Cybersecurity in der vernetzten Produktion

Studie zu IT-Sicherheit in produzierenden Unternehmen

Raphael Kiesel, Jan Dering und Robert H. Schmitt

Die Vernetzung und Digitalisierung bringt ein enormes Wachstumspotenzial mit sich und wird in den kommenden Jahren elementar für den Wirtschaftsstandort Deutschland sein. Die Bedenken hinsichtlich der IT-Sicherheit sind für viele Unternehmen derzeit jedoch ein maßgebliches Hindernis für eine Umsetzung der Digitalisierung. Aus diesem Grund wurde im Rahmen einer Studie am Fraunhofer-Institut für Produktionstechnologie IPT ein ganzheitlicher Production Security Readiness Check (PSRC) entwickelt, der produzierenden Unternehmen aufzeigt, welches Sicherheitsniveau sie aktuell erfüllen.

- ✓ Potenziale der IT-Sicherheit in der vernetzten Produktion
- ✓ Unternehmensbereiche, die von IT-Sicherheit betroffen sind
- ✓ Möglichkeiten zur Bestimmung des IT-Sicherheitsniveaus in der Produktion

126 Milliarden Euro zusätzlich an Wertschöpfung bis 2025 – auf diese Höhe beziffert McKinsey das Potenzial durch konsequente Digitalisierung produzierender Unternehmen in Deutschland [1, 2]. Im Jahr 2018 erbrachte das produzierende Gewerbe über ein Viertel des gesamten deutschen Bruttoinlandsprodukts [3]. Trotz des großen Wachstumspotentials liegt die Digitalisierungsrate in der Produktion von deutschen Großunternehmen erst bei knapp 30 Prozent (KMU bei 20 Prozent) [4]. Eines der maßgeblichen Vernetzungshemmnisse ist die Cybersicherheit [5]. Ging es bisher primär um die funktionale Sicherheit der Produktionsanlagen, so rückt nun die Cybersicherheit bedingt durch den Wandel von geschlossenen zu offenen cyberphysischen Systemen (CPS) immer mehr in den Vordergrund. Neben dieser zusätzlichen Herausforderung müssen Unternehmen weitere Aufgaben, die sich aus langen Anlagenlebenszyklen (z. B. fehlende Updates), dem Einsatz von unsicheren Netzwerk-Protokollen sowie den unzureichenden Patch-Policies ergeben, bewältigen.

Aus diesen Gründen wurde im Rahmen einer Studie am Fraunhofer-Institut für Produktionstechnologie ein ganzheitlicher Production Security Readiness Check (PSRC) auf Basis aktueller Normen, Standards und Guidelines entwickelt, welcher produzierenden Unternehmen aufzeigt, auf welchem Sicherheitsniveau sie sich aktuell befinden und welchem Risiko sie ausgesetzt sind. Basierend auf dem Sicherheitsniveau des Unternehmens können aus dem PSRC zudem Handlungsoptionen abgeleitet werden.

Was gilt es zu schützen?

Elektronische Informationen sind zu schützende Güter. Dabei sind insbesondere drei Ziele zu verfolgen: Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Systeme. So ist sicherzustellen, dass sensible Informationen nicht an unbefugte Personen gelangen (Vertraulichkeit) oder von unautorisierten Dritten verändert werden können (Integrität). Parallel soll der Zugang zu Informationen im besten Fall dauerhaft gewährleistet werden (Verfügbarkeit).

Industrielle Produktion aus Perspektive der IT

Die verschiedenen Bereiche der heutigen industriellen Automatisierung werden in der Pyramide (Bild 1) dargestellt. Die dort veranschaulichten Ebenen im Unternehmen stehen in einem Kommunikationsverhältnis zueinander. Die fortschreitende Vernetzung innerhalb der Produktion führt dazu, dass IT-(Information Technology) und OT-(Operational Technology) Netzwerke miteinander verschmelzen. Produktionsanlagen, die früher isoliert mit proprietären Protokollen in der IACS-Le (Industrial Automation and Control Systems) Umgebung betrieben wurden, übernehmen heute Netzwerkprotokolle der IT-Netzwerke. Schwachstellen existieren in jeder einzelnen Ebene der Automatisierungspyramide: In einer von FireEye publizierten Studie im Jahr 2016 betrafen mehr als die

Raphael Kiesel ist Gruppenleiter für das Themenfeld Vernetzte Produktions-IT am Fraunhofer IPT in Aachen und managt die Community des „International Center for Networked, Adaptive Production".

Jan Dering war Masterand im Bereich Vernetzte Produktions-IT der Abteilung Produktionsqualität am Fraunhofer IPT.

Prof. Dr.-Ing. Robert H. Schmitt leitet den Lehrstuhl für Fertigungsmesstechnik und Qualitätsmanagement an der RWTH Aachen und ist Mitglied im Direktorium des Fraunhofer IPT.

www.ipt.fraunhofer.de

https://doi.org/10.30844/FS19-4_21-24

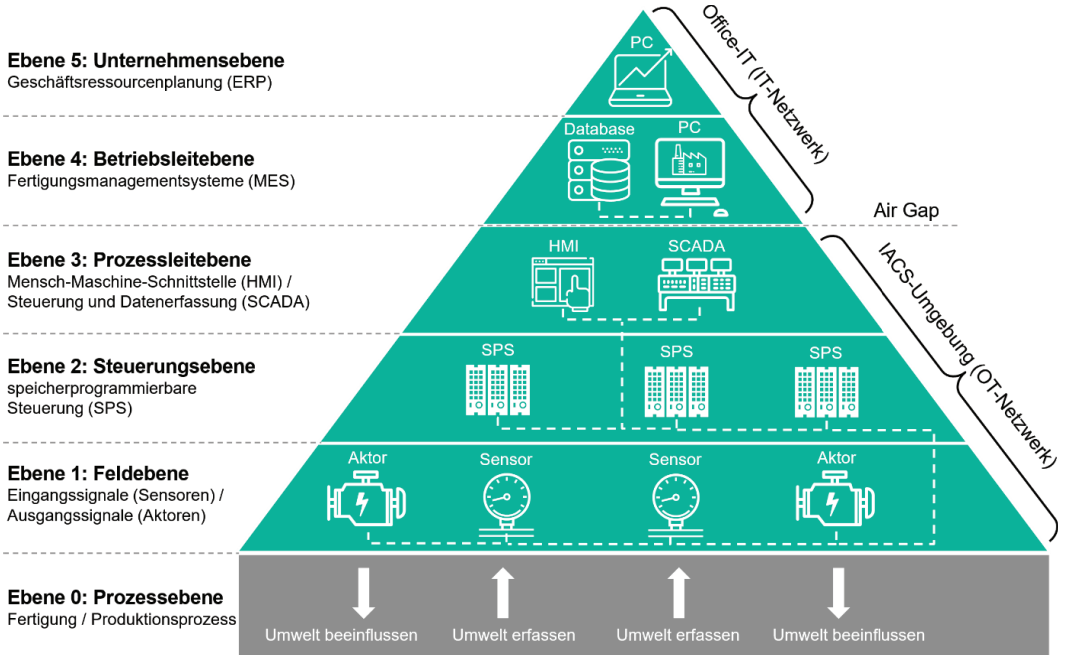


Bild 1: Automatisierungspyramide in der Produktion (IPT, eigene Darstellung)

Hälfte der veröffentlichten IACS-spezifischen Schwachstellen die Prozessleitebene.

Die Prozessleitebene ist von kritischer Natur, das heißt der Zugang dazu führt automatisch zur verbundenen Feldebene und somit zum physischen Prozess. Das Suchen nach Schwachstellen innerhalb der Steuerungs- und Feldebene wird überflüssig.

Um Sicherheitsmaßnahmen zu implementieren, ist es elementar, die genutzten Methoden der Angreifer zu verstehen.

Studienablauf und Ergebnisse

Zur Ermittlung des Sicherheitsniveaus von Unternehmen wurde der Production Security Readiness Check (PSRC) entwickelt. Der PSRC ist ein Modell zur selbständigen Messung des Cybersecurity-Status von produzierenden Unternehmen und hilft diesen, ihren Cybersecurity-Status zu bewerten und zu verbessern. Der PSRC wurde so entwickelt, dass er von produzierenden Unternehmen jeder Branche, Struktur und Größe genutzt werden kann. Der Check basiert auf dem Cybersecurity Capability Maturity Model (C2M2) und einer Kombination gängiger Cybersecurity-Standards wie der ISO 27001, der IEC 62443, dem NIST CSF und dem BSI IT-Grundschutz. Der PSRC besteht aus neun Domänen, die jene Themen abbilden, die für einen ganzheitlichen Sicherheitsansatz betrachtet werden müssen:

- Risikomanagement (RM)
- Asset-, Change- und Konfigurationsmanagement (ACKM)
- Identitäts- und Zugangsmanagement (IZM)
- Bedrohungs- und Schwachstellenmanagement (BSM)
- Situationsbewusstsein (SB)
- Informationsaustausch (IAK)
- Reaktion auf Ereignisse und Vorfälle und Kontinuität der Produktion (EVKP)
- Supply-Chain-Management (SCM)
- Risikofaktor Mensch (RFM)

Für die Stichprobe wurde nach Unternehmen mit einer Mindestmitarbeiterzahl von 20 aus dem produzierenden Gewerbe gesucht. Aus dem gegebenen Unternehmenspool wurden Unternehmen aus diversen Industriezweigen befragt. Diese Unternehmen bewerteten selbstständig ihren Sicherheitsstatus mithilfe der einzelnen Domänen des PSRC. Zur Konkretisierung der Ergebnisse wurden ausführliche (Telefon-)Interviews durchgeführt. Die Grundlage der Auswertung bildeten einzelne Praktiken zur Erhöhung der Cybersecurity innerhalb einer Domäne. Beispielsweise bewertet das Unternehmen in der ACKM-Domäne, ob es die Praktik „ACKM-1.1a: Es existiert ein Inventar an OT- und IT-Assets, die für die Produktion relevant sind“ nicht (Status 0), teilweise (Status 1), weitgehend (Status 2) oder vollständig (Status 3) umgesetzt hat. Basierend auf den Einzelwertungen der jeweiligen Praktiken wird der Umsetzungsstand aller Praktiken einer Domäne ermittelt.

Am Beispiel der Asset-, Change- und Konfigurationsmanagement-Domäne (ACKM) werden die quantitativen Ergebnisse erläutert (Bild 3). Die ACKM-Domäne beschreibt die Verwaltung, Konfiguration und Änderung von IT- und

OT-Assets. Unter Assets werden alle Vermögenswerte eines Unternehmens verstanden, einschließlich der gesamten Hard- und Software in der Produktion. Die ACKM-Domäne weist im Mittel respektive im Median einen höheren Umsetzungsstand für Großunternehmen als für die KMU auf.

In einer detaillierten Betrachtung zeigte sich, dass die teilnehmenden Unternehmen über ein Basis-Inventar an IT- und OT-Assets, die für die Produktion relevant sind, verfügen. Alle weiteren, das Inventar unterstützenden Zusatzinformationen, wie z. B. das Mapping von physischen und logischen Verbindungen zwischen Assets, wird im Mittel entweder nicht (KMU) oder nur teilweise (GU) umgesetzt. Das bedeutet, dass nicht alle Verbindungen eindeutig nachzuverfolgen sind. Die Ergebnisse der anderen acht Domänen sind in der Folge erläutert.

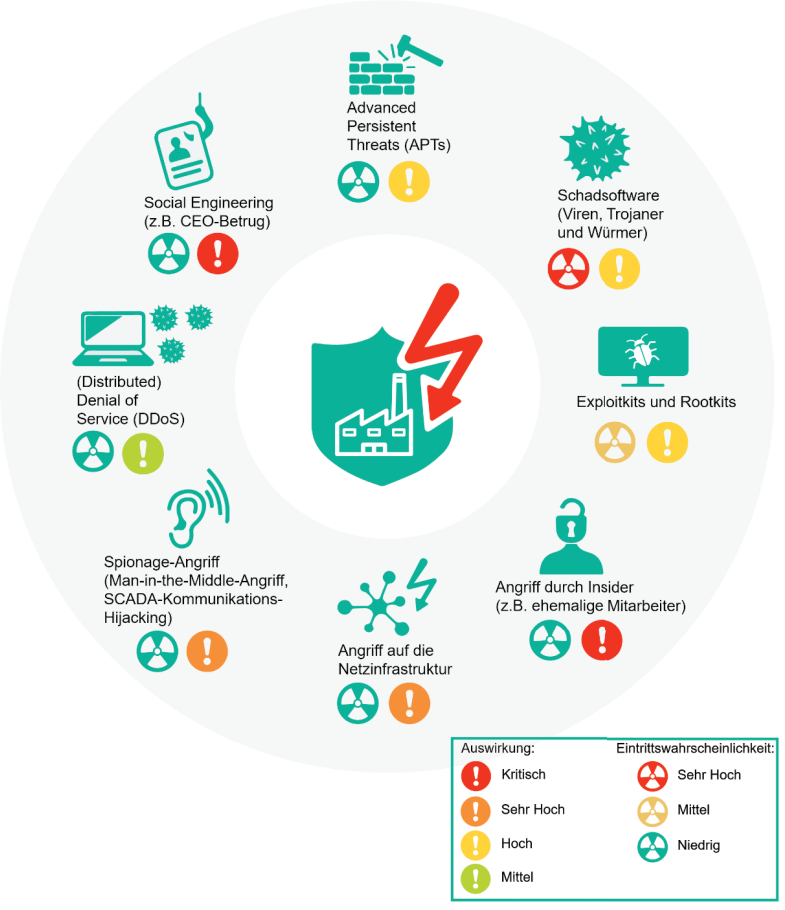
Großunternehmen (insbesondere börsennotierte) besitzen ein allgemeines Risikomanagement (RM) mit gut dokumentierten Handbüchern. Innerhalb des Risikomanagements wird Cybersecurity überwiegend aktiv im Office-Netzwerk angegangen. In der Produktion wurde das Risiko durch Cyberangriffe zwar erkannt, aber nur in wenigen Fällen aktiv in Angriff genommen. Bei den teilnehmenden KMU verhält es sich ähnlich, wobei die Umsetzung der Sicherheitsmaßnahmen im Mittel niedriger ausfällt.

Im Vergleich zu den anderen Domänen erreichte die Identitäts- und Zugangsmanagement-Domäne (IZM) bei den KMU und GU den höchsten Umsetzungsstand. In dieser Domäne existieren ausgereifte Verzeichnisdienste wie Windows Active Directory (AD) und Standard-Software wie SAP, die den Unternehmen helfen, den gesamten Lifecycle – von der Erstellung bis zur Deaktivierung – eines logischen bzw. physischen Zugangs zu managen.

Die Ergebnisse der Bedrohungs- und Schwachstellenmanagement-Domäne (BSM) ähneln denen der Risikomanagement-Domäne. Während die GU über eine strukturierte Vorgehensweise zur Eliminierung von Schwachstellen und Bedrohungen verfügen, wenden die KMU diese Tätigkeiten ad hoc an. Beide Unternehmensklassen überfordert jedoch die Zunahme der Update-Zyklen der Assets. Der Umgang mit Schwachstellen an verschiedenen Komponenten weist enorme Unterschiede auf. Während Windows-Komponenten einem aktiven Patchmanagement-System unterzogen werden, betreiben die Unternehmen für SPS-Steuerungen de facto kein aktives Patchen.

In der Domäne „Situationsbewusstsein" (SB) bewerteten Unternehmen primär ihre Aktivitäten rund um das Thema Logging und Monitoring. Diese werden zwar durchgeführt, aber ohne umfassenden oder zielführenden Rahmen. Die Produktion wird dabei nicht speziell betrachtet, sondern es wird unter-

Bild 2: Gängige Angriffsmethoden und -mittel auf industrielle Produktionsanlagen (IPT, eigene Darstellung)



Literatur

[1] Vereinigung der Bayerischen Wirtschaft e. V.: Studie Digitalisierung als Rahmenbedingung für Wachstum. München, 2017, S.2

[2] McKinsey & Company: Digitalisierung im Mittelstand erhöht Wachstum in Deutschland um 0,3 Prozentpunkte pro Jahr. URL https://www.mckinsey.com/de/news/presse/digitalisierung-im-mittelstand-erhoht-wachstum-in-deutschland-um-03-prozentpunkte-pro-jahr [Stand: 27.08.2019]

[3] Statistisches Bundesamt: Bruttoinlandsprodukt 2018 für Deutschland. Statistisches Bundesamt, Wiesbaden, 2019, S. 11

[4] Lichtblau, K.; Schleiermacher, T.; Goecke, H.; Schützdeller, P.: Digitalisierung der KMU in Deutschland. Köln: IW Consult, 2018, S.28

[5] Icks, A.; Schröder, C.; Brink, S.; Dienes, C.; Schneck, S.: Digitalisierungsprozesse von KMU im Verarbeitenden Gewerbe. In: IfM-Materialien Nr. 255, Bonn, S.23, 31 2017

https://doi.org/10.30844/FS19-4_21-24

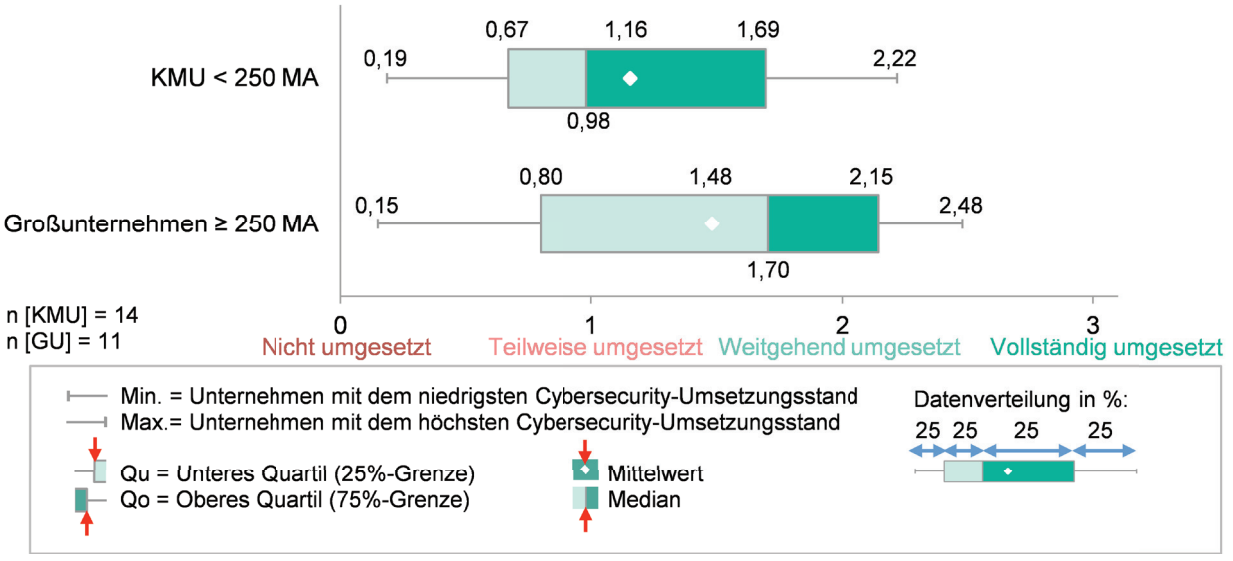


Bild 3: Umsetzungsstand aller Cybersecurity-Praktiken in der ACKM-Domäne

nehmensweit im IT- und OT-Netzwerk protokolliert. Besonders die GU setzen sogenannte „Security Information and Event Management" Systeme ein, die das Unternehmen bei Überwachungsaktivitäten unterstützen.

Der Informationsaustausch und die Kommunikation (IAK) bezüglich Cybersecurity-Themen werden im Mittel nicht (ausreichend) betrieben. Die IAK-Domäne weist den zweitniedrigsten Umsetzungsstand aller Domänen auf. Die meisten Unternehmen vertrauen rein auf ihre eigenen Ressourcen und informieren sich selbstständig, ohne in einem Austauschnetzwerk aktiv zu sein.

Die Reaktionen auf Cyber-Ereignisse und -Vorfälle als auch die Aktivitäten rund um die Kontinuität der Produktion (EVKP) werden im Mittel nur gering umgesetzt. Aufgrund von hochentwickelten Angriffsmethoden befürchten viele Unternehmen, dass sie eine Vielzahl an Angriffen nicht erkennen. Ein proaktives Denken, welches Vorfälle generell verhindern soll, etabliert sich nur langsam. Die Kontinuität der Produktion wird bei den GU durch ein Business Continuity Management (BCM) gewährleistet.

Der Umgang mit Cybersecurity-Praktiken in Bezug auf die komplette Lieferkette (SCM) ist weder den befragten KMU noch den GU vertraut. Bei der Beschaffung von neuen Anlagen werden Security-Anforderung im Lastenheft nur selten aufgeführt. Ebenfalls wird die IT-Abteilung selten in den Beschaffungsprozess mit involviert. Verantwortlichkeiten für die IT-Sicherheit der Anlage sind zudem zwischen dem Hersteller und dem Betreiber einer Anlage nur unzureichend geregelt.

Obwohl Schulungen zum Thema Cybersecurity für viele Unternehmen wichtig sind, ist die Domäne „Risikofaktor Mensch" (RFM) nur gering umgesetzt. Im Mittel gestaltet sich die konsequente Durchführung dieser Schulungen als schwierig. Es wird lediglich im Intranet auf die Existenz von Schadsoftware hingewiesen, aber eine aktive sich wiederholende Schulung findet entweder gar nicht oder nur selten statt.

IT Sicherheit in der Produktion

Ein detaillierter Bericht der qualitativen und quantitativen Ergebnisse der durchgeführten Studie wird Ende des Jahres 2019 in einem Whitepaper des Fraunhofer IPT zum Thema „IT Sicherheit in der Produktion" veröffentlicht.

Cybersecurity in Integrated Production

Networking and digitization of production have an enormous growth potential and will be elementary for Germany's economy in the coming years. For many companies, however, concerns about IT security are currently a major obstacle to the implementation of digitization. For this reason, a holistic Production Security Readiness Check (PSRC) was developed as part of a study at the Fraunhofer Institute for Production Technology IPT, which shows manufacturing companies which security level they currently meet and need.

Keywords:
IT Security, Connectivity, Level of Security, Legal Provisions

Schlüsselwörter:
IT-Sicherheit, Vernetzung, Sicherheitsniveau, gesetzliche Regelungen