# Gemeinsam gegen Cyber-Bedrohungen

An der Stanford University, unweit vom Silicon Valley liegt, fand in diesem Jahr die dritte ASE-Konferenz (Academy of Science and Engineering) statt, dieses Mal mit den Themen Cyber-Security, Big Data und Social Sciences. Am letzten Tag fand zusätzlich ein Cyber-Security-Workshop statt, der von Fraunhofer SIT aus Darmstadt organisiert wurde und zur Zielsetzung hatte, eine Cyber-Security-Allianz zwischen den USA und Deutschland zu initialisieren. Hierzu waren Vertreter aus der Industrie und dem akademischen Umfeld angereist.

## Sicherheit ist das A und O

Ein Ergebnis der Konferenz: IT-Sicherheit ist auch für Big Data relevant. Schließlich wurde allein 2013 eine Datenmenge von ca. 4,4 Zbyte produziert, von denen laut Statistik ca. 43 % schützenswert, aber nur die Hälfte ausreichend gesichert ist. Interessant, dass auch in den USA inzwischen das Cloud Computing nicht mehr ganz so euphorisch gesehen wird. Die Rechts- und Zugriffssicherheit sowie der Datenschutz haben nunmehr auch Nordamerika erreicht. Vorherrschend wurde daher die Cloud Security diskutiert. Man war sich einig, dass diese erst zufriedenstellend gelöst werden muss, bevor die Cloud ein erfolgreiches Geschäftsmodell für Unternehmen werden kann.

Zusätzlich nehmen mobile Attacken zu und werden zunehmend intelligenter. 5 Mio. Viren (Malware) werden für 2014 bereits erwartet – die fünffache Menge im Vergleich zu 2103. Zwar sind inzwischen Antimalware-Programme auf dem Markt, die aber oft nicht die notwendigen Absicherungswerte erreichen. Zu viele mobile Apps sind unsicher und können relativ einfach gehackt werden. Hinzu kommt, dass es sog. Fake-AV-Programme für Smartphones gibt, die eine trügerische Sicherheit vorspielen. Diese Sicherheitsprobleme werden sich künftig auch auf das mobile Internet in Automobilen auswirken. So wurde z.B. auf der Konferenz eindrucksvoll demonstriert, wie ein Auto mittels Android-Anbindung gehackt und der Start des Motors verhindert werden konnte.

## Kommt eine Cyber-Security-Allianz?

Auf dem Cyber-Security-Workshop wurden Cyber-Bedrohungen und erste Lösungsansätze diskutiert. So wurde u.a. die Stuxnet-Attacke als warnendes Beispiel für die fehlende Cyber-Widerstandsfähigkeit genannt. Sie konnte nur deshalb erfolgreich durchgeführt werden, weil der Fokus der Industrie nach wie vor auf Verfügbarkeit und Flexibilität liegt und nicht auf IT-Sicherheit. Zudem gibt es nur eine kleine Menge an ICS-Sicherheitsexperten (ICS – Integrated Computer Solutions), da dieses Thema an Schulen und Universitäten zu wenig gefördert wird.

Verschiedene Sicherheitsproblematiken wurden genannt. So stellt das Videospiel „Watchdog" das Szenario eines ICS-Hackers nach und trainiert spielerisch das Hacking. Es war nach Erscheinen innerhalb kürzester Zeit ausverkauft. Des Weiteren wurde beispielhaft ein ICS-Honeypot in einer Industrieanlage aufgesetzt, der innerhalb kürzester Zeit gehackt wurde. Heute sind diverse Industrieanlagen ohne entsprechende Sicherheitsmaßnahmen bereits mit dem Internet direkt verbunden, damit z.B. Firmwareupdates einfach durchgeführt werden können. Und laufend kommen neue Systeme hinzu.

Notwendige Maßnahmen, um künftige Katastrophen zu verhindern, wären der verstärkte Einsatz von IDS/IPS, die Authentifizierung von Industriegeräten (Hardware), sichere Remote-Access-Verbindungen sowie eine Sensor-überprüfung. Zusätzlich müssten neue Testmethoden entwickelt werden, da man die Absicherung der ICS-Infrastruktur nur mit spezifischen ICS-Ansätzen verbessern kann.

Diverse Beiträge beschäftigten sich mit der Authentifizierung von Hardwarekomponenten. Alle beruhten auf dem Einsatz von Trusted Network Connect (TNC), IF-MAP und Trusted Platform Module (TPM) – alles Spezifikationen der Trusted Computing Group (TCG). So wurde z.B. in einem Smart-Grid-Projekt auf die Kombination von TPM und TNC gesetzt. Damit setzte das Projekt die Hardwareintegrität ei-


*Die ASE-Konferenz an der Universität Stanford (USA) versuchte drei wichtige Themen zusammenzubringen: Cyber-Security, Big Data und Social Sciences (Foto: )*

nes Smart-Meter-Gateways elektronisch um und ermöglichte, diesen Zustand sicher remote abzufragen.

Abschließend diskutierten u.a. Vertreter von PNNL (Pacific Northwest National Laboratory), University of Washington und Fraunhofer SIT die Möglichkeiten, das Internet der Dinge besser abzusichern. Dabei kam man überein, dass es eine Foundation zur Entwicklung widerstandsfähigerer Systeme geben sollte. Zudem wird zu wenig fachübergreifend nach Lösungen gesucht. IT-Sicherheit sollte aber immer ein integraler Bestandteil einer Entwicklung sein.

Problematisch bleibt allerdings, dass sich IT-Sicherheit nicht messen lässt. Verfügbarkeit hingegen schon, doch die hängt im Grunde wieder von der IT-Sicherheit ab. Hier sollte man ansetzen, um auch Geschäftsführer von der Wichtigkeit überzeugen zu können. Durch immer komplexere Systeme wird jedoch die Absicherung immer schwieriger. Zur Entwicklung eines ganzheitlichen Lösungsansatzes wird eine Allianz zwischen den USA und Deutschland angestrebt, damit in Forschungsprojekten gemeinsam nach Lösungen gesucht werden kann.

*Prof. Kai-Oliver Detken, Decoit GmbH, Bremen*