CAMERA DEI DEPUTATI N. **2366**

PROPOSTA DI LEGGE

D'INIZIATIVA DEI DEPUTATI

MOLLICONE, AMICH, CANGIANO, CIABURRO, GARDINI, LAMPIS, LA SALANDRA, MAIORANO, MASCARETTI, ZURZOLO

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

Presentata il 22 aprile 2025

ONOREVOLI COLLEGHI ! – La presente proposta di legge prevede una delega al Governo per la definizione di una strategia volta ad evitare il pagamento di riscatto per il furto di dati nel caso di attacchi informatici a scopo di estorsione, cosiddetti « *ransomware* ».

A prescindere dalla natura e dalla capacità di azione di tali attacchi informatici, le conseguenze sulle vittime possono essere molteplici. In primo luogo, l'impatto degli attacchi può essere di natura economico, tenendo conto delle somme eventualmente pagate per il riscatto, dei danni economici derivanti dall'interruzione o dal rallentamento delle attività e delle operazioni informatiche nonché dei costi per il ripristino dei sistemi e delle informazioni.

In secondo luogo, gli impatti possono essere di natura operativa qualora si verifichi una perdita di dati a seguito della loro cifratura o non si disponga di sistemi aggiornati di copia dei dati stessi (*backup)*. Tali effetti possono essere ancora più rilevanti qualora l'attacco sia lanciato da un gran numero di sistemi compromessi e infetti volto a rendere il sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse e il sovraccarico delle connessioni di rete dei sistemi, cosiddetto « *Distributed Denial of Service* – DDoS », ossia una pratica adottata da alcuni attori criminali per esercitare una maggiore pressione sulle vittime e indurle a pagare il riscatto.

Un ulteriore impatto frequentemente sperimentato dalle vittime di *ransomware* consiste nel danno reputazionale, in quanto le organizzazioni colpite sono spesso considerate pubblicamente come responsabili del-

l'inefficace gestione della sicurezza di dati e informazioni. A ciò si aggiunge, infine, l'esposizione a rischi di natura legale nel caso in cui i dati esfiltrati sottoposti alle normative vigenti in materia di protezione dei dati personali siano resi pubblici.

Gli attori criminali hanno perfezionato le metodologie di raccolta informativa e profilazione dei soggetti destinatari degli attacchi informatici. Queste attività, denominate « *Big Game Hunting* » (BGH), consentono ai gruppi criminali *(ransomware gang)* di selezionare le vittime in base al loro potenziale economico e alla loro presumibile capacità di pagare importi significativi a titolo di riscatto, calibrando così le richieste estorsive in funzione della solidità finanziaria dell'obiettivo.

Secondo il « 2024 *Incident Response Report* » pubblicato dalla società statunitense Palo Alto Networks, nel 2023 il valore stimato dei riscatti richiesti è aumentato di circa il 7 per cento rispetto al 2022 mentre il valore del riscatto effettivamente pagato equivale, in termini di valore mediano, a circa il 34 per cento del valore originariamente richiesto nello stesso anno da parte degli attori criminali.

Circa il 62 per cento delle vittime avrebbe negoziato con gli autori degli attacchi per il pagamento del riscatto.

PROPOSTA DI LEGGE

—

Art. 1.

1. Il Governo è delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi volti alla definizione di una strategia nazionale per il contrasto degli attacchi informatici a scopo di estorsione, sulla base dei seguenti princìpi e criteri direttivi:

a) previsione del divieto di pagamento di un riscatto a seguito delle condotte di cui all'articolo 629, terzo comma, 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 e imminente per la sicurezza nazionale connesso all'attacco informatico a scopo di estorsione;

b) introduzione di una disposizione che specifichi che l'attacco informatico a scopo di estorsione condotto contro 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, e che generi effetti sui soggetti stessi, possa essere qualificato, indipendentemente dall'autore, come un incidente o una compromissione che comporta un pregiudizio per la sicurezza nazionale, come definiti rispettivamente dall'articolo 1, comma 1, lettere *h)*, *g)* e *f)*, del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131. Tale qualificazione è effettuata dal Presidente del Consiglio dei ministri, ai sensi dell'articolo 2, comma 2, 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 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, 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) rafforzamento della collaborazione tra le istituzioni scolastiche del sistema nazionale di istruzione e formazione, comprese le istituzioni dell'alta formazione artistica, musicale e coreutica, e l'Agenzia per la cybersicurezza nazionale al fine di garantire una maggiore e crescente consapevolezza nella popolazione giovanile.

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. Agli oneri derivanti dall'attuazione della lettera *e)* del comma 1 del presente articolo, pari a 300.000 euro annui a decorrere dall'anno 2025, si provvede mediante corrispondente riduzione del Fondo di cui all'articolo 200 della legge 23 dicembre 2014, n. 190. 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.

PAGINA BIANCA

PAGINA BIANCA

19PDL0140030