txOne networks

Einblicke in die Industrie

Cybersicherheitstrends für die Lebensmittel- und Getränkeindustrie

Betriebsstörungen in der Lebensmittel- und Getränkeindustrie können auf dem Feld, auf dem Bauernhof, in der Fabrik oder auf der Vertriebs- und Einzelhandelsebene beginnen. Mit der fortschreitenden Digitalisierung der Abläufe in jeder Phase der Lieferkette, werden die Angriffsflächen immer größer, wodurch Unternehmen zunehmend anfälliger für böswillige Aktivitäten werden. Angesichts einiger hochkarätiger Angriffe, die kürzlich Schlagzeilen gemacht haben, werfen wir einen genaueren Blick auf die Motivationen der Bedrohungsakteure, die den Sektor ins Visier nehmen, die Angriffstrends und die finanziellen Auswirkungen krimineller Aktivitäten auf die betroffenen Organisationen.

Häufigkeit der Angriffe

Die Lebensmittel- und Getränkeindustrie steht weltweit an siebter Stelle der am häufigsten angegriffenen Branchen und **musste im Jahr 2023 5,5 %[1] aller Ransomware-Angriffe verkraften.**

[1]Global AG Tech Initiative (April 2024). Die Realität von Ransomware-Angriffen in der Landwirtschaft

Anzahl der Cybersicherheitsvorfälle in der Lebensmittelindustrie nach Jahr

Jahr	Anzahl der Vorfälle
2018	2
2019	5
2020	45
2021	65
2022	38
2023	39

Bis Februar 2024 wurden 7 Ransomware-Angriffe in der Industrie gemeldet, was auf einen potenziellen Anstieg der Gesamtzahl der Ransomware-Angriffe für das Jahr gegenüber 2023 hindeutet.

Top 10 Länder nach Anzahl der Ransomware-Angriffe auf Unternehmen der Lebensmittel- und Getränkeindustrie[2]

[2]Rebecca Moody (Juni 2023). Comparitech, „Worldwide Food beverage ransomware attacks"

Motivationen, Taktiken und Ziele von Bedrohungsakteuren

Top 3 Gründe, warum Cyberkriminelle die Lebensmittel- und Getränkelieferkette ins Visier nehmen:

Finanzieller Gewinn

Hacktivismus für Umweltschutz

Verursachung öffentlicher Schäden

Alphv, Revil, LockBit, Play und BlackBasta waren die häufigsten Ransomware-Stämme, die gegen Unternehmen der Lebensmittel- und Getränkeindustrie eingesetzt wurden

Anteil der Ransomware-Angriffe nach Organisationstyp im Jahr 2022[3]

[3]Rebecca Moody (Juni 2023). Comparitech, „Worldwide Food beverage ransomware attacks"

Die Auswirkungen eines Cyberangriffs

- Störung in Produktion und Vertrieb
- Erhöhte Verschwendung von Rohstoffen oder Fertigerzeugnissen
- Mögliche Engpässe bei Lebensmitteln/Zutaten
- Preiserhöhungen
- Höhere Gesundheits- und Sicherheitsrisiken
- Rufschädigung

2018 - Mai 2023

Weltweite wirtschaftliche Kosten durch Ausfallzeiten*

1,36 Mrd. USD[4]

*infolge von Ransomware-Angriffen auf Lebensmittel-, Getränke- und Landwirtschaftsunternehmen

[4]Rebecca Moody (Juni 2023). Comparitech, „Worldwide Food beverage ransomware attacks"

Ein bewährtes Rezept für Sicherheit

TXOne Networks sichert den Betrieb von mehr als 3.600 Unternehmen weltweit mit Lösungen für Cybersicherheit, die auf ICS- und OT-Umgebungen zugeschnitten sind. Unsere Lösungen basieren auf dem OT-Zero-Trust-Prinzip und schaffen maßgeschneiderte, OT-native Sicherheitsrichtlinien, die darauf abzielen, die Lieferkette für Lebensmittel und Getränke vor bösartigen Angriffen zu schützen und die betriebliche Kontinuität sicherzustellen.

Durch den Einsatz fortschrittlicher Technologien und Expertenwissen bieten wir einen ganzheitlichen Ansatz für Cybersicherheit, der Inspektionen vor der Dienstleistung, Endpoint- und Netzwerkschutz während der Onboarding-, Staging-, Produktions- und Wartungsphasen umfasst.

Erfahren Sie, wie TXOne Ihr Unternehmen mit OT-nativen Lösungen sichern kann, die Ihre Assets während ihres gesamten Lebenszyklus schützen.

Kontaktieren Sie uns