Pierdavide Scambi (*)

# Logistica e sicurezza: occhio al rischio cyber

**Il settore dei trasporti, dello storage e delivery sono stati durante il 2020 i primi tre obiettivi colpiti più severamente dagli attacchi informatici, assieme al comparto bancario. Il settore dei trasporti è nel mirino delle minacce cyber e i criminali informatici sono talvolta anche "sponsorizzati" da uno Stato, in una forma di sleale concorrenza mirata a ridurre la capacità logistica e di fornitura dei paesi competitor.**

(*) Studio Scambi Vicenza **www.studioscambi.com**

Le grandi aziende ormai sono consapevoli riguardo ai rischi e alla sicurezza IT, ecco perchè gli attacchi informatici si sono indirizzati su quello che viene considerato l'anello debole del sistema, ovvero le terze parti: i subappaltatori che di rimando si innestano nella supply chain e nella logistica. Il consumatore ripone la propria fiducia nel brand conosciuto, ma nel complicato processo di acquisizione di un bene, si innestano moltissime lavorazioni che vengono subappaltate ad altre aziende, generalmente di dimensioni minori, e meno preparate a gestire il rischio di un cyber attacco.

## Il ruolo dell'utente

Dal canto loro, gli acquirenti sono diventati sempre più esigenti e vogliono monitorare in real time la loro spedizione, aprendo ulteriori falle nel sistema ed aumentando la già esponenziale interconnettività della supply chain e della logistica 4.0. La tecnologia (AI e robotica) costituisce infatti la base della logistica 4.0, ponendo al centro il cliente e la sostenibilità ambientale e attingendo alla Smart Containerization, che realizza l'integrazione di servizi logistici negli ambienti domestici smart. Il produttore o il gestore logistico devono garantire consegne sempre più rapide e sopperire ai ritardi in tempo reale. Le applicazioni che forniscono servizi di track-and-trace, impongono alle aziende di essere rapide, flessibili e veloci e le obbligano a garantire la sicurezza nella fase logistica con software avanzati di supervisione e monitoraggio.

## Gli attacchi-tipo

Tra le principali tipologie di attacchi scoperti ad oggi si annoverano: spam, imitazione opportunistica e mirata. Inoltre gli attacchi di imitazione sono in aumento, rappresentando il 26% delle rilevazioni totali – e ora includono il phishing o "vishing", un attacco evoluto in cui gli hackers usano l'ingegneria sociale per accedere ai dati personali e finanziari mediante il sistema telefonico della vittima (sms).

Ibm Security ha valutato il comportamento dei consumatori nell'utilizzo degli strumenti digitali durante la pandemia e gli effetti per la cybersecurity nel lungo periodo, con un campione di 22 mila adulti in 22 Paesi. La tendenza al digitale ha prodotto un'insufficiente attenzione nella generazione di password e comportamenti superficiali che hanno minato e minano la cybersecurity. Infatti, la compromissione delle credenziali utente è uno dei principali vettori degli attacchi informatici segnalati nel 2020.

## Come difendersi

Per difendersi da tali minacce, le organizzazioni devono adottare un approccio capace di diffondersi in campi e aspetti un tempo estranei alla sicurezza, ad esempio la posta elettronica, servendosi di strumenti che consentano una maggiore visibilità all'interno e oltre il perimetro. Il quadro normativo nazionale parte dal decreto-legge 14 giugno 2021, n. 82 convertito con modificazioni nella legge 4 agosto 2021, n. 10 recante: «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale». Esso rappresenta lo scenario legislativo delle misure da adottare per la sicurezza delle reti e dei sistemi informativi, ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS. A livello di Unione Europea, è in vigore la direttiva (UE) 2016/1148 del 6 luglio 2016, che reca misure per uno standard comune di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. direttiva NIS - Network and Information Security") allo scopo di raggiungere un "livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale; contribuendo ad incrementare il livello comune di sicurezza".

## Business continuity

A questo proposito, oltre ai processi di riorganizzazione aziendale fisica, si impone di prestare massima attenzione alla continuità operativa. Il Risk management, legato alla supply chain ed alla logistica, si deve necessariamente basare su un'articolata predisposizione della continuità operativa, oltre che sulla gestione del rischio. Per l'autorevole BCI (Business Continuity Institute), circa l'82% delle società che hanno un efficiente sistema di gestione della Continuità Operativa (BCM – Business Continuity Management) sono state in grado di limitare gli impatti di crisi, incidenti, e le emergenze. Queste imprese, inoltre, hanno voluto promuovere i propri programmi di BMC anche al di fuori del loro contesto aziendale richiedendo ai vari "attori" della catena di implementare il proprio programma di BMC e di testare, attraverso periodici audit e verifiche, di potere essere responsivi entro i parametri concordati.

Va da sé che i trasporti fisici, oramai legati ai trasporti digitali, sono purtroppo soggetti alle stesse prudenze e regole di sicurezza.

**Per un approfondimento sulla Direttiva NIS e lo stato di attuazione**

**Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale**