Il nuovo quadro normativo: la Filiera Alimentare come infrastruttura critica

Per molto tempo abbiamo pensato alla sicurezza informatica come a un perimetro confinato dentro gli uffici amministrativi, una questione di password da cambiare o di email di phishing da evitare.

Oggi, però, la realtà industriale dell'agroalimentare racconta tutta un'altra storia. Le nostre fabbriche sono diventate ecosistemi digitali straordinariamente efficienti: i sensori monitorano le temperature in tempo reale, i sistemi gestionali dialogano direttamente con le linee di confezionamento e l'interconnessione 4.0 permette di governare la produzione con un clic.

Questa accelerazione tecnologica, se da un lato ha ridotto gli sprechi e ottimizzato i margini, dall'altro ha spalancato le porte a rischi del tutto nuovi, spostando la superficie di vulnerabilità dai server aziendali direttamente ai macchinari di stabilimento.

Proprio per questo motivo, il legislatore europeo ha deciso di intervenire con decisione. Con l'introduzione della Direttiva NIS2 — recepita nel nostro ordinamento attraverso il **D.Lgs. 138/2024** — il comparto della produzione, trasformazione e distribuzione degli alimenti è stato ufficialmente inserito tra i settori critici per la sicurezza nazionale.
Non si tratta di una semplice etichetta burocratica: l'Unione Europea ha riconosciuto che bloccare la catena logistica o compromettere i sistemi di un grande player del Food & Beverage non significa solo danneggiare un'azienda privata, ma mettere a rischio l'approvvigionamento alimentare di un intero Paese.
In questo nuovo scenario, la protezione digitale smette di essere un accessorio tecnico e diventa, a tutti gli effetti, un pilastro della continuità fisica della produzione.

Le responsabilità civili, penali e sanzionatorie in capo al CdA

La vera rivoluzione introdotta dal decreto di recepimento della NIS2 non risiede tanto negli obblighi tecnologici, quanto nella radicale trasformazione della catena di comando e della responsabilità.
Fino a ieri, un incidente informatico veniva gestito come un imprevisto tecnico di cui l'ufficio IT doveva trovare la soluzione. Da oggi le regole cambiano: la normativa chiama in causa direttamente i vertici dell'organizzazione. Gli articoli del decreto legislativo stabiliscono che la responsabilità ultima della gestione del rischio cyber ricade interamente sull'organo direttivo. È il Consiglio di Amministrazione che deve approvare formalmente le strategie di difesa, sovrintendere alla loro applicazione e rispondere in prima persona delle eventuali vulnerabilità sistemiche.

Per i membri del board, questa svolta si traduce in profili di rischio patrimoniale e professionale che non possono essere ignorati. Le sanzioni finanziarie introdotte per le aziende che non si adeguano sono draconiane e possono raggiungere i **7 milioni di euro o l'1,4% del fatturato globale annuo**, a seconda di quale sia l'importo più elevato.
Ma il legislatore si è spinto oltre, introducendo meccanismi di responsabilità personale per gli amministratori. In caso di gravi e reiterate inadempienze, infatti, i membri del CdA

rischiano sanzioni amministrative dirette e persino la sospensione temporanea dall'esercizio delle funzioni dirigenziali. La cybersecurity esce così definitivamente dalla sfera dei costi tecnici per entrare a pieno titolo in quella dei rischi legali e reputazionali che un amministratore ha il dovere fiduciario di governare.

I vantaggi commerciali ed economici dell'allineamento precoce

Guardare alla NIS2 esclusivamente come a un pesante fardello normativo o a un centro di costo significa, tuttavia, perdere di vista una straordinaria opportunità strategica. Nel mercato globale contemporaneo, la conformità a standard di sicurezza elevati si sta trasformando rapidamente in un potentissimo "abilitatore di business". Le grandi catene della Grande Distribuzione Organizzata (GDO) e i partner commerciali internazionali sono sempre più ossessionati dalla sicurezza della propria supply chain. Nessun grande distributore può permettersi il rischio che un attacco informatico ai danni di un fornitore blocchi le consegne sugli scaffali o comprometta l'integrità dei lotti. Di conseguenza, le aziende agroalimentari che dimostreranno per prime un solido allineamento alla direttiva otterranno un vero e proprio passaporto commerciale, diventando i partner preferenziali e più affidabili sul mercato.

Accanto al ritorno commerciale, l'adeguamento tempestivo genera benefici economici diretti e misurabili all'interno dello stabilimento. Nel settore alimentare, dove si lavorano materie prime altamente deperibili, un fermo macchina di poche ore dovuto a un ransomware può causare la perdita di intere giornate di produzione e scarti di prodotto dai costi esorbitanti. Investire nella resilienza significa azzerare questi scenari, proteggendo direttamente la redditività aziendale. Inoltre, disporre di un framework di sicurezza certificato e conforme alla legge rappresenta un fattore di riduzione del rischio che permette di rinegoziare in modo estremamente favorevole i premi delle polizze assicurative Cyber Risk, trasformando la compliance in un investimento capace di autofinanziarsi nel tempo.

Roadmap di attuazione per l'organo direttivo

Per tradurre questi principi in una strategia aziendale concreta, il Consiglio di Amministrazione deve impostare un percorso di attuazione chiaro, strutturato per fasi successive che permettano di governare la transizione senza scossoni operativi. Il primo passo è di natura prettamente istituzionale: l'azienda ha l'obbligo di registrarsi e censirsi sulla piattaforma digitale predisposta dall'**Agenzia per la Cybersicurezza Nazionale (ACN)**. Questo passaggio consente di formalizzare la posizione dell'impresa davanti all'autorità di vigilanza e di avviare ufficialmente il canale di comunicazione per la segnalazione di eventuali incidenti.

Subito dopo, la priorità si sposta sul fattore umano e sulla cultura aziendale, a partire proprio dai vertici. La norma prevede infatti l'obbligatorietà di percorsi formativi specifici sulla sicurezza digitale dedicati ai membri del board e al management, affinché la governance abbia gli strumenti critici per valutare i rischi e approvare i piani di investimento in modo consapevole. Infine, l'azione si sposta sul campo attraverso un audit approfondito condotto da terze parti indipendenti. L'obiettivo di questa analisi non è solo mappare le vulnerabilità dei sistemi IT e dei macchinari OT, ma valutare l'intera rete dei fornitori e dei manutentori

esterni. Solo comprendendo a fondo le interdipendenze della propria catena di fornitura, il CdA potrà varare un piano di gestione del rischio capace di proteggere l'azienda e proiettarla con sicurezza verso il futuro del mercato agroalimentare.