

Attacchi hacker, Federlogistica chiede al MIMS formazione preventiva

All'indomani dell'azione rivendicata dal collettivo russo Killnet, l'associazione di categoria torna a ribadire l'importanza di un maggiore coordinamento tra imprese, governo e Agenzia per la cybersicurezza



(Zukunft Für Alle Kongress/Flickr)

Oltre a diversi siti istituzionali italiani – tra cui il Consiglio superiore della magistratura, l'Agenzia delle Dogane, i ministeri di Esteri, dell'Istruzione e dei Beni Culturali – l'attacco hacker di ieri del collettivo russo Killnet ha colpito anche le infrastrutture digitali di tante aziende di trasporto e logistica, come società di autotrasporto, spedizionieri, doganalisti, aziende ferroviarie, aeroportuali e terminal portuali. È bene sottolineare, però, che a fronte della lunga lista di siti che il collettivo ha dichiarato di aver colpito, al momento [non pare che ci siano stati particolari danni](#).

In ogni caso, soprattutto per prevenire blackout futuri, il presidente di Federlogistica-Contrasporto, Luigi Merlo chiede al ministero delle infrastrutture di farsi carico delle funzioni di «regia e supporto, sia alle strutture pubbliche sia quelle imprese del settore trasporti, logistica e dello shipping, che svolgono un ruolo strategico, come i terminal portuali, coordinandosi con l'Agenzia nazionale per la cybersicurezza». Si chiede un maggiore coordinamento tra imprese e governo, oltre a «un piano di formazione per disporre delle figure professionali oggi praticamente inesistenti», afferma Merlo.

Federlogistica-Confrtrasporto, parallelamente ad altre associazioni di categoria, ha evidenziato da settimane, in concomitanza con altri attacchi informatici subiti da altri Paesi europei, la fragilità dei sistemi informatici italiani, per i quali chiede maggiore protezione. «Deve essere anche messo a punto in tempi rapidissimi – prosegue Merlo - un progetto di formazione che consenta al sistema di disporre di quelle figure professionali di alto livello che sono indispensabili per una mappatura e un aggiornamento costante sui pericoli cyber e sulle misure di reazione agli stessi. Se ai ritardi derivanti dal black out dei porti cinesi – conclude Merlo – dovessero sommarsi le conseguenze di un cyber attack efficace ai nodi strategici del nostro sistema logistico e portuale, l'economia dell'intero Paese subirebbe un colpo mortale, in un momento già caratterizzato da una estrema fragilità e debolezza».