Senato della Repubblica

XIX LEGISLATURA

N. 1441

DISEGNO DI LEGGE

d'iniziativa del senatore BASSO

COMUNICATO ALLA PRESIDENZA IL 3 APRILE 2025

Delega al Governo per la definizione di una strategia nazionale per il contrasto degli attacchi informatici a scopo di estorsione

ONOREVOLI SENATRICI E SENATORI. – Negli ultimi anni, l'Italia ha affrontato una crescita esponenziale delle minacce cibernetiche, con un aumento del 12 per cento degli attacchi informatici nel 2023 rispetto all'anno precedente. Di questi, il 69 per cento è attribuibile a attività cybercriminali, con il *ransomware* che rappresenta una delle principali minacce. Il costo medio di un attacco per un'azienda italiana è stimato intorno ai 200.000 euro, mentre solo il 34 per cento delle aziende ha implementato un piano di risposta agli incidenti informatici.

A livello internazionale, il panorama geopolitico ha ulteriormente complicato lo scenario della *cybersecurity*. L'Italia, pur rappresentando solo l'1,8 per cento del PIL mondiale, è stata bersaglio del 10 per cento degli attacchi informatici globali, evidenziando una sproporzione significativa che sottolinea la vulnerabilità del Paese.

Inoltre, l'emergere di gruppi *hacker* filorussi, come *NoName*057(16), ha portato a una serie di attacchi contro siti istituzionali e aziende italiane, spesso in risposta a posizioni politiche assunte dall'Italia nel contesto internazionale. Ad esempio, nel febbraio 2025, questo gruppo ha rivendicato attacchi a siti governativi italiani in seguito a dichiarazioni del Presidente della Repubblica.

Alla luce di questo contesto preoccupante, il presente disegno di legge si pone l'obiettivo di rafforzare la resilienza nazionale contro gli attacchi *ransomware* attraverso una serie di misure articolate:

a) divieto di pagamento del riscatto: si introduce il divieto per i soggetti pubblici e privati inclusi nel Perimetro di Sicurezza Nazionale Cibernetica di pagare riscatti a seguito di attacchi *ransomware*. In casi di grave rischio per la sicurezza nazionale, il Presidente del Consiglio dei ministri può autorizzare deroghe specifiche;

b) qualificazione dell'attacco come minaccia alla sicurezza nazionale: si attribuisce al Presidente del Consiglio dei ministri la facoltà di classificare un attacco *ransomware* come incidente che compromette la sicurezza nazionale, attivando le relative misure di *intelligence*;

c) attività sotto copertura estese all'estero: si estende la possibilità per le Forze dell'ordine di svolgere attività sotto copertura anche su reti e sistemi informatici situati al di fuori del territorio nazionale, per contrastare reati informatici transnazionali;

d) obbligo di notifica tempestiva: si impone a tutti i soggetti pubblici e privati l'obbligo di notificare al CSIRT *(Computer Security Incident Response Team*) Italia eventuali attacchi *ransomware* entro sei ore dalla loro conoscenza, pena sanzioni amministrative proporzionate;

e) Piano operativo di supporto: si incarica l'Agenzia per la cybersicurezza nazionale di predisporre un piano di azione concreto a sostegno dei soggetti colpiti da attacchi *ransomware*, fornendo assistenza tecnica e strategica;

f) istituzione di una *task-force* nazionale: si crea una *task-force* permanente presso il CSIRT Italia dedicata al contrasto degli attacchi *ransomware*, con funzioni di coordinamento e supporto operativo;

g) incentivi economici e fondo nazionale: si prevede l'introduzione di incentivi economici per l'Agenzia per la cybersicu-

rezza nazionale e la creazione di un Fondo nazionale di risposta agli attacchi *ransomware*, destinato a supportare i soggetti colpiti nel ristoro delle perdite economiche subite;

h) formazione obbligatoria e incentivi per le piccole e medie imprese: si introduce l'obbligo di formazione annuale in materia di cybersicurezza per i dipendenti pubblici e si prevedono incentivi fiscali per la formazione nelle piccole e medie imprese (PMI), al fine di accrescere la consapevolezza e le capacità di prevenzione degli attacchi *ransomware*;

i) cyber-assicurazioni: si incentivano la sottoscrizione di polizze assicurative contro i rischi informatici, in particolare per le PMI, come strumento di resilienza economica e gestione del rischio;

l) requisiti minimi di cybersicurezza: si stabiliscono requisiti minimi obbligatori di cybersicurezza (come l'uso di autenticazione multifattore, *backup* regolari, sistemi *antivirus* aggiornati) per poter accedere ai benefici previsti dal Fondo nazionale di risposta agli attacchi *ransomware*.

m) coordinamento con normative europee: si prevede un esplicito coordinamento e integrazione con la normativa europea vigente in materia di cybersicurezza, tra cui la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, e il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, cosiddetto « regolamento DORA », per assicurare coerenza normativa e massimizzare l'efficacia delle misure adottate.

n) collaborazione attiva con le autorità: si estendono i benefici del Fondo nazionale di risposta anche ai soggetti che, pur non avendo rispettato completamente i criteri tecnici previsti, abbiano comunque collaborato attivamente con le autorità competenti fornendo elementi utili alle indagini;

m) misure contro *ransomware-as-a-service* (RaaS): si introducono sanzioni specifiche per coloro che sviluppano, distribuiscono o facilitano l'uso di piattaforme *ransomware-as-a-service*, anche quando non direttamente coinvolti in attacchi specifici;

n) audit post-incidente: si prevede l'obbligo, per i soggetti pubblici e privati colpiti da attacco *ransomware*, di effettuare un *audit* post-incidente, con analisi delle vulnerabilità sfruttate, delle misure adottate e dei tempi di recupero, e trasmissione di un *report* finale all'Agenzia per la cybersicurezza nazionale, al fine di contribuire al rafforzamento sistemico della resilienza del Paese.

Il presente disegno di legge rappresenta una risposta organica, tempestiva e lungimirante a una delle minacce più insidiose della nostra epoca digitale. Il fenomeno degli attacchi *ransomware* non è più solo una questione tecnica, ma un fattore strutturale che può mettere in crisi la continuità operativa di imprese, pubbliche amministrazioni e infrastrutture critiche, con ripercussioni economiche, sociali e geopolitiche.

Attraverso il rafforzamento delle capacità di prevenzione, la promozione della cultura della sicurezza informatica, la tempestività nella risposta agli incidenti, e l'istituzione di strumenti di sostegno concreto alle vittime, il disegno di legge si propone di colmare le attuali lacune normative e operative, in piena coerenza con gli indirizzi europei e con il principio di sicurezza nazionale partecipata.

Con queste misure, l'Italia può dotarsi non solo di una normativa aggiornata, ma anche di una strategia che mette al centro la responsabilità condivisa tra istituzioni, imprese e cittadini nel contrasto al crimine informatico.

DISEGNO DI LEGGE

Art. 1.

1. Entro sei mesi dalla data di entrata in vigore della presente legge, il Governo è delegato ad adottare uno o più decreti legislativi per la definizione di una strategia nazionale per il contrasto agli attacchi informatici a scopo di estorsione di tipo *ransomware*, nel rispetto dei seguenti princìpi e criteri direttivi:

a) previsione di un divieto di pagamento di un riscatto a seguito delle condotte di cui all'articolo 629, comma 3, del codice penale per i soggetti pubblici e privati di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133. La violazione di tale divieto comporta una sanzione amministrativa commisurata alla violazione. Tale divieto può essere derogato attraverso una specifica determinazione del Presidente del Consiglio dei ministri in presenza di un rischio grave ed imminente per la sicurezza nazionale connesso all'attacco *ransomware*;

b) introduzione di una previsione che specifichi che l'attacco *ransomware* condotto contro e che generi effetti su soggetti pubblici e privati di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, possa essere qualificato, indipendentemente dal soggetto agente, come un incidente o una compromissione che comporta un pregiudizio per la sicurezza nazionale, così come definiti rispettivamente nell'articolo 1, comma 1, lettere *h)*, *g)* e *f)*, del regolamento di cui al decreto del Presidente del Consiglio dei mini-

stri 30 luglio 2020, n. 131. Tale qualificazione è effettuata dal Presidente del Consiglio dei ministri, ai sensi dell'articolo 2, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

c) nel caso di cui alla lettera *b)*, attribuzione al Presidente del Consiglio dei ministri del potere di decidere l'eventuale applicazione delle misure di *intelligence* di contrasto in ambito cibernetico previste dall'articolo 7-*ter* del decreto-legge del 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, e dai relativi decreti attuativi, anche quando ci si trovi in situazioni di crisi o emergenza che siano fronteggiabili solo con azioni di resilienza;

d) introduzione di una disposizione che preveda che gli ufficiali di polizia giudiziaria delle Forze dell'ordine possano svolgere le attività sotto copertura di cui all'articolo 9, comma 1, lettera *b)-ter,* della legge 16 marzo 2006, n. 146, anche su reti, sistemi informativi e servizi informatici utilizzati per compiere reati informatici posti al di fuori dei confini nazionali;

e) previsione di un obbligo di notifica in capo a qualsivoglia soggetto pubblico e privato che subisca un attacco *ransomware*, ad esclusione dei casi in cui gli effetti dell'attacco siano bloccati dalle misure di sicurezza della vittima prima dell'esecuzione del *ransomware* stesso. Tale notifica deve essere effettuata al CSIRT Italia entro sei ore dal momento in cui il soggetto ne sia venuto a conoscenza, pena una sanzione amministrativa commisurata alla violazione. Il CSIRT Italia deve provvedere tempestivamente a trasmettere tale notifica all'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, nonché, se pertinente e secondo le ri-

spettive attribuzioni di vigilanza, alle autorità competenti previste regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, previste dall'articolo 3, comma 1, del decreto legislativo 10 marzo 2025, n. 23. Il CSIRT Italia deve provvedere, altresì, a trasmettere tempestivamente tale notifica agli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124, per le loro finalità istituzionali e, ove rilevanti per la difesa dello Stato, al Ministero della difesa, in qualità di Autorità nazionale di gestione delle crisi informatiche ai sensi dell'articolo 13 del decreto legislativo 4 settembre 2024. L'adempimento dell'obbligo di notifica dell'attacco *ransomware* deve lasciare impregiudicati eventuali ulteriori obblighi di notifica di incidenti informatici già previsti all'interno delle altre normative vigenti;

f) introduzione di una disposizione che preveda che l'Agenzia per la cybersicurezza nazionale predisponga un piano di azione a concreto sostegno dei soggetti pubblici e privati colpiti da un attacco *ransomware*, con un *focus* particolare anche per le pubbliche amministrazioni locali e le piccole e medie imprese, il quale preveda almeno il supporto operativo nelle fasi di gestione degli attacchi *ransomware*, contenimento dei loro effetti, recupero dell'operatività delle reti, dei sistemi informativi e dei servizi informatici colpiti e valutazione delle alternative all'eventuale pagamento del riscatto. Il piano di azione deve indicare anche le buone prassi e le misure di sicurezza informatica preventive a cui i soggetti pubblici e privati possono fare riferimento per mitigare il rischio di essere colpiti da un attacco *ransomware*;

g) istituzione di una *task-force* nazionale per il contrasto agli attacchi *ransomware*, collocata nel CSIRT Italia, che svolga il ruolo di:

1) coordinamento delle attività di cui alla lettera *f)*;

2) attuazione di quanto previsto alla lettera *f)*;

3) punto di riferimento e contatto unico per i soggetti pubblici e privati colpiti da un attacco *ransomware* durante la gestione dell'emergenza;

4) punto di riferimento unico per la raccolta, analisi e condivisione delle informazioni per la resilienza agli attacchi *ransomware*, sia a livello nazionale che internazionale. La *task-force* del CSIRT Italia, nell'attuazione di quanto previsto alla lettera *f)*, è integrata con i soggetti di cui alla lettera *e)* destinatari della notifica dell'attacco *ransomware* dal CSIRT Italia;

h) introduzione di incentivi sul piano economico in favore dell'Agenzia per la cybersicurezza nazionale per la realizzazione delle attività di cui alle lettere *f)* e *g)*;

i) creazione di un « Fondo nazionale di risposta agli attacchi *ransomware* » per supportare i soggetti pubblici e privati nel ristoro, anche solo parziale, delle perdite economiche subite a seguito di un attacco *ransomware*, anche al fine di disincentivare il pagamento del riscatto. Prevedere, inoltre, che possano fare richiesta di ristoro economico al Fondo solo quei soggetti pubblici e privati che abbiano effettuato la notifica di cui alla lettera *e)* nei termini e secondo le modalità ivi previste e di aver applicato quanto previsto nel piano di azione di cui alla lettera *f)*;

l) previsione di un obbligo di formazione annuale in materia di cybersicurezza per i dipendenti pubblici, con l'introduzione di incentivi fiscali a favore delle piccole e medie imprese che investano nella formazione del personale, al fine di rafforzare la consapevolezza e le capacità di prevenzione degli attacchi *ransomware*;

m) introduzione di incentivi economici e fiscali per la sottoscrizione di polizze assicurative contro i rischi informatici cosiddette « cyber-assicurazioni », in particolare a

beneficio delle piccole e medie imprese, come strumento di resilienza finanziaria e di gestione del rischio cibernetico;

l) definizione di requisiti minimi obbligatori di cybersicurezza, tra cui l'adozione di autenticazione a più fattori, sistemi di *backup* aggiornati, *antivirus* e aggiornamenti regolari, quale condizione necessaria per l'accesso ai benefici previsti dal Fondo nazionale di risposta agli attacchi *ransomware*;

m) esplicita previsione di coordinamento e integrazione con la normativa europea vigente in materia di cybersicurezza, incluse la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022 e il citato regolamento (UE) 2022/2554, al fine di assicurare coerenza normativa ed evitare duplicazioni o conflitti tra discipline;

n) estensione dell'accesso al Fondo nazionale di risposta agli attacchi *ransomware* anche ai soggetti che, pur non avendo soddisfatto integralmente i requisiti di cui alle lettere precedenti, abbiano dimostrato collaborazione attiva con le autorità competenti fornendo informazioni rilevanti ai fini investigativi o di prevenzione;

o) introduzione di sanzioni specifiche e autonome nei confronti di soggetti che sviluppano, distribuiscono, promuovono o facilitano piattaforme di *ransomware-as-a-service* (RaaS), anche in assenza di un loro diretto coinvolgimento negli attacchi;

p) previsione dell'obbligo, in capo ai soggetti pubblici e privati colpiti da attacco *ransomware*, di effettuare un *audit* post-incidente, comprendente l'analisi tecnica dell'attacco, la valutazione delle vulnerabilità sfruttate, la descrizione delle contromisure adottate e il tempo di recupero, con trasmissione del relativo rapporto all'Agenzia per la cybersicurezza nazionale;

q) introduzione di una disciplina di protezione giuridica, cosiddetto « *safe harbor* »,

per i soggetti che, in buona fede, segnalino vulnerabilità informatiche rilevanti ai sensi delle procedure di divulgazione responsabile, al fine di incentivare il contributo della società civile alla sicurezza del sistema informatico nazionale.

2. Gli schemi dei decreti legislativi di cui al comma 1 sono adottati su proposta del presidente del Consiglio dei ministri e del Ministro dell'interno, sentita l'Agenzia per la cybersicurezza nazionale, e sono successivamente trasmessi alle Camere per l'espressione del parere delle Commissioni parlamentari competenti per materia e per i profili finanziari. Decorsi sessanta giorni dalla data della trasmissione, i decreti possono essere emanati anche in mancanza dei pareri. Qualora detto termine scada nei trenta giorni antecedenti la scadenza del termine previsto per l'esercizio della delega o successivamente, quest'ultimo è prorogato di sessanta giorni. Entro i trenta giorni successivi all'espressione dei pareri, il Governo, ove non intenda conformarsi ai pareri parlamentari, ritrasmette i testi alle Camere, corredati dei necessari elementi integrativi di informazione, per l'espressione dei pareri definitivi da parte delle Commissioni parlamentari competenti, che sono espressi entro trenta giorni dalla data di trasmissione. Decorso tale termine, i decreti possono essere comunque emanati.

3. Entro un anno dalla data di entrata in vigore di ciascuno dei decreti legislativi adottati nell'esercizio della delega di cui al comma 1, il Governo può adottare uno o più decreti legislativi contenenti disposizioni correttive e integrative dei decreti legislativi medesimi, nel rispetto dei princìpi e criteri direttivi di cui al comma 1 e secondo la procedura di cui al comma 2.

4. Qualora uno o più decreti legislativi di cui al comma 1 determinino nuovi o maggiori oneri che non trovino compensazione al proprio interno, gli stessi decreti legislativi sono adottati solo successivamente o

contestualmente all'entrata in vigore dei provvedimenti legislativi che stanziano le occorrenti risorse finanziarie, in conformità all'articolo 17, comma 2, della legge 31 dicembre 2009, n. 196.

€ 1,00