Capgemini press contacts:
Tiziana Sforza
Marketing & Communication
tiziana.sforza@capgemini.com
+39 348 7018984

Più della metà delle imprese manifatturiere prevede un aumento degli attacchi informatici nei prossimi 12 mesi, ma solo poche sono pronte a intervenire

Milano, 30 giugno 2022 – Da un nuovo report del Capgemini Research Institute emerge che il 51% delle imprese manifatturiere ritiene che il numero di attacchi informatici nelle smart factory[1] sia destinato ad aumentare nei prossimi 12 mesi, ma nonostante ciò quasi la metà (47%) afferma che la cybersecurity in ambito smart factory non sia una priorità per i C-level. Secondo il report, dal titolo *"Smart & Secure: Why smart factories need to prioritize cybersecurity"*, ben poche aziende manifatturiere dispongono infatti di procedure consolidate di cybersecurity, nonostante la natura stessa delle smart factory aumenti esponenzialmente i rischi di attacchi informatici nell'era dell'Intelligent Industry.

Circa il 53% delle organizzazioni del settore, in particolare il 60% di quelle attive nell'industria pesante e il 56% di quelle del settore farmaceutico e Life Sciences, riconosce che in futuro le smart factory saranno il principale bersaglio degli attacchi informatici. Tuttavia, un alto livello di consapevolezza non si traduce automaticamente in altrettanta preparazione a livello aziendale: la mancanza di attenzione da parte del management, il budget limitato e i fattori umani risultano i principali ostacoli per un'efficace cybersecurity nelle aziende manifatturiere.

Francesco Fantazzini, **CIS Italy Managing Director di Capgemini**, ha dichiarato: *"I vantaggi della digital transformation spingono le aziende manifatturiere a investire significativamente nelle smart factory, ma se le pratiche di cybersecurity non vengono implementate fin dall'inizio, gli sforzi potrebbero essere vanificati in un batter d'occhio. Un maggior numero di dispositivi connessi, in particolare di operational technology (OT) e Industrial Internet of Things (IIOT), rende le smart factory un facile bersaglio per gli attacchi informatici. Se questo aspetto non diventa prioritario per le aziende, le stesse faticheranno ad affrontare queste sfide, educare dipendenti e fornitori e facilitare la comunicazione tra i team di cybersecurity e la dirigenza".*

Le organizzazioni devono affrontare numerosi ostacoli per migliorare la cybersecurity nelle smart factory

Lo studio evidenzia che, per molte organizzazioni, la cybersecurity non viene contemplata tra gli elementi prioritari in fase di progettazione: solo il 51% la implementa infatti di default nelle proprie smart factory. A differenza delle piattaforme IT, non tutte le organizzazioni potrebbero inoltre essere in grado di analizzare le apparecchiature di una smart factory mentre queste sono in funzione.

La visibilità a livello di sistema dei dispositivi IIOT e OT è indispensabile per rilevare eventuali violazioni: il 77% degli intervistati considera il ripetuto ricorso a processi non convenzionali per la riparazione o

[1] Le smart factory sfruttano piattaforme e tecnologie digitali per ottenere miglioramenti significativi in termini di produttività, qualità, flessibilità e servizio. Si basano su tre tecnologie digitali chiave: connettività (utilizzando l'Industrial Internet of Things per raccogliere dati attraverso i sensori), automazione intelligente (ad es. robotica avanzata, visione artificiale, controllo distribuito, droni, ecc.) e gestione e analisi dei dati in cloud.

l'aggiornamento dei sistemi OT e IIOT nelle smart factory come una fonte di preoccupazione. Questo problema deriva in parte dalla scarsa disponibilità di tool e processi adeguati, ma per una percentuale significativa di intervistati (51%) le minacce informatiche alla smart factory derivano soprattutto dalla propria rete di partner e fornitori. Il 28% ha inoltre affermato che il numero di dipendenti che hanno introdotto in rete dispositivi infettati da virus per installare o aggiornare i macchinari delle smart factory è cresciuto del 20% dal 2019 a oggi.

La principale minaccia alla cybersecurity è rappresentata dalle persone, non dalla tecnologia

Per quanto riguarda gli attacchi informatici, sono poche le organizzazioni intervistate che affermano che i team di cybersecurity dispongono delle conoscenze e delle competenze necessarie per introdurre tempestivamente patch di sicurezza senza supporto esterno. Una causa diffusa di questa inadeguatezza è la mancanza di una figura dedicata alla cybersecurity che gestisca il programma di aggiornamento richiesto.

Un altro problema è relativo alla scarsità di competenze legate alla cybersecurity in ambito smart factory: per il 57% delle organizzazioni è infatti molto più evidente rispetto a quella in ambito IT. Secondo molte imprese, le motivazioni sono da riscontrare nella vasta gamma di dispositivi OT e IIOT da monitorare per rilevare e prevenire i tentativi di violazione, e anche i responsabili della cybersecurity dichiarano di non essere in grado di rispondere efficacemente agli attacchi informatici nelle smart factory e nei siti produttivi.

La mancanza di collaborazione tra i responsabili delle smart factory e i Chief Security Officer è un altro tema di preoccupazione per oltre la metà degli intervistati: questa difficoltà nella comunicazione ostacola la capacità delle organizzazioni di individuare tempestivamente gli attacchi informatici, peggiorando l'entità dei danni.

Le aziende leader nella cybersecurity ottengono un vantaggio competitivo

Il report evidenzia che i "Cybersecurity Leader", capaci di adottare procedure consolidate in termini di awareness, preparazione e implementazione della cybersecurity nelle smart factory, ottengono un vantaggio competitivo sotto diversi punti di vista. Le aree in cui si registrano i maggiori benefici sono il riconoscimento tempestivo dei modelli di attacco informatico (74%) e la riduzione dell'impatto degli attacchi stessi (72%), che nelle altre organizzazioni si fermano rispettivamente al 46% e al 41%.

Analizzando l'approccio dei "Cybersecurity Leader", il report propone un piano d'azione in sei fasi per sviluppare una solida strategia di cybersecurity per le smart factory:

- Effettuare un assessment iniziale del livello di cybersecurity;
- Rendere l'intera organizzazione consapevole delle minacce informatiche legate alle smart factory;
- Identificare la risk ownership per gli attacchi informatici nelle smart factory;
- Stabilire un quadro di riferimento per la cybersecurity delle smart factory;
- Creare procedure di cybersecurity su misura per le smart factory;
- Definire una struttura di governance e una comunicazione efficace con l'IT aziendale.

Per consultare una copia completa del report, cliccare qui.

Metodologia di ricerca

Il Capgemini Research Institute ha condotto un'indagine su 950 organizzazioni ed effettuato interviste approfondite con responsabili di numerose aziende. La survey globale si è svolta tra ottobre e novembre 2021 e i settori presi in esame comprendono industria pesante, Pharma & Life Sciences, Chemicals, Hi-Tech, Consumer Products, Automotive, Aerospace & Defense.

Capgemini
Capgemini è leader mondiale nel supportare le aziende nel loro percorso di trasformazione digitale e di business facendo leva sul potere della tecnologia. Lo scopo del Gruppo è garantire un futuro inclusivo e sostenibile, sprigionando l'energia umana attraverso la tecnologia. Capgemini è un'organizzazione responsabile e diversificata di oltre 340.000 persone presente in più di 50 paesi nel mondo. 55 anni di esperienza e una profonda conoscenza dei settori di mercato rendono Capgemini un partner affidabile per i suoi clienti, in grado di fornire soluzioni innovative per le loro esigenze di business, dalla strategia alla progettazione alle operation, grazie alle competenze in ambito cloud, dati, AI, connettività, software, digital engineering e piattaforme. Nel 2021 il Gruppo ha registrato ricavi complessivi pari a 18 miliardi di euro.

Get The Future You Want | www.capgemini.com/it-it/

Capgemini Research Institute
Il Capgemini Research Institute è il think-tank interno di Capgemini dedicato a tutto ciò che è digitale. L'istituto pubblica lavori di ricerca in merito all'impatto delle tecnologie digitali sulle grandi aziende tradizionali. Il team fa leva sul network mondiale di esperti Capgemini e lavora a stretto contatto con partner accademici e tecnologici. L'istituto possiede centri di ricerca dedicati in India, Singapore, nel Regno Unito e negli Stati Uniti. Recentemente, è stato nominato il miglior istituto di ricerca al mondo per la qualità dei suoi lavori da una giuria di analisti indipendenti.

Per saperne di più consultare il sito https://www.capgemini.com/researchinstitute/