4. Bonner Dialog für Cybersicherheit zum Thema Industrie 4.0 - mit Sicherheit sicher?

4. Bonner Dialog für Cybersicherheit zum Thema Industrie 4.0 - mit Sicherheit sicher?
Die Digitalisierung aller Lebensbereiche entwickelt sich immer weiter. Unter dem Begriff Industrie 4.0 wird die zunehmende Vernetzung der industriellen Produktion mit bestehenden und neuen Sensorsystemen verstanden. Hierdurch eröffnen sich ganz neue Tätigkeitsfelder und Produktbereiche für die heimische Industrie. Aber es stellen sich auch ganz neue Anforderungen an Sicherheitssysteme einer so vernetzten Produktion.
Der 4. Bonner Dialog für Cybersicherheit gab Einblicke in die Potentiale und in die Anforderungen an sichere Produktionssysteme der Zukunft. Schutz bedeutet die Forderung nach mehr Sicherheit. Doch sicher ist nicht gleich sicher. Wo brauchen wir welches Sicherheitsniveau? "Wer im Zeitalter von Industrie 4.0 versucht, den Speiseplan der Kantine in gleicher Weise zu schützen wie die sensibelsten Konstruktionspläne, der wird Schiffbruch erleiden: Wir brauchen Konzepte abgestufter Sicherheit - im Cyber Space wie auch in der physischen Welt", sagte Prof. Dr. Peter Martini, Leiter des Fraunhofer FKIE und des Instituts für Informatik 4 an der Universität Bonn, der das Thema Cyber Security intensiv vorantreibt. "Der Glaube, dass alle Daten gleich (schützenswert) seien, ist ein Irrglaube". Derzeit sei überdies die Bereitschaft für Sicherheit zu bezahlen gering.
Die Vision ist längst Realität und Industrie 4.0 ist in der Gegenwart angekommen. "Wenn wir Industrie 4.0 jetzt nicht nutzen, werden wir keine Chance mehr haben", so die Aussage von Mahbobi. Goodarz Mahbobi, Geschäftsführer und Mitbegründer der axxessio GmbH, referierte aus der Perspektive der Wirtschaft zum Thema Industrie 4.0 - Eine Chance für die Wirtschaft in Deutschland. Ein Querschnittsthema für die IT-Wirtschaft und die Industrie. Daten sind heute überall und wir schwimmen nahezu in ihnen. Neue Herausforderungen ergeben sich beispielsweise für die Autoindustrie, wie Mahbobi veranschaulichte. Bald schon wird der physische Autoschlüssel überflüssig sein.
Doch wo liegen die Chancen von Industrie 4.0 in und für Deutschland? Sicherheit wird eine große Rolle spielen, aber an welchen Stellen ist das Thema IT-Sicherheit besonders relevant? Hat die NSA-Affäre Auswirkungen auf das Voranschreiten der Digitalisierung der Automation?
Liegt eine Chance für die deutsche Industrie vielleicht gerade darin, dass sich eine veränderte Nachfrage nach vertrauenswürdigen Herstellern und Produkten feststellen lässt? Diese und weitere Fragen diskutierten Vertreter aus Wirtschaft und Wissenschaft gemeinsam mit dem Publikum. Neben Goodarz Mahbobi und Prof. Dr. Peter Martini beteiligten sich an der Podiumsdiskussion Dr. Rainer Baumgart, Vorstandsvorsitzender der secunet Security Networks AG und Dr. Jürgen Kohr, Senior Vice President von T-Systems und seit 2013 Leiter der Business Unit Cyber Security bei T-Systems. Prof. Dr. Michael Meier, Professor am Institut für Informatik 4 an der Universität Bonn und Leiter der Abteilung Cyber Security am Fraunhofer FKIE moderierte die Diskussionsrunde zur Fragestellung "Industrie 4.0 - Die vernetzte Industrie stellt neue Herausforderungen an den Mittelstand - Chancen oder Risiken - was ist möglich?"
Die vierte industrielle Revolution fällt in kaum einem Bundesland auf so fruchtbaren Boden wie in Nordrhein-Westfalen. Nordrhein-Westfalen ist gleichzeitig eine IKT-Region, die deutschlandweit und international eine viel beachtete Position innehat. Hier entstehen die komplexen, vernetzten Systeme der Zukunft. Die Vernetzung schreitet trotz aller Cyberrisiken immer weiter voran. Der Faktor Mensch ist im Rahmen von Industrie 4.0 ein zentrales Thema. Dabei geht es um die Frage nach möglichen Mensch-Roboter-Kooperationen. "Die Roboter werden aus ihren Käfigen kommen", lautete ein Statement des Abends. Unter dem Stichwort Industrie 4.0 werden Fabriken und ganze Wertschöpfungsketten digitalisiert. Security by Design muss auch für die Software gelten. "Es lohnt sich, sich rechtzeitig mit dem Thema ?Sicherheit zu beschäftigen. Das erkennen Unternehmen zunehmend und fragen Sicherheitskonzepte nach, bevor sie Projekte starten", sagt Dr. Jürgen Kohr. Möchte man einzelne Komponenten wie Bausteine vernetzen, wenn IT nicht aus Europa kommt? IT-Sicherheit "made in Germany" steht für vertrauenswürdige IT-Technologie. Deutschland habe sehr gute Voraussetzungen, um sich in dem Themenfeld international zu positionieren. Um die Industrie durch Innovation wettbewerbsfähig zu halten, gilt es dem Fachkräftemangel durch geeignete Maßnahmen entgegen zu wirken. Die Wissenschaft muss interdisziplinär nach Lösungsansätzen suchen und nicht zuletzt müssen Politik, Wirtschaft und Wissenschaft gemeinsam das Thema angehen.
Dabei gilt es auch das Thema Datenschutz gezielt zu behandeln und die Benutzbarkeit (Usability) mitzudenken. In vielen Bereichen herrsche noch ein mangelndes Bewusstsein für die Notwendigkeit, sich gegen Cyberangriffe zu schützen. Heute neigt man dazu, die eigene digitale Souveränität allzu schnell preiszugeben. Es muss mehr getan werden, um ein breiteres Bewusstsein für die Bedrohungslage zu erzeugen.
Auch Standards für Industrie 4.0 müssen zügig geschaffen werden, was wiederum eine Chance für Deutschland, nicht zuletzt für den Mittelstand, darstellt. Man sollte nicht auf fertige Lösungen warten. Was können Standardisierungen bewirken? Was bewirken deutsche Standards und ist Cyber Security politisch umsetzbar, selbst wenn technische Konzepte vorhanden sind? In diesem Zusammenhang wurde auch der Aspekt einer gesetzlichen Intervention kontrovers diskutiert.
Im Fokus der Dialoge stehen immer wieder allgegenwärtige Bedrohungen der digitalen Welt und mögliche Sicherheitsperspektiven. Sicherheit bleibt auch heute eine Herausforderung. Nicht nur die Sicherheitspolitik steht vor wachsenden Herausforderungen, um Cyberangriffe abzuwenden. Das Charakteristische an der inzwischen fest etablierten Veranstaltungsreihe ist der Dialog zwischen Wissenschaft, Politik und Unternehmen aus der Bonner Region. IT-Sicherheit ist ein wirtschaftlich, gesellschaftlich und politisch hochrelevantes Thema. Bonn ist eine wachsende Stadt und ein bedeutender Wirtschaftsstandort, an dem ca. 10.000 IT-Beschäftigte angesiedelt sind. Cyber Security wird vom Standort Bonn durch unterschiedlichste Akteure mit gestaltet. Hier sitzen international tätige Unternehmen der Telekommunikationswirtschaft und spezialisierte Mittelständler im Bereich der IT-Sicherheit. Bonn ist Dienstsitz der Bundesnetzagentur, der Bundesbeauftragten für Datenschutz und die Informationsfreiheit und nicht zuletzt ist das Bundesamt für die Sicherheit in der Informationstechnik (BSI) in Bonn angesiedelt. Zusätzlich gibt es in Bonn zahlreiche wissenschaftliche Einrichtungen, die sich mit dem Thema Sicherheit in den unterschiedlichsten Facetten beschäftigen. Dazu zählen verschiedene Institute der Universität Bonn aber auch diverse Fraunhofer Einrichtungen.
Die Stärken des Standortes sind auch von einer Untersuchung der Europäischen Kommission bestätigt worden. In dieser Untersuchung liegt Bonn als IT-Standort in Deutschland hinter München, Darmstadt und Karlsruhe auf Rang vier. Bonn sei der "Hidden Champion für Datensicherheit und Datenschutz", so Oberbürgermeister Jürgen Nimptsch. "Helfen Sie uns, diese Stärke weiter auszubauen und nach außen zu kommunizieren!"

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE
Fraunhoferstr. 20
53343 Wachtberg
Telefon: 0228 9435-287
Telefax: 0228 9435-685
Mail: fkie@fkie.fraunhofer.de
URL: http://www.fkie.fraunhofer.de
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=582684" width="1" height="1">

Pressekontakt

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE

53343 Wachtberg

fkie.fraunhofer.de
fkie@fkie.fraunhofer.de

Firmenkontakt

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE

53343 Wachtberg

fkie.fraunhofer.de
fkie@fkie.fraunhofer.de

Seit den Ereignissen des 11. September 2001 betrachten Politik, Wirtschaft und Gesellschaft das Thema Sicherheit unter veränderten Gesichtspunkten. Im militärischen Sektor wie auch im Bereich innere Sicherheit folgt daraus ein erweitertes Spektrum von Aufgaben, deren Bewältigung anspruchsvolle technische Infrastrukturen erfordert ? im Fraunhofer FKIE werden sie gestaltet und weiterentwickelt. Wehrtechnische Systeme zur vernetzten Operationsführung sind unsere Kernkompetenz. Doch zunehmend ergeben sich daraus auch Synergieeffekte für zivile Anwendungen im Umwelt- und Katastrophenschutz sowie in der Unternehmensführung. So haben etwa auch große Konzerne ein Interesse, ihre Datennetze vor Cyber-Angriffen zu schützen. Dual-Use-Forschung nennen wir das.Voraussetzung und Herausforderung zugleich ist für unsere Arbeit die schnelle Weiterentwicklung der Informationstechnologie, die große Potenziale für die Verbesserung von Verteidigungs- und Sicherheitsanwendungen birgt. Dementsprechend gliedert sich unsere Vorgehensweise in folgende Schwerpunkte: Wir identifizieren Potenziale, erarbeiten Methoden und Verfahren zu ihrer Umsetzung in Anwendungen, erbringen den Nachweis der Machbarkeit und nehmen auf der Basis exemplarischer Realisierungen eine Abschätzung des Aufwandes vor. Auf diese Weise gestaltet und entwickelt das FKIE Systeme, die den gesamten militärischen Führungs- und Aufklärungsprozess der Bundeswehr aufgaben- und anforderungsgerecht unterstützen.