Fraunhofer IOSB

visIT

[IT-Sicherheit für die Produktion]

Essay WIBU-SYSTEMS AG

Das IT-Sicherheitslabor des IOSB

SecurePLUGandWORK

Cyber-Security in kritischen Infrastrukturen

Ontologie-basierte Erkennung von Cyber-Attacken

acatech-Workshop

IT-Sicherheit für Industrie 4.0

www.iosb.fraunhofer.de

ISSN 1616-8240

Fraunhofer IOSB

Impressum

Herausgeber
Prof. Dr.-Ing. habil. Jürgen Beyerer

Redaktion
Sibylle Wirth

Layout und graphische Bearbeitung
Christine Spalek

Druck
E&B engelhardt und bauer
Karlsruhe

Anschrift der Redaktion

Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung IOSB

Fraunhoferstr. 1
76131 Karlsruhe
Telefon +49 721 6091-300
Fax +49 721 6091-413
presse@iosb.fraunhofer.de

ein Institut der Fraunhofer-Gesellschaft
zur Förderung der angewandten
Forschung e. V. München

15. Jahrgang
ISSN 1616-8240

Bildquellen

Titel, Seite 15 oben:
MEV
Seite 3, 6, 8, 14/15:
indigo Werbefotografie
Manfred Zentsch

Alle andere Abbildungen:
© Fraunhofer IOSB

INHALT

Essay

Themen

Infothek

Editorial

Liebe Freunde des IOSB,

Prof. Dr.-Ing. habil. Jürgen Beyerer

in diesem Heft nehmen wir das Leitthema IT-Sicherheit für die Produktion, speziell aus dem Blickwinkel von Industrie 4.0 unter die Lupe. Mit der »Digitalen Agenda« hat die Bundesregierung eine Beschreibung unserer zukünftigen wichtigsten Handlungsfelder zum Leben in einer vernetzten Welt vorgelegt. Insbesondere unsere Wirtschaft wird durch die Initiative Industrie 4.0 einen tiefgreifenden Wandel vornehmen. Der Erfolg dieser Initiative hängt maßgeblich von der Robustheit, Resilienz und damit Vertrauenswürdigkeit der IT-Sicherheit ab.

Das IOSB stellt sich als wichtiger Partner für die Industrie und den Mittelstand vor und zur Verfügung; vereinen wir in unserem Haus doch sowohl Kompetenz und Know-how aus dem Bereich der Automatisierung als auch langjährige Erfahrung auf dem Gebiet der IT-Sicherheit und dem Internet-of-Things.

Oliver Winzenried von der WIBU-Systems AG beschreibt in seinem Essay die Bedrohungsszenarien für Hersteller und Anlagenbetreiber. Gleichzeitig zeigt er Lösungsmöglichkeiten und Abwehrtechniken für Betriebe auf, um diesen Bedrohungen entgegen zu treten.

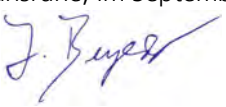
Das IOSB baut derzeit ein neues IT-Sicherheitslabor auf. Hier können in einer gesicherten Umgebung mögliche Angriffsszenarien oder Schwachstellen in hochgradig vernetzten Produktionsanlagen und Cloud-Anwendungen im Vorfeld getestet werden, um die notwendigen Mechanismen einer Angriffsabwehr zu konfigurieren.

Unsere Achillesferse sind kritische Infrastrukturen, wie die Energieversorgung, aber auch Verkehr, Telekommunikation und das Finanzwesen. Die dort eingesetzten SCADA-Systeme bedürfen einer Aufrüstung, um den neuen Cyber-Attacken keine Angriffsflanken zu bieten. Eine Ontologie-basierte Erkennung solcher Attacken stellt ein mögliches Werkzeug dar.

Das vom BMBF geförderte und vom IOSB initiierte Groß-Projekt »SecurePlug&Work« hat das Ziel, Verfahren und Methoden zur sicheren Autokonfiguration basierend auf existierenden Standards, die für die industrielle Produktion eingesetzt werden können, zu entwickeln und verfügbar zu machen. Eine Studie für das BMWi über die Analyse der IT-Sicherheitsanforderungen im Lichte von Industrie 4.0 wurde soeben gestartet.

Das IOSB engagiert sich aktiv in vorhandenen Netzwerken zum Thema Sicherheit, wie beispielsweise bei der acatech.

Karlsruhe, im September 2014



Prof. Dr.-Ing. habil. Jürgen Beyerer

Essay

IT-SICHERHEIT IN DER PRODUKTION

Hersteller / Maschinenbauer

- Nachbau einer Maschine
- Nachahmen einer Maschine
  - Extraktion von geistigem Eigentum
- Manipulation (Gewährleistung)
  - Nicht autorisierte Updates
  - Veränderung des Betriebsstunden-zählers
  - Veränderung des Flugschreibers
- Nicht autorisierter Zugriff auf Service Dokumente
- Nicht autorisierter Zugriff auf Quell-code

Betreiber

- Manipulation
  - Sabotage
  - Geheimdienste / Unzufriedene Mitarbeiter
- Geistiges Eigentum
  - Rezepte / Betriebsparameter / Schnittmuster
- Produktions-Daten
  - Maschinentagebuch
  - Produktionsmengen
- Nicht autorisierter Zugang zur Maschine
  - Servicefall
  - Betrieb / Operator

Abb. 1: Bedrohungen für Hersteller / Maschinenbauer und Betreiber von Produktionsanlagen.

Deutschland hat das erste IT-Sicherheitsgesetz. Endlich. Innenminister de Maizière spricht von »Sicherheitsgurten für die IT in kritischen Infrastrukturen«. Die »Digitale Agenda« soll Deutschland zum Vorreiter machen. Werden hier die verschiedenen von der Digitalisierung betroffenen Felder gegeneinander abgewogen und die Interessen ausgeglichen, das Funktionieren der Infrastrukturen, Unternehmens-Know-how und Rechte der Bürger sichergestellt und gleichzeitig ein gutes Klima für Innovation und Fortschritt geschaffen, so besteht die Chance für Deutschland in der Tat.

Mit Industrie 4.0 wird die effiziente Produktion bis zu Losgröße 1 ermöglicht. Dazu steckt immer mehr Know-how über das zu produzierende Produkt im Produktionsprozess. Cyber Physical Systems und Embedded Steuerungssysteme werden stark vernetzt. Know-how-Schutz, flexible Funktionsfreischaltung und Sicherheit vor Manipulation, Cyber-Security, werden überlebenswichtig für Hersteller und Betreiber.

Die IT-Sicherheit in der Produktion ist essentiell notwendig und bekommt damit einen neuen Stellenwert. Ergebnisse aus der IT-Sicherheitsforschung werden auch für die Produktion genutzt.

Die VDMA-Studie »Status Quo der Security in Produktion und Automation 2013/14« betrachtete Schutz vor Ausfall, Know-how-Abfluss, Spionage und Manipulation in Maschinen und Anlagen. Die NSA-Affäre zeigte kaum Auswirkungen auf die Security-Strategie der Maschinenbauer, allerdings stieg das Bewusstsein dafür. Der Cyber Defense Maturity Report 2014 von Forescout kam zu dem Ergebnis, dass die heute ergriffenen Maßnahmen unausgereift und ineffektiv sind und 96 Prozent der Unternehmen mindestens einen Sicherheitsvorfall hatten. Als Top-5-Bedrohungen im Maschinen- und Anlagenbau kristallisierten sich laut VDMA heraus:

- Menschliches Fehlverhalten und Sabotage
- Einschleusen von Schadcode auf Maschinen und Anlagen

KONTAKT

Dipl.-Ing. Oliver Winzenried

Mitbegründer und Vorstand der WIBU-SYSTEMS AG in Deutschland

Telefon +49 721 931720
info@wibu.com
www.wibu.com

Abb. 2: CodeMeter-Produkte zum sicheren Speichern kryptografischer Schlüssel und Rechte.

- Technisches Fehlverhalten und höhere Gewalt
- Online-Angriffe über Office- / Enterprise-Netze
- Unberechtigter Zugriff auf Ressourcen

Organisatorische Maßnahmen sind die Grundvoraussetzung, um Fehler zu minimieren, insbesondere wo technische Maßnahmen nicht vorhanden sind.

Internationale Standards zu allgemeiner IT-Security, wie der ISO / IEC 27000er Reihe oder dem BSI-Grundschutz sind vorhanden, jedoch ist fraglich, ob sie sich als Standards für die Produktion eignen. Passender scheinen IEC 62443 oder ISA99, ein Standard für industrielle Automatisierungssysteme, der noch nicht komplett fertig ist und analog zu den Safety Level SIL sog. Security Assurance Level SAL1…4 definiert.

OPC Unified Architecture, OPC UA, ist ein offener Kommunikationsstandard nach IEC 62541, der herstellerunabhängig und interoperabel ist und folgendes bietet:

- Datenverschlüsselung gegen Spionage und Produktpiraterie (Confidentiality)
- Datenintegrität gegen Verändern (Integrity)
- Anwendungsauthentifizierung (Application Authentication)
- Benutzerauthentifizierung (User Authentication)
- Rollenbasierte Berechtigungsmodelle (User Authorization)
- Aufzeichnung sicherheitsrelevanter Ereignisse (Auditing)
- Verfügbarkeit des Systems, hier darf nicht ein Virencheck erfolgen, der das System viele Minuten lahmlegt (Availability)

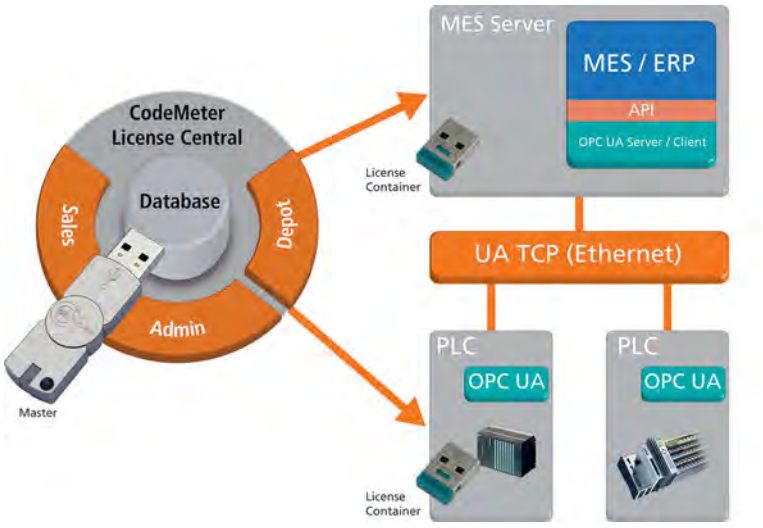


Abb. 3: Verteilen von Zertifikaten in Sensoren, Aktoren und Systeme in der Produktion.

Technische Lösungen für die Produktion bieten heute:

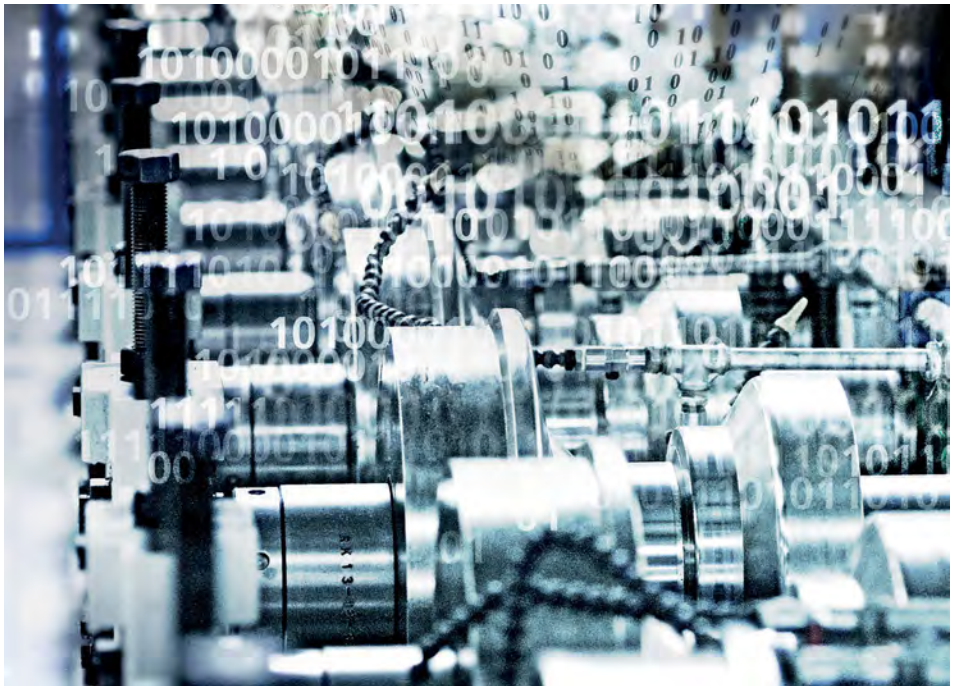
- **Schutz:** Nachbau und Kopieren erschweren sowie Know-how-Schutz durch Schutz vor Reverse-Engineering; schützen durch Verschlüsselung von Software und Produktionsdaten.
- **Lizenzierung:** Logistik vereinfachen, indem die Funktionalität konfiguriert wird. Dies ermöglicht After-Sales-Geschäft und neue Geschäftsmodelle für Hardware. Durch Integration in den Vertriebsprozess und ERP-Anbindung wird das Ausliefern und Konfigurieren automatisiert.
- **Security:** Durch signierte Daten und Programme und Secure Boot wird sichergestellt, dass nur unveränderte und von einem berechtigten Herausgeber kommende Daten verwendet werden.

Eine kommerzielle IT-Sicherheitslösung für die Produktion ist CodeMeter von Wibu-Systems. Smart-Card-basierte CmDongles, z. B. als USB-Dongle oder uSD-Card, oder das softwarenbasierte Aktivierungsverfahren CmActLicense mit Bindung an das Zielsystem, speichern die Schlüssel und Rechte. Die Integration in SPS-Entwicklungsumgebungen wie CODESYS, B&R Automation Studio oder Studio 5000 von Rockwell Automation erleichtert Herstellern die Anwendung.

IT-Sicherheit wird entscheidend für den Erfolg von Industrie 4.0 und die globale Produktion sein. Deutschland hat eine tolle Chance, sowohl effizient und sicher im Land zu produzieren als auch Anlagen und IT-Sicherheit als Weltmarktführer anzubieten. Packen wir es an.

IT-SICHERHEIT IN DER INDUSTRIEL

DAS IT-SICHERHEITSLABOR DES IOSB



Moderne Produktionsanlagen sind hochgradig vernetzt: Eingebettete Systeme kommunizieren selbstständig miteinander, Planungssysteme aus der Cloud berechnen Auftragsschritte und Maschinenbelegungen, Anlagenführer überwachen und steuern aus der Ferne, Wartungspersonal greift weltweit zu und führt Konfigurationsänderungen aus.

In der vernetzten Welt endet der Schutz von Produktionsanlagen nicht mehr am Gebäude oder am Fabrik-Gelände. Über die Netzwerk-Verbindungen können Angreifer in die Systeme eindringen und diese manipulieren, Schadcode-Infektionen können weite Bereiche vollständig lahmlegen und dabei auch immense physische Schäden sowie Gefahren für Leib und Leben verursachen. Nicht erst seit Meldungen über Stuxnet, Duqu, Flame und Havex ist klar, dass Produktionsanlagen Ziele für Cyber-Angriffe sind.

IT-Sicherheit in der industriellen Produktion muss dabei spezifische Randbedingungen berücksichtigen, die im Büro-Umfeld, bei PC-Arbeitsplätzen und Internet-Servern so nicht zu finden sind. Die Steuerung von Produktionsanlagen stellt Echtzeit-Anforderungen, die Veränderungen auf den Systemen schwierig bis unmöglich machen. So können Software-Patches auf den Systemen, Installation von Überwachungs-Software, Malware-Scannern und Antivirus-Programmen die Funktionsfähigkeit beeinträchtigen, Firewalls im Netzwerk und verschlüsselte Verbindungen zwischen den Systemen können die Echtzeitbedingungen beeinträchtigen. Auch der vergleichsweise lange Nutzungszeitraum von Hard- und Software in der Produktion unterscheidet sich erheblich von anderen IT-Einsatzgebieten.

Für Produktionsumgebungen müssen daher neue Strategien und Verfahrens-

KONTAKT

Dipl.-Inform. Birger Krägelin

IT-Sicherheitsbeauftragter
Fraunhofer IOSB Karlsruhe

Telefon +49 721 6091-454
birger.kraegelin@iosb.fraunhofer.de
www.iosb.fraunhofer.de/

LEN PRODUKTION

weisen gefunden werden, um IT-Sicherheit in der Praxis umzusetzen, und das nicht nur in neuen Systemen, sondern vor allem in Altanlagen.

IDEALE TESTUMGEBUNG

Das Fraunhofer IOSB bietet in seinem IT-Sicherheitslabor eine ideale Testumgebung, um reale Szenarien nachzustellen und die Auswirkungen 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.

Aktuell werden Arbeiten in drei Schwerpunktbereichen durchgeführt:

ANOMALIE-ERKENNUNG AUF FELDEBENE

Condition Monitoring für unterschiedliche Anwendungen ist ein langjähriges Arbeitsgebiet des Fraunhofer IOSB. Aufgabe des Condition Monitoring ist die Analyse von Prozessgrößen in Produktionsprozessen und die Erkennung von Systemzuständen und Zustandsveränderungen, ohne dass exaktes Vorwissen über den Prozess selbst vorliegt.

Erkannte Anomalien der Prozessgrößen sind Indizien für Veränderungen im Prozess. Diese können beispielsweise auf Änderungen im Prozessablauf, auf Defekte oder Alterungserscheinungen in Produktionsanlagen zurückzuführen sein - oder auch auf versehentliche oder beabsichtigte Eingriffe in die Prozessführung als Folge von Angriffen auf die Produktions-IT.

Die Beobachtung von Kommunikationsverbindungen ermöglicht darüber hinaus eine frühzeitige Erkennung von Eingriffen, bevor sich Veränderungen im Prozessablauf zeigen.

PRODUKTIONSSTEUERUNG UND -ÜBERWACHUNG

Für die Steuerung und Überwachung werden vermehrt herstellerunabhängige standardisierte Kommunikationsprotokolle eingesetzt, die auf der Basis von Internet-Protokollen den weltweiten Zugriff erlauben. Mit OPC-UA steht dabei ein Framework zur Verfügung, das als Basis für die weltweite Vernetzung in den Industrie 4.0- Anstrengungen dienen wird.

Die Sicherheitsfunktionen aus den OPC-UA-Standards werden bewertet, Einsatz- und Umsetzungsempfehlungen erarbeitet und konkrete Implementierungen auf Schwachstellen untersucht.

Für die Verlagerung von Funktionen zu externen Dienstanbietern oder die Nutzung von Funktionen in Public Cloud Umgebungen werden Sicherheitsrichtlinien erarbeitet.

VULNERABILITY-ANALYSE

Die Erkennung von Schwachstellen in Konfigurationen und Fehlern in Software-Implementierungen von Komponenten und Geräten ist ein weiteres Arbeitsgebiet der IT-Sicherheitsexperten des Fraunhofer IOSB. Im Einzelnen werden Schwachstellen in Firewall-Konfigurationen, in der Implementierung von Authentifikations- und Verschlüsselungsverfahren sowie spezifische Design-Schwächen in den eingesetzten Kommunikationsprotokollen gesucht.

Für die Vulnerability-Analyse können dabei die Ressourcen der Private Cloud gebündelt werden, um verteilte Angriffe (Distributed Denial of Service Attacken) gegen reale Systeme und Komponenten durchzuführen oder mit Fuzzing-Werkzeugen Implementierungsfehler zu finden. Die Private Cloud gibt darüber hinaus die Möglichkeit, virtuelle Umgebungen zu schaffen, um das Verhalten von Malware zu untersuchen und Abwehr-Strategien zu entwickeln.

Die Einrichtungen des IT-Sicherheitslabors werden daneben auch zu Ausbildungs- und Trainingszwecken genutzt. Schulungsveranstaltungen zum Einsatz von OPC-UA-Mechanismen und zur Planung und zum Aufbau sicherer Produktionsnetze runden das Angebot ab.

SECUREPLUGANDWORK
BEKANNTMACHUNG »IN
– EIN BEITRAG ZUM ZUK

KONTAKT
Dr. Miriam Schleipen

Informationsmanagement
und Leittechnik (ILT)
Fraunhofer IOSB Karlsruhe

Telefon +49 721 6091-382
miriam.schleipen@iosb.fraunhofer.de
www.iosb.fraunhofer.de

KONTAKT
Dr.-Ing. Olaf Sauer

Geschäftsfeld
Automatisierung
Fraunhofer IOSB Karlsruhe

Telefon +49 721 6091-477
olaf.sauer@iosb.fraunhofer.de
www.iosb.fraunhofer.de/

Industrie 4.0 umfasst unter anderem intelligente Anlagenkomponenten, Maschinen und Anlagen sowie IT-Systeme, die miteinander vernetzt und über die relevanten ‚Partner' mit ihren Fähigkeiten informiert sind. Diese werden häufig als Cyber-physische Systeme (CPS) bezeichnet.

Bei einem Neuaufbau oder Umbau von Anlagen, Maschinen und Komponenten können alle Partner nun auf die Veränderung entsprechend reagieren. Änderungen sind beispielsweise in der eingebetteten Software der Feldgeräte, im Programmcode der Steuerungen, aber auch in überlagerten IT-Systemen wie bspw. MES nötig. Diese Veränderungen werden heute häufig manuell durchgeführt und sind daher zeitintensiv und fehleranfällig. Im Rahmen von Industrie 4.0 sollen die Änderungen (teil-)automatisiert ablaufen, ähnlich wie bei einer USB-Schnittstelle und USB-Geräten am PC. Die Situation im Umfeld der Produktion ist allerdings erheblich komplexer.

In den Umsetzungsempfehlungen wird diese Fähigkeit im Use-Case 1 ‚Resiliente Fabrik' als »Plug & Produce-Fähigkeit der Fertigungsmodule« [1, S. 105] beschrieben. Dort werden unter anderem folgende Enabler / Handlungsempfehlungen für diesen Use-Case gefordert:

- Fähigkeits- und funktionsorientierte Beschreibung der Bearbeitungsaufgabe
- Schnittstellenstandards für universell kombinierbare Fertigungsmodule
- Modulare und selbstkonfigurierende Software

Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte und vom Projektträger Karlsruhe betreute Projekt SecurePLUGandWORK (Förderkennzeichen 02PJ2590 ff, siehe http://www.secureplugandwork.de) ermöglicht die Plug-and-Work-Fähigkeit in den produktionsnahen Softwarekomponenten über die verschiedenen Ebenen der Fertigungshierarchie, und zwar unter Nutzung offener Standards, die bereits heute in der Industrie eingesetzt werden.

Den Vorgaben für ein Plug & Produce durch die Umsetzungsempfehlungen [1] wird mit einer Architektur (siehe Bild) begegnet, die verschiedene Standards kombiniert:

- Was wird kommuniziert? AutomationML (IEC 62714) dient zur Beschreibung der Komponenten und Anlagen inklusive deren Fähigkeiten.
- Wie wird kommuniziert? - OPC-UA (IEC 62547) übernimmt die Rolle einer Schnittstelle inklusive des Daten- und Kommunikationsmanagements. Alle Komponenten werden mit einer entsprechenden Schnittstelle ausgestattet. Dies kann ein OPC UA Server der Steuerung sein, aber auch eine neu integrierte Kommunikationskomponente (auf Basis eines Embedded System), das einerseits die Anbindung in die Feldebene ermöglicht und andererseits per OPC UA mit allen anderen Partnern spricht. Komponenten, die auf Grund der Rentabilität nicht kommunikationsfähig sind, können über eine eindeutige Identifizierung auch Stellvertreterobjekten in dieser OPC UA Kommunikationsinfrastruktur zugeordnet werden.

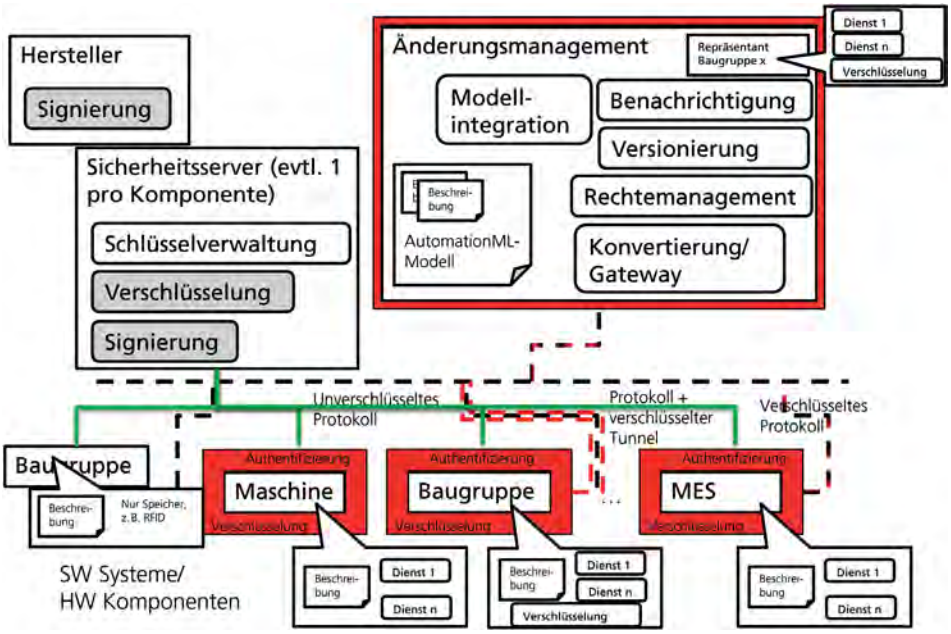
- EIN VERBUNDPROJEKT IM RAHMEN DER
NTELLIGENTE VERNETZUNG IN DER PRODUKTION
KUNFTSPROJEKT ‚INDUSTRIE 4.0'«

- Wer kommuniziert? Zusätzlich zu der Ausstattung / Erweiterung der Automatisierungs- und Produktionskomponenten, werden zentrale und für alle nutzbare SecurePLUGandWORK-Komponenten erzeugt, die auf diesen beiden Standards basieren und sich beispielsweise mit der Modellbildung, Konsistenzprüfung oder Benachrichtigung befassen.

Darüber hinaus spielt die Sicherheit (Security) komplexer vernetzter Anlagen eine große Rolle. Daher wurde in die Architektur ein grundlegendes Sicherheitskonzept basierend auf OPC-UA integriert.

Laut dem Industrie 4.0-Glossar von [2] handelt es sich bei CPS um »Systeme, die reale (physische) Objekte und Prozesse verknüpfen mit informationsverarbeitenden (virtuellen) Objekten und Prozessen über offene, teilweise globale und jederzeit miteinander verbundene Informationsnetze.« [3] Cyber-physische Systeme besitzen also - wie der Name schon sagt – einen physischen, sowie einen virtuellen Anteil. Neben einer reinen Software-Umsetzung, muss also auch die Hardware entsprechend befähigt werden und Plug & Work unterstützen. Dies wird beispielsweise durch die Berücksichtigung verschiedener Feldbusse im Gesamtkonzept erreicht. Auch Einschränkungen der Hardware wie beispielsweise die fehlende Kommunikationsfähigkeit wird durch entsprechende Nachrüstkits basierend auf kostengünstigen Komponenten Rechnung getragen. Im Forschungsprojekt kommt ein RaspberryPi zum Einsatz, im Praxiseinsatz kann auch auf noch kleinere ARM basierte Systeme herunterskaliert werden.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
BETREUT VOM
PTKA Projektträger Karlsruhe
Karlsruher Institut für Technologie



Architektur für SecurePLUGandWORK (Quelle: Pflichtenheft Projekt SecurePLUGandWORK).

Literatur:
[1] Promotorengruppe Kommunikation der Forschungsunion Wirtschaft – Wissenschaft / acatech (Hrsg.): Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. April 2013
[2] http://www.vdi.de/technik/fachthemen/mess-und-automatisierungstechnik/fachbereiche/anwendungsfelder-der-automation/gma-fa-721-industrie-40/
[3] Pfrommer, J.; Schleipen, M.; Usländer, T.; Epple, U.; Heidel, R.; Urbas, L.; Sauer, O.; Beyerer, J.: Begrifflichkeiten um Industrie 4.0 – Ordnung im Sprachwirrwarr. In: Jumar, U.; Diedrich, C.: 13. Fachtagung EKA - Entwurf komplexer Automatisierungssysteme

CYBER-SECURITY IN KRITISCHEN INFRASTRUKTUREN

BEDROHUNGEN

Unsere heutige Welt ist ohne das reibungslose Funktionieren komplexer Infrastrukturen nicht vorstellbar. Diese umfassen Elektrizität, Öl, Gas und Wasser, aber auch Verkehr, Telekommunikation, Banken etc. Der Betrieb dieser Infrastruktursysteme wird kontrolliert und überwacht durch sog. SCADA Systeme, die Schwachstellen gegenüber einer Vielzahl von Bedrohungen aufweisen. Da der Begriff der Kritikalität in diesem Zusammenhang kein absoluter ist, lassen sich viele der folgenden Überlegungen auch auf die allgemeine IT-gestützte Automatisierungstechnik im Bereich der Prozess- und Fertigungstechnik anwenden.

Bislang wurde beim Entwurf und beim Aufbau von SCADA Systemen wenig Augenmerk auf IT Sicherheit gelegt. Kontrollsysteme waren elektronisch isoliert von allen anderen Netzwerken und deren Sicherheit beschränkte sich auf physische Sicherheit. Heute jedoch sind Kontrollsysteme vernetzt von der Feldebene über das Unternehmensnetzwerk bis hin zum Internet. Die Kontrollsysteme selbst waren früher proprietäre Lösungen. Heutige SCADA Systeme basieren auf offenen internationalen Standards wie Ethernet, TCP/IP und gängigen Hard- und Softwareprodukten und weisen dadurch die gleichen Angriffsflächen und Gefährdungen auf, die aus der klassischen Büro- und Heimumgebung bekannt sind.

BESONDERHEITEN DER SCADA INFRASTRUKTUREN

Wenn die Nutzung von offenen internationalen Standards und gängigen Hard- und Softwareprodukten die SCADA Systeme verletzlich machen, in welchem Maße lassen sich SCADA Systeme dann durch die klassischen Verfahren und Techniken der IT Security schützen? Welche Besonderheiten zeigen SCADA Systeme verglichen mit klassischen IT Systemen, die die klassische IT Security nicht anwendbar erscheinen lassen?

Patch Management ist eine zentrale Maßnahme zur Aufrechterhaltung der Integrität eines IT Systems und ist ein gutes Beispiel für die Besonderheiten von SCADA Systemen. Im Bereich der klassischen IT erfolgt die Aktualisierung der Software regelmäßig. In SCADA Systemen ist dies nicht durchführbar, da der Austausch von Softwarekomponenten umfangreiche Tests und eine Betriebsunterbrechung erfordert, die auf Grund der Verfügbarkeitsanforderungen nicht akzeptabel ist. Dies führt dazu, dass in SCADA Infrastrukturen sehr häufig überalterte Software angetroffen wird, deren Sicherheitsschwachstellen bekannt sind.

Die Lieferanten von Automatisierungskomponenten haben in den letzten Jahren begonnen, Sicherheitsfunktionalitäten in ihre Produkte zu integrieren bzw. separate Sicherheitskomponenten anzubieten (Firewalls, verschlüsselte Kommunikation, Integritätstests etc.). Es bleibt jedoch die Frage, wie existierende Altsysteme geschützt werden können, die nicht ersetzt werden können und die damit über keinen derartigen Selbstschutz verfügen.

LÖSUNGEN

Im Rahmen des FP7 Projekts PRECYSE (Prevention, Protection and Reaction to Cyber Attacks to Critical Infrastructures, Fördernummer FP7-SEC-2012-1-285181) werden Architekturen, Methodologien und Werkzeuge zum Schutz der IT Kom-

KONTAKT

Dipl.-Ing. Jörg Kippe

Sichere Kommunikationsarchitekturen (SKA)
Fraunhofer IOSB Karlsruhe

Telefon +49 721 6091-337
joerg.kippe@iosb.fraunhofer.de
www.iosb.fraunhofer.de/

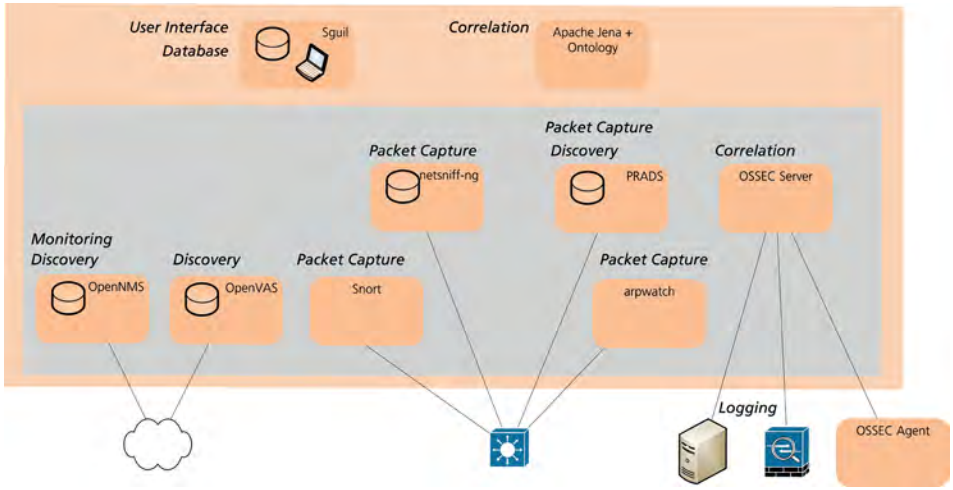


Abb. 1: Architekturschema des verteilten Monitoring und Intrusion Detection Systems.

ponenten kritischer Infrastrukturen erarbeitet. Im Bereich von Werkzeugen beschäftigen wir uns mit Überwachungs- und Detektionssystemen, die den Schutz von Systemen erlauben, die nicht durch direkte Maßnahmen geschützt werden können.

Eine einzelne Monitoring oder Intrusion Detection Komponente alleine kann immer nur einen bestimmten Ausschnitt an Informationen liefern. Ausgehend von dieser Überlegung verfolgen wir den Ansatz, ein verteiltes System von Monitoring und Intrusion Detection Komponenten, auf der Basis verfügbarer Open Source Produkte zu integrieren.

Die eingesetzten Komponenten lassen sich hinsichtlich der verwendeten Observationsverfahren sowie hinsichtlich der Art der erzeugten Ausgabedaten unterscheiden:

- Packet Capture: Packet Capture ist das Beobachten des gesamten Datenverkehrs im Netzwerk.
- Logging: Protokollierung der interne Abläufe sowie auftretender als Textmeldungen.
- Monitoring: Die Überwachung der Verfügbarkeit und Performance von Netzelementen, Endsystemen und Services.
- Discovery: Die Bestimmung der in einem Netzwerk vorhandenen Systemen und deren Eigenschaften – als auch die topologische Netzwerkstruktur.

Während die ersten beiden Verfahren direkt sicherheitsrelevante Informationen liefern können, generieren die beiden letzteren Metainformationen, die für die Analyse von Sicherheitsproblemen hilfreich sein können.

Besonderes Augenmerk ist auf die Art der erzeugten Ausgabedaten zu legen, wenn verschiedene Monitoring- und Detektions-Komponenten integriert werden sollen, ist es von Vorteil, entsprechende Standards, soweit vorhanden, zu benutzen:

- Alert Data: Am häufigsten treten Ereignismeldungen auf, mit denen sicherheitsrelevante Ereignisse angezeigt werden. (Datenformat: IDMEF [1]).
- Session Data: Diese beschreiben die Kommunikation zwischen zwei Systemen hinsichtlich Quelle, Ziel, Beginn- und Endzeitpunkt der Kommunikation sowie der Anzahl der ausgetauschten Pakete und Bytes (Datenformat: IPFIX [2]).
- Asset Data: Das ist die Beschreibung der vorhandenen Systeme, deren Eigenschaften und Schwachstellen (Datenformat ARF [3]).
- Statusinformationen und topologische Informationen: Hier existieren keine standardisierten Formate, deshalb verwenden wir eine private XML-Codierungen mit NETCONF [4] als Transportprotokoll.

Abb. 1 zeigt ein entsprechendes Architekturschema und die ausgewählten Open Source Komponenten, mit deren Hilfe das verteilte Monitoring- und Detektionssystem aufgebaut wurde. Die Basisinstallation bildet die Linux Distribution Security Onion, die um weitere Komponenten ergänzt ist, hierzu gehören:

- Snort
- Arpwatch
- netsniff-ng
- PRADS
- OSSEC
- OpenNMS
- OpenVAS
- Sguil

ZUSAMMENFASSUNG

Ein bekanntes Problem im Bereich der Intrusion Detection Systeme ist die große Anzahl sog. »False Positives«. Das sind Alarmmeldungen, die zwar irgendein verdächtiges Verhalten anzeigen, die aber keinem Angriff entsprechen. Aus diesem Grunde ist immer noch ein menschlicher Experte notwendig, der die eigentliche Ursache bestimmt. Entsprechend groß ist das Interesse an einfacheren Lösungen, bei denen die Auswertung weniger Fachwissen bedarf. Aus diesem Grunde verfolgen wir den Ansatz, Ontologie-basierte Schlussfolgerungskomponenten einzusetzen. Darüber berichtet ein separater Beitrag.

Literatur:

[1] Debar et.al.: RFC 4765: The Intrusion Detection Message Exchange Format. March 2007
[2] Claise, B.: RFC 5101: Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information. January 2008
[3] Halbardier, A.; Waltermine, D.; Johnson, M.: NIST Interagency Report 7694: Specification for the Asset Reporting Format 1.1. June 2011
[4] Enns, R. et.al.: RFC 6241: Network Configuration Protocol (NETCONF). June 2011

ONTOLOGIE-BASIERTE ERKENNUNG

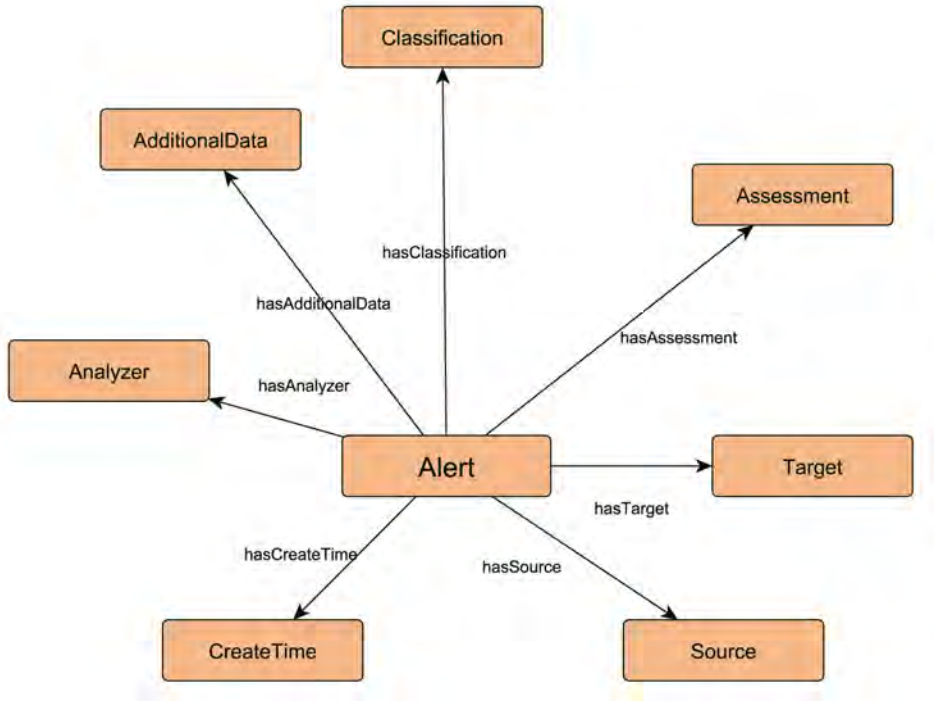


Abb. 1: Alarm-Ontologie [3].

MOTIVATION

SCADA-Systeme (Supervisory Control and Data Acquisition) steuern Produktionsanlagen, Verkehrs- oder Versorgungssysteme (z. B. Strom-, Wasserversorgung). Sie enthalten zunehmend Komponenten, die sie mit Systemen außerhalb ihres internen Netzwerkes verbinden. Dadurch sind sie jedoch auch durch externe Gefahren und Angreifer verwundbar. Um solche Angriffe zu erkennen und zu dokumentieren, gibt es bereits vielzählige Angriffserkennungssysteme (Intrusion Detection System, IDS). Die Aufgabe besteht nun in der einheitlichen Abbildung von Attacken sowie ihrer Weiterverarbeitung.

In Vorarbeiten zur Abbildung von Sicherheitsattacken in Ontologien stellten sich diese für den Zweck als geeignet heraus. Eine Ontologie ist hier eine formal geordnete Darstellung einer Menge von Begrifflichkeiten und der Beziehungen, die zwischen ihnen in einem bestimmten Themenbereich bestehen.

LÖSUNG MIT ONTOLOGIEN

Die erstellte Ontologie modelliert sowohl das SCADA-System als auch die Angriffe auf dieses und bildet Instanzen von Attacken darin ab. So lassen sich die von verschiedenen, bereits vorhandenen Sicherheitskomponenten eines SCADA-Systems erzeugten Sicherheitsreports unter Nutzung vorhandener Sprachstandards und Werkzeuge einheitlich abbilden und normalisieren. Dabei wurde darauf geachtet, nur Informationen zu berücksichtigen, die in jedem der verschiedenartigen Sicherheitsreports vorhanden und für die geplante Anwendung von Bedeutung waren. Wichtige Merkmale einer Sicherheitsattacke sind unter anderem die Art,

KONTAKT
Dr.-Ing. Christoph Thomalla

Informationsmanagement und Leittechnik (ILT)
Fraunhofer IOSB Karlsruhe

Telefon +49 721 6091-311
christoph.thomalla@iosb.fraunhofer.de
www.iosb.fraunhofer.de/ILT

VON CYBER-ATTACKEN

das Ziel und der Verursacher. Auftretende Probleme bei den verfügbaren Daten, ihrer einheitlichen Darstellung und Verknüpfung wurden gelöst. Bei der Erstellung der Ontologie konnten bereits vorhandene Sprachen und Werkzeuge genutzt werden.

Die Ontologie-Wissensbasis besteht aus vier Teilmodellen, der Alarm-, Angriffs-, System- und Vulnerability-Ontologie.

Die Alarm-Ontologie beschreibt Sicherheitswarnungen im IDMEF-Format angelehnt an [1]. Das Schema ist in Bild 1 abgebildet mit den Hauptelementen Analyzer – das Erkennungssystem, das den Alarm verursacht hat, zusätzlicher textlicher Beschreibung und des Alarmtyps. Dies kann ein Verweis auf einen Eintrag in der CVE-Datenbasis (Common Vulnerability Enumeration [2]) oder auf die Regel sein, die den Alarm getriggert hat. Assessment bewertet die Auswirkung auf das System. Target ist das Zielsystem, das von dem Alarm betroffen ist. Source ist das Quellsystem, das den Alarm ausgelöst hat.

Die Angriffs-Ontologie beschreibt Angriffe und stellt Ergebnisse des Reasoning-Prozesses dar.

Die System-Ontologie ist abgeleitet von der Topologie-Information des Ziel-Netzwerks, der Komponenten und Beziehungen. Die Hauptelemente sind die Netzwerk-Adresse des Systems, das Netzwerk, mit dem das System verbunden ist, der Dienst auf dem System, das Betriebssystem mit Versionsnummer und Lieferant und der Zweck des Systems.

Die Vulnerability-Ontologie beschreibt Schwachstellen von Systemkomponenten. Diese Information ist von der Asset-Information abgeleitet, die von der Vulnerability-Test-Komponente (OpenVAS) erzeugt wurde. Die Hauptelemente sind die Beschreibung der Schwachstelle, mögliche Gegenmaßnahmen, der Verweis auf den CVE-Eintrag, die Informationsquelle zu dieser Schwachstelle und der Teil des Zielsystems, auf den diese Schwachstelle sich bezieht.

Der Ontologie-Reasoner erlaubt zusätzliche Tatsachen über die modellierten Konzepte abzuleiten. Nachdem man sich von eingehenden Sicherheitswarnungen aus dem Netz vergewissert hat, erzeugt der Jena Reasoner [4] ein neues Modell, das weitere Informationen, abgeleitet durch regelbasiertes Reasoning, enthalten kann.

ANGRIFFSERKENNUNG

Die entwickelte Anwendung hält sicherheitsrelevante Ereignisse aus gelieferten Log-Files sowie Informationen über Systeme und deren Schwachstellen in Ontologien fest. Diese Ontologien wurden mit Daten frei verfügbarer Angriffserkennungssysteme initialisiert, um auf diesen Zusammenhänge zwischen verschiedenen Alarmen herzustellen und somit Angriffe zu erkennen sowie generell Alarme zu klassifizieren. Für das Werkzeug wurden Regeln erstellt und mit Hilfe von Schlussfolgerungen auf den Daten der Ontologien können zum einen ausführliche Ausgaben zu Bedrohungen protokolliert, aber auch konkrete Maßnahmen ergriffen werden. Neben einfachen Regeln für die Klassifikation wurden Regeln zur Erkennung von DOS-Attacken und für weitere Angriffe erstellt. Mit spezifischen Regeln für die Angriffserkennungssysteme können komplexe Angriffe auf SCADA-Systeme erkannt werden. Dies wurde in einer Reihe von Tests u.a. am Beispiel von Firewall-Regeln aufgezeigt, die Angreifern dann den weiteren Zugriff auf das System verwehren.

VORTEILE

Aus den Daten frei verfügbarer Angriffserkennungssysteme und Log-Files werden Zusammenhänge zwischen verschiedenen Alarmen hergestellt, um Angriffe zu erkennen sowie konkrete Gegenmaßnahmen zu ergreifen. Durch die Kombination ihrer Ergebnisse wird ihre Leistung gesteigert und selbst erstellte Regeln können auf ihre Wirksamkeit getestet werden, bevor sie Eingang in freie oder kommerzielle Systeme finden.

Die Entwicklung erfolgte im Rahmen des EU-Projekts PRECYSE (Prevention, protection and REaction to CYber attackS to critical infrastructurEs) mit der Fördernummer FP7-SEC-2012-1-285181. Mehr dazu steht in [5].

Literatur:
[1] Nora Cuppens-Boulahia, Frederic Cuppens, Fabien Autrel, and Herve Debar: An ontology-based approach to react to network attacks. Int. J. Inf. Comput. Secur. 3, 3/4 (January 2009), 280-305
[2] http://cve.mitre.org/
[3] Krauß, D.: Eine SCADA-spezifische Ontologie für kritische Infrastrukturen, Bachelor-Thesis, KIT, 2014
[4] http://jena.apache.org/
[5] Kippe, J.: Cyber-Security in kritischen Infrastrukturen, visIT 3, Fraunhofer IOSB, 2014

SICHERHEIT IST CHEFSACHE

BERICHT ZUM KARLSRUHER ACATECH-WORKSHOP »SICHERHEIT IST CHEFSACHE« DER THEMENNETZWERKE SICHERHEIT UND PRODUKTENTWICKLUNG & PRODUKTION IM JULI 2014

In der Deutschen Akademie der Technikwissenschaften, kurz acatech, engagieren sich führende Wissenschaftler, um aktuelle und längerfristig bedeutsame Themen im Dialog zu erarbeiten und so zu strukturieren, dass sie in politische Prozesse eingesteuert werden können. Hierzu werden Themennetzwerke (TN) geschaffen, die in regelmäßigen Treffen und gemeinsam initiierten Projekten interdisziplinär und doch fachlich fokussiert arbeiten. Das acatech-TN Sicherheit wird vom IOSB-Direktor Prof. Dr.-Ing. Jürgen Beyerer geleitet. In einer Kooperationsinitiative mit dem TN Produktentwicklung & Produktion unter Leitung von Prof. Dr.-Ing. Reiner Anderl, TU Darmstadt, fand am 3.7.14 am Fraunhofer IOSB in Karlsruhe der Workshop »Sicherheit ist Chefsache« statt, Leitthema: *Herausforderungen durch die neuen Paradigmen der Zukunftsprojekte »Smart Service Welt« und »Industrie 4.0« – Wir brauchen eine neue industrielle Sicherheitskultur!*

In der Vorbereitung erkannten die Teilnehmer, dass den Chancen von Industrie 4.0 viele noch offene Fragen gegenüber stehen, u. a. nach Implikationen und neuen Gefahren für die Sicherheit: der Produktion, der Produkte, des Menschen und der Unternehmen. Ziel der Veranstaltung war es, Projektideen zu skizzieren, um auf eine Auswahl der identifizierten Fragen gemeinsam praxistaugliche Antworten herauszuarbeiten, akzeptabel, effektiv und gleichzeitig Datenschutz- und Privatheitsbelangen Rechnung tragend. Hierfür wurden ca. 25 Wissenschaftler und Industrievertreter eingeladen. Nach acht Impulsvorträgen, u. a. aus den Blickwinkeln der industriellen Praxis, der Informationstechnik und der Rechtswissenschaften, definierten die Teilnehmer eine Reihe von Projektideen, aus denen drei zur Weiterverfolgung ausgewählt wurden: Wirtschaftlichkeit von Sicherheit, Resilienz (-Engineering) für die Produktion und – übergreifend – politische Handlungsempfehlungen. Im erstgenannten Thema soll bspw. erarbeitet werden, wie reale Kosten von Sicherheit abgebildet und die Sicherheits-Awareness bei Unternehmen gesteigert werden können. Im zweitgenannten Projekt, das unter Leitung des IOSB zu etablieren ist, soll u. a. eine Risikomodellierung im Kontext von Industrie 4.0 methodisch fundiert und die Wechselwirkung zwischen physikalischer und IT-Sicherheit betrachtet werden. Gemäß acatech-Ansatz wird die Projektarbeit mit effektiver Politikberatung und klaren Handlungsempfehlungen verbunden.

KONTAKT

Dr.-Ing. Andreas Meissner

Geschäftsfeld
Zivile Sicherheit
Fraunhofer IOSB Karlsruhe

Telefon +49 721 6091-402
andreas.meissner@iosb.fraunhofer.de
www.iosb.fraunhofer.de

IT-Sicherheit für Industrie 4.0

Aus betriebswirtschaftlicher Sicht bezeichnet Industrie 4.0 eine »neue Stufe der Organisation und Steuerung der gesamten Wertschöpfungskette über den gesamten Lebenszyklus von Produkten«. Beispielsweise soll durch Internet-basierte Überwachung weltweit installierter Anlagen und dedizierten Datenanalyseverfahren präventive Wartung ermöglicht werden, bevor eine Störung und damit ein Schaden auftritt. Dafür ist »die Verfügbarkeit aller relevanten Informationen in Echtzeit durch Vernetzung aller an der Wertschöpfung beteiligten Instanzen« notwendig [1]. Die Sicherstellung der IT-Sicherheit stellt die Software-Architekten allerdings vor eine Herausforderung. Wie kann erreicht werden, dass Informationen nur denjenigen Unternehmen (z. B. Wartungsdienstleistern) und Personen zugänglich sind, die dazu berechtigt sind? Und dies in der Form und Aggregationstiefe, die für ihre jeweilige Aufgabe angemessen ist? Welche Schutzmaßnahmen müssen ergriffen werden, damit die Befähigung für Fernwartung nicht gleichzeitig das Risiko für Cyber-Attacken und Industriesabotage und -spionage erhöht?

Wenn passgenaue Sicherheitsmechanismen nicht bereits systematisch beim Entwurf der Industrie 4.0- Software-Architekturen berücksichtigt werden (»Security by Design«), wird die Initiative bei den Anwendern kein Vertrauen genießen. Die Sicherheitsmechanismen sollen von den informationellen Schutzzielen eines Unternehmens abgeleitet werden, um die Handhabbarkeit zu gewährleisten und die Kosten nicht unnötig zu steigern.

Zusammen mit anderen Fraunhofer-Instituten (ESK, SIT, ISI) und der Industrie (u. a. Software AG, Bosch) erstellt das IOSB im Auftrag der SIRRIX AG eine entsprechende Studie für das Bundeswirtschaftsministerium. Gegenstand ist eine Analyse der IT-Sicherheitsanforderungen im Lichte der in den Gremien diskutierten Industrie 4.0 Szenarien und eine Spiegelung an bewährten IT-Sicherheitsstandards, ggf. aus anderen Anwendungsdomänen. Daraus soll der Handlungs- und Entwicklungsbedarf für Industrie 4.0 abgeleitet werden. Das IOSB wird die Ergebnisse unmittelbar in die Arbeiten zu einem Referenzmodell für eine Industrie 4.0 Referenzarchitektur einfließen lassen [2].

Referenzen:

[1] Plattform »Industrie 4.0«: Was »Industrie 4.0« (für uns) ist. http://www.plattform-i40.de/blog/was-industrie-40-für-uns-ist

[2] Usländer, T. (Ed.): Industrie 4.0 - Auf dem Weg zu einem Referenzmodell. VDI Statusreport. VDI / VDE-Gesellschaft Mess- und Automatisierungstechnik, Düsseldorf, April 2014. http://www.vdi.de/industrie40

KONTAKT

Dr.-Ing. Thomas Usländer

Informationsmanagement und Leittechnik (ILT)
Fraunhofer IOSB Karlsruhe

Telefon +49 721 6091-480
thomas.uslaender@iosb.fraunhofer.de
www.iosb.fraunhofer.de/ILT

Karlsruhe

Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung IOSB
Fraunhoferstraße 1
76131 Karlsruhe
Telefon +49 721 6091-0
Fax +49 721 6091-413
info@iosb.fraunhofer.de
www.iosb.fraunhofer.de

Ettlingen

Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung IOSB
Gutleuthausstr. 1
76275 Ettlingen
Telefon +49 7243 992-0
Fax +49 7243 992-299
www.iosb.fraunhofer.de

Ilmenau

Fraunhofer IOSB, Institutsteil
Angewandte Systemtechnik AST
Am Vogelherd 50
98693 Ilmenau
Telefon +49 3677 4610
Fax +49 3677 461-100
info@iosb-ast.fraunhofer.de
www.iosb-ast.fraunhofer.de

Lemgo

Fraunhofer IOSB-INA
Anwendungszentrum
Industrial Automation
Langenbruch 6
32657 Lemgo
Telefon +49 5261 702-572
Fax +49 5261 702-137
juergen.jasperneite@iosb-ina.fraunhofer.de
www.iosb-ina.fraunhofer.de

Beijing

Representative for Production and
Information Technologies
Unit 0610, Landmark Tower II
8 North Dongsanhuan Road
Chaoyang District
100004 Beijing, PR China
Telefon +86 10 6590 0621
Fax +86 10 6590 0619
muh@fraunhofer.com.cn