Logistica 4.0 e cybersecurity:

di **Massimo Centofanti**
Cyber Security Technology Unit Manager di aizoOn Consulting*

Ogni rivoluzione comporta rischi e questo vale anche per il mondo della logistica 4.0, dove le nuove tecnologie sono associate a importanti minacce di cybersecurity. Ecco perché è importante conoscere i rischi che le aziende corrono e identificare le soluzioni giuste per renderle resilienti. In particolare, il futuro della logistica si chiama Digital Twins, modelli digitali, vere e proprie rappresentazioni della realtà che costituiranno il sistema arterioso della logistica 4.0 destinata a svolgere un ruolo determinante nel sistema di produzione just in time con obiettivi di ordini consegnati in tempi sempre più brevi e monitorati in tempo reale. Una varietà di applicazioni si produrrà lungo l'intera catena del valore. Tutto ciò consentirà una gestione più efficiente delle flotte di container, il monitoraggio delle spedizioni e la progettazione di sistemi logistici integrati, grazie all'impiego di tecnologia sofisticata in cui macchine, impianti di logistica e prodotti sono tra loro connessi. Una nuova prospettiva influenzerà anche i magazzini. Avremo magazzini intelligenti che, grazie alla digitalizzazione, saranno in grado di verificare la disponibilità di prodotti; processi automatizzati di carico che aggregheranno le informazioni delle giacenze con quella delle merci in transito, localizzando lo stato di una spedizione e consolidando il processo dell'ultimo chilometro per la consegna: veri e propri magazzini mobili.

La logistica 4.0 richiede l'applicazione di nuove tecnologie e di nuovi modelli digitali, tesi, in primo luogo, a raggiungere più elevati livelli di efficienza e di produttività

Grazie all'AI e al machine learning, il flusso dei dati verrà analizzato automaticamente e miglioreranno il controllo e l'indirizzamento degli ordini, permettendo ai vari operatori di logistica 4.0 - aggregando meglio i prodotti sulla base di previsioni sempre più sofisticate e precise - di ridurre i tempi di consegna.
Questa rivoluzione non si produrrà nel vuoto: già il manufacturing digitalizzato, che si evolve verso una produzione sempre più on-demand in grado di soddisfare il binomio della variabilità della domanda e della rapidità della risposta, ha modificato il modo di produrre e distribuire. I Digital Twins, dunque, saranno protagonisti di un contesto sempre più smart e connesso, vivacizzato dalla robotica, dalle blockchain e dalla realtà aumentata. Queste evoluzioni si tradurranno in un approccio sempre più orientato alla decentralizzazione della gestione e trasporto delle merci e una logistica 4.0 sempre più "liquida", in grado di ridurre le barriere geografiche tra i vari centri di stoccaggio, che si convertiranno in moderni spazi digitalizzati, i cosiddetti cloud-storage di componenti fisici.

Come dicevamo, ogni rivoluzione comporta rischi. La logistica 4.0 apre nuove potenziali falle nel comparto della security a causa di due fenomeni in particolare: la frammentazione di attori nella supply chain e la massiccia apertura verso l'esterno dei flussi di dati. L'attenzione alla sicurezza, in pratica, dovrà essere rivolta non solo al proprio contesto organizzativo, ma anche verso i soggetti che fanno parte dell'ecosistema con cui l'azienda interagisce nella propria catena del valore. Siccome nei nuovi scenari digitali la supply chain rappresenta un elemento critico per la sopravvivenza delle aziende, è fondamentale adottare misure di sicurezza efficaci che nascano dalla collaborazione delle diverse componenti della filiera, attraverso strumenti mirati e linee guida precise che vengano condivise da tutti i protagonisti.

come conciliarli?

IL PROFILO DI AIZOON

aizoOn – socio di SOS-LOGistica - è una società di consulenza tecnologica di innovazione, indipendente, che opera a livello globale sostenendo i suoi clienti nella transizione all'era digitale. Adotta un modello operativo digital oriented, basato su logiche trans-disciplinari, agili e iterattive, collaborative e aperte, abilitanti l'innovazione applicata. Ha un approccio a rete e si avvale della collaborazione di partner tecnologici e di ricerca. Svolge inoltre, attività di ispezione e opera nella verifica della sostenibilità, della responsabilità sociale di impresa, della sicurezza alimentare, dei sistemi informatici. Realizza, infine, attività di informazione e formazione su tali temi.

Il maggior ricorso alle nuove tecnologie, se fa crescere l'efficienza, comporta anche un maggiore decentralizzazione della gestione delle informazioni, incrementando l'esigenza di sicurezza

Dal Third Annual State of Cyber Resilience study di Accenture emergeva infatti già prima della pandemia che il 40% delle violazioni avviene proprio attraverso attacchi a soggetti che fanno parte dell'ecosistema delle aziende, i cosiddetti indirect attacks, e questo evento non potrà che aumentare proprio alla luce dei due fenomeni richiamati sopra.

In concreto, per garantire una sicura logistica 4.0, sarà necessario attuare una precisa analisi dei rischi e delle minacce di tutto il processo di filiera al fine di:

- identificare tutti i processi critici della catena della logistica, a livello sia interno sia esterno, e delle interconnessioni con i processi di industria 4.0 e supply chain 4.0;
- attuare un'analisi del flusso delle informazioni/dati lungo tutta la filiera, identificando i potenziali rischi di data security&cyber security e coinvolgendo in questo processo tutte le parti interessate;
- svolgere l'attività di analisi degli impatti (BI-Business Impact Analysis) economici, normativi, strategici, ambientali e reputazionali derivanti dai rischi/minacce identificati;
- predisporre piani di Risk Management&Business Continuity coinvolgendo le parti interessate (Risk Manager, Business Continuity Manager, Security Manager, IT&Cyber Security Manager, la funzione legale, finanziaria, fiscale e della comunicazione, ecc.);
- garantire l'incorporazione della cultura del rischio, della sicurezza e della continuità operativa all'interno dell'organizzazione, ricordando quanto sia fondamentale il supporto del Top Management e il coinvolgimento di tutta l'organizzazione nei piani di Risk Management&Business Continuity;
- redigere procedure e implementare standard di sicurezza interna ed esterna (fase di carico e scarico, varchi di accesso, perimetro del magazzino, fasi di stoccaggio e fasi di trasporto), effettuare indagini di intelligence sulla condotta del personale, sugli standard di sicurezza fisica adottati sui mezzi di trasporto e degli spazi in cui i beni dell'organizzazione transiteranno o sosteranno durante le fasi del processo di logistica;
- svolgere indagini di mercato e benchmarking per verificare l' adeguatezza della tecnologia adottata rispetto ad altri operatori di settore e migliorare le procedure di gestione dei rischi, della salvaguardia della sicurezza e della resilienza aziendale.

La grande opportunità costituita dalla logistica 4.0 può trasformarsi in un boomerang se non saranno opportunamente gestite anche le sue potenziali ricadute negative. Il minimo malfunzionamento di una componente del sistema informativo dovuto ad un cyber attack può comportare serie conseguenze in termini di costi diretti, perdita di clienti e danni di immagine per la logistica 4.0 in quanto la catena logistica deve rendere conto del proprio snodarsi a più attori lungo la filiera (azienda, fornitori, spedizionieri, trasportatori, clienti e clienti dei clienti, ecc.).
Il punto di partenza per una corretta gestione di questi rischi è, come sempre, la consapevolezza. ■