**„DIGITALISIERUNG JETZT! – PRODUKTION & FERTIGUNG“
in der FAZ Digital & FAZ Kiosk aus dem unabhängigen Verlagshaus Mediaplanet Deutschland.**

Dieser Artikel ist **in Zusammenarbeit mit NCP** entstanden.

FOTO: NIRUTFOTOSTOCK ADOBE.COM

Sichere Komponenten für sensible Kommunikation

Wer in seinem Maschinenpark langfristig von den Vorteilen der Industrie 4.0 profitieren will, sollte für das Sammeln sowie die Analyse und das Management von Big Data auf **Gesamtlösungen** vertrauen. Für sichere Datenkommunikation zwischen Maschinen sorgen zum Beispiel **etablierte Softwarekomponenten von NCP**.

Text Dominik Maaßen

Konzerne, aber auch KMU stehen in Sachen IIoT gleich vor mehreren Herausforderungen: Zum einen muss es dem Unternehmen gelingen, die unterschiedlichen Daten aus den verschiedenen Systemen zu sammeln sowie sinnvoll zu verarbeiten und zu analysieren. Das stellt intern die Mitarbeiter vor ganz neue Probleme. Der Bereich IT und die OT, die sogenannte Operational Technology, die früher strikt getrennt waren, wachsen durch Themen wie IIoT/Industrie 4.0 immer mehr zusammen. Der Spezialist aus der Produktion definiert nun die relevanten Daten, die der Spezialist aus der IT aufbereitet und visualisiert.

Datenschatz dank Retrofit

Erschwerend kommt hinzu: Maschinen und Anlagen in der Produktion haben sehr oft eine Laufzeit von mehr als zehn bis 15 Jahren. Das heißt, mit den Maschinen, die heute der Umsatztreiber für das Unternehmen sind, können direkt noch keine Industrie-4.0-Szenarien umgesetzt werden. Um Maschinenkommunikation möglich zu machen, braucht es für viele Maschinen ein „Retrofit“ mit passenden Technologien zur Datenanalyse.

Aufgrund der vernetzten Systeme und der zunehmenden Anbindung an die Cloud ergeben sich außerdem neue Einfallstore für Angriffe durch Cyberkriminelle: Im Bereich der IT-Sicherheit darf die in der Vergangenheit manchmal vernachlässigte Produktion jetzt nicht mehr außer Acht gelassen werden. Die IT muss neue Angriffsszenarien auf vernetzte Maschinen überwachen und absichern.

Know-how und Risikoabschätzung

Wer als Geschäftsführer oder Leiter der IT die Firma clever umrüsten möchte, sollte Industrie 4.0 daher niemals allein von der technologischen Seite betrachten. Es reicht nicht die eine Lösung vom Markt, um den Datenschatz zu heben. Auch die menschlichen Fähigkeiten müssen in die Überlegungen mit einfließen. Es braucht das Know-how, welche Daten zu welchem Zweck an welcher Stelle und wie weiterverarbeitet werden. Mitarbeiter wollen in diese neue Welt mitgenommen werden.

Grundlegend für eine Fernwartungslösung im hoch automatisierten IIoT-/Industrie-4.0-Umfeld sind daher ein klares Konzept und eine Risikoabschätzung: Fragen, welche Maschinen, Anlagen und Steuerungen überhaupt externen Zugriff brauchen und wie, müssen im Vorfeld geklärt werden. Gerade die Sicherheit steht hier im Fokus und sollte von Beginn an höchste Priorität haben. Denn ein unerlaubter Zugriff kann negative Konsequenzen bis hin zum Totalausfall der gesamten Produktionsprozesse haben.

Qualitätsfaktor IT-Sicherheit

Essenziell kann zum Beispiel sein, innerhalb der Produktion, in einer einzelnen Halle und darüber hinaus, sogenannte „IIoT-Inseln“ von zusammenhängenden Maschinen und Anlagen zu bilden. Diese lassen sich zentral verwalten, sicherheitstechnisch steuern und überwachen. Diese „IIoT-Insel-Segmentierung“ gewährt einen hohen Schutz für die Produktion des Unternehmens und grenzt mögliche Gefahren ein. Der klare Mehrwert ist neben einer sauberen Produktionsstruktur das Eindämmen eines Cyberangriffs oder Security-Vorfalls auf die jeweilige Insel. Somit ist der Schaden in einer einzelnen Insel isoliert und die Verbreitung etwaiger Schadcodes ist massiv eingeschränkt. Denn die restliche Produktion ist davon unberührt.

IT-Sicherheit wird so zum wichtigen Qualitätsfaktor: Im Mittelpunkt steht immer eine sichere, verschlüsselte Kommunikation aller vernetzten Komponenten inklusive einer starken Authentifizierung. Etablierte Anbieter, wie NCP aus Nürnberg, unterstützen hier durch ganzheitliche Lösungen. Das Produktportfolio beschränkt sich dabei nicht nur auf ein spezielles Umfeld, sondern es steht bei der Beratung und Betreuung der Kunden immer eine problemorientierte Lösung im Raum.

Brücke zwischen IT und OT

Bei der Verzahnung von IT und OT kann eine zentrale Verwaltungskomponente, wie zum Beispiel das NCP Management, eine sichere Brücke schlagen, um die Kommunikation innerhalb der Produktion, der IT und der verbundenen Anlagen abzusichern. Dank des NCP Management können sowohl Zugänge von Mitarbeitern abgesichert wie auch die Identitäten von Maschinen verwaltet werden. Im Zusammenspiel mit den weiteren Komponenten wie Clients und Gateways entwickelt sich das Management zu einer ganzheitlichen Lösung, die auch weitestgehend automatisierte Zugriffe beispielsweise von Servicetechnikern auf Maschinen ermöglicht.

Softwarekomponenten von NCP

NCP verfügt für die verschiedenen Szenarien der Industrie 4.0 immer über passende Softwarekomponenten für den sicheren Datenaustausch. Mehrere Komponenten an verschiedenen Stellen der Infrastruktur gewährleisten im Rahmen einer Gesamtlösung die Kontrolle und sichere Datenverschlüsselung: Remote Gateways sorgen für die sichere Kommunikation von Anlagen, Maschinen oder Systemen. Hinzu kommen ein zentrales Gateway, das sie sicher anbindet, sowie ein Managementsystem für die Administration, das Monitoring und die Integration in vorhandene Infrastrukturen.

Smart Maintenance

Im Servicealltag bedeutet das konkret: Dank der Smart Maintenance Solution von NCP erhält ein Techniker im Servicefall binnen Minuten sicheren Fernzugriff auf die zu wartende Maschine. Der Zugriff ist zeitlich auf die Dauer der Wartung begrenzt und außerdem ist sichergestellt, dass sowohl die Maschine als auch der Techniker exklusiv verbunden werden. Erfahrungsgemäß ist gerade die Zeit zwischen der Aktivierung des Servicetechnikers und der Möglichkeit der Verbindung essenziell für die Industrieunternehmen. Je weniger Zeit dazwischen liegt, desto besser geeignet ist die Lösung, da weniger Produktionsausfall zu erwarten ist.

Sämtliche Verbindungen zwischen den Endgeräten und den beiden Gateways sind außerdem mit modernsten Algorithmen, zum Beispiel Suite B Cryptography, verschlüsselt. Ein weiteres Security-Feature stellen zentral verwaltete Maschinenzertifikate in einer Public Key Infrastructure (PKI) dar. Hierdurch wird eine eindeutige Authentifizierung aller Endgeräte gewährleistet.

Mandantenfähig und leicht integrierbar

Die NCP-Komponenten sind mandantenfähig, das heißt, die Lösung kann für zahlreiche Kunden beziehungsweise Industrieunternehmen gleichzeitig genutzt werden. Dadurch ist das Managementsystem für den Einsatz in Cloud-Umgebungen oder in Industrie-4.0-Strukturen prädestiniert, innerhalb derer beispielsweise mehrere Produktionsstandorte oder Unternehmensbereiche eine gemeinsame Plattform nutzen. NCP bietet so im Zusammenspiel der zahlreichen Komponenten das Management mit einer ganzheitlichen Lösung – und Unternehmen können das volle Spektrum der Industrie 4.0 ausschöpfen. ■

Sebastian Oelmann
Product Manager
Industrie 4.0 | IoT

> Eine IT-/OT-Infrastruktur ist nur so stark wie das schwächste System. Deshalb ist eine sichere Datenkommunikation in allen Bereichen unerlässlich.
> *Sebastian Oelmann*

Mehr über
NCP engineering GmbH:
ncp-e.com/de

Mehr zu den
IIoT Lösungen von NCP:
ncp-e.com/de/loesungen/industrie-40

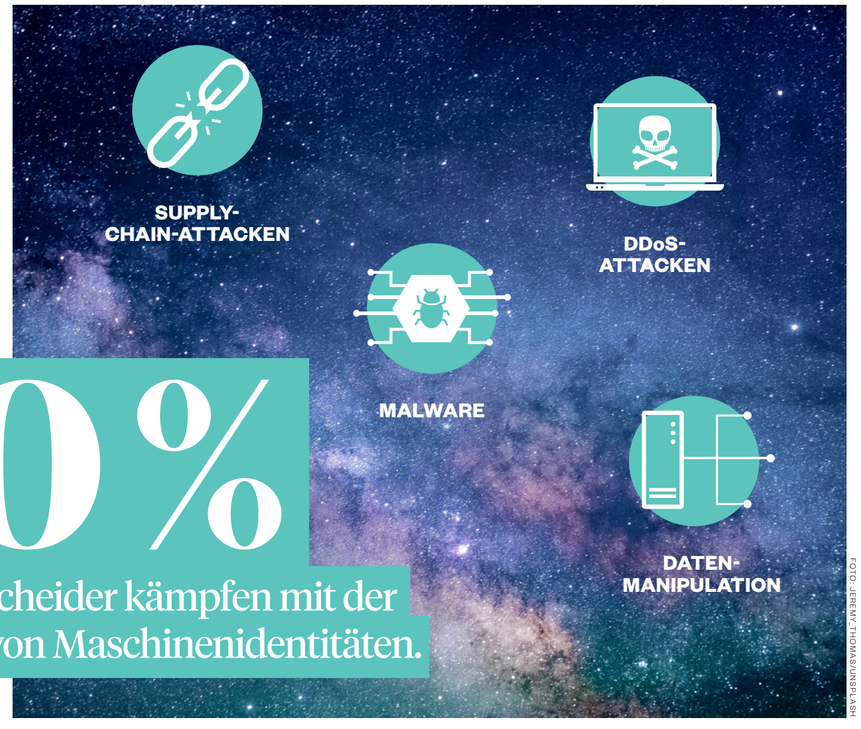

FOTO: JEREMY THOMAS/UNSPLASH

80 %
der IT-Entscheider kämpfen mit der Sicherheit von Maschinenidentitäten.