

# Logistica e cybersecurity, servono più risorse e formazione

Genova – Società di hackeraggio pagate per minare la logistica di Paesi concorrenti, sistemi operativi pagati su abbonamento disponibili dark web, a partire da 40 euro al mese, che eseguono attacchi sistematici alle aziende per poter ricavare cospicui riscatti

24/01/2022

•  
•  
•

**Genova – Società di hackeraggio pagate per minare la logistica di Paesi concorrenti**, sistemi operativi pagati su abbonamento disponibili dark web, a partire da 40 euro al mese, che eseguono attacchi sistematici alle aziende per poter ricavare cospicui riscatti. **Nel 2021**, spiega Paola Girdinio, presidente del centro di competenza Start 4.0 il costo della cybersecurity è stato sei volte quello del Prodotto interno lordo di tutto il mondo. Per questo, a fronte di numeri sempre più alti e di una sensibilità che giocoforza sta crescendo tra le aziende (secondo l'ultimo Allianz Risk Barometer, la cybersecurity è al primo posto dei rischi più temuti dai direttori finanziari delle principali società di trasporto globali) i soldi messi a disposizione del Piano nazionale dei Recupero e resilienza (623 milioni su 270 miliardi) sembrano comunque pochi.

**E' una delle tematiche emerse dall'incontro "Cyber Security, un'emergenza per la filiera Trasporti & logistica"** organizzato oggi pomeriggio a Genova da Confrtrasporto-Confcommercio insieme a Federlogistica nell'ambito degli incontri della Logistic Digital Community, con la collaborazione tecnica di Liguria Digitale. Pochi soldi, e un soggetto – il ministero delle Infrastrutture e mobilità sostenibile – che "sembra sempre più un centro ricerche e sempre meno un ministero, nonostante la maggior parte della quota economica degli interventi del Pnrr siano proprio in capo a questo soggetto" denuncia Luigi Merlo, presidente di Federlogistica. **Eppure**, proprio nel campo dei trasporti, il settore pubblico deve colmare un vuoto significativo, visto il fallimento dell'esperienza di Uirnet e la mancata creazione di un linguaggio digitale comune per tutti i centri modali del Paese, a partire da porti e interporti. "Invece – aggiunge Merlo – proprio alcuni giorni fa il ministero ha

rilanciato l'ennesimo Piano nazionale della Logistica: una cosa che poteva andare bene negli anni Settanta, e che invece non è più adeguata al periodo che stiamo vivendo”.

**La questione più scottante** – e come ha spiegato Davide Falteri, presidente del Consorzio Global, gli incontri della Logistic Digital Community servono proprio a inquadrare i temi specifici e più funzionali alle aziende – è certamente quello della formazione del personale: non si tratta unicamente di chi deve gestire i servizi tecnologici di una società, ma in genere tutte le persone che fanno parte dell'organizzazione. **In un certo senso**, dice Falteri, con la cybersecurity sta accadendo ciò che in passato e purtroppo talvolta ancora oggi accade con la legge 626 sulla sicurezza del lavoro: qualche soggetto sottovaluta punti importanti, e questo può creare problemi seri.

**Seri quanto?** Giovanni Satta, docente del dipartimento di Economia dell'Università di Genova, prova a metterli in fila: “Non ci sono solo i costi diretti, quelli derivati dalla perdita dei dati, dall'interruzione del lavoro, dell'eventuale pagamento del riscatto, dal ripristino dell'infrastruttura informatica e comunque dalla ricaduta negativa su tutto il ciclo produttivo: c'è anche un costo, più difficile da calcolare ma ugualmente concreto, derivato dalla perdita di fiducia da parte del cliente, che si ritrova ad avere un servizio peggiore e rallentato, cui si aggiungono costi di reputazione”, che si pagano nel lungo periodo. “Il problema – aggiunge Satta – è che l'investimento sulla cybersecurity è oneroso, e spesso le imprese tendono a rinviarlo”. **In Italia gli investimenti in cybersecurity sono stati lo scorso anno pari a 1,3 miliardi di euro**, globalmente tra le quote più basse, ma la cosa più preoccupante, rileva Satta, è che solo il 2% di queste risorse è stato investito nel cybertraining.

**Vero è che l'accesso ai finanziamenti non è facile**, e che le imprese italiane, anche quelle della logistica, spesso hanno piccole dimensioni e non possiedono una struttura finanziaria in grado di sostenere i costi per proteggersi dagli attacchi informatici, come ha sottolineato Paolo Odone, presidente della Confcommercio di Genova, che ha anche sollecitato un investimento da parte della Regione Liguria in questo senso, e la fornitura da parte di Liguria Digitale di un pacchetto informatico proprio tagliato sulle esigenze dei più piccoli. **Un suggerimento accolto da Riccardo Battaglini**, direttore dell'unità di business Pubblica amministrazione e mercato di Liguria Digitale. All'incontro, che ha seguito i saluti istituzionali di Enrico Castanini, amministratore unico di Liguria Digitale; Giovanni Toti, presidente della

Regione Liguria; Marco Bucci, sindaco di Genova, hanno partecipato anche Alessandra Mancini, avvocato presso B-Right Lawyers, che ha parlato delle nuove responsabilità in materia di compliance in tema cyber) e Gianluigi Lercari, amministratore delegato del gruppo Lercari, che ha spiegato i riflessi assicurativi e di cybersecurity attraverso gli strumenti di analisi e di mitigazione del rischio.