Acronis

WHITE PAPER

Perché i produttori europei hanno bisogno di un piano di resilienza aziendale

Riduci i tempi di inattività, rafforza la preparazione alla direttiva NIS 2 e migliora i requisiti per l'assicurazione contro i rischi informatici

Sintesi riepilogativa

I produttori europei si trovano ad affrontare una convergenza di difficoltà:

L'interruzione operativa non pianificata è una delle minacce più significative per le prestazioni del settore manifatturiero in tutto il continente.

La Direttiva NIS 2, in continua evoluzione, ha portato la continuità operativa e il disaster recovery a un livello di responsabilità dirigenziale.

Allo stesso tempo, le compagnie di assicurazione contro i rischi informatici richiedono prove più concrete della resilienza prima di concedere le polizze.

Il problema è che queste pressioni non sono più separate. Un singolo incidente o emergenza di cyber security ha ormai un impatto diretto sulle operazioni, sulla conformità e sul recupero finanziario. In risposta, i produttori devono andare oltre strategie di backup frammentate per i loro ambienti di tecnologia operativa (OT) e adottare un vero piano di resilienza aziendale incentrato sul ripristino della produzione.

La sfida della leadership: un incidente, tre impatti

Molte organizzazioni gestiscono ancora separatamente backup, conformità e assicurazione. In teoria, durante un incidente convergono. Ma cosa succede quando non lo fanno?

Se un produttore non è in grado di ripristinare la produzione in modo controllato e documentato, deve affrontare tre conseguenze immediate:

- L'interruzione della produzione e il mancato rispetto degli impegni di consegna.
- Un'esposizione normativa ai sensi della NIS 2.
- Un maggiore rischio di contestazioni o riduzioni dei risarcimenti assicurativi.

Un approccio debole al ripristino crea quindi un rischio aziendale composito, non solo un problema tecnico.

Panorama europeo delle minacce e approfondimenti regionali

Gli incidenti informatici stanno già causando interruzioni operative nelle attività manifatturiere in tutta Europa e il ransomware resta la minaccia principale per gli ambienti industriali. I produttori europei devono affrontare rischi convergenti. I gruppi specializzati in ransomware stanno prendendo di mira il settore manifatturiero, aumentando il numero di incidenti gravi ed estendendo l'esposizione alle vulnerabilità. Allo stesso tempo, molte piccole e medie imprese (PMI), inclusi i produttori, non dispongono di strategie di cyber security mature e sono pertanto vulnerabili agli attacchi. Le iniziative guidate da Industry 4.0 hanno inoltre ampliato la superficie di attacco negli ambienti OT e molti produttori non hanno adottato misure adeguate per proteggere i propri dati.

Il ripristino dopo un attacco informatico è costoso. Secondo IBM, a livello globale, nel 2025 il costo medio di una violazione dei dati in un ambiente industriale è stato di 5 milioni di dollari.[1] Con l'aumento del numero e della gravità del ransomware e di altri attacchi in tutta Europa, i produttori, come altre PMI, devono sviluppare una strategia efficace per la protezione e il ripristino. I numeri suggeriscono che la situazione sta peggiorando, non migliorando.

Ad esempio:

Europa: secondo il report ENISA Threat Landscape 2025, quasi il 15% degli attacchi ransomware analizzati nel report era diretto al settore manifatturiero, che è risultato il quinto settore più preso di mira tra i quasi 20 settori studiati nel report.[2]

Regno Unito: il National Cyber Security Centre (NCSC) del Regno Unito segnala che il settore manifatturiero è tra quelli più frequentemente presi di mira dal ransomware.[3]

Germania: Any.run ha riferito nel 2026 che, poiché i produttori tedeschi avevano integrato tecnologie Industry 4.0, sensori IoT, OT operative e sistemi di produzione integrati nel cloud, gli attacchi andavano oltre la perdita di dati fino a causare il potenziale arresto delle operazioni, danni fisici alle apparecchiature
e interruzione operativa della supply chain. Poiché il personale in stabilimento era raramente esperto di cyber security, gli attacchi di social engineering risultavano particolarmente efficaci.[4]

Francia: l'agenzia francese per la cyber security (ANSSI) ha affermato in un report del 2026 che i produttori francesi erano diventati obiettivi principali sia di interruzioni operative sponsorizzate da stati sia di attacchi ransomware. Il report specificava che i produttori più piccoli erano particolarmente vulnerabili al sabotaggio digitale.[5]

Italia: un report sulla cyber security di Telecom Italia ha rilevato nel 2025 che le aziende manifatturiere italiane sono state l'obiettivo di circa il 26% degli attacchi ransomware nel paese dal 2022 al 2024.[6]

Paesi nordici: Mordor Intelligence riporta che i programmi Industry 4.0 che ampliano le superfici di attacco OT stanno trainando gli investimenti in soluzioni di cyber security nei paesi nordici, con un notevole tasso composto di crescita annua complessivo di oltre l'8%. I produttori stanno rispondendo ai rischi facendo convergere le difese IT e OT.[7]

Sebbene le statistiche specifiche per l'OT restino limitate, i dati nazionali disponibili evidenziano una più ampia escalation del rischio informatico negli ambienti manifatturieri, compresi i sistemi industriali e le PMI.

[1] IBM, Cost of a Data Breach Report 2025: The AI Oversight Gap, ricerca condotta dal Ponemon Institute, pubblicata nel 2025, basata sull'analisi di 600 organizzazioni in 16 Paesi tra marzo 2024 e febbraio 2025.

[2] ENISA Threat Landscape 2025, versione 1.2, Agenzia dell'Unione europea per la cibersicurezza, gennaio 2026.

[3] National Cyber Security Centre. (2024). NCSC annual review 2024. GCHQ.

[4] ANY.RUN. (1° aprile 2026). Major cyberattacks in March 2026: OAuth phishing, SVG smuggling, Magecart, and more.

[5] Agence nationale de la sécurité des systèmes d'information. (11 marzo 2026). Panorama de la cybermenace 2025 (CERTFR-2026-CTI-002). ANSSI.

[6] Telecom Italia (TIM) e Cyber Security Foundation. (12 giugno 2025). Cyber security report 2025. Gruppo TIM.

[7] Mordor Intelligence, Nordics cybersecurity market size and share analysis: growth trends and forecasts (2026–2031), con una stima delle dimensioni del mercato pari a 14,92 miliardi di dollari nel 2026 e in crescita fino a 22,25 miliardi di dollari entro il 2031 (CAGR dell'8,36%), pubblicato nel 2026.

Attacchi informatici reali contro il settore manifatturiero in Europa

In tutta Europa, gli incidenti informatici negli ambienti OT non sono più eventi IT isolati. Sono eventi di produzione che possono interrompere gravemente le attività e causare un'interruzione operativa prolungata. Alcuni esempi recenti:

- **Jaguar Land Rover:** un attacco informatico del 2025 a Jaguar Land Rover, ormai tristemente noto, ha interrotto la produzione nel Regno Unito per diverse settimane con un costo di almeno 50 milioni di sterline a settimana,[8] secondo le stime, causando anche perdite di posti di lavoro. L'attacco ha dimostrato in che modo un'interruzione operativa dell'IT aziendale possa avere un impatto diretto sulle attività di produzione.
- **Volkswagen Group France:** nell'ottobre 2025, Volkswagen Group France ha subito un attacco da parte del gruppo specializzato in ransomware Qilin che ha portato all'esfiltrazione di circa 2.000 file e 150 GB di dati sensibili.[9]
- **Dodd Group:** nel 2025, l'appaltatore della difesa britannico Dodd Group ha subito un attacco informatico che ha provocato la divulgazione di file sensibili del Ministero della Difesa del Regno Unito contenenti informazioni su basi dell'aeronautica e della marina.[10]

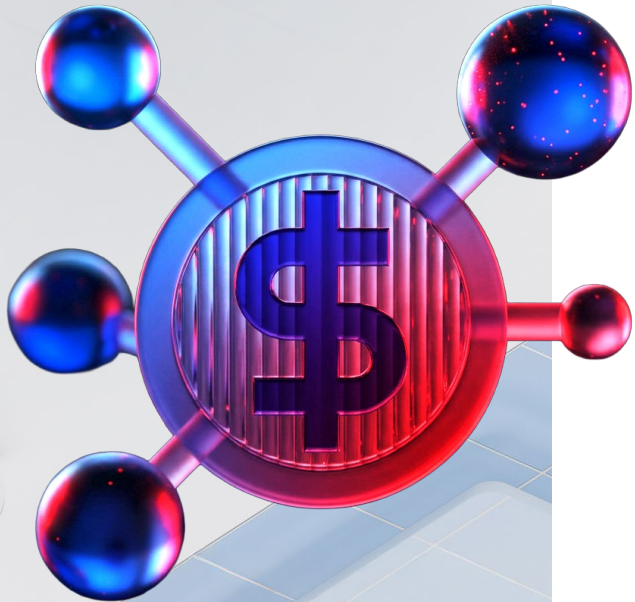
Cosa richiede la NIS 2 in pratica

La conformità resta un problema importante negli ambienti OT, dove le potenziali sanzioni finanziarie possono sommarsi al costo dell'interruzione operativa non pianificata.
La NIS 2 introduce un cambiamento fondamentale: dalla prevenzione a una resilienza dimostrabile.

Ai sensi dell'articolo 21, le organizzazioni devono essere in grado di dimostrare di poter continuare le attività operative e recuperare efficacemente. Questo significa:

- Continuità operativa e piano di disaster recovery
- Gestione dei backup allineata alle esigenze operative.
- Gestione delle crisi e strutture di governance.

Il cambiamento critico è la responsabilità: le organizzazioni devono dimostrare che il ripristino funziona nella pratica, non solo sulla carta. Dunque, la capacità di ripristino è ora un requisito di conformità, non una semplice preferenza operativa.



[8] BBC News, Jaguar Land Rover cyber-attack disrupts production and supply chain, pubblicato a settembre 2025.
[9] Cybernews. (16 ottobre 2025). Volkswagen France hit by ransomware, Qilin gang claims.
[10] Security Affairs. (20 ottobre 2025). Russian Lynk group leaks sensitive U.K. MoD files, including info on eight military bases.

Perché il ripristino OT è diverso

Gli ambienti OT introducono complessità che le tradizionali strategie di ripristino IT non affrontano pienamente, tra cui sistemi legacy, processi produttivi strettamente interconnessi e rigide condizioni di riavvio che rendono critico il sequenziamento del ripristino.

Di conseguenza, la resilienza nel settore manifatturiero dipende dal ripristino della capacità produttiva e non solo dei sistemi o dei dati.

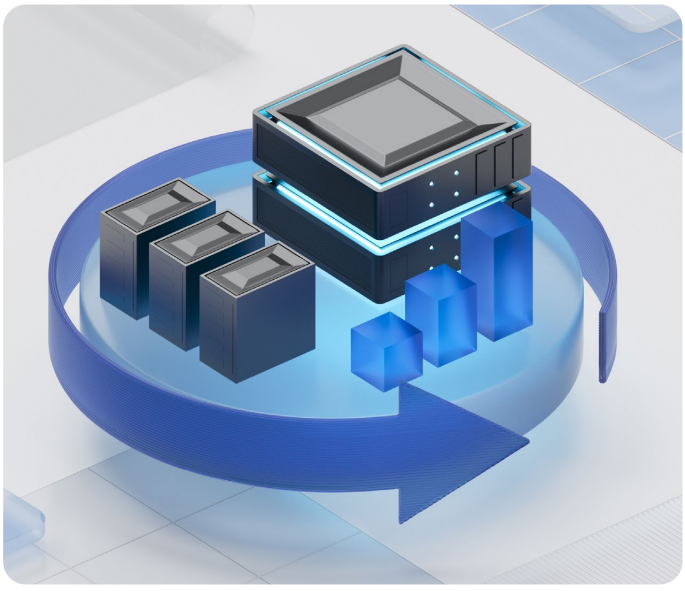
Dal backup alla resilienza aziendale

Un piano di resilienza aziendale implica molto più del solo backup: collega continuità operativa, conformità e ripristino in un unico framework.

Come minimo, le organizzazioni devono definire:

- Una governance chiara tra siti e funzioni.
- Capacità di ripristino consapevoli dell'OT.
- Convalida regolare dei processi di ripristino.

L'obiettivo non è semplicemente il recupero dei dati, ma garantire che i produttori possano ripristinare rapidamente la produzione in modo controllato e prevedibile.



Assicurazione informatica e difendibilità

I fornitori di assicurazioni informatiche stanno aumentando il livello di controllo sulle organizzazioni manifatturiere, in particolare per quanto riguarda il rischio di interruzione dell'attività aziendale. L'esito delle richieste di risarcimento è sempre più influenzato dalla capacità di un'organizzazione di dimostrare preparazione ed esecuzione del ripristino.

Le aspettative principali ora includono:

- Prove dell'esistenza di processi definiti di continuità operativa e ripristino.
- Tempistiche e azioni di ripristino documentate.
- Allineamento tra gli impegni della policy e la capacità operativa.

Senza questi elementi, le organizzazioni rischiano di entrare in una zona grigia dei sinistri in cui la copertura può essere ridotta o contestata.

Cosa dovrebbero fare ora i leader del settore manifatturiero

I produttori devono affrontare la resilienza come una priorità aziendale piuttosto che come un progetto tecnico.

I leader dovrebbero concentrarsi su tre azioni immediate:

- Comprendere le dipendenze critiche della produzione e i rischi di ripristino.
- Allineare la pianificazione della continuità operativa alle aspettative della direttiva NIS 2.
- Definire un piano strutturato di resilienza aziendale.

Questo cambiamento consente alle organizzazioni di ridurre il rischio di interruzione operativa rafforzando al contempo sia la conformità sia la protezione finanziaria.

In che modo Acronis supporta la resilienza OT

Con Acronis Cyber Protect per OT, i sistemi possono essere ripristinati con una singola azione, senza richiedere competenze IT approfondite. Soprattutto negli ambienti air-gap, One-Click Recovery è una funzionalità essenziale. I produttori possono ridurre al minimo l'interruzione operativa e massimizzare la velocità di ripristino senza interventi né interruzioni operative.

Acronis Cyber Protect per OT consente ai produttori di rafforzare la resilienza in ambienti complessi. Supporta le organizzazioni nell'affrontare la convergenza delle seguenti sfide:

- Proteggere i sistemi critici da interruzioni operative indesiderate.
- Convalidare i processi di ripristino e altri elementi essenziali per la conformità.
- Generare le prove richieste per l'assicurazione contro i rischi informatici.

Come componente della piattaforma Acronis Cyber Platform, integrata nativamente, che riunisce più funzioni di cyber security in un'unica console e in un unico punto di gestione, Acronis Cyber Protect per OT consente ai produttori di migliorare l'operatività e ridurre le interruzioni operative indesiderate, oltre a beneficiare di tempi di ripristino più rapidi e di un allineamento più solido tra la resilienza operativa e la gestione del rischio aziendale.

PER SAPERNE DI PIÙ

Acronis

Per saperne di più, visita acronis.com