

Fornire approfondimenti di settore



Tendenze sulla sicurezza informatica per l'industria alimentare e delle bevande

La disruption nel settore alimentare e delle bevande può avere origine sul campo, in fattoria, in fabbrica o a livello di distribuzione e vendita al dettaglio. Con la continua digitalizzazione delle operazioni in ogni fase della filiera, le superfici di attacco si stanno ampliando, rendendo le organizzazioni sempre più vulnerabili e suscettibili a attività dannose. Alla luce di alcuni attacchi di alto profilo che hanno recentemente attirato l'attenzione, analizziamo più da vicino le motivazioni degli attori delle minacce che prendono di mira il settore, le tendenze degli attacchi e l'impatto finanziario delle attività dei criminali informatici sulle loro vittime.

Frequenza degli attacchi

Il settore della produzione alimentare e delle bevande è il settimo più colpito a livello globale, subendo il **5,5% di tutti gli attacchi ransomware nel 2023**.

¹Global AG Tech Initiative (April 2024). La realtà degli attacchi ransomware in agricoltura

Numero di incidenti di sicurezza informatica nel settore alimentare per anno

Anno	Numero di incidenti
2018	2
2019	5
2020	45
2021	65
2022	38
2023	39

A febbraio 2024, erano stati segnalati 7 attacchi ransomware nel settore, suggerendo un possibile incremento del numero totale di attacchi ransomware quest'anno rispetto al 2023.

I primi 10 paesi per numero di attacchi ransomware alle aziende alimentari e delle bevande²



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

Motivazioni, strategie e obiettivi degli attori della minaccia

Le tre principali motivazioni per cui i criminali informatici prendono di mira la filiera alimentare e delle bevande:



Alphv, Revil, LockBit, Play e BlackBasta sono stati i ceppi di ransomware predominanti nelle attacchi alle organizzazioni del settore alimentare e delle bevande.

Quota di attacchi ransomware per tipo di organizzazione nel 2022³



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

L'impatto di un attacco informatico

Interruzioni nella produzione e distribuzione

Aumento dello spreco di materie prime o prodotti finiti

Potenziati carenze di cibo/ingredienti

Aumenti dei prezzi

Aumento dei rischi per la salute e la sicurezza

Danni alla reputazione

2018-2023

Costi totali per l'economia mondiale dovuti a tempi di inattività*

1,36 miliardi di dollari

*causati da attacchi ransomware contro aziende del settore alimentare, delle bevande e agricolo tra il 2018 e maggio 2023.

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

Una ricetta comprovata e testata per la sicurezza

TXOne Networks protegge le operazioni di oltre 3.600 organizzazioni in tutto il mondo con soluzioni di sicurezza informatica su misura per ambienti ICS e OT. Le nostre soluzioni si fondano su un approccio zero trust per l'OT, sviluppando policy di sicurezza personalizzate, intrinsecamente legate all'OT e progettate per garantire la sicurezza. Ci impegniamo a proteggere il settore alimentare e delle bevande dagli attacchi dannosi e a garantire la continuità operativa.

Grazie all'uso di tecnologie avanzate e alla consulenza di esperti, proponiamo un approccio olistico alla sicurezza informatica, che include l'ispezione pre-servizio, la protezione degli endpoint e la difesa della rete durante le fasi di onboarding, messa in scena, produzione e manutenzione.

Scopri come TXOne può proteggere la tua organizzazione con soluzioni OT native che proteggono i tuoi asset durante il loro intero ciclo di vita.

[Contattaci](#)

