FHS St.Gallen
Hochschule
für Angewandte Wissenschaften

Abstract

Titel: IT Security Ansätze in Industrie 4.0 für KMU

Kurzzusammenfassung: Begriff Industrie 4.0 drang erstmals im Jahr 2011 an die Öffentlichkeit. Kaum ein anderes Thema ist in den vergangenen Jahren in der Industriebranche so oft diskutiert worden. Industrie 4.0 verspricht immense Vorteile durch die Integration und Automatisierung über die Prozessgrenzen hinweg. Die dazu nötige IT-Durchdringung und Vernetzung der Anlagen bringt hohe Risiken mit sich. Es gibt bereits viele Ansätze und Rahmenwerke über IT-Security. Es handeln sich dabei um umfangreiche und aufwendige Werke. Für KMU stellt sich die Frage, ob die nötigen Ressourcen vorhanden sind, um diese Werke vollumfänglich umzusetzen. Die Bachelorarbeit untersucht nun diese Ansätze und ihre Massnahmen auf KMU-Tauglichkeit.

Verfasser/-in: Raffael Wettach

Herausgeber/-in: **Prof. Dr. Christian Thiel**

Publikationsformat:
☒ BATH
☐ MATH
☐ Semesterarbeit
☐ Forschungsbericht
☐ Anderes

Veröffentlichung (Jahr): 2017

Sprache: Deutsch

Zitation: Wettach, R. (2017). *IT Security Ansätze in Industrie 4.0 für KMU.* (Unveröffentlichte Bachelor Thesis). FHS St. Gallen, Hochschule für angewandte Wissenschaften.

Schlagwörter (3-5 Tags): IT Security, Industrie 4.0, KMU

Ausgangslage

Die Vision Industrie 4.0 beschreibt die Szenerie der totalen IT-Durchdringung aller Schritte entlang der Wertschöpfungskette. Die Vernetzung der Produktionsanlagen entwickelte sich in den letzten Jahren rapide. Das Thema IT-Security wurde dabei vernachlässigt. Es gibt nun erste Ansätze wie man im Sicherheitsmanagement die Trennung von Office- und Fertigungs-IT überwinden kann. Es handelt sich dabei aber um umfangreiche und aufwendige Rahmenwerke. Es ist fraglich, ob KMU die Ressourcen und Möglichkeiten haben, diese vollumfänglich umzusetzen. Falls nicht stellt sich die Frage nach Alternativen.

Ziele

Inwieweit sind bestehende IT-Security Ansätze und Rahmenwerke für KMU mit Fokus auf Industrie 4.0 durchführbar und gibt es daraus abgeleitet, sinnvolle IT-Security-Massnahmen die umgesetzt werden können?

Ziel 1: Erhebung und Erstellung einer „State of the Art"-Übersicht zu bestehenden Ansätzen und Rahmenwerken im Allgemeinen und im Kontext von KMU und Industrie 4.0.

Ziel 2: Analyse der erhobenen „State of the Art" Ansätze und Rahmenwerke (vgl. Ziel 1) anhand von klar definierten Bewertungskriterien, welche auf die Bedürfnisse von KMUs abgestimmt sind.

Ziel 3: Empfehlung eines Frameworks, einer Kombination mehrerer Frameworks oder eigene begründete Handlungsvorschläge zur Durchführung von IT-Security-Massnahmen für KMUs in Industrie 4.0 auf Basis der in Ziel 1 und 2 gewonnenen Erkenntnisse

Methodik

Der Verfasser erarbeitete sich in einem ersten Schritt einen Überblick über verschiedenste Ansätze und Rahmenwerke, welche Informationssicherheitsaspekte behandeln. Folgend wurde eine „State of the Art"-Übersicht mittels Internetrecherche und Dokumentenstudium erarbeitet. Die wesentlichsten Aspekte und Eckdaten wurden tabellarisch zusammengefasst. Anhand der „State of the Art"-Übersicht konzipierte der Verfasser drei Kategorien. Die Ansätze und Rahmenwerke wurden den drei Kategorien zugeteilt. Anschliessend wurden die Kategorien anhand von spezifischen Kriterien auf KMU-Tauglichkeit analysiert. Ansätze und Werke aus den verbleibenden Kategorien wurden weiter auf KMU-Tauglichkeit überprüft. Dies setzte

der Verfasser anhand einer Nutzwertanalyse um. Basieren auf den Resultaten der Nutzwertanalyse wurden die am besten bewerteten Ansätze und Rahmenwerke kritisch diskutiert und dementsprechend Handlungsempfehlungen ausgearbeitet. Aufgrund gewonnener Erkenntnisse aus der Nutzwertanalyse und den Handlungsempfehlungen, wurden die Massnahmen gewisser Ansätze und Rahmenwerke miteinander verglichen. Basierend auf diesem Vergleich ermittelte der Verfasser die wichtigsten Massnahmenbereiche und bereitete diese tabellarisch auf.

Ergebnisse

„State of the Art"-Übersicht

In der „State of the Art"-Übersicht wurden 28 Ansätze und Rahmenwerke von 8 verschiedenen Herausgebern beschrieben.

Bundesamt für Sicherheit in der Informationstechnik
- BSI-Standard 100-1
- BSI-Standard 100-2
- BSI-Standard 100-3
- BSI-Standard 100-4
- IT-Grundschutz-Kataloge
- ICS-Security Top 10 Bedrohungen
- LARS ICSICS-Security-Kompendium
- IT-Grundschutz Profil klein
- IT-Grundschutz Profil mittel
- IT-Grundschutz Profil gross
- Webkurs IT-Grundschutz
- Leitfaden Informationssicherheit

ISO/IEC
- ISO/IEC 27000
- ISO/IEC 27001
- ISO/IEC 27002
- ISO/IEC 27003
- ISO/IEC 27004
- ISO/IEC 27005
- ISO/IEC 62443

Information System Audit and Control Association
- COBIT 5 for Information Security

Melde- und Analysestelle Informationssicherung
- Merkblatt IT-Sicherheit für KMUs
- Massnahmen zum Schutz von Industriellen Kontrollsystemen
- Massnahmen zum Schutz von Content Management Systemen

Information Security Society Switzerland (ISSS)
- Mehr Informationssicherheit für Klein- und Mittelbetriebe

Bundesministerium für Wirtschaft und Energie
- Leitfaden IT-Security in der Industrie 4.0

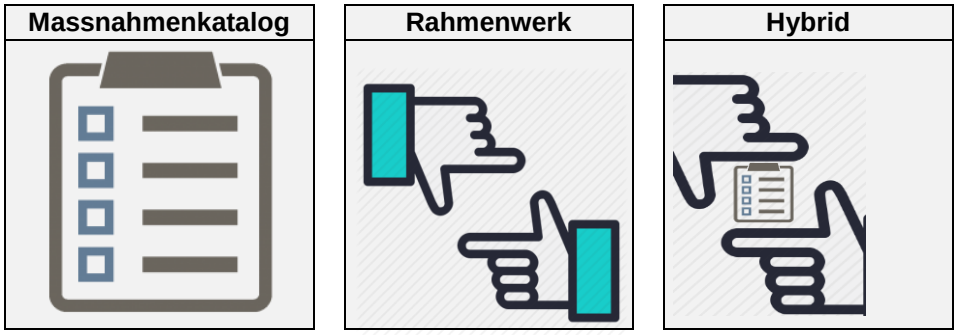
Verband Deutscher Maschinen- und Anlagenbau
- Leitfaden Industrie 4.0 Security
- Leitfaden Industrial Security: IEC 62443

VDI/VDE
- VDI/VDE 2182 Richtlinie

Die „State of the Art"-Übersicht wurde tabellarisch zusammengefasst mit den wichtigsten Aspekten und Eckdaten: Herausgeber, Inhalt, Einordnung, Zielgruppe, Vorausgesetzte Kenntnisse, Aufbau/Umsetzung, Sprache, Zertifizierung, Seitenzahl, Erscheinungsjahr.

Analyse der Kategorien

Der Verfasser hat die Ansätze und Rahmenwerke kategorisiert. Dazu wurden drei verschiedene Kategorien konzipiert.



Die Analyse der Kategorien hat gezeigt, dass die Publikationen aus der Kategorie Rahmenwerk nicht gut für KMU geeignet sind Gründe dafür sind unter anderem die Komplexität, fachspezifisches Vokabular, zu grosser Umfang usw. Aus diesem Grund wurden diese Publikationen im weiteren Verlauf der Analyse nicht mehr berücksichtigt.

Analyse der einzelnen Werke

Die Auswertung der Nutzwertanalyse hat gezeigt, dass die IT-Grundschutz-Kataloge, der Leitfaden Industrie 4.0 Security, das ICS-Security-Kompendium und LARS ICS das Spitzenfeld der Nutzwertanalyse bilden.

Schlussfolgerungen

Empfehlungen auf Basis der Nutzwertanalyse

Soll anhand eines einzelnen Werkes möglichst viel erreicht werden, empfiehlt es sich das Softwaretool LARS ICS umzusetzen. Aus dem Grund, da das LARS ICS dem Nutzer in einem ersten Schritt hilft die eigene Sicherheitssituation zu analysieren und mögliche Schwachstellen aufzudecken. In einem zweiten Schritt werden mögliche Massnahmen aufgezeigt, die helfen die Schwachstellen zu schützen.

Empfehlungen der wichtigsten Massnahmenbereiche

Aus mangelnder Zeit und knappen Ressourcen können meist nicht alle Massnahmen der Werke umgesetzt werden. Aus diesem Grund wurden die wichtigsten Massnahmenbereiche identifiziert und in einer Tabelle zusammengefasst. Ein KMU sollte sich zuerst um diese Bereiche kümmern:

- Schulung / Sensibilisierung zur Informationssicherheit
- Backupkonzept
- Berechtigungskonzept
- Patchmanagement
- Authentisierung
- Virenschutz
- Risikoanalyse
- Verantwortlichkeiten (Organisationsstruktur)
- Logging/Monitoring
- Netzsegmentierung
- Firewall
- physischer Schutz
- Sicherheitsvorfälle
- Verwalten und Entsorgen von Datenträgern

Wichtigste Literaturquellen

Bundesamt für Sicherheit in der Informationstechnik [BSI]. (2016b). *IT-Grundschutz-Kataloge. 15. Ergänzungslieferung-2016.* Gefunden am 23.03.2017 unter https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf

Bundesamt für Sicherheit in der Informationstechnik [BSI]. (2008a). *BSI-Standard 100-1. Managementsysteme für Informationssicherheit (ISMS).* Gefunden am 24.03.2017 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1001.pdf?__blob=publicationFile&v=1

Bundesministerium für Wirtschaft und Energie [BMWi]. (2016a). *Leitfaden IT-Security in der Industrie 4.0: Handlungsfelder für Betreiber* [elektronische Version]. Berlin: Autor

Bundesamt für Sicherheit in der Informationstechnik [BSI]. (2013). *ICS-Security-Kompendium*. Gefunden am 24.03.2017 unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=2

Bundesamt für Sicherheit in der Informationstechnik [BSI]. (Ohne Datum c). *LARS ICS. Light and Right Security ICS – Benutzerhandbuch.* Gefunden am 09.02.2017 unter https://www.bsi.bund.de/ACS/DE/_/zusatzinfos_ange-

bote/141124_Hand-buch_LARS.pdf;jsessinid=BA97A34772731E8C49FCE8C6E4C6FD2A.1_cid341?__blob=publicationFile&v=1