

Lebensmittelindustrie: Reduzierung von Cybersecurity-Bedrohungen

Categories : [Ex-Schutz & Anlagensicherheit](#), [Food](#), [Im Fokus](#), [Meldungen](#)

Date : 10. Februar 2021

Eine Investition in Automatisierung und IIoT-Technologien (Industrie 4.0) bringt für Hersteller in der Lebensmittelindustrie deutliche Vorteile. Dazu gehört die Fähigkeit, fehlerhafte Ausrüstung frühzeitig zu erkennen und Ausfallzeiten zu reduzieren – mit dem Ziel, die Qualität zu verbessern und die Produktion zu maximieren. Werden nun IIoT-Geräte in einem Netzwerk verwendet, können Daten in Echtzeit gesammelt und analysiert werden, um die erforderlichen Maßnahmen zur Gewährleistung der Lebensmittelsicherheit zu identifizieren. Je mehr Anlagen jedoch digitalisiert werden, desto größer wird die Gefahr für Cybersecurity-Angriffe. Ein kürzlich veröffentlichter Bericht von Imperva deckte auf, dass während der COVID-19-Pandemie gezielte Angriffe auf die Lebensmittelindustrie in vielen Ländern zugenommen haben. In der Folge zögerten viele Hersteller, effizienz- und produktivitätssteigernde Lösungen umzusetzen.

Obwohl es Normen zur Sicherheit von Automatisierungstechnologien gibt, besteht in der Lebensmittelindustrie das spezifische Problem der Komplexität der Anlagen und Systeme, die oft einzeln nacheinander implementiert werden, was zu unzusammenhängenden Systemen, veralteter Ausrüstung und einer Reihe von Schwachstellen führen kann. Laut einer Studie des Instituts Food Protection and Defence Institute (FPDI), die vom Ministerium für Innere Sicherheit der USA unterstützt wurde, sind in der Lebensmittelproduktion eingesetzte Industrielleitsysteme (Industrial Control System/ICS) zunehmend Cyber-Angriffen ausgesetzt. Die Notwendigkeit, unsere Lebensmittelversorgung zu schützen, verstärkt die Bedeutung guter Sicherheitsverfahren im Internet bei Lebensmittelherstellern zusätzlich. Einer der größten Faktoren dieser wachsenden Bedrohungen ist die weit verbreitete Verwendung überholter ICS. Legacy-Systeme bringen erhöhte Sicherheitsbedenken mit sich, und die Notwendigkeit, ein hohes Maß an Übereinstimmung mit den Inhaltsstoff-verhältnissen aufrechtzuerhalten, erfordert zuverlässige und sichere Abläufe, um wettbewerbsfähig zu bleiben und Rendite zu erzielen. Aus diesem Grund muss das für die Anlagenleitsysteme zuständige Personal mit Cybersecurity-Tools wie Firewalls, Endpoint Protection, Netzwerk-Switches, Sicherheitspatches, Sicherheitsüberwachung und der Attackenerkennung vertraut sein, was normalerweise in den Zuständigkeitsbereich von IT-Abteilungen fällt. Dies hat zur Folge, dass die Zusammenarbeit zwischen der IT-Abteilung und der Abteilung für Prozesssteuerung zunehmend an Bedeutung gewinnt, insbesondere wenn ein Unternehmen die Anlage einer digitalen Transformation unterzieht bzw. Altsysteme auf den neuesten Stand bringt. Industrie 4.0 (IIoT) und die Einführung neuer Technologien bedeuten oft Abhängigkeiten von mobilen, Wireless- und externen Systemen sowie Cloud-basierte Systeme, die - obwohl sie in der Regel effizienter sind - die Angriffsfläche für diejenigen vergrößern, die Schaden anrichten wollen.

Unternehmen sind verschiedenen Gefahren ausgesetzt, von unabsichtlichen Insider-Regelverstößen bis hin zu gezielten Angriffen krimineller Organisationen, wobei die größte Sorge darin besteht, dass Prozessbedingungen beeinträchtigt werden und Produkte unzureichend sterilisiert werden, was zu Lebensmittelvergiftungen und Rückrufaktionen führen kann. Daher ist es wichtig, eine Cybersecurity-Kultur im gesamten Unternehmen aufzubauen und zu pflegen - und zwar von der Chefetage bis hin zum Anlagenpersonal, wo auch immer sich ein Vorfall ereignen kann. Die Vereinheitlichung des Sprachgebrauchs über betriebliche und geografische Grenzen hinweg ist der Schlüssel für eine erfolgreiche Strategie, ein Betriebskonzept und bei Bedarf ein Verfahren zur Reaktion auf Vorfälle. Es ist zwingend erforderlich, dass Unternehmen bei der Identifizierung von Schwachstellen und der Einbindung des digitalen Risikomanagements in die tägliche Geschäftspraxis wachsam bleiben. Entscheidend ist, geeignete Schutzsysteme einzusetzen. Neue Leitsysteme gewährleisten mehr Sicherheit im Betrieb,

allerdings liegen die größten Herausforderungen im Schutz der installierten Basis.

Definition der IIoT-Cybersecurity

Daten existieren in der Regel in drei Bereichen der Anlage: Sicherheit, Steuerung und Analyse. Aus IIoT-Sicht sollten Daten in den Sicherheits- und Steuerungsbereichen nur zur Überwachung oder für den Lesezugriff bestimmt sein, und teilweise werden Datendioden oder andere Sicherheitskontrollen verwendet, um sicherzustellen, dass dies strikt eingehalten wird. Die Trennung der Möglichkeiten hinsichtlich der Anlagenbereiche ist von höchster Bedeutung für den Erhalt der betrieblichen Integrität und Sicherheit in jedem einzelnen Bereich. Im Analysebereich ist es entscheidend, dass Architektur- und Betriebssicherheit aufrechterhalten werden können, um Zugriffe auf oder Schäden an Sicherheits- und Kontrollfunktionen zu vermeiden.

Da es die meisten IIoT-Lösungen sowohl im IT- als auch im OT-Bereich gibt, ist es für fachspezifische Experten wichtig, den passenden Plan aufzustellen, mit dem das richtige Maß an Sicherheit erzielt werden kann. Es gibt unzählige Normen und Verfahren, die sich um das Thema IIoT drehen; es ist jedoch nicht immer einfach herauszufinden, welche den richtigen Ansatz und das richtige Maß bieten. Die Antwort liegt vermutlich in einer Kombination verschiedener Normen wie IEC 62443 und IEC 27000.

Die Ziele der Beteiligten in IT und OT müssen ebenfalls überprüft sowie Anforderungen formuliert werden, um Lücken und Betriebsrisiken zu vermeiden. Es ist wichtig zu verstehen, welche Stärken die jeweiligen Funktionen haben und wie Geschäftsziele erreicht werden können, während ein Höchstmaß an Sicherheit zu wahren ist. Jeder Experte bringt etwas anderes vor, da die IT einen hoch standardisierten Prozess und die OT eine technisiertere Lösung bevorzugt. In diesem Bereich ist Zusammenarbeit ein Muss.

Unternehmen sollten darüber hinaus festlegen, wer für einzelne IIoT-Lösungen verantwortlich ist. Es sollte eine Matrix erarbeitet werden, um Hauptzuständigkeitsbereiche sowie die richtigen Ressourcen und Qualifikationen zu bestimmen, die für den Betrieb und die Pflege der Lösungen benötigt werden. Es wird befürchtet, dass neue Verbindungen für das IIoT das Sicherheitsniveau senken, wenn jedoch vertrauenswürdige Bereiche, Leitungen und Systemeingriffe angemessen gesichert werden, muss dies nicht der Fall sein, obwohl unterschiedliche Überwachungs- und Verwaltungsgrade erforderlich sein können.

Ein kompletter Austausch ist nicht notwendig

Der möglicherweise beste Ansatz: Klein anfangen und die Bemühungen ausbauen. Unternehmen können mit den vorhandenen Lösungen beginnen und diese Technologie optimal nutzen, um Kosten gering zu halten und gleichzeitig ein höheres Sicherheitsniveau zu erreichen. Dafür sind einige Arbeiten nötig, da Cybersecurity oft komplex ist und kontinuierliche Verbesserung erfordert. Um eine sichere Interoperabilität zwischen Legacy-Systemen ohne moderne Sicherheitsfunktionen und neuen IIoT-Lösungen zu erreichen, ist häufig eine technische Lösung erforderlich. Dafür müssen der Endnutzer und der ICS-Anbieter eng zusammenarbeiten, um sichere Lösungen zu schaffen, die die Anforderungen und Ziele erfüllen. Die Technologie ist aber nur ein Baustein der Lösung, da auch das Personal einen entscheidenden Anteil an einer sicheren digitalen Transformation hat.

Neue Sicherheitsansätze

Um OT- und IT-Umgebungen zusammenzuführen, sind neue Sicherheitsansätze von Nöten. Secure First Mile™ Konnektivität ist einer dieser Ansätze, der Architekturen bietet, die die sichere Übertragung von Anlagendaten hin zu externen Anwendungen, Experten-Diensten bzw. mobilen Anwendern vereinfachen. Die sichere Übertragung von Sensordaten in der OT-Umgebung an Analyse-Tools oder Dienste in der IT-Umgebung kann mit verschiedenen Architekturen erreicht werden, wobei die vorhandene Infrastruktur der Anlage oft den besten Ansatz vorgibt.

Cloud-Sicherheit

Auch wenn sie sich nicht für jede Anwendung oder jedes System eignen, werden Cloud-Technologien als Teil einer Gesamtlösung für die Bereitstellung von Echtzeitdaten von Anlagen oder bestimmten Betriebsteilen immer beliebter. Private, Public und Hybrid Clouds sind Methoden für das Hosting und die Bereitstellung von Rechenleistung und Anwendungen. Die Auswahl richtet sich sowohl nach den Kosten als auch nach Sicherheitsoptionen. Cloud-Anbieter wie Microsoft bieten ungemein effektive Verfahren für sichere Lösungen. Microsoft investiert fast 1 Mrd. Euro jährlich in Cybersecurity. Einige Vorteile dieser Investition sind zertifizierte Datenzentren, sichere Konnektivitätslösungen und Spitzentechnologien, um eine sichere Konnektivität zwischen Endnutzernetzwerken und Geräten zu bewerkstelligen. Andere Vorteile sind Data Governance und Datenschutz, Geofencing von Daten, Vermeidung von Datenlecks, gemeinsame Datennutzung sowie zuverlässigere Backup- und Wiederherstellungssysteme, die zum Schutz Ihrer Daten native Cloud-Funktionen nutzen.

Fazit

Der Einsatz der richtigen Systeme zum Schutz vor digitalen Bedrohungen ist entscheidend für die Gewährleistung einer sicheren Lebensmittelversorgung und eines zuverlässigen Betriebs. Jedes Unternehmen ist einzigartig und erfordert einen zielgerichteten Ansatz bei der Auswahl der Technologien und Qualifikationen, die die Anforderungen am besten erfüllen. Dieser Schutz vor den Bedrohungen der Gegenwart und Zukunft fällt nicht einer einzelnen Person oder Technologie zu. Er ist nur durch Zusammenarbeit und die sogenannte Ownership Culture - wie bei der Industriesicherheit – zu erreichen. Cyber-Sicherheit ist keine „Angelegenheit“ sondern eine „Verpflichtung“ für das Unternehmen. Hierzu braucht es Menschen, Prozesse und Technologien. Es gibt keine Wundermittel, keine Abkürzung und keine einfache Verfahrensweise, um die grundlegenden Ebenen der Cybersecurity zu erreichen.