

Martedì 10 Novembre 2026
Notizie mercati esteri [1]

Oltre l'Illusione della Protezione Perfetta. Perché le aziende italiane devono passare dalla difesa cieca alla resilienza operativa

Il Paradosso della Cybersecurity Italiana

Per anni molte aziende italiane hanno affrontato la sicurezza informatica come un problema meramente tecnologico, delegando interamente la gestione ai reparti IT o a fornitori esterni. Tuttavia, come sottolineato da **Charles Hosner** (Global Cyber Resilience Lead di Accenture) in una recente intervista al quotidiano svedese *Dagens Industri*, la sicurezza informatica moderna non è una questione di server o software: è una questione di **leadership, gestione delle priorità e sopravvivenza aziendale**.

Nel tessuto economico italiano, caratterizzato da filiere manifatturiere e PMI ad alta specializzazione, l'illusione della "protezione perfetta al 100%" rischia di diventare un pozzo senza fondo per i bilanci. Si spendono cifre importanti in soluzioni tecnologiche sofisticate, per poi scoprire che l'azienda rimane vulnerabile a causa di errori umani, mancanza di governance e incapacità di ripartire dopo un blocco.

La provocazione di Hosner:

«Non servono i laser per risolvere il problema di aver lasciato la porta aperta. Basta chiudere la porta a chiave. Smettetela di aggiungere mura al castello quando sta arrivando un'onda anomala: investite nel ridurre i danni.»

Perché la Manifattura Italiana è il Bersaglio Perfetto

Il panorama del cybercrime è radicalmente cambiato. In passato i bersagli principali erano le grandi istituzioni bancarie e le infrastrutture militari. Oggi, con la diffusione capillare del ransomware, i criminali informatici hanno virato verso settori con una minore maturità di difesa ma con un'elevatissima urgenza di continuità operativa: **il manifatturiero e il retail**.

Settore	Vulnerabilità Tipica	Impatto del Cyberattacco
Manifattura / Industriale	Sistemi OT obsoleti e interconnessi	Blocco della catena di montaggio e

	alla rete IT	penali sulla consegna
Retail & Distribuzione	Gestione frammentata della Supply Chain	Impossibilità di fatturazione e blocco della logistica
Servizi & Consulenza	Elevata dipendenza da credenziali e fattore umano	Fuga di dati clienti e danni reputazionali

Per una PMI manifatturiera del Made in Italy, fermare la linea di produzione per tre settimane significa perdere contratti chiave e reputazione internazionale. Per i cybercriminali, estorcere un riscatto a un'azienda bloccata è diventato incredibilmente semplice e redditizio.

Il Cambio di Paradigma: Dal 95/5 al 50/50

Attualmente, la maggior parte delle aziende assegna circa il **95% del budget** informatico alla prevenzione (firewall, antivirus, sistemi di monitoraggio avanzati) e solo il **5% alla resilienza** (piani di continuità, ripristino rapido, simulazioni di crisi). Inoltre, spesso si acquistano software complessi estraendone solo il **10% del valore effettivo**.

La proposta di Hosner è un riequilibrio drastico: **investire il 50% delle risorse nella capacità di ripristino rapido (Recovery)**.

Poiché è impossibile evitare ogni singolo incidente (specialmente con l'avvento dell'Intelligenza Artificiale che rende i sistemi imprevedibili), il vero fattore differenziante diventa la velocità con cui un'azienda riporta il proprio *core business* all'80% della produttività dopo un attacco.

Le 5 Domande che ogni CEO o Board Italiano deve porsi

- **Abbiamo mappato la nostra catena del valore?**
  - *Sappiamo esattamente quali 10 server o processi devono ripartire per primi per salvare il conto economico in caso di blocco totale?*
- **Il nostro team IT parla la lingua del business?**
  - *La sicurezza applica controlli mirati sui 6 asset fondamentali o blocca l'operatività ovunque a pioggia, paralizzando l'azienda?*
- **Qual è il nostro RTO reale (Recovery Time Objective)?**
  - *Se venissimo colpiti oggi da un ransomware, quanti giorni impiegheremmo a tornare sul mercato? 90 giorni? Come possiamo scendere a 30?*
- **Affidiamo la sopravvivenza all'eroismo dei singoli?**
  - *Dipendiamo da dipendenti che lavorano 100 ore a settimana in emergenza o abbiamo una strategia di ripristino chiara e testata?*
- **Siamo pronti per l'impatto dell'IA?**
  - *Con sistemi sempre più complessi e caotici, abbiamo strutturato una gestione efficace delle conseguenze anziché affidarci solo alla prevenzione?*

Conclusioni per la Leadership

La Direttiva Europea **NIS2** attribuisce ormai ai vertici aziendali la responsabilità diretta e personale in materia di sicurezza informatica. Non è più consentito considerare la cybersecurity come "roba da tecnici". L'igiene digitale di base, la conoscenza profonda dei propri processi critici e la preparazione al ripristino d'emergenza sono gli unici veri scudi per proteggere il valore e il futuro delle aziende italiane.

(Contributo editoriale a cura della Camera di Commercio Italiana per la Svezia **[2]**)
Ultima modifica: Martedì 10 Novembre 2026

Condividi

Reti Sociali

ARGOMENTI

Sicurezza Informatica [3]

Source URL: https://www.assocamerestero.com/notizie/oltre-lillusione-della-protezione-perfetta-perche-aziende-italiane-devono-passare-dalla

Collegamenti
[1] https://www.assocamerestero.com/notizie/%3Ffield_notizia_categoria_tid%3D1122
[2] https://www.assocamerestero.it/ccie/camera-commercio-italiana-svezia
[3] https://www.assocamerestero.com/ricerca-per-argomenti/%3Ftid%3D1132