PRESSEBERICHT

Zweite Jahreskonferenz des BMBF-Förderschwerpunkts

„IT-Sicherheit für Kritische Infrastrukturen“

20. und 21. Juni 2016, Haus der Wissenschaft in Bremen

150 Gäste aus nahezu allen KRITIS-Domänen treffen sich zum zweitägigen wissenschaftlichen Austausch über das Thema IT-Security

Am 20. und 21. Juni 2016 kamen die Beteiligten des vom Bundesministeriums für Bildung und Forschung (BMBF) geförderten Förderschwerpunkts „IT-Sicherheit für Kritische Infrastrukturen“ – kurz ITS|KRITIS – zur Zweiten Jahreskonferenz in Bremen zusammen, um sich gemeinsam mit insgesamt 150 Gästen aus Wissenschaft, Wirtschaft, Politik und von Behörden über die aktuellen technischen, rechtlichen und politischen Entwicklungen für KRITIS auszutauschen sowie erste Forschungsergebnisse vorzustellen. Die diesjährigen Veranstalter luden zur wissenschaftlichen Vernetzung der insgesamt zwölf interdisziplinär aufgestellten Forschungsprojekte in das traditionsreiche Haus der Wissenschaft ein. Das vielfältige Programm kombinierte wissenschaftliche Vorträge verschiedener Fachdisziplinen, Keynote-Speeches, Workshops und Präsentationen der einzelnen Forschungsprojekte. Den wissenschaftlichen Rahmen bildete eine zweitägige Posterausstellung im Foyer des Hauses.

Prof. Matthias Stauch, Staatsrat beim Senator für Justiz und Verfassung der Freien Hansestadt Bremen, richtete zur Eröffnung der Konferenz das Begrüßungswort an die Gäste. Er drückte seine besondere Freude über die Wahl des diesjährigen Veranstaltungsortes aus, sei das Bundesland Bremen doch auch als Industriestandort von besonderer Bedeutung. Die Digitalisierung industrieller Prozesse – Industrie 4.0 – das sei aus wirtschaftlicher Sicht ein wesentlicher, nicht zu vernachlässigender Wettbewerbsfaktor. Die Digitalisierung und Revolutionierung betreffe aber nicht nur die Produktion, sondern auch die kommunikativen Prozesse und die Zirkulation von Waren. Besonders betont wurde von Stauch die gesellschaftliche Verantwortung; dem Faktor Mensch komme unter dem Stichwort „Arbeit 4.0“ im digitalisierten Produktionsprozess hohe Bedeutung zu. Bei alledem sei IT-Sicherheit eine Grundvoraussetzung.

Dem Verhältnis von Datenschutz und Datensicherheit in Kritischen Infrastrukturen widmete sich im Folgenden Peter Schaar, vormaliger Bundesbeauftragter für den Datenschutz und die Informationsfreiheit sowie Vorsitzender der Europäischen Akademie für Informationsfreiheit

und Datenschutz (EAID) Berlin, in einer Keynote-Speech mit dem Titel „Datenschutz und IT-Sicherheit – Gleichklang oder Widerspruch“. Auch wenn in der öffentlichen Wahrnehmung zwischen IT-Sicherheit und Datenschutz nicht unterschieden werde, müsse hier klar differenziert werden. IT-Sicherheit meine den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Datenschutz hingegen sei ein seit dem so genannten Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) höchstrichterlich anerkanntes Grundrecht, das als allgemeines Persönlichkeitsrecht der Wahrung der Menschenwürde und der freien Entfaltung der Persönlichkeit diene. Dieses Grundrecht sei in der Rechtsprechung des BVerfG seit 2008 neu ausgerichtet worden hin zu einem Anspruch des Einzelnen auf die Intimität und Vertraulichkeit informationstechnischer Systeme, in welche nur in begründeten Einzelfällen eingegriffen werden dürfe. Schaar zeigte anhand einzelner Beispiele auf, dass IT-Sicherheit und Datenschutz sich immer wieder auch in Konfliktbereichen gegenüber stehen und nannte Lösungsansätze, um solche Konfliktfälle beherrschbar zu machen. Ein ausbalanciertes, faires System zu schaffen, das sei im wirtschaftlichen und im politischen Interesse.

Prof. Dr. Hanno Friedrich von der Kühne Logistics University Hamburg (KLU) stellte anschließend die Forschungsergebnisse des Forschungsprojektes SEAK zur Bewältigung von Versorgungsengpässen in der Lebensmittel-Supply-Chain vor. Dabei wurden verschiedene Sicherheitsszenarien genauer beleuchtet, darunter Hitzewellen, ein Arbeitskräfteausfall und ein IT-Ausfall. Friedrich kam zu dem Ergebnis, dass Notfallpläne zwar für Ausfälle der IT, nicht hingegen für Beeinträchtigungen in der Logistik in den Unternehmen vorhanden seien. Die Notwendigkeit präventiven Risikomanagements für extreme Ereignisse sei insgesamt nur schwer vermittelbar, dennoch müssten im Notfall mangels ausreichender staatlicher operativer Ressourcen Unternehmen die Versorgung übernehmen.

Das wissenschaftliche Vortragsprogramm des Konferenztages wurde durch das Live Hacking einer simulierten Windenergieanlage ergänzt, durchgeführt wurde dieses von den Sicherheitsexperten Dirk Reimers und Markus Ohnmacht. Zum Abschluss des öffentlichen Programms referierte Supervisory Special Agent Edward H. You, Federal Bureau of Investigation (FBI), Washington, D.C., der unter dem Vortragstitel „Current and Future Challanges to Cypersecurity, the Economy, Defense, and Health“ das Thema Cyber-Security aus Sicht einer US-amerikanischen Bundesbehörde beleuchtete. Ausdrücklich wies You dabei auf den Wert von Gesundheitsdaten hin, insbesondere wenn diese im Sinne intimer

Persönlichkeitsprofile mit sonstigen personenbezogenen Daten kombiniert würden. Hier gebe es für die Zukunft ein erhebliches Schutzpotenzial, das vor allem durch Maßnahmen effektiver IT-Security umgesetzt werden könne.

Den zweiten Veranstaltungstag eröffnete Dr. Timo Hauschild, Referatsleiter beim Bundesamt für Sicherheit in der Informationstechnik (BSI), mit seinem Vortrag über „Resiliente IT in Kritischen Infrastrukturen – UP KRITIS und IT-Sicherheitsgesetz als Wegbereiter“. Er wies auf die enorme Bedeutung der IT in sämtlichen anerkannten Kritischen Infrastrukturen hin; diese ließen sich ohne eine funktionierende Informationstechnik regelmäßig nicht beherrschen. Sodann legte Hauschild den Fokus seiner Betrachtung auf den Anwendungsbereich des IT-Sicherheitsgesetzes sowie des BSI-Gesetzes (BSIG) und erläuterte, dass hiernach die Definition Kritischer Infrastrukturen gem. § 2 Abs. 10 BSIG enger gefasst sei als im fachwissenschaftlichen Sprachgebrauch, was insbesondere auf eine fehlende Gesetzgebungskompetenz des Bundesgesetzgebers zurückgeführt werden könne. Hauschild stellte weiterhin dar, unter welchen Voraussetzungen von Kritischen Infrastrukturen im Sinne des BSIG gesprochen werden könne. Anschließend wies er auf die wesentlichen Neuregelungen des durch das IT-Sicherheitsgesetz eingefügten § 8b BSIG hin und schilderte sodann die Konzeption der §§ 8a und 8b BSIG. Dabei veranschaulichte er die Rolle und Eingliederung des BSI in die gesetzlichen Vorschriften. Schließlich stellte Hauschild den UP KRITIS, eine öffentlich-private Kooperation zwischen den Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen vor. Dessen Ziel sei es, die Vorgaben des BSIG zum Nutzen aller umzusetzen und damit die Versorgung mit Dienstleistungen Kritischer Infrastrukturen in Deutschland aufrechtzuerhalten.

Das weitere Programm der Zweiten Jahrestagung sah parallel verlaufende Workshops, Vorträge sowie ein Serious Game vor. Insgesamt bildete die Zweite Jahreskonferenz zur IT-Sicherheit in Kritischen Infrastrukturen gerade aufgrund der Vielfältigkeit der Forschungsschwerpunkte und der weiten Abdeckung der KRITIS-Domänen eine gute Gelegenheit, um innerhalb von zwei Tagen ein aktuelles Update in Sachen nationaler IT-Security-Forschung zu erhalten. Gerade aufgrund der Vielzahl von anwesenden Wissenschaftlern, Betreibern und Behördenvertretern war es zudem möglich, das eigene Sicherheitsnetzwerk weiter zu verfestigen und zu vertiefen. Man darf gespannt sein, welche Forschungsergebnisse auf der dritten ITS|KRITIS-Jahreskonferenz im Sommer 2017 vorgestellt werden.