hochschule mannheim

Sicherheitsanalyse der Netzwerkkommunikation in Industrie 4.0 Umgebungen und Erweiterung einer prototypischen Industrie 4.0 Security Testumgebung um Funktionalitäten im Bereich der Netzwerksicherheit

Philipp Minges

Bachelor-Thesis

zur Erlangung des akademischen Grades Bachelor of Science (B.Sc.)

Studiengang Informatik

Fakultät für Informatik

Hochschule Mannheim

15.07.2018

Betreuer

Prof. Sachar Paulus, Hochschule Mannheim

TODO - Zweitkorrektor

Minges, Philipp:
Sicherheitsanalyse der Netzwerkkommunikation in Industrie 4.0 Umgebungen und Erweiterung einer prototypischen Industrie 4.0 Security Testumgebung um Funktionalitäten im Bereich der Netzwerksicherheit / Philipp Minges. –
Bachelor-Thesis, Mannheim: Hochschule Mannheim, 2018. 7 Seiten.

Minges, Philipp:
TODO - Title EN / Philipp Minges. –
Bachelor Thesis, Mannheim: University of Applied Sciences Mannheim, 2018. 7 pages.

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Ich bin damit einverstanden, dass meine Arbeit veröffentlicht wird, d. h. dass die Arbeit elektronisch gespeichert, in andere Formate konvertiert, auf den Servern der Hochschule Mannheim öffentlich zugänglich gemacht und über das Internet verbreitet werden darf.

Mannheim, 15.07.2018

Philipp Minges

Abstract

Sicherheitsanalyse der Netzwerkkommunikation in Industrie 4.0 Umgebungen und Erweiterung einer prototypischen Industrie 4.0 Security Testumgebung um Funktionalitäten im Bereich der Netzwerksicherheit

Nach der Einführung des Begriffs „Industrie 4.0“ im Jahr 2011 und dem gleichzeitigen Start der 4. industriellen Revolution werden Kommunikationsnetze in der Industrie immer mehr zur Automatisierung der Produktion von Gütern oder zum unternehmensinternen sowie -externen Datenaustausch genutzt. Um diese Echtzeitkommunikation oder auch Möglichkeiten der Fernwartung zu gewährleisten, werden immer mehr Anlagen mit Netzwerkzugängen ausgestattet. Die Kommunikation der Industrie 4.0 Netze und Systeme findet unternehmensübergreifend über einen unsicheren Kanal statt und kann somit ohne bereitgestellte Sicherheitsmaßnahmen genauso angegriffen werden, wie herkömmliche Heim- oder Büronetzwerke. Das Ziel dieser Arbeit ist es zum einen, die Netzwerkkommunikation zwischen Industrie 4.0 Komponenten anhand aktueller Standards zu analysieren, mögliche Angriffsvektoren darzustellen und deren Eintrittswahrscheinlichkeit sowie Schaden zu bewerten. Zum anderen wird ein vorhandenes Industrie 4.0 Security Testsystem anhand der gewonnenen Erkenntnisse im Bereich der Netzwerksicherheit zu Lehr- und Testzwecken prototypisch erweitert.

TODO - Title EN

TODO - Abstract EN

Inhaltsverzeichnis

Kapitel 1

Einleitung

Mit der heutigen, immer weiter fortschreitenden Vernetzung von Geräten aus Unternehmensinfrastrukturen und Heimnetzen über das Internet, erfährt die Industrie und deren Wertschöpfung einen strukturellen Wandel. Im Gegensatz zur Industrie 3.0, in der die Kommunikation der Geräte nur innerhalb einer Produktionsstätte oder eines Unternehmens stattgefunden hat, erstreckt sich die Kommunikation in Industrie 4.0 Umgebungen über die Unternehmensgrenzen hinweg. Es werden Konzepte zur Einbindung aller Komponenten eines Firmenprozesses, welcher z. B. Produktion, Service- Instandhaltungsaufgaben beinhaltet, realisiert. Diese Systeme kommunizieren miteinander und nutzen dafür immer häufiger eine Ethernet Netzwerkwerkstruktur. Dies setzt die Produktionsanlagen sowie die genutzten Softwaresysteme den gleichen potentiellen Gefahren durch Viren, Würmer oder Trojaner aus, wie reguläre Büro- oder Heim-PC.

Viele Kritische Infrastrukturen (KRITIS), wie Produktionsanlagen zur Energie- und Wasserversorgung nutzen automatisierte Prozesssteuerungssysteme, Industrie-PC (IPC), speicherprogrammierbare Steuerungen (SPS) und Supervisory Control and Data Acquisition (SCADA) Systeme zur Steuerung der Abläufe in den Produktionsanlagen zwischen verteilten Systemen. Die ständige Verfügbarkeit und Überwachung dieser Dienste ist für eine funktionierende Infrastruktur essentiell. Systeme der KRITIS können nicht angehalten werden, um Sicherheitsupdates und einen anschließenden Systemneustart durchzuführen. Bei vielen dieser Prozesssteuerungssystemen wurde der Aspekt der IT-Sicherheit nicht berücksichtigt, da eine Vernetzung der Systeme im heutigen Ausmaß nicht vorgesehen war. Die Systeme bieten keine Möglichkeit der Verschlüsselung des Datenverkehrs oder der Authentifizierung der Benutzer.

Die Sicherheit der Produktionsanlagen und deren Netzwerkkommunikation spielt für ein Unternehmen im Industrie 4.0 Umfeld mit Hinblick auf Verfügbarkeit, Zuverlässigkeit und Authentizität eine essentielle Rolle. Sollte es durch Angriffe möglich sein, die Produktion zu sabotieren oder Anlagen und Systeme zu manipulieren, so können die Folgen schwerwiegend sein. Es kann zu Produktionsausfällen kommen und es können Vertragsstrafen drohen. Ein bekannter Angriff wurde im Jahr 2016 auf das Netz des deutschen Bundestages durchgeführt. Dort wurde ein Zusammenbruch der getroffenen Sicherheitsmaßnahmen erreicht. Es wurden über mehrere Monate unbemerkt sensible Daten entwendet. [TODO - Quelle]

TODO - Stuxnet -> auf Produktionsanlagen zugegriffen

Die beschriebenen Probleme bei der Umsetzung einer sicheren Kommunikation im Industrie 4.0 Umfeld sowie die dargestellten, erfolgreich durchgeführten Angriffe auf bestehende Infrastrukturen bieten mir einen Anlass, den aktuellen Stand der IT-Sicherheit beim Datenaustausch in einer heterogenen Industrie 4.0 Umgebung zu analysieren und mögliche Risiken aufzuzeigen.

Um das erwünschte Ergebnis zu erhalten, muss im ersten Schritt eine Literaturanalyse durchgeführt werden. Mit Hilfe dieser werden die Grundlagen zur Analyse der Kommunikation geschaffen.

Anschließend wird die Sicherheitsanalyse der Netzwerkkommunikation in Industrie 4.0 Umgebungen durchgeführt. Diese beinhaltet die Analyse des Kommunikationsstacks der Netzwerkebene und der verwendeten Protokolle sowie Standards.

Zuletzt werden die Ergebnisse der Analyse durch eine prototypische Implementierung und Erweiterung eines vorhandenen Industrie 4.0 Security Testsystems dargestellt und validiert.

TODO W.A. Halang 2016 und Bundesministerium für Wirtschaft und Energie 2016

Kapitel 2

Grundlagen

2.1 Historie

Industrie 3.0 -> Industrie 4.0 - Kommunikation über Unternehmensgrenzen, Kommunikation nicht mehr über ERP und MES sondern direkt von unteren Schichten, wie z.B. Maschinen oder Komponenten

2.2 Die 4. industrielle Revolution

2.2.1 Automatisierungspyramide

2.2.2 Schichtenmodell

2.3 Grundprinzipien der sicheren Kommunikation

2.3.1 Vertraulichkeit/Zugriffsschutz

2.3.2 (Daten-)Integrität/Änderungsschutz

2.3.3 Authentizität/Fälschungsschutz

2.3.4 Verbindlichkeit/Nichtabstreitbarkeit

2.3.5 Anonymität

Für diese neuen Szenarien gelten weiterhin die klassischen Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit.

Des Weiteren werden Bestellungen oder Logistikprozesse durch I4.0 Kommunikation abgewickelt. Diese stellen einen rechtlichen Rahmen dar, welcher weitere Schutzziele beinhaltet:

TODO – Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Nichtabstreitbarkeit, Verbindlichkeit, Zurechenbarkeit

2.4 Kommunikation in Industrie 4.0

Im Gegensatz zur I3.0, in welcher Daten auf lokaler Ebene oder zwischen einzelnen internen Unternehmensebenen ausgetauscht wurden, stellt in der I4.0 der Austausch von Daten und Informationen über Unternehmensgrenzen hinweg eine wesentliche Herausforderung dar. Dabei findet die Kommunikation nicht mehr über ein Enterprise-Resource-Planning-System (ERP) statt, sondern auch direkt von einer darunterliegenden Ebene, wie z. B. einer Maschine mit ihrem Lieferanten. Durch diese enge Vernetzung können sowohl Menschen, als auch Maschinen die Kommunikationspartner sein.

2.4.1 Anforderungen

2.4.2 Komponenten einer I4.0 Architektur

2.4.3 Kommunikationsstrukturen

End2End

Gateways

Publish-Subscribe

Kommunikation mit Netzwerk als Partner

Kapitel 3

Analyse

3.1 Probleme bei Migration alter Systeme

3.2 Sicherheitsanforderungen des Kommunikationsstacks

3.2.1 Physical Layer

3.2.2 Data Link Layer

3.2.3 Network Layer

3.2.4 Transport Layer und End2End Security

3.2.5 Prozess- und Businesslogik - Application Layer

3.3 Protokollstandards

3.3.1 OPC UA

3.3.2 MConnect

3.3.3 TODO

3.4 Angriffsvektoren

3.4.1 Verschlüsselung

3.4.2 Paketversand

3.4.3 TODO

3.5 Auswertung der Ergebnisse

3.6 Maßnahmenkatalog

Kapitel 4

Implementierung

Abkürzungsverzeichnis

KRITIS Kritische Infrastrukturen

IPC Industrie-PC

SPS speicherprogrammierbare Steuerungen

SCADA Supervisory Control and Data Acquisition

Tabellenverzeichnis

Abbildungsverzeichnis

Listings

Literatur

Bundesministerium für Wirtschaft und Energie, BMWi (2016). „Technischer Überblick: Sichere unternehmensübergreifende Kommunikation“. In:

W.A. Halang, H. Unger (Hrsg.) (2016). *Internet der Dinge*. Springer Vieweg.