bei der Nachbearbeitung der ausgezählten Ergebnissen des Kanton St. Gallen wird eine erwartete Datei ohne Fehlermeldung einfach nicht generiert. Auch die Wiederholung der Schritte bringt keine Besserung, so dass die Sitzungsleitung beschließt, diesen Lauf zu unterbrechen und eine Pause einzuberufen.

Nach der angekündigten vorübergehenden Verweisung aus dem Saal (die Zwischenergebnisse sind zu dem Zeitpunkt noch Amtsgeheimnis) kommen wir rechtzeitig auf den Anfang der Pause zurück. Die Wahlkommission verweilt draußen bei Kaffee und Croissants, während die Techniker im Saal alleine detaillierte Debug-Logs studieren, von deren Existenz die Wahlkommission wohl keine Kenntnis hat. Keiner dieser Schritte ist im ausgehändigten Protokoll beschrieben.

Lockere Pause

Gegen Ende der langen Pause flanieren wir nochmals an der ganzen IT-Ausrüstung vorbei und versuchen nachzuvollziehen was mit welchem Kabel verbunden ist.

Plötzlich fällt uns auf, dass wir ja ganz alleine im Saal stehen. In diesem Moment hätten wir beliebige Handlungen an allen Geräten vornehmen können – z. B. präparierte USB-Sticks einstecken, um nach Wiederaufnahme der Sitzung mittels autorun ein Chaos zu stiften.

Es stellt sich beispielsweise die Frage, was eigentlich wäre, wenn plötzlich ein lächelnder Putin oder Trump projiziert würde. Wie würde das in Social-Media ankommen? Wür-

de jemand den Ergebnissen der Kantone mit elektronischen Abstimmungen noch trauen? Wir realisieren, dass das Cybervoting in jedem Schritt an einem seidenen Faden hängt – und das kantonsübergreifend.

Außerplanmässige Lösung

Während der Pause kommt es mit der Staatskanzlei St. Gallen zur Absprache, dass man ohne die fehlende Datei auskomme. Der Plan ist also, weiterzumachen als ob nichts geschehen wäre. Unbegründeterweise wird angenommen, dass das Programm schlicht den Dienst verweigert hat, die Ergebnisse aber nicht verfälscht wurden.

Kopie zwecks Analyse

Zwecks weiteren Untersuchungen zur Panne wird aber noch eine Kopie eines der Speichermedien angefertigt und mit einer offiziellen Plombe (Kabelbinder) versehen. Auch das ist im Protokoll nicht vorgesehen. Es existiert nun also ein zusätzliches Speichermedium mit Daten über die Wahl.

Vertrauen entsteht nicht

Insgesamt fällt auf, dass es in der Praxis kein echtes Sicherheitskonzept gibt. Es mangelt bereits am Fundament für den Aufbau eines systematischen Information-Security-Management-Systems (ISMS).

Ein Bewusstsein für die Risiken scheint wenig ausgeprägt. Es gibt keine systematische Integration von baulichen, organisatorischen, personellen und technischen Mittel. Würde man das ISMS systematisch aufbauen, würde man die Zielkonflikte erkennen, die das Cybervoting inne hat. Es verlagert und konzentriert die Absicherung der Wahlen hin zur Wahlkommission, die jedoch wie die Bevölkerung selbst keine besondere IT-Kenntnisse hat, und mit praktisch völlig ungesicherten Geräten hantiert. Die Staatskanzleien üben zudem keine effektive Kontrolle aus.

Es liegt uns hierbei auch E-Mail-Korrespondenz mit am Genfer System beteiligten Kantone vor, die bestätigen, dass sie üblicherweise alles dem Kanton Genf und seiner Wahlkommission überlassen. Die Öffentlichkeit erfährt über abenteuerliche Operational-Security-Zustände und Pannen gar nichts. Offiziell zählt dieser Anlass nun offenbar zu den 200 und mehr „erfolgreichen Versuchen“ – wie die Bundeskanzlei gerne in den Medien betont und in einem „Faktenblatt – Vote électronique“ herausstreicht [2].

Wir haben bisher nur diese einzige Cybervoting-Wahlbeoachtung durchgeführt und sind schonmal entsetzt; wobei auch bei anderen Wahlbeobachtungen nicht immer alles reibungslos abläuft, wie ein vorhergehender Erlebnisbericht vom Journalisten Christoph Lenz im Tages-Anzeiger zeigt [3].

Dort hat zumindest das Word von Microsoft gestreikt, eine proprietäre Software, die in einer derart sensiblen Umgebung, wo Endergebnisse vollelektronisch ohne Nachzählungsmöglichkeit erzeugt werden, gar nicht erst zum Einsatz kommen sollte.

Der Versuch auch den Einsatz des zweiten Cybervoting Systems zu beobachten (das der Post) wurde uns im Februar von diversen Kantonen verwehrt – u. a. vom Kanton Thurgau, der sich auf das Amtsgeheimnis (!) berufen hat. Dies trägt weiterhin nicht zu unserem Vertrauen in Teilergebnisse, die mit Cybervoting generiert werden, bei [vgl. 4, 5].

Referenzen

[1] https://github.com/republique-et-canton-de-geneve/chvote-1-0/issues/20

[2] https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Faktenblatt%20E-Voting.pdf.download.pdf/Faktenblatt_DE.pdf

[3] https://www.tagesanzeiger.ch/schweiz/standard/Was-wenn-der-Tresorraum-der-Schweizer-Demokratie-geknackt-wird/story/29881888

[4] https://www.woz.ch/-958c

[5] https://www.tagblatt.ch/ostschweiz/frauenfeld/hacker-wenden-sich-wegen-e-voting-an-den-thurgauer-rechtsdienst-ld.1091346

Die Unvereinbarkeit in Wien

von fredl und pascoda
<pascoda_fredl@posteo.net>

Wir sind fredl und pascoda und schuld daran, dass Wien eine Unvereinbarkeitserklärung (UE) [1] hat. Pascoda studiert „Media and Human Centered Computing“ an der TU Wien, und fredl ist irgendwo in der IT unterwegs. Wir sind beide Vorstand im Chaos Computer Club Wien (C3W) und hatten auf einer Demo die Idee, die UE des CCC e. V. aus dem Jahre 2005 [2] in neuem Glanz erstrahlen zu lassen. Diese Idee fand sofort sehr viel Zuspruch im C3W und so haben wir, mit sehr viel großartiger Hilfe unserer Mitglieder, nicht nur die UE selbst geschrieben, sondern vielleicht sogar für etwas Frühlingswind in weiteren Erfas gesorgt.

Seither ist vieles passiert: Die Veröffentlichung hat weite Kreise gezogen [3]; Einige Erfas haben sich entschieden, es uns gleich zu tun; Viele haben sich bedankt. Deshalb, aber auch aus vielen anderen Gründen, wollen wir mit diesem Artikel die ganze Geschichte Revue passieren lassen.

Wer ganz ohne Umschweife unsere Erklärung zu unserer Unvereinbarkeitserklärung lesen möchte und wissen will, warum sie uns wichtig ist, ist im ersten Teil zu Hause. Wer den Kontext verstehen möchte, ist im zweiten Teil dieses Artikel richtig aufgehoben. Und diverse Ausdrücke, die außerhalb von Österreich (potentiell auch in Wien) schwierig zu verstehen sein könnten, haben wir für euch in einer Infobox gesammelt (Seite 0x14).

Unsere Unvereinbarkeitserklärung

Wir wollen mit unserer Unvereinbarkeitserklärung vor allem eine klare rote Linie für Vereinsveranstaltungen, wie unsere monatliche Treffen (das „Chaos. Communication. Caffeine.“), sowie die PrivacyWeek [4], etablieren. Sie soll aber auch ein klares Statement in Zeiten setzen, in denen Menschlichkeit mehr und mehr zu fehlen scheint. Immer wieder sind viele Organisationen und auch Personen(grup-

pen) im Umfeld des C3W, aber auch des großen Cs, sowie in lokalen Hackspaces der Meinung, dass der CCC unpolitisch wäre. Tatsächlich sind wir aber der Meinung: wer sich als „neutral“ oder aber auch unpolitisch positioniert, unterstützt den Status Quo, und damit die existierende Ungleichheit und Ungerechtigkeit unserer Gesellschaft. Deshalb können wir als Verein nur eines tun: Position beziehen, gegen Rechts.

Wir haben im Folgenden einige Teile unserer UE zitiert und versuchen zugleich unsere Beweggründe zu erklären. Es ist keine vollständige Auflistung der wichtigsten Punkte, sondern viel mehr eine Zusammenstellung jener Teile, die Erklärung benötigen könnten.

> *Der Chaos Computer Club Wien erklärt das Vertreten von Rassismus und die Verharmlosung der historischen sowie aktuellen rechten Gewalt für unvereinbar mit einer Mitgliedschaft. Dazu zählt für uns die Mitgliedschaft in entsprechenden Gruppierungen ebenso wie die Unterstützung derselben (etwa durch Mitarbeit im Wahlkampf oder bei Demonstrationen). Auch das „passive“ Befürworten rechten Gedankenguts stellt für uns ein absolutes „No Go“ dar und ist daher mit einer Mitgliedschaft im C3W nicht vereinbar.* [1]

Wir haben hier im Grunde das Hauptstatement der UE des CCC e. V. übernommen und mit einer für uns wichtigen Komponente ergänzt: Das „passive Befürworten“. Warum?

Während öffentlicher Widerstand zwar nicht jeder Person möglich ist, ist es durchaus machbar, etwa durch demokratische Mittel (zum Beispiel: die Teilnahme an Wahlen) oder auch auf anderen Wegen, für ein besseres Miteinander einzustehen. Wichtig ist: Es ist keine*r dazu verpflichtet offenzulegen wer wie gewählt hat, oder wer etwas gegen Rechts gemacht hat. Wer aber Handlungsmöglichkeiten relativiert („es gab ja nichts besseres zu wählen“ oder „ich habe ja nur das geringste Übel gewählt“) oder Organisationen Reichweite gibt (etwa durch Sticker, Buttons, T-Shirts, …) muss sich im Klaren sein, dass damit sehr wohl Ziele unterstützt werden, die eine*r*m selbst vielleicht nicht ganz passen. Ebenso muss beachtet werden, dass diese Ziele in letzter Konsequenz mit einer Mitgliedschaft im CCC nicht vereinbar sind.

> *Wer Verantwortung über staatliche Infrastruktur trägt, hat sich auch den Mitgliedern der Gesellschaft gegenüber für Fehlverhalten zu verantworten. Handlungen im Rahmen dieser Verantwortung müssen transparent und von allen Mitgliedern der Gesellschaft nachvollziehbar sein. Diese Machtposition darf nicht missbraucht werden.* [1]

Zugegeben, die Forderung nach Transparenz und dem verantwortungsvollen Umgang mit Macht ist in Österreich etwas naiv. So etwas wie eine Rücktrittskultur haben wir nicht. Politiker*innen bleiben trotz schlimmer verbaler Entgleisungen [5] oder Mitgliedschaften in rechtsextremen Verbindungen [6] im Amt. Mit dem Wehrrechtsänderungsgesetz 2019 erhält das Bundesheer umfassende Zugriffsrechte auf Stamm- und Metadaten. Alles, was es dafür braucht, ist die Berufung auf die „nationale Sicherheit“. Richter oder Staatsanwälte braucht es nicht. [7]

> *Überwachung bedeutet nicht Sicherheit, sie bleibt Überwachung. Sie bedeutet Einschränkung und Repression für jede*n. Besonders hart betroffen davon sind ohnehin die schwächsten Teile der Gesellschaft, benachteiligte und marginalisierte Gruppen, von denen einige in der aktuellen politischen Rhetorik*

*pauschal als Gefährder*innen gebrandmarkt und vorverurteilt werden. Der im aktuellen Regierungsprogramm skizzierte Kurs deutet auf einen weiteren massiven Ausbau derartiger diskriminierender und erniedrigender Praktiken hin. Diese lehnen wir entschieden ab.* [1]

Mit dieser Formulierung beziehen wir uns vor allem auf die Rhetorik und den Inhalt des berühmten, nicht tot zu bekommenden, Überwachungspakets [8]. Undefinierte „Gefährder", die einfach so auch in bisher privat geltenden Bereichen überwacht werden sollen und die Aussage, „nur Verbrecher benutzen Prepaid-Simkarten" (wenn tatsächlich oft einfach die finanziellen Ressourcen für einen Vertrag fehlen), seien als Beispiele erwähnt. Mittlerweile hat die Regierung eine Ausweispflicht beim Kauf von Prepaid-Simkarten erlassen. Warum, unter anderem, der pauschale Generalverdacht so problematisch ist, ist bereits in einer Stellungnahme [9] aus 2017 durch epicenter.works passend ausformuliert.

Die Besetzung der Regierungsposten im Kabinett durch den aktuellen Bundeskanzler und seinen Stellvertreter zeigt außerdem eine starke Tendenz zu nationalistischem, rassistischem und antisemitischem Gedankengut. Weiter ist anzumerken, dass die Rhetorik dieser Regierung gegenüber marginalisierten Gruppen üblicherweise von rechten bis rechtsextremen Gruppierungen verwendet wird. [1]

Burschen- und Mädelschaften in Österreich vertreten meist reaktionäres, teils rechtes bis rechtsextremes Gedankengut. Sie stellen Seilschaften dar, durch die Gleichgesinnte einander in ihren Karrieren unterstützen. Einige Mitglieder österreichischer Burschen- und Mädelschaften vernetzen sich aktiv international mit diversen Vertreter*innen der Identitären Bewegung und der Alt-Right. Weitere Details sammelt die „Forschungsgruppe Ideologien und Politiken der Ungleichheit" (FIPU) z. B. in ihrem Korporiertenkarrieren-Tracker [10]. Um nur einige Personalien der Regierung Kurz zu nennen, die brisante Verflechtungen nach Rechts besitzen und schon im Dezember 2017 bekannt waren: Vizekanzler/Minister für Sport und Öffentlichen Dienst ist HC Strache, Innenminister ist Norbert Hofer – beide sind Mitglieder in pennalen Burschenschaften (also Schülerverbindungen). Die 3. Nationalratspräsidentin Anneliese Kitzmüller ist Mitglied in einer Mädelschaft, also einer der wenigen Studentinnenverbindungen. Im Kabinett des Innenministers finden sich ebenfalls mehrere Mitglieder von Burschen- bzw. Mädelschaften.

Wer sich tiefer in die österreichische Politik Mitte-Rechts und etwa die Geschichte von FPÖ und Burschenschaften einlesen will, ist mit der Broschüre „Völkische Verbindungen" der Hochschüler*innenschaft der Universität Wien gut versorgt [11]. Einen kurzen Einblick in die Entstehung der Regierung Kurz und unserer Unvereinbarkeitserklärung liefern wir im nächsten Abschnitt.

Vergangenheit

Tag der Nationalratswahl 15.10.2017, etwa 17 Uhr:
Die ersten Hochrechnungen für die Nationalratswahl werden veröffentlicht.

Österreich atmet auf, denn ein gefühlt endloser Wahlkampf geht zu Ende – für viele jedoch mit Schrecken. Die Wahlen wurden um ziemlich genau ein Jahr vorgezogen, denn die SPÖVP-Koalition hatte sich quasi unheilbar zerrüttet. Und schon die Inhalte im Wahlkampf haben klar gemacht, in welche Richtung die ÖVP (jetzt: „Team Kurz – Die neue ÖVP") ge-

hen würde: ein Eintreten gegen Vermögens- und Erbschaftssteuern und eine „Mindestsicherung light“ für Menschen ohne österreichische Staatsbürgerschaft, Einsparungen bei „Bürokratie und fehlgeleiteten Sozialleistungen“, härtere Umsetzung des Dublin-Abkommens (aka Erschwerung der Flucht nach Österreich).

Nach den Wahlen ist klar:
eine Mehrheit im Parlament gibt es de facto nur durch eine schwarz-rote oder eine schwarz-blaue Koalition.

Am 25.10.17 beginnen die Verhandlungen für schwarz-blau. Im Verhandlungsteam der FPÖ finden sich einige problematische Personen, etwa Christian Höbart, der als Mitglied des Nationalrats auf Facebook Asylbewerber als „Erd- und Höhlenmenschen“ bezeichnete [5].

Nur zwei Monate nach der Wahl, am 18.12.2017, ist bereits Tag X:
die Angelobung der {schwarz|türkis}-{blau|braun}en Regierung durch den Bundespräsidenten steht an. Dies ist die zweite Regierung von FPÖVP nach 2000–2003 bzw. 2003–2007 (Teile der FPÖ hatten sich abgespalten, es entstand das „Bündnis Zukunft Österreich“, kurz BZÖ, die Regierung musste umgebaut werden). Von Februar bis September 2000 wurden Sanktionen seitens der damaligen EU-Mitgliedsstaaten gegen Österreich verhängt, weil befürchtet wurde, dass der Rassismus der FPÖ auf die Regierungsarbeit abfärben würde. Eine Erläuterung, warum die FPÖ nicht nur als rassistisch, sondern sogar als rechtsextrem einzustufen ist, liefert die Gruppierung „Stoppt die Rechten“ [12]. Einige Altlasten von damals beschäftigen die österreichische Justiz noch heute: Etwa der Eurofighter-Skandal um die Anschaffung neuer Abfangjäger, oder die Privatisierung der BUWOG [13].

Auf der Demonstration gegen die Angelobung, zu der relativ kurzfristig an einem Montagvormittag im Dezember offiziell etwa 5.500 Personen erscheinen, unterhalten sich die beiden Autoren über die öffentliche Haltung des C3W. Und eines wird klar: Wir müssen uns positionieren. Die Idee des Bedarfs für eine erneuerte Unvereinbarkeitserklärung entsteht.

Schon am nächsten Tag, am monatlichen Caffeine, wird die Idee besprochen und angenommen. Es findet sich rasch eine Gruppe, und binnen weniger Stunden steht ein erster Textvorschlag.

Wie am Caffeine beschlossen, wird die Unvereinbarkeitserklärung als Weihnachtsgeschenk pünktlich um 19 Uhr am 24.12.2017 auf der Website [1] veröffentlicht. Die Wiener Unvereinbarkeitserklärung ist geboren und wird mit sehr viel positivem Feedback angenommen.

Zukunft

Was uns die Zukunft bringt ist natürlich ungewiss, doch als Erfa des CCC werden wir weiterhin Position gegen Rechts beziehen, denn:

> *Wir sind eine galaktische Gemeinschaft von Lebewesen, unabhängig von Alter, Geschlecht und Abstammung sowie gesellschaftlicher Stellung, offen für alle mit neuen Ideen. Wer jedoch mit Ideen von Rassismus, Ausgrenzung und damit verbundener struktureller und körperlicher Gewalt auf uns zukommt, hat sich vom Dialog verabschiedet und ist jenseits der Akzeptanzgrenze. Wer es darauf anlegt, das Zusammenleben in dieser Gesellschaft zu zerstören und auf eine alternative Gesellschaft hinarbeitet, deren Grundsätze auf Chauvinismus und Nationalismus beruht, arbeitet gegen die moralischen Grundsätze, die uns als Club verbinden.* [2]

Infobox Austriazismen:

In Österreich werden Parteien oft mit „ihrer“ Farbe referenziert. Koalitionen erhalten entsprechende Kombi-Bezeichnungen. Blau: die Farbe und somit eine Bezeichnung für die Freiheitliche Partei Österreichs (FPÖ), die aus dem Verband der Unabhängigen (VdU) hervorgegangen ist. Die FPÖ ist seit jeher ein Sammelbecken für Alt- und Neonazis, deshalb oft Bezeichnungen/Wortspiele mit „braun“.
Rot: Farbe und somit Bezeichnung für die Sozialdemokratische Partei Österreichs (SPÖ).
Schwarz: war früher die Farbe und somit Bezeichnung der ÖVP. Mit Parteiübernahme durch Sebastian Kurz im Jahr 2017 erhielt die Partei ein neues Image als „Team Kurz – Die neue ÖVP“. Seither ist die neue Farbe (für alten Inhalt) Türkis, entsprechend auch hier die Wortspiele.

Referenzen

[1] Unvereinbarkeitserklärung des C3W https://c3w.at/posts/2017/unvereinbarkeitserklaerung/

[2] Vorstand des CCC e. V.: „Farbe bekennen gegen Rechts“ (08.05.2005), https://www.ccc.de/de/updates/2005/unvereinbarkeitserklaerung

[3] Tweet zur UE des C3W: https://twitter.com/c3wien/status/944991256031186945

[4] https://privacyweek.at/

[5] ORF.at: „Asyl: Mikl-Leitner kritisiert ‚Scharfmacher‘ Höbart und Babler“ (08.11.2014), https://orf.at/v2/stories/2252956

[6] Wikipediaeintrag Udo Landbauer, https://de.wikipedia.org/wiki/Udo_Landbauer

[7] Erich Moechel: „Bundesheer erhält Zugriff auf Daten bei Providern“ (24.02.2019), https://fm4.orf.at/stories/2965986/

[8] https://xn--berwachungspaket-izb.at/

[9] Angelika Adensamer, Alexander Czadilek, Thomas Lohninger und Christof Tschohl für epicenter.works „Stellungnahme [zum Sicherheitspolizeigesetz]“ (18.08.2017) https://epicenter.works/sites/default/files/epicenter.works_-_spg_bstmg_stvo_und_tkg_326_me_xxv_gp.pdf

[10] Forschungsgruppe Ideologien und Politiken der Ungleichheit (FIPU): Korporiertenkarrieren-Tracker (20.12.2017), https://forschungsgruppefipu.wordpress.com/2017/12/20/korporierten-karrieren-tracker/

[11] Broschüre „Völkische Verbindungen“ (2009), https://www.oeh.univie.ac.at/content/broschuerevoelkischeverbindungen

[12] Verein Stoppt die Rechten: „Ist die FPÖ rechtsextrem?“, https://www.stopptdierechten.at/think/warum-ist-er-rechts/

[13] Florian Klenk: „Supernaked: Die Akte Grasser als Film“ (12.12.2017), https://www.falter.at/archiv/wp/supernaked-die-akte-grasser-als-film

Datenschutz im Chaos Computer Club

von FrauHase <datenschutz@ccc.de>

Vieles wurde über den Datenschutz, die Datenschutzgrundverordnung (DSGVO) und das Bundesdatenschutzgesetz (BDSG) in den letzten Monaten und Jahren geschrieben. Man könnte fast meinen, dass es sich um eine völlig neue gesetzliche Regelung handelt. Doch was den Datenschutz angeht, war Deutschland Vorreiter.

Woher kommt der Datenschutz?

Häufig wird im Rahmen des Datenschutzes das Volkszählungsurteil von 1983 als Beginn des Datenschutzes genannt. Doch die Debatte um einen Schutz von persönlichen Daten auf automatisierte Art und Weise geht zurück in die sechziger Jahre des vorherigen Jahrhunderts. In den USA plante man die zentrale Registrierung aller US-Bürger und da es in den USA bis dahin kein zentrales Meldewesen gab, stieß die Regierung unter John F. Kennedy auf eine rege Debatte und letztlich scheiterte das Vorhaben. Doch der Ruf nach einem Gesetz zum Schutze der persönlichen Daten blieb und endete auch nicht vor Staatsgrenzen.

Aufgrund der weltweiten Diskussionen rund um den Datenschutz wurde im Jahr 1970 in Hessen das weltweit erste Datenschutzgesetz verabschiedet. Das erste Bundesdatenschutzgesetz folgte dann 1977. Nach den ersten deutschen Datenschutzgesetzen durften persönliche Daten nur dann verarbeitet werden, wenn eine gesetzliche Grundlage vorhanden war. Daher durften beispielsweise die persönlichen Daten durch das Meldegesetz in den Meldebehörden automatisiert verarbeitet werden. Diese Interpretation wurde dann durch das Volkszählungsurteil von 1983 korrigiert. Im Urteil wurde aus dem allgemeinen Persönlichkeitsrecht ein „Recht auf informationelle Selbstbestimmung“ abgeleitet und damit wurde im Urteil auch klargestellt, dass auch durch legitimierte Datenverarbeitung auf unzulässige Weise in die Grundrechte der betroffenen Personen eingegriffen werden kann.

Übrigens verabschiedeten die Amerikaner den Privacy Act 1974, in dem nur staatliche Stellen reguliert wurden. Auf europäischer Ebene gab es seit 1995 die Datenschutzrichtlinie 1995/46/EG, welche 25. Mai 2018 durch die DSGVO abgelöst wurde.

[3]

Was gilt ...

Damit wird klar, dass der Datenschutz kein neues Thema ist, auch wenn dies in den letzten Monaten und Jahren so geklungen haben mag. Die gesetzlichen Vorgaben gelten, sobald Daten, die einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können, automatisiert oder teilautomatisiert

verarbeitet werden. Diese Daten nennt man auch personenbezogene oder personenbeziehbare Daten.

Sobald also personenbezogene Daten in einem Dateisystem gespeichert werden, fällt diese Erfassung, Speicherung, Änderung etc. unter die DSGVO und das BDSG. Dabei ist es unerheblich, ob man ein eingetragener Verein ist oder nicht.

Entsprechend der ursprünglichen Idee des Datenschutzes darf nicht einfach mal alles gespeichert werden. Für die Speicherung oder Weitergabe von personenbezogenen Daten bedarf es entweder einer gesetzlichen Grundlage (z. B. bei der Speicherung von Mitgliedername und Kontaktadresse vorhanden) oder einer gesonderten Einwilligung. Diese Einwilligung muss freiwillig sein und ein Widerruf muss jederzeit möglich sein. Damit eine Einwilligung auch auf der freien Entscheidung einer Person beruhen kann, muss diese die Möglichkeit gehabt haben, sich ausreichend und auf verständliche Weise informieren zu können. Im Gegensatz zum alten BDSG kann eine Einwilligung auch mündlich oder elektronisch erfolgen.

Wer ist zuständig?

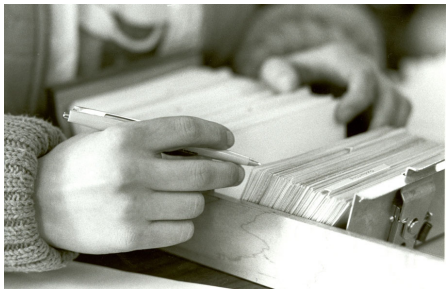
Sobald zehn oder mehr Personen mit der Verarbeitung von personenbezogenen Daten auf automatisierte oder teilautomatisierte Art und Weise befasst sind, wird ein Datenschutzbeauftragter gesetzlich vorgeschrieben. Die automatisierte oder teilautomatisierte Datenverarbeitung von personenbezogenen Daten kann dabei Tätigkeiten wie die Pflege der Mitgliederdatenbank und das Beantworten von Anfragen per E-Mail einschließen.

Sofern kein Datenschutzbeauftragter notwendig ist, heißt dies jedoch nicht, dass keiner für den Datenschutz verantwortlich ist. In einem Verein ist dann automatisch der Vereinsvorstand für die Einhaltung des Datenschutzes verantwortlich. So kommt es häufig vor, dass doch ein Datenschutzbeauftragter benannt wird, auch wenn es dazu keine formale Verpflichtung gibt.

Der Datenschutzbeauftragte sollte aufgrund seiner beruflichen Qualifikation und des Fachwissens benannt werden. Zu den Aufgaben des Datenschutzbeauftragten zählen unter anderem: Beratung der Mitglieder hinsichtlich Fragen und Pflichten zum Datenschutz, Überwachung der Einhaltung der datenschutzrechtlichen Vorgaben und die Beantwortung von Auskunftsersuchen.

Papiertiger

Das Verzeichnis von Verarbeitungstätigkeiten muss erst ab 250 Mitgliedern geführt werden. Insbesondere um einen Überblick über die Dienste zu erlangen, in denen personenbezogene Daten verarbeitet werden, kann es durchaus als sinnvoll erachtet werden, wenn das Verzeichnis auch bei weniger als 250 Mitgliedern erstellt und gepflegt wird. Die Angaben, die im Verzeichnis aufzuführen sind, werden in Artikel 30 Absatz 1 DSGVO beschrieben. Hierzu gehören der Name und die Kontaktdaten des Verantwortlichen, die Zwecke der Verarbeitung und die Beschreibung der Kategorien personenbezogener Daten usw.



[4]

Eine Datenschutzfolgeabschätzung wird in unserem Umfeld vermutlich weniger notwendig sein, da wir im Club-Umfeld weder Scoring oder automatisierte Entscheidungsfindung vornehmen, noch eine systematische Überwachung durchführen. Die Landesbehörden haben in der Regel Positivlisten veröffentlicht, also Listen in denen Tätigkeiten beschrieben werden, zu denen eine Datenschutzfolgeabschätzung durchzuführen ist. Über diese Positivlisten kann abgeglichen werden, ob eine Datenschutzfolgeabschätzung durchzuführen ist.

Informationspflichten und Auskunftsrechte

Der Grundsatz der Transparenz, wie dieser in Art. 5 der DSGVO genannt wird, führt zu Informationspflichten (Art. 12–14), dem der Club/Verein nachzukommen hat, denn es kann bei Verletzung dieser Pflichten durch die zuständige Datenschutzbehörde ein Bußgeld ausgerufen werden. So sollten auf dem Mitgliedsantrag und jedem anderen Formular, über das personenbezogene Daten erhoben werden, mindestens die in Art. 13 DSGVO genannten Informationen aufgeführt sein. Wer nun nicht selbst die Muße hat, um einen eigenen Text auszuarbeiten, kann auch auf das Muster im Praxisratgeber [1] „Datenschutz im Verein nach der DSGVO“, der vom Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg herausgegeben wird, zurückgreifen.

Auch das Auskunftsrecht, das jeder Bürger gegenüber einer Institution durch die DSGVO eingeräumt bekommt, basiert auf dem Grundsatz der Transparenz. Und das ist auch gut so, denn wie will man sonst wissen, wo Daten gespeichert sind, um gegebenenfalls weitere Rechte, wie beispielsweise eine Berichtigung geltend zu machen. Vor der Beantwortung einer Anfrage muss überprüft werden, ob überhaupt personenbezogene Daten über den Anfragenden verarbeitet wurden. Neben der Mitgliederdatenbank, sind hier auch Wikis, Mailinglisten und E-Mail-Postfächer mögliche Quellen. Das Ergebnis ist dann dem Anfragenden mitzuteilen. Sofern personenbezogene Daten verarbeitet werden, dann ist auch das eigentliche Auskunftsersuchen zu beantworten. Dieses kann beispielsweise Angaben über die Verarbeitungszwecke, die geplante Speicherdauer, Informationen zu den Betroffenenrechten wie Berichtigung, Löschung oder Einschränkung der Verarbeitung, einen Hinweis auf das Beschwerderecht bei der Aufsichtsbehörde etc. beinhalten.

Es ist bei der Bearbeitung eines Auskunftsersuchens wichtig zu beachten, dass die Auskunft binnen eines Monats zu erfolgen hat und nur in Ausnahmefällen eine Verlängerung der Frist möglich ist.

An dieser Stelle möchte ich einmal den Club lohnend erwähnen, da dieser jährlich an seine Mitglieder einen Auszug der über das Mitglied gespeicherten Daten versendet. Diesen Datenbrief [2] fordern wir als CCC übrigens seit 2010, um die informationelle Selbstverteidigung des Bürgers zu stärken und die Anhäufung von personenbezogenen Daten möglichst unattraktiv zu machen.

Rechte Betroffener wahren

Neben den zuvor genannten Rechten gibt es auch ein Recht auf Berichtigung, Sperrung oder Löschung. Das Recht auf Berichtigung kann ein Betroffener ausüben, wenn Daten fehlerhaft sind. Auch kann ein Betroffener die Löschung seiner Daten verlangen. In diesem Fall ist dann zu prüfen, ob die Daten noch aufgrund einer Rechtsgrundlage gespeichert bleiben müssen. So kann beispielsweise ein

Mitglied nicht verlangen, dass sein Mitgliedsdatensatz gelöscht wird. Aber es können Informationen, die rechtlich nicht notwendig sind, aus dem Datensatz gelöscht werden. Immer dann, wenn die Daten nicht gelöscht werden können, besteht ein Recht auf einen Sperrvermerk.

Auftragsverarbeitung

Wenn der Club einem Dienstleister Aufgaben überträgt und dabei auch die Weitergabe von Mitgliederdaten notwendig ist, dann ist ein Vertrag über diese Auftragsverarbeitung abzuschließen.

Beispielsweise ist ein Vertrag abzuschließen, wenn durch einen Dienstleister der Versand von Mitgliederschreiben oder Datenschleudern durchgeführt wird. Auch wenn die Mitgliederdaten bei einem Dienstleister gehostet werden, ist zu prüfen, ob ein Auftragsverarbeitungsvertrag abzuschließen ist.

Der Club muss dabei darauf achten, dass zur Absicherung der Mitgliederdaten ein ausreichender Schutz vorhanden ist. Es müssen dem Schutzbedarf der personenbezogenen Daten angemessene technische und organisatorische Maßnahmen ergriffen werden.

Technische und organisatorische Maßnahmen

Doch nicht nur bei der Auftragsverarbeitung, sondern auch bei der Verarbeitung von personenbezogenen Daten im Club-Umfeld sind diese technischen und organisatorischen Maßnahmen anzuwenden. Zu den technischen Maßnahmen gehören beispielsweise Maßnahmen wie Alarmanlage, Verschlüsselung sowie die Protokollierung von Erfassung und Änderung personenbezogener Daten. Zu den organisatorischen Maßnahmen gehören beispielsweise das Führen eines Gästebuchs, das Vier-Augenprinzip und ein Berechtigungskonzept.

Die Art der jeweiligen Maßnahme ist vom Schutzbedarf der zu schützenden Daten abhängig. D. h. es sind die Auswirkungen bei Nichtgreifen einer Maßnahme auf den Betroffenen zu bewerten. So sind bei Bekanntwerden einer Erkrankung die möglichen Auswirkungen für einen Betroffenen in der Regel höher als wenn der Name unbeabsichtigt veröffentlicht werden würde.

Fazit

Der Club, die lokalen Erfa-Kreise und die Chaostreffs sollten ihre Augen nicht vor den regulatorischen Vorgaben rund um den Datenschutz verschließen. Die Regelungen des Datenschutzes gelten auch für nicht eingetragene Vereine und ein Nichteinhalten kann zu Auflagen oder Bußgeldern gegenüber dem Club, aber auch gegenüber den Verantwortlichen führen. Zum Start sind einige „Papiertiger"-Tätigkeiten durchzuführen, die dann kontinuierlich weitergeführt werden sollten.

Wer hierzu Rückfragen hat oder Hilfestellung benötigt darf sich gerne an mich wenden, ich unterstütze gerne die lokale Umsetzung.

Referenzen

[1] „Praxisratgeber für Vereine" (2018), https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-f%C3%BCr-Vereine.pdf
[2] „Forderung Datenbrief des CCC", https://www.ccc.de/datenbrief
[3] Bildquelle: https://de.m.wikipedia.org/wiki/Datei:Herne_Stadtarchiv_alte_Akten.jpg
[4] Bildquelle: https://www.flickr.com/photos/mennonitechurchusa-archives/6987770030/

CCC tuwat Arbeitsgruppe „Kritische Infrastrukturen“

von HonkHase <manuel@atug.de> und ijon <ijon@c-base.org>

Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. *Hinweis:* eine Übersicht über die verwendeten Akronyme findet sich auf Seite 0x1D.

Im Sinne des BSI-Gesetz [1] werden Kritische Infrastrukturen wie folgt definiert:

> *Kritische Infrastrukturen [...] sind Einrichtungen, Anlagen oder Teile davon, die*
> 1. *den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und*
> 2. *von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.*
>
> *[...]* BSIG § 2, Abs. 10

Dazu kommen noch die Sektoren „Staat und Verwaltung“ sowie „Medien und Kultur“. Genaueres dazu definiert über das BSIG hinaus die „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ [BSI-KritisV; 2].

Wir als Bürger sind gegenüber Kritischer Infrastruktur machtlos. Wir haben keinen direkten und unmittelbaren Einfluss auf den Betrieb im Regelfall oder im Krisenfall. Das Vertrauen in dieses hohe Gut der Verantwortung haben wir an den Staat abgegeben.

Kritische Infrastruktur wird natürlich ebenfalls durch IT umgesetzt, die nie 100 %ig sicher betrieben werden kann. Wir haben es hier leider nicht mit einer konkreten Einzelfall-Betrachtung zu tun wie bei PC-Wahl[3] oder O’Zapftis [Staatstrojaner; 4], sondern mit Anlagen, die beispielsweise sehr komplex, Jahrzehnte alt, von einem Monopolisten betrieben, Unikate, SCADA oder auch IoT sind. Oftmals unterliegen die Systeme sogar mehreren der genannten problematischen Umstände.

Angegriffene kritische Infrastruktur [12]

Derzeit laufen die Systeme bei uns in Deutschland so zuverlässig, dass (fast) niemand mehr intensive Vorsorge betreibt. Oder fällt Dir spontan ein, wo der nächste öffentliche Trinkwasserbrunnen ist und hast Du

Trinkwasser-geeignete Kanister im Keller? Oder die empfohlene Menge Notfallrationen an Lebensmitteln zu Hause gelagert?

Die Mehrheit der Menschen in Deutschland kann Dir diese Fragen spontan eher nicht beantworten, weil es Wissen ist, dass aufgrund der extremen Seltenheit solcher Ausfälle nicht gebraucht wird [Stichwort „Verletzlichkeitsparadoxon"; 6]. Solche Ausfälle gehören hier in Deutschland nicht zur Lebensrealität, daher hat die Bevölkerung kaum für solche Situationen vorgesorgt.

Wenn also diese Unmenge an Sicherheitslücken in unterschiedlichsten kritischen Systemen wirklich ausgenutzt werden würde und infolgedessen Teile unserer Kritischen Infrastrukturen umfangreich ausfallen, wäre die Bevölkerung hier in Deutschland darauf noch schlechter vorbereitet als in anderen Teilen der Welt. Dort sind Ausfälle grundlegender Infrastruktur ein wiederkehrendes und somit bekanntes Ereignis.

Nehmen wir mal an, dass dieser Fall eintritt. Also jemand (Drittstaaten, Geheimdienste, Terroristen, Blackhats, Script Kiddies …) nutzt vorhandene Sicherheitslücken aus und schaltet eine signifikante Menge Kritischer Infrastrukturen destruktiv ab…

Wer kommt dann eigentlich der Bevölkerung zu Hilfe?

Es hat den Anschein, als ob die Ressourcen die in dieser Republik vorhanden sind, bei einer Cyberapokalypse nur ein Tropfen auf den heißen Stein wären und vornehmlich nur einen „Staats und Regierungsbetrieb sicherstellen" sollen oder können. Kapazitäten und Ressourcen, die sich um das (nachrangigere?) Ziel von Krisenbewältigung/Krisenschutz (engl. „Disaster Relief" fühlt sich treffender an) gegenüber der Bevölkerung kümmern, sind kaum existent.

Wir haben es also nicht nur mit fehlendem Problembewusstsein zu tun, sondern auch mit einem konkreten Mangel an Ressourcen auf allen Seiten. Ressourcen umfasst hier:

Menschen Zu wenige Menschen wollen was mit Computern für den Staat tun.

Geld Betreiber kritischer Infrastruktur müssen investieren, der Staat muss auch Geld für defensive Schutzmaßnahmen ausgeben, tut er aber bisher nur in zu geringem Maße.

Strukturen Welche Struktur/Organisation käme dann eigentlich und hilft der Bevölkerung?

Prozesse Was tut so eine Struktur/Organisation dann eigentlich als erstes, als zweites, usw. wenn „die Scheiße den Ventilator getroffen" hat?

Da es hier noch Handlungsspielraum und Potential nach oben gibt haben wir uns als tuwat Gruppe Kritische Infrastrukturen zusammengetan, uns ausgetauscht, diskutiert und recherchiert. Und anschließend einen Forderungskatalog zur Verbesserung der Gesamtsituation erarbeitet, den wir euch nicht vorenthalten wollen.

Liste unserer politischen Forderungen

Unabhängigkeit des BSI!

Wir fordern die Unabhängigkeit des BSI vom BMI. Man könnte das BSI wie den Bundesbeauftragten für den Datenschutz direkt dem Bundestag unterstellen. Oder die Rechtsaufsicht verbleibt beim BMI, die Fachaufsicht aber dem BSI, denn die Fach- und Rechtsaufsicht lassen sich teilen – demokratisch. Diese Struktur ist Voraussetzung, dass 3–5-Letter Behörden wie z. B. BfV, BKA, BND, ZITIS und CODE der UniBw oder die von BMVg und BMI ge-

meinsam neu gegründete „Cyber-militärische Agentur der Bundesregierung“ (neudeutsch auch „Agentur für Innovation in der Cybersicherheit“ ADIC genannt), nicht von den Mängelberichten, die Betreiber an das BSI melden müssen, profitieren können. Dies ist derzeit z. B. bei Terrorgefahr oder Verdacht auf die Spionagetätigkeit einer fremden Macht der Fall. So würde das Vertrauen der Bürger in das BSI gestärkt und das Amt auch seinem Namen noch besser gerecht werden, denn dann könnte das BSI mit anderen unabhängigen Aufsichtsbehörden wie z. B. der BaFin oder der BNetzA auf Augenhöhe agieren und mehr im Benehmen statt im Einvernehmen agieren. Selbstverständlich dürfen die Know-How-Träger im BSI trotzdem nicht zu anderen Behörden wie z. B. ZITIS, CODE und UniBw abgeworben werden.

Personalausstattung relevanter Behörden!

Wir fordern mehr personelle Ressourcen und fachliche Kompetenzen für BSI, BBK und THW zum Schutz von IT-Komponenten in kritischen Infrastrukturen. Dies erfordert:

- Angemessene Budgets
- Kontinuierliche Ausbildungen und Weiterbildungen
- Nachwuchsförderung

Kompetente Mitarbeiter bekommen die oben genannten nur neu angeworben und gehalten, wenn eine Anpassung des Dienstrechts und der Vergütungsstrukturen vorgenommen wird, um Fachkräfte auch im Wettbewerb mit der Wirtschaft gewinnen zu können. Das bestehende Dienstrecht ist sehr formal und erlaubt die Verbeamtung selbst fähigster IT-Fachkräfte nur in niederen Laufbahngruppen, sofern die notwendigen formalen Laufbahnvoraussetzungen nicht erfüllt sind. Dadurch kann vielen IT-Fachkräften nur eine verhältnismäßig niedrige Besoldung angeboten werden, die am Arbeitsmarkt nicht konkurrenzfähig ist. Eine Flexibilisierung des Laufbahnrechts könnte dieses Problem entschärfen. Im Bereich der Tarifbeschäftigten muss die Möglichkeit der Zahlung konkurrenzfähiger Vergütungen ebenfalls geschaffen werden, z. B. durch Anpassung des Tarifvertrags für den Öffentlichen Dienst (TVöD). Die bisherige Möglichkeit, zeitlich begrenzte Zulagen zu zahlen, genügen auf Dauer nicht.

Nachwuchsförderung ist dringend notwendig, denn mit jeder digitalisierten Anlage verschwindet über die Jahre auch das Fachwissen, wie die Anlage (z. B. im Bereich Wasser und Energie) notfalls auch ohne Computersysteme betrieben werden kann. Nicht nur durch Digitalisierung, sondern auch durch Renteneintritt der alten Hasen verschwindet solche, in der Krise unschätzbar wertvolle, Fähigkeiten.

Open Source in KRITIS!

Im KRITIS-Umfeld eingesetzte Software muss grundsätzlich als Open Source bereitgestellt werden oder der Quellcode muss zumindest in treuhänderische Verwaltung gegeben werden.

Software für den Betrieb der Anlagen aus den Anlagenkategorien der BSI-KritisV von kritischen Infrastrukturen muss frei sein, oder der Quellcode in treuhänderischer Verwaltung gehalten werden, damit diese auch viele Jahre und Jahrzehnte sicher betrieben werden kann. Auch wenn der Hersteller die Software nicht mehr unterstützt oder selbst nicht mehr existiert. Dies folgt als Teil-Lösung für das Problem, dass (Hardware-)Komponenten, z. B. in Produktionsanlagen, nicht ohne weiteres ausgetauscht werden können. Dies fordern wir in Anlehnung an das vom CCC unterstützte Public Money, Public Code.[7, 8]

Für SCADA- und PLC-Systeme, die bei Kritischen Infrastrukturen angewendet werden,

gibt es bereits in einer Bundestags-Drucksache 17/12541, unter einen Beschluss der Enquete Kommission für digitale Infrastruktur:

> *Der Open-Source-Weg, also das Kerckhoff-Prinzip, ist daher für Kritische Infrastrukturen ein geeigneter Weg. […]*
>
> *Wie in der Wirtschaft üblich, sollte gerade gegenüber Herstellern von Software für bestimmte Kritische Infrastrukturen zwingend darauf geachtet werden, dass der Source Code zur Überprüfung zugänglich gemacht wird.*
>
> [9, S. 98, Abschnitt 4b)]

Regulierung, Aufsicht, Kontrolle!

Kritische Infrastruktur sollte bestenfalls nicht unter vollständiger Kontrolle der Privatwirtschaft stehen.

Für jeden KRITIS-Sektor betrachten wir als Arbeitsgruppe derzeit einzeln, wie die notwendigen Kontrollmechanismen implementiert werden könnten und welche genau notwendig sind. Grundsätzlich müssen kritische Infrastrukturen sorgsamer und ausfallsicherer betrieben und ausgebaut werden, als andere Infrastrukturen. Dies widerspricht grundsätzlich den Bestrebungen des freien Marktes. Detaillierte Regulierungen, unabhängige Kontrollinstanzen und kompetente Aufsichtsbehörden für die einzelnen Sektoren sind daher notwendig.

Wir fordern, keine Budgets für Behörden, Dienste und Agenturen bereitzustellen, um damit Sicherheitslücken für einen Hackback (neudeutsch wird dies freundlich als „aktive Cyber-Abwehr" bezeichnet), Staatstrojaner zu entwickeln oder zu kaufen.

Weiterhin müssen alle Behörden, Dienste und Agenturen verpflichtet werden, ihnen bekannt gewordene Schwachstellen über das BSI als neutrale und unabhängige Stelle an den Hersteller zu melden, denn der Bevölkerungsschutz fängt bei der Kommunikation vorhandener Schwachstellen an den Hersteller zu ihrer Behebung an.

Strikt defensive Cybersicherheitsstrategie!

Wir setzen uns ein für eine strikt defensive Cybersicherheitsstrategie[10]. Wir verurteilen den Einsatz und die Bereitstellung offensiver Wirkmittel im Cyberraum. Insbesondere kritische Infrastrukturen sind anfällig für Angriffe von Cyberkriminellen oder von Drittstaaten – egal ob feindlich gesinnt oder „Freunde". Da eine zweifelsfreie Attribution der Herkunft eines Cyberangriffs nach dem Stand der Technik ausgeschlossen ist, muss davon ausgegangen werden, das sowohl der Angriff wie auch ein Gegenangriff immer auch zivile Infrastruktur treffen kann. Dies ist laut den Zusatzprotokollen der Genfer Konvention von 1977 klar ausgeschlossen [vgl. Art. 52 und 54 ZP I 11]. Auch die deutlich ältere Haager Landkriegsordnung untersagt Angriffe auf zivile Infrastruktur im weiteren Sinne.

Wir fordern daher ein internationales Abkommen, dass jegliche offensive Wirkmittel im digitalen Raum als Digitalwaffen (D-Waffen) einstuft und diese im Rahmen eines Sperrvertrags international verbietet, ähnlich wie die vorhandenen ABC-Waffensperrverträge. Im Idealfall kann man dann zukünftig nur noch von ABCD-Waffensperrverträgen sprechen.

Weiterhin sind wir der Meinung, dass Deutschland mit gutem Beispiel vorangehen muss und solche Waffen weder entwickeln noch einsetzen darf. Die geplanten Gesetzesänderungen zum Einsatz offensiver Wirkmittel im Cyberraum, an denen das BMI arbeitet, dürfen nicht durchgeführt werden.

Wir erkennen an, dass wir unsere (Kritische) Infrastrukturen bisher nicht ausreichend

schützen und fordern daher, alle informationstechnischen Systeme mit dem Gedanken „Security by Design“ zu gestaltet. Dies schützt proaktiv gegen erfolgreiche Angriffe aus dem Cyberraum. Alle Programmierer und Administratoren müssen konstant weitergebildet werden, was der aktuelle Stand der Technik ist. Dies gilt nicht nur im Bereich des Betriebs sondern auch in der Entwicklung und der Gestaltung sicherer Systeme. Dazu fordern wir die Einrichtung mehrerer Lehrstühle zur defensiven IT-Sicherheitsforschung und -Lehre.

Übersicht über Akronyme

ADIV: Agentur für Innovation in der Cybersicherheit
BaFin: Bundesanstalt für Finanzdienstleistungsaufsicht
BBK: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfV: Bundesamt für Verfassungsschutz
BKA: Bundeskriminalamt
BMI: Bundesministerium des Innern, für Bau und Heimat
BMVg: Bundesministerium der Verteidigung
BND: Bundesnachrichtendienst
BNetzA: Bundesnetzagentur
BSI: Bundesamt für Sicherheit in der Informationstechnik
CODE: Forschungsinstitut Cyber Defence der Universität der Bundeswehr München
IoT: Internet of Things
PLC: Programmable Logic Controller
SCADA: Supervisory Control and Data Acquisition
THW: Technisches Hilfswerk
ZITIS: Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Referenzen

[1] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG): https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[2] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV): https://www.gesetze-im-internet.de/bsi-kritisv/

[3] 46halbe: „PC-Wahl – Open-Source-Spende: CCC schließt größte Schwachstelle in PC-Wahl“ (18.09.2017), https://www.ccc.de/de/updates/2017/pc-wahl-again

[4] Presseteam des CCC: „Chaos Computer Club analysiert aktuelle Version des Staatstrojaners“ (26.10.2011), https://www.ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner

[5] Checkliste des BBK: https://www.bbk.bund.de/DE/Ratgeber/VorsorgefuerdenKatfall/Checkliste/Checkliste.html

[6] BSI: „BSI Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Abs. 2 BSIG“ (2017), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/b3s_Orientier

ungshilfe_1_0.pdf?__blob=publicationFile
[7] 46halbe: „Offener Brief: Public Money? Public Code!“ (12.09.2017), https://www.ccc.de/de/updates/2017/public-money-public-code
[8] Projekt Public Money, Public Code: https://publiccode.eu/de/
[9] Neunter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft“ http://dipbt.bundestag.de/doc/btd/17/125/1712541.pdf
[10] Erdgeist: „Chaos Computer Club fordert strikt defensive Cyber-Sicherheitsstrategie“ (29.08.2018), https://www.ccc.de/de/updates/2018/defensive-cyber-strategie
[11] Wikipedia, Zusatzprotokolle der Genfer Konvention von 1977 https://de.wikipedia.org/wiki/Genfer_Konventionen#Zusatzprotokolle_von_1977
[12] Bildquelle: CC-BY-SA 2.0 https://www.flickr.com/photos/dougbeckers/33520117275

Clemens Grünewald

Leserbriefe

Hallo liebes Team, wie mir zu meinem Erschrecken und großem Bedauern erfahren musste (und von selber hätte merken müssen!), ist das Foto auf der aktuellen DS-Ausgabe nicht von mir, sondern von Henning Hahn (@Schmierwurst, Mail siehe CC).

Henning hat mir zu Recht schon den Kopf abgerissen und ich habe vollkorn bereits informiert.

Bitte stellt in der Online-Ausgabe sicher, dass dort die richtigen Credits stehen und vollkorn sagte mir schon, dass er sich über einen „Leserbrief / Klarstellung“ von Henning freuen würde. Ich bin mir sicher ihr findet da zusammen eine Lösung.

Es tut mir sehr Leid, dass ihr unter meiner Verpeilung leiden müsst, ich hätte das ganz klar besser prüfen und meinem Verpeilerhirn misstrauen müssen (Henning hatte mir das Bild in nem Threema-Chat geschickt und von dort hat es den Weg in „meine Fotos“ gefunden :(und es wurde noch nie ein Foto von mir veröffentlicht und ich hätte mal eine Minute länger darüber nachdenken sollen, was es bedeutet ein Foto auf dem DS Cover zu veröffentlichen …). Besonders Leid tut es mir natürlich für Henning, aber ich hoffe durch Richtigstellung und Namensnennung in der Online-Ausgabe wird wenigstens etwas Gerechtigkeit wiederhergestellt.

Ich geh mal in die Ecke mich schämen.

Liebe Grüße
<lasse>

Hi Henning, Natürlich werden wir das in der DS100, die dieses Jahr erscheint, gut sichtbar korrigieren – bitte nimm auch von uns eine Entschuldigung an, dass so etwas passieren konnte.

Viele Grüße
<rixx>

Moin rixx, danke für Deine Mail und sorry für meine verspätete Antwort.

Wenn Ihr das in der noch ausstehenden Online-Ausgabe der DS99 korrigieren könntet und, wie Du vorschlägst, in der DS100 gut sichtbar eine Gegendarstellung bringt, dann bin ich als Urheberrechtsverletzter doch weitestgehend besänftigt und werde von weiteren Schritten absehen.

Allerdings lasse ich mir noch offen, bei günstiger Gelegenheit von besagtem Hr. Lasse mein Lebendgewicht in feinstem Tschunk und/oder reinstem Bier aufwiegen zu lassen!

Grüße
<Henning>

Hallo liebe Datenschleuder-Redaktion, Sehr verehrte CCC-Mitglieder, in der aktuell heiklen Urheberrechtsreform und ihrer offenen Fragen ließ mich eine konkrete Aussage nicht mehr los: In Zukunft soll es möglich sein einen urheberrechtlichen Anspruch auf beliebige Drei-Wort-Kombinationen zu erheben. Zu diesem Zweck kam mir die Idee eines kubischen Duden. In ihm würden alle Drei-Wort-Kombinationen der deutschen Sprache enthalten sein und so künftig eine Inanspruchnahme der Urheberrechtsreform, zumindest in diesem speziellen Fall, verhindert werden.

Realisierbar wäre ein solcher Duden[3] indem eine Datenbank alle Duden-Wörter erfasst, diese pro Datensatz um eine Datenbank aller Duden-Wörter erweitert, deren Datensät-

ze wiederum mit einer Datenbank aller Duden-Wörter erweitert werden. Die Datenmenge ist erstmal gigantisch, eben Anzahl aller Wörter[3], aber gespeichert werden müsste lediglich eine Duden-Datenbank und die relativen Verweise zu den zu verkettenden Worten.

Würde man eine so generierte Datenbank abfragen, erhielte man eine Liste mit allen Möglichkeiten drei Worte der deutschen Sprache zu verketten und somit ein Werk, das sowohl gegen bestehendes Urheberrecht verstößt, gleichzeitig aber auch weitere Ansprüche auf Drei-Wort-Kombinationen verhindert. Diese Methode lässt sich auf alle Sprachen ausweiten, mit oder ohne Satzzeichen, die Wort-Ketten auf 4, 5, n erweitern, etc. Übergibt man das Recht an diesem Werk einer Art „GNU General Public License“ (oder einem eigens geschaffenen Indie-Verlag, der Herrn Voss bei jedem dritten Wort eine Rechnung ausstellen könnte höhö) machen sich alle Menschen, die Sprache verwenden an sich selbst straf-/haftbar und die Reform offenbart ihre Unsinnigkeit.

Ich hoffe euch von dieser Idee überzeugen zu können und warte gespannt auf eure Reaktion.

Habt einen schönen Tag

<Felix F.>

Moin Felix, hach, das ist feinstes Nerd-Sniping. Wie viel Speicherplatz bräuchte so ein Werk? Wir sind auf konservative Schätzungen von $3,18 \cdot 10^{16}$ Bytes (~28 Petabytes) bis zu umfangreicheren Schätzungen von $1,03823 \cdot 10^{29}$ Bytes (viel) gekommen. Und das ist noch immer ohne Austriazismen, Pennsylvania Dutch, bayerische Bergdörfer und all sowas.

Was war noch gleich die Frage?

Gruß

<vollkorn>

Hallo, Ich wollte mal fragen ob es möglich wäre die Datenschleuder-Downloads auch per RSS-Feed zu erhalten?

<NickFreeman>

Hallo Nick, Ganz neu stellen wir die Download-Links auch als RSS-Feed zur Verfügung. Die Adresse lautet https://ds.ccc.de/ds-feed.xml.

<dome>

Hallo, mir ist nicht klar geworden, weshalb durch ein Fax ein Hackerangriff stattfinden soll.

Eher glaube ich, dass man das Medium schlecht machen will, worin ich durch den Aufruf „The world must stop using FAX!“ eher bestätigt werde.

<Lucian>

Hallo, Das ist recht einfach: Inzwischen ist ein Fax(gerät) nicht mehr das analoge Gerät, das es früher mal war; Faxen ist inzwischen eine von vielen Funktionen eines Multifunktions-Druckers. Diese Drucker beinhalten einen kleinen Computer, der den Ausdruck koordiniert, aber auch die Daten für den Ausdruck vorbereitet. Dem ist (fast) egal woher die Daten kommen – er bekommt die Daten geliefert und bereitet sie für den Druckteil auf. Wenn in der entsprechenden Software Fehler sind, ist der Drucker darüber angreif- und ausnutzbar. Der Angriff kann ein einfacher Denial-of-Service-Angriff sein (der Drucker druckt nicht mehr), kann aber auch soweit gehen, dass er die Daten der internen Speicher (wo die Daten zum Druck aufbereitet werden) an eine Internet-Adresse weiterleiten soll. Das mag im internen Netz (reine Druckeraufgaben) noch akzeptiert

sein, weil das Ausnutzen nur lokal möglich ist und den Mitarbeitern vertraut – aber dadurch, dass ein Faxgerät üblicherweise an einem Telefonanschluss hängt, über den die ganze Welt dieses Faxgerät anrufen kann, ist dieser Multifunktionsdrucker von außen kompromittierbar. So wie ein Webserver, der schutzlos im Internet steht, ist ein Faxgerät von jedem Telefon der Welt aus anrufbar – und im Gegensatz zu Webservern ist so ein Faxgerät nicht gegen bösartige Angriffe geschützt.

<rince>

Zwei kritische Leser

Hallo Datenschleuder, vor wenigen Tagen habe ich bei Bekannten ein Chromecast-Gerät installiert. Zuvor natürlich die notwendigen Daten wie SSID und WLAN-Schlüssel bereitgelegt. Diese Mühe war überflüssig, die Einrichtung des Chromecast lief fast automatisch ab. Dem Mister Google waren schon SSID und WLAN-Schlüssel bekannt und damit stehen ihm weltweit alle Netzwerke offen wie Scheunentore. Dazu ist sicher nicht die Installation eines Chromecast-Gerätes notwendig. Möglichst lange und komplizierte Passwörter sind somit nur ein Witz. Das ist sicher auch den Mitstreitern des Mister Google bekannt.

Politik, Wirtschaft, Banken usw. faseln über Datensicherheit und viele Bürger „haben ja nichts zu verbergen“. Alles also harmlos?

<Ernst>

Moin Ernst, vorerst entschuldige bitte die dreimonatige Reaktionszeit. Das könnte daran liegen, dass niemand von uns einen Chromecast benutzt und nachvollziehen kann wie die WLAN-Daten in den Chromecast kamen. Aber die dahinterliegende Frage scheint mir zu sein: „Wie kam Google jemals an diese Daten?“ Und damit sind wir genau bei der Debatte, die du ansprichst: Wir müssen auf politischer, wirtschaftlicher und privater Ebene dafür Sorge tragen, dass unsere Daten unsere bleiben und nicht hinter unserem Rücken gesammelt, gespeichert und verwendet werden. Vielen Dank für dieses schöne Beispiel weshalb wir uns, unter anderem, regelmäßig im CCC engagieren.

<vollkorn>

Hallo vollkorn, danke für die Mail. Ich weiß das zu schätzen was [der] CCC an Arbeit leistet. Jedenfalls sollten alle User vorsichtiger sein.

<Ernst>

Betreff: CCC ist nicht der ADAC für Datenmuggel (Datenschleuder #99, Seite 7)

Sehr geehrte Damen und Herren, dann bin ich wohl falsch hier. Ich kündige hiermit meine Mitgliedschaft mit sofortiger Wirkung (Kontaktdaten weiter unten). Mein Dauerauftrag wird gekündigt.

Für eine kurze Bestätigung wären wir Ihnen dankbar.

<Harald H.>

http://www.jukebox-world.de/Forum/Bilder/Rock-Ola/1488.jpg

Re: Bilderrätsel #99

Im Bilderrätsel der letzten Ausgabe ist das Innere einer *Rock-Ola 1478 120 Selection*-Jukebox (ca. 1959) zu sehen. Das Rad in der Mitte repräsentiert die Warteschlange der als nächstes abzuspielenden Songs. Jeder Stift steht für eine Plattenseite; wenn der Stift innen steht, hält ein umfahrender „Schlitten“ an dieser Stelle an und die Maschine holt die entsprechende Platte.

Nur zwei korrekte Antworten von Alexander Eschler und st0ne fanden ihren Weg zur Datenschleuder-Redaktion. Folgend die Nachricht von st0ne, der auch gleich ein Bild der JukeBox mitgeliefert hat.

Hallo, ich vermute es ist eine Rockola Musikbox. <siehe Abbildung oben>

Und zwar ist es genau der „Speicher“ wo die Seiten der Singles vorgewählt werden können.

Ist der Stift rausgeschoben erkennt er das beim „Scan“ (ein Umlauf um diese Trommel) und spielt die A bzw. B Seite der Platte.

hoffe das stimmt :-)

<st0ne>

Zu sehen ist das Innere einer *Rock-Ola 1478 120 Selection*-Jukebox (ca 1959). Das Rad in der Mitte repräsentiert die Warteschlange an als nächstes abzuspielenden Songs. Jeder Stift steht für eine Plattenseite; wenn der Stift innen steht, hält ein umfahrender „Schlitten“ an dieser Stelle an und die Maschine holt die entsprechende Platte.

<vollkorn>

Bilderrätsel dieser Ausgabe

Auf der Umschlaginnenseite dieser Ausgabe sieht man ein aufgeschraubtes Gerät. Oben angeordnet sind die sehr charakteristischen Bedienelemente und auf dem Board gibt es auch ein paar Hinweise auf die Herkunft dieses Apparats, der jahrzehntelang eng verknüpft mit Unterhaltung war.

Eine Idee, was das sein könnte? Schreibe uns deine Vermutung an <ds@ccc.de>.

Datenschleudern beim Versand. benni

Danke CCC (Shoes & Bags)

von vollkorn
<vollkorn@hamburg.ccc.de>

Ein Schuhladen sorgte fünf Jahre lang für ein wenig Verwirrung. Doch das ist jetzt wieder vorbei. Eine Danksagung.

Der CCC – wer kennt nicht diese drei Buchstaben und wofür sie stehen? Die sich in leuchtendem Orange in unseren Köpfen eingebrannt und auf deutsche Stadtbilder abgezeichnet haben? „Cena czyni cuda“, zu Deutsch etwa „Der Preis bewirkt Wunder“. Der polnische Schuh- und Modeladen, im Jahr 1999 gegründet, trat an seinen Aktionären viel Geld einzubringen. Ein Tempel der „Geiz ist geil“-Kultur, der seit 2013 in Deutschland auf fruchtbaren Boden fiel und schnell viele Anhänger fand.

Ein weiterer Träger der drei Cs, der um das platzbeschränkte Markengedächtnis von Menschen ringt, der Begegnungsorte für seine Anhänger in allen größeren Städten eröffnet. Die 30 Erfahrungsaustauschkreise des Clubs waren schnell übertroffen. Immerhin 75 Filialen wurden innerhalb von fünf Jahren in Deutschland eröffnet und ambitionierte Pläne für über 1000 Läden wurden geschmiedet [1]. Ein wichtiger Eckstein deutscher Shopping-Kultur wurde erfolgreich etabliert.

Den Chaos Computer Club stellte dieser kometenhafte Aufstieg des Neulings aus dem Off natürlich vor neue Herausforderungen, die sich hauptsächlich in der Außenkommunikation widerspiegelten. Zum Beispiel in Austrittserklärungen aus dem Verein mit sehr langen Chaosnummern. Wie sich herausstellte gibt es auch einen CCC-Club für treue Kunden mit vielen Vorteilen und langen Mitgliedsnummern. Oder ausführliche, klagende Berichte über kaputte Schuhe und unbarmherzige Verkäufer, die keinesfalls Kulanz walten lassen wollten, obwohl der Schuh doch nur einmal getragen wurde. Wie viele Zeitungsleser:innen sich wohl wunderten warum denn jetzt schon wieder ein:e Vertreter:in eines Schuhladens beim Bundesverfassungsgericht war? Ach, und all die Spam-Mails, die versuchen uns Rucksäcke zu verkaufen. Nun, sowas passiert eben, wenn man einfach an die erstbeste Mailadresse zum Stichwort „ccc“ bei Google schreibt, denn der Schuhladen hat es immer nur auf die letzten Plätze der ersten Ergebnisseite geschafft. Wir können nur erahnen wie viele Computerprobleme im Gegenzug von den Mitarbeitenden des Schuhladens gelöst wurden. An dieser Stelle ein großes Danke an diese anonymen Helfer:innen!

Am 9. November 2018 erschien die Meldung, dass CCC Shoes & Bags sich aus Deutschland zurückziehen wird. Die Filialen werden, wie sich später aufklärte, von Reno übernommen. Erleichterung ging durch die Reihen der Chaot:innen, die sich um die zahlreichen Mailadressen des Clubs kümmern. Und vielleicht haben auch ein paar Schuhverkäufer:innen aufgeatment, als sie merkten, dass sie in Zukunft weniger Fragen zur DSGVO gestellt bekommen werden. Endlich hat der Schuhladen eingesehen, dass die drei Cs in Deutschland schon vorbelegt sind und haben das einzig vernünftige getan: sie uns wieder überlassen. Was sie uns leider nicht überlassen wollen sind die großen, orangefarbenen CCC-Schilder, wie ich von einigen Leuten hörte, die sich die Ohren wund telefonierten um so ein Schild für ihren Hackspace zu ergattern.

Möglicherweise gibt es einen ungeborgenen Schatz an Anekdoten über CCC-Verwechslungen. Chaot:innen, die sich mit ihren nicht-Nerd-Freund:innen „vorm CCC“ verabredet haben und nicht trafen? Verwirrende, aber erheiternde Mailverkehre? Hackspace-Besucher:innen mit unerfüllbaren Erwartungen? Schreib deine Verwechslungsgeschichte an <ds@ccc.de> für die Leserbriefe.

Danke CCC Shoes & Bags, für fünf Jahre an Verwechslungen, die oft einer gewissen Komik nicht entbehren konnten, und der Einsicht, dass „CCC“ in Deutschland einfach schon vergeben ist.

Referenzen

[1] Schuhkette verschwindet aus Deutschland: Reno schnappt sich die Filialen https://www.chip.de/news/Schuhkette-verschwindet-aus-Deutschland-Reno-schnappt-sich-die-Filialen_152568583.html

vollkorn

groff – Ein praktischer Einstieg und historischer Abriss

von Marco Bakera <marco@bakera.de>

Wie bei vielen alten und in Vergessenheit geratenen Technologien, lohnt sich häufig ein Blick und Abgleich mit der Gegenwart – so auch bei groff. Der schnelle Arbeitsprozess, die einfache Syntax und die Allgegenwart von groff auf Linux-Systemen machen es in vielen Fällen zu einem würdigen Ersatz für LaTeX oder andere Textsysteme.

Ein langer Weg

Wie lassen sich technische Dokumente besonders ansprechend auf Computern darstellen? Diese Kernfrage beschäftigte schon in den 1960er Jahren viele Techniker und Ingenieure. Dinge, die uns heute selbstverständlich erscheinen, mussten irgendwann einmal erfunden werden. Wie verteile ich etwa die Wörter so auf eine Zeile, dass sie gut gefüllt aussieht? Wie platziert man Absätze ansprechend auf einer Seite? Wie kann ich die Silbentrennung von Wörtern realisieren? Wie sollen Tabellen oder mathematische Formeln gesetzt werden? Wie lassen sich Schriftarten in einem Dokumenten mischen und wie Sonderzeichen ausgeben?

Als erster Entwurf für die Lösung dieser Probleme entstand Mitte der 1960er Jahre am Massachusetts Institute of Technology (MIT) ein Programm mit dem Namen „RUNOFF“. Der Name war eine Anlehnung an den Ausspruch „I'll run off a document“ und eines der ersten Programme, das versuchte, aus dem Buchdruck bekannte Ansprüche des Textsatzes auf Computerbildschirme zu übertragen. Erstmals versuchte man, mit Computern Zeichen und Absätze günstig auf mehrere Seite zu verteilen und Wörter auf Zeilen so anzuordnen, wie wir es heute durch linksbündigen und rechtsbündigen Text sowie Blocksatz gewohnt sind.

Eine spätere Portierung des Programms wurde nur noch mit „roff“ abgekürzt, gefolgt von einer weiteren Implementierung, die den Namen „nroff“ erhielt – für „newer roff“. Das Versionswirrwarr ist aber noch längst nicht beendet. Es gab noch eine Version, die den Namen „troff“ erhielt – für „typewriter roff“. Sie erfreute sich so großer Beliebtheit, dass sie noch bis 1994 stetig weiterentwickelt wurde. Eine spätere Implementierung für die GNU-Softwaresammlung erhielt schließlich den Namen „groff“ – sie ist bis heute in jeder Linux-Installation vorhanden und für die Darstellung von man-Pages verantwortlich.

Zwei Wege nach Rom

Bevor wir in die Tiefen von groff einsteigen, halten wir jedoch kurz inne. Überlegen wir zunächst einmal, auf welche Weise Texte über-

haupt am Computer erstellt werden können. Es existieren im Wesentlichen zwei technische Möglichkeiten: Entweder wird der Text direkt in einem Programm wie Word oder LibreOffice verfasst, oder man schreibt eine Textdatei mit Steuerzeichen (auch: Auszeichnungssprache), die im Anschluss interpretiert wird und die endgültige Darstellung liefert. Beide Wege haben ihre Vor- und Nachteile.

Bei dem direkten Weg sieht man das Ergebnis sofort und hat eine gute Vorstellung davon, wie das Endergebnis aussehen wird. Der Weg über eine Textdatei mit Formatierungsinformationen hat dagegen den Vorteil, dass man einen beliebigen bekannten Texteditor hierfür verwenden kann und den Text auch in anderen Programmen leichter weiterverarbeiten kann. Zudem ist die Wahrscheinlichkeit hoch, dass man ihn auch noch Jahrzehnte später lesen kann. Beispiele für die textbasierten Formate sind LaTeX, HTML oder Markdown – und eben auch groff.

Von troff zu groff

Doch troff ist eigentlich nur der Unterbau, der die volle Kontrolle über jedes Zeichen und jeden Pixel auf der Ausgabeseite ermöglicht. So ähnlich wie TeX der Unterbau für LaTeX ist: Erst das Makropaket LaTeX ermöglichte die einfache Nutzung des TeX-Systems für größere Dokumente. groff wiederum fasst troff, verschiedene weitere Programme und Makrosysteme zusammen und vereinfacht die Nutzung.

Es existieren verschiedene Makrosysteme für beide Programme, die alle mit kryptischen Abkürzungen benannt wurden: ms, mom, me, man und weitere. Sie unterscheiden sich in ihren Einsatzgebieten, der Komplexität und der Verbreitung. Das Makropaket mom vergleicht sich selbst als „LaTeX für groff“ und spezialisiert sich auf die Erstellung von PDF-Dokumenten.

Vorteile von groff

Im Vergleich zu LaTeX ist der Aufbau eines groff-Dokumentes deutlich einsteigerfreundlicher. groff selbst kann man in wenigen Stunden, ein mächtiges Makropaket wie etwa mom in ein bis zwei Tagen gut erlernen und erste Dokumente damit erzeugen.

Ein weiterer großer Vorteil von groff ist, dass es selten nachinstalliert werden muss, da es auf jedem Linux bereits vorhanden ist. Auch die Installationsgröße von wenigen Megabyte ist vergleichsweise klein und die Dokumente werden im Vergleich zu LaTeX deutlich schneller erzeugt. Jeder, der schon einmal das Kommando `man` verwendet hat, spürt diese Geschwindigkeit; schließlich wird bei jedem Aufruf das Dokument aus den Quellen neu gelayoutet und anschließend angezeigt. In der Datei /etc/manpath.config sind die Pfade aufgelistet, in denen sich die groff-Quelltexte der man-Pages befinden – z. B. unter /usr/share/man.

Die Syntax der man-Pages ist jedoch wenig einsteigerfreundlich.

Ein einfaches Beispiel

Nach der langen Vorrede schauen wir uns ein einfaches Dokument an, das mit Hilfe des mom Makropaketes erstellt wurde. Das Paket ist ideal, um PDF-Dokumente zu erstellen.

```
1 .NUMBER_LINES 1
2  .TITLE "Hallo Welt"
3  .AUTHOR "Max Muster"
4  .PAPER A4
5  .PRINTSTYLE TYPESET
6  .START
7  Hier startet mein Text.
```

Makrobefehle werden mit einem Punkt am Anfang der Zeile eingeleitet und können um Argumente ergänzt werden, die direkt hin-

ter dem Makronamen stehen. Alles andere ist Text, der so ausgegeben wird, wie er eingegeben wurde.

Die ersten drei Zeilen sind noch selbsterklärend und legen den Titel und Autor sowie die Papiergröße des Dokumentes fest. Es folgt mit `PRINTSTYLE` ein Ausgabeformat, welches entweder `TYPESET` oder `TYPEWRITE` sein kann. Mit `TYPEWRITE` wird eine alte Schreibmaschine nachgeahmt – ein schöneres Layout erhält man jedoch mit der in Zeile 4 gewählten Option.

Damit ist das Dokument bereits fertig und kann generiert werden. Der komplex anmutende Aufruf von groff lautet hierfür

```
groff -Tpdf -mom -k -m den
    groff.mom > groff.pdf
```

Gehen wir die Optionen der Reihe nach durch. Die Option `-T` legt das Ausgabeformat PDF fest, mit `-mom` wird das Makropaket mom aktiviert, `-m den` aktiviert das Makropaket für die deutsche Silbentrennung nach der reformierten deutschen Rechtschreibung und `-k` sorgt für die korrekte Konvertierung von deutschen Umlauten in der Quelldatei, welche in diesem Fall `groff.mom` heißt. Das fertige PDF-Dokument wird durch eine Umleitung der Ausgabe in der Datei `groff.pdf` erzeugt.

Präprozessoren

groff wird mit verschiedenen Präprozessoren ausgeliefert, die für das Erstellen von Diagrammen, mathematischen und chemischen Formeln oder Tabellen eingesetzt werden. Diese kleinen Programme lassen sich eigenständig ausführen oder über einen Kommandozeilenschalter von groff aktivieren: dies wären `-t` für Tabellen, `-e` für Formeln (Englisch „equation“) und `-p` für pic-Diagramme.

Schauen wir uns die verschiedenen Präprozessoren einmal beispielhaft an.

Formeln mit eqn

Mit dem Präprozessor *eqn* ist es möglich, komplexe Formeln zu setzen. Ein Beispiel soll dies verdeutlichen:

$$f'(x) = \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0}$$

Die Formel wurde mit dem folgenden Code und mit Hilfe des EQ- und EN-Makros erstellt.

```
1 .EQ
2 f' (x) =
3  lim from {x -> x sub 0}
4   {f(x) - f(x sub 0 )}
5     over {x - x sub 0}
6 .EN
```

Brüche werden mit „ZÄHLER over NENNER“ notiert und Zahlen können mit `sup` hoch- und mit `sub` tiefgestellt werden. Wenn mehrere Terme hoch- oder tiefgestellt werden sollen, kann dies mit geschweiften Klammern geschehen.

Wer den Formeleditor in LibreOffice schon einmal verwendet hat, dem kommt diese Form der Darstellung bekannt vor.

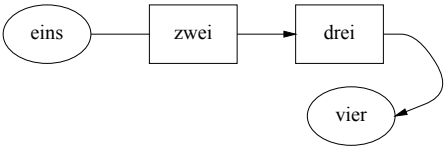
Diagramme mit pic

Mit Hilfe des Präprozessors „pic“ können Diagramme erzeugt werden, die in einer eigenen Sprache verfasst werden. Diagramme starten mit PS und enden mit PE. Einfache Symbole wie Rechtecke und Ellipsen werden aneinandergereiht und direkt oder über Linien und Pfeile miteinander verbunden. Das folgende Beispielfragment sollt dies verdeutlichen.

```
.PS
ellipse "eins"
line

box "zwei"
arrow
box "drei"
spline right 0.3
  then 0.3 down
  then 0.2 left ->
ellipse "vier"
.PE
```

Es erzeugt folgende Abbildung:



Beim Lesen des Quelltext kann man sich das Ergebnis bereits gut vorstellen. Die Sprache hat viele mächtige Konstrukte, mit denen aufwändige Diagramme erzeugt werden können. [2]

Weitere Informationen

Wer Spaß an der Einfachheit von groff gefunden hat, findet in dem Buch „Unix Text Processing“ von Dale Dougherty und Tim O’Reilly viele weitere Anregungen und Informationen. Es beschreibt troff/nroff und verschiedene Präprozessoren. Eine kleine Einführung in die Bedienung des Editors vi rundet das Buch ab. Da es vergriffen ist, muss man sich in Antiquariaten umschauen. Glücklicherweise gibt es auch eine freie Version. [1]

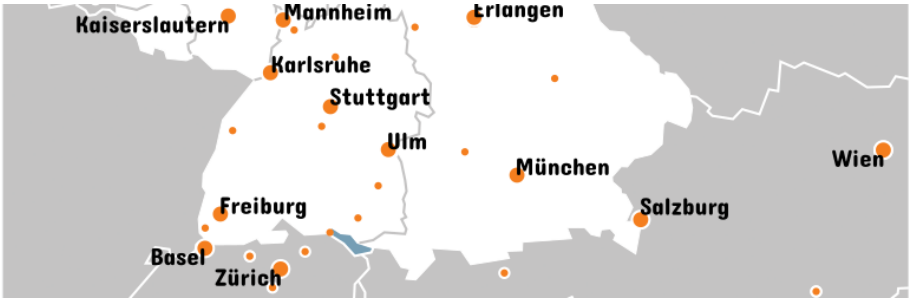
Unter Linux findet man auch über das Infosystem nach der Eingabe von `info groff` viele Details zum groff-System. Hilfe bei der Eingabe von besonderen Zeichen wie Pfeilen (→ ⇒), dem zusammengezogenen o und e (œ), dem polnischem Ł oder dem griechischen ☒ liefert die man-Page von `groff_char`. Auch die deutschen Anführungszeichen für den Beginn „ und das Ende “ einer wörtlichen Rede sind dort vertreten.

Referenzen

[1] „Unix Text Processing (Hayden Books)“ (1987), O’Reilly Open Books Project, https://www.oreilly.com/openbook/utp/

[2] „Making Pictures With GNU PIC“, Eric Steven Raymond, https://www.complang.tuwien.ac.at/doc/groff/html/pic.html

Anastasia Dulgier über Unsplash https://unsplash.com/photos/pDPe0MYcmbU



Erfahrungsaustauschkreise

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

Hamburg :: CCCHH :: CCC Hansestadt Hamburg e. V.	https://hamburg.ccc.de/
letzter Di 20 Uhr :: CCCHH, Zeiseweg 9, 22765 Hamburg	
Hannover :: C3H :: Leitstelle 511 - Chaos Computer Club Hannover e. V.	https://hannover.ccc.de/
Mi 19 Uhr u. letzter So 16 Uhr :: Leitstelle 511, Klaus-Müller-Kilian-Weg 2, 30167 Hannover	
Kaiserslautern :: Chaos inKL. e. V.	http://www.chaos-inkl.de
Sa 19 Uhr :: Klubraum, Rudolf-Breitscheid-Straße 65, 67655 Kaiserslautern	
Karlsruhe :: Entropia :: Entropia e. V.	https://entropia.de/
Sa 19:30 Uhr :: Entropia, Steinstraße 23, 76133 Karlsruhe	
Kassel :: CCC Kassel :: flipdot e. V.	https://flipdot.org/
Di 19 Uhr :: flipdot, Franz-Ulrich-Straße 18, 34117 Kassel	
Köln :: C4 :: Chaos Computer Club Cologne e. V.	https://koeln.ccc.de/
letzter Do 20 Uhr :: Chaoslabor, Heliosstraße 6 a, 50825 Köln	
Mannheim :: C3MA :: Chaos Computer Club Mannheim e. V.	https://www.ccc-mannheim.de/
Fr 19 Uhr :: Neckarauer Str. 106-116, 68163 Mannheim	
München :: muCCC :: Chaos Computer Club München e. V.	https://muc.ccc.de/
2. Di 20 Uhr :: muc, Schleißheimerstraße 39, 80797 München	
Paderborn :: C3PB :: C3PB e. V.	https://c3pb.de/
Mi 19 Uhr, 1. So ab 12 Uhr :: Westernmauer 12-16, 33098 Paderborn	
Salzburg :: Chaostreff Salzburg	https://sbg.chaostreff.at/
Fr 20 Uhr :: Ulrike-Gschwandtner-Straße 5, 5020 Salzburg	
Stuttgart :: CCCS :: Chaos Computer Club Stuttgart e. V.	https://cccs.de/
1. Di 18 Uhr (Lichtblick), 3. Mi (shackspace)" :: Stuttgart	
Ulm :: CCCU :: Hackerspace Ulm e. V.	https://ulm.ccc.de/
oft :: Freiraum, Platzgasse 18, 89073 Ulm	
Wien :: C3W :: Chaos Computer Club Wien	https://c3w.at/
3. Di 19 Uhr :: Metalab, Rathausstraße 6, 1010 Wien	
Wiesbaden :: CCCWI :: Chaos Computer Club Wiesbaden e. V.	https://cccwi.de/
Di 19 Uhr :: Sedanplatz 7, 65183 Wiesbaden	
Würzburg :: N2N :: Nerd2Nerd e. V.	https://nerd2nerd.org/
Do 18:30 Uhr :: FabLab Würzburg, Veitshöchheimer Straße 14, 97080 Würzburg	
Zürich :: CCCZH :: Chaos Computer Club Zürich	https://www.ccczh.ch/
Mi 19 Uhr :: Röschibachstrasse 26, 8037 Zürich	

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

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

2⁴. Datenspuren in Dresden

von norbert
<norbert@c3d2.de>

Schauen wir einmal zurück: Als 2004 die ersten Datenspuren stattfanden hieß es: Privatsphäre war gestern. 2004 wurde Facebook gegründet, Google startete seinen Maildienst unter dem Namen Gmail und die Einführung der LKW-Maut wurde um ein Jahr verschoben. Themen der Datenspuren damals waren u. a.

- „Hinter den Kameras des Mautsystems“ von F. Rosengart
- „E-Mail-Verschlüsselung“ von K. Rosenbaum
- „Vorratsdatenspeicherung“ von M. Hannich
- „Datenschutz in Sachsen und Europa“ von A. Schneider

Auf dem Podium wurde diskutiert: „Habe ich etwas zu verbergen?“

Was hat sich seither verändert?

Die Bundesregierung hat mit der Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) eine Bundesanstalt für Krypto- und Big Data Analyse geschaffen. Der BND darf dazu Daten an zentralen Kommunikationsstellen abgreifen – mittlerweile auch legal. Denn der NSA-Unterschuchungsausschuss hat zwar Einblicke in die Arbeit des BND ermöglicht, aber im Endeffekt nichts verändert.

Dagegen wurde unser eigenes Sicherheitsgefühl durch mehrere kritische Lücken in Open-Source-Software erschüttert, z. B. Heartbleed in OpenSSL, KRACK in WPA2, Dirty COW im Linux-Kernel. Hinzu kam der IT-Super-GAU in Form von Meltdown und Spectre. Bis heute gibt es keinen Fix, sondern nur Linderung, weil der Fehler tief in den gängigen Prozessorarchitekturen sitzt.

Das Internet wird von privaten und staatlichen Akteuren für Sabotage, Spionage und Manipulation genutzt. Niemand kann ohne Spam-Filter E-Mail nutzen. Mit Spearfishing wird versucht, auch achtsame Nutzer unter Kontrolle zu bringen und dank „Internet of Crap“ kann jeder für wenig Geld DDoS-Angriffe fahren. China hat sein „Internet“ bereits abgeschottet, Russland macht gerade erste Versuche damit. Wann ziehen die USA oder die EU nach? Steht das Internet vor dem Kollaps?

Das BSI will dem jedenfalls nichts entgegensetzen. Router und „Dinge“ dürfen auch weiterhin ohne garantierten Lebenszyklus auf den Markt und ins Internet. Dafür steht die Vorratsdatenspeicherung wieder einmal vor Gericht – und täglich grüßt das Murmeltier.

Patch gehabt

Was kommt jetzt noch, wenn 2004 Privatsphäre schon gestern war? Auf dem 34C3 hieß es *TUWAT*. Was haben wir getan? Technische Patches allein werden uns nicht weiterbringen. Wir brauchen auch politische, rechtliche und gesellschaftliche Patches. Kommt auf die Datenspuren 2019, stellt Eure Patches vor und tauscht Euch aus:

Datenspuren 2019 – Patch gehabt!
Eintritt frei: am 21./22. September
im Zentralwerk, Riesaer Straße 32
Dresden

Besonderes Augenmerk wollen wir den Fragen widmen, wie wir ein freies, wertschätzendes und wertschöpfendes Internet erhalten können und wie wir mit unseren Gesundheitsdaten (eGK, eGA) umgehen wollen.

Auf existierenden Strukturen aufbauen: Das Chaos in Potsdam

Ein Interview der Datenschleuder mit Christoph, profemo und tzwenn

In Potsdam hat sich jüngst ein neuer Chaostreff mit dem leicht merkbaren Namen CCCP [1] gegründet. Denen wollen wir doch mal auf den Zahn fühlen. Was ist geplant? Wir sprechen mit Christoph, profemo und tzwenn, die sich bereiterklärt haben unsere Fragen zu beantworten.

Datenschleuder: *Wer hatte eigentlich die Idee, einen Potsdamer Chaostreff zu gründen?*
alle: profemo! Er hat initial eingeladen.
profemo: Mit einem Bekannten hatten wir die Idee, dass in Potsdam ein Chaostreff fehlt.

Datenschleuder: *Und wann wurde aus der Idee ein Plan und dann ein Hackerspace?*
profemo: Im Mai letzten Jahres haben wir erstmals alle Interessierten eingeladen.

Datenschleuder: *Wieviele Personen engagieren sich aktuell bei Euch?*
Christoph: Im Kern-Team sind zehn Menschen aktiv. Zu den Treffen hatten wir sogar schon mal über dreißig Leute. Für die Demovorbereitung gegen die Urheberrechtsrichtlinie hier in Potsdam waren es etwa 45 Personen.

tzwenn: Wir hatten für die Demo einen Infoabend mit Referenten [@presroi] und danach Schilder gebastelt.

Datenschleuder: *Wenn Ihr von der Demovorbereitung sprecht: Kann man schlussfolgern, dass Ihr sowohl politisch arbeiten wollt als auch Werkzeuge und Platz zum Basteln habt?*
Christoph: Genau. Wir hatten auch unseren lokalen Wahlcomputer-Skandal an der Uni, wozu tzwenn einen Hack und einen Vortrag gemacht hat.

Datenschleuder: *Ein Wahlcomputer-Skandal! Worin bestand der?*
tzwenn: Dass die Uni Potsdam jedes Jahr auf andere Art die Wahl elektronisch abhalten möchte oder zumindest das Wahlberechtigtenverzeichnis digitalisiert per Mensa-Chip-Karte einrichten will. Ich bin durch die Uni-Gremien

gezogen, bis ich an den Quelltext kam, und habe dann die Exploits gesucht, die ich noch nicht aus dem Binary hatte. Stellt sich raus: unter anderem SQL-Injection in freier Wildbahn, also können beliebige Personen von der Wahl ausgeschlossen werden oder zweimal wählen.

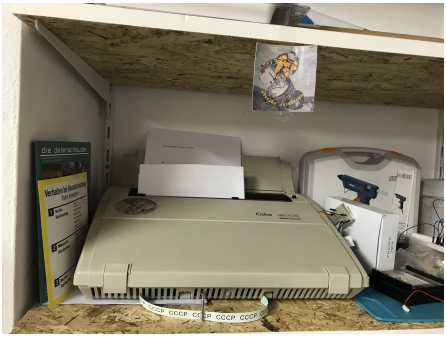
Datenschleuder: *Welcher RFID-Chip ist auf der Potsdamer Mensakarte?*
tzwenn: InterCard ist der Hersteller. Wichtiger war aber die selbstgeschriebene serverseitige Software, die das Wählerverzeichnis ersetzen sollte. Inzwischen möchte die Uni beim Online-Wahlen-Anbieter POLYAS eine Komplettlösung einkaufen, wogegen ich ebenfalls arbeite.

Datenschleuder: *Ist es eigentlich mit der Hackerethik vereinbar, den Hack öffentlich zu machen anstatt durch die Manipulation des Ergebnisses Verbesserungen an der Uni herbeizuführen?*
tzwenn: Der „Probelauf“ im Jahr 2017 ging aus unerklärlichen Gründen schief. Ich finde, wenn ich Elend durch Hinweise vermeiden kann, sollte es vermieden werden.

Datenschleuder: *Das war natürlich auch keine ernstgemeinte Frage. Aber zurück zum CCCP: War es eigentlich schwer, in Potsdam Räume zu finden? Wieviel Platz habt Ihr derzeit?*
Christoph: In der „machBar“ haben wir so grob hundert Quadratmeter. Dazu kommt ein benachbartes BioLab.
profemo: Die „machBar“ ist ein Fablab, in dem wir uns treffen, die gibt es schon länger und entwickelt sich langsam zu einem schönen Hackerspace. Wir haben vor Ort vom Lasercutter bis zum Biolab alles Mögliche zum Basteln.

Datenschleuder: *Welche Biowaffen werden in dem BioLab erstellt?*
Christoph: Gerade Kombucha-Leder (vegan) als Experiment.
profemo: Im Labor wird vor allem mit Pilzen gearbeitet.
Christoph: Derzeit ist das Lab mit seinen Möglichkeiten aber unserem Wissen krass voraus.

Datenschleuder: *Was sind denn Eure Wünsche für Themen oder für Werkzeuge, die Ihr in naher Zukunft anstrebt?*
profemo: Die Idee vom CCCP ist es, Aktivitäten einen Rahmen zu geben, damit keiner sich alleine abmühen muss.
tzwenn: Ansonsten haben wir auch Bau- und Bastelprojekte.
Christoph: Zum Beispiel mach ich gerade mit ein paar Leuten eine alte DDR-Schreibmaschine wieder flott: eine Erika 3004 electronic. [2]

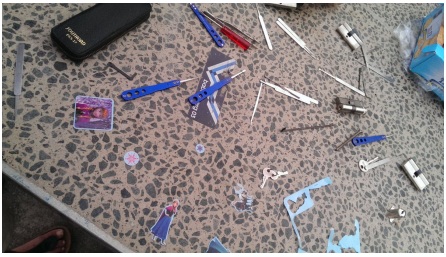


Erika 3004 electronic

Datenschleuder: *Vintage-Projekte!*
Christoph: Ich hab sie für vierzehn Euro unter Kleinanzeigen bekommen, und sie hat ein Digital-Interface! Also habe ich ein Oszilloskop rangeklemmt und mal geschaut. Stellt sich heraus: Ist fast eine normale UART – nur die DDR hat bei ASCII nicht mitgemacht. Also

haben wir ein kleines Embedded Board als Dolmetscher drin versteckt. Jetzt kann sie auch mit den „Amerikanern“ unter den PCs reden.

Datenschleuder: *Da drängt sich die Frage auf, was Ihr so für Hintergründe habt, denn das riecht ja nach technischem Vorwissen. Was macht Ihr sonst so im Leben, was mit Technik?*
Christoph: Also im Job bin ich Programmierer. Als Hobby bring ich Kids das Coden bei, aber nicht bei Chaos macht Schule, sondern beim CoderDojo.
profemo: Ich bin Sozialwissenschaftler, aber in der Wirtschaftsinformatik gelandet.
tzwenn: Ich promoviere Informatik-nah. Allgemein sind viele der Leute im Treff Informatik-Studis. Aber auch Physiker-, Linguist- und Cognitive-Science-Leute sind anwesend.



Lockpicking-Session Baumwolltier

Datenschleuder: *Habt Ihr in den hundert Quadratmetern auch eine Küche oder Dusche? Und wie tragt Ihr Euch finanziell bei der noch kleinen Aktiven-Menge?*
Christoph: Das passiert alles über den Space: Wir sind nur circa ein Siebtel der Grüppchen in der machBar.
profemo: Die „machBar“ besteht aus verschiedenen Gruppen. Es gibt zum Beispiel die Leute, die eher als Maker bezeichnet werden können, dann eine Gruppe im oklab, dann wieder Leute, die sich im Biolab umtun.

Datenschleuder: *Also war es eine große Starthilfe, auf existierenden Strukturen aufbauen zu können?*
Christoph: Absolut! Gerade jetzt diesen Winter, wo es richtig losging. Wir kochen zum Beispiel immer mit ein paar Platten aus dem Biolab. Wir hatten auch schon Glühwein vom Chemie-Rührkocher.
tzwenn: Wir sind auch dankbar für den Bootloader hier, weshalb jetzt die Vereinsbildung natürlich unseren Kostenbeitrag ermöglichen soll.

Datenschleuder: *Nun kann ja jeder ein Lab, ein Hacker- oder Makerspace oder ein Biolabor aufmachen. Warum wolltet Ihr das beim CCC andocken, nur wegen des schönen Namens CCCP?*
profemo: Es war kurios, dass es in Brandenburg noch keine Strukturen gab, die sich mit Hackerethik und Netzpolitik im Sinne des CCC auseinandersetzen. Alles wurde immer ins Schwarze Loch nach Berlin gesogen. Als wir dann mal wieder mit vielen Potsdamern auf dem Congress saßen, haben wir dann beschlossen, das zu ändern.
Christoph: Wir haben uns immer auf dem Congress oder Camp getroffen und erstaunt festgestellt, dass wir alle quasi Nachbarn sind.

profemo: Für den letzten Congress haben wir uns dann als erste Amtshandlung eine kleine Assembly innerhalb der ChaosZone organisiert. In Potsdam gab es vor dem Chaostreff schon die uplug-Gruppe, Maker, oklab und Freifunker, aber halt keinen Club.

Datenschleuder: *Mit wievielen Leuten wart Ihr dann in Leipzig?*

Christoph: In Leipzig circa dreißig Leute.

Datenschleuder: *Wenn Euch jemand besuchen oder kennenlernen will, wann sollte man am besten vorbeikommen? Habt Ihr Veranstaltungen, die regelmäßig oder unregelmäßig stattfinden?*
Christoph: Immer mittwochs, 19 Uhr in der „machBar“ im Freiland. Es gibt verschiedene Kanäle, wo man Dinge über uns erfahren kann, zum Beispiel radio.ccc-p.org als Podcast. Ist erstmal nur eine Folge, aber ein Hyperbandrauschen ist in Erstellung. Also schon zwei Folgen, tzwenn hat direkt einen Feed programmiert!
profemo: Ansonsten planen wir derzeit mit anderen eine Veranstaltungsreihe, aber die wird auch vor allem mittwochs stattfinden.

LED-Leuchtprojekt-Zwischenstand
Baumwolltier

Datenschleuder: *Wieviel Leute passen bei Euch rein, wenn Ihr das anbietet?*
Christoph: Zwanzig Personen locker, für einzelne Veranstaltungen gehen bis zu fünfzig.

tzwenn: Wir könnten auch Zusatzräume spontan anmieten.
profemo: Für größere Veranstaltungen können wir also auf andere Räume auf demselben Gelände ausweichen.
Christoph: Da ist dann Platz für bis zu dreihundert Menschen.

Datenschleuder: *Das soziale Leben in einem Space ist ja bekanntlich auch nicht unwichtig. Feiert Ihr auch zusammen, gibt es mal Musik und Party?*
profemo: Bisher selten. Aber kann ja noch kommen.
Christoph: Ich find ja, Cryptoparties haben zu viel Crypto und zu wenig Party. Das muss und wird sich ändern!

Datenschleuder: *Gibt es Anschaffungen, die Ihr gern hättet, aber zu denen derzeit das Geld nicht reicht? Sucht Ihr noch Unterstützung, finanziell oder ideell?*
Christoph: Buntes Licht! Eine Werkstatt hat nämlich Vor- und Nachteile: Wir haben zig Lasercutter, 3D-Drucker, Fräsen. Aber dieses fiese weiße Licht…
profemo: Neue Deckenlampen und die regelmäßige Miete werden das nächste Projekt.

Datenschleuder: *Also noch zuviel Zahnarzt-Flair?*
Christoph: CNC-Zahnarzt!
profemo: Wir müssen das alles noch in das richtige Licht rücken!

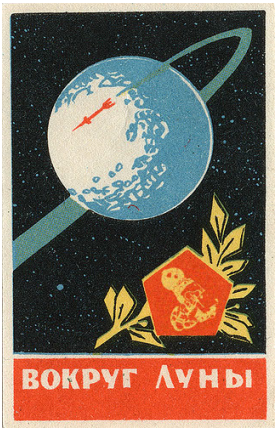
Datenschleuder: *Wollt Ihr denn wachsen? Eine angenehme und gemütliche Atmosphäre lockt ja hoffentlich neue Leute an.*
Christoph: Das Kern-Team könnte gestärkt werden. „Besucher“ haben wir viele, netter ist es mit mehr Aktiven.
profemo: Der Space hat insgesamt noch Entwicklungspotential, sei es im Chaostreff oder im Biolab. Da sind wir offen für Leute, die sich einbringen wollen.
Christoph: Aber wir sind schon über die kritische Masse hinweg, denke ich. Der CCCP ist gekommen, um zu bleiben!
profemo: Als nächstes steht an, dass wir uns um die Ehren eines richtigen Erfas bemühen, aber alles Gute muss Weile haben!

Datenschleuder: *Zuletzt, wir sind ja hier im CCC: Was ist für Euch die aus technischer Sicht gefährlichste Idee, die aktuell aus der Politik droht?*
profemo: Verfassungsschutz-Trojaner und deren heimliche Installation, also dass sie dafür in die Wohnungen einbrechen dürfen sollen.

Datenschleuder: *Vielen Dank für das Interview und viel Erfolg für die Zukunft des Space! Habt Ihr noch eine Nachricht, die Ihr den Lesern mitgeben wollt?*
profemo: Bringt Euch mehr ein, baut stabile Infrastruktur und redet mit den Leuten, damit sie nicht auf dumme Ideen kommen. Zusammen erschaffen wir schöne Dinge! Als Aktive aus der Provinz können wir nur empfehlen, einfach mal den ersten Schritt zu machen. Es kommen viele aus der Deckung und machen mit.
Christoph: Geht auf ccc-p.org und kommt vorbei! Und falls Euch das zu weit weg ist, dann ist es ein Zeichen, dass Ihr auch einen lokalen Treff booten müsst.
tzwenn: Chaosinteresse findet sich überall!

Referenzen

[1] Der CCCP im Netz: https://ccc-p.org/
Mastodon: @cccp@chaos.social
Twitter: @ChaosPotsdam
[2] GitHub-Repo zur Erika 3004; https://github.com/Chaostreff-Potsdam/erika3004



CCCP Congress-Propaganda-Reihe

Hackspace und Chaos in Siegen

von nanooq <nanooq@chaos-siegen.de>

In Siegen gibt es je einen Verein für den Hackspace und einen für das Chaos. Diese Konstellation ist im Chaos nicht neu, in Siegen beschreibt sie die beiden wichtigsten Vereine. Nun beantragt Chaos Siegen den Erfa-Status und berichtet exklusiv in der Datenschleuder. Ein Bericht von der Gründung des Hackspace, die Wirkung auf die lokale Szene und die Etablierung des Chaostreffs.

HaSi e. V.: Hackspace Siegen

Auf dem Camp 2011 spielten wir ein Spiel:

> *Es gibt keinen Hackspace in Siegen und Chaoten in der Stadt kenne ich auch nicht, also gehe ich zum Zelt vom Chaostreff Dortmund, jammere etwas und schnorre Club Mate.*

Damals war Club Mate noch der heiße Scheiß – und Dortmund lieferte sie *en masse* (Tun se immer noch.). Irgendwann gab es zur Mate noch ein

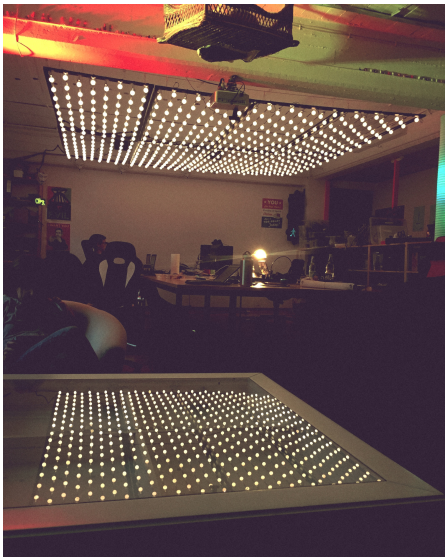
> *Du bist schon die dritte Person aus Siegen, die hier vorbei kam. Ihr solltet euch mal kennen lernen.*

Nach etwas Warten fand dort das erste Treffen statt. (Eigentlich nur wegen der Mate.) Danach folgte ein Zweites in größerer Runde, um Details zu besprechen und beim dritten Mal trafen wir uns in einem leeren Schaufensterladenlokal, der unser erster Vereinsraum wurde.

Blinkinvader war unser erstes Projekt.

Unsere Chaosquote war hoch, aber wir waren nicht viele. Um schnell mehr zu werden, gründeten wir einen thematisch breiter aufgestellten Hackspace, das HaSi - von **Ha**ckspace **Si**egen. Wir hielten das für den einfachsten Weg. Denn Siegen, das Siegerland und Südwestfalen bildeten eine große Chaos-Diaspora. Es gibt hier viele Nerds. *Vielleicht finden die im Hackspace ihren inneren Chaoten?*

Wahrscheinlich war die Vermutung genauso richtig, wie sie falsch war…

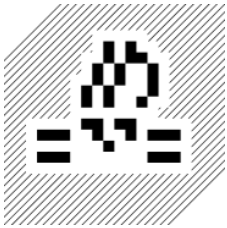


Balldachin. Zack TheSystem

In den folgenden Jahren entwickelte sich das HaSi weiter und konnte, aus eigener (Mitgliedsbeitrags-) Kraft in größere Räume ziehen: 140 m^2 in einer ehemaligen Pelzfabrik – sowas denkst du dir nicht aus!

Heute haben wir im Eingangsbereich eine selbst gebastelte Space-Bar (bis zur Fertigstellung wurde sie Progress-Bar genannt) mit allem Schnick und Schnack.

Es gibt praktische Deckenmöbel (Seite 0x31) mit darunterliegenden Sofalandschaften und eine Konsolenecke in der ein riesiger Bildschirm thront.



Logo des HaSi e. V.

Neben der gemütlichen Seite steht ein großer Tisch mit Leinwand und Beamer, Balldachin und Stühle. Es gibt, wie es sich für einen Hackspace gehört, aber auch Internet, Projektkisten in Projektregalen und Drucker.

Aber auch einen weiteren Flur, an unserer Holzwerkstatt vorbei zu den Toiletten für Pinguine und Kängurus. Das Känguru-Klo hat auch eine kaputte Dusche. Dann ein kleines Stück Küche, Vorratskammer und den Stillarbeitsraum. Dort befinden sich Laser, 3D-Drucker, Harry Plotter, Harry Plätter, die Lötstationen, ewig viele farbige Folienrollen und Button-Maschinen. Läuft bei uns.

Der gemeinnützige Verein trägt sich durch Mitgliedsbeiträge, organisiert gemeinschaftliche Veranstaltungen und wirbt Neulinge. Die personelle Vernetzung reicht von Theater und Künstlern über Aktionisten, Parteien und Bürgerrechtsgruppen, Datenschutzbeauftragte, Unverpackt-Genossenschaften und Foodsharing bis zum lokalen Fab Lab, Urban Gardening, einem Getränkehandel und Weitere. Andere Orte zum Treffen und Dinge zu tun sind entstanden: Die lokale Szene trifft sich

nun nicht nur beim Blinkenlight des HaSi, sondern auch im Fab Lab der Universität Siegen oder beim „L'art pour l'art" im Atelierhaus Oberstadt.

Stillarbeitsraum.

Chaos Siegen e. V.

Im Hafen ist das Schiff sicher, aber dafür wurde es nicht gebaut.

Spruch auf einer mittlerweile zerbrocheen, alten Kaffeetasse

Nachdem sich das HaSi als ein Hafen für die lokale Szene bewiesen hat, bestiegen ein paar Chaoten ein neues Schiff *Chaos Siegen* und stachen in See. Es ist auf politische Aktionen und CCC-Veranstaltungen ausgerichtet: Chaos macht Schule, Cryptoparties, ein Laberpodcast zu CCC-Themen [schamlose Eigenwerbung: 3], der *Europäische Datenschutztag* und eine Vielzahl von Veranstaltungen, Workshops und Demonstrationen [4]. Erwähnenswert ist, dass Chaos Siegen e. V. aufgrund der aktuell kritischen Rechtslage bewusst nicht gemeinnützig ist, um das (politische) Engagement dadurch nicht einschränken zu müssen. Wer der Siegener Szene gegen Quittung spenden möchte, wende sich gerne an das HaSi. Wer CCC-Themen in Siegen voran treiben möchte, wende sich an das Chaos.

Im Protokoll des Bootstrap-Treffens auf dem 29C3 definiert inj4n das Chaos in Siegen als Schnittstelle zwischen HaSi und dem CCC. Dies ist auch in unserer Satzung festgehalten [5] und verankert im Vorstandsamt des Erfakreisvertreters. Siegen stellte 1,2 % der Gäste auf der Easterhegg 2019 – wir waren sieben Personen. Chaos Siegen ist regelmäßig bei Chaos West und bastelte für den Kongress, unter anderem, die Palme, die Ananas und die kleine Lounge.

Chaos Siegen arbeitet projektorientiert in Arbeitstreffen und präsentiert Ergebnisse in Öktionen (**Ö**ffentliche A**ktionen**) [6] oder Blog-Artikeln. Wir pflegen das *savoir vivre* in unseren Wellnesstreffen, indem wir Essen gehen (Indisch, mongolisch, italienisch, japanisch, türkisch, vietnamesisch …) Eigentlich wollen wir auch mal in die Sauna gehen – aber nanooq ist verklemmt.

Die Arbeitstreffen finden entweder privat oder im HaSi statt. Es gibt keine eigenen Vereinsräume, die Szene versorgt uns damit und wir geben zurück: Öffentlichkeitsarbeit, Werbung für Veranstaltungen, Teilnahme an Kunsttagen, Organisation von Demonstrationen und Zugang zu coolen Leuten (uns)!

Logo Chaos-Siegen

Jeder kann bei uns mitmachen, eine Mitgliedschaft ist nicht notwendig. Aber wir haben hier eine Besonderheit: Mitglieder haben wir nur wegen der juristischen Form – Die wiederum haben wir um nicht als terroristische Vereinigung zu gelten. Einmal im Jahr gibt es eine Mitgliederversammlung und ordentliche

Mitglieder haben Stimmrecht. Um ein solches Mitglied zu werden, muss man in der Lage sein, die eigene Mitgliedschaft im CCC und im HaSi vorzuweisen. Das bedeutet wir haben einen Anteil von 100% CCC-Mitgliedern im Chaos Siegen.

Reden wir über Geld. Es gibt keine Miete zu bezahlen, nur Kontoführungsgebühren, Webspace und alle drei Jahre einen Notar für Änderungen im Vereinsregister. Alles andere Geld geben wir für Chaos macht Schule, Cryptopartys und Material für unsere Workshops aus – und für Reisekostenzuschüsse zu CCC-Veranstaltungen.

Zum Abschluss eine Anekdote über unseren Namen. Die erste Idee war „Meinungsaustausch Siegen“, dann hätten wir uns „MauSi“ abgekürzt. Weil wir auch HaSi-Mitglieder sind, hätten wir uns gegenseitig offiziell mit „Hasi-Mausi“ ansprechen dürfen.

Das ist es nun nicht geworden und das ist sehr schade. Aber, wenn wir Erfa sind, dann heißen wir offiziell „Chaos Computer Club Siegen“, also

CCC Siegen ⇒ C3 Si ⇒ <3 Si ⇒ ♡ Si

ausgesprochen „Herzi“. Wenn du offizielle „Hasi-Herzis“ im Club haben willst, wende dich jetzt an deinen Erfakreisvertreter und fordere „Ja!“ zum Erfa-Antrag von Chaos Siegen.

Referenzen

[1] Website Hackspace Siegen https://hasi.it/

[2] Website Chaos Siegen im Netz, https://chaos-siegen.de/

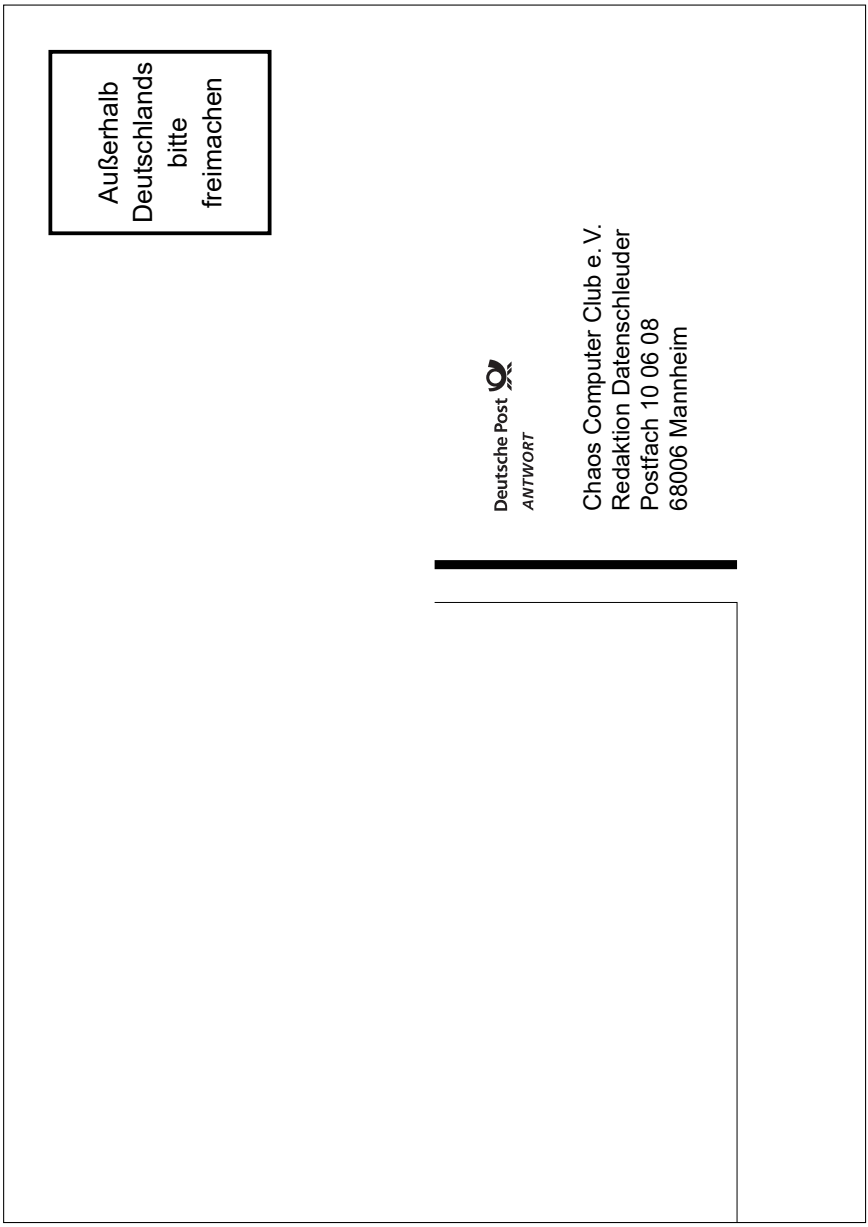
[3] Podcast Chaos Siegen, https://podcast.chaos-siegen.de

[4] Veranstaltungskalender, https://kalender.chaos-siegen.de

[5] FAQ zur Satzung des Chaos Siegen e.V.: https://chaos-siegen.de/satzung

[6] Gitlab Gruppe des Chaos Siegen: https://gitlab.com/chaos-siegen

35C3: Palme, Ananas und Lounge. Simon Budig



Antwort-Postkarte zum Ausschneiden, Siehe Geleitwort (Seite 0x01)
Beförderung durch die Chaospost ist selbstverständlich kostenlos. Innerhalb Deutschlands muss die Karte auch nicht zwingend frankiert werden, allerdings spart ihr dem Club Geld, indem ihr selbst eine Marke draufklebt.

Für Sendungen aus dem Ausland bitte freimachen und die Markierung mit „Deutsche Post, Antwort“ streichen.