Cyber Resilience Act: Cybersicherheit für die industrielle Wärmebehandlung

Mike Löpke, Marko Kuzmits

Die Digitalisierung verändert auch die Wärmebehandlungsindustrie grundlegend. Moderne Anlagen sind zunehmend mit digitalen Plattformen vernetzt, die Prozessdaten erfassen, analysieren und Produktionsprozesse überwachen oder steuern. Mit dem Cyber Resilience Act (CRA) schafft die EU erstmals ein verbindliches Rahmenwerk für die Cybersicherheit digitaler Produkte und definiert Anforderungen an Entwicklung, Betrieb und Wartung industrieller Plattformen.

Ein Praxisbeispiel zeigt bereits heute die Relevanz von Cybersicherheit, unabhängig von neuen gesetzlichen Vorgaben. Bei einem mittelständischen Wärmebehandlungsunternehmen in Deutschland wurde erstmals ein routinemäßiger Penetrationstest des Produktionsnetzwerks durchgeführt, ausgelöst von steigenden Kundenanforderungen und Sicherheitsstandards wie zum Beispiel TISAX (Trusted Information Security Assessment Exchange) aus der Automobilindustrie.

Der umfassende Prüfbericht identifizierte zahlreiche Schwachstellen – von Warnhinweisen bis zu kritischen Sicherheitsrisiken. Betroffen waren Komponenten entlang der gesamten Infrastruktur, von Netzwerk-Switches bis zu Anlagensteuerungen und Reglern. Viele Systeme waren seit Jahren im Einsatz, teilweise ohne verfügbare Updates oder Herstellersupport.

Empfohlen wurden unter anderem der Austausch veralteter Regler sowie, wenn möglich, Firmware- und Netzwerkupdates.

In der Praxis ist dies jedoch oft schwer umsetzbar, da viele Systeme und Hersteller nicht auf moderne Cybersicherheitsanforderungen vorbereitet sind und entsprechende Modernisierungslösungen fehlen.

Cyber Resilience Act als regulatorischer Rahmen

Vor diesem Hintergrund gewinnt der Cyber Resilience Act (CRA) zunehmend an Bedeutung. Die EU-Verordnung schafft ein einheitliches Regelwerk für die Cybersicherheit von Produkten mit digitalen Elementen - in der Wärmebehandlung betrifft dies die Reglertechnik, Steuerungssoftware, Prozessleitsysteme und IoT-Plattformen.

Ziel der Verordnung ist es, digitale Produkte über ihren gesamten Lebenszyklus sicher zu entwickeln, zu betreiben und zu aktualisieren. Hersteller müssen somit Sicherheitsanforderungen frühzeitig berücksichtigen, Schwachstellen managen und Sicherheitsupdates bereitstellen.

Digitalisierung von Wärmebehandlungsanlagen

Parallel zu diesen regulatorischen Entwicklungen schreitet die Digitalisierung industrieller Wärmebehandlungsprozesse weiter voran. Anlagen werden zunehmend mit digitalen Plattformen verbunden, die Prozessdaten erfassen, analysieren und für die Optimierung

oder Dokumentation bereitstellen. Systeme wie das Prozessleitsystem FOCOS 4.0 von Aichelin und die IoT-Plattform QMULUS von UPC-Marathon stehen exemplarisch für diese Entwicklung. Beide Systeme bieten Steuerungs- und Reglerlösungen in verschiedenen Varianten an und ermöglichen die Überwachung, Dokumentation und Analyse von Wärmebehandlungsprozessen sowie Condition Monitoring und Prozessoptimierung.

Mit der zunehmenden Vernetzung – auch mit ERP-Systemen - rückt Cybersicherheit stärker in den Fokus. Plattformen wie QMULUS können in Cloud- oder lokalen Umgebungen betrieben werden und erfordern robuste Sicherheitskonzepte für Kommunikation, Datenmanagement und Zugriff.

In Nordamerika wurden vergleichbare Anforderungen bereits durch Programme wie Cybersecurity Maturity Model Certification (CMMC) etabliert. Entsprechende Anforderungen an sichere Softwarearchitekturen und kontrollierte Zugriffe sind daher seit Jahren Bestandteil der Entwicklung bei Aichelin.

Sicherheitsarchitektur moderner Industrieplattformen

Moderne Industrieplattformen berücksichtigen Cybersicherheit bereits in der Architektur. Die Kommunikation zwischen Anlagen, Edge-Systemen und Cloud-Infrastrukturen erfolgt über gesicherte Protokolle, während Daten sowohl während der Übertragung als auch bei der Speicherung verschlüsselt werden. Ein zentraler Aspekt ist die Resilienz der Infrastruktur. Cloud-Infrastrukturen arbeiten mit redundanten Rechenzentren, während Daten lokal zwischengespeichert werden können. Auch der Schutz sensibler Produktionsdaten ist wesentlich. Betreiber entscheiden, welche Daten verarbeitet oder anonymisiert werden. Abhängig von den Sicherheitsanforderungen kommen unterschiedliche Cloudmodelle, wie Gov-Cloud zum Einsatz.

Quelle: Aichelin Ges.m.b.H.

Bild 1: Cyber Resilience Act

Neben der Systemarchitektur ist auch die kontinuierliche Wartung entscheidend. Sicherheitsupdates, Software-Aktualisierungen und Hotfixes ermöglichen die Behebung neuer Schwachstellen ohne wesentliche Unterbrechung des Anlagenbetriebes.

Neue organisatorische Anforderungen

Der Cyber Resilience Act betrifft auch organisatorische Prozesse. Hersteller müssen künftig Mechanismen etablieren, um Sicherheitsvorfälle oder potenzielle Schwachstellen frühzeitig zu erkennen, zu dokumentieren und gegebenenfalls zu melden.

Dazu gehören Monitoring-Systeme zur Erkennung unautorisierter Zugriffe sowie Verfahren zur Bewertung und Dokumentation sicherheitsrelevanter Ereignisse. Dies erfordert geeignete technische Werkzeuge und eine stärkere Integration von Cybersicherheit in Entwicklungs- und Betriebsprozesse.

Fazit

Mit dem Cyber Resilience Act wird Cybersicherheit zu einem festen Bestandteil digitaler Industrieprodukte. Für die Wärmebehandlungsindustrie bedeutet dies, dass Software, Prozessleitsysteme und digitale Plattformen konsequent nach definierten Sicherheitsprinzipien entwickelt und betrieben werden müssen.

Als globaler Hersteller und Servicepartner industrieller Wärmebehandlungsanlagen ist die AICHELIN Group in diesem Bereich gut vorbereitet: Cybersicherheit wird zu einer zentralen Voraussetzung für den zuverlässigen Betrieb digital vernetzter Wärmebehandlungsanlagen.

AUTOREN

Dipl.-Math. Mike Löpke
United Process Controls GmbH
info@qmulus.ai

Dipl.-Wirt.-Ing. (FH) Marko Kuzmits
Aichelin Ges.m.b.H.
marko.kuzmits@aichelin.com