Sicherheitslücken – Kehrseite der Digitalisierung

So lange eine Industrieanlage reibungslos läuft, generiert sie Gewinn. Steht sie still und kommt es zu Produktionseinbussen, bringt sie dem Unternehmen schnell Verluste ein. Daher stellt die Verfügbarkeit der eigenen Produktionsstätten das wichtigste Gut für Industrieunternehmen dar.

Johannes Raff

Die digitale Transformation des Industriesektors führt zu einer deutlichen Erhöhung dieser Verfügbarkeit: Dies, indem sämtliche Maschinen, Fertigungsschritte sowie die Logistik miteinander digital verbunden werden. Das Resultat ist eine durchgehende Produktionskette, die einen hohen Automatisierungsgrad aufweist und somit effizient und gleichzeitig kostengünstig operiert.

Nicht alles eitel Sonnenschein

Doch neben diesen klaren Vorteilen machen Branchenkenner immer wieder auch auf Gefahrenszenarien aufmerksam. Denn die Digitalisierung hat eine Kehrseite: Kommt es zu einem technischen Problem oder gar einem «Angriff von aussen», beschränkt sich der potenzielle Schadensradius nicht mehr nur auf eine einzelne Maschine oder Anlage – sondern kann im schlimmsten Fall die gesamte Fertigungskette betreffen. Stehen dann in der Folge die Maschinen still, bzw. kommt es zu einem länger andauernden Produktionsstopp, kann das gerade für KMU schnell existenzbedrohend werden.

Weshalb kommt es trotz des hohen Niveaus an Innovation in der Industrie zu dieser grossen Bandbreite an Schwachstellen und wie unterbindet man Sicherheitsvorfälle präventiv? Und mit welchen konkreten Gefahrenszenarien hat man es zu tun?

Der erste Schritt in Richtung «mehr Sicherheit» muss nicht in den Fertigungshallen der Unternehmen geschehen – sondern in den Köpfen des Managements. Denn die Anlagenbetreiber müssen sich zuerst im Klaren darüber sein, dass sie neu zu den potenziellen Zielen von Cyberkriminellen und Industriespionen gehören. Diese Angriffe, gezielt oder wahllos, häufen sich kontinuierlich und betreffen Unternehmen jeder Grösse.

Grosse Komplexität

Die Digitalisierung als Treiber der Vernetzung stellt die Betriebsteams von Produktionsanlagen vor ähnliche Herausforderungen wie im Facility Management oder beim Betrieb von grossflächig verteilten Sensoren und Anlagen. Die Komplexität liegt in einer Vielzahl von Protokollen (SCADA, ICS, S7, usw.), Herstellern und individuell konstruierten Anlagen und Applikationen.

Zulieferer sollten optimalerweise bereits vor der Inbetriebnahme auf die Anlagen zugreifen können. Dies, ohne grosse Aufwände in IT- und OT-Teams zu generieren, welche von einer Vielzahl von Individuallösungen zurecht überwältigt sind.

Fernwartung als Gefahr?

Einer der ganz grossen Vorteile der Digitalisierung im Industriebereich ist die Möglichkeit der «Predictive Maintenance». Zu diesem Zweck überwacht der Maschinenhersteller oder Betreiber das Gerät beim Kunden kontinuierlich. Dank dieser ständigen Beobachtung kann etwa ein Ausfall einer Maschinenkomponente vorausgesagt und die Wartung präventiv angesetzt werden. Auf diese Weise lassen sich Stillstandzeiten minimieren und mit anderen Anlagen kompensieren.

Muss das Rad neu erfunden werden?

Die Technologien aus Industrie und IT verschmelzen immer weiter, dies sollte auch bei der Industrial Security der Fall sein. Für viele Problemstellungen gibt es bereits Erfahrungen und Lösungen aus der Cyber-Security. So ist es erforderlich, eine zentrale IAM-Lösung (Identity und Access Management) für alle Zugriffe auf die Produktionsanlagen zu gewährleisten, Daten beim Transport zu verschlüsseln und Anlagen voneinander zu trennen, um so die Gefahr einer Infizierung einzudämmen. Cyber Defense Mechanismen sollten direkt an der Anlage, Verhaltensanalyse und Security Event Management zentral über alle Komponenten umgesetzt werden.

Um diesen Herausforderungen in einem Produktionsumfeld begegnen zu können, müssen die Komponenten mit den individuell konstruierten Anlagen und Protokollen umgehen, um auf stetig wechselnde Anforderungen reagieren können. Dies wird per automatisiertem Deployment und Template basierter Konfiguration möglich.

Ein flexibles IT-Sicherheitsmanagement ist essenziell. Es muss agil auf neue Gefahrenszenarien reagieren und potenzielle Sicherheitsvorfälle antizipieren können. Hierfür empfiehlt sich eine Kooperation mit einem externen Sicherheitsdienstleister. Diese spezialisierten Unternehmen sind in der Lage, die technischen Anlagen Stresstests zu unterziehen und gezielt Schwachstellen aufzudecken. Die Sicherheit sollte nicht an die interne IT-Abteilung delegiert, sondern als zentrale Managementaufgabe wahrgenommen werden. ■

JOHANNES RAFF
Clue Security Services AG, Baar