Ministero della Giustizia

INTERROGAZIONE A RISPOSTA SCRITTA N. 4-03642 DEL DEP. DORI (res. n. 368 del 18 ottobre 2024)

R I S P O S T A

Con riferimento all'atto di sindacato ispettivo in oggetto, con cui il deputato interrogante, traendo spunto dall'inchiesta su Carmelo Miano, *l'hacher* arrestato dalla Polizia postale al termine di indagini coordinate dalla procura di Napoli in relazione alle "effrazioni" alla rete informatica del Ministero della Giustizia, solleva specifici quesiti in ordine alle iniziative, anche normative, volte a "*contrastare i cybercrimini"* e a *"a rafforzare tra l'altro, i poteri di coordinamento della Procura nazionale antimafia e antiterrorismo a partire dalla tutela dei sistemi interni, con il coinvolgimento anche dell'Agenzia per la cybersicurezza Nazionale di recente istituzione",* si rappresenta quanto segue.

Sulla specifica vicenda giudiziaria, con note del 5 novembre 2024 e del 15 maggio 2025, il Procuratore della Repubblica presso il Tribunale di Napoli, opportunamente interpellato dalla competente articolazione ministeriale, ha trasmesso dettagliate relazioni che, per completezza di esposizione, si riportano integralmente di seguito.

"L'indagine ha avuto ad oggetto un vasto attacco informatico ai danni di infrastrutture critiche, tra cui il Ministero della Giustizia. L'attività investigativa ha avuto origine nel giugno 2023, allorché i responsabili dei sistemi Giustizia notavano un'attività anomala su computer di un distretto giudiziario siciliano (Gela): un virus informatico che consentiva l'apprensione di dati riservati ed il suo invio verso un server centrale sito a Napoli, a scopo di successiva

esfiltrazione. L'analisi a più ampio spettro, condotta con l'ausilio tecnologico degli esperti informatici del CINI (Consorzio Interuniversitario per l'informatica), cui il Ministero della Giustizia aveva affidato i primi accertamenti tecnici, rilevava la compromissione di numerosi PC e Server della rete Giustizia, oltre che di utenze dotate di altissimi privilegi di amministratore di sistema. […]. L'hacker, grazie alle sue non comuni capacità, si avvaleva di sofisticati e capillari software malevoli che consentivano la lettura dei dati delle macchine attaccate (comprese le password inserite e i programmi in esecuzione), che venivano prelevati, raccolti sul server centrale di Napoli ed infine esfiltrati verso l'esterno, cancellando ogni traccia. L'attaccante ostile veniva identificato in M. C.[…].".

"[…] All'esito dell'arresto di M. C., avvenuto in data 1.10.2024, sono state avviate - e sono tuttora in corso con la collaborazione del CNA1PIC del Servizio Centrale Polizia Postale e del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza — complesse analisi di ricostruzione informatica del copioso materiale sequestrato nel corso delle perquisizioni; […] questo Ufficio di Procura ha ulteriormente proseguito, con il coordinamento della D.N.A., le assidue attività di interlocuzione con l'A.C.N. e con la DGSIA, per il raccordo sulla completa attuazione del già programmato piano di remediation, in conformità con la disciplina introdotta con la L.90/24, ai fini della totale eradicazione dell'attaccante ostile dal perimetro della RUG; Si evidenzia, in ogni caso, che successivamente all'arresto del M., le indagini in corso non hanno fatto emergere ulteriori tracce di attività intrusive o di esfiltrazione riconducibili ad ulteriori attori ostili; […]".

L'episodio ha rappresentato l'unica minaccia significativa alla sicurezza del sistema Giustizia, arginata con tempestività dall'Amministrazione grazie alle incisive misure adottate sin dall'insediamento del Governo, come già rappresentato in occasione del *question time* del 30 ottobre 2024 alla Camera dei deputati.

Infatti, sono state avviate, a far data dalla metà del 2023, misure organizzative, quali l'istituzione di apposito Ufficio sicurezza informatica, ed attivate strette interlocuzioni con l'Agenzia per la Cybersicurezza Nazionale (ACN) nell'ambito

delle misure di implementazione della strategia di cybersicurezza nazionale da questa gestita, al fine di colmare le vulnerabilità, infrastrutturali e organizzative presenti nella rete informatica del Ministero.

Inoltre, in attuazione della legge n. 137 del 2023, sono stati estesi i poteri di impulso e coordinamento del Procuratore Nazionale Antimafia e Antiterrorismo anche con riferimento ai più gravi reati informatici, e sono state ampliate le funzioni dell'Agenzia per la Cybersicurezza Nazionale al fine di incrementare le capacità nazionali di prevenzione e di gestione degli incidenti e degli attacchi informatici.

In tale ottica il Ministero ha avviato una ancora più forte collaborazione con l'Agenzia ACN con cui è stato definito, ed attuato a partire da inizio 2024, un piano di intervento operativo sui sistemi informativi del Ministero finalizzato a ridurre il rischio cyber e migliorare la sicurezza complessiva degli asset e la protezione dei dati del Ministero.

Le iniziative intraprese, sono state progettate in accordo al Framework Nazionale per la Cybersecurity, nato appositamente per supportare la protezione dei dati personali e la gestione della sicurezza cibernetica delle amministrazioni. In particolare, il Ministero della Giustizia ha:

• implementato soluzioni di rafforzamento, controllo e monitoraggio della gestione delle identità e degli accessi ai servizi e ai dati dell'Amministrazione. Questo anche introducendo meccanismi di autenticazione a più fattori degli utenti;

• adottato strumenti avanzati per monitorare e analizzare il perimetro e gli asset dell'Amministrazione, migliorando così la capacità di individuare rapidamente vulnerabilità e potenziali minacce. Questo grazie anche all'installazione di agenti dedicati sull'intera infrastruttura dell'Amministrazione costituita da oltre 120.000 computer personali e macchine server distribuite in tutti gli uffici giudiziari dell'intero territorio nazionale;

• potenziato le soluzioni di difesa perimetrale, tramite l'impiego di sistemi di prevenzione delle intrusioni per ridurre l'esposizione ai rischi. In tal modo è ora possibile l'individuazione, in tempo reale, di attività sospette e l'analisi di

comportamenti anomali (quali accessi fuori orario di lavoro e/o da postazioni anomale o da particolari luoghi geografici quali stati esteri, ecc..);

• incrementato la capacità di risposta agli incidenti, rendono ora possibile una reazione più rapida, efficace e capillare in caso di attacchi, minimizzando l'impatto delle minacce;

• definito e applicato le procedure di recupero per garantire la continuità operativa ed il ripristino rapido dei servizi in caso di incidente mediante piani di risposta che prevedono l'isolamento immediato dei sistemi compromessi e l'attivazione di contromisure per contenere la diffusione degli attacchi;

• attivato in particolare un servizio di Security Operation Center (SOC) con il monitoraggio H24 degli allarmi provenienti dai sistemi di monitoraggio continuo installati sui sistemi ministeriali.

Dal gennaio 2024 ACN ha avviato un piano di eradicazione finalizzato a ristabilire il pieno controllo sull'infrastruttura ICT del Ministero comprendente un reset completo dei profili di amministratore di sistema.

La manovra si è conclusa all'inizio del mese di ottobre 2024.

Gli strumenti di monitoraggio così implementati non hanno evidenziato ulteriori accessi abusivi o trasferimento di dati sensibili né tantomeno la pubblicazione di informazioni della rete Giustizia nei circuiti del dark web. Le segnalazioni pervenute sono relative a vecchi dati e credenziali obsolete e non più attive.

Si proseguirà in questa direzione a tutela della protezione dei dati trattati.

Il Ministro
Carlo Nordio

Testo dell'interrogazione