21. Karlsruher Automations-Treff

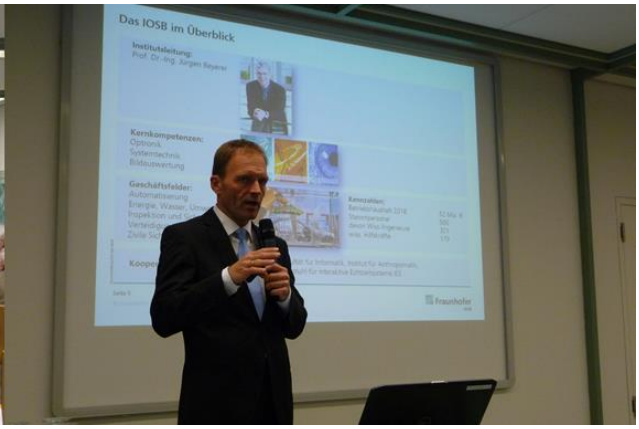
"IT-Sicherheit in der Produktion – heute und in Industrie 4.0"

am Donnerstag, 09. November 2017, im Fraunhofer IOSB

(Dr. Michael Okon)

Im 21. Karlsruher Automations-Treff (KAT), der zum zweiten Mal nach 2011 am Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) stattfand, wurde die IT-Sicherheit in der Automatisierungstechnik branchenübergreifend und aus dem Blickwinkel der angewandten Forschung beleuchtet. Mit rund 60 Teilnehmern fand die Veranstaltung, in der unter dem Titel „IT-Sicherheit in der Produktion – heute und in Industrie 4.0" in zwei Vorträgen aktuelle Arbeiten und Angebote des Instituts vorgestellt wurden, eine hohe Resonanz. Eingerahmt wurden die Vorträge von einer Vorstellung des Fraunhofer IOSB durch den stellvertretenden Institutsleiter und Koordinator des Geschäftsfeldes Automatisierung Herrn Dr. Olaf Sauer, Vorführungen von mehreren Demonstratoren und dem obligatorischen „Get Together", bei dem in angenehmer Atmosphäre bei einem kleinen Imbiss und Getränken Gespräche über das Gehörte und Gesehene geführt werden konnten.

Im Vortragsteil der Veranstaltung wurden eine Weiterbildungsinitiative der Fraunhofer Academy für Sicherheitsfachkräfte und aktuelle Forschungsergebnisse im Bereich IT-Sicherheit behandelt.



Im ersten Vortrag stellte Herr Dipl.-Inform. Gerhard Sutschet das „Lernlabor Cybersicherheit" vor. Diese Weiterbildungsinitiative der Fraunhofer Academy soll Sicherheitsfachkräfte in unterschiedlichen Gebieten, wie z. B. „Industrielle Produktion", „Energieverteilnetze", „Softwarequalität und Zertifizierung", „Embedded Systems", etc., ansprechen. Dabei wird das Weiterbildungsangebot jeweils in Zusammenarbeit eines Fraunhofer-Instituts und einer Partner-Hochschule entwickelt. Das Fraunhofer IOSB arbeitet hier zusammen mit der Hochschule Ostwestfalen-Lippe an Weiterbildungs-Modulen zum Thema „Industrielle Produktion".

Herr Sutschet zeigte auf, warum dieses Thema, das in der Vergangenheit wenig Beachtung fand, im Rahmen der Initiative Industrie 4.0 zunehmend an Bedeutung gewinnt. Fachkräfte auf diesem Gebiet gibt es derzeit in kleinen und mittelständischen Unternehmen kaum. Das Fraunhofer IOSB richtet sich mit seinem Weiterbildungsangebot explizit an diese Unternehmen, um ihnen die Möglichkeit zu eröffnen, im Zeitalter von Industrie 4.0 sowohl effizient ihre Produktion abzusichern als auch mit anderen Unternehmen zu kommunizieren.

Im zweiten Vortrag berichtete Herr Dr.-Ing. Christian Haas über aktuelle Forschungsarbeiten im Bereich IT-Sicherheit für Industrie 4.0. Ein Schwerpunkt des Vortrags war das Industrial Security Testing Framework IsuTest. ISuTest ermöglicht das automatisierte Überprüfen der Security-Eigenschaften von Automatisierungssystemen mithilfe von definierten Testfällen und baut auf dem auf Office-IT ausgerichteten „OpenVAS“ (Open Vulnerability Assessment System) auf.

ISuTest ermöglicht Angriffe auf Automatisierungssysteme durchzuführen und daraus resultierende Reaktionen zu prüfen. Anhand dieser kann die Auswirkung auf die Funktionsfähigkeit und damit die Anfälligkeit gegenüber einem Angriff untersucht werden. Durch sein offenes und modulares Design ermöglicht ISuTest einfaches und effizientes Testen nahezu beliebiger Automatisierungs-Komponenten. Das Framework wurde anhand von einigen Testbeispielen an aktueller Automatisierungs-Hardware und die Auswirkungen von Angriffen auf diese eingeführt und erläutert.

Nach den Vorträgen konnten drei Demonstratoren zum Thema IT-Sicherheit besichtigt werden:

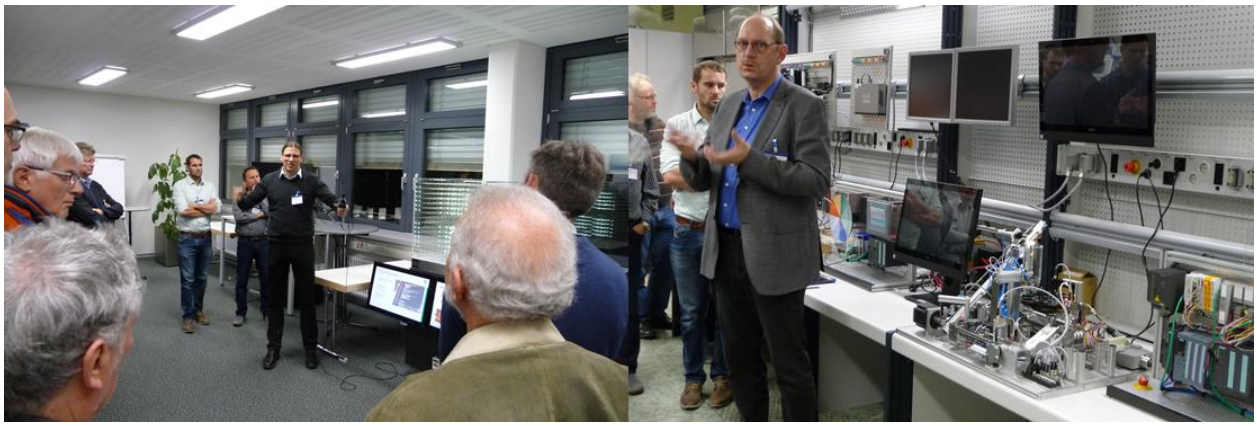
- Lernlabor Cybersicherheit

Das Lernlabor Cybersicherheit der Fraunhofer Academy ist eine Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen. Fach- und Führungskräfte aus Industrie und öffentlicher Verwaltung erhalten eine kompakte Qualifizierung in hochwertigen Laboren mit aktueller IT-Infrastruktur. Sie stellen dort reale Bedrohungsszenarien nach, lernen deren Bedeutung und Konsequenzen zu erkennen und studieren geeignete Lösungskonzepte praxisnah in ihrem Einsatz und Wirkungsgrad. Das Themenfeld »Industrielle Produktion/Industrie 4.0« umfasst Netzwerk- und Sicherheitstechniken für Automatisierungssysteme im Hinblick auf

vernetzte Systeme, Internetanbindung und Cloud-Techniken für Automatisierungsaufgaben. Betrachtet wird dies auf verschiedenen Ebenen: »Field Level«, »Control Level«, »SCADA« (Supervisory Control and Data Acquisition (SCADA): Überwachen und Steuern technischer Prozesse) und »MES« (Manufacturing Execution System). Zudem werden zukünftige Veränderungen, die die bisher streng getrennten Ebenen in ihren Funktionen auflösen, mit einbezogen.

Behandelt werden sowohl typische Schwachstellen in Design und Implementierung in eingebetteten Systemen und industriellen Komponenten (z.B. Industrie-Roboter) als auch neueste Entwicklungen im Bereich von Kommunikations-Protokollen und Sicherheitsfunktionen sowie der Entwicklung sicherer Software für die zunehmend Software-intensiven Bereiche der industriellen Produktion. Die Weiterbildung richtet sich sowohl an Planer und Betreiber von Automatisierungssystemen (Planungs-Ingenieure, Wartungstechniker) als auch an Entwickler von Automatisierungslösungen (Software-Designer, Programmierer). Zielgruppe sind auf Anwenderseite alle Branchen der produzierenden Industrie (Automobil, Chemie, ...) sowie die Hersteller von Automatisierungslösungen.

In der Demo wurden verschiedene Demonstratoren gezeigt, die im Rahmen der Weiterbildung eingesetzt werden.



- IT-Sicherheitslabor für die industrielle Produktion

Das Fraunhofer IOSB bietet in seinem IT-Sicherheitslabor eine ideale Testumgebung, um reale Angriffsszenarien nachzustellen und die Auswirkungen solcher Angriffe zu untersuchen. Dazu verfügt das IT-Sicherheitslabor über eine eigene Modellfabrik mit realen Automatisierungskomponenten, die eine simulierte Produktionsanlage steuern. Alle Netzwerk-Ebenen einer Fabrik-Umgebung sind dabei mit typischen Komponenten vorhanden, darunter Industrial Ethernet Komponenten, Industrie-Firewalls und Wireless-Komponenten. Eine eigene Private Cloud erlaubt es den Experten des IOSB, unterschiedliche Konfigurationen schnell und flexibel herzustellen und die Modellfabrik auf unterschiedliche Szenarien einzustellen. In der Private Cloud stehen dazu flexibel Ressourcen zur Verfügung, um den Netzwerkverkehr in allen Bereichen zu analysieren, Netzwerkverbindungen über Sicherheitseinrichtungen zu leiten oder Angriffe gegen Komponenten durchzuführen.

In der Demo wurden verschiedene Angriffe auf typische Industriekomponenten und Prozesse gezeigt.

- KASTEL Demonstrator Blurry-Box®

Dieser Demonstrator zeigt einen 16 x 16 x 16 LED-Cube auf dem ein Videospiel visualisiert wird, das sich mit einem Joystick steuern lässt. Dieses Spiel wird durch das neue Softwareschutzverfahren Blurry-Box® geschützt. Das Blurry-Box®-Verfahren wurde im Rahmen einer Zusammenarbeit zwischen dem Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL) und der in Karlsruhe beheimateten Firma Wibu-Systems AG entwickelt. Es ist das erste praktisch einsetzbare Softwareschutzverfahren, das im Einklang mit dem Kerckhoffs'schen Prinzip steht. Das Kerckhoffs'sche Prinzip besagt, dass die Sicherheit eines Verfahrens nicht auf der Geheimhaltung der eingesetzten Methoden beruhen darf. Das Blurry-Box®-Verfahren verwendet ein Hardware-Dongle als Vertrauensanker, das in diesem Demonstrator von einem Raspberry Pi repräsentiert wird. Auf zwei Monitoren unterhalb des LED-Cubes werden für das Spiel relevante Dinge (Menü, Bedienungsanleitung etc.) dargestellt sowie die Funktionsweise des Blurry-Box®-Verfahrens erklärt. Das mit Blurry-Box® geschützte Videospiel läuft flüssig, trotz der Schutzmaßnahmen, die angewendet werden. Dies zeigt die praktische Anwendbarkeit des Blurry-Box®-Verfahrens.

Den Abschluss bildete das traditionelle „Get Together" im Vorraum des Max-Syrbe-Saals zum Gedankenaustausch bei Getränken und einem kleinen Imbiss.

Vielen Dank den Initiatoren und dem Fraunhofer IOSB, insbesondere der Abteilung Informationsmanagement und Leittechnik (ILT) für die Vorbereitung und Durchführung dieser erfolgreichen Veranstaltung.

Weitere Informationen zum Arbeitskreis „Mess- und Automatisierungstechnik" bzw. zum Karlsruher Automations-Treff finden Sie im Internet unter http://www.vdi.de/bv-karlsruhe/gma.