txOne networks

SINTESI ESECUTIVA

Una ricetta per la resilienza

Rafforzare la sicurezza informatica nel settore del food & beverage

Da un lato, l'integrazione delle tecnologie connesse a Internet nel settore alimentare e delle bevande sta trasformando le operazioni; dall'altro, presenta anche notevoli sfide per la cybersecurity. Questo settore è diventato il settimo più bersagliato a livello globale, subendo ingenti perdite economiche a causa di ransomware e altre minacce informatiche. Questo ebook esplora queste problematiche urgenti, fornendo spunti strategici e soluzioni pratiche per rafforzare le difese di cybersecurity OT nella catena di approvvigionamento alimentare e delle bevande. Attraverso la comprensione e l'implementazione di queste misure, le organizzazioni possono proteggersi dalle minacce emergenti e preservare il loro patrimonio negli ambienti di produzione.

L'espansione delle superfici di attacco, causata dalla rapida adozione di macchinari agricoli interconnessi, strumenti di raccolta dati e strutture di elaborazione, sta rendendo le organizzazioni sempre più vulnerabili a minacce dannose. La presenza di sistemi legacy obsoleti, insieme a tecnologie più recenti, amplifica ulteriormente queste vulnerabilità, poiché i sistemi più datati potrebbero non avere misure di sicurezza aggiornate. La situazione è ulteriormente complicata dalla crescente dipendenza da fornitori terzi per software e tecnologia, dove una violazione informatica in qualsiasi punto della rete può compromettere tutti i fornitori connessi.

Attratti da obiettivi più facili, i criminali informatici stanno spostando la loro attenzione sul settore alimentare e delle bevande, motivati da ragioni che spaziano dal guadagno finanziario all'attivismo ambientale. I metodi di attacco comprendono l'ingegneria sociale, l'approfittamento delle vulnerabilità software e la manomissione diretta dei sistemi critici da parte di operatori interni. Queste minacce comportano gravi rischi, tra cui interruzioni operative e problemi di salute e sicurezza, con potenziali conseguenze significative per le aziende e i consumatori.

Le recenti modifiche legislative, tra cui la direttiva UE NIS2 e il Cyber Resilience Act, stanno esercitando una crescente pressione, imponendo nuovi requisiti di sicurezza informatica alle entità operanti nella produzione e distribuzione alimentare. Le organizzazioni di medie e grandi dimensioni si trovano ora a dover affrontare una serie di obblighi di conformità rigorosi, mentre anche le imprese più piccole potrebbero essere coinvolte a seconda della loro rilevanza.

Per potenziare le difese di sicurezza informatica industriale, adeguarsi alle nuove normative e proteggere l'intera supply chain da possibili interruzioni, le organizzazioni dovrebbero adottare e investire nelle seguenti sette pratiche fondamentali:

Rilevamento delle minacce

Mantenere un elenco documentato delle minacce specifiche del settore e implementare sistemi per rilevare e segnalare le deviazioni dalle operazioni normali.

Validazione di terze parti

Valutare regolarmente i rischi informatici associati agli asset OT/ICS e ai fornitori di terze parti.

Gestione delle vulnerabilità

Applicare tempestivamente le patch o utilizzare patch virtuali per una protezione immediata.

Segmentazione della rete

Segmentare le reti per limitare l'accesso e contenere le minacce.

Controllo dei dispositivi non autorizzati

Implementare politiche per bloccare dispositivi e supporti non autorizzati.

Servizi esposti a Internet

Evitare di esporre servizi vulnerabili su Internet.

Risposta agli incidenti

Sviluppare e aggiornare i piani di risposta agli incidenti, conducendo esercitazioni regolari.

Scaricate l'eBook per ottenere informazioni utili dai nostri esperti e supportare la vostra strategia di cybersecurity OT.

Ricevete copia gratis