Hermes
Centro Studi Europeo

STRATEGIA ITALIA
PENSARE IL FUTURO, COSTRUIRE LA CRESCITA.

CYBERSECURITY / IMPRESE E MONDI PRODUTTIVI / SICUREZZA

DOSSIER

Un attacco informatico può fermare la spesa?

Dai sistemi digitali agli scaffali: la vulnerabilità della catena del freddo

Come un comando a distanza può incidere
su merci, attività economiche e fiducia dei cittadini.

04 NOVEMBRE 2026

Fatti documentati, meccanismi e scenari

IL FILO DEL RACCONTO

Il freddo che non vediamo

Entriamo in un supermercato e prendiamo una confezione dal banco dei surgelati. È un gesto ordinario, reso possibile da una successione di operazioni che quasi mai osserviamo: produzione, conservazione, trasporto e vendita. In ciascun passaggio, qualcuno deve mantenere condizioni adeguate e sapere se qualcosa è cambiato.

Accanto a compressori, porte e celle frigorifere lavorano sensori, dispositivi di controllo e software. Consentono di leggere una temperatura, inviare un allarme o intervenire su un impianto senza essere sul posto. Il servizio che appare materiale dipende così anche da una rete di informazioni e autorizzazioni.

Questa connessione aiuta a capire la domanda del dossier. Un attacco informatico può ostacolare la disponibilità di alcuni prodotti e il funzionamento di un’attività, se raggiunge i sistemi che ne governano la conservazione. Non significa che un singolo incidente possa fermare automaticamente la spesa di un intero Paese.

Gli eventi dell’autunno 2026 riportano l’attenzione su questa dipendenza. Per comprenderli occorre seguire il percorso dal comando digitale all’effetto fisico e poi dal danno locale alle conseguenze economiche. Occorre anche distinguere ciò che è documentato da ciò che rimane da accertare.

> Il confine tra digitale e fisico passa anche dentro un banco frigorifero.

Il dossier ricostruisce il quadro disponibile al 3 novembre 2026. I riferimenti verificabili comprendono esclusivamente fonti istituzionali, norme e dati. Le connessioni interpretative e gli scenari sono elaborazioni di Hermes Centro Studi Europeo; non attribuiscono responsabilità non accertate.

01 / I FATTI E I LORO LIMITI

Dall’allarme francese all’attenzione italiana

Il 13 ottobre 2026 un bollettino nazionale richiama gli operatori della distribuzione alimentare e della filiera del freddo dopo un incidente che ha coinvolto catene di supermercati francesi. Il meccanismo descritto riguarda installazioni obsolete, accessi di amministrazione esposti e autenticazione debole, con alterazioni dei parametri degli impianti.

Il 3 novembre lo stesso avviso viene riproposto in primo piano a seguito di recenti eventi rilevati sul territorio nazionale. La cronologia è importante: non si tratta di un documento nato quel giorno, ma di un richiamo rinnovato alla luce dell’evoluzione del quadro.

- **13 ottobre / Primo bollettino**

  Richiamo alla filiera dopo l’incidente francese.

- **3 novembre / Nuova evidenza nazionale**

  L’avviso torna in primo piano dopo eventi in Italia.

Il bollettino non fornisce un censimento completo dei punti vendita italiani coinvolti, un ammontare nazionale dei danni o l’identità degli autori. Non consente quindi di trasferire all’Italia cifre riferite ad altri Paesi o di affermare che ogni episodio abbia la stessa origine.

> Un allarme documenta un rischio e una necessità di attenzione. Non sostituisce l’accertamento delle responsabilità.

Questa distinzione non ridimensiona il problema: permette di raccontarlo con precisione. La vulnerabilità di una funzione essenziale è già un fatto rilevante, anche prima di conoscere il bilancio finale di un incidente.

02 / IL PONTE TRA DUE MONDI

Quando il software muove una macchina

Un programma gestionale tratta informazioni. Un sistema di controllo industriale può invece produrre un cambiamento fisico: azionare un componente o regolare un processo. L’espressione Operational Technology, spesso abbreviata in OT, indica questo insieme di dispositivi e sistemi che osservano o governano l’ambiente materiale.

In una catena del freddo, il sensore misura una grandezza; il controllore utilizza le informazioni secondo una configurazione; gli apparati eseguono le operazioni previste. Una piattaforma di supervisione può riunire letture e funzioni di comando di più impianti. Non tutti gli esercizi possiedono la stessa architettura.

MISURARE	Sensori e letture del processo
REGOLARE	Controllori e parametri autorizzati
AGIRE	Apparati e condizioni fisiche

Lo schema descrive funzioni generali e non riproduce l’architettura di un impianto colpito.

Questi ambienti hanno esigenze particolari di continuità, affidabilità e sicurezza delle persone. Un riavvio o un aggiornamento che su un normale computer è tollerabile può avere conseguenze diverse su un processo in corso. La protezione informatica deve quindi dialogare con la conoscenza tecnica dell’impianto.

Il problema cambia natura: non riguarda soltanto la riservatezza di un documento, ma anche la correttezza di un’azione. Una temperatura leggibile sullo schermo è utile soltanto se il dato è affidabile e se corrisponde alle condizioni effettive.

03 / LE CONNESSIONI INVISIBILI

La comodità dell’accesso è anche una responsabilità

La manutenzione a distanza è un servizio utile: riduce gli spostamenti e consente interventi rapidi. Introduce però un collegamento attraverso il quale persone o software possono raggiungere funzioni operative. La sua sicurezza dipende da chi può entrare, da ciò che gli è consentito fare e dalla possibilità di ricostruire le attività.

Un accesso pensato per un manutentore non dovrebbe diventare un permesso generale su ogni impianto. Limitare risorse e operazioni autorizzate, separare gli ambienti e gestire gli account sono principi che riducono la possibilità che una singola compromissione si estenda. Non sono garanzie assolute di invulnerabilità.

La centralizzazione rende più semplice governare più sedi. Allo stesso tempo può concentrare la capacità di intervento: una funzione comune compromessa può produrre effetti più ampi di quelli di un singolo dispositivo isolato. È una possibilità architetturale, non la prova che tutti gli incidenti osservati siano partiti da una piattaforma unica.

Il tempo aggiunge un’altra variabile. Un’apparecchiatura può continuare a svolgere il proprio compito materiale anche quando una parte del suo software non riceve più supporto. Funzionare non equivale quindi a essere ancora adeguatamente mantenuta sul piano digitale.

> Un servizio connesso può funzionare perfettamente e avere comunque bisogno di protezioni che il cliente non vede.

Per comprendere un incidente non basta sapere che un dispositivo era collegato a Internet. Servono configurazioni, registrazioni e riscontri. Una tecnologia di connessione, da sola, non dimostra né la causa di un attacco né l’identità di chi lo ha condotto.

04 / IL TEMPO E LA TEMPERATURA

Raffreddare di nuovo non riporta indietro il tempo

Il freddo rallenta processi biologici e chimici, ma la conservazione dipende anche dalla storia del prodotto. Contano la temperatura raggiunta, la durata dell'esposizione, la natura dell'alimento e le condizioni di confezionamento. La lettura di un solo istante non ricostruisce tutto il percorso.

-18 °C

riferimento per la conservazione dei surgelati

1 anno

conservazione minima delle registrazioni nei casi previsti

Il valore di -18 °C riguarda i surgelati e non è una soglia universale per tutti gli alimenti refrigerati. La registrazione delle temperature è prevista, per i surgelati, nei mezzi di trasporto e nei locali di immagazzinamento e conservazione; il quadro europeo contempla deroghe specifiche per vendita al dettaglio e distribuzione locale.

Le registrazioni sono conservate per almeno un anno, o più a lungo quando lo richiedono natura e durata di conservazione del prodotto. Questa informazione non significa che ogni banco debba disporre dello stesso sistema, né che una registrazione sia automaticamente immune da alterazioni.

I microrganismi presenti in un alimento possono riprendere a crescere in condizioni favorevoli durante lo scongelamento. Riportare il prodotto a una temperatura inferiore non dimostra che la precedente esposizione sia stata irrilevante. Per questo la valutazione delle merci richiede competenze e procedure di sicurezza alimentare.

Sul piano del racconto, il passaggio decisivo è semplice: ripristinare una macchina e valutare un alimento sono due attività collegate ma diverse. La prima riguarda il funzionamento dell'impianto; la seconda ricostruisce se il prodotto abbia mantenuto condizioni compatibili con la sua sicurezza.

I valori riportati descrivono riferimenti normativi e tecnici generali. Non quantificano le condizioni o i danni degli incidenti dell'autunno 2026.

05 / LE CONSEGUENZE ECONOMICHE

Il costo va oltre la merce deteriorata

Quando una parte della merce non può essere venduta, il primo effetto visibile è la perdita del prodotto. Ma l’economia dell’incidente comprende altre voci: verifiche, ripristino tecnico, smaltimento quando necessario, rifornimenti sostitutivi e tempo impiegato dalle persone. La disponibilità di fornitori alternativi può influire sulla durata del disservizio.

Le vendite perse non coincidono con il danno economico netto. Un acquisto può essere rinviato, sostituito con un altro prodotto o trasferito a un altro punto vendita. Per stimare il danno bisogna evitare di sommare grandezze che si sovrappongono e distinguere ricavi, costi e margini.

Un’interruzione locale può anche trasmettere lavoro aggiuntivo lungo la filiera. Un magazzino riorganizza le consegne; un trasportatore modifica una tratta; un produttore riceve richieste urgenti. Sono possibili conseguenze operative, la cui entità dipende dalla scala e dalla durata dell’evento, non effetti identici in ogni caso.

> Merce, attività, ripristino e fiducia: sono dimensioni diverse, da misurare senza duplicazioni.

La fiducia ha tempi propri. Una comunicazione confusa può far apparire generale un problema circoscritto; una comunicazione precisa può chiarire prodotti, sedi e misure effettivamente coinvolti. Non è possibile tradurre questo effetto in una cifra credibile senza dati specifici.

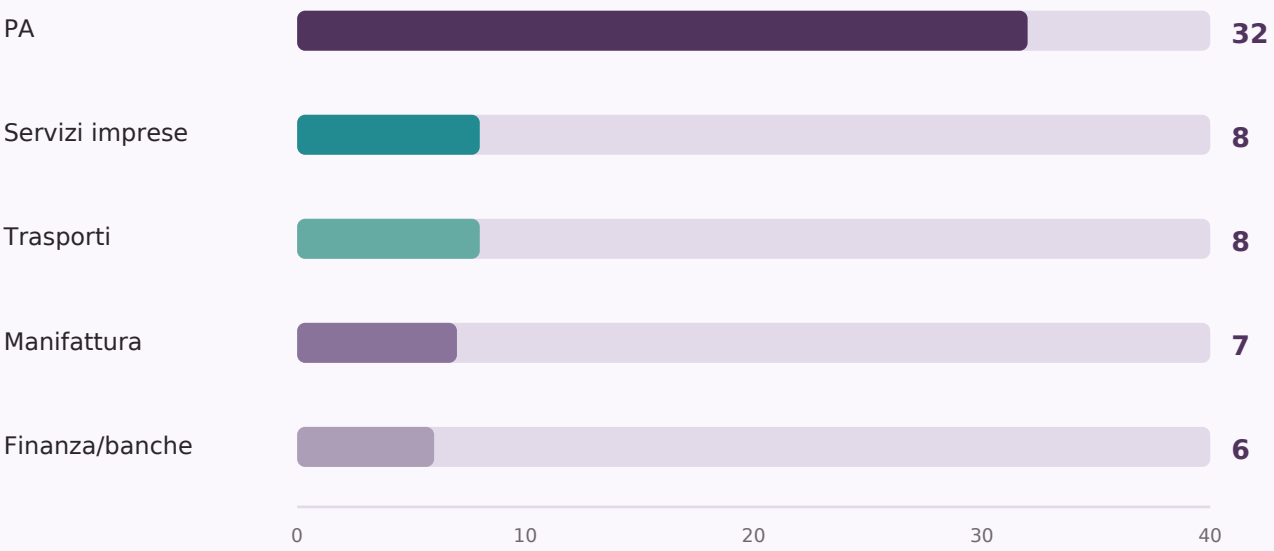
Al 3 novembre il materiale istituzionale qui utilizzato non permette di stimare una perdita complessiva nazionale per questi eventi. Attribuire un numero darebbe un’apparenza di precisione a un’informazione che resta da verificare.

06 / IL CONTESTO EUROPEO

Un rischio che attraversa molti servizi quotidiani

La refrigerazione rende particolarmente evidente il legame tra sicurezza informatica e attività materiali. Il panorama europeo comprende però anche trasporti, manifattura, servizi e amministrazioni. La diffusione delle connessioni estende le dipendenze digitali oltre i sistemi che il pubblico associa abitualmente a un computer.

SETTORI COLPITI NEL QUADRO EUROPEO • DATI 2025 • %



Quote riportate nel quadro ENISA 2026 relativo al 2025. Sono mostrati alcuni settori: le barre non devono sommare al 100%. Non sono probabilità di attacco, quote di danni economici o dati specifici sui supermercati.

Le diverse minacce non vanno confuse. Un attacco che rende irraggiungibile un servizio online, un software che blocca i dati e una modifica non autorizzata a un impianto possono avere meccanismi e conseguenze diversi. Anche le etichette usate nel dibattito pubblico richiedono riscontri.

La geopolitica può influire sull’attività informatica ostile, ma non ne spiega automaticamente ogni episodio. Dalla rilevanza strategica di una filiera non deriva la prova del coinvolgimento di uno Stato. Per attribuire una responsabilità servono elementi investigativi e valutazioni competenti.

Il quadro europeo aiuta quindi a collocare il caso senza trasformarlo in una conclusione generale: i servizi quotidiani hanno dipendenze comuni, ma ciascun incidente conserva una propria storia tecnica e organizzativa.

07 / REGOLE E RESPONSABILITÀ

Due piani di sicurezza che si incontrano

La sicurezza alimentare e quella informatica hanno oggetti diversi, ma possono incontrarsi nello stesso evento. Un sistema può tornare operativo mentre restano da verificare le condizioni delle merci; un alimento può essere sottratto alla vendita anche se il punto vendita prosegue altre attività.

La disciplina europea sull'igiene richiede il mantenimento della catena del freddo e considera le condizioni che possono determinare un rischio per la salute. Le procedure basate sui principi HACCP collegano l'analisi dei pericoli ai controlli del processo alimentare. Non trasformano la causa informatica in una questione esclusivamente tecnica.

Sul versante cyber, la direttiva NIS2 e il decreto legislativo n. 138/2024 inseriscono determinate attività alimentari nel quadro di gestione del rischio e degli incidenti. Il settore comprende distribuzione all'ingrosso e produzione e trasformazione industriali: non significa che ogni negozio sia automaticamente soggetto agli stessi obblighi.

Il perimetro dipende dai criteri applicabili al soggetto e dalle disposizioni nazionali. Il MASAF è l'autorità di settore per la produzione, trasformazione e distribuzione di alimenti nel quadro NIS. Gli obblighi concreti e i relativi termini vanno verificati per l'organizzazione interessata, evitando un calendario unico ricavato da informazioni generiche.

> La causa può essere digitale. La gestione delle conseguenze coinvolge impianti, persone, alimenti e responsabilità aziendali.

Questa convergenza spiega perché l'accertamento richieda competenze diverse. Ricostruire un accesso, verificare un dispositivo e decidere la destinazione di una merce sono passaggi distinti dello stesso evento. Nessuno, da solo, restituisce l'intero quadro.

RIFERIMENTI VERIFICABILI

Fonti, norme e dati / 1

01 / ACN - CSIRT Italia; ripubblicazione CSIRT Toscana
Bollettino BL01/261013/CSIRT-ITA, Misure urgenti di verifica e mitigazione per operatori della distribuzione alimentare e della filiera del freddo. Prima versione 13 ottobre 2026; versione 1.1 del 3 novembre 2026.

Apri la fonte istituzionale
Cronologia p. 3. Ripubblicazione istituzionale del medesimo avviso: non è una seconda indagine indipendente.

02 / NIST
SP 800-82, revisione 3, Guide to Operational Technology (OT) Security, settembre 2023. Versione finale; la revisione 4 è ancora una proposta in consultazione al 3 novembre 2026.

Apri la fonte istituzionale
Funzioni OT, requisiti di sicurezza fisica e continuità, p. 4.

03 / CISA e partner istituzionali
Primary Mitigations to Reduce Cyber Threats to Operational Technology, maggio 2025.

Apri la fonte istituzionale
Accesso remoto, separazione degli ambienti e privilegi, p. 5. Principi generali, non ricostruzione forense dei casi citati.

04 / Ministero della Salute
FAQ: Conservare gli alimenti col freddo.

Apri la fonte istituzionale
Riferimento di -18 °C per i surgelati, p. 6; non soglia unica per tutti gli alimenti.

05 / EFSA
Defrosting food safely, 21 aprile 2021.

Apri la fonte istituzionale
Rapporto tra scongelamento e crescita microbica, p. 6. Il dossier non sostituisce la valutazione degli alimenti coinvolti in un incidente.

Grafico e schema: elaborazioni di Hermes Centro Studi Europeo. Non sono utilizzate stime non documentate del numero di vittime o dei danni complessivi in Italia.

RIFERIMENTI VERIFICABILI

Fonti, norme e dati / 2

06 / Unione europea
Regolamento (CE) n. 37/2005, articoli 2 e 3. Registrazione delle temperature dei surgelati e deroghe.

Apri la fonte istituzionale
Dato p. 6: registrazioni conservate almeno un anno o più a lungo nei casi previsti; deroghe per dettaglio e distribuzione locale.

07 / ENISA
Threat Landscape, quadro 2026, periodo di riferimento gennaio-dicembre 2025.

Apri la fonte istituzionale
Grafico p. 8: PA 32%; servizi alle imprese 8%; trasporti 8%; manifattura 7%; finanza/banche 6%. Selezione di settori, non stima del rischio individuale.

08 / Unione europea
Regolamento (CE) n. 852/2004, articolo 5 e allegato II, capitolo IX: igiene e conservazione degli alimenti.

Apri la fonte istituzionale
Quadro p. 9: HACCP e catena del freddo.

09 / Unione europea
Direttiva (UE) 2022/2555, articolo 2 e allegato II, settore 4.

Apri la fonte istituzionale
Perimetro alimentare NIS2, p. 9; l’applicazione non deriva dalla sola presenza di un banco frigorifero.

10 / Normattiva; MASAF
Decreto legislativo 4 settembre 2024, n. 138, articolo 3 e allegato II. Autorità di settore NIS per gli alimenti.

Apri la fonte istituzionale
Ulteriore riferimento: masaf.gov.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/24226. Ruolo istituzionale e ambito, p. 9.

Grafico e schema: elaborazioni di Hermes Centro Studi Europeo. Non sono utilizzate stime non documentate del numero di vittime o dei danni complessivi in Italia.

IL SIGNIFICATO DEL CASO

La spesa quotidiana ha una parte invisibile

Torniamo al gesto iniziale: una confezione scelta da un banco, un acquisto che sembra semplice. Il suo percorso attraversa persone, impianti e decisioni. La tecnologia rende possibile coordinare questa complessità; proprio per questo le sue condizioni di funzionamento diventano parte del servizio.

Un episodio circoscritto, se rapidamente identificato e gestito, può restare locale. Una compromissione che coinvolga funzioni condivise può invece richiedere interventi su più sedi. Sono scenari condizionati dall'architettura, dalle capacità di risposta e dall'entità effettiva del problema: non previsioni di un blocco nazionale.

Il punto non è immaginare uno scaffale vuoto come destino inevitabile. È comprendere la catena di dipendenze che collega un accesso autorizzato, un comando corretto e una merce conservata nelle condizioni previste. L'invisibilità di questo lavoro non ne riduce l'importanza.

Gli eventi dell'autunno 2026 mostrano anche il valore della precisione. Sapere che esiste un rischio non significa conoscere già il responsabile. Sapere che un impianto è ripartito non significa avere ricostruito l'intera storia del prodotto. Distinguere questi piani aiuta a evitare sia allarmismi sia rassicurazioni premature.

> La sicurezza digitale entra nella vita quotidiana quando una decisione del software diventa una condizione del mondo fisico. Anche mentre facciamo la spesa.