

Shipping Italy

Il quotidiano online del trasporto marittimo

Cosa insegna il Crowdstrike e l'importanza della protezione dei dati per l'operatività dei trasporti

Nicola Capuzzo · Tuesday, July 30th, 2024

*Contributo a cura di Ing. Katia Redini **

** digital advisory & formazione*

Senz'altro in questi giorni si sprecono gli articoli che parlano degli enormi disagi nei trasporti (e non solo) causati dal malfunzionamento del sistema di Crowdstrike.

Quello che è meno evidente e su cui vale la pena soffermarsi è la necessità vitale di disporre di dati (e la loro forma aggregata che costituisce informazioni) affinché tutto il comparto dei trasporti e della logistica possa operare.

Questi dati devono essere sempre disponibili (cosa che evidentemente è mancata per i problemi di aggiornamento della piattaforma Falcon) oltre a dover essere tenuti integri e confidenziali. In gergo tecnico, nell'ambito della sicurezza informatica questo è ciò che viene indicato come "triade CIA" e per quanto possa sembrare un complesso intreccio di tecnologie e metodi di intelligence per soli addetti ai lavori è invece una questione che dovrebbe impattare su chiunque operi in un'organizzazione. Perché la creazione, la gestione e la protezione dei dati (personali, industriali, aziendali, operativi,...) riguarda tutti: dagli operatori del Terminal, agli impiegati dell'area amministrativa, allo Spedizioniere, agli autisti di camion e tutti gli attori (tantissimi) coinvolti, ognuno nell'area di propria competenza, nell'ecosistema dei vari processi che contraddistinguono i trasporti e la logistica, settore caratterizzato da uno scambio intenso di dati.

L'interazione uomo-macchina c'è sempre quando si parla di tecnologie di Information Technology a supporto del business. A questa si affianca la crescente interazione macchina-macchina (che va in generale sotto il nome di Internet-of-Things e che troviamo nell'accezione della Logistica 4.0), ovvero il "dialogo" tra sistemi basato su dati digitali estremamente presente nel settore della logistica essendo l'automazione un elemento necessario per l'efficientamento e la velocizzazione delle attività, alle comunicazioni satellitari per navi, aerei, treni, camion agli smart port.

Chiudiamo la panoramica tecnologica che caratterizza l'infrastruttura digitale nei trasporti con

l'OT (Operational Technology) costituita da sistemi ICS per il monitoraggio di processi fisici e infine la sempre più diffusa adozione (siamo solo all'inizio) dell'Intelligenza Artificiale che potrà diventare elemento differenziante nella competitività globale.

Perché nulla si inceppi in questo districato sistema interconnesso, la sicurezza informatica è indispensabile. Ed è proprio questo il nocciolo centrale.

Un diffuso gap culturale induce a pensare che la sicurezza informatica riguardi esclusivamente il personale IT che deve occuparsi di installazioni di software o altri dispositivi che proteggano la rete aziendale. Nulla di più sbagliato.

Del resto anche il problema globale di CrowdStrike non è stato causato da un attacco informatico ma la mancata disponibilità di dati e sistemi c'è stata.

La sicurezza dell'informazione passa anzitutto dalle persone, dalla loro formazione e dal rispetto delle procedure che vengono attuate in azienda ed in tutta la supply-chain.

Per sensibilizzare sul tema in modo semplice, suggerisco sempre di ragionare con l'approccio del "Ma se...?" provando ad immaginare cosa succederebbe alterando, bloccando o distruggendo dati che impattano sulla creazione ad esempio di DDT, Bill of landing, AWB, Bollette Doganali, Manifesto merci, etc. o sul tracking di un viaggio, nella gestione automatica di ingresso/uscite dei camion da un terminal, nel carico/scarico container su nave o treno...Si interrompe il servizio con tutte le conseguenze del caso.

Queste situazioni, tralasciando l'ipotesi di un attacco da parte del cyber-crime verso l'infrastruttura tecnologica, nascono troppo spesso dal fattore umano intendendo con questo le vulnerabilità dei nostri comportamenti o il commettere un errore (con o senza dolo). E torniamo quindi alla sicurezza dell'informazione e alla protezione dei dati perché è questo che interessa nel cercare di garantire resilienza operativa e la business continuity.

Dall'imprevedibilità di un guasto a un sistema che ha messo in ginocchio a livello globale così tanti settori strategici occorre trarre un insegnamento e sicuramente la definizione di buone procedure di risposta ad un incidente informatico rientrano tra le best practices da attivare.

Il tema della sicurezza dell'informazione a 360° deve essere visto come la tutela al business e l'innegabile dipendenza dal digitale non può che portare a questa conclusione.

Avendo procedure e adeguata formazione a tutto il personale significa non fermare i processi produttivi e operativi, significa non subire ingenti perdite finanziarie, non creare danni alla reputazione dell'azienda e non andare incontro a sanzioni.

Temi troppe volte ripetuti? Probabile. Così come è piuttosto evidente che ancora il gap culturale vada colmato.

ISCRIVITI ALLA NEWSLETTER QUOTIDIANA GRATUITA DI SHIPPING ITALY

**SHIPPING ITALY E' ANCHE SU WHATSAPP: BASTA CLICCARE QUI PER
ISCRIVERSI AL CANALE ED ESSERE SEMPRE AGGIORNATI**

This entry was posted on Tuesday, July 30th, 2024 at 8:30 am and is filed under [Economia](#)
You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. Both comments and pings are currently closed.

