36C3: Von Netzpolitik und Klimawandel

Einmischen statt stillhalten

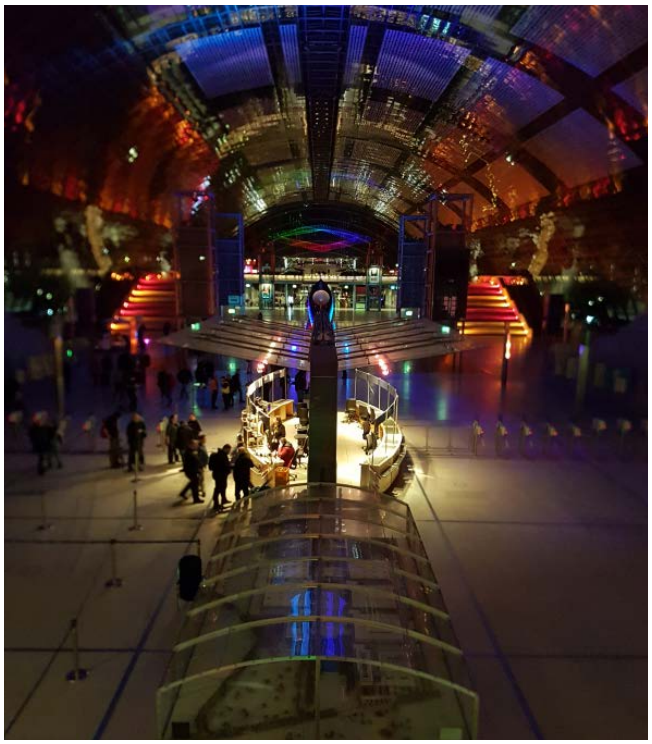
Manuel Atug

Der 36. Chaos Communication Congress war weiter denn je davon entfernt, sich allein auf die Technik zu konzentrieren und der Politik den Rest zu überlassen. Zu oft geht das daneben, wie zahlreiche Beispiele zeigen.

Vier Tage lang beleuchtete der traditionell zwischen den Jahren stattfindende Chaos Communication Congress technische, politische, gesellschaftliche und auch utopische Themen, in diesem Jahr unter dem Motto „Resource Exhaustion“. Wie schon im vergangenen Jahr wurden rund 17 000 Teilnehmer in den bunt gestalteten Räumlichkeiten auf der Messe Leipzig erwartet, darunter mehr als 2000 freiwillige Helfer.

Dem Motto angemessen ging es beim 36. Kongress des Chaos Computer Clubs (36C3) nicht mehr nur um die reine Technik und erweiterte netzpolitische Themen, vielmehr stand auch die Klimapolitik auf dem Themenplan. Des Weiteren wurde viel über Rechtsradikale und den Umgang der Gesellschaft mit ihnen diskutiert. Insgesamt ist der Kongress deutlich politischer geworden, da die Digitalisierung in immer mehr Gebiete unserer Gesellschaft Einzug hält und die netzpolitischen Entscheidungen und daraus entstehenden Gesetze stärker in unsere Freiheitsrechte eingreifen – wenn nicht die Mitglieder des CCC mit ihrer Sachkenntnis und andere Teile der Zivilgesellschaft gegensteuern. Die Community lebt die aus einem frühen Science-Fiction-Film stammende Devise „Be excellent to each other“ auf allen Ebenen, nicht nur auf der technischen.

Natürlich gab es auch wieder jede Menge Sticker, die man aus Sticker-Exchange-Boxen mitnehmen oder dort hineinlegen konnte. In Verballhornung der heutzutage allgegenwärtigen Security Operations Center (SOC) gab es ein „CCC Sticker Operations Center“ – C3 STOC, gar mit eigenem Twitter-Account. Es warb für eine „dezentralisierte“ Stickerverteilung via Boxen, da die zentrale Verteilung im vergangenen Jahr zur Schlangenbildung geführt hatte. Zentralisierung funktioniert eben nicht, so die knappe Schlussfolgerung des C3 STOC im Kongress-Wiki.



Bunt und mit fantasievollen Dekorationen präsentierte sich der CCC auf der Messe Leipzig (Abb. 1).

Live, gestreamt oder in Gruppe

Der Chaos Communication Congress ist inzwischen so groß und vielfältig geworden, dass man nicht mehr von „dem“ Kongress sprechen kann, da es inzwischen so viele Aspekte, Derivate und Abwandlungen gibt, dass jeder seine eigene Form der Veranstaltung erlebt und mitgestaltet. Sei es als Assembly, also als Gruppierung, oder sogar mit einer eigenen Bühne in Form eines kleinen „Kongresses im Kongress“. Für alle, die nicht vor Ort teilnehmen konnten oder wollten, gab es wie gewohnt die Möglichkeit, die Livestreams zu Hause anzuschauen oder eben gemeinsam in einem Hackerspace einen „Congress everywhere“ zu gestalten. Dezentralisierung funktioniert auch hier als Mittel zur Skalierung.

Anhand des Fahrplans, der weiterhin im Netz veröffentlich ist, können Interessierte das Programm sichten und die im Netz frei verfügbaren Videoaufzeichnungen nachhören (alle im Text erwähnten Videos und Quellen sind über den Link ix.de/z49e zu finden). Die Vorträge sind teilweise nicht nur ins Englische und Deutsche übersetzt, sondern auch in weitere Sprachen.

Security-Albträume „in echt“

Die Security Nightmares 0x14 geben inzwischen schon wie gewohnt einen IT-Security-Albtraum-Ausblick auf das nächste sowie einen Rückblick auf das vergangene Jahr. Erheiternd und bestürzend, manchmal sogar resignierend stellten Frank Rieger und Ron Hendrik Fulda wieder einmal dar, welche Fails verschiedener Akteure uns begleitet und genervt haben. So aktualisierte im vergangenen Jahr etwa das Kammergericht Berlin seine Faxgeräte, um nach einem Trojanerangriff (analog) weiterarbeiten zu können.

In den Bereich „genervt“ fällt die verschärfte Diskussion um Hintertüren in den USA, die außer Unsicherheit nichts bringt, von Politikern aber immer wieder ins Spiel gebracht wird. Und schließlich wurden im vergangenen Jahr bei den Top-3-Herstellern von Antivirensoftware 30 TByte an Daten aus dem Unternehmen getragen – offenbar hatten sie ihre eigenen Produkte nicht im Einsatz.

Beim dezentralen CCC-Jahresrückblick gaben Vertreter verschiedener Gruppen einen Überblick über die Aktivitäten im und um den Chaos Computer Club herum. So berichtete unter anderem Frank Rieger von den Bemühungen des CCC, Politiker – „die Berliner Lobbyblase“ – mit sachgerechten Informationen zu

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der iX aus 30625 Hannover

versorgen. Zur Panik in Sachen IKT-Ausrüster Huawei merkte er an, dass sämtliche Telco-Anbieter ähnlich viele schwerwiegende Bugs in ihren Produkten hätten. Das Einbauen von Backdoors sei also reine Zeitverschwendung.

Parallel zur Huawei-Debatte beschäftigte sich die Politik mit dem IT-Sicherheitsgesetz 2.0. Als problematisch erachtet der CCC, dass das Bundesinnenministerium neben den guten Ansätzen einen „Wünsch-dir-was"-Kasten für die innere Sicherheit eingebaut hat, der dazu führt, dass die IT-Sicherheit verschlechtert wird. Zum Beispiel das Ansinnen, Anonymisierungsdienste zu kriminalisieren oder ihre Nutzung strafbar zu machen. Die ständigen Angriffe auf die Wirtschaft im vergangenen Jahr haben allerdings zur Erkenntnis geführt, dass man sich wieder stärker auf die IT-Sicherheit konzentrieren muss. Daher gab es viele Anhörungen und Fachgespräche mit dem CCC. Eine Forderung des CCC an die Politik ist es, das BSI als oberste IT-Sicherheitsbehörde vom BMI unabhängiger zu machen, damit IT- und innere Sicherheit nicht ständig vermischt werden und letztere erstere nicht länger beeinträchtigt.

Industrielle (Un-)Sicherheit

Im Vortrag „On the insecure nature of turbine control systems in power generation" zeigten repdet, @_moradek_ und c0rs, wie sie das Prozessleitsystem Siemens SPPA-T/P 3000 zur Industrieautomatisierung bei Turbinen in Kraftwerken exemplarisch auf Sicherheitslücken analysierten. Das technisch im Detail vorgestellte Ergebnis mit 54 Schwachstellen ist desaströs. Die Forscher hoben aber hervor, dass es bei vergleichbaren Komponenten anderer Hersteller ähnlich schlecht aussehe. Im Rahmen eines Responsible-Disclosure-Prozesses wurde der Hersteller über alle Schwachstellen informiert, damit er Updates bereitstellen und seine Kunden darauf hinweisen konnte.

Quelle: CCC

Nach dem Scheitern der Zentralisierung im vergangenen Jahr wurden die Sticker 2020 dezentralisiert verteilt (Abb. 2).

In „Hirne hacken" zeigte Linus Neumann eindrucksvoll und witzig anhand zahlreicher Beispiele, welche menschlichen Faktoren Kriminelle für ihre Zwecke ausnutzen und wie Lösungsansätze aussehen können. Zwei internationale Studien von Neumann mit einer vierstelligen Zahl von Probanden haben etwa ergeben, dass das theoretische Lernen bei Awareness-Schulungen, zum Beispiel zu Phishing-Situationen, nahezu wirkungslos ist. Hingegen zeigt eine sichtbare (simulierte) Infektion durch eine Phishingmail, also das eigene Erleben eines Angriffs, einen deutlichen Lerneffekt. Am Rande: Neumann gestand, dass auch er nicht gegen solche Phishingmails gefeit und schon einmal darauf hereingefallen sei.

Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, legte in seinem Vortrag „Weichenstellung – In welcher digitalen Welt werden wir leben?" dar, dass Datenschutz ein Vorteil ist und andere Regionen inzwischen mit der Datensparsamkeit werben. Die Wirtschaftsverbände sollten sich daher wieder auf eben diesen Unique Selling Point besinnen. Auch propagierte er, dass wir uns aus Wertegründen für den Datenschutz entscheiden müssen.

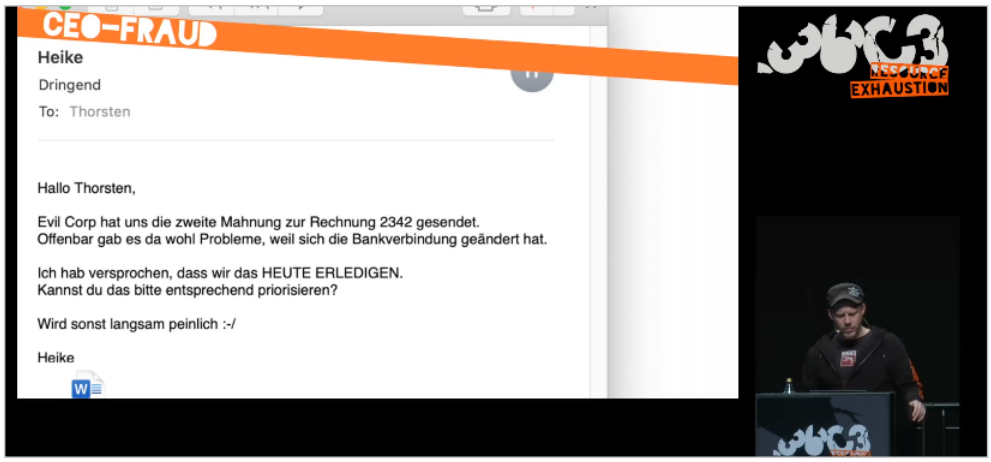
Im Beitrag „FinFisher verklagen – Rechtsbrüche beim Export von Überwachungssoftware" wurde erneut ein Staatstrojaner analysiert. Ulf Burmeyer, Mitgründer und Vorsitzender der Gesellschaft für Freiheitsrechte (GFF), und ths vom CCC legten dar, wieso die Attribuierung einer Überwachungssoftware – also wem sie zugeschrieben wird – nicht trivial ist. 28 Sample-Dateien verwiesen jedoch sehr deutlich auf die Spionagesoftware FinFisher (auch als FinSpy bekannt). Mit ihrer Hilfe wurden Oppositionelle und Journalisten in der Türkei überwacht.

Verstoß gegen Exportbeschränkungen?

Die GFF hat gemeinsam mit Reporter ohne Grenzen, dem European Center for Constitutional and Human Rights und netzpolitik.org Strafanzeige gegen die Geschäftsführer der Unternehmen FinFisher GmbH, FinFisher Labs GmbH und Elaman GmbH erstattet, da durch die Analyse des CCC dringende Anhaltspunkte dafür vorliegen, dass das Münchener Firmenkonglomerat die Spionagesoftware FinSpy ohne Genehmigung der Bundesregierung an die türkische Regierung verkauft hat. Unter ix.de/z49e finden Interessierte den 60-seitigen Bericht, die FinSpy-Tools selbst – da diese auf einem GitHub-Account zum Analysieren veröffentlicht wurden – und die dazugehörige Dokumentation frei zum Abruf.

Welche Kardinalfehler in der Anfang 2021 kommenden digitalen Patientenakte ge-

Quelle: CCC



Druck erzeugen und den Nutzer unter Stress zu setzen ist eine der Strategien, mit denen Kriminelle oft erfolgreich sind (Abb. 3).

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der iX aus 30625 Hannover

Vermutlich würden einige Hersteller gerne solche oder ähnliche Aufkleber auf ihren Produkten anbringen – sinnvoller ist es allerdings, die Sicherheitslücken in ihnen zu beseitigen (Abb. 4).

macht wurden, belegten Martin Tschirsich, cbro (Dr. med. Christian Brodowski) und Dr. André Zilch in „‚Hacker hin oder her': Die elektronische Patientenakte kommt!" Für die Analyse mussten sie zunächst 10 000 Seiten Spezifikation der gematik GmbH durcharbeiten. Von besonderer Bedeutung ist die Identifikation der einzelnen Akteure, da, wie die gematik selbst häufig betont, die Authentisierung ein zentraler Punkt des Systems ist.

Für einen Institutionsausweis benötigt man fünf Daten des Arztes. Vier davon stehen auf jedem Rezept, lediglich das Geburtsdatum muss man sich anderweitig besorgen. Schon kann ein solcher Praxisausweis beantragt werden. Die Lieferanschrift kann man selbst auswählen, da der Ausweis nicht direkt an die Praxis geschickt wird. Mit diesem Ausweis hat man uneingeschränkten Zugang zur Telematik-Infrastruktur. Der Heilberufsausweis kann ohne persönliche Verifikation durch ein Bankidentverfahren beantragt werden. Auch hier kann man die Lieferadresse selbst wählen. Eine Unterschrift des Arztes ist dann zwar noch erforderlich, aber diese steht ja ebenfalls auf den Rezepten. Überdies ist bei der ausgebenden Stelle keine Unterschrift zum Abgleich hinterlegt.

Die Gesundheitskarte (eGK) wiederum ist der zentrale Zutrittsschlüssel für Versicherte zum Gesundheitswesen. Damit ist sie unter anderem auch der Schlüssel für die elektronische Patientenakte, die lebenslang alle relevanten medizinischen Informationen über den Versicherten vorhält. Die Identität muss rechtlich auf Basis des Sozialgesetzbuchs festgestellt werden. Verstöße dagegen, selbst im Einzelfall, sind unzulässig, da es sich um medizinische Daten handelt und das Vertrauen in das System damit sofort zerstört wäre.

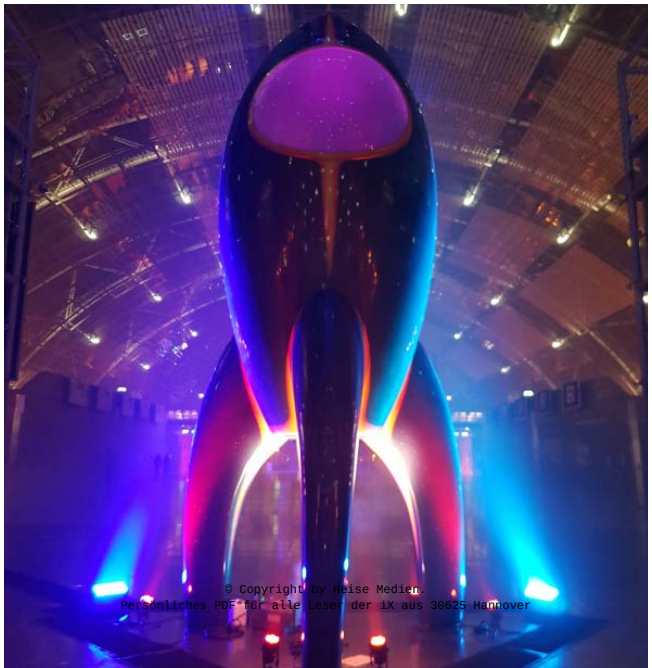
Erschwindelte Gesundheitskarten

Die Vortragenden berichteten, wie einer von ihnen im Zeitraum 2014 bis 2019 in sechs Fällen unberechtigterweise an eine eGK gelangen konnte. Es gibt dafür zwei wesentliche Angriffsszenarien: durch Adressänderung entweder beim Versicherten oder beim Arbeitgeber. Ein eingescannter Brief per E-Mail reichte bereits aus und die eGK wurde an eine neue Adresse zugestellt. Außerdem konnten sich die Sicherheitsexperten einen der Konnektoren besorgen, über die sich eine Praxis mit der Telematik-Infrastruktur verbindet. Diesen gibt es eigentlich nur für Arztpraxen als Bundle in einem teuren Paket. Mit einem einfachen Fax konnten die Experten allerdings bei einem Anbieter ein Gerät einzeln bestellen. Positiv merkten sie abschließend noch an, dass zum einen wesentliche gesetzliche Rahmenbedingungen geschaffen wurden und zum anderen die gematik bei der Umsetzung auch vieles richtig gemacht habe.

„Der netzpolitische Jahresrückblick – War alles schon mal besser" von Markus Beckedahl (netzpolitik.org) begann mit dem Doxing-Fall Anfang 2019 und stellte unter Verweis auf die Hackerethik des CCC klar, dass so etwas weder selbst durchgeführt noch unterstützt werden sollte. Das IT-Sicherheitsgesetz 2.0 wurde in einer Referentenentwurfsfassung geleakt, es liegt aber noch immer keine offizielle Entwurfsfassung vor. Die Regierung täte gut daran, der Bevölkerung Einblick zu gewähren und Entwürfe grundsätzlich öffentlich bereitzustellen.

Beckedahl konstatierte auch, dass noch immer keine defensive Cyberstrategie der Regierung vorliegt. Im Gegenteil: Innenminister Horst Seehofer forderte Staatstrojaner für den Verfassungsschutz – wovon sich netzpolitik.org und der CCC klar distanzieren, da diese nur zu weniger Sicherheit führen. Das ebenfalls geleakte 18-seitige Gutachten der Wissenschaftlichen Dienste des Bundestages zu Hackback hat klargemacht, dass ein solches Vorgehen sehr gefährlich und vor allem auch wirkungslos ist. Die Sicherheit im Zusammenhang mit 5G wiederum ist ein vorgeschobenes Argument, da man überall Ende-zu-Ende-Verschlüsselung implementieren und auf Überwachungsschnittstellen verzichten könnte. Macht man aber nicht. Der Streit um Huawei ist daher eine rein industriepolitische Debatte. Der Vorwurf der USA, dass China Hintertüren einsetzt, ist seit Snowden absurd, wenn man sich anschaut, wie viele Hintertüren Cisco einbaut.

Bei der Upload-Filter-Thematik wurden wir von Ahnungslosen vertreten, so die kurze, aber verheerende Zusammenfassung von Beckedahl zur Artikel-13-Debatte. Die Datenethikkommission dagegen hat nach nur einem Jahr einen ersten Bericht abgeliefert, der sich sehen lassen kann und zahlreiche Vorschläge beispielsweise zu einem transparenten und diskriminierungsfreien Umgang mit Daten und algorithmischen Systemen enthält. Ebenfalls positiv hervorzuheben ist schließlich, dass ab sofort für Digitalisierungsprojekte in Deutschland die Prinzipien von Open Source und offene Standards gelten sollen, da durch öffentliche Mittel finanzierte Software allen Bürgern dienen soll. (ur@ix.de)



Kein Kongress ohne Maskottchen: Seit 2003 ist die Rakete „Fairydust" bei allen CCC-Veranstaltungen präsent (Abb. 5).

© Copyright by Heise Medien
Persönliches PDF für alle Leser der iX aus 30625 Hannover

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der iX aus 30625 Hannover