txOne networks

KURZFASSUNG

Ein Rezept für Stabilität

Stärkung der Cybersicherheit in der Lebensmittel- und Getränkeindustrie

Während die Integration von internetfähigen Technologien im Lebensmittel- und Getränkesektor die Abläufe revolutioniert, bringt sie auch erhebliche Herausforderungen in die Cybersicherheit mit sich. Die Lebensmittel- und Getränkeindustrie steht weltweit an siebter Stelle der am häufigsten angegriffenen Branchen und leidet unter erheblichen wirtschaftlichen Verlusten durch Ransomware und andere Cyberbedrohungen. Dieses E-Book befasst sich mit diesen dringenden Herausforderungen und bietet strategische Einblicke sowie praxisorientierte Lösungen, die darauf abzielen, die OT-Cybersicherheitsabwehr in der Lebensmittel- und Getränkelieferkette zu stärken. Durch das Verständnis und die Umsetzung dieser Maßnahmen können Organisationen sich gegen aufkommende Bedrohungen schützen und ihre "Golden Batch" in Produktionsumgebungen bewahren.

Die rapide Einführung von vernetzten landwirtschaftlichen Maschinen, Datenerfassungstools und Verarbeitungsanlagen führt zu einer Erweiterung der Angriffsfläche, was Unternehmen zunehmend anfällig für böswillige Aktivitäten macht. Die Kombination von veralteten Altsystemen und neuen Technologien schafft zusätzliche Schwachstellen, da ältere Systeme möglicherweise nicht über aktuelle Sicherheitsmaßnahmen verfügen. Diese Situation wird durch die zunehmende Abhängigkeit von Drittanbietern für Software und Technologie verschärft, da ein Cyberangriff an einer beliebigen Stelle im Netzwerk alle verbundenen Anbieter gefährden kann.

Cyberkriminelle richten ihre Aufmerksamkeit zunehmend auf die Lebensmittel- und Getränkeindustrie, angelockt von „leichter erreichbaren Zielen" und motiviert durch finanzielle Gewinne oder Umweltaktivismus. Angriffsvektoren umfassen Social Engineering, die Ausnutzung von Software-Schwachstellen und die direkte Manipulation kritischer Systeme durch Insider. Diese Bedrohungen bergen ernsthafte Risiken, darunter Betriebsunterbrechungen oder Gesundheits- und Sicherheitsprobleme, die schwerwiegende Folgen für Unternehmen und Verbraucher haben können.

Jüngste Gesetzesänderungen, wie die EU-NIS2-Richtlinie und der Cyber Resilience Act, erhöhen den Druck, indem sie neue Cybersicherheitsanforderungen für Unternehmen in der Lebensmittelproduktion und -verteilung auferlegen. Mittelständische und große Unternehmen sehen sich nun mit einer Reihe strenger Compliance-Verpflichtungen konfrontiert, während kleinere Unternehmen je nach ihrer Bedeutung ebenfalls davon betroffen sein können.

Um ihre Sicherheitsmaßnahmen zu verstärken, den neuen Vorschriften zu entsprechen und die Lieferkette vor Störungen zu schützen, sollten Organisationen in die folgenden 7 Kernpraktiken investieren:

Bedrohungserkennung

Führen Sie eine dokumentierte Liste branchenspezifischer Bedrohungen und implementieren Sie Systeme zur Erkennung und Benachrichtigung bei Abweichungen vom normalen Betrieb.

Drittanbieter-Bewertung

Bewerten Sie regelmäßig die Cyberrisiken im Zusammenhang mit OT/ICS-Assets und Drittanbietern.

Vulnerability Management

Wenden Sie Patches umgehend an oder nutzen Sie virtuelle Patches für sofortigen Schutz.

Netzwerksegmentierung

Segmentieren Sie Netzwerke, um den Zugriff zu beschränken und Bedrohungen einzudämmen.

Kontrolle nicht autorisierter Geräte

Implementieren Sie Richtlinien, um nicht autorisierte Geräte und Medien zu blockieren.

Mit dem Internet verbundene Dienste

Vermeiden Sie es, anfällige Dienste im Internet zugänglich zu machen.

Incident Response

Entwickeln und aktualisieren Sie Incident-Response-Pläne und führen Sie regelmäßige Übungen durch.

Laden Sie das E-Book herunter, um praxisnahe Einblicke von unseren Experten zu erhalten und Ihre Cybersicherheitsstrategie zu unterstützen.

E-Book kostenlos herunterladen