32C3: Weniger Technik, mehr Politik

Akzentverschiebung

Christoph Puppe

Nicht nur IT-Sicherheitsaspekte standen beim diesjährigen Chaos Communication Congress im Mittelpunkt. Der in den letzten Jahren begonnene Trend zu mehr politischen Themen und Einordnungen setzte sich fort.

Wie an jedem Jahresende trafen sich zwischen den Feiertagen Hacker, Maker und nichttechnikbezogene Aktivisten beim Chaos Communication Congress unter dem Motto „Gated Communities“. Diese stehen in der etwas provokanten Interpretation der Veranstalter für abgeschottete Bereiche – „schwer bewachte Inseln der Bequemlichkeit“ –, in denen die Bevölkerung sich zwar sicher fühlt, im Gegenzug aber nicht mehr selbst denken und bestimmen kann (und will).

Zwischen den IT-Sicherheitsthemen fanden sich viele Vorträge über globale Erwärmung, Flüchtlinge sowie die politischen Aspekte von Verschlüsselung und genereller IT-Sicherheit. Ein Zeichen für den deutlich weniger technischen Fokus setzte bereits die Eröffnungsrede der somalischen Menschenrechtlerin Fatuma Musa Afrah, die als Flüchtling nach Deutschland kam und die IT-Experten dazu aufforderte, auch die Welt um sich herum wahrzunehmen.

Wie schon die drei Veranstaltungsräume vorheriger CCC-Kongresse ist auch die aktuelle Heimat, das Congress Center Hamburg (CCH), zu klein. Alle 12 500 Karten wurden bereits Monate im Voraus bestellt und die Tagestickets waren spätestens eine Stunde nach Öffnung der Kassen ausverkauft. Wo ab 2017 der Kongress stattfinden kann, ist damit eine ungeklärte Frage, da das CCH, das dann saniert wird, das größte deutsche Konferenzzentrum ist und seit der Schließung des ICC keine weitere Option existiert.

Unsichere Kreditkarten-Terminals

Ein Highlight der Veranstaltung wurde bereits im Vorfeld bekannt. Der GSM-Spezialist Karsten Nohl hatte auch in diesem Jahr wieder ein Forschungsergebnis zu präsentieren, das alle betrifft. Nach der Verschlüsselung und dem Abhören von GSM hat er sich nun EC-Karten-Terminals zugewandt. Im Vortrag „Shopshifting“ zeigte er mit seinen Kollegen Fabian Bräunlein und dexter einen Angriff auf ein Hardware Security Module (HSM), das die Prüfsumme einer Zahlungsanfrage kontrolliert. Da das HSM jede Stelle einzeln prüft und ein Zeitunterschied bei richtiger und falscher Anfrage besteht, muss der Angreifer also nur jede Stelle einzeln ausprobieren. Er kann so in wenigen Versuchen die richtige Prüfziffer herausfinden und die Nachrichten zwischen den Terminals verändern. Fünf Millisekunden Differenz reichen dazu bereits aus.

Der Angriff geht damit gegen eine Implementierung des Protokolls. Da aber immer eine symmetrische Verschlüsselung im Einsatz ist, ist der Angriff auch gegen andere Terminals als das benutzte denkbar. In einem zweiten Angriff über einen „Man in the Middle“ zeigten sie im Vortrag, wie einfach die PIN des Kunden auszulesen ist und man sich Geld überweisen kann. Um diese Angriffe zu verhindern, müssten in Deutschland über eine halbe Million Terminals ausgetauscht werden.

Für Aufregung hatte im Herbst 2015 ein Urteil des Europäischen Gerichtshofs (EuGH) gesorgt. Die Richter erklärten das Safe-Harbor-System zum Schutz personenbezogener Daten im EU-Ausland für ungültig, da es gegen unveräußerliche Grundrechte der EU-Bürger verstößt. Das Urteil des EuGH für diesen Fall erging überraschend schnell und eindeutig. Max Schrems berichtete über den Weg seiner Klage gegen Facebook und es gab mehrfachen Zwischenapplaus für pikante Details.

Unter anderem zeigte er eine Statistik der mit 20 Personen besetzten Dienststelle des irischen Datenschutzbeauftragten. Im Schnitt beantwortete sie circa 3 % aller Anfragen, obwohl es eigentlich 100 % sein müssten. Denn das Gesetz schreibt vor, dass jeder Vorgang bearbeitet werden muss. Der Datenschutzbeauftragte erklärte das unter anderem damit, dass keiner der Mitarbeiter Jurist oder IT-Experte sei. Dies ist insofern brisant, als die großen, zumeist ausländischen Cloud- und Social-Network-Anbieter ihren Sitz in Irland haben und somit der dortige Datenschutzbeauftragte für sämtliche diese Firmen betreffenden Vorgänge zuständig ist.

Quelle: Sascha Ludwig

Aus CCH wird CCC – diese Verwandlung der Initialen für die Dauer des Kongresses hat Tradition (Abb. 1).

Eine zweite Spiegel-Affäre?

Noch gibt es keine Lösung für einen legalen Datentransfer, aber die Verantwortlichen arbeiten unter Hochdruck an einer Nachfolgeregelung zu Safe Harbor. Verurteilungen wegen Verstoßes gegen Datenschutzgesetze wurden seit diesem obersten Richterspruch keine bekannt.

Auch die Ermittlungen der deutschen Staatsanwaltschaft gegen die beiden Journalisten von netzpolitik.org und der NSA-Untersuchungsausschuss waren mehrfach angesprochene Themen. Markus Beckedahl war einer der des Landesverrats Angeklagten und präsentierte diesen Fall, der kurze Zeit nach Bekanntwerden bis auf den Tisch des Innenministers und der Kanzlerin gelangte. Die Frage, wer ab wann wusste, dass ein Journalist angeklagt ist, wurde wohl nicht abschließend geklärt.

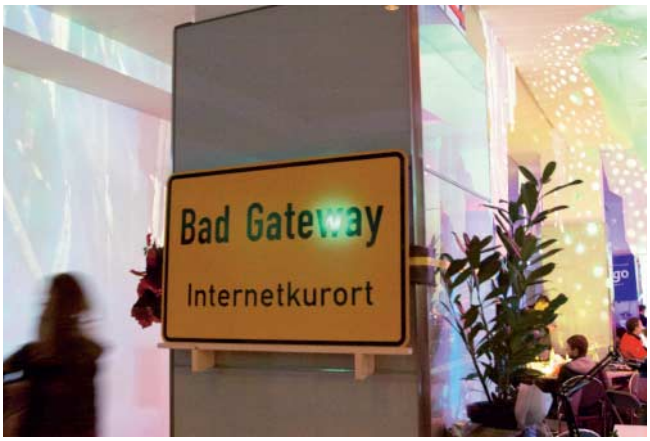
Im Kontext des vom Bundesgerichtshof angeordneten verbesserten Schutzes von Journalisten, der vor kaum einem Jahr in Kraft getreten ist, handelt es sich hierbei um einen bemerkenswerten Vorgang, der in der Größenordnung des Spiegel-Skandals mit Strauß zu sehen ist. Er wurde nach dem Rücktritt des Generalbundesanwalts innerhalb weniger Tage beendet und die Anzeige zurückgezogen. Damit kann der Vorgang nicht abschließend durch ein Gericht geklärt werden, solange niemand Anzeige gegen die Behörde erstattet.

Da nur wenige Menschen das Satellitentelefon Iridium nutzen, war die öffentliche Auf-

merksamkeit für den Vortrag von Sec und schneider im Vergleich zu dem Beitrag über das Hacken der GSM-Verschlüsselung gering. Die beiden Sicherheitsexperten zeigten ihre Erfolge beim Reverse Engineering der proprietären Funkprotokolle, die Iridium für die Übermittlung von Daten und Sprache nutzt. Mit Hardware für etwas mehr als 100 Euro lassen sich nun alle Telefonate und fast alle Pager-Nachrichten abhören, die innerhalb dieser Zelle übertragen werden. Da eine Zelle immerhin einen Radius von 400 km hat und der Angreifer nur einen Empfänger in diesem Umkreis benötigt, handelt es sich um einen praktikablen Angriff. Dass ein relativ junges Protokoll wie dieses keine Authentifizierung der Teilnehmer und keine Verschlüsselung der Inhalte vorsieht, überraschte viele.

Wie es aussieht, wenn ein totalitäres Regime die Entwicklung von Software vollständig kontrolliert, präsentierten Florian Grunow und

Quelle: Sascha Ludwig



An originellen Dekorationen mangelte es in den Veranstaltungsräumen nicht (Abb. 2).

Niklaus Schiess am Beispiel des nordkoreanischen Betriebssystems „Red Star“. Es bringt unter anderem in jede Bilddatei ein Wasserzeichen ein, das den Benutzer eindeutig identifiziert. Wer dieses Betriebssystem auf Basis von Linux nutzt, um ein Foto zu posten, ist damit sofort erkennbar und kann verfolgt werden. Dieser und andere Vorträge zeigten, wie wichtig eine offene und legale Forschung nach Sicherheitslücken und eine aktive Open-Source-Szene für die Sicherheit der Bürger ist.

Welche Entwicklung sich in der Legalität der Sicherheitsforschung gerade abzeichnet, zeigte die Podiumsdiskussion „Cyber all the Wassenaars“ mit den Sicherheitsexperten van Holst, Cardozo, mlp und Tynan. Sie beschrieben die Bestrebungen der Unterzeichnerstaaten des Wassenaar-Abkommens, den Export von Informationen zu Schwachstellen darin zu reglementieren. Dieses internationale Abkommen regelt den Export von Waffen sowie als Waffe benutzbarer Geräte und ist von fast allen Industrienationen ratifiziert. Derzeit gibt es Gespräche, Informationen zu Schwachstellen als „Cyber-Waffe“ mit in die Liste für die Exportkontrollen aufzunehmen. Dies birgt die Gefahr, dass schon ein Vortrag über eine Schwachstelle vor Studenten aus dem Ausland oder eine Mail an eine Mailingliste als Verstoß gegen Waffenexportgesetze verstanden werden könnten.

Ein Trost bleibt denjenigen, die keine Eintrittskarte mehr ergattern konnten oder den Kongress verpasst haben: Mittlerweile stehen die Videos zahlreicher Vorträge auf der Webseite des CCC zum Nachschauen bereit (https://media.ccc.de/c/32c3). (ur)