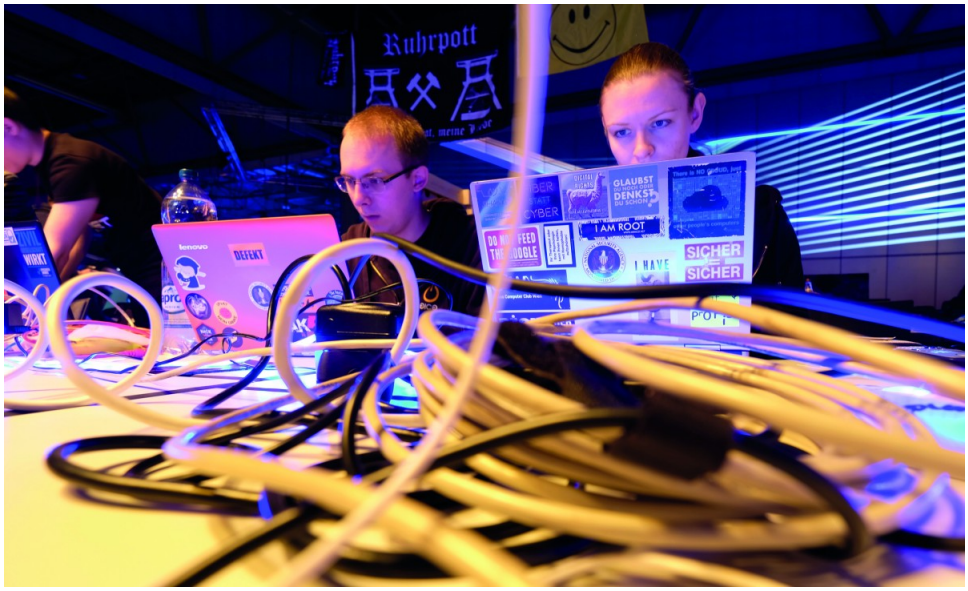
Tageblatt
LËTZEBUERG

TECHNOLOGIE



Der Strom der anderen

28. Dezember 2017. 21:00 Uhr - Akt: 28. Dezember 2017. 21:08 Uhr

Lucien Montebrusco

Das Mekka der Hacker ist neuerdings in Leipzig. Rund 15.000 Technikliebhaber nehmen bis Samstag am Chaos Communication Congress 34C3 teil.

Das Ziel der jährlichen Treffen ist ein edles: Technologien hinterfragen, Persönlichkeitsrechte des Einzelnen schützen, ihn vor Missbrauch seiner Daten bewahren. Das sind die Fragen, die seit Mittwoch bis einschließlich Samstag in Leipzig auf Einladung des Chaos Computer Club (CCC) diskutiert werden. In den letzten Jahren fand das Treffen im Hamburger Congress Center statt. Angesichts des wachsenden Erfolgs des Hackerconvents wurde das sanierungsbedürftige Gebäude in Hamburg zu klein. Also zog man in die sächsische Hauptstadt um.

Der 2008 gegründete „Chaos Computer Club Lëtzebuerg" (C3L) ist mit gleich sechs Mitgliedern nach Leipzig gereist. Normal, schließlich ist der deutsche C3 die Mutter der Luxemburger Hackervereinigung, sagt Sam Grüneisen, Pressesprecher von C3L. Außerdem sei der Chaos Communication Congress das größte derartige Event Europas – wenn nicht sogar weltweit, so Grüneisen dem *Tageblatt* gegenüber.

Das besondere Interesse der Luxemburger weckte am ersten Konferenztag eine Veranstaltung zur Sicherheit von Ladestationen für Elektroautos in Deutschland. Mathias Dalheimer vom Fraunhofer-Institut für Techno- und Wirtschaftsmathematik (ITWM) in Kaiserslautern hatte den Chip auf den Ladekarten und die darauf gespeicherten Daten analysiert. Das System sei total unsicher, meint Grüneisen.

Tanken kann der Besitzer eines E-Wagens, indem er seine Karte an die Ladestation hält. Doch die darauf gespeicherten Daten könnten problemlos herausgelesen werden. Die Identifikationsnummer könne ohne Weiteres auf eine andere unbeschriebene Karte übertragen werden, sodass sich eine Drittperson dank der gestohlenen Daten an der Stromladestation bedienen kann. Als äußerst anfällig erwiesen sich die Zapfsäulen selbst. So könnte man sich sehr leicht Zugang zu den Steuerelementen verschaffen und mithilfe eines USB-Sticks andere Daten ins System laden. Die Folgen könnten dramatisch sein. Dabei wäre das Aufladen eines E-Wagens auf Kosten des Stromlieferanten noch die kleinste Panne. Tatsächlich könnte das gesamte Ladesystem lahmgelegt werden, sagt Grüneisen. Das alles seien Kinderkrankheiten einer neuen Technologie, meint der Pressesprecher von C3L.

Auswirkungen der Digitalisierung

Doch sie zeugten davon, dass eine Technologie bereits in Betrieb genommen werde, noch ehe sämtliche Sicherheitstests absolviert wurden. Eines des ersten Anliegen des 1981 gegründeten CCC war stets, auf die Auswirkungen der Digitalisierung und deren fehlerhafte Umsetzung hinzuweisen.

In Luxemburg sind andere Ladestationen eingerichtet worden bzw. vorgesehen. Die wollen die Hacker von C3L, sobald man wieder in Luxemburg sei, testen. Inspiration für weitere Projekte gab es auch bereits. Doch darüber wollte Grüneisen keine Details geben. Die Zurückhaltung wich jedoch bei der Schilderung erster Eindrücke über das Event. Ein Riesending, allein von der Fläche, die für das Treffen bereitgestellt wird. So etwas könnte man in Luxemburg nicht organisieren, meint Grüneisen.

Insbesondere angetan hat es ihm die Halle, die dem Hardware-Hacking gewidmet ist. Darunter versteht man die Modifizierung von Hardware, um sie für andere Zwecke als vom Hersteller vorgesehen nutzen zu können oder ihr neue Funktionalitäten zu verleihen. Grüneisen spricht von sehr vielen „kreativen Sachen“, die da zu bestaunen sind. Er sieht darin auch eine Rückbesinnung auf die Ursprünge der Bewegung. Deren Gründer hatten nicht mehr und nicht weniger als einen „Neustart der Gesellschaft“ im Sinn.

Das 34C3-Motto „tuwat“ selbst soll an die Ursprünge des CCC erinnern. „Tuwat.txt“ (tu was) lautete der Titel eines 1981 in der Berliner Tageszeitung veröffentlichen Aufrufs, in den Redaktionsräumen der Zeitung über den „Komputereinsatz“ zu diskutieren. Mit dem Aufruf des tuwat.txt begann die Geschichte des Chaos Computer Club.

KI besser kontrollieren

Netzaktivist Markus Beckedahl hat beim 34C3 vor Risiken im Umgang mit Algorithmen gewarnt und eine bessere Kontrolle der Künstlichen Intelligenz (KI) gefordert.
„Wir brauchen Regularien, um zu schauen, wie kriegen wir eine Nachvollziehbarkeit und eine demokratische Kontrolle von dem hin, wie Algorithmen eingesetzt werden“, sagte der Gründer des Blogs Netzpolitik.org.

Das Thema Künstliche Intelligenz habe neue Dimensionen erreicht. So gebe es Durchbrüche im maschinellen Lernen oder neue Daten- und Analysekapazitäten. Zugleich würden Algorithmen häufig in sensiblen Bereichen eingesetzt, etwa bei der Kreditvergabe oder im Gesundheitsbereich. „Gesundheitsalgorithmen muss man anders regulieren als Facebook-Algorithmen.“

Beckedahl warnte vor der zunehmenden Macht der KI-Technologie und forderte mehr Transparenz für die Gesellschaft. Um Unternehmen besser zu kontrollieren, sollten Geschäftsgeheimnisse aufgelockert werden. Auch müsse es neue Kontrollinstitutionen geben, „irgendwo zwischen Datenschutzbehörden und Kartellämtern“.
Der Begriff Algorithmus umschreibt eine Folge von Anweisungen, etwa in einer Software, mit denen ein bestimmtes Problem gelöst werden kann. (dpa)

Online-Banking

Die zunehmende Benutzerfreundlichkeit beim Online-Banking mit dem Smartphone geht nach Überzeugung von Informatikern der Uni Erlangen-Nürnberg zwangsläufig auf Kosten der Sicherheit. Der Trend zur Nutzung von Online-Banking mit nur einer App berge die Gefahr von Betrug und Manipulationen etwa bei Überweisungen, warnte Vincent Taupert auf dem Kongress des „Chaos Computer Club“. Sicherer sei die Zwei-Geräte-Authentifizierung mit einer getrennten Übermittlung der TAN-Daten (Transaktionsnummer, ein Einmalkennwort aus sechs Dezimalziffern).

Saugroboter

Die Sicherheitsexperten Dennis Giese und Daniel Wegemer haben am Mittwoch auf der 34C3 dargelegt, wie sie sich Zugang zum Steuerungssoftware eines handelsüblichen Saugroboters chinesischer Produktion verschafft haben. Dem Nachrichtenportal heise.de fanden sie auch heraus, „welche Daten das Gerät lokal und in der Cloud speichert“. Ziel war es, den Roboter mit Administratorrechten vollständig selbst beherrschen und in Eigenregie nutzen zu können. heise.de zufolge sei es den zwei Experten nach fünf bis zehn Minuten gelungen, sich in das System einzuloggen, eigene Software zu installieren oder die Sensoren zu nutzen. „Die Tüftler rieten Nutzern ‘smarter’ Gegenstände, diese möglichst nicht im vom Hersteller bereitgestellten Zustand unkontrolliert zu verwenden. Hacker könnten darauf Schadcodes installieren und im Fall des Saugroboters etwa Wohnungen ausspähen“, so heise.de.