LA STAMPA

topnews

Un decreto legge entro l'estate per l'Agenzia nazionale di Cybersecurity: servirà anche ad attaccare

Il sottosegretario alla Difesa, Giorgio Mulè: «Lavoriamo al progetto di Cyber Defence Academy, sarà un centro di alta formazione». Dalla Ue in arrivo un miliardo di euro di nuovi finanziamenti

GIULIANO BALESTRERI

PUBBLICATO IL
15 Maggio 2021

L'Italia accelera sulla cybersecurity. A fianco del pacchetto da 620 milioni contenuto nel Pnrr è in arrivo un decreto legge per istituire l'Agenzia per la cybersicurezza nazionale. La fragilità dell'infrastruttura italiana e il costante aumento di attacchi hacker, dall'oleodotto americano messo ko al tilt provocato al sistema sanitario irlandese, hanno convinto il governo ad accelerare i tempi. E il decreto legge - da quanto si apprende - sarebbe lo strumento più efficace per rispondere alle esigenze del Paese.

Nel suo intervento al webinar organizzato dal Parlamento europeo sulla "Strategia Ue per rafforzare la sicurezza informatico", il sottosegretario alla Difesa, Giorgio Mulè ha spiegato che l'agenzia nazionale «dovrà nel più breve tempo possibile poggiare le sue fondamenta all'interno del tessuto legislativo con una norma di primo livello che dovrà vedere coinvolto appieno il Parlamento per recepirne gli indirizzi e le correzioni». Una conferma indiretta dell'intenzione di ricorrere a un decreto legge da presentare alle Camere prima dell'estate.

Il piano italiano entra a pieno diritto nella strategia comunitaria che prevede finanziamenti per circa un miliardo di euro destinati «ai Centri operativi nazionali della cybersecurity a cui andranno le migliori tecnologie come l'Intelligenza Artificiale, i Big Data, per prevenire le minacce e migliorare l'ecosistema» ha aggiunto Roberto Viola, direttore generale Dg Connect della Commissione europea. Viola ha anche voluto esprimere un «plauso al Governo italiano perché ha previsto un Centro nazionale» ed è arrivato a ipotizzare «sanzioni per le aziende» che non adotteranno strumenti adeguati alla cybersecurity.

Mulè esclude le sanzioni e, invece, insiste sul bisogno di «coinvolgere il mondo civile coniugandolo con quello militare e di intelligence. Il nuovo organismo dovrà creare una nuova cultura digitale capace di fare formazione. A questo proposito si sta lavorando al progetto di Cyber Defence Academy, cioè di un centro di alta formazione dove le esperienze maturate nel comparto difesa dovranno coniugarsi con le competenze già presenti nella pubblica amministrazione marciando in maniera osmotica con le imprese private».
L'Agenzia dovrebbe partire con 300 persone per arrivare a impiegarne circa mille in cinque anni, ma sarà sganciata da servizi segreti per andare sotto il cappello della Presidente del consiglio dei

ministri. Ma soprattutto non avrà solo compito difensivo: potrà contrattaccare in caso di minacce internazionali.

D'altra parte la sicurezza informatica è sempre più cruciale: nel 2019 il numero degli attacchi in Europa è triplicato a quota 700 milioni con un costo globale, stimato per il 2020, di 5.500 miliardi di euro. E con quasi 20 miliardi di dispositivi connessi in tutto il Vecchio continente, il rischio è in costante crescita.

Il rischio è che lo sforzo non basti. Per Gabriele Faggioli, responsabile scientifico dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano e Ceo di Digital360, «manca una visione moderna del problema. Si supporta il perimetro nazionale, ma per le imprese, in particolare le Pmi, non c'è nulla. Come Clusit, associazione italiana per la sicurezza informatica, avevamo suggerito una scheda di incentivi simile a industria 4.0, ma non siamo stati ascoltati».

Eppure il tallone d'Achille sono proprio le imprese private. «Sono quelle che pagano i riscatti chiesti dagli hacker» spiega Riccardo Baldanzi, amministratore delegato di 7Layers, società controllata al 70% da Fastweb: «Ci sono tante aziende violate che potrebbero non accorgersi mai di aver subito un attacco informatico. Dipende se l'obiettivo è un riscatto o un dato».

L'82% degli assalti si conclude con la richiesta di un riscatto: «Gli attacchi geopolitici sono molto pericolosi, ma sono pochi – spiega Faggioli – Per fortuna sono sempre di più le aziende che denunciano, anche perché chi paga si espone a rischi sempre maggiori. Oltre finanziare i criminali della rete».

Maurizio Mensi, professore diritto dell'economia alla Scuola Nazionale di amministrazione ed esperto di cybersicurezza, è tra i membri italiani del Comitato economico e sociale europeo insiste sulle necessità di creare una sorta di white list per i fornitori: «Servono garanzie, altrimenti il Paese di esporrà a rischi costanti. Penso per esempio ai prodotti tecnologici forniti dai cinesi: una norma di Pechino obbliga le aziende a fornire al governo tutti dati in loro possesso, appena richiesto».

Un problema non di poco conto considerando dai termoscanner presenti a Palazzo Chigi fino alle telecamere di sorveglianze usati nelle procure, gli apparati made in China sono tra i più comuni.