TeleTrusT – Bundesverband IT-Sicherheit e.V.

TeleTrusT-Workshop "Industrial Security" 2015

München, 11.06.2015

KMU-fokussierte Handlungsvorschläge zur Steigerung der IT-Sicherheit auf dem Weg zu Industrie 4.0

Michael Gröne
Sirrix AG security technologies

Ursprünge in der Spitzenforschung

- Gegründet 2005 als Spin-Off des Instituts für Kryptographie und Sicherheit am DFKI in Saarbrücken
- Heute High-Tech Produkthaus im IT-Sicherheitsbereich
- Teil des ROHDE & SCHWARZ Konzerns

Fokussierung auf Kernziele:

- Commercial-of-the-Shelf (COTS)-Systeme mit minimalem Aufwand für den behördlichen und den unternehmensweiten Einsatz sicher machen.
- Standardsysteme nachweisbar vertrauenswürdig machen

Sirrix AG heute

- Internationaler Technologieführer im Bereich „Trusted Infrastructures“

acatech – Deutsche Akademie der Technikwissenschaften

Deutschland Land der Ideen – Ausgewählter Ort 2012

Software-Cluster

TeleTrusT – Pioneers in IT security.

eurobits – Europäisches Kompetenzzentrum für IT-Sicherheit • Bochum

TRUSTED COMPUTING GROUP™

BITKOM

nrw·uniTS – IT-Sicherheit Nordrhein-Westfalen

Großer Preis des MITTELSTANDES – Oskar-Patzelt-Stiftung

Deloitte. Technology Fast 50 2012 Deutschland

Deloitte. Technology Fast50 2013

INNOVATIONSPREIS-IT SIEGER 2013 initiative mittelstand IT-SECURITY

INNOVATIONSPREIS-IT 2014 initiative mittelstand MITTELSTAND

IT-Sicherheit für die

Studie im Auftr

- Rechtliche Aspekte
  - z.B. Exportkon
- Technische Aspekte
  - z.B. Security by
- Organisatorische As
  - z.B. Technikint

Sirrix AG
security technologies

BOSCH

software AG

UNIVERSITÄT DES SAARLANDES

Fraunhofer SIT

Fraunhofer IOSB

Fraunhofer ESK

Fraunhofer ISI

Bundesamt für Sicherheit in der Informationstechnik

hgi Horst Görtz Institut für IT-Sicherheit

wts TAX LEGAL CONSULTING

esec

TRUMPF

BAYER Bayer Technology Services

BASF The Chemical Company

DKE VDE DIN

OPC FOUNDATION

TeleTrusT Pioneers in IT security. 1989 25 Jahre 2014

VDI|VDE|IT

DACHSER Intelligent Logistics

SIEMENS

ARBURG

Plattform INDUSTRIE 4.0

BITKOM

Expertenbeirat

SecurITy made in Germany

Kernfragestellungen der Studie

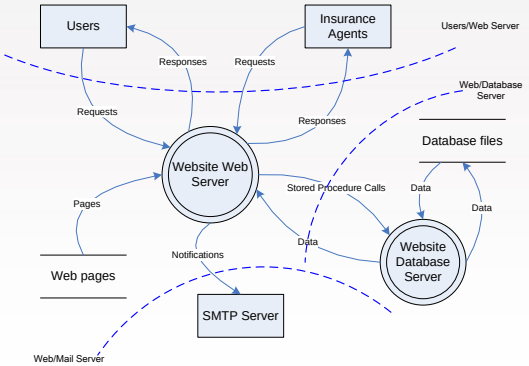
- Wie ist die **Ausgangslage** – Aktivitäten und Wissensbestände?
- Was sind die relevanten **Herausforderungen, Bedrohungen & Risiken**?
  - I4.0-spezifische Herausforderungen – auch in politischer Hinsicht - bei internationalen Datentransfers und länderübergreifenden Kooperationen
- Welche **Maßnahmen** und **Implementierungshindernisse** existieren?
- Welche neuartigen **Sicherheitskonzepte** sind notwendig?
- Welche **Handlungs-** und **Lösungsmöglichkeiten** (insb. für KMU) existieren?

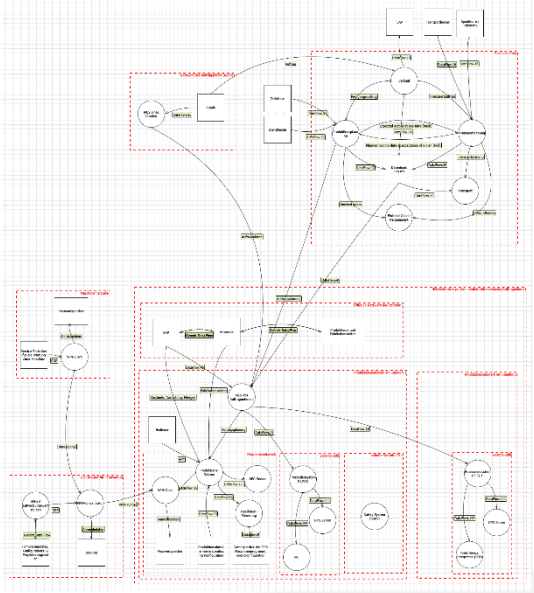
Risiken und Herausforderungen: Wesentliche Veränderungen durch I4.0

- Entstehung von unternehmensübergreifenden dynamischen Ad-hoc-Wertschöpfungsnetzwerken

- Hauptcharakteristika der I4.0-Wertschöpfungsketten:
  - Ablösung der klassischen Automatisierungspyramide
  - Verteilung der Wertschöpfungsprozesse auf verschiedene Akteure
  - Hohe Dynamik der Kooperationsdauer der im Wertschöpfungsprozess beteiligten Partner
  - Unterschiedliche technologische und auch organisatorische Ausstattung der Partner: kleine Unternehmen (wie z.B. ein 2-Mitarbeiter-Ingenierbüro) vs. Konzerne/Großunternehmen

Basis für erste vorläufige Handlungsvorschläge





Fallbeispiele

- Automobilbau – Inbetriebnahme produktionsrelevanter Echtzeitsysteme
- Maschinen- und Anlagenbau – Fernwartung
- Chemische Industrie – Netzwerksegmentierung in der Produktion
- Logistik – Integration von Logistikprozessen

Beschreibung von Systemgrenzen, Kommunikationsprozessen und Datenflüssen

Entwicklung von Datenflussmodellen

Integration eines Bedrohungs- und Risikomodells

SecurITy made in Germany

Basis für erste vorläufige Handlungsvorschläge

Schutzziele

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität

STRIDE-Analyse

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privileges

Bedrohungen:

- Konsolidiert: 26 relevante Bedrohungen, z.B. für
  - Prozesse im Rechenzentrum: Rechteausweitung; Verfügbarkeit (DoS-Angriffe)
  - Internetkommunikation: Unterbrechung von Datenflüssen über Unternehmensgrenzen
  - Produktion/Maschinenbetreiber: Angriffe auf Verfügbarkeit; Leugnung

Bedrohung	Eigenschaft	Definition
Spoofing	Authentifizierung	gefälschter Absender
Tampering	Integrität	Manipulation der Daten
Repudiation	Authentifizierung	Verweigern der Anerkennung
Information Disclosure	Vertraulichkeit	Datenkompromittierung
Denial of Service	Verfügbarkeit	Systemabstürze
Elevation of Privileges	Autorisierung	Benutzerrollenwechsel

SecurITy made in Germany

Erste Erkenntnisse - Technische Handlungsvorschläge

Industrial Rights Management

Handlungsempfehlung: Verschlüsselung sensibler Daten

Betrifft: Hersteller von Produktionsanlagen und Komponenten

Feststellung: Durch die Auswahl und den Einsatz verschlüsselungsfähiger Protokolle, können sensible Daten, wie z.B. Produktions- und Fabrikationsdaten, mittels symmetrischer und asymmetrischer Kryptografie geschützt werden.

Empfehlung: Bei der Planung und Entwicklung neuer Komponenten, Systeme und Anlagen sollte wo immer möglich eine Verschlüsselung von sensiblen Daten entsprechend der jeweiligen Sicherheitsarchitektur vorgesehen werden.

Erste Erkenntnisse - Technische Handlungsvorschläge

Industrial Rights Management

Handlungsempfehlung: Integritätsprüfungen

Betrifft: Hersteller von Produktionsanlagen und Komponenten

Feststellung: Die Integrität von Hard- und Softwarekomponenten ist eine wichtige Voraussetzung für eine sinnvolle Verwendung von Verschlüsselungstechnologien.

Empfehlung: Bei der Planung und Entwicklung neuer Komponenten, Systeme und Anlagen sollten Möglichkeiten zur Integritätsprüfung während der Boot- und Laufzeit geschaffen werden.

Erste Erkenntnisse - Technische Handlungsvorschläge

Industrial Rights Management

Handlungsempfehlung: Hardware-basierte Sicherheitsanker

Betrifft: Hersteller von Komponenten

Feststellung: Hardware-Sicherheitsanker in allen Endgeräten stellen eine sinnvolle Basis für zukünftige Sicherheitskonzepte für Automatisierungskomponenten und Produktionsanlagen dar.

Empfehlung: Bei der Planung und Entwicklung neuer Komponenten sollte ein 'hardware-basierter Sicherheitsanker' vorgesehen werden, wie z.B. das in der Office-IT etablierte Trusted Platform Module (TPM), Smartsards, HSM.

Erste Erkenntnisse - Technische Handlungsvorschläge

Production Line IT-Security Monitoring

Handlungsempfehlung: Entwicklung von Anomalieerkennungssystemen

Betrifft: Hersteller und Betreiber von Produktionsanlagen und Komponenten

Feststellung: Neue, adaptive Verfahren notwendig, welche IT-Systeme nicht isoliert betrachten, sondern zielgerichtet den Produktionsprozess selbst schützen. Es müssen neue Methoden gefunden werden, um die IT-Landschaft der Produktion im laufenden Betrieb einer Analyse und Absicherung zu unterziehen, ohne die primären Schutzziele zu gefährden.

Empfehlung: Die Forschung und Entwicklung an intelligenten, kombinierten und adaptiven Anomalieerkennungssystemen („Produktionsprozess-malwarescanner“) sollte intensiviert werden.

SecurITy made in Germany

Erste Erkenntnisse - Organisatorische Handlungsvorschläge

Technikintegration

Handlungsempfehlung: Anerkennung der sich verändernden Bedrohungslage und Bewertung des Nutzen-Risiko-Verhältnisses bei Veränderungen

Betrifft: Betreiber von Produktionsanlagen und Komponenten (insb. KMU)
Feststellung: Wenig Bewusstsein für die sich durch Technikintegration verändernde Bedrohungslage (Überprüfung etablierter Praktiken auf Angemessenheit; Integration neuer Technik ohne eingehende Prüfung)
Empfehlung: Integrierte Abschätzung von technischen und organisatorischen Folgen der Integration neuer Techniken in bestehende Prozesse (Eignung für die Industrie 4.0 und Nutzen-Risiko-Verhältnis).

Erste Erkenntnisse - Organisatorische Handlungsvorschläge

Vertrauen

Handlungsempfehlung: Top-down-Förderung von Vertrauen in das Konzept und die Vision I4.0 - Kommunikation des Commitments der Geschäftsführung

Betrifft: Unternehmen (insb. KMU)
Feststellung: Unternehmen fällt es mitunter schwer grundlegendes Vertrauen in das Konzept oder die Vision von Industrie 4.0 zu schaffen.
Empfehlung: Wandel als zentrales Innovationsthema im Unternehmen verstehen und auch so zu kommunizieren. Top-down. Kommunikation des Commitments der Geschäftsführung. Positive Erfahrungsberichte aus anderen Unternehmen und Industriezweigen können den Prozess der Vertrauensbildung unterstützen.

VIELEN DANK!

Michael Gröne, M.Sc.
Senior Projektmanager und Consultant
Sirrix AG security technologies
Lise-Meitner-Allee 4
44801 Bochum

Tel +49 (0)681/95986-0
Fax +49 (0)681/95986-500

Email info@sirrix.com
Web www.sirrix.com