Atto Camera 1717

"Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"

Contributo

di

alle

Commissioni riunite I Affari costituzionali e II Giustizia della Camera dei Deputati

Introduzione

Ringraziamo le Commissioni riunite I Affari costituzionali e II Giustizia della Camera dei Deputati per l'opportunità offerta a Fortinet di contribuire all'istruttoria del disegno di legge di iniziativa del Governo: *"Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici".*

Fortinet® è un'azienda leader globale nelle soluzioni di Cybersicurezza. Fondata nel 2000 negli Stati Uniti, la sua sede principale è a Sunnyvale, California.

Da oltre 20 anni Fortinet è uno dei leader più innovativi nell'evoluzione della Cybersicurezza e nella convergenza di networking e sicurezza. Le sue soluzioni per la sicurezza della rete sono le più implementate, le più brevettate e le più convalidate del settore. Secondo dati indipendenti*, il 50% delle unità di sicurezza cibernetica (Next-Generation Firewalls) utilizzate nel mondo è prodotto da Fortinet.

In Italia l'azienda è presente dal 2004 con due sedi, Milano e Roma, ed è fornitore rilevante della P.A., mentre in ambito più ampio è da molti anni titolare di una apprezzata partnership con la NATO sia tramite unità di sicurezza che grazie a servizi di intelligence preventiva e formazione del personale.

Un disegno di legge che va nella giusta direzione

Guardiamo con grande interesse al testo del DDL oggetto della discussione, che tratta una tematica estremamente importante e urgente per la sicurezza del nostro Paese. L'esame del disegno di legge offre a Fortinet una preziosa opportunità per condividere con le Commissioni riunite il punto di vista e le osservazioni di chi opera "in prima linea" per prevenire e contrastare il cyber-crime sull'articolato che introduce varie previsioni da noi reputate del tutto positive:

- *Artt. 1, 2, 3* – le pubbliche amministrazioni (indicate nel presente disegno di legge) sono tenute a segnalare e notificare gli incidenti tempestivamente. Sono tenute altresì ad adottare gli interventi risolutivi indicati dall'ACN in caso di vulnerabilità potenzialmente esposte.
- *Art. 6* - le pubbliche amministrazioni (indicate nel presente disegno di legge) debbono provvedere a individuare, ove non già presente, una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, preposta alle relative attività di cybersicurezza e presso la quale opererà l'istituenda figura del referente per la cybersicurezza, che svolge, tra l'altro, la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale nell'obbligo di notifica degli incidenti.
- *Art. 7* – Si rafforza il ruolo di ACN conferendole, in ragione del ruolo di Autorità nazionale per la cybersicurezza, la possibilità di promuovere e sviluppare ogni iniziativa, anche di partenariato pubblico-privato, per la valorizzazione dell'intelligenza artificiale come risorsa per il rafforzamento della sicurezza e della resilienza cibernetiche nazionali, anche al fine di favorire un uso etico e corretto dei sistemi basati su tale tecnologia.
- *Artt. 11, 12* – Vengono apportate modifiche al codice penale dei reati informatici con l'inasprimento delle pene per alcuni tipi di reati.

*Fonte:IDC

Alcune proposte migliorative

Questa audizione è l'opportunità preziosa per evidenziare, oltre agli aspetti del tutto positivi del disegno di legge, anche quei passaggi che invece a nostro parere sarebbe utile migliorare ulteriormente durante l'iter parlamentare. Alla luce dell'esperienza maturata da Fortinet lavorando con Pubbliche Amministrazioni italiane nel corso dell'ultimo decennio, lasciamo alla valutazione delle Commissioni riunite i seguenti commenti relativi alle seguenti aree:

Competenze tecniche e risorse delle Pubbliche Amministrazioni.

- ***Necessità di prevedere risorse finanziare ad hoc.*** Non tutte le Pubbliche Amministrazioni hanno avuto nel corso degli ultimi anni capacità finanziaria e adeguate competenze tecniche tali da acquisire opportunamente le soluzioni necessarie in materia di cybersicurezza. Allo stesso tempo, ancora meno amministrazioni hanno potuto contare su un numero di persone competenti sufficiente a poter progettare e configurare le soluzioni acquisite.
- ***Ciò è tanto più valido per le Pubbliche Amministrazioni Locali, bersaglio crescente degli attacchi informatici.*** Gli adempimenti potrebbero rivelarsi particolarmente onerosi per i soggetti più piccoli con il rischio di inadempienza e quindi di vedere immutato l'attuale livello di cybersicurezza. E' quindi essenziale aiutare con risorse e/o agevolazioni le Pubbliche Amministrazioni, soprattutto i soggetti più piccoli come quelle locali. Va considerato oltretutto che le Pubbliche Amministrazioni Locali includono una parte importante di infrastrutture critiche, tra cui: la sanità, i trasporti, la gestione delle acque, la distribuzione dell'energia, etc.
- ***Introduzione di criteri di valutazione della cybersicurezza e meccanismi di premialità nelle gare pubbliche.*** Sarebbe opportuno impegnare le pubbliche amministrazioni ad utilizzare gli elementi di cybersicurezza come criteri premianti nella valutazione delle offerte di beni e servizi informatici, anche per progetti non strettamente correlati alla cybersecurity (esempi: software, servizi, infrastruttura digitale). Questo potrebbe da un lato aiutare a spendere meglio le risorse disponibili, o da assegnare, e dall'altro favorire a parità di spesa una attenzione maggiore al tema della sicurezza ICT per ogni tipo di P.A. che si appresti ad acquisire beni e servizi.
- ***Tempistiche all'insegna della gradualità.*** Le Pubbliche Amministrazioni con le risorse umane attuali, hanno bisogno di tempo per poter eseguire un'analisi delle attuali carenze e delle necessarie integrazioni: tanto più che l'Art. 18 del disegno di legge chiarisce che dall'attuazione delle sue disposizioni non derivano nuovi o maggiori oneri per la finanza pubblica e che le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni della stessa con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente. Occorre dunque prevedere che quanto previsto dal DDL venga realizzato con modalità e tempistiche attuabili. In tal modo i soggetti interessati potrebbero anche valutare meglio la disponibilità di fondi PNRR ed ACN per il finanziamento degli interventi necessari. Idem per quanto riguarda l'individuazione e/o la formazione ove necessario i soggetti preposti a fare da referenti: la gradualità potrebbe permettere una migliore selezione e preparazione.
- ***Ricorso a competenze esterne o ACN.*** Per poter identificare un incidente, e dunque segnalarlo, bisogna possedere soluzioni di cybersecurity state-of-art, adeguatamente progettate e opportunamente configurate. Il disegno di legge non prevede un'attività a monte

di guida e supervisione dell'ACN ma lascia alla singola le Pubblica Amministrazione (e dunque alla capacità delle singole persone) la possibilità di stabilire un opportuno livello di sicurezza. Sarebbe quindi opportuno prevedere tale attività di guida e supervisione.

Per poter velocizzare questa attività di analisi con i relativi interventi migliorativi si rende dunque necessario integrare in maniera sostanziale il personale specializzato nella sicurezza informatica di ogni Pubblica Amministrazione o addirittura ove necessario sopperire alle figure mancanti attraverso consulenze esterne (che possono essere provenienti da ACN o da aziende del settore identificate).

- ***Appuntamenti periodici dei referenti*.** Nell'ambito delle attività di guida e supervisione auspicate precedentemente sarebbe opportuno favorire degli appuntamenti periodici dei referenti della cybersicurezza degli enti pubblici di cui all'Art. 1, comma 1, con ACN/Polizia Postale/Anti-mafia/Anti-terrorismo al fine di creare cooperazione, ed avere aggiornamenti costanti sulle minacce riscontrate nel mondo e sul territorio Italiano. In questi appuntamenti dovrebbero essere altresì condivisi le minacce comunemente affrontate per una migliore mappatura di rischi, tecniche ed attori nonché i controlli da effettuare per verificare se tali minacce identificate mediante attività costanti di Threat Intelligence possono costituire una reale preoccupazione per le pubbliche amministrazioni ed evidenziare nel caso le "best practices" per indirizzare le soluzioni.

- ***Armonizzazione con la NIS2***. Considerata l'imminente attuazione, entro ottobre, della Direttiva NIS2, tra i cui soggetti destinatari vi è proprio la Pubblica Amministrazione, con obblighi ed azioni similari a quelle oggetto del disegno di legge in esame, diventa essenziale raccordare quanto in discussione con gli obblighi della Direttiva NIS2, per evitare il rischio di disallineamenti e/o sovrapposizioni.

Formazione a scuola

- Andando a proposte aggiuntive correlate ai temi del disegno di legge, aggiungiamo che per prevenire la carenza di figure specializzate nella cybersicurezza all'interno delle le Pubbliche Amministrazioni è essenziale trovare soluzioni efficaci sul piano della formazione.
- **Per far crescere la cultura generale della sicurezza informatica e poter aumentare il numero di laureati nelle discipline STEM - per le quali purtroppo l'Italia non eccelle in alcuna classifica internazionale, anche solo europea - è essenziale introdurre la materia della cybersicurezza sin dalle scuole medie (meglio ancora sarebbe dalle scuole elementari) dove i giovanissimi iniziano ad utilizzare dispositivi altamente tecnologici. E' solo in questi contesti, infatti, che possiamo accompagnarli ad un corretto utilizzo degli stessi e appassionarli alla materia e ridurre il gap fra utilizzo e consapevolezza dei rischio cyber che oggi connota fortemente l'utilizzo del digitale, soprattutto dei social, fra i giovani.**

  Anche l'introduzione di una ora a settimana dedicata, magari con il contributo di esperti di settore ed aziende del mondo privato disponibili a collaborare in tale direzione, costituirebbe un significativo passo avanti verso una maggiore sensibilizzazione e preparazione.