Notizen von der Sicherheitskonferenz IT-Defense

Wer vieles bringt

Namhafte Referenten und ein breit gefächerter Themenmix – das bot die IT-Sicherheitskonferenz IT-Defense, die Ende Januar/Anfang Februar in München Station machte. Jens-Christoph Brendel

Abbildung 1: Marcus J. Ranum während seines Vortrags.

Die IT-Defense hat sich einige Alleinstellungsmerkmale unter vergleichbaren Konferenzen bewahrt: Erstens finanziert sie sich ausschließlich aus dem Ticketerlös, hat also keine Sponsoren und präsentiert folglich auch keine Sponsorenvorträge, die anderswo oft in die Nähe von Werbeveranstaltungen geraten. Auch eine streng akademische Konferenz will sie nicht sein.

Zweitens will sie nicht um jeden Preis wachsen, sondern begrenzt die Teilnehmerzahl auf eben noch übersichtliche gut 200 Personen, für die sich auch in mittelgroßen Hotels noch Säle finden – das sorgt für eine familiäre Atmosphäre. Das Limit bedingt, dass jedes Jahr potenzielle Teilnehmer abgewiesen werden, wenn sie zu spät buchen. Drittens streamt sie keine Vorträge, was gerade bei ihrem Thema IT-Sicherheit manchen Referenten womöglich freier sprechen lässt. Viertens gibt es nur einen Track.

Letzteres hat Vor- und Nachteile. So verpasst niemand etwas, was in einem parallelen Vortrag behandelt würde – es können aber auch weniger Vorträge zum Zuge kommen und die müssen für jeden Geschmack etwas bieten. Das wiederum führt zu einem Gemischtwarenladen aus sehr speziellen und technisch orientierten Vorträgen und solchen, die eher strategische oder rechtliche Aspekte aufgreifen.

Dazu kommen noch die letzten Referate an beiden Veranstaltungstagen, die noch einmal aus dem Rahmen fallen, indem sie sich eher unerwarteten Themen zuwenden. Wer vieles bringt, wird manchem etwas bringen. Man darf nur keine Konferenz erwarten, auf der sich eine Spezialisierung gezielt vertiefen ließe.

Klangvolle Namen

Nicht selten waren auf der IT-Defense schon Referenten mit klangvollen Namen zu Gast, in diesem Jahr fehlten zwar die ganz großen Stars, doch einige Redner dürften zumindest Eingeweihten ein Begriff sein. So auch Mikko Hypponen vom Sicherheitsunternehmen F-Secure, der unter anderem beklagte, dass viele IoT-Geräte ausschließlich über den Preis verkauft würden, weshalb ihre Hersteller keine Sicherheitsvorkehrungen einbauten. Entsprechend unsicher sind sie. Das so genannte Hypponens Law sagt: „Whenever an application is described as ‚smart', it's vulnerable."

Auch den Namen von Paula Januszkiewicz haben sicher viele schon gehört, sie ist die Gründerin des weltweit agierenden Securityspezialisten Cqure und auf vielen Konferenzen aktiv. Sie sprach über Angriffe gegen Windows-Systeme, die vornehmlich auf menschliche Schwachstellen zielten: schwache Passwörter, nicht gelockte Desktops, scheinbar verlorene USB-Sticks, Phishing, unbeobachtete Geräte und dergleichen.

Einem strategischen Thema wandte sich der ebenfalls nicht unbekannte amerikanische Sicherheitsforscher Marcus J. Ranum (Abbildung 1) zu, auf dessen Konto etliche Innovationen bei Firewalls und Intrusion-Detection-Systemen gehen. Er verwies darauf, dass die Kostenverlagerung im Zuge des Cloud Computing die Sicherheitsprobleme nicht löse, sondern sie nur verschiebe. Gebraucht würden Datendesigner, die genau wüssten, wo welche Daten zu welchem Zweck verarbeitet würden. Künstliche Intelligenz werde das noch auf Jahre hinaus nicht leisten können.

Zu den technisch anspruchsvollen Vorträgen zählte beispielsweise der von Philipp Koppe und Benjamin Kollenda vom Horst-Görtz-Institut der Ruhr-Uni Bonn. Die Referenten erläuterten, wie sie den Microcode älterer x86-CPUs per Reverse Engineering untersucht haben, und demonstrierten, wie sich aus der Manipulation von Microcode-Updates Angriffe ableiten lassen, die schwer abzuwehren und kaum zu reparieren sind.

Ein weiterer Vortrag von Starbug, dem Biometrie-Experten des Chaos Computer Clubs, machte deutlich, dass sich viele biometrische Sensoren nach wie vor recht einfach austricksen lassen, selbst in den neuesten Smartphones von Samsung. Dafür reicht zum Beispiel eine über den Ausdruck eines Iris-Fotos gelegte Kontaktlinse – schon lässt sich die gepriesene Iris-Erkennung täuschen. ■