Presidenza

del Consiglio dei Ministri

IL MINISTRO PER LA PUBBLICA AMMINISTRAZIONE

QUESTION TIME

Interrogazione a risposta immediata in Assemblea d'iniziativa
dell'On. Felice Maurizio D'ETTORE (CI)

On. Prof. Renato Brunetta
Ministro per la Pubblica amministrazione

Camera dei deputati, 1 giugno 2022

L'Onorevole interrogante si rivolge al Ministro per la pubblica amministrazione per sapere, con riguardo alle minacce hacker ai sistemi informatici istituzionali e, in particolare, con riguardo ai temi della formazione del personale, quali iniziative di competenza intenda intraprendere per far fronte al pericolo degli attacchi hacker per scongiurare il pericolo di una paralisi informatica e della sottrazione di dati sensibili per quanto riguarda le pubbliche amministrazioni.

Signor Presidente, Onorevoli Deputati,

in relazione al quesito posto dall'On.le interrogante evidenzio innanzitutto alcuni elementi tecnici acquisiti dall'Agenzia per la Cybersicurezza Nazionale, ricordando che in tale materia le competenze della Presidenza del Consiglio dei Ministri coinvolgono diversi attori (l'Agenzia, il Dipartimento del Ministro Colao, il Dipartimento della funzione pubblica per quanto riguarda la formazione del personale), che agiscono sotto l'egida di Palazzo Chigi.

La recente minaccia del gruppo di Hacker russi Killnet, di infliggere un "colpo irreparabile" all'Italia con l'obiettivo di paralizzarne i server, ci ricorda quanto sia urgente affrontare il tema della sicurezza cibernetica, contrastando ogni minaccia al Paese con tutti gli strumenti della politica, dalla formazione al *capacity building*.

L'attacco perpetrato proprio ieri da Killnet ai danni del sito istituzionale dello CSIRT Italia – il *Computer Security Incidente Response Team* – istituito presso l'Agenzia per la Cybersicurezza Nazionale è stato mitigato dai sistemi di protezione del portale, e non ha intaccato la disponibilità del sito web per gli utenti.

Questo evento ci evidenzia come sia necessario:

1. **dotare tutte le istituzioni - a tutti i livelli di Governo - delle capacità e delle competenze per riconoscere i rischi connessi alla sicurezza cibernetica;**
2. **regolamentare le attività dello spazio cibernetico nell'ambito di uno strettissimo coordinamento europeo e internazionale.**

Proprio per questo, il 23 maggio scorso il Consiglio UE ha definito in un documento ambizioso nuovi meccanismi di gestione delle crisi e di risposta comune alle minacce, esercitazioni congiunte, ma anche un ambito comune di cyberspazio.

Come evidenziato dall'onorevole interrogante, dall'11 maggio scorso sono stati osservati attacchi verso numerosi portali di Pubbliche Amministrazioni ed operatori privati tesi ad interrompere la fruizione dei servizi da essi erogati.

Sotto il profilo tecnico tali eventi – come quello di ieri - ricadono nella famiglia dei *Distributed Denial of Service (DDoS)*, ovvero attacchi effettuati attraverso l'utilizzo di sorgenti multiple distribuite che tendono a colpire i servizi esposti su Internet, impedendone la fruibilità.

Gli attacchi che hanno interessato il settore sanitario, invece, sono stati caratterizzati dall'utilizzo di *malware* – ovvero da programmi informatici usati per disturbare le operazioni svolte da un utente di un computer - che hanno compromesso le reti informatiche permettendo agli attaccanti di accedere a sistemi di varia natura, anche cifrandoli.

Rispetto ai rischi a cui è esposto il settore sanitario, l'Agenzia per la Cybersicurezza nei mesi di settembre ed ottobre 2021 ha effettuato una campagna di sensibilizzazione, attraverso una serie di seminari tematici, indirizzata alle strutture sanitarie di tutte le Regioni. Inoltre, in occasione di alcuni attacchi a strutture sanitarie (come, ad esempio, gli ospedali Sacco e Fatebenefratelli di Milano) il personale dell'Agenzia è intervenuto in loco a supporto per le attività di contenimento, analisi dell'attacco e ripristino dei servizi essenziali.

Lo scorso 17 maggio il Presidente del Consiglio dei Ministri, sentito il Comitato interministeriale per la cybersicurezza (CIC), ha adottato la **Strategia nazionale di cybersicurezza**, comprensiva del **Piano di implementazione** (contenente 82 misure).

In tale strategia, si segnala che la transizione verso tecnologie *Cloud* della PA (siano esse del Polo Strategico Nazionale - PSN o del Public Cloud) rappresenta un elemento fondante per garantire adeguate garanzie di autonomia tecnologica del Paese.

A questo si accompagna lo sviluppo di capacità di protezione per le infrastrutture nazionali, realizzate anche mediante programmi con i privati, e attraverso soluzioni tecnologiche finalizzate a ridurre in modo proattivo potenziali superfici di attacco, nonché attraverso il monitoraggio delle configurazioni dei domini di posta elettronica della PA, supportando e facilitando l'applicazione delle migliori configurazioni di sicurezza contro eventi di *phishing* o abusi collegati.

Occorre, infine, evidenziare – e vengo alla materia di mia più stretta competenza - come nelle pubbliche amministrazioni uno dei temi centrali sia quello dell'acquisizione di competenze e profili professionali specializzati da reclutare.

In questo quadro e nell'ottica del PNRR, il Dipartimento della funzione pubblica, di concerto con il Ministero dell'economia e delle finanze, sta elaborando specifiche Linee Guida per la definizione, da parte della contrattazione collettiva, di nuovi e aggiornati profili professionali, che comprenderanno anche quelli necessari ad implementare la capacità di risposta delle pubbliche amministrazioni a queste nuove e temibili sfide.

Inoltre, la possibilità di accedere ai fondi PNRR costituirà sicuramente una efficace risposta alle problematiche richiamate. In particolare, la Cybersecurity è uno dei 7 investimenti della Digitalizzazione della PA (componente M1C1) al quale sono destinati circa 620 milioni di euro di cui 241 per la creazione di una infrastruttura per la cybersicurezza; 231 per il rafforzamento delle principali strutture operative del perimetro di sicurezza nazionale cibernetica (PNSC); 15 per il rafforzamento delle capacità nazionali di difesa informatica del Ministero dell'Interno, della Difesa, della Guardia di Finanza, del Ministero della Giustizia e del Consiglio di Stato.

Per quanto riguarda più specificamente la formazione del personale, invece, con l'Agenzia per la cybersicurezza nazionale, con la SNA, in collaborazione con il Dipartimento della funzione pubblica, è nato il progetto denominato "*Summer school cyber security*".

L'iniziativa nasce dall'esigenza di organizzare attività di formazione intensiva per fornire competenze approfondite sui temi della *cyber security* ai vertici delle pubbliche amministrazioni, attraverso la condivisone e il confronto con esperti del settore.

Nella sede della SNA a partire da luglio 2022 verranno svolti moduli formativi, replicabili sul territorio e ripetuti nel tempo, di durata variabile in funzione del ruolo ricoperto.

Anche al fine di garantire il massimo livello di interazione e approfondimento il percorso di formazione coinvolgerà un numero limitato di partecipanti per ogni sessione individuati d'intesa con le amministrazioni pubbliche interessate.