Jörn Müller-Quade, Kryptographie-Experte und Professor am KIT in Karlsruhe

Das K.-u.-K.-Prinzip

Sie hat Kriege entschieden und Affären verheimlicht: Die Wissenschaft der Kryptographie ist eng mit dem IT-Standort Karlsruhe verknüpft. Warum, zeigt eine Ausstellung im ZKM

Es ist ein Abend der Premieren – und der Rekorde. Zum ersten Mal seit Gründung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) vor zwölf Jahren kamen mehr als 200 Besucher zu einer Veranstaltung. In diesem Fall ins ZKM zur Eröffnung der europaweit ersten Ausstellung zum Thema Kryptographie, der Mitmach-Ausstellung Kryptologikum, das die KA-IT-Si gemeinsam mit dem ZKM sowie dem Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL) am KIT initiiert hat. Das Ziel: die Besucher mit Exponaten in die Kryptographie einführen – und ihnen das neue K.-u.-K-Prinzip näherbringen: Schließlich sind die Historie der Kryptograhie und Karlsruhe eng verbandelt. Vor 100 Jahren erfand der Karlsruher Friedrich Rehmann eine der ersten Verschlüsselungsmaschinen – und am KIT wurde vor 30 Jahren der erste Kryptographie-Lehrstuhl gegründet.

Das alles aus gutem Grund, erklärt Jörn Müller-Quade, Professor und Inhaber des Lehrstuhls für IT-Sicherheit und Leiter des Instituts für Kryptographie und Sicherheit (IKS): „Kryptographie schafft Wunder, die es ohne Kryptographie nicht gäbe." Sagte es und nahm die 200 Besucher mit auf einen Crash-Kurs in Sachen Kryptographiegeschichte.

Für die Gesellschaft, etwa im Altertum und Mittelalter, galt die Kryptographie als Blackbox, als Mysterium, das nicht zu entschlüsseln und nicht zu begreifen war. „Die Kryptographie hat Kriege entschieden, Affären verheimlicht, und ermöglicht heute Geschäfte im Internet." Doch erst im Lauf des Zweiten Weltkriegs geriet sie endgültig in den Fokus, als die Alliierten die deutsche Verschlüsselungsmaschine Enigma brachen und den Krieg so entscheidend beeinflussten. Denn dank Enigma hatten die Deutschen lange unbemerkt ihre Angriffe geplant und koordiniert. „Das war der Startschuss für die wissenschaftliche Auseinandersetzung mit der Kryptographie", so Müller-Quade.

Die wurde zudem durch den Kalten Krieg befeuert, etwa durch eine Chiffriermaschine, mit der die deutsche Botschaft in Moskau ihre Nachrichten verschlüsselte. Die Anlage galt als prinzipiell unbrechbar – bis die Russen die elektromagnetischen Impulse der Maschinen abfingen und die Nachrichten dadurch entschlüsselten. Fazit: „Absolute Sicherheit gibt es nur im Modell", so Müller-Quade. Dennoch ist die Kryptographie für die IT unverzichtbar und bildet quasi die Basis für die sichere Kommunikation zwischen IT-Geräten, eine der Kernkompetenzen auch des KA-IT-Si-Netzwerks. Eben das neue K.-u.-K.-Prinzip. ***rs***

KA-IT-Si
Karlsruher IT-Sicherheitsinitiative

Veranstaltung

„Schau mir in die Augen, Kleines", lautet das Motto der nächsten KA-IT-Si-Veranstaltung, bei der Friederike Schellhas-Mende vom Karlsruher Institut für Technologie (KIT) über die Retina-Authentisierung an Mobilgeräten berichtet.

Wo Fraunhofer IOSB, Karlsruhe
Wann 14. März 2013

Mehr Informationen unter www.ka-it-si.de

Foto: Jigal Fichtner