CCC-Jubiläumskongress: NSA und kein Ende

Chaos als Programm

Christoph Puppe

Mit dem 30C3 feierte der Chaos Computer Club das Jubiläum einer Veranstaltung, die sich in dieser Zeit stark gewandelt hat. Rund 8000 Besucher aus aller Welt kamen nach Hamburg, um sich mit Überwachung und Whistleblowing sowie weiteren zeitgemäßen Sicherheitsthemen auseinanderzusetzen.

Was vor 30 Jahren mit wenigen Hundert Teilnehmern im Eidelstädter Bürgerhaus als Treffen von Hackern begann, ist heute eine international beachtete Instanz. Wegen Platzmangels zog der „Chaos Communication Congress“ Ende der 90er-Jahre nach Berlin um und findet nun, nachdem auch hier notorischer Platzmangel und Eintrittskartenverlosungen für Unmut sorgten, seit dem letzten Jahr im Hamburger Congress Center statt. Dieses ist groß genug, den ständig seine eigenen Besucherrekorde brechenden Kongress zu beherbergen.

Nicht nur der Austragungsort, auch die behandelten Themen sowie die Ausrichtung änderten sich im Laufe der Jahre. Eine ähnliche Entwicklung wie der Chaos Computer Club selbst, der sich von einer Vereinigung der Hacker, die teilweise in den Grauzonen der Legalität operieren, zu einem Think Tank freiheitlich orientierter Internetbewohner wandelte, nahm auch der Kongress: Wo früher der kreative Umgang mit der eigenen oder anderer Leute Technik das Vortragsprogramm eindeutig dominierte, sind nun politische Themen in den Vordergrund gerückt.

NSA, Snowden und Whistleblower

Das Thema, das dieses Jahr erwartungsgemäß das Programm bestimmte, waren die Enthüllungen von Edward Snowden zu den Machenschaften der NSA. Der ehemalige The-Guardian-Autor Glenn Greenwald, der als enger Vertrauter von Snowden mit diesem zusammen die Veröffentlichung der Dokumente koordinierte, hielt die Keynote. Neben der Danksagung an Snowden bedachte er auch die Whistleblower, die ihm vorangingen, besonders hier Chelsea Manning (vormals Bradley Manning) und Wikileaks. Nicht erwähnt wurde leider Cryptome, die erste Enthüllungsplattform dieser Art, die sich schon in den 90er-Jahren für Informations- und Meinungsfreiheit einsetzte und ihren Beitrag zur Kultur der Veröffentlichung von Dokumenten leistete.

Außer der Keynote riefen zwei weitere Vorträge ein starkes internationales Echo hervor. So kündigte Annie Machon, eine ehemaligen Mitarbeiterin des MI5, einen Hilfsfonds für Whistleblower an, und Jacob Appelbaum präsentierte neue Erkenntnisse über die NSA und deren Zugriff auf iPhones. Das Injizieren von schädlichem Code per Funk über eine Entfernung von mehreren Kilometern sowie das Ausspähen von Bildschirm- und Tastaturinformationen per Radar waren nur zwei der vorgestellten Angriffsmethoden.

Mit den Auswirkungen der veröffentlichten Dokumente auf unser heutiges Verständnis von Sicherheit bei Verschlüsselung beschäftigte sich der Vortrag des bekannten deutschen Kryptologen Rüdiger Weiß. Er fasste die Erkenntnisse gewohnt unterhaltsam zusammen und kam zu dem Schluss, dass gute Verschlüsselung auch weiterhin ein wirksamer Schutz vor staatlichen und anderen Lauschern ist. Neben den aktuellen Fragen warf der Beitrag von Josef Foschepoth, dem Autor von „Überwachtes Deutschland“, ein Schlaglicht auf die Geschichte der Überwachung in Deutschland seit dem zweiten Weltkrieg. Dass der vor Kurzem aus dem Amt geschiedene ehemals oberste Datenschützer Deutschlands, Peter Schaar, einen Vortrag über die Rolle und die Möglichkeiten des Datenschutzes hielt, ist wie viele andere Beiträge ein Zeichen, dass der Chaos Communication Congress sich zu einer selbst von der Politik ernst genommenen Plattform entwickelt hat.

Einige Beiträge thematisierten die technischen Aspekte der mangelnden Sicherheit von Netzen. Wie man Buffer-Overflows und andere Fallstricke der hardwarenahen Programmierung umgeht oder es zumindest mehr oder weniger erfolglos versucht, referierte Andreas Bogk vom Berliner CCC.

Der Router als Überwachungsindikator

Der bekannte Hacker FX of Phenoelit zeigte interessante Auswirkungen von Überwachungsschnittstellen auf die Sicherheit von Routern. So kann ein einziges ICMP-Paket einen Router von Cisco mit einer nicht dokumentierten Funktion für das Ausleiten von Daten zwecks Überwachung zum Absturz bringen. Wer also testen möchte, ob auf dem Übertragungsweg mitgehört wird, kann durch das Senden dieses Paketes das Routing verändern und daran erkennen, dass der eben ausgefallene Router von staatlicher Überwachung betroffen war.

Erneut auf dem 30C3 zu hören war das Thema Industrie 4.0. Das Team Gleb Gritsai und Sergey Gordeychik zeigte aktuelle Bedrohungen für Anlagen zur Industriesteuerung. Dazu Schwächen in Protokollen, die bei ihrem Design von hermetisch geschlossenen Umgebungen ausgingen und daher keine oder nur rudimentäre Sicherheitsfunktionen aufweisen, sowie sicherheitsrelevante Bugs.

Kunst, Kultur und Kinder

Wie seit den Berliner Tagen des Kongresses üblich, geizte auch der 30C3 nicht mit Kunst und Kultur. Neben der liebevoll eingerichteten Lounge mit bekannten DJs und einigen eher unbekannten Klang-Künstlern zeigte eine Theatergruppe ihr „Nö!“ zum Verfassungsschutz. Überdies waren in den Gängen und im Hackcenter viele kleinere und größere Projekte zu sehen, die 3D-Drucker, Plotter, Laser und Leuchtdioden in Installationen nutzten. Zusammen mit dem Kinderbereich, der dieses Jahr einen eigenen Workshoptag anbot und das Projekt „Chaos macht Schule“ des CCC präsentierte, ergab sich ein für alle Beteiligten bunter und lebhafter Kongress. Die Videos der Vorträge sind im Internet nachzuschauen (s. „Alle Links“). (ur)

So bunt wie der Veranstaltungsort gestaltete sich der 30. Chaos Computer Congress, der sich im Lauf der Jahre eine internationale Reputation erarbeitet hat.

Alle Links: www.ix.de/ix1402010