CAMERA DEI DEPUTATI N. 3535

PROPOSTA DI LEGGE

D'INIZIATIVA DEI DEPUTATI

ENRICO BORGHI, CECCANTI, PAGANI, DE MENECH, CIAMPI, FIANO, GIORGIS, MAURI, POLLASTRINI, RACITI, CARÈ, FRAILIS, LOSACCO, LOTTI

Modifiche all'articolo 5 del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e altre disposizioni in materia di sicurezza nazionale cibernetica

Presentata il 25 marzo 2022

ONOREVOLI COLLEGHI ! – L'ultima Relazione sulla politica dell'informazione per la sicurezza, predisposta dagli organi del Sistema di informazione per la sicurezza della Repubblica ha evidenziato come, nel 2021, in linea di continuità con quanto accaduto nel 2020, gli attacchi cibernetici perpetrati ai danni di soggetti rilevanti per la sicurezza nazionale abbiano interessato prevalentemente i maggiori operatori pubblici e privati nazionali.

A conferma di una tendenza già rilevata negli ultimi anni, il complesso dei dati raccolti e messi a disposizione dai servizi nazionali di informazione per la sicurezza ha fatto emergere come gli attacchi cibernetici abbiano riguardato per lo più i sistemi informatici e le reti di soggetti pubblici (69 per cento). Tra questi ultimi, quelli maggiormente colpiti sono risultate essere le amministrazioni centrali dello Stato (56 per cento, valore in aumento di oltre 18 punti percentuali rispetto all'anno precedente) e infrastrutture di tecnologia dell'informazione (IT) riferibili a enti locali e strutture sanitarie (per un complessivo 30 per cento sul totale).

Gli attacchi cibernetici perpetrati nei confronti dei soggetti privati, invece, hanno interessato prevalentemente il settore energetico (24 per cento, in sensibile aumento rispetto al 2020), quello dei trasporti (18 per cento, in aumento di 16 punti percentuali) e delle telecomunicazioni (12 per

cento, in crescita di 10 punti percentuali rispetto all'anno precedente).

Peraltro, la minaccia principale per la nostra sicurezza nazionale è rappresentata principalmente dagli attacchi operati mediante virus informatici a fini di estorsione (cosiddetti « *ransomware* »). Infatti, sebbene si tratti di programmi utilizzati principalmente dai criminali informatici per ottenere il pagamento di un riscatto, ne è stato rilevato un crescente utilizzo anche ad opera di soggetti statali. Questi ultimi, però, perseguono fini differenti: sfruttano i *ransomware* per occultare tracce di precedenti operazioni di spionaggio o per bloccare le attività produttive, anche in settori rilevanti per la sicurezza nazionale.

Lo scenario sopra delineato è stato descritto di recente anche dall'Agenzia dell'Unione europea per la sicurezza cibernetica (ENISA), che, nel suo rapporto annuale *Threat Landscape 2021*, ha posto in evidenza come, tra aprile 2020 e luglio 2021, i settori più colpiti dagli attacchi cibernetici siano stati la pubblica amministrazione e i governi (198 attacchi segnalati), i fornitori di servizi digitali (152 attacchi segnalati), le strutture sanitarie e mediche (143 attacchi segnalati) e il settore bancario e finanziario (97 attacchi segnalati).

A livello internazionale, inoltre, il *Global Cybersecurity Outlook 2022* del Forum economico mondiale, che delinea le principali tendenze in materia di sicurezza cibernetica e analizza le questioni prioritarie nel breve e nel medio periodo, ha evidenziato come tra le principali preoccupazioni degli alti dirigenti del settore pubblico e privato vi sia proprio il malfunzionamento delle infrastrutture critiche a seguito di un attacco cibernetico.

Tali timori, peraltro, non sono il frutto di un'analisi predittiva, ma discendono dall'osservazione degli eventi che hanno caratterizzato la cronaca degli ultimi anni a livello sia nazionale che internazionale. Infatti, sono state numerose le notizie di attacchi cibernetici che hanno generato ripercussioni sulla capacità di esercitare una funzione essenziale dello Stato o di erogare un servizio essenziale per gli interessi di esso, così come definiti all'interno della normativa sul perimetro di sicurezza nazionale cibernetica, ossia, tra gli altri, quelli legati ai settori energetico, sanitario, bancario e finanziario, delle telecomunicazioni, dei trasporti, eccetera.

Si prendano come esempi l'attacco informatico che ha colpito nel 2020 l'ospedale Spallanzani, in prima linea nel fronteggiare l'emergenza sanitaria del COVID-19, oppure quello che, nell'estate del 2021, ha interessato il centro elaborazione dati e i sistemi informatici della regione Lazio, compromettendo l'utilizzo dei dati di alcuni servizi digitali, come quelli relativi proprio alla prenotazione dei vaccini per il COVID-19.

Il 2022, peraltro, non sembra essere cominciato sotto i migliori auspici, considerato che, nei primi due mesi dell'anno, già tre distinti attacchi cibernetici hanno colpito aziende europee che operano nel settore del trasporto e stoccaggio di petrolio, compromettendo la loro capacità di gestire i flussi di greggio: la Oiltanking, con sede in Germania, la SEA-Invest, che opera principalmente in Belgio, e la Evos, attiva in Olanda.

Ancora, a livello internazionale, uno degli episodi recenti più eclatanti è stato, a giugno 2021, quello dell'attacco alla Colonial Pipeline, che garantisce quasi metà degli approvvigionamenti di carburanti della costa orientale degli Stati Uniti d'America e dove un semplice attacco *ransomware* ha paralizzato le forniture per 2,5 milioni di barili al giorno di benzina, *diesel* e altri prodotti petroliferi, con un impatto più che rilevante sul tessuto economico-sociale e sui cittadini. Del resto, è notizia recente che il *Financial Crimes Enforcement Network* del Dipartimento del Tesoro degli Stati Uniti abbia individuato – nei soli primi sei mesi del 2021 – transazioni in *bitcoin* legate alle prime dieci varianti di *ransomware* più usate dalle organizzazioni criminali per un valore complessivo di 5,2 miliardi di dollari.

In ultimo, ma non per importanza, appare evidente anche come, nello scenario dell'attuale conflitto tra la Russia e l'Ucraina, il Governo di Mosca potrebbe sfruttare gli attacchi informatici come stru-

mento di ritorsione nei confronti delle sanzioni imposte dai Paesi appartenenti all'Alleanza atlantica, prendendo di mira proprio i servizi e le funzioni essenziali del nostro Stato e di quelli dei nostri alleati.

In considerazione dei dati e degli episodi suindicati, nonché dell'analisi di questa tendenza indubbiamente preoccupante e del suo indubbio incremento nel prossimo futuro, non si può fare a meno di osservare come alcune tipologie di attacchi cibernetici costituiscano un sempre più rilevante vettore di minaccia anche per la sicurezza nazionale.

Ciò in quanto, al di là di chi sia il reale soggetto attaccante (Stati, organizzazioni criminali o terroristiche, *hacker-for-hire*, attivisti, eccetera), gli effetti di simili attacchi cibernetici potrebbero arrivare a causare, come detto in precedenza, il blocco dell'esercizio di una funzione essenziale dello Stato o della prestazione di un servizio essenziale per gli interessi dello Stato, interrompendone il regolare funzionamento, causando effetti sui cittadini e trasformando, quindi, l'attacco cibernetico in un'evidente minaccia per la sicurezza nazionale.

Al fine di rafforzare la posizione dell'Italia appare utile, allora, intervenire all'interno della normativa sul perimetro di sicurezza nazionale cibernetica, al fine di classificare e graduare in maniera differente questo genere di attacchi cibernetici – identificandoli come « evento cibernetico critico » – e di assicurare al Presidente del Consiglio dei ministri il potere di chiedere, ove ritenuto necessario, che venga attuata ogni misura proporzionata per il loro contrasto al fine di tutelare la sicurezza nazionale.

PROPOSTA DI LEGGE

—

Art. 1.

(Adozione di misure per il contrasto di eventi cibernetici suscettibili di recare pregiudizio alla sicurezza nazionale)

1. All'articolo 5 del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, sono apportate le seguenti modificazioni:

a) dopo il comma 1 è inserito il seguente:

« *1.1.* Il Presidente del Consiglio dei ministri, in presenza di un evento cibernetico suscettibile di dar luogo a una situazione di crisi cibernetica, come rispettivamente definiti ai sensi delle lettere *m)* e *o)* del comma 1 dell'articolo 2 del decreto del Presidente del Consiglio dei ministri 17 febbraio 2017, pubblicato nella *Gazzetta Ufficiale* n. 87 del 13 aprile 2017, previa deliberazione del Comitato interministeriale per la sicurezza della Repubblica, può disporre che lo stesso sia classificato come pregiudizio per la sicurezza nazionale e che siano adottate le misure di contrasto necessarie e proporzionate al fine di tutelare la sicurezza nazionale »;

b) al comma 1-*bis*, le parole: « del comma 1 » sono sostituite dalle seguenti: « dei commi 1 e 1.1 ».

Art. 2.

(Accertamento del livello di sicurezza dei prodotti e dei servizi informatici)

1. I titolari dei diritti di proprietà industriale, di cui al codice della proprietà industriale, di cui al decreto legislativo 10 febbraio 2005, n. 30, e intellettuale, di cui alla legge 22 aprile 1941, n. 633, relativi a prodotti e programmi per elaboratori, basi di dati e piattaforme per la loro gestione e

a servizi di comunicazione elettronica in qualsiasi modo e a qualsiasi titolo messi a disposizione delle pubbliche amministrazioni, degli operatori economici o dei cittadini istituiscono, a propria cura e spese, centri di trasparenza tramite i quali mettono a disposizione dell'Agenzia per la cybersicurezza nazionale, dell'Agenzia per l'Italia digitale e dei soggetti eventualmente da queste indicati tutte le informazioni necessarie per accertare l'effettivo livello di sicurezza dei prodotti, dei programmi e dei servizi medesimi.

2. Con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'interno e con il Ministro della difesa, sentite l'Agenzia per la cybersicurezza nazionale e l'Agenzia per l'Italia digitale, sono adottate le disposizioni necessarie per l'istituzione e la gestione dei centri di trasparenza e per l'esecuzione degli accertamenti di cui al comma 1.

Art. 3.

(Libera utilizzabilità dei diritti di proprietà industriale relativi a prodotti informatici non più in commercio)

1. I diritti di proprietà industriale di cui al codice di cui al decreto legislativo 10 febbraio 2005, n. 30, e intellettuale, di cui alla legge 22 aprile 1941, n. 633, relativi a prodotti *hardware* e *software* e alle basi di dati che non sono più in commercio o per i quali il produttore ha dichiarato la cessazione del supporto sono liberamente utilizzabili da chiunque anche ai fini dell'offerta di prodotti e servizi.

2. I titolari dei diritti di proprietà industriale e intellettuale di cui al comma 1 mettono a disposizione gratuitamente tutte le informazioni, compresi i progetti e i codici sorgente, necessari al libero riutilizzo dei diritti medesimi relativi ai prodotti ivi indicati.

Art. 4.

(Nullità di clausole contrattuali e divieto di pratiche commerciali elusive)

1. Le disposizioni degli articoli 2 e 3 costituiscono norme imperative. È nulla

qualunque pattuizione o clausola contrattuale contraria alle predette disposizioni o volta a eluderne l'applicazione. La nullità della clausola non comporta la nullità del contratto.

2. Costituisce pratica commerciale scorretta ai sensi del titolo III della parte II del codice del consumo, di cui al decreto legislativo 6 settembre 2005, n. 206, la predisposizione di offerte o di modelli tecnologici o commerciali, comprese le modalità di determinazione dei prezzi e degli sconti, aventi la finalità di eludere l'applicazione delle disposizioni degli articoli 2 e 3.

3. L'Autorità garante della concorrenza e del mercato, in relazione a quanto disposto dal presente articolo, esercita le attribuzioni ad essa conferite dagli articoli 27 e 37-*bis* del codice di cui al decreto legislativo 6 settembre 2005, n. 206.

PAGINA BIANCA

18PDL0184270