Beef Jerky, Hoverboards und Hacker*innen

Von Misch Pautsch

Veröffentlicht am 15. Okt. 2021

Wie erreicht man eine Gruppe Hacker*innen? Per Mail, anscheinend. Sie antworten – wenig überraschend – schnell. Oder, indem man den offiziell gemeldeten Sitz ihrer Asbl in Luxemburg Stadt besucht: Die „Chaosstuff". Hört sich alles gar nicht so suspekt an, wie das Wort „Hacker*in" andeuten würde. Ein Gespräch mit Bastler*innen.

Der Name Chaos Computer Club fällt in den Medien meist in Momenten, in denen etwas ordentlich schiefläuft. In Luxemburg war dies kürzlich wieder der Fall, als das Datenleak auf der neuen Internetseite für Online-Petitionen diskutiert wurde. Aber auch die Chamber-Leak Affäre 2018, und in Deutschland das Leck auf der Wahlkampf-App der CDU im Mai 2021, die beide in – nun zurückgezogenen – legalen Schritten endeten. In beiden Fällen haben je der Luxemburgische und Deutsche Chaos Computer Club die rechtliche Schritte gegen die Whistleblower stark kritisiert und dafür plädiert, dass die Verantwortlichen der Seiten ihre Verantwortung auch wahrnehmen, statt die Boten schlechter Nachrichten ins Visier zu nehmen.

„Diese Momente sind wohl diejenigen, für die uns die meisten Leute kennen", bestätigt Dennis Fink des Computer Club Luxemburg (C3L): „Und es ist sicherlich ein großer Teil unserer Arbeit, möglicherweise der wichtigste, Aufklärungsarbeit über Technik, Digitalisierung, Urheberrecht, und Datenschutz zu leisten." Wenn der Name einer Gruppe jedoch fast immer nur im Kontext negativer Nachrichten auftaucht, riskiert dieser bittere Beigeschmack manchmal, auf die Beteiligten abzufärben. Es hilft nicht, dass der Begriff des „Hackers" kulturell schwer belastet, ist: Ihm hängt, je nach Umstand, etwas spitzbubenhaftes bis durch und durch kriminelles an."

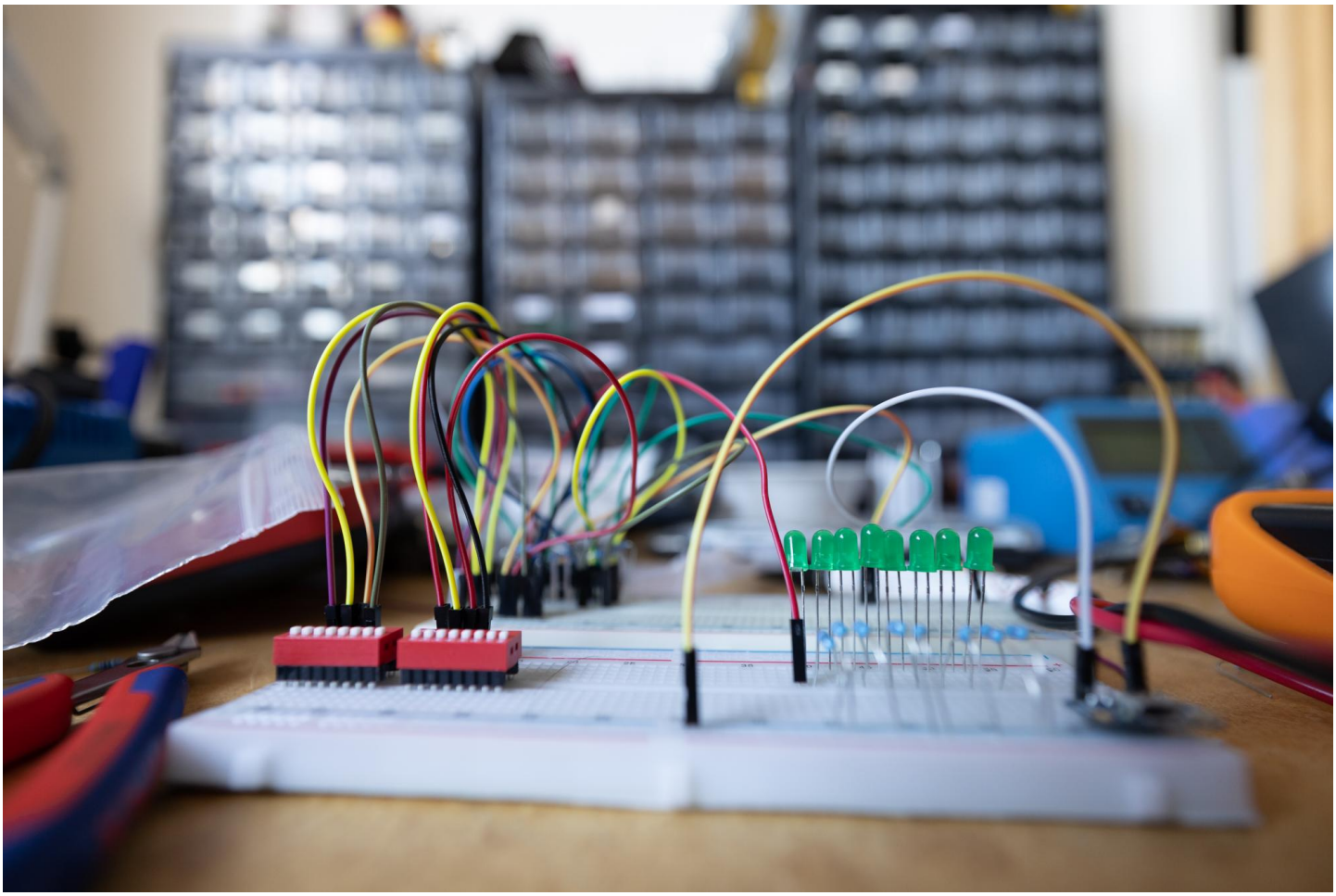
Dennis Fink

„Immer, wenn in der Presse von einem Hacker-Angriff geredet wird“, bedauert Fink, „sprechen sie über das was wir ‚Cracker‘ nennen. Also Personen oder Gruppen, die einen persönlichen Nutzen aus oft kriminellen Angriffen ziehen. ‚Blackhats‘, wie viele sie nennen.“ Dies ist eine Referenz auf klassische Western-Filmen, in denen die Bösewichte meist schwarze Cowboy-Hüte trugen, und die Helden weiße. „Nun sind wir nicht ganz ‚Whitehats‘, also jene IT-Experten, die beispielsweise für Sicherheitsfirmen oder den Staat arbeiten – sondern, eher „Greyhats“, wir haben also eine kritische Haltung gegenüber dem Staat, während wir uns für die Rechte der Leute einsetzen.“

Umfunktioniert

Die Öffentlichkeitsarbeit ist sicherlich der prominenteste Teil des Vereines, aber er ist nur einer von vielen, weniger Schlagzeilen-erhaschenden. Die Mitglieder des C3L sind „Hacker*innen“ im klassischen Sinne: Sie sind Bastler*innen. Die ersten selbsternannten Hacker*innen waren die Studentierende im „Tech Model Railroad Club“ am MIT (Massachusetts Institute of Technology). Der Name ist keine clevere Coverstory, um schattige Aktionen in einem Clubraum zu decken. Nein, die Gruppe war eine Ansammlung von Miniatur-Eisenbahn-Liebhaber*innen, die ihr Hobby nach und

nach mit „Hacks“ ausbauten, also technischen Lösungen für Schwierigkeiten, die sie beim Herumbasteln hatten.



Der C3L, wie alle Chaos Computer Clubs, führt diese Tradition fort. Wer Technik für etwas einsetzt, für das sie eigentlich nicht gedacht ist, hackt. „In dem Sinne sind wir eindeutig Hacker. Das beste Beispiel ist ein Entfeuchter in unserem Atelier, der für die Herstellung von Beef Jerky gedacht ist. Wir benutzen ihn, um das Material trocken zu halten, das wir für den 3D-Drucker brauchen. Es reagierte auf hohe Feuchtigkeit, also brauchten wir eine Lösung. Einen Hack.“

Genau wie im Tech Model Railroad Club, der sich schrittweise mehr Richtung IT entwickelt hat, um die eigenen Modelle weiter zu automatisieren, kann im C3L jede*r über seine Interessen reden. „Das geht von der Frage, wie ich Chilis am besten anbaue – das war ein größeres Projekt – über ein Rollbrett, das wir mit den Teilen eines Hoverboards so umgebaut haben, dass wir es fernsteuern können, bis hin zu den nerdigsten Diskussionsrunden über Parameter in Verschlüsselungsalgorythmen“, erklärt Fink. Für viele ist die Frage nach IT-Sicherheit und Datenschutz jedoch der Kern des C3L.

„Über allem steht, neben der Hackerethik, eine ‚Regel': Be excellent to each other. Unser gemeinsames Ziel ist es, der Gesellschaft zu helfen, uns für Informationsfreit einzusetzen und private Daten zu schützen." Ein Stichmoment für die Zusammenarbeit mit den öffentlichen Akteuren waren laut Fink zwei Videokonferenzen mit Parteien, in der die Gruppe Ihre Meinung zur geplanten Copyright-Reform teilen konnte. „Mehrere Abgeordnete haben vorher schon auf unsere Presseschreiben hin Parlamentarische Anfragen gestellt, aber wir hoffen natürlich, dass diese Entwicklung Richtung Dialog weitergeht. Bei der Copyright-Reform zum Beispiel sieht es, soweit ich weiß, im Moment aus, als ob unser Feedback zu keiner Änderung geführt hat. In viele der Abschnitte ist in meinen Augen nicht sehr viel Gehirnschmalz geflossen."

„Du würdest ja auch keinem Fremden deine Kreditkarte geben."

Dennis Fink, C3L

Eine andere Entwicklung, die der C3L mit kritischem Auge beobachtet, ist die schnelle Entwicklung biometrischer Datenerfassung und -erkennung. Auf EU-Ebene wird ein Verbot von Technologien, die Menschen unter anderem am Gang, an ihrer Körperhaltung, ihrem Tipp-Verhalten oder per Gesichtserkennung identifizieren könnte, bereits länger diskutiert. Eine endgültige Entscheidung über weiteres Vorgehen wurde jedoch noch nicht gefällt. „Wir sehen die Tendenz, dass solche Systeme auch in Überwachungskameras eingebaut werden können und werden. Bewegungsprofile werden noch besser erkannt werden können, in zwei, drei Jahren wird es wohl möglich sein, Emotionen zu erfassen. Gleichzeitig sehen wir, dass auch hier überall Kameras hin gekleistert werden …“

Vernetzt

Das ewige Argument, wer nichts falsche mache, habe auch nichts zu befürchten, lässt Fink mit einem Schmunzeln nicht gelten. Weil Verfechter für Datenschutz die gleiche alte Leier schon zu oft gehört haben, haben sie auch gleich eine Antwort parat: „Du schließt ja auch das Klo, wenn du zuhause auf die Toilette gehst. Das ist natürlich etwas salopp, also anders: Du würdest ja auch keinem Fremden deine Kreditkarte geben.“ Daten über Menschen haben, verleihe Macht, nicht umsonst ist der Markt um Konsumentenverhalten spätestens seit dem Eindringen sozialer Medien in jeden Lebensabschnitt zu einem der wichtigsten Handelsbereiche geworden: Es ist das Geschäft von Facebook und Google, den Titanen der digitalen Revolution. Und zunehmend ein Werkzeug sozialer Kontrolle.

„Warum sollte ein Staat dürfen, was andere nicht dürfen?“, fragt Fink. „Viele Leute wissen nicht, was Privatsphäre uns und der ganzen Menschheit jeden Tag bringt. Sie erlaubt uns, uns zu entfalten, zu sein wer wir sind. Beispiel Depression. Nicht jeder muss wissen, wenn jemand eine psychische Belastung hat. Weder der Staat noch die Krankenkasse.“ Dass Kosten für Versicherungen zum Beispiel steigen, „weil jeder alles über dich weiß, finden wir, muss nicht sein.“

Selbst wer den großen Datensammlern blind vertraut, staatlich oder privat, tut gut daran zu hoffen, dass seine Informationen nicht in falsche Hände geraten. Wie zum Beispiel während einer Reihe an Ransomware-Attacken auf Krankenhäuser in den USA. Cracker haben deren Computersysteme teils tagelang gesperrt, die nicht nur die Behandlung vieler Patient*innen verzögert, sondern auch laut Pressesprecher*innen der betroffenen Krankenhäuser die Sterberate während der Zeit deutlich stiegen lies.

Ermittler vermuten russische Banden mit staatlicher Unterstützung hinter dem Angriff, der nicht der einzige bleiben sollte: Ähnliche Angriffe legten am 7. Mai 2021 eine die

Colonial-Pipeline lahm, wenig später am 1. Juni dann den in den USA größten Fleischprodukt-Verarbeiter JBS.

Ein Klick?

„Weißt du, dass jeder Stromzähler in Luxemburg und die meisten in Europa mit dem Internet verbunden sind? ‚Smartmeter'." Fink zieht die Augenbrauen hoch. „Die sind natürlich supercool. Man kann ablesen, wie viel man wann verbraucht, sie können in Smartgrids integriert werden, die das Stromnetzwerk stabiler machen. Nur haben sie leider einen Haken. Der Betreiber kann sie einfach so", er schnippt mit den Fingern, „auf Distanz abstellen. Das macht er normalerweise natürlich nicht. Aber da sie mit dem Internet verbunden sind, ist das Internet auch mit ihnen verbunden. Es muss nur eine einzige Person eine Sicherheitslücke finden, um ganz Luxemburg den Strom abzudrehen, wenn ihr danach ist", gibt der C3L zu bedenken.

„Warum können diese Netzwerke nicht an einem anderen Netz hängen? Auch in den Krankenhäusern. Warum müssen diese Computer alle mit dem Internet verbunden sein? Bei einiger Infrastruktur ist es natürlich nötig, aber immer bei aller? Warum kein Intranet anlegen? Oder, wie wir hier manchmal scherzend sagen, ein ‚Luxembourg-net'? Natürlich wäre es teurer, aber lieber das, als mit der Angst zu leben, dass eine Person das Stromnetz in ganz Europa sabotieren kann."

Das Konzept der Datensparsamkeit ist für IT-Sicherheit zentral und sollte, meint Fink, auch mehr eingefordert werden. Eine der zentralen Fragen bei den Chamber-Leaks war, warum die sensitiven Daten überhaupt auf einem öffentlich zugänglichen Server lagen, sagt Fink: „Auf einem Server der mit dem Internet verbunden ist, sollten nur die Daten liegen, die nötig sind.“ Sobald etwas auf dem Internet ist, wird es nicht mehr vergessen. „Darum sehen wir jede dieser Situationen wie eine kleine Schlacht, in der wir versuchen, Entscheidungen, die wir als problematisch ansehen, entgegenzuwirken. Manche Kämpfe gewinnen wir, manche verlieren wir“.

Solange es Interessengruppen gibt, die versuchen Privatsphäre einzuschränken, Backdoors offen zu halten und Internetbenutzer*innen potenziell gefährliche Technologien aufzuzwingen, werden die Hacker*innen einen Blick auf die Entwicklungen behalten. Und zwischendurch darüber reden, wie sie Chilis am besten bewässern.