# Piano cybersecurity, gli 007 possono anche contrattaccare

ServizioLa strategia nazionale

## La strategia nazionale di cybersicurezza 2022-2026 è stata predisposta dall’Agenzia per la cybersicurezza nazionale e presentata dall’Autorità delegata per la sicurezza della Repubblica, Franco Gabrielli e dal direttore dell’Agenzia, Roberto Baldoni.

25 maggio 2022

Alert dell’Agenzia per la cyber-sicurezza, 71 “porte” da chiudere
2′ di lettura

Un piano in 82 punti per aumentare la resistenza dell’Italia contro il rischio cyber in continuo aumento e puntare alla “sovranità digitale”, facendo crescere professionalità e prodotti (software e hardware) “autoctoni”. È la Strategia nazionale di cybersicurezza 2022-2026 predisposta dall’Agenzia per la cybersicurezza nazionale e presentata oggi dall’Autorità delegata per la sicurezza della Repubblica, Franco Gabrielli e dal direttore dell’Agenzia, Roberto Baldoni.

## Le nuove risorse stanziate

Imponenti le risorse disponibili: l'1,2% degli investimenti nazionali lordi annui, al netto dei fondi europei e del Pnrr (623 milioni di euro). È un "cambio di passo", lo ha definito Gabrielli, che mira a colmare i ritardi accumulati dal Paese in questo settore e rispondere così a sfide destinate a crescere, come indicano anche i recenti attacchi che hanno colpito siti istituzionali – dal Senato alla Polizia – e che il sottosegretario ha comunque invitato a non enfatizzare. «Non serve – ha spiegato – un atteggiamento isterico. Se ogni volta che c'è un attacco 'Ddos' (Denial of service) pensiamo che il Paese è alla mercé di potenze straniere non si capisce il livello di minaccia».

## Gabrielli: 007 possono fare contrattacchi

Per Gabrielli è importante che «ciascuno faccia il suo». E la Strategia mette in chiaro le competenze di tutti i soggetti coinvolti, dai ministeri alle forze di polizia, dalla Difesa all'intelligence che, ha ricordato, «già oggi, a legislazione vigente, gode delle garanzie funzionali e può svolgere attività di contrattacco in campo cyber». Mentre l'Agenzia, ha puntualizzato Baldoni, «deve diventare il faro a cui tutti si dovranno interconnettere, ma la gestione degli attacchi non si delega all'Agenzia. Noi forniamo le misure, le linee guida, ma poi ognuno deve adottarle al suo interno. Nella cybersicurezza non si delega».

## Minaccia disinformazione on line

E per troppo tempo l'impegno dei soggetti sia pubblici che privati sul piano delle difese cyber è stato basso. Ne è nato

un deficit strutturale, infrastrutturale ed anche culturale che, hanno convenuto Gabrielli e Baldoni, «non possiamo più permetterci». La Strategia con il connesso Piano di implementazione mette così nero su bianco le misure che tutte le amministrazioni pubbliche devono attuare; al 31 dicembre l'Agenzia – che ha anche il potere di irrogare sanzioni agli inadempienti – valuterà se gli obiettivi sono stati raggiunti. Il documento prende anche in considerazione la minaccia della disinformazione on line che mira a «condizionare/influenzare processi politici, economici e sociali del Paese» e prevede «l'implementazione di un'azione di coordinamento nazionale» per prevenirla.

## Il capitolo dell'autonomia strategica

C'è infine il capitolo dell'autonomia strategica. L'Italia "consuma" prodotti digitali prodotti da altri Paesi e ciò la rende vulnerabile, come avviene per l'energia. È stata quindi avviato un percorso – che non sarà breve – per liberarsi da dipendenze "pericolose": l'esempio è quello degli antivirus russi Kaspersky, ad esempio. A questo scopo sarà creato un Parco nazionale della cybersicurezza e hub delocalizzati sull'intero territorio italiano. Si tratta, indica la Strategia, «di un incubatore di capacità e tecnologie, al cui

interno giovani talenti e startup possano entrare in contatto con le grandi aziende e con le diverse realtà nazionali che, a vario titolo, operano nel settore». Sostenendo lo sviluppo e la produzione di software e hardware nazionali da impiegare nelle reti e nei sistemi di maggiore rilevanza strategica.

Read More