Wie neue EU-Regularien Maschinenbauer zu sicheren Kommunikationsarchitekturen zwingen

„Cybersecurity ist heute keine Option mehr“

Artikel anhören!

Mit neuen regulatorischen Vorgaben wie dem Cyber Resilience Act steigt der Druck auf Maschinenbauer und Gerätehersteller, Cybersecurity systematisch in ihre Produkte zu integrieren. Gleichzeitig eröffnet eine sichere Kommunikationsinfrastruktur neue Möglichkeiten für digitale Services und datenbasierte Geschäftsmodelle. Wie sich industrielle Netzwerke absichern lassen und welche Rolle Kommunikationskomponenten dabei spielen, erläutert Thierry Bieber, Business Development Manager bei HMS Industrial Networks, im Gespräch mit dem SPS-MAGAZIN.

Bild: HMS Industrial Networks GmbH

Herr Bieber, Cybersecurity ist bei HMS ein zentrales Thema. Warum ist IT- und OT-Security heute zu einem strategischen Muss für die industrielle Automatisierung geworden?

Wir beschäftigen uns bereits seit sechs oder sieben Jahren intensiver mit Cybersecurity. Damals haben wir auch unser erstes IoT-Security-Modul auf den Markt gebracht. Die Akzeptanz war zu Beginn allerdings relativ gering, weil viele Unternehmen keinen unmittelbaren Handlungsdruck gesehen haben. Cybersecurity wurde häufig eher als optionales Zusatzthema betrachtet. Mit den neuen regulatorischen Anforderungen – insbesondere dem Cyber Resilience Act der EU – hat sich diese Situation deutlich verändert. Heute sind nicht nur Betreiber von Anlagen gefordert, sondern auch Geräte- und Maschinenhersteller müssen Cybersecurity systematisch in ihre Produkte integrieren.

Viele Unternehmen stehen deshalb aktuell vor der Frage, wie sie diese Anforderungen konkret umsetzen können. Unser Ansatz ist es, hier als Enabler aufzutreten. Wir möchten Herstellern Werkzeuge und Technologien zur Verfügung stellen, mit denen sie sichere Kommunikationslösungen implementieren können. Idealerweise wird Cybersecurity dabei nicht nur als Pflicht verstanden, sondern auch als Grundlage für eine sichere digitale Vernetzung.

> **Cybersecurity wird zur Grundfunktion industrieller Kommunikation.**
>
> **Thierry Bieber, HMS Industrial Networks**

Wo sehen Sie aktuell die größten sicherheitsrelevanten Schwachstellen in industriellen Netzwerken?

Die klassische Feldebene – beispielsweise Netzwerke mit Profinet oder Ethernet/IP – befindet sich häufig noch in relativ geschützten Produktionsumgebungen. Dadurch ist sie bislang weniger direkt von externen Angriffen betroffen als klassische IT-Systeme. Allerdings verändert sich die industrielle Infrastruktur zunehmend. Immer mehr Automatisierungskomponenten verfügen über integrierte Webinterfaces, über die sich Geräte konfigurieren lassen. Gleichzeitig entstehen neue Zugriffsmöglichkeiten, etwa über Service-Schnittstellen oder neue Digitalisierungsansätze. Damit entstehen zusätzliche potenzielle Angriffsflächen. Besonders kritisch sind häufig die Übergänge zwischen OT-Netzwerken und IT-Infrastrukturen. Genau an diesen Schnittstellen wird es künftig entscheidend sein, Sicherheitsmechanismen konsequent umzusetzen.

Welche Rolle spielen Kommunikationskomponenten für die Cybersecurity einer Anlage?

Kommunikationsschnittstellen verbinden unterschiedliche Netzwerke miteinander und übernehmen damit eine Schlüsselrolle innerhalb der gesamten Architektur. Sie sind gewissermaßen das Bindeglied zwischen der Feldebene, übergeordneten IT-Systemen und zunehmend auch Cloud-Plattformen. Bei HMS unterscheiden wir beispielsweise zwischen klassischen OT-Schnittstellen für die reine Feldkommunikation und erweiterten IoT-Schnittstellen, die zusätzliche Security-Funktionen integrieren. Dazu gehören etwa Mechanismen für Zertifikatsmanagement, Verschlüs-

selung oder Secure Boot. Solche Funktionen werden insbesondere dann relevant, wenn Maschinen oder Geräte nicht nur innerhalb eines geschlossenen Produktionsnetzwerks betrieben werden, sondern auch Daten an übergeordnete Systeme, Edge-Plattformen oder Cloud-Anwendungen übertragen.

Sie sprechen häufig von Security by Design. Was bedeutet dieser Ansatz konkret für industrielle Kommunikationsprodukte?

Security by Design bedeutet, dass Cybersecurity von Anfang an Bestandteil der Produktentwicklung ist. Hersteller müssen bereits in der Designphase analysieren, welche Kommunikationsschnittstellen ein Gerät besitzt und welche Risiken daraus entstehen können. Auf dieser Grundlage lässt sich entscheiden, welche Sicherheitsmechanismen erforderlich sind. In einem geschlossenen Produktionsnetz können andere Anforderungen gelten als in einer offenen Infrastruktur mit Internetanbindung. Ein weiterer wichtiger Aspekt ist, nur diejenigen Kommunikationsfunktionen zu aktivieren, die tatsächlich benötigt werden. Jede zusätzliche Schnittstelle oder Funktion kann potenziell auch eine neue Angriffsfläche darstellen.

Viele Unternehmen fühlen sich von Normen wie IEC62443 überfordert. Wie sollten Maschinenbauer mit diesen Anforderungen umgehen?

Der CRA enthält übergeordnete Anforderungen. Die konkreten Unsetzungen müssen noch in Harmonized Standards beschrieben werden. Deshalb herrscht bei Herstellern teilweise Unsicherheit bzgl. der Umsetzung. Die IEC62443 definiert einen Rahmen und beschreibt grundlegende Anforderungen an die Cybersecurity industrieller Systeme. Diese Norm bietet bereits heute eine sehr gute Orientierung für Gerätehersteller. Die Anforderungen der verschiedenen Security Level helfen Unternehmen dabei, ihre Produkte systematisch zu bewerten und schrittweise sicherer zu gestalten.

Wie setzt HMS diese Anforderungen in der eigenen Entwicklung um?

Wir haben unsere Entwicklungsprozesse an den Anforderungen der Norm ausgerichtet und entsprechend zertifizieren lassen. Darüber hinaus ist unser Unternehmen nach ISO27001 zertifiziert. Damit stellen wir sicher, dass sowohl unsere Produktentwicklung als auch unser Informationsmanagement klar definierten Sicherheitsprozessen folgen. Parallel arbeiten wir daran, auch unsere Produkte zunehmend nach den Anforderungen der IEC62443 auszurichten. Dazu gehören beispielsweise Gateways und Embedded-Kommunikationsschnittstellen, die künftig danach zertifiziert werden.

Bild: TeDo Verlag GmbH

Thierry Bieber (rechts) im Gespräch mit Ines Stotz vom SPS-MAGAZIN über Cybersecurity in industriellen Kommunikationsnetzen.

Wie unterstützen Sie Ihre Kunden bei der Umsetzung normkonformer Lösungen?

Cybersecurity betrifft viele Aspekte – von organisatorischen Prozessen über Entwicklungsrichtlinien bis hin zur technischen Gerätearchitektur. Ein Teil der Verantwortung liegt daher immer beim Gerätehersteller selbst. Wir unterstützen unsere Kunden vor allem durch Know-how und technische Bausteine. Dazu gehören unsere Kommunikationsmodule mit integrierten Security-Funktionen sowie umfangreiche Dokumentationen und Empfehlungen zur sicheren Nutzung. Darüber hinaus arbeiten wir eng mit unseren Kunden zusammen, häufig in Form von technischen Workshops oder Projektgesprächen, um konkrete Anforderungen zu analysieren und geeignete Architekturen zu entwickeln.

Kann Cybersecurity auch positive Effekte auf Verfügbarkeit oder Wartbarkeit haben?

Ja, das ist durchaus ein interessanter Nebeneffekt. Viele industrielle Anlagen wurden früher einmal installiert und anschließend möglichst lange unverändert betrieben. Cybersecurity erfordert jedoch, dass Geräte regelmäßig aktualisiert werden können, etwa durch Firmware-Updates. Dadurch entstehen neue Konzepte für Update-Management und automatisierte Wartungsprozesse. Langfristig führt das zu flexibleren Systemen, die sich leichter an neue Anforderungen anpassen lassen und zusätzliche Funktionen schneller integrieren können.

Wird Cybersecurity künftig auch ein Wettbewerbsfaktor im Maschinenbau?

Kurzfristig empfinden viele Unternehmen Cybersecurity als zusätzliche Hürde. Langfristig sehe ich darin jedoch eher einen Vorteil. Europa ist mit seinen regulatorischen Anforderungen derzeit relativ weit vorne. Gleichzeitig beobachten wir ähnliche Entwicklungen auch in anderen Regionen der Welt, etwa in den USA oder in China. Unternehmen, die sich frühzeitig mit Cybersecurity beschäftigen, sind deshalb besser auf zukünftige globale Anforderungen vorbereitet.

Gibt es für bestehende Anlagen pragmatische Lösungen?

Ja. In vielen Fällen lassen sich Sicherheitsmechanismen über externe Gateways realisieren, wie sie z.B. auch HMS anbietet. Diese Geräte werden zwischen interne Produktionsnetzwerke und externe Systeme geschaltet und können den Datenverkehr gezielt absichern. Dadurch entsteht eine klare Trennung zwischen interner und externer Kommunikation. Für Maschinenbauer kann das ein relativ einfacher Weg sein, um Cybersecurity-Anforderungen umzusetzen, ohne die gesamte Architektur neu entwickeln zu müssen. ■