A cura del team Public Affairs

RETI

Cybersicurezza: necessità urgente e fattore abilitante per la crescita

“Dobbiamo liberarci dalla dipendenza dalla tecnologia russa, [...] per esempio quella dai sistemi antivirus prodotti dai russi e utilizzati dalle nostre pubbliche amministrazioni che stiamo verificando e programmando di dismettere, per evitare che da strumento di protezione possano diventare strumento di attacco”. È quello che ha dichiarato in una recente intervista al Corriere della sera, **Franco Gabrielli**, sottosegretario alla Presidenza del Consiglio - Autorità Delegata per la Sicurezza della Repubblica.

Comunicazioni del Presidente Draghi in Parlamento e crisi in Ucraina

Le parole pronunciate da Gabrielli vanno inquadrate nel contesto più ampio delineato dal **Presidente Draghi** in Parlamento lo scorso 1° marzo. Nell’aggiornare il Parlamento sul conflitto in Ucraina, il premier ha sottolineato come il deterioramento delle relazioni tra la Russia e l’Unione Europea e la NATO abbia reso ancora più aggressiva rispetto al passato, **la postura di Mosca verso l’Occidente negli ambiti della cibernetica** e della disinformazione, con l’obiettivo di minarne la coesione e la capacità di risposta. È stata ricordata, quindi, l’attivazione di un “apposito **Nucleo per la Cybersicurezza** al fine di condividere le informazioni raccolte”, al cui interno è stato istituito un tavolo permanente dedicato alla crisi in atto.
Segnali circa rischi potenziali per l’acuirsi delle **attività malevole** nello spazio cibernetico in relazione alla situazione ucraina erano stati lanciati dal CSIRT (Computer Security Incident Response Team - Italia) insediato presso l'Agenzia per la cybersicurezza nazionale (ACN). Non si tratta di una novità se si considera che già nel 2016, in occasione del Vertice di Varsavia, la **NATO** aveva indicato il dominio cibernetico come ulteriore dominio di possibile conflitto rispetto a quelli tradizionali: cielo, terra, mare e spazio. Se a cavallo del Millennio le principali preoccupazioni relative alla sicurezza nazionale provenivano da soggetti statuali instabili o dal terrorismo internazionale, oggi queste preoccupazioni derivano sempre più frequentemente dall’ambito della **sicurezza informatica**. È per questo che nell’ambito della discussione generale sulla relazione annuale 2021 del Copasir di questa settimana, diversi parlamentari hanno auspicato l’approvazione di un provvedimento che ponga sullo stesso piano gli attacchi terroristici e quelli cyber.

Un quadro europeo e nazionale in evoluzione

Negli ultimi anni, infatti, il dominio cibernetico ha rappresentato in maniera crescente uno spazio privilegiato per attività ostili a danno di **target nazionali ed europei**, in primis pubblici e istituzionali, esposti a minacce per via della pervasività degli strumenti di comunicazione elettronica e di digitalizzazione delle informazioni e dei processi.
Una minaccia alla quale si è inteso rispondere a livello comunitario con la cosiddetta **Direttiva NIS** (*Network and Information Security*, 2016/1148) di cui è attualmente in discussione a Bruxelles l’aggiornamento (NIS 2). La Direttiva fu recepita nell'ordinamento italiano con il decreto legislativo n. 65 del 18 maggio 2018 che dettava la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individuava i soggetti competenti a dare attuazione alla Direttiva stessa. Nello specifico, al Presidente del Consiglio compete l'adozione, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), della **strategia nazionale di sicurezza cibernetica** per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale. Presso la Presidenza del Consiglio fu istituito, quindi, il **CSIRT**, quale "gruppo di intervento per la sicurezza informatica in caso di incidente". Punto di contatto unico, incaricato di coordinare le questioni relative

alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione Europea, venne quindi designato il **Dipartimento delle informazioni per la sicurezza** (DIS).

Su questa scia, nel 2019 il Governo Conte II ha approvato il DL recante Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (Decreto-legge 21 settembre 2019, n. 105), poi convertito dalla legge 133/2019. Obiettivo del provvedimento era assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un **perimetro di sicurezza nazionale cibernetica** e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi. Sono inclusi nel perimetro, in sostanza, soggetti (la lista è secretata ed aggiornata a cura della Presidenza del Consiglio) che a vario titolo operano nei seguenti **settori**: interno; difesa; spazio e aerospazio; energia; telecomunicazioni; economia e finanza; trasporti; servizi digitali; tecnologie critiche; enti previdenziali/lavoro. Settori elencati nel DPCM 30 luglio 2020, n. 131. Il DL 105/2019 ha previsto altresì l'emanazione di ulteriori decreti del Presidente del Consiglio e del Presidente della Repubblica volti a disciplinare e qualificare gli incidenti informatici, gli strumenti sottoposti ai controlli del perimetro, le azioni da intraprendere in caso di incidenti e gli standard qualitativi di sicurezza oggetto di certificazione da parte del Centro di Valutazione e Certificazione Nazionale (decreto, quest'ultimo, di prossima pubblicazione in Gazzetta Ufficiale).

Non ci si è fermati qui, tuttavia, poiché il Decreto-legge 14 giugno 2021, n. 82, approvato dal Governo Draghi, ha riformato la **governance del settore** modificando l'architettura istituzionale e, in particolare, istituendo la già citata **Agenzia per la cybersicurezza nazionale**. L'Agenzia ha assunto la gran parte delle competenze precedentemente attribuite ad altri organi, primi tra tutti il DIS, il Mise e l'AgID. Essa è posta sotto il controllo della Presidenza del Consiglio, ed è al Presidente del Consiglio, infatti, che spetta la nomina del direttore e del vicedirettore. L'ACN inoltre, gode di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. Al Presidente del Consiglio sono attribuite in via esclusiva l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, l'adozione della strategia nazionale di cybersicurezza, mentre le altre competenze possono essere svolte dall'Autorità Delegata per la Sicurezza della Repubblica (oggi il sottosegretario Gabrielli). Il Presidente Draghi, lo scorso 5 agosto 2021 ha nominato Direttore Generale dell'ACN il Professor **Roberto Baldoni**, già Vice Direttore del DIS, mentre il mese successivo ha nominato Vice Direttore la Dottoressa **Nunzia Ciardi**, già a capo del Servizio Polizia Postale e delle Comunicazioni.

La mission dell'Agenzia è quella di "assicurare la prosperità economica e la sicurezza del Paese nel contesto della trasformazione digitale, attraverso un processo multidimensionale di gestione del rischio cibernetico e di quello tecnologico, lavorando per prevenire e mitigare il maggior numero di attacchi cibernetici, e per diminuire la **dipendenza nazionale da tecnologia extra UE**". Un aspetto. quest'ultimo, che può sostanziarsi, nell'immediato, proprio nella dismissione del sistema antivirus Kaspersky paventata da Gabrielli.

In linea con quanto fatto dalla **Commissione europea**, e in particolare dal Commissario per il Mercato Interno Thierry Breton, l'Italia prova insomma a mettere in pratica i principi di "**autonomia strategica - sovranità digitale**" che intendono svincolare il nostro ecosistema economico e tecnologico da soggetti considerati a rischio. Anche a Bruxelles, in questi giorni, e non a caso, è in discussione l'EU Chips Act, mentre è in procinto di essere lanciato lo European Cyber Resilience Act che complementa il Cybersecurity Act del 2019.

Il PNRR per una sicurezza cibernetica "valore" trasversale

Un ecosistema digitale sicuro è garanzia per il Paese quando ad essere in gioco sono gli asset strategici, ma è un elemento necessario - altresì - a tutela dei cittadini e della **prosperità del sistema economico** se consideriamo che la digitalizzazione aumenta nel complesso il livello di vulnerabilità della società da minacce cyber. La sicurezza cibernetica, per questa ragione, costituisce uno degli interventi previsti dal **Piano nazionale di ripresa e resilienza** (PNRR) trasmesso dal Governo alla Commissione europea nell'aprile del 2021.

Rafforzare l'ecosistema digitale nazionale potenziando i servizi di monitoraggio e gestione della minaccia cyber è l'obiettivo dell'investimento 1.5 ("*Cybersecurity*") della **prima Missione** del Piano di cui sono recentemente stati pubblicati i bandi (Servizio e Ristoro). Un obiettivo che si intende perseguire rafforzando in maniera significativa le capacità di alert, prevenzione e risposta a rischi ed eventi cyber grazie a una rete di servizi nazionali, integrata con i principali partner pubblici e privati.

È previsto lo sviluppo di un sistema all'avanguardia che interconnetta strettamente, a livello nazionale e internazionale, il mondo della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia. L'investimento si articola su **tre pilastri**: rafforzare la resilienza di sistema, favorendo sinergie e interconnessione delle capacità di monitoraggio, condivisione di informazioni e risposta agli eventi di natura cyber; rafforzare le capacità nazionali di scrutinio e certificazione tecnologica al fine di valutare e certificare beni, sistemi e servizi ICT; potenziare le capacità cyber della PA per la messa in sicurezza dei dati e dei servizi dei cittadini. Si tratta di quelli che il PNRR definisce "**interventi abilitanti**" per l'accessibilità, l'efficienza e la sicurezza dell'infrastruttura digitale.

Ma la cyber-sicurezza dovrebbe essere **trasversale** per lo meno a tutti i progetti della Missione 1, e non solo (la Missione 2 prevede la realizzazione di un sistema avanzato ed integrato di monitoraggio e previsione dei rischi conseguenza del cambiamento climatico o di innovazione digitale dei sistemi aeroportuali). Proprio in ragione della diffusione capillare degli strumenti digitali, e della vulnerabilità che ne consegue, potrebbe essere opportuno oggi **integrare i contratti e i bandi pubblici** con specifiche "**clausole cyber**". Esempi pratici sarebbero: misure volte a disporre che, analogamente a quanto previsto in relazione agli oneri per la sicurezza per i contratti aventi per oggetto i lavori, siano **esplicitati gli oneri per la cybersicurezza** in quelli aventi per oggetto forniture di beni e servizi in ambito digitale; l'individuazione, secondo criteri di adeguatezza, proporzionalità e ragionevolezza, di una soglia minima atta a garantire che le soluzioni di cybersicurezza siano idonee ad assicurare la protezione dei dati nell'ambito del bene o servizio ICT oggetto del contratto o del bando.

Criticità e sfide per il sistema Paese

La sicurezza cibernetica è sì una sfida da affrontare nell'immediato, a maggior ragione alla luce del contesto globale e delle dichiarazioni riportate in premessa, ma è un tema che impone anche riflessioni sul medio-lungo periodo in riferimento alle considerazioni svolte sulle **ricadute positive per il sistema Paese**.

i. Competenze

Perché, però, la sfida possa essere vinta risultano imprescindibili alcuni elementi. È fondamentale, in primis, che le Pubbliche Amministrazioni e le imprese si dotino di adeguate **competenze**. Per le imprese tecnologie attive in Italia la mancanza di competenze IT rappresenta, infatti, un fattore di grande preoccupazione e comporta una grave perdita di potenziali ricavi. La carenza di competenze è una lacuna cui negli ultimi anni si è cercato di porre rimedio mediante strumenti normativi e non,

come **Repubblica Digitale** e il cosiddetto **Fondo nuove competenze** (di cui all'articolo 88, comma 1, del D.L. 34/2020) istituito nel 2020 e recentemente modificato, prima con il D.L. 146/2021 (c.d. Decreto Fiscale) e poi con il Decreto-legge 1 marzo 2022, n. 17 (DL recante misure urgenti per il contenimento dei costi dell'energia elettrica e del gas naturale, per lo sviluppo delle energie rinnovabili e per il rilancio delle politiche industriali). Quest'ultima disposizione amplia l'ambito di interventi di riqualificazione e adeguamento strutturale delle competenze dei lavoratori finanziabili con il Fondo, che viene esteso a coloro che abbiano sottoscritto accordi di sviluppo per progetti di investimento strategico ovvero siano ricorsi al Fondo per il sostegno alla transizione industriale. E poi il Credito d'imposta formazione 4.0, che si rivolge, tra le altre, alle attività formative su big data e analisi dei dati, cloud e fog computing, cybersecurity, simulazione e sistemi cyber-fisici.

ii. Salari

Il **costo del lavoro** dei professionisti cyber rischia di incidere negativamente in maniera determinante sulle prospettive di crescita settoriali e nazionali. Basti pensare che, da un lato, l'Italia vede partire ogni anno migliaia di talenti e, dall'altro, la forza attrattiva del nostro Paese risulta limitata da salari relativamente bassi. Il Governo è chiamato a realizzare un **regime salariale speciale** per i professionisti della cyber-security al fine di aumentare l'appetibilità italiana. Diversi commentatori hanno sollevato dubbi sulla proposta di elevare gli stipendi per particolari fasce di lavoratori, essendo loro meglio retribuiti della media nazionale, ma va assolutamente sottolineato che la peculiarità del lavoro che essi svolgono comporta **benefici sistemici rilevanti** che si riverberano altresì nel contesto della **sicurezza nazionale**.

iii. Il Modello Pubblico-Privato

Il Decreto-legge 14 giugno 2021, n. 82 prevede tra le funzioni dell'Agenzia per la Cybersicurezza Nazionale che questa possa costituire e partecipare a **partenariati pubblico-privati** sul territorio nazionale e - previa autorizzazione del Presidente del Consiglio dei ministri - a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri. Inoltre, l'ACN può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore. Per l'**ecosistema economico digitale italiano** queste facoltà dell'Agenzia rappresentano un elemento di grande interesse nell'ottica di propiziare **crescita e benefici diffusi per il settore** attraverso la leva pubblica, anche e soprattutto nel contesto del PNRR.

iv. Cyber Start-Up

Sebbene vi siano alcune interessanti eccezioni come Swascan, Kopjra e Exein, l'ecosistema delle start-up nel settore della sicurezza informatica in Italia mostra evidenti segni di difficoltà rispetto ad altri ambiti tecnologici. Le start-up cyber, infatti, necessitano di **grandi investimenti** economici per poter muovere i primi passi e vivono in questo modo un percorso di gestazione del tutto *sui generis*. Per creare il primo "**unicorno**" italiano della cybersecurity sarebbe dunque condizione necessaria, ma non sufficiente, la costituzione di Fondi di Venture Capital esplicitamente rivolti alla sicurezza del web, in linea con il progetto Cysero di AVM Gestioni che ha recentemente ricevuto un investimento da 20 milioni di euro da Cdp Venture Capital Sgr.