24C3: Spontandemo gegen Überwachung und Vorratsdatenspeicherung

Volldampf Richtung 1984

Christoph Puppe

Die Sorge um den Verlust von Bürgerrechten und des letzten Rests an Privatsphäre trieb rund 1000 Hacker auf den Berliner Alexanderplatz. Dort demonstrierten die sich traditionell zum Jahresende versammelnden Teilnehmer des Chaos Communication Congress gegen die nun endgültig abgesegnete Vorratsdatenspeicherung.

Mit einer spontaner Demonstration gegen Vorratsdatenspeicherung mit dem Slogan „Guten Rutsch ins Jahr 1984“ setzten die Teilnehmer des traditionell zum Jahresende stattfindenden Chaos Communication Congress einen starken Akzent gegen den Abbau von Privatsphäre und die Einschränkung des Rechts auf informationelle Selbstbestimmung.

Den über 4000 Besuchern bot sich im schon bekannten Berliner Congress Center eine abwechslungsreiche Zeit mit den fast sämtlich auf Englisch gehaltenen Vorträgen sowie stolzen 25 wissensvermittelnden Workshops. Die 100 Vorträge verteilten sich thematisch auf die Kategorien „Society“, „Culture“ und „Hacking“. Der neu hinzugekommene Track „Making“ steht in der Tradition des Magazins „Make“ aus dem O’Reilly-Verlag und widmet sich dem Selbstbasteln von Dingen, grob gesagt.

Kampfstricker am Werk

Themen dieses Tracks waren unter anderem die freie Geodatenbank OpenStreetMap, wie man einen Roboter-Aufstand überlebt, selbstgebaute Drohnen und das in Hackerkreisen wundersamerweise so beliebte Stricken – Letzteres mit dem vielversprechenden Titel „The history of guerilla knitting“. Martin Müller und Antoine Drouin boten mit ihrem Vortrag „Paparazzi – The Free Autopilot“ einen Einblick in eine Open-Source-Entwicklung eines autonom fliegenden Modellflugzeugs. Der beeindruckende Film der im Flugzeug angebrachten Kamera zusammen mit den Details des Projektverlaufs und der GPS-basierten Steuerung begeisterte die Zuschauer. Der Track „Science“ bot thematisch von einer Analyse ansteckender Krankheiten in World of Warcraft über die Art und Weise der DNA-Programmierung bis hin zu Verschwörungstheorien viel Überraschendes.

Mit Spannung erwarteten die Zuschauer den eher „klassischen“ Hacking-Vortrag von FX von Phenoelit zur Sicherheit von Barcodes. Nach einer Einführung zu Geschichte und Einsatzzweck des Barcodes – etwa für IDs, Tags, Datentransport oder „GGU“ (ganz grober Unfug) – erläuterte er, was man mit manipulierten Scannern oder Barcodes anstellen kann: einen Badge, der als Zahlungsmittel an der Bar gilt, mehrfach kopieren, ein temporär gültiges Parkticket in einer Dresdener Hotelgarage in ein unbegrenzt gültiges für kostenloses Parken umwandeln oder auch Schummeleien mit Pfandsystemen. Summa summarum weisen alle gängigen Barcode-Systeme gravierende Sicherheitsmängel auf.

Luke Jennings führte einen von ihm selbst entwickelten Angriff gegen unter Windows gespeicherte Zugangs-Token vor. Mit seiner Software lassen sich die Access-Token der Domänen-Administratoren dazu benutzen, sämtliche Aktionen in einer Windows-Domain auszuführen, die sonst dieser Gruppe vorbehalten sind. Ein Domänen-Admin muss sich nur einmal seit dem letzten Booten in den vom Angreifer übernommenen PC eingeloggt haben, damit dies möglich wird. Jennings hat das notwendige Werkzeug auf Sourceforge veröffentlicht.

Unsichere Steuerungsprozesse

Der jüngste Vortragende war auch gleichzeitig der am weitesten gereiste, der 17-Jährige kuza55 war aus Australien nach Berlin gekommen, um einen Vortrag über Tricks beim Hacken von Webapplikationen zu halten. Weitere Beiträge behandelten Unsicherheiten bei Oracle, das Sniffen von 10-Gigabit-Ethernet, zielgerichtete Angriffe mit Malware, den Storm Worm, das Cracken von Sonys Playstation Portable sowie das Hacken von SCADA. SCADA ist kein Betriebssystem, das keiner kennt, sondern die Abkürzung für „Supervisory Control and Data Acquisition“, sprich die Steuerung von Prozessen in der Industrie, von Fließbändern, über Öl-Förderungsanlagen bis hin zu Kraftwerken. Mayhem und Raoul „Nobody“ Chiesa zeigten erfolgreiche Angriffe gegen solche Anlagen und konnten überzeugend darstellen, dass sie ziemlich einfach durchzuführen sind.

Der zur Tradition gehörende Vortrag „Security Nightmares“ von Ron und Frank Rieger über die wichtigsten Sicherheitsprobleme und „worüber wir nächstes Jahr lachen werden“ bot am letzten Tag einen gewohnt heiteren Abschluss dieses Tracks. 2007 brachte beispielsweise den Superwurm in Form des kombinierten Schadprogramms „Storm Worm“ und weitere Malware mit auffälligen Schadroutinen. Fürs kommende Jahr rechnen die Hacker mit einer Zunahme von Schadcode für iPhone & Co. sowie einem verstärkten Handel mit Exploits.

Im Track „Society“ war das Unwort des Jahres 2007 „Bundestrojaner“, auch Thema eines Vortrags von Andreas Bogk, Constanze Kurz und Felix von Leitner. Unter der Überschrift „Die Wahrheit haben wir auch nicht, aber gute Mythen“ boten sie einen Überblick und reichlich Details zu den technischen und gesellschaftlichen Diskussionen. Lesenswert dazu ist auch das Buch „1984.exe“ von Constanze Kurz. Die zahlreichen weiteren Überwachungs- und Datensammelprojekte der Bundesregierung, aber auch der EU – Stichworte Vorrats- und Flugdatenspeicherung, RFID, Copyrightverschärfung – trugen dazu bei, dass es diesem Track nicht an Vorträgen mangelte.

Der CCC wäre jedoch nicht er selbst, wenn nicht auch Gegenmaßnahmen zur Sprache kämen – etwa in den Vorträgen „23 Wege, für Deine Rechte zu kämpfen“ und „Distributed campaigns for promoting and defending freedom in digital societies“. Und den Erfolg seines gesellschaftspolitischen Engagements hat der Club im vergangenen Jahr mit seiner Kampagne gegen die umstrittenen, weil unsicheren Wahlcomputer hinreichend bewiesen. (ur)

Onlinequellen

Kongress-Homepage	events.ccc.de/congress/2007/Main_Page
Mitschnitte der 24C3-Beiträge	events.ccc.de/congress/2007/Conference_Recordings
Magazin „Make	makezine.com/magazine
Freie Geodatenbank:	www.openstreetmap.de
Phenoelit:	www.phenoelit-us.org
Tool zur Manipulation von Windows-Zugangs-Token:	sourceforge.net/projects/incognito
Constanze Kurz, 1984.exe	www.transcript-verlag.de/ts766/ts766.htm