Quanto e come l'emergenza sanitaria ha modificato l'approccio alla difesa della filiera agroalimentare?

a cura della Redazione

Tra gli effetti collaterali della pandemia Covid-19, si sono delineate a livello globale nuove minacce per la filiera agroalimentare che vanno a sommarsi a quelle preesistenti, innalzando il livello di allerta degli stake-holders.
Aumenta di conseguenza l'importanza e la consapevolezza del ruolo della **Food Defence**, la disciplina che comprende norme, competenze, tecnologie e servizi preposti alla tutela complessiva del cibo.
essecome apre una sezione tematica permanente dedicata alla Food Defence per approfondire e divulgare gli argomenti relativi ad uno dei più rilevanti mercati verticali per l'industria della sicurezza, iniziando con un'intervista a **Francesco Rana**, corporate security manager di un primario gruppo agroalimentare italiano.

Tutela del cibo nella "nuova normalità": quali sono le principali minacce per la filiera agroalimentare percepite in questa fase, dalla produzione alla trasformazione fino al consumatore?
In un clima decisamente critico, il settore agroalimentare ha tenuto il colpo. Anzi, come noto i consumi nell'ambito food & beverage sono stati tra i pochi ad aver segnato delle variazioni positive durante il lockdown ma anche dopo, confermandosi anticiclici rispetto alle altre filiere.
Ovviamente, questo trend positivo ha determinato l'aumento di esposizione al rischio di natura fraudolenta, inducendoci ad innalzare il livello, già elevato, di attenzione e sensibilità per quella che è denominata "Food Defence".
Le attività di mitigazione del rischio, concentrate sulle alterazioni indotte da manipolazioni non autorizzate delle derrate, sul tampering degli imballi e delle confezioni lungo tutta la filiera, si sono pienamente integrate con tutte le prescrizioni governative emanate per contrastare l'emergenza sanitaria.
Questa "nuova normalità" ha indotto una maggiore e più efficace comprensione dell'utilità di procedure e sistemi a protezione del processo produttivo.
Non trascuriamo comunque il fatto che, nella crisi sanitaria che stiamo vivendo, si insinua inevitabilmente ogni forma di frode. La frode alimentare trova terreno fertile poiché la crisi induce a concedere deroghe per garantire la continuità operativa.

In questo contesto c'è stato inevitabilmente un incremento di casi di frode segnalati.
D'obbligo, pertanto, è aggiornare le valutazioni dei rischi facendo attenzione a tali vulnerabilità collegate alla crisi acuta e di medio termine ormai profilata.

Come si manifestano nel comparto gli attacchi cyber che stanno imperversando a livello goblale?
La pandemia Covid 19 ha accelerato la trasformazione digitale in tutti i comparti industriali, incluso quello agroalimentare, tuttavia qualche ambito ha riscontrato difficoltà, peraltro scontare, ad inseguire questa trasformazione.
Forse perché il successo della trasformazione digitale sta non solo nell'adozione di tecnologie avanzate, ma anche nell'adattamento delle strutture organizzative: le iniziative digitali possono facilmente fallire se le strutture organizzative e i processi decisionali non si adattano al nuovo mandato.
Su questo terreno ancora incerto, la criminalità informatica si attiva con phishing multilivello, malware, attacchi informatici mirati proprio alle aziende agroalimentari che vedono il ritorno degli "hacktivisti", ossia gli attivisti della rete che usano le proprie competenze da hacker per mettere in atto forme di protesta o di disobbedienza civile.
Tutto ciò determina una ipersensibilità del comparto, in virtù della quasi completa automatizzazione dei processi e, soprattutt,o dell'impegno continuo e costante alla qualità del prodotto nei confronti del consumatore finale.
Le aziende più lungimiranti, ipotizzando questi scenari di rischio, hanno implementato protezioni efficaci (ad esempio tramite la segmentazione delle reti), in modo da proteggere il business.
Non posso non fare un accenno allo smart working che in questo periodo ha visto un consistente aumento di utilizzo. Lavorare da casa per preservare la popolazione aziendale, continuando a garantire, per quanto possibile, l'operatività e la continuità dei servizi, è un cambio di rotta importante nelle modalità di intendere il lavoro.
Una nuova situazione che rientra nella trasformazione digitale che, se da una parte presenta effetti decisamente positivi, dall'altra comporta pericoli sulla sicurezza di aziende e individui in termini di cyber risk, in quanto hacker e criminali informatici sono ormai da mesi in agguato

approfittando della situazione emergenziale, per colpire tramite l'utilizzo di e-mail, siti web, telefonate e anche messaggi di testo, ed accedere a network privati e informazioni riservate.

Ritiene che il quadro normativo sia in linea con la situazione attuale? Cosa si dovrebbe chiedere al legislatore nazionale e/o europeo?
La domanda mi fa ritornare sull'argomento del riconoscimento alla filiera agroalimentare di Infrastruttura Critica, argomento affrontato in tempi non sospetti da autorevoli ricercatori alla luce della Direttiva Europea 2008/114/CE.
La Dir. 2008/114/CE all'Art. 2 punto a), definisce "Infrastruttura Critica" *«un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni»*
La filiera agroalimentare per dimensione si attesta, in Italia, al secondo posto dopo il comparto metalmeccanico e si pone a livello europeo in 3° posizione per fatturato dopo Francia e Germania; dati importanti a cui si aggiunge il ruolo nevralgico che la stessa ha avuto e continua ad avere durante questa crisi sanitaria.
Con le sue tipicità, è un'infrastruttura che va protetta e difesa da attacchi intenzionali e da disastri naturali.
Sempre la stessa direttiva 2008/114/CE all'Art. 2, lettera b) definisce "Infrastruttura Critica Europea" *«un'infrastruttura critica ubicata negli Stati membri il cui danneggiamento o la*

cui distruzione avrebbe un significativo impatto su almeno due Stati membri. La rilevanza dell'impatto è valutata in termini intersettoriali».

La responsabilità della protezione delle infrastrutture critiche nazionali viene quindi demandata ai loro proprietari e agli Stati membri, considerando critiche solamente il comparto energia ed i trasporti ed escludendo evidentemente la filiera agroalimentare.

L'Italia nel 2011 ha recepito la Direttiva Europea con il Dlgs dell'11 Aprile n. 61 nelle quali designa, come infrastrutture critiche, solamente quelle indicate dalla Dir. 2008/114/CE.

L'auspicio è che, in virtù della strategicità che il settore riveste, oggi più che mai, dato che il paese sta attraversando un periodo storico critico ed in considerazione delle vulnerabilità connesse al settore stesso, l'esigenza di considerare il settore agroalimentare una infrastruttura critica è diventata una priorità.

Le soluzioni oggi disponibili per mettere in sicurezza il cibo rispetto ai diversi rischi (sanitari, predatori ecc,) rispondono alle esigenze attuali? Dal vostro punto di vista cosa sarebbe necessario?

Anche se il mondo del cyber crime ha catturato in maniera preponderante la nostra attenzione, non foss'altro perché il nemico attacca in maniera subdola, a volte per caso, scatenando i suoi effetti dirompenti spesso a distanza di tempo, nell'ambito della food defense abbiamo la necessità di proteggere l'infrastruttura alimentare anche e soprattutto fisicamente.

Il mercato offre una vasta gamma di soluzioni tecnologiche decisamente in linea con le esigenze del settore.

Nell'ottica della protezione concentrica degli obiettivi

sensibili è opportuno partire dalla protezione perimetrale con sistemi di video sorveglianza evoluti (telecamere termiche/video analisi) e sistemi antintrusione.

Anche il controllo accessi mediante l'utilizzo di teste di lettura dei classici badge o anche di apposite app scaricate sugli smartphone, riveste una fondamentale importanza.

Nelle fasi topiche della pandemia le autorità di controllo hanno valutato positivamente l'utilizzo di tali tecnologie a protezione delle infrastrutture e dei processi di lavorazione.

Resta inteso che la risorsa umana, debitamente formata, trova già trova ma, a mio avviso, dovrebbe trovare più spazio nel processo della security.

Ogni tipologia di strumento tecnologico deve consentire una difesa preventiva da ogni forma di attacco ma la gestione della situazione è in capo alla risorsa umana.

L'integrazione di sistemi, tecnologie e procedure non può prescindere dall'esistenza di un affidabile centro di controllo (Security Control Room) che può assolvere anche ad altre necessità come ad esempio. i controlli sull'automazione dei processi in fasce notturne.