

## Dossier Sicurezza informatica

# Frigo manomessi e fermi in fabbrica, la minaccia cyber si tocca con mano

**Cybersecurity.** Il manifatturiero concentra il 18,4% degli incidenti informatici censiti nel nostro Paese, contro il 5,4% mondiale. In fabbrica il 98% degli episodi ha effetti critici: cresce la pressione sulle aziende tra carenza di specialisti e adempimenti complessi

**Andrea Biondi**

**F**rigoriferi manomessi a distanza, alimenti da buttare, reparti fuori uso. La Francia messa in questi giorni a ferro e fuoco da casseurs e devastazioni andate ben oltre le proteste studentesche, la mattina del 12 ottobre si è svegliata così. L'attacco che nella notte tra l'11 e il 12 ottobre ha colpito centinaia di supermercati francesi, da Intermarché a Coopérative U, ha reso tangibile il rischio cyber: basta alterare il funzionamento di un impianto per distruggere merce e ricavi. Da qui il campanello d'allarme per il rischio di una pericolosa escalation. In Italia l'Agenzia per la cybersicurezza nazionale ha richiamato l'attenzione della distribuzione e della filiera del freddo su installazioni obsolete, accessi esposti su Internet e autenticazione carente.

Supermercati come le fabbriche: la sicurezza informatica protegge ormai la capacità di operare e di produrre. Del resto, per mettere sotto pressione una fabbrica basta fermarla. È questa la leva economica che rende il manifatturiero un bersaglio della criminalità informatica: ogni ora senza produzione può significare consegne

saltate, ordini a rischio e contraccolpi sui fornitori. E purtroppo il fenomeno appare in accelerazione.

A darne prova algebrica sono i numeri dell'ultimo approfondimento Clusit sul manufacturing, dello scorso 9 settembre. Secondo il report in Italia, nei primi sei mesi del 2026, gli incidenti noti sono stati 45, contro 63 nell'intero 2025. E il 98% degli episodi osservati ha avuto conseguenze classificate come alte o critiche.

La cybersecurity entra così sempre di più nel conto della competitività industriale. E il confronto internazionale, guardando in casa nostra, mette

a fuoco quanto pesi l'industria nel quadro italiano delle problematiche legate alla cybersicurezza. Il manifatturiero concentra il 18,4% dei 245 incidenti censiti nel Paese nel semestre, mentre a livello mondiale la quota si ferma al 5,4%. Un'incidenza oltre tre volte superiore, che non autorizza a concludere che le nostre fabbriche siano tre volte più vulnerabili: contano la struttura produttiva, la composizione del campione e la visibilità degli attacchi. Ma il segnale resta forte. Nel 2025 il settore valeva il 12,4% degli episodi italiani. Se il ritmo del semestre proseguisse, nel 2026 si arriverebbe a circa 90 casi. È una proiezio-

ne, non un consuntivo, e ridimensiona l'idea di un allentamento della pressione dopo la crescita dell'8,6% registrata nel 2025.

Anche fuori dall'Italia la curva sale. Clusit conta 267 incidenti nel manifatturiero mondiale nel primo semestre, dopo i 400 del 2025, che aveva segnato un aumento del 69,5%. La motivazione dominante è il denaro. Nel semestre 260 dei 267 episodi globali sono ricondotti al cybercrime; in Italia sono 44 su 45. Spionaggio, sabotaggio e attivismo hanno un ruolo residuale nel campione.

La fabbrica interessa perché l'interruzione del lavoro aumenta la pressione sulla parte lesa e il ritorno per chi attacca. Il danno può inoltre viaggiare lungo la filiera: un'impresa dipende dalla continuità dei fornitori e la sua esposizione supera il perimetro dei sistemi che controlla direttamente. Per un'industria interconnessa, la sicurezza diventa anche una questione di affidabilità nei rapporti commerciali.

In Italia il malware, il software malevolo, è associato all'89% degli incidenti manifatturieri del semestre, contro il 76% del 2025. La quota mondiale resta invece al 42%. Sarebbe però fuorviante leggere questi nu-

meri come una mappa delle porte d'ingresso: il programma che blocca o compromette i sistemi può essere la fase visibile di un'intrusione partita da credenziali rubate, inganni al personale o vulnerabilità. Inoltre, i casi italiani con tecnica non divulgata scendono dal 21% al 7%: una maggiore disponibilità di informazioni può contribuire a spiegare l'aumento del malware classificato. A livello globale la tecnica rimane sconosciuta nel 48% degli episodi.

Il conto degli impatti lascia poco spazio all'ottimismo. In Italia gli incidenti critici scendono dal 13% al 7%, ma quelli di gravità alta salgono dall'81% al 91%. Quasi tutti i casi osservati continuano a produrre conseguenze significative. La risposta indicata da Clusit affianca alla prevenzione la capacità di contenere il danno: separare gli ambienti informatici, organizzare la continuità operativa, predisporre il ripristino e coordinare la crisi. Per l'impresa la prova decisiva è quanto

riesca a lavorare durante l'emergenza e quanto rapidamente possa ripartire.

Sul versante delle risorse, un quadro precedente ai nuovi dati arriva dall'Osservatorio cybersicurezza di I-Com, pubblicato a dicembre 2025 e aggiornato al 26 novembre. L'indagine riguarda 86 imprese di diversi settori, dalle utilities ai trasporti al digitale, e non va letta come una fotografia del solo manifatturiero. Il 51% dei rispondenti aveva deciso di aumentare le risorse per la sicurezza, anche per gli sviluppi della regolamentazio-

**Nel primo semestre Clusit censisce 45 incidenti nel manifatturiero italiano, erano 63 in tutto il 2025**



ne; il 37% stava ancora valutando e il 12% aveva escluso incrementi. La fascia di investimento più indicata era il 3-5% del budget informatico.

Spendere, però, richiede anche persone e scelte organizzative. Tra le difficoltà nell'adeguarsi alle norme, 38 risposte segnalavano la moltiplicazione delle prescrizioni, 32 la carenza di competenze interne o sul mercato e 31 l'incertezza interpretativa. L'80% puntava sulla consapevolezza e sulla formazione del personale, differenziata per ruolo. È qui che i due rapporti si incontrano: gli adempimenti assorbono risorse, ma la misura della sicurezza resta la tenuta dell'azienda quando viene colpita.

© RIPRODUZIONE RISERVATA



**Sotto attacco.** Dalle fabbriche ai frigoriferi dei supermercati (sopra quelli colpiti nel recente attacco in Francia), gli attacchi minacciano la continuità operativa con conseguenze economiche sempre più rilevanti

# 98%

## Le conseguenze più gravi

È la percentuale degli incidenti informatici nel manifatturiero italiano classificati da Clusit con gravità alta o critica nei primi sei mesi del 2026. In particolare, il 91% presenta conseguenze alte e il 7% critiche.

# 89%

## Il malware in fabbrica

È la percentuale degli incidenti manifatturieri italiani associata all'utilizzo di software malevoli nel primo semestre 2026, in crescita rispetto al 76% del 2025. A livello mondiale la quota è del 42%. Il malware può rappresentare la fase finale di intrusioni avviate attraverso credenziali sottratte, vulnerabilità o inganni al personale.

## I numeri

# 45

### Le fabbriche colpite

Sono gli incidenti informatici che hanno interessato il manifatturiero italiano nei primi sei mesi del 2026, secondo Clusit. Nell'intero 2025 erano stati 63. Se il ritmo del primo semestre dovesse proseguire, l'anno potrebbe chiudersi con circa 90 casi. Una proiezione che evidenzia l'accelerazione delle minacce contro un settore particolarmente esposto ai costi delle interruzioni produttive.

# 18,4%

### Il peso dell'industria

È la quota degli incidenti informatici italiani che ha interessato il manifatturiero nel primo semestre 2026, contro il 12,4% registrato nell'intero 2025. A livello mondiale l'incidenza del settore si ferma al 5,4 per cento. Una differenza che riflette anche la struttura industriale del Paese e la composizione degli incidenti osservati, senza dimostrare una effettiva maggiore vulnerabilità delle imprese italiane.

# 51%

### Gli investimenti

È la quota delle 86 imprese interpellate dall'Osservatorio I-Com che ha deciso di aumentare le risorse destinate alla cybersecurity. Un altro 37% sta valutando nuovi stanziamenti, mentre il 12% non prevede incrementi.

# 80%

### La formazione

È la percentuale delle imprese intervistate da I-Com che indica nella consapevolezza e nella formazione dei dipendenti uno strumento per migliorare la cybersecurity. I percorsi devono essere differenziati in funzione delle mansioni e delle competenze. La protezione non dipende soltanto dalle tecnologie: comportamenti individuali, gestione delle credenziali e capacità di riconoscere le minacce sono parte della difesa.