Audizione informale di Cisco Systems (Italy) Srl, in relazione all'esame del disegno di legge C. 2100 Governo recante conversione in legge del decreto-legge n. 105 del 2019 recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.

I Commissione - IX Commissione, 8 ottobre 2019

Dichiarazione di apertura

- Presidenti, Vicepresidenti, Membri delle Commissioni. È un onore essere qui oggi e accogliamo con favore l'opportunità di commentare questo importantissimo decreto legge che contribuirà ad aumentare la sicurezza e la resilienza delle infrastrutture critiche nazionali italiane.

- Cisco è il leader mondiale nelle tecnologie che trasformano il modo in cui le persone si connettono, comunicano e collaborano attraverso reti e architetture sicure ed intelligenti che integrano prodotti, servizi e piattaforme software. Pertanto, molte delle società che saranno soggette a questa legge sono nostri clienti e i nostri prodotti saranno soggetti a valutazione.

- Cisco è presente in Italia da oltre 25 anni e collabora con le istituzioni nel loro processo di digitalizzazione e contribuisce attivamente all'attuazione dell'Agenda digitale italiana. Ci impegniamo a sviluppare competenze digitali italiane con le nostre Networking Academies dove studiano circa 45.000 studenti all'anno.

- Il nostro CEO, Chuck Robbins, ha appena confermato al presidente Conte nuove iniziative strategiche di Cisco in Italia, per il periodo 2019-2022, per aumentare il livello di sicurezza informatica nel nostro paese, continuare a sviluppare competenze digitali e progetti di responsabilità sociale.

Posizione di Cisco sulla sicurezza delle infrastrutture critiche

- Le infrastrutture critiche sono essenziali per il funzionamento della nostra economia e società. Gli eventi che minano la riservatezza, l'integrità o la disponibilità dei servizi forniti dagli operatori di infrastrutture critiche e delle reti, i sistemi di informazione e i dati su cui esse si basano possono avere conseguenze devastanti.

- I Governi sono consapevoli di questo rischio e si sono concentrati su di esso - motivo per cui abbiamo visto l'adozione della Direttiva dell'Unione Europea sulla sicurezza delle reti e dei sistemi di informazione (Direttiva NIS) nel 2016. I cosiddetti operatori di servizi essenziali devono adottare misure di sicurezza tecniche e organizzative e denunciare incidenti di sicurezza. L'applicazione di queste misure è vigilata dalle autorità competenti.

- L'Unione Europea ha inoltre adottato il Cyber Security Act, che apre la strada alle certificazioni di sicurezza a livello europeo, ed incentrate sulla garanzia dei prodotti, del cloud e dell'IoT.

Visione Cisco e differenziazione sulla fiducia

- La missione di Cisco è garantire ai nostri clienti affidabilità, trasparenza e sicurezza e ci impegniamo a soddisfare questi standard ogni giorno inserendo la sicurezza nel tessuto stesso della nostra attività attraverso persone, processi, policy e tecnologia, con l'obiettivo unico di proteggere dati e infrastrutture. I nostri impegni principali sono:

- **Ciclo di vita dello sviluppo sicuro di Cisco**: Il ciclo di vita di sviluppo sicuro (SDL) di Cisco garantisce che la sicurezza sia integrata nei prodotti a partire dalla fase di progettazione, che la politica di sicurezza sia implementata in modo coerente per i prodotti dell'azienda e che i requisiti di sicurezza evolvano in base al panorama delle minacce.

- **Le tecnologie affidabili**, denominate trustworthy technologies, sono costruite tenendo conto delle minacce odierne e sono integrate in più soluzioni di Cisco. Questi componenti sono presenti nei nostri prodotti e convalidano l'integrità di un dispositivo dalla fase di avvio, fino ad arrivare alla fase di esecuzione del codice. Un processo ripetibile e misurabile che aumenta la resilienza e l'affidabilità del prodotto.

- **Sicurezza della catena del valore dei nostri prodotti**: il programma di approvvigionamento di Cisco include l'intera filiera produttiva, hardware e software, comprendendo i team di ingegneria, produzione e servizi tecnici per collaborare con fornitori globali e partner di canale per minimizzare il rischio di introduzione di software e componenti modificate e rendere difficile la contraffazione dei nostri prodotti.

- **Vulnerabilità e divulgazione dei dati**: la trasparenza è un elemento fondamentale per operare come partner di fiducia. Cisco si impegna fermamente nel fornire ai clienti tutte le informazioni necessarie per proteggere la propria azienda. Ciò significa fornire un accesso equo e simultaneo alle informazioni sulle vulnerabilità di sicurezza dei nostri prodotti per tutti, a livello globale. Questo viene fatto non solo segnalando le vulnerabilità rilevate da organizzazioni esterne, ma anche dichiarando tutte quelle che vengono trovate internamente.

- **Test rigorosi e affidabilità**: i clienti richiedono fiducia esplicita. Cisco dedica risorse significative per verificare che le nostre soluzioni passino rigorosi test di qualità e misure delle prestazioni in termini di sicurezza, affidabilità, protezione dei dati e privacy. Ad esempio, Cisco si avvale di un team interno di hacker etici che emulano attacchi così come farebbe un hacker esterno, per identificare debolezze nei prodotti e facilitare le azioni correttive prima che vengano immessi sul mercato.

- **Protezione dei dati e privacy**: la protezione dei dati e la privacy non devono limitarsi a termini e condizioni contrattuali. Cisco è focalizzata sull'aumento continuo di trasparenza, accuratezza, accessibilità e sicurezza dei dati. Per esempio, per molti dei nostri prodotti, forniamo ai clienti una mappa di processo dei dati (data map) che illustra il tipo di dati ricevuti ed elaborati dal prodotto, le operazioni effettuate, dove vengono salvati, il percorso all'interno dei nostri sistemi e chi ha accesso ai dati.

Decreto legge e raccomandazioni

- Supportiamo gli obiettivi e la direzione generale del "Decreto Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica". Vorremmo cogliere l'occasione per condividere con voi le nostre opinioni e osservazioni a riguardo.

Schema di test dei prodotti da parte del CVCN

- Riteniamo che lo schema di sperimentazione debba essere in grado di tenere il passo con la velocità dell'innovazione ed essere definito su un approccio rigoroso e basato sul rischio per testare e accreditare la tecnologia.

- I test dovrebbero essere svolti da personale CVCN, assistito da laboratori di prova qualificati, e condotti in collaborazione con il produttore e il gestore dell'infrastruttura critica in modo da definire una base di fiducia in cui tutte le parti hanno l'opportunità di comprendere gli interessi e le priorità dei vari attori coinvolti.

- I test dovrebbero richiedere ai produttori di facilitare la verifica dei criteri di sicurezza della progettazione e dell'implementazione dei prodotti utilizzati nell'infrastruttura critica. Ciò dovrebbe essere effettuato mediante prove ed ispezioni di tutti i componenti, compreso il codice sorgente, se necessario, come richiesto dalle autorità competenti.

- La valutazione della sicurezza di un prodotto dovrebbe includere anche una valutazione delle pratiche di sicurezza dei produttori, compresa la solidità delle loro pratiche di sviluppo sicuro e la loro trasparenza riguardo alle vulnerabilità, che è essenziale per assicurare resilienza ed integrità delle soluzioni.

- Per consentire efficienza e scalabilità ed evitare ritardi, i test dovrebbero:
  - Creare un percorso per la pre-approvazione di prodotti e soluzioni anziché solo un approccio reattivo post-approvvigionamento, caso per caso.
  - Rientrare in un quadro di riconoscimento reciproco a livello dell'Unione Europea basato su un modello di autorità incaricate all'autorizzazione e all'utilizzo delle tecnologie. Una volta approvata, dagli enti preposti, una tecnologia dovrebbe essere autorizzata in tutta l'Unione.
  - Gestire le iterazioni di prodotto testando solo la parte aggiornata di una release. Questo per superare la tensione tra la necessità di mantenere una assicurazione di sicurezza del prodotto e le implicazioni in termini di costi e ritardi nel dover verificare ogni versione nella sua interezza.

Requisiti degli operatori di infrastrutture critiche

- Sebbene la valutazione dei singoli prodotti sia un passo nella giusta direzione, raccomandiamo un approccio olistico che tenga conto del ruolo delle persone, dei processi e della tecnologia nella protezione delle infrastrutture critiche nazionali.

- La sicurezza non si esaurisce nel momento in cui un produttore immette un prodotto sul mercato. Il modo in cui l'operatore di Infrastrutture Critiche progetta, implementa, controlla, e gestisce reti e sistemi di informazione è cruciale.

- Un'architettura di sicurezza ben funzionante, resiliente e affidabile, può aiutare a prevenire, rilevare e reagire alle minacce cibernetiche.

- Un aspetto importante per creare un'architettura resiliente e sicura sono le soluzioni trustworthy (tecnologie intrinsecamente sicure). Queste soluzioni non solo riducono il rischio di compromissione dell'integrità e resilienza dovuta ad attacchi cibernetici ma possono aiutare gli operatori di rete a verificare l'integrità degli apparati una volta implementati all'interno di una rete. Esempi di componenti di soluzioni trustworthy sono: validazione di moduli crittografici; firme digitali del software che possono essere verificate in fase di esecuzione; avvio sicuro ancorato all'hardware per verificare automaticamente l'integrità del software; tecnologie (e processi) per verificare che l'hardware sia autentico e difese di run-time che aiutino a proteggere dagli attacchi basati su iniezione di codice malevolo durante l'esecuzione del software.

- Queste funzionalità sono fondamentali per mantenere la corretta postura di sicurezza e integrità dei componenti dell'architettura.

- Particolare importanza dovrebbe essere data anche alla gestione del ciclo di vita dell'architettura di sicurezza e dei suoi componenti. La gestione degli assets, degli aggiornamenti software e delle vulnerabilità è di fondamentale importanza. Le apparecchiature software e hardware alla fine del loro ciclo di vita devono essere considerate obsolete, dato che rappresentano uno dei maggiori rischi quando si tratta di garantire la sicurezza e la resilienza di un'architettura.

Dichiarazione di chiusura

- Desideriamo ringraziarvi ancora una volta per l'opportunità di commentare questo importante provvedimento e siamo a disposizione per collaborare con le Istituzioni che saranno incaricate di provvedere all'implementazione delle norme.

- Grazie per l'attenzione.