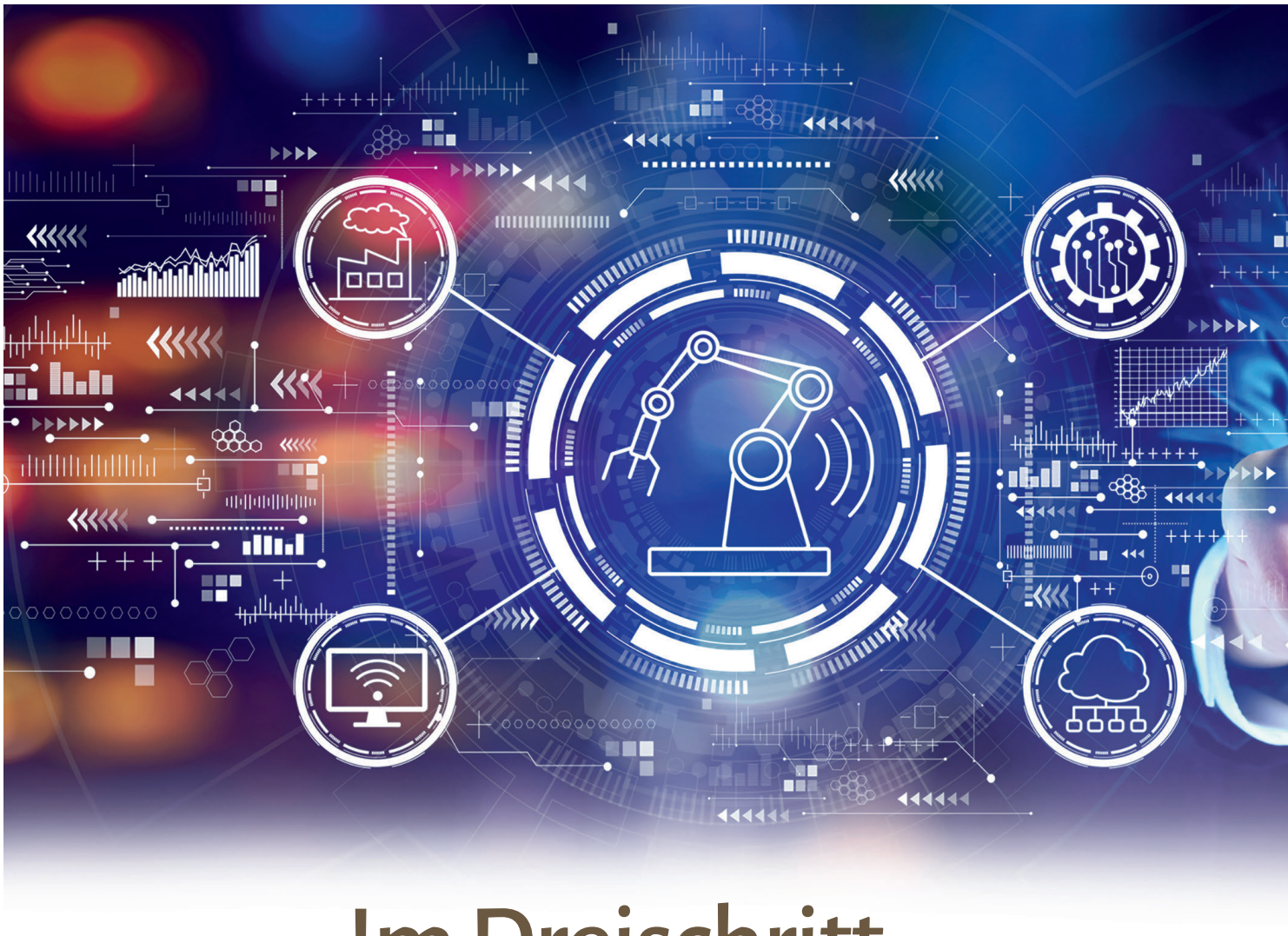

Im Dreischritt zur sicheren Produktion

Bedarfsorientierte und effiziente IT-Sicherheitskonzepte für KMU

Industrie 4.0, Internet-of-Things und Bring-Your-Own-Device sind Konzepte, die auf ausreichender IT-Sicherheit beruhen. Diese ist eine wesentliche Voraussetzung erfolgreicher Digitalisierung und Vernetzung der Produktion. Das Fraunhofer IPT schlägt drei Schritte vor, damit Unternehmen ein individuelles IT-Sicherheitskonzept erstellen können.

Timo Heutmann und Robert H. Schmitt

Damit produzierende KMU auch zukünftig der Motor der Wirtschaft bleiben, gilt es das Potenzial von Industrie 4.0 zu nutzen. Wesentlicher Erfolgsfaktor wird sein, organisationsbedingte Brüche in Fertigungs- und Zulieferabläufen durch unternehmensübergreifende Vernetzungen der Systeme zu überwinden, um gemeinsam effizienter und flexibler zu werden. Mit zunehmenden Digitalisierungs- und Vernetzungsaktivitäten im Zuge von Industrie 4.0 stehen produzierende Unternehmen jedoch vor der Herausforderung, das Risiko neugeschaffener Angriffsflächen und Sicherheitslücken durch cyber-

physische Systeme zu reduzieren. IT-Sicherheit nimmt damit eine bedeutende Rolle bei Industrie 4.0-Aktivitäten ein.

Fehlende bzw. unzureichende IT-Sicherheit führt u. a. zu verringerter Produktivität, monetärem Schaden durch Aufwände für Reaktionen oder Wiederbeschaffungen, Bußgelder und Rechtsurteile, Wettbewerbsnachteile oder Rufschädigung. Der Schaden kann enorm sein. Zudem kommen ad-hoc-Investitionen in neue Hard- und Software, um die Kontrolle über das eigene Unternehmen wiederzuerlangen. IT-Sicherheit dient damit dem Schutz eines Objekts (z. B. eine Maschine) vor der Umgebung, um desaströse Folgen zu vermeiden. Neben einer Betrachtung von IT-Sicherheit als reinen Kostenfaktor sollten deren Potenziale zur Befähigung von Industrie 4.0 mehr in den Fokus rücken.

Beispielsweise werden die Ergebnisse von Künstliche Intelligenz (KI) -Projekten durch IT-Sicherheit in den Anforderungsdimensionen Datenbasis und KI-Modell unterstützt:

- Einerseits benötigt die Datenbasis oftmals Datenschutz, da meistens sensible Informationen verarbeitet werden. Zudem teilen sich Datenqualität und IT-Sicherheit zu eines wesentlichen Teil gleiche Dimensionen bzw. Ziele. Fehlende Integrität durch Manipulation führt zu verfälschten Sachverhalten und Unvollständigkeit der Daten.
- Andererseits befähigt IT-Sicherheit zu verlässlichen KI-Modellen, indem die Korrektheit der KI-Ausgaben und die Robustheit gegenüber externen Einflüssen gesichert wird. Somit kann IT-Sicherheit als Befähiger von KI-Projekten interpretiert werden, auf dessen Basis diese Produktionsprozesse verbessert werden können.

Herausforderungen bei IT-Sicherheitskonzepten

Produzierende Unternehmen scheuen sich jedoch noch, in IT-Sicherheitslösungen zu investieren. Und dies angesichts des Risikos von Cyber-Angriffen und der Möglichkeiten von Industrie 4.0. Begründet wird dies oft mit knappen monetären Ressourcen. Aber besonders bei KMU ist das Wissen über potenzielle IT-Sicherheitsrisiken und notwendige IT-Schutzmaßnahmen nicht immer vorhanden. Dabei sind Unternehmen jeder Größe seit Inkrafttreten der EU-Datenschutzgrundverordnung (EU-DGSVO) zum Schutz persönlicher Daten verpflichtet. Häufig mangelt es KMU jedoch an bedarfsorientierten IT-Sicherheitslösungen, welche die Wichtigkeit (z. B. Know-How) und Kritikalität der Produktionsdaten in Betracht ziehen. Indes ist das Kosten-Nutzen-Verhältnis zwischen der Investition in IT-Sicherheit und dem Wertschöpfungspotenzial durch Produktionsvernetzung schwierig quantifizierbar.

Im Forschungsprojekt ESPRI wird daher die Software KMUsecure zur kontinuierlichen Überwachung und bedarfsorientierten Ermittlung von IT-Sicherheitslösungen für produzierende KMU entwickelt. Neben Sicherheitslösungen zeigt sie die wirtschaftlichen Potenziale der Produktionsoptimierung durch Maßnahmen der Vernetzung auf. Die drei wesentlichen Schritte sind dabei (Bild 1):

- Informations- und Datenflüsse identifizieren,
- diese hinsichtlich Sicherheitskritikalität bewerten und
- notwendige IT-Sicherheitsmaßnahmen ableiten .

Datenströme aufnehmen kann entweder manuell oder automatisiert mit Lösungen wie SCUDOS des Projektpartners Allgeier IT Solutions erfolgen. Dabei wird aufgezeigt, welche Daten mittels welcher Schnittstelle bzw. welchem Gerät ausgetauscht werden. Zudem werden die verschiedenen Informationstypen (z. B. Produktdaten, Prozessdaten, Kostendaten, Personendaten) identifiziert. Vielfalt und Anzahl von Maschinen sowie Geräten nehemen rasant zu. In dieser Situation bietet ein automatischer Datenaustausch eine durchgängige Kenntnis des Informationsflusses innerhalb des Produktionsnetzwerks. Zudem werden Geschäftsprozesse und die Produktion während der Ana- »»

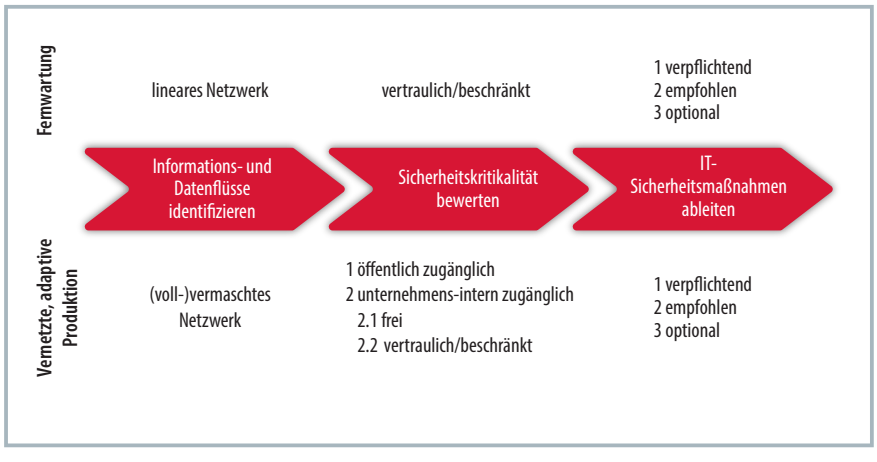

Bild 1. Drei Schritte führen zu einer sicheren Produktion, die vor Angriffen über Datenleitungen geschützt ist.

Quelle: Fraunhofer IPT © Hanser

lysen nicht unterbrochen. Die Bedrohungsanalyse zur Bewertung der Sicherheitskritikalität von Daten und Schnittstellen umfasst den Abgleich bestehender Daten mit IT-Sicherheitsvorgaben aus Gesetzen, Normen und Anwenderanforderungen. Eine Klassifizierung durch Bewertung des Sicherheitsbedarfs erfolgt auf dieser Basis. Sie leitet sich aus der möglichen Verlusthöhe und Verlustfrequenz ab, die pro Bedrohung und zugehörigem Schutzziel quantifiziert wird.

Basierend auf den Analysen und Klassifizierungen werden dem Anwender IT-Schutzmaßnahmen vorgeschlagen, die bei einer steigenden internen oder externen Vernetzung ratsam für den Schutz des Know-hows sind. Sie dienen als Entscheidungshilfe bei der Lösungsauswahl. Transparenz und Nachvollziehbarkeit für Entscheider sind dabei kritische Erfolgsfaktoren.

IT-Sicherheit im Praxistest unter verschiedenen Bedingungen

Das dreistufige IT-Sicherheitsverfahren wird zusammen mit Projektpartnern erprobt:

- *Vernetzte, adaptive Produktion* bei Wolfgang Doose Werkzeug- & Vorrichtungsbau GmbH & Co KG und
- *Fernwartung* des Projektpartners MAKA Systems GmbH.

In beiden Fällen können Daten- und Informationsflüsse mittels einer angepassten Wertstrommethode aufgenommen werden. Der Datenfluss orientiert sich dabei an den drei Ebenen:

- Objekt,
- Cloud und
- Applikation.

Ein Datentransfer wird somit von der Aufnahmeebene Objekt (z. B. Sensor in Maschine) über die Speicherebene Cloud (z. B. in Form eines Data Lakes) zur Verarbeitungsebene Applikation (z. B. KI-Analyse) generalistisch beschrieben. Der Informationsfluss führt in der vernetzten, adaptiven Produktion über die Hierarchielevel einer Produktion von Maschine bzw. Arbeitsplatz bis hin zum Produktionsnetzwerk. Der Informationsfluss der Fernwartung orientiert sich am Datenfluss, da meistens eine direkte, abgeschlossene Verbindung zwischen Maschine und externem Servicemitarbeiter aufgebaut wird. Die Netzwerktopografie der Fernwartung ist damit im Vergleich zur vernetzten, adaptiven Produktion weniger komplex, da lediglich ein lineares Netzwerk *Maschine-zu-externem-Servicemitarbeiter* aufgebaut wird. Im Anwendungsfall schließen sich die diversen Maschinen, Mitarbeiter und Transporteinheiten zu (voll-)vermaschten Netzwerken zusammen.

Hierauf basierend werden Daten entsprechend ihrer Kritikalität, welches auf den jeweiligen Schutzzielen der IT-Sicherheit (u. a. Vertraulichkeit, Integrität, Verfügbarkeit) basiert. Die hieraus abgeleitete Klassifikation für die *vernetzte, adaptive Produktion* gliedert sich in:

- öffentlich zugängliche Daten bzw. Informationen und
- unternehmensintern zugängliche Daten bzw. Informationen (frei zugänglich und intern beschränkt zugänglich).

Im Anwendungsfall *Fernwartung* werden Daten grundsätzlich als *vertraulich bzw. beschränkt zugänglich* klassifiziert, um den Zugang Dritter zu sensiblen Maschinen- und Fertigungsdaten zu unterbinden.

Die abschließende Erstellung eines IT-Sicherheitskonzepts enthält eine priorisierte Maßnahmenliste. Diese schlägt notwendige, empfohlene und optionale Maßnahmen zur Erhöhung des IT-Sicherheitlevels vor, welche zum einen auf deren Notwendigkeit bzw. des Sicherheitsbedarfs der Daten bzw. Informationen basiert, zum anderen auch eine wirtschaftliche Bewertung vornimmt. Letztere konzentriert sich auf die Gegenüberstellung von:

- IT-Sicherheitsrisiko (Verlusthöhe und Verlustfrequenz) sowie
- dem Industrie 4.0-Potenzial (Umsatzerhöhung, Effizienzsteigerung, Durchlaufzeitreduzierung).

Somit liegt Managern produzierender Unternehmen eine Entscheidungsgrundlage vor, die ein ganzheitliches IT-Sicherheitskonzept bietet. ■

INFORMATION & SERVICE

FORSCHUNGSPROJEKT

Das Forschungsprojekt ESPRI – Effiziente und bedarfsorientierte Erstellung von IT-Sicherheitskonzepten für produzierende KMU – wird gefördert durch das Bundesministerium für Bildung und Forschung (BMBF) im Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt" unter dem Förderkennzeichen 16KIS1123.

AUTOREN

Timo Heutmann, M.Eng. ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Produktionstechnologie IPT in Aachen.

Prof. Dr.-Ing. Robert H. Schmitt ist Inhaber des Lehrstuhls für Fertigungsmesstechnik und Qualitätsmanagement an der RWTH Aachen University und Teil des Direktoriums am Fraunhofer-Institut für Produktionstechnologie IPT.

KONTAKT

Timo Heutmann
T 0241 8904-245
timo.heutmann@ipt.fraunhofer.de