

Verschlüsselung VON Informationen

DARMSTADT (red). Unter dem Motto „From Tweets to Quantum“ treffen sich bis heute, Dienstag, mehr als 150 IT-Sicherheitsforscher in Darmstadt, um über die Verschlüsselung der Zukunft zu diskutieren. Sicher muss sie sein, aber auch effizient, praktikabel und benutzerfreundlich. Der Sonderforschungsbereich Crossing der TU Darmstadt hat zum zweiten Mal renommierte Experten zur Jahreskonferenz eingeladen.

Die Organisatoren der Konferenz sind Professor Johannes Buchmann und Professor Ahmad-Reza Sadeghi. Die Konferenz, so Sadeghi, sei eine Plattform für richtungsweisende Forschung im Bereich IT-Sicherheit und Privatsphäre. „Was sind die heutigen und zukünftigen Herausforderungen? Nur wenn die verschiedenen Disziplinen zusammenarbeiten, können wir Lösungen dafür finden.“

Systeme und Menschen als „Angriffsziele“

Die beiden Wissenschaftler sind davon überzeugt, dass wichtige Impulse von der Cybersicherheits-Forschung in die Gesellschaft ausgehen können. „Durch die enorme Abhängigkeit von der Digitalisierung werden die Menschen und die Systeme, die sie nutzen, attraktive Angriffsziele“, sagt Sadeghi. „Wir arbeiten daran, solche Angriffe abzuwehren.“

Ein zentrales Thema bei Crossing ist laut Johannes Buchmann die nächste Generation von Kryptographie, also die Verschlüsselung der Zukunft. Fakt sei, dass mächtige Quantencomputer, an denen große Firmen wie Google und IBM arbeiten, viele heutige kryptographische Verfahren unsicher machen. Crossing arbeitet an alternativen Verschlüsselungsmethoden, gegen die sogar Quantencomputer keine Chance haben. Im Angesicht der jüngsten „Datenlecks“ raten sie Nutzern, ihre Accounts mit starken Passwörtern zu sichern und ihre Daten nur bei Anbietern eingeben, die Verschlüsselung nutzen.