Osservatorio
di Politica internazionale

Senato
della Repubblica
Camera
dei deputati
Ministero
degli Affari Esteri
e della Cooperazione
Internazionale

Maggio 2025

116

Note

Resilienza digitale: alcune riflessioni dal caso CrowdStrike

di Davide Lo Prete e Alessandro Savini

Sommario

1. Executive summary

Il 19 luglio 2024, un aggiornamento difettoso del software Falcon Sensor di CrowdStrike ha provocato una paralisi informatica senza precedenti, colpendo milioni di dispositivi a livello globale. L'errore, generato da un bug in un aggiornamento per i sistemi Windows, ha messo ancor più drammaticamente in evidenza quanto le moderne infrastrutture digitali siano profondamente interconnesse e, al tempo stesso, vulnerabili a singoli punti di rottura lungo la catena di approvvigionamento digitale. Il caso CrowdStrike segna un punto di svolta nel dibattito sulla sicurezza delle supply chain informatiche, dimostrando come il malfunzionamento di un singolo componente software possa generare effetti a cascata in grado di colpire i gangli vitali dell'economia e della società. Sanità, trasporti, settore bancario ed energia: gli effetti dell'incidente hanno attraversato in modo trasversale diversi ambiti strategici, coinvolgendo anche le cosiddette infrastrutture critiche, ossia quelle strutture e servizi la cui interruzione può produrre gravi

conseguenze sull'ordine pubblico, la sicurezza nazionale e la vita quotidiana dei cittadini. In Italia, dove molte infrastrutture critiche fanno affidamento su fornitori esterni e su tecnologie non sempre sviluppate in ambito nazionale, la protezione della supply chain digitale assume un'importanza cruciale. Il rafforzamento del quadro normativo e istituzionale avviato negli ultimi anni – in linea con le direttive europee – si è concretizzato attraverso la definizione del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e il ruolo crescente dell'Agenzia per la Cybersicurezza Nazionale (ACN). La presente Nota del Centro Studi Geopolitica.info, redatta per l'Osservatorio di Politica Internazionale (progetto di collaborazione tra Senato della Repubblica, Camera dei deputati e Ministero degli Affari esteri e della Cooperazione internazionale), si propone di analizzare gli impatti dell'incidente CrowdStrike, con particolare attenzione alla sua rilevanza per le infrastrutture critiche nazionali. L'obiettivo è delineare l'importanza di un approccio sistemico alla cyber resilience, basato non solo sulla prevenzione tecnica, ma anche sulla continuità operativa, sulla capacità di risposta e ripristino in seguito a un incidente e sulla messa in sicurezza dell'intera catena di approvvigionamento digitale, alla luce delle più recenti evoluzioni normative.

2. Il *bug* che ha paralizzato il mondo: la *supply chain* come vulnerabilità sistemica

Il 19 luglio 2024, un aggiornamento difettoso del *software* Falcon Sensor – sviluppato da CrowdStrike, uno dei principali *provider* globali di soluzioni di *cyber security* – ha provocato una paralisi informatica su scala mondiale, compromettendo il funzionamento di milioni di dispositivi.

Secondo quanto riportato dalla stessa azienda, la causa dell'incidente risiedeva in un errore nel "Channel File 29", un componente del *driver* del Falcon Sensor, piattaforma *cloud* progettata per la protezione degli *endpoint* (nodi di comunicazione in rete). L'aggiornamento, distribuito automaticamente tramite i consueti canali, provocava un *crash* all'avvio di Windows, rendendo inutilizzabili i sistemi operativi sui quali il *software* era installato (CrowdStrike, 2024). L'effetto domino non si è fatto attendere: compagnie aeree costrette a cancellare voli, ospedali in blackout tecnologico, centri nevralgici del traffico urbano in tilt. In Italia, sono stati registrati disservizi in alcuni grandi aeroporti, ritardi nei servizi ferroviari e rallentamenti nella pubblica amministrazione. Secondo fonti ufficiali di CrowdStrike, il problema è stato risolto nel giro di alcune ore grazie a un *roll-back* dell'aggiornamento, ma le ripercussioni sull'operatività sono durate giorni, in quanto il danno si era già esteso a livello globale, con più di 8,5 milioni di *endpoint* interessati (Microsoft, 2024). Pur non essendo un attacco malevolo, il caso ha avuto l'effetto di un attacco *cyber* su scala globale, dimostrando come anche incidenti non intenzionali possano avere impatti sistemici se non vengono gestiti correttamente in fase preventiva e di risposta.

Negli ultimi anni, la *supply chain* digitale è divenuta un obiettivo sempre più appetibile per gli attori di minaccia (*threat actor*), siano essi gruppi cybercriminali o *state-sponsored*. L'elemento comune a tutti gli attacchi più sofisticati dell'ultimo decennio è, infatti, l'infiltrazione attraverso fornitori terzi, aggiornamenti *software* compromessi o componenti *hardware* vulnerabili. Basti pensare al caso di SolarWinds nel 2020, quando un aggiornamento malevolo del *software* di gestione Orion compromise le reti di enti pubblici e privati in tutto il mondo, o a quello di Kaseya nel 2021, dove un aggiornamento veicolò un *ransomware* che colpì migliaia di imprese (Radu, 2021; Willet 2021). A differenza di questi episodi, il caso CrowdStrike non è stato frutto di un attacco, ma la dinamica – e soprattutto la portata – è risultata sorprendentemente analoga. In sintesi, un singolo punto di *failure* in un prodotto utilizzato su larga scala può causare, se non opportunamente controllato, una crisi globale.

I dati globali confermano la crescente minaccia rappresentata dagli attacchi alla *supply chain*. Nel 2024, circa 180.000 clienti sono stati colpiti da attacchi alla *supply chain*, registrando un aumento del 33% rispetto all'anno precedente. Esperti del settore prevedono che i costi annuali globali derivanti da attacchi tramite la catena di approvvigionamento raggiungeranno i 60 miliardi di dollari entro il 2025, con una crescita annuale del 15%, fino a raggiungere i 138 miliardi entro il 2031 (cfr. bibliografia).

Nel contesto italiano, dove molte infrastrutture critiche dipendono da fornitori esterni – spesso internazionali – per la protezione dei propri sistemi, il tema della *supply chain cyber* assume una rilevanza ancora maggiore. La questione non è più "se" rafforzare la sicurezza lungo la catena, ma "come" farlo in tempi rapidi e in modo sistemico. Le infrastrutture critiche sono un bersaglio sempre più attraente per tutte le categorie di *threat actor*: dai *cyber* criminali, interessati a massimizzare i profitti illeciti, agli attori *state-sponsored* per finalità di spionaggio o vantaggio

competitivo, fino ai gruppi hacktivisti. Secondo il più recente rapporto Clusit, nel 2024 l'Italia è stata colpita dal 2,91% delle minacce globali, rispetto allo 0,79% dell'anno precedente.

3. Collaborazione internazionale: un imperativo strategico

Il caso CrowdStrike evidenzia l'importanza della collaborazione internazionale nella risposta a incidenti *cyber* su larga scala. Iniziative come la *International Counter Ransomware Initiative* (CRI), promossa dagli Stati Uniti, mirano a rafforzare la cooperazione tra i Paesi per contrastare le minacce informatiche. La CRI, che riunisce oltre 60 Stati e organizzazioni internazionali, promuove la condivisione di informazioni, la definizione di standard comuni e l'adozione di strategie coordinate contro attori malevoli (Lewis, 2025).

Accanto a queste iniziative, un ruolo fondamentale è svolto dagli *Information Sharing and Analysis Centers* (ISAC), organismi settoriali che facilitano il dialogo tra pubblico e privato nei vari comparti strategici (energia, trasporti, finanza, sanità). In Europa, un esempio rilevante è l'*Energy* ISAC, promosso dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA) e da autorità nazionali, mentre in Italia si sta rafforzando la rete di collaborazione tramite strutture come il Centro di Valutazione e Certificazione Nazionale (CVCN), l'Agenzia nazionale per la cybersicurezza nazionale (ACN) e il suo organo di monitoraggio preventivo e risposta agli incidenti informatici (CSIRT Italia), che incoraggiano la condivisione proattiva di *cyber threat intelligence* e *incident data* tra enti pubblici e operatori privati.

Ulteriori iniziative - come l'EU *Cyber Solidarity Act*, il *Cybersecurity Act e il Cybersecurity Emergency Mechanism dell'Unione Europea* (UE) - puntano proprio a rendere più efficace la risposta congiunta tra Stati membri in caso di crisi *cyber*. Rafforzare la partecipazione italiana a queste piattaforme e incentivare la collaborazione tra aziende e strutture nazionali può costituire un importante volano di resilienza, riducendo drasticamente i tempi di rilevamento, contenimento e ripristino in caso di eventi simili a quello del luglio 2024.

4. Il quadro normativo europeo

A tal riguardo, è di centrale importanza il *framework* normativo che ha definito l'UE negli ultimi anni, adottando normative quali la Direttiva NIS 2 (Direttiva UE n. 2022 del 2555, recepita in Italia con il D.lgs n. 138 del 2024), il Regolamento DORA (Regolamento UE 2022/2554 sulla Resilienza operativa digitale del settore DORA), il Regolamento UE *Cyber Resilience Act* 2024/2847) e la Direttiva UE sulla Resilienza delle Entità Critiche (Direttiva UE 2022/2557 recepita in Italia con il D. lgs. n. 134 del 2024) .

Entrata in vigore a livello europeo nel gennaio 2023, la direttiva NIS 2 rappresenta un'evoluzione della precedente Direttiva NIS (Direttiva (UE) 2016/1148, recepita in Italia con il D.lgs n. 65 del 2018. L'aggiornamento si è reso necessario alla luce dei profondi cambiamenti tecnologici, dell'accelerazione della digitalizzazione indotta dalla pandemia da COVID-19 e dell'evoluzione costante del panorama delle minacce *cyber*. Il nuovo impianto normativo estende il campo di applicazione della Direttiva a un numero più ampio di settori strategici e introduce requisiti di sicurezza più stringenti, con particolare attenzione alla protezione della catena di fornitura. La Direttiva NIS 2 intende inoltre colmare

alcune lacune emerse nell'attuazione della prima versione, tra cui un livello di resilienza *cyber* insufficiente rispetto alla crescente complessità del contesto, la frammentazione delle misure tra gli Stati membri e l'assenza di un meccanismo efficace di risposta coordinata agli incidenti *cyber* su larga scala.

Aspetto chiave della Direttiva è l'ampliamento dei settori, ricomprendendo anche settori quali la gestione dei rifiuti, i *social network*, il settore manifatturiero e quello alimentare. Vengono inoltre stabilite delle soglie dimensionali specifiche, che fanno ricomprendere tutte le medie e grandi imprese che operano nei settori definiti. A differenza della precedente direttiva NIS 1, poi, la NIS 2 definisce un elenco di misure di sicurezza di alto livello, che gli Stati Membri devono dettagliare nel recepimento della normativa e che vanno dalla redazione di politiche di sicurezza alla definizione di piani di formazione per i dipendenti.

Attenzione particolare viene data poi alla sicurezza della catena di approvvigionamento, per cui la Direttiva impone alle organizzazioni di gestire i rischi legati alla *supply chain*, sia a livello contrattuale, sia in termini di valutazione della postura di *cyber security* dei fornitori. Inoltre, è previsto che gli Stati Membri, in collaborazione con la Commissione e l'ENISA possano effettuare delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche.

Come precedentemente rilevato, la Direttiva NIS 2 è stata recepita in Italia a ottobre 2024 e gli obblighi di base sono stati pubblicati ad aprile 2025, basati sul Framework Nazionale per la Cybersecurity e la Data Protection aggiornato. Le organizzazioni incluse nell'elenco dei soggetti NIS avranno 9 mesi per adeguarsi all'obbligo di notifica degli incidenti e 18 mesi per implementare le misure di sicurezza previste negli obblighi di base definiti dall'ACN.

In questo scenario, il richiamato Regolamento DORA del 2022 rappresenta una risposta strategica dell'Unione Europea per rafforzare la resilienza *cyber* del settore finanziario, oggi sempre più esposto a rischi sistemici legati alla dipendenza da fornitori ICT terzi. Il Regolamento – entrato in vigore il 17 gennaio 2025 – impone agli operatori finanziari non solo di gestire in modo strutturato il rischio ICT, ma anche di assicurarsi che i loro fornitori critici adottino misure di sicurezza coerenti e trasparenti. Elementi come la valutazione della concentrazione dei fornitori, il *testing* basato su scenari di attacco realistici e il monitoraggio continuo della *supply chain* digitale diventano leve fondamentali per ridurre l'impatto di eventi a cascata come quelli osservati nel caso CrowdStrike. In questo senso, il Regolamento DORA rappresenta non solo una norma, ma un cambio di paradigma: dalla gestione reattiva e proattiva degli incidenti alla costruzione di una resilienza operativa digitale *end-to-end*.

A rafforzare ulteriormente questo approccio integrato alla sicurezza della *supply chain* si affianca il successivo Regolamento UE 2024/2847 *Cyber Resilience Act*, la cui applicazione è prevista a partire dal 2027. Questo regolamento introduce requisiti specifici di *cyber security* per produttori, importatori e distributori di prodotti digitali. Il Regolamento mira ad ottenere la sicurezza già in fase di sviluppo (*Security by Design*), dovendo i produttori fornire prodotti con configurazioni sicure e garantire un'adeguata gestione delle vulnerabilità tramite aggiornamenti di sicurezza costanti. Il Regolamento prevede anche un processo di certificazione che consentirà di ottenere il marchio CE per i prodotti conformi, garantendo alle aziende, in fase di approvvigionamento, di scegliere in modo consapevole i fornitori maggiormente sicuri.

Ulteriore normativa utile a rafforzare la resilienza a livello europeo, sebbene non unicamente *cyber*, è la citata Direttiva UE sulla Resilienza delle Entità Critiche del 2022/2557 recepita in Italia con il D. lgs. n. 134 del 2024.

Questa introduce importanti novità rispetto alla precedente Direttiva 2008/114/CE, applicandosi a 11 settori, tra cui quelli già ricompresi nella precedente (energia e trasporti). Tale ampliamento è dovuto alla crescente complessità e interconnessione delle infrastrutture critiche, che fa sì che l'interruzione di un servizio essenziale, anche laddove limitata a un soggetto o a un settore, può avere effetti a cascata più ampi, su tutta l'UE (Commissione Europea, 2023). La direttiva impone alle organizzazioni di effettuare una valutazione del rischio relativa a differenti tipologie di minacce, ivi incluse quelle *cyber*, sviluppare piani di resilienza contenenti le misure di mitigazione dei rischi e notificare gli incidenti significativi. Tra le misure viene data particolare attenzione a quelle utili a garantire la continuità operativa e il ripristino da eventuali incidenti e disastri.

Infine, l'UE ha definito il sistema europeo di certificazione della *cyber security* basato sui criteri comuni (EUCC), che svolge un ruolo chiave nel rafforzare la sicurezza di prodotti e servizi critici in ambito digitale. Tale schema permetterà di associare a ogni prodotto i requisiti di c*yber security* implementati dal produttore e il livello di affidabilità garantito, creando così un ecosistema di resilienza, in cui aziende e pubbliche amministrazioni possono far affidamento su catene di approvvigionamento certificate a livello nazionale ed europeo. A tal riguardo, l'Italia ha attuato il sistema di certificazione lo scorso febbraio, tramite l'adozione di alcune linee guida da parte dell'ACN

Tali normative si configurano come pilastri fondamentali della strategia europea di difesa e resilienza *cyber*, contribuendo da un lato al rafforzamento dei presidi di sicurezza, dall'altro alla promozione di una cooperazione strutturata e di una condivisione efficace delle informazioni tra Stati Membri, aspetti imprescindibili in un dominio intrinsecamente transnazionale come quello *cyber*. In questo contesto, si afferma sempre più un approccio orientato alla "*security by design*", che mira a integrare requisiti di sicurezza fin dalle fasi iniziali di sviluppo e progettazione dei prodotti digitali. Tale orientamento consente di mitigare il rischio di vulnerabilità strutturali e di innalzare il livello di affidabilità dell'intero ecosistema tecnologico europeo.

5. L'architettura di *cyber security* in Italia

A livello nazionale, l'Italia si è dotata da tempo di un quadro normativo volto a rafforzare la cybersicurezza degli attori strategici per il Sistema Paese, contribuendo alla tutela degli interessi nazionali.

Da un punto di vista legislativo, dopo il recepimento, attraverso il D.lgs n. 65 del 2018, della citata Direttiva NIS nel 2018, con il decreto legge n. 105 del 2019, - convertito nella legge 18 novembre 2019, n. 133 – è stato definito il Perimetro di sicurezza cibernetica nazionale al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o la fornitura di un servizio essenziale per lo Stato e dal cui malfunzionamento, interruzione, anche parziali o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

La legge 133/2019 ed i successivi provvedimenti attuativi hanno delineato, in particolare, un insieme di obblighi per le organizzazioni che erogano servizi essenziali. Tra questi, rientrano l'adozione di misure minime di sicurezza, la notifica degli incidenti e la gestione dei rischi lungo la catena di approvvigionamento. In tale ambito, opera il Centro di Valutazione e Certificazione Nazionale (CVCN), al quale i soggetti inclusi nel Perimetro sono tenuti a notificare gli approvvigionamenti relativi ai cosiddetti "Beni ICT", ovvero sistemi informativi e tecnologie funzionali all'erogazione dei servizi essenziali.

Con il successivo decreto legge n. 82 del 2021, si è inoltre, proceduto alla definizione dell'architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la cybersicurezza nazionale, in attuazione di precisi obiettivi del Piano nazionale di ripresa e resilienza (PNRR): la sicurezza cibernetica costituisce, infatti, uno dei principali interventi previsti dal PNRR nell'ambito della trasformazione digitale della p.a. e della digitalizzazione del Paese.

In Italia è proprio l'ACN l'organo istituzionale deputato a garantire la *cyber security* e *cyber resilience* nazionale. A tal proposito giova ricordare che la *governance* del sistema di sicurezza cibernetica ha al suo vertice il Presidente del Consiglio dei ministri, al quale è attribuita l'alta direzione e la responsabilità generale delle politiche di cybersicurezza nonché l'adozione della relativa strategia nazionale e - previa deliberazione del Consiglio dei ministri - la nomina e la revoca dei vertici dell'Agenzia per la cybersicurezza nazionale; di tali nomine sono preventivamente informati il Comitato parlamentare per la sicurezza della Repubblica (COPASIR) e le competenti Commissioni parlamentari. Il Presidente del Consiglio dei ministri trasmette al Parlamento (entro il 30 aprile di ogni anno) una relazione sull'attività svolta dall'Agenzia nell'anno precedente (qui l'ultima Relazione). Così come trasmette al COPASIR (entro il 30 giugno di ogni anno) una relazione sulle attività svolte nell'anno precedente dall'Agenzia concernenti la tutela della sicurezza nazionale nello spazio cibernetico per i profili di competenza del Comitato.

A sua volta l'Agenzia ha tra i suoi compiti fondamentali quello di coordinare le attività di prevenzione, monitoraggio e risposta agli incidenti informatici che possono colpire infrastrutture critiche e settori strategici del Paese. In linea con il quadro normativo europeo, l'Agenzia ha inoltre il compito di vigilare sull'attuazione degli obblighi di sicurezza da parte degli operatori inclusi nel Perimetro di Sicurezza Nazionale Cibernetica e nella Direttiva NIS 2, supportando al contempo lo sviluppo di competenze, certificazioni e tecnologie nazionali.

Nel contesto del caso CrowdStrike, il ruolo dell'ACN si rivela ancora più centrale: dalla promozione di piani di continuità operativa e *cyber resilience* per gli operatori di servizi essenziali, alla gestione delle comunicazioni con il CSIRT fino alla collaborazione con il settore privato e con altri enti pubblici per rafforzare la consapevolezza e l'adozione di standard minimi di sicurezza lungo tutta la *supply chain* digitale.

Questo impianto normativo, che si innesta e si integra con il quadro europeo, rafforza la postura di sicurezza nazionale, con un'attenzione particolare alla sicurezza della s*upply chain* tecnologica. Anche alla luce dell'incidente CrowdStrike, tale approccio contribuisce ad accrescere la capacità di prevenzione, risposta e recupero da eventi *cyber* con potenziali impatti sistemici sulle infrastrutture critiche.

Il rafforzamento della resilienza *cyber* ha conosciuto da ultimo un'ulteriore evoluzione nel 2024 con l'entrata in vigore della legge 90/2024, che introduce nuovi obblighi a carico delle Pubbliche Amministrazioni e dei soggetti inclusi nel

PSNC. Tra le principali misure, si segnalano obblighi stringenti in materia di gestione delle vulnerabilità – con un termine massimo di 15 giorni per la loro risoluzione a seguito della notifica da parte dell'ACN – nonché requisiti specifici per l'utilizzo della crittografia e per l'acquisizione di beni e servizi informatici, in linea con criteri tecnici e linee guida definite dall'Agenzia.

6. Lezioni apprese

Il guasto informatico che ha visto protagonista CrowdStrike è stato un evento di portata globale che ha colpito indiscriminatamente più settori, dimostrando quanto il cyberspazio sia oggi un dominio inestricabilmente legato al funzionamento della nostra società. Da questo caso emergono almeno quattro priorità strategiche su cui riflettere.

La prima riguarda la resilienza delle infrastrutture critiche. L'incidente ha evidenziato quanto anche le realtà più mature possano trovarsi vulnerabili di fronte a un evento massivo, non necessariamente doloso, ma ad alto impatto sistemico. È fondamentale che le infrastrutture critiche, pubbliche e private, adottino piani di *business continuity* e *incident response* che includano scenari ad alta frequenza ma a bassa intenzionalità. La continuità operativa non può essere affidata solo a procedure statiche, ma va testata periodicamente tramite esercitazioni simulate, aggiornamento degli scenari di crisi e definizione chiara dei flussi decisionali interni. Per i soggetti regolati, modelli come il Digital Operational Resilience Testing previsto dal Regolamento DORA costituiscono un riferimento imprescindibile. In un'ottica più ampia, il *threat landscape report* pubblicato da ENISA rappresenta un utile strumento di supporto alla modellazione degli scenari *cyber*. Adottare un approccio di *cybersecurity* al fine di prevenire gli incidenti non è più sufficiente nel contesto complesso odierno. Le organizzazioni devono spostare l'attenzione sulla *cyber resilience*, che parte dal concetto che nessun sistema è esente da vulnerabilità e che, quindi, un incidente si possa verificare in qualsiasi momento. L'obiettivo non è più soltanto prevenire l'incidente, ma gestirne efficacemente le conseguenze una volta che si è verificato, assicurando la continuità operativa, il rapido ripristino dei sistemi compromessi e la tutela della reputazione dell'organizzazione. In un contesto in cui la superficie di attacco si espande costantemente, la capacità di assorbire e contenere l'impatto di un attacco rappresenta un elemento cruciale di resilienza. Del resto, le implicazioni per le organizzazioni possono essere drammatiche: si stima che circa il 60% delle piccole e medie imprese che subiscono un attacco informatico cessi l'attività entro sei mesi (Leigh, 2023).

La seconda priorità strategica è relativa alla verifica e diversificazione delle forniture ICT. Il caso CrowdStrike ha dimostrato l'impatto potenziale che un singolo punto di fallimento può generare su scala globale, quando vi è una concentrazione eccessiva su un solo fornitore. Molte organizzazioni si sono trovate senza alternative tecniche o *backup agent*, esponendosi a un'interruzione completa delle attività. Diventa quindi prioritario introdurre audit periodici sui fornitori tecnologici, valutare i rischi legati alla *vendor lock-in* (dipendenza dal provider), e implementare politiche attive di diversificazione delle soluzioni. Per la maggior parte delle grandi organizzazioni, la catena di approvvigionamento rappresenta il più grande ostacolo nel raggiungere la *cyber resilience* (WEF, 2025), in quanto è più facile garantire la sicurezza del proprio perimetro interno rispetto ad avere una chiara visibilità sulle misure messe in atto dalle terze parti. In tal senso, la Direttiva NIS 2 introduce l'obbligo di gestire il rischio *cyber* lungo la catena di

approvvigionamento, prevedendo clausole contrattuali e valutazione periodica dei fornitori, al fine di creare un ecosistema che sia resiliente, a fronte di un panorama delle minacce sempre più sofisticato e in continua evoluzione.

La terza riguarda la supervisione normativa e la promozione di partenariati pubblico-privati, al fine di rafforzare la *governance* pubblica della *cyber security*, in linea con i più recenti interventi normativi adottati in mabito europeo.

Come rilevato, in particolare, anche nel Documento conclusivo dell' Indagine conoscitiva sulla difesa cibernetica: nuovi profili e criticità, svolta dalla IV Commissione della Camera dei deputati, (aprile 2025), le autorità nazionali e sovranazionali devono adottare un approccio proattivo, promuovendo e rafforzando il modello di cooperazione tra pubblico e privato.

Infine, è di cruciale importanza sviluppare una cultura del rischio e gestire il ciclo di vita del *software*. Il caso CrowdStrike ha evidenziato quanto sia fragile il ciclo di rilascio degli aggiornamenti, soprattutto quando è automatizzato su larga scala senza validazioni incrociate. Serve una cultura della sicurezza in ogni fase del ciclo di vita del *software*, dalla progettazione fino al *deployment* e alla gestione degli aggiornamenti.

Se da un lato l'incidente può essere considerato come un "evento sentinella" per migliorare la sicurezza della *supply chain IT*, dall'altro costituisce anche un'occasione preziosa per consolidare una cultura della resilienza in tutti quei settori – pubblici e privati – che operano nel perimetro delle infrastrutture critiche. Per l'Italia, ciò significa accelerare l'attuazione delle politiche già avviate, potenziare le capacità di *threat intelligence* e analisi del rischio e assicurare una maggiore convergenza tra sicurezza nazionale e sicurezza aziendale. Un ulteriore fronte di miglioramento è rappresentato dall'adozione di *framework* di gestione della *supply chain* – come NIST SP 800-161 o ISO/IEC 27036 – che potrebbero diventare standard obbligatori per i fornitori degli operatori di servizi essenziali.

L'Italia, in quanto Stato membro dell'UE e parte attiva nei consessi internazionali dedicati alla *cyber security*, ha ora l'opportunità di rafforzare la propria postura strategica sul tema, a partire da una lezione semplice ma fondamentale: nessuna difesa è efficace se non tiene conto della complessità e interconnessione del cyberspazio. È proprio nei momenti di crisi che si testano – e si rafforzano – le fondamenta di una vera resilienza nazionale e collettiva.

7. Bibliografia

Documento conclusivo dell'Indagine conoscitiva sulla difesa cibernetica: nuovi profili e criticità, svolta dalla IV Commissione della Camera dei deputati, (aprile 2025)

Agenzia per la Cybersicurezza Nazionale (2025). *NIS – La Normativa*. Consultabile su: https://www.acn.gov.it/portale/nis/la-normativa

Agenzia per la Cybersicurezza Nazionale (2025). *Al via l'attuazione nazionale dell'EUCC, il primo sistema europeo di certificazione della cybersicurezza*. Consultabile su: https://www.acn.gov.it/portale/w/al-via-l-attuazione-nazionale-dell-eucc-il-primo-sistema-europeo-di-certificazione-della-cybersicurezza

Clusit (2025). *Rapporto Clusit sulla cybersecurity in Italia e nel mondo 2025*. Consultabile su: https://clusit.it/rapporto-clusit/

Commissione Europea (2023). *Enhancing EU resilience: A step forward to identify critical entities for key sectors*. Consultabile su: https://ec.europa.eu/commission/presscorner/detail/it/ip_23_3992

Commissione Europea (2025). *Direttiva NIS 2: nuove norme sulla cibersicurezza delle reti e dei sistemi informativi*. Consultabile su: https://digital-strategy.ec.europa.eu/it/policies/nis2-directive

Commissione Europea (2025). *Quadro di certificazione della cibersicurezza dell'UE*. Consultabile su: https://digital-strategy.ec.europa.eu/it/policies/cybersecurity-certification-framework

CrowdStrike (2024). *External Technical Root Cause Analysis — Channel File 291*. Consultabile su: https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf

EIOPA *Digital Operational Resilience Act (DORA)*. Consultabile su: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Framework Nazionale per la Cybersecurity e la Data Protection - Edizione 2025

Kranjec, J. (2024). Over 183,000 Customers Were Affected by Supply Chain Cyberattacks in 2024, 33% more than Last Year. *Stocklytics*. Consultabile su: https://stocklytics.com/content/over-183000-customers-were-affected-by-supply-chain-cyberattacks-in-2024-33-more-than-last-year/?utm_source=chatgpt.com

Leigh, D. (2023). 60% Of SMEs That Suffer A Cyber Attack Go Out Of Business Within Six Months. *TechRound*. Consultabile su: https://techround.co.uk/news/60-of-smes-that-suffer-a-cyber-attack-go-out-of-business-within-six-months/

Lewis, J. A. (2025). Next Steps for the International Counter Ransomware Initiative. *Center for Strategic & International Studies*. Consultabile su: https://www.csis.org/analysis/next-steps-international-counter-ransomware-initiative

Lo Prete, D. (2021). Agenzia per la Cybersicurezza Nazionale: la responsabilità italiana nel dominio cibernetico. Intervista all'On. Alberto Pagani. *Geopolitica.info*. Consultabile su: https://www.geopolitica.info/agenzia-per-la-cybersicurezza-nazionale-la-responsabilita-italiana-nel-dominio-cibernetico-intervista-allon-alberto-pagani/

Lo Prete, D. (2021). Perimetro di sicurezza cibernetica nazionale: lo scudo cyber ai blocchi di partenza. *Geopolitica.info*. Consultabile su: https://www.geopolitica.info/perimetro-di-sicurezza-cibernetica-nazionale-lo-scudo-cyber-ai-blocchi-di-partenza/

Marenaci, D. (2023). L'Italia rafforza le difese contro l'ondata di attacchi hacker. *Geopolitica.info*. Consultabile su: https://www.geopolitica.info/litalia-rafforza-le-difese-contro-londata-di-attacchi-hacker/

Microsoft (2024). *Helping our customers through the CrowdStrike outage*. Consultabile su: https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

Radu, R. (2021). What we learned from the Kaseya attack: recommendations for a human-centric approach to curb ransomware. *CyberPeace Institute*. Consultabile su: https://cyberpeaceinstitute.org/publications/what-we-learned-from-the-kaseya-attack-recommendations-for-a-human-centric-approach-to-curb-ransomware/

Willet, M. (2021). Lessons of the SolarWinds hack. *International Institute for Strategic Studies*. Consultabile su: https://www.iiss.org/sv/online-analysis/survival-online/2021/04/lessons-of-the-solarwinds-hack/

World Economic Forum (2025). *Global Cybersecurity Outlook 2025*. Consultabile su: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

Osservatorio di Politica internazionale

www.parlamento.it/osservatoriointernazionale

Senato della Repubblica

Camera dei Deputati

Ministero degli Affari Esteri
e della Cooperazione
Internazionale

Coordinamento redazionale:

Camera dei deputati
Servizio Studi - Dipartimento Affari esteri
Tel. 06.67604939
Email: st_affari_esteri@camera.it