Memoria di Cisco

sulla

Comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza al Parlamento europeo e al Consiglio "La politica di ciberdifesa dell'UE" (JOIN(2022)49 final)

XIV Commissione Politiche dell'Unione Europea della Camera dei Deputati

Audizione del 31 maggio 2023

Cisco è tra le azienda leader a livello mondiale per le tecnologie per le infrastrutture e i servizi Internet.

Con l'invenzione del "router" a metà anni 80 abbiamo reso possibile la connessione tra reti di computer e di telecomunicazione eterogenee e dato il contributo fondamentale alla nascita e allo sviluppo di Internet.

Oggi, siamo un'azienda globale con 51B$ di fatturato, oltre 70.000 dipendenti, 600 dei quali in Italia, e siamo presenti in 140 paesi del mondo.

Ancora oggi stimiamo che la maggior parte del traffico Internet passi su apparati inventati e sviluppati da Cisco.

Cisco è un'azienda globale, con il suo quartier generale in California, ma ha, e ha sempre avuto, un'anima fortemente italiana, basti ricordare che:

- la linea dei prodotti per le reti locali, Cisco Catalyst viene dalla prima azienda acquisita da Cisco, nel 1993: la "*Crescendo Communication*" fondata da ingegneri ex Olivetti in California, gli stessi che per molti anni hanno guidato la crescita e la strategia di Cisco per le linee di prodotti più di successo.
- Nel 1999 abbiamo acquisito la *Pirelli Optical System*, oggi *Cisco Photonics di sede a Vimercate*, che, per la competenza degli ingegneri e ricercatori italiani è diventato il centro di eccellenza mondiale di Cisco per le tecnologie fotoniche e presto anche di Quantum Communication.
- Nel 2020 abbiamo acquisito la *Fluidmesh Network di Pisa*, startup nata dalle idee di 4 studenti nell' incubatore del Politecnico di Milano e che oggi rappresenta la soluzione più affidabile e sicura per le connessioni wireless in ambienti critici, quali miniere, porti e in mobilità ad alta velocità.
- La rivoluzione delle reti elettriche "intelligenti" è nata in Cisco Italia dalle intuizioni dei nostri team e dalla stretta collaborazione con ENEL e Terna, rendendo l'Italia un esempio mondiale nel campo delle Smart Grid.

Inoltre, da anni, Cisco Italy è impegnata a dare il suo contributo nello sviluppo dell'ecosistema digitale italiano cooperando con le Istituzioni e contribuendo attivamente alla realizzazione dell'*Agenda Digitale* nel nostro Paese. La dimostrazione concreta di tale impegno è il *programma di investimenti Digitaliani*, creato già nel 2016 per dare nuovi stimoli alla digitalizzazione del Paese e che ha visto Cisco investire Italia in progetti per infrastrutture strategiche, formazione, servizi digitali per il settore pubblico, per l'Impresa 4.0, la Sanità e il settore agroalimentare.

Sin dall'inizio abbiamo creduto che le tecnologie Internet avrebbero "*trasformato e migliorato il modo in cui viviamo, lavoriamo, studiamo e giochiamo*": la realtà "connessa "di oggi e la società digitale a cui aspiriamo, con tutti i suoi vantaggi e anche i limiti, ha confermato la nostra visione.

Abbiamo sempre investito nella ricerca e nell'innovazione, ogni anno spendiamo tra i 5 e 7 B$ in ricerca e, in questi 48 anni, abbiamo sviluppato e brevettato 35000 nuove tecnologie che sono oggi parte fondamentale delle reti di telecomunicazione dei service provider, delle reti delle Pubbliche Amministrazioni e della Difesa, dei collegamenti spaziali e sottomarini, nei sistemi di videoconferenza e di streaming video.

I nostri sistemi sono presenti in tutte le infrastrutture critiche e strategiche europee ed italiane.

Oggi la nostra strategia mira ad aiutare i nostri clienti a connettersi in maniera sicura, ad automatizzare i processi per accelerare la loro agilità digitale e a ridisegnare il modo in cui lavoriamo per essere più sostenibili per il pianeta[1].
Le soluzioni che oggi Cisco sviluppa e commercializza sono organizzate in 4 architetture principali;

- sistemi per reti cablate, ottiche e radio,
- video-collaborazione,
- data center e cloud
- cibersicurezza, nostra priorità e tecnologia trasversale a tutte le soluzioni, prodotti, applicazioni e servizi che progettiamo.

Cisco per la Ciberdifesa dell'Unione Europea

In Italia, a gennaio, è stato firmato un *Protocollo d'Intesa con l'Agenzia per la Cybersecurity Nazionale (ACN)* che prevede la collaborazione ad azioni comuni tese a prevenire attacchi informatici, a supporto della resilienza cibernetica e della sicurezza digitale del Paese. Gli ambiti di collaborazione previsti dall'intesa riguardano la *formazione, la condivisione di conoscenze tecnologiche, la ricerca e la cooperazione e lo scambio di informazioni e metodologie di analisi in tema di cyber threat intelligence*.

- Cisco mette a disposizione dell'agenzia l'esperienza dei 1.500 docenti delle 340 Cisco Networking Academy che operano in Italia con i loro percorsi specialistici in cibersicurezza e in altre discipline informatiche e che ogni anno formano 60.000 studenti.
- Cisco è pronta a condividere con l'Agenzia per la Cybersicurezza Nazionale il suo patrimonio di esperienza per la sicurezza di reti, per la protezione delle infrastrutture digitali critiche, dati e applicazioni e la threat intelligence e analisi delle minacce di Cisco TALOS.
- A ciò si aggiunge la disponibilità da parte di Cisco a collaborare ad attività di ricerca sulle nuove tecnologie per la sicurezza informatica.

Proprio per questi obiettivi e per collaborare con la ricerca e le aziende italiane abbiamo aperto a Milano nel 2020 il *Cisco Co-Innovation Center sulla Cybersecurity e Data Privacy* – parte della rete mondiale dei centri di innovazione di Cisco, il **primo in Europa** ad essere dedicato alla **sicurezza informatica e alla privacy.**
Cisco collabora con le principali Agenzie di Cybersicurezza ed Enti Governativi e della Difesa, e, in modo specifico, con le organizzazioni che studiano e definiscono i nuovi standard e framework per la confidenzialità, integrità e resilienza dei sistemi critici e strategici.

- I nostri specialisti di cybersecurity siedono nei workgroup di ENISA e portano la nostra esperienza nella definizione delle nuove certificazioni per gli apparati e servizi cloud per le infrastrutture

[1] https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-summary-2022.pdf

critiche: *European Common Criteria ed European Cloud Services and European 5G Schemes, previsti dall' European Union Cybersecurity Act*.

- Da diversi anni abbiamo accordi di collaborazione in ambito Cyber con la NATO[2], con i Ministeri della Difesa degli Stati Uniti e di altri Paesi Alleati.
- Negli Stati Uniti collaboriamo con il NIST, il CISA, l'NSA e FBI e in Europa con Interpol[3], Europol[4] e altre organizzazioni di sicurezza e di polizia.
- La nostra divisione di specialisti, analisti e ricercatori di cibersicurezza Cisco Talos è tra le più grandi organizzazioni non governative di Threat Intelligence con più di 500 specialisti, molti dei quali schierati oggi a difesa delle infrastrutture critiche Ucraine[5].
- Cisco Talos è focalizzata 24 ore su 24 alla ricerca di nuove minacce e vulnerabilità e, grazie alla nostra ampissima presenza nelle reti mondiali e alla collaborazione dei clienti che aderiscono ai nostri programmi di collaborazione e protezione, vantiamo la più ampia visibilità sul traffico internet e la maggiore quantità di dati telemetrici di sicurezza che ci permette di individuare i prodromi di molte delle nuove minacce informatiche e di informare e proteggere in nostri clienti aggiornando tempestivamente i loro apparati e sistemi di ciberdifesa.
- Abbiamo già disponibili soluzioni e tecnologie capaci di resistere agli attacchi informatici dei "futuri" Computer Quantistici.

La Comunicazione sulla politica di ciberdifesa dell'UE

Cisco accoglie favorevolmente la direzione intrapresa dall'UE in materia di ciberdifesa e ringrazia questa commissione e l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza per l'opportunità di fornire il suo contributo al documento di discussione sulle politiche e la strategia dell'Unione Europea. Si congratula con la Commissione Europea, il Parlamento e il Governo Italiano per l'attenzione che sta prestando nel definire una politica e una strategia vitale per la sicurezza e la difesa dei cittadini europei.

La Comunicazione contiene elementi chiavi per lo sviluppo dell'ecosistema cyber sia guardando all'ambito della difesa che a quello civile. Il pilastro chiave della Comunicazione è rappresentato dalla volontà di agire insieme per rafforzare la cyber difesa europea, potenziando il modello di governance politico militare europeo per la risposta alle crisi cibernetiche e i meccanismi di cooperazione dell'Unione Europea e dei Paesi Alleati, rafforzando lo scambio informativo e la cooperazione tra la comunità militare e civile pubblica e privata per sviluppare sistemi e competenze all'avanguardia e essere pronti a difendersi e a rispondere agli attacchi più sofisticati.

[2] https://www.ncia.nato.int/about-us/newsroom/nato-expands-cyber-partnership-with-industry.html
[3] https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2017/INTERPOL-and-Cisco-collaborate-to-combat-cybercrime
[4] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners
[5] https://blog.talosintelligence.com/fighting-the-good-fight-life-inside-the-talos-ukraine-task-unit/

1. Certificazioni Europee di Cybersecurity

Tra le azioni chiave menzionate dalla Comunicazione dell'UE sulla politica di ciberdifesa riteniamo essere cruciale "lo sviluppo e adozione di sistemi di certificazione della cibersicurezza a livello UE per l'industria della cibersicurezza e le imprese private".

- *In tal senso auspichiamo un'accelerazione nell' approvazione da parte del Parlamento e della Commissione Europea delle Certificazioni Europee di Cybersecurity EUCC (per gli apparati di rete), ancora in fase di revisione in ENISA.*
- *Analogamente, riteniamo si debba lavorare a livello europeo e possibilmente anche con i Paesi aderenti alla NATO, per uniformare le norme e le procedure di qualificazione, di screening e di auditing dei fornitori e dei servizi ICT, per il settore difesa, le infrastrutture critiche e anche quelli specifici degli altri settori di mercato.*

L'unificazione di tali processi permetterebbe di alleggerire il peso burocratico ed economico sui clienti e sui fornitori ed eliminerebbe, le diverse interpretazioni delle normative nazionali, semplificando i processi di qualificazione dei sistemi per le infrastrutture critiche e accelerando l'adozione di sistemi sicuri e affidabili.

2. Problemi sistemici e di mercato: partire dalle basi e tendere a una sicurezza pervasiva

È necessario dare piena attuazione agli interventi legislativi Europei e Italiani già previsti e intervenire con politiche di stimolo agli investimenti cyber in primis sui service provider e sui gestori delle infrastrutture critiche ma anche con azioni specifiche sulle pubbliche amministrazioni.

- I Service provider, che sono per definizione la struttura portante di tutte le reti di telecomunicazione, incluse quelle strategiche e di difesa, in Europa sono in un mercato caratterizzato dalla bassissima marginalità' e profittabilità, causati dall'ampia concorrenza che ha determinato un notevole abbassamento dei prezzi dei servizi che offrono[6]. Questo è sicuramente vantaggioso per gli utenti ma si traduce automaticamente in bassi investimenti in cibersicurezza. Molti ISP a causa di questi problemi concentrano i loro investimenti sui ciò che è più appetibile per il mercato: la cibersecurezza automaticamente passa in secondo piano: non è una loro priorità. *Ci auspichiamo che L'Unione europea agisca a tal riguardo con una politica mirata sui Service Provider per incentivare l'acquisizione di soluzioni di sicurezza all'avanguardia, aumentando in questo modo rapidamente la resilienza e le difese cibernetiche europee.*
- *In linea con quanto indicato dalla direttiva Europea NIS 2, condividiamo l'importanza di perseguire una* cibersicurezza di base comune a tutti i *sistemi ICT Europei , utilizzando tecnologie sofisticate e di qualità in modo pervasivo.*
  In tal senso, Cisco auspica che ENISA e ACN definiscano requisiti minimi di cybersicurezza, uniformi, chiari e obbligatori per tutte le tipologie di sistemi, applicazioni e servizi ICT per le Pubbliche Amministrazioni e le Infrastrutture Critiche in modo che tutte le centrali di acquisto pubbliche abbiano requisiti di gara allineati e consistenti. Gli attacchi informatici colpiscono gli anelli deboli delle reti, dove sono presenti sistemi non gestiti e a basso costo, per poi da lì raggiugere i nodi nevralgici.

[6] https://www.asstel.it/wp-content/uploads/2023/03/rapporto-sulla-filiera-delle-telecomunicazioni-2022.pdf

3. Sviluppo Sicuro e Sicurezza della Filiera dei Fornitori

Per alzare efficacemente i livelli di sicurezza e di difesa cibernetici europei, è essenziale disporre di un modello di responsabilità di sicurezza condivisa, in cui la tecnologia abbia basi sicure, sviluppo sicuro e operazioni sicure e gli utenti della tecnologia hanno l'obbligo di configurare, gestire e manutenere correttamente i propri sistemi IT e garantire che la propria forza lavoro sia adeguatamente formata sulle buone pratiche di sicurezza informatica.

- *Alla luce degli attacchi indiretti, sempre più sofisticati, che colpiscono le filiere dei fornitori per raggiungere poi obbiettivi strategici, crediamo sia importante lavorare sulle "tecnologie che permettono di garantire l'autenticità e la genuinità dei sistemi ICT", soprattutto quelli destinati alle infrastrutture critiche e strategiche.*
  In particolare, suggeriamo l'adozione di tecnologie di firma digitale peri il software, dei cosiddetti" Trusted Platform Module (TPM) che permettano di identificare univocamente e di controllare autenticità dell'hardware e del software su esso installato, proteggendoli da manomissioni da parte di terzi.
  L'uso di queste tecnologie è un elemento essenziale di una buona cibersicurezza e ***Cisco lo fa da più tempo di chiunque altro nel settore.***

A tal riguardo segnaliamo il documento " *Principles and Approaches for Security-by-Design and -Default*"[7] approvato lo scorso aprile dal CISA, FBI e NSA Statunitensi e dalle Autorità Nazionali di Cibersicurezza di Germania, Olanda, Australia, Canada, Regno Unito e Nuova Zelanda , come ottimo esempio di linee guida unificate per definire il concetto di "Sicurezza intrinseca" . Auspichiamo l'adozione di simili linee guida anche nelle prossime revisioni della regolamentazione per la sicurezza e la difesa dell'Unione Europea.

- Analogamente, abbiamo visibilità che molti sistemi ICT restano in esercizio anche dopo la data di fine supporto da parte del produttore, diventando altamente vulnerabili.
  A tal riguardo aiuterebbe normare in modo esplicito i processi di manutenzione evolutiva e le modalità di sostituzione dei sistemi ICT critici e strategici in esercizio per evitare che siano ancora in uso dopo la data di fine supporto da parte del produttore. Ciò ridurrebbe la vulnerabilità dei sistemi ad attacchi noti, ma che poi sono anche quelli più numerosi, e limiterebbe nel tempo le debolezze da questi generate.

4. Indipendenza Tecnologica e Sovranità digitale

Condividiamo l'aspirazione e gli obiettivi dell'Unione Europea di incentivare e investire nello sviluppo di tecnologie ICT all'avanguardia, e di padroneggiare in particolare quelle per la cibersicurezza e la ciberdifesa dei cittadini europei. Occorre colmare il gap tecnologico di risorse e conoscenze e ridurre la dipendenza strategica da paesi esterni nello sviluppo e produzione di componenti e sistemi elettronici, in particolare per la Difesa, per le infrastrutture critiche e per il settore ICT in generale.

[7] https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default

- *auspichiamo un' ampia e piena cooperazione con i Paesi Alleati nel contesto del partenariato strategico UE-NATO. La collaborazione con aziende all'avanguardia mondiale nella cibersicurezza, come la Cisco stessa, è un'opportunità chiave per lo sviluppo della stessa industria tecnologica europea, al fine di massimizzare gli sforzi e.*

Occorre accelerare il raggiungimento di un accordo tra Unione Europea e il Governo degli Stati Uniti d'America in relazione al *Regolamento Generale per la Protezione dei Dati Personali (n.2016/679)* e *Clarifying Lawful Overseas Use of Data Act* (o Cloud Act) e avere una posizione univoca Europea sulla localizzazione di dati e applicazioni oggi gestiti in Cloud da operatori non-Europei.

A tal fine potrebbe aiutare un approccio che distingua gli aspetti di diritto dagli aspetti tecnici: *la sovranità dei dati è fondamentale per ragioni economiche e di privacy ed è giusto far valere il diritto dell'Unione Europea ma ciò non deve essere confuso con un problema di buone pratiche di sicurezza. Una buona sicurezza deriva dalla progettazione, dallo sviluppo, dal funzionamento e dalla manutenzione di base e dall'utilizzo di approcci consolidati come ad esempio lo "Zero Trust".*

5. Cyber Solidarity Act e Cyber Skills Academy

La CDP fa anche riferimento alla c.d. Cyber Solidarity Initiative (CSI). In particolare, Cisco supporta con convinzione gli investimenti previsti dalla proposta di regolamento (UE) 2019/881 (c.d. "Cyber Solidarity Act"), che fornisce le basi per costruire una rete di centri operativi di sicurezza (SOC) nazionali e transfrontalieri ("European Cyber Shield"), nonché un meccanismo di emergenza informatica che consiste in servizi di risposta agli incidenti da parte di fornitori di fiducia pre-concordati.

A tal riguardo Cisco è pronta a replicare quanto già sta facendo con il suo team Talos in Ucraina per la difesa delle infrastrutture strategiche, l'analisi degli attacchi, la gestione degli incidenti e il ripristino immediato delle dorsali di telecomunicazione danneggiate.[8]

Cisco tramite il suo team di specialisti di cibersicurezza Talos, inoltre, risulta già qualificato dall' Istituto Federale per la Sicurezza Informatica delle Germania, per fornire supporto e competenze in caso di incidenti, attacchi cyber crisi informatiche estese.

Siamo inoltre pronti a formare il personale civile e militare dei SOC dei CSIRT con le nostre Academy e la nostra rete di partner e le nostre conoscenze. Condividiamo infatti la proposta sull'istituzione della Cyber Skills Academy a livello Europeo: rappresenta un elemento chiave per il rafforzamento dell'ecosistema cyber europeo. L'obiettivo dell'Academy è infatti simile a quello che abbiamo perseguito in questi anni con le Cisco Academy: riunire iniziative pubbliche e private per colmare il divario di talenti nel campo della cybersecurity come anche per le altre tecnologie ICT.

Cisco si sta già muovendo in questa direzione, infatti, durante l'incontro con il Vicepresidente della Commissione Margaritis Schinas a marzo, il CEO di Cisco Chuck Robbins ha annunciato **l'obiettivo di**

[8] https://blog.talosintelligence.com/ukraine-summary-report-cisco-talos-year-in-review-2022/

formare 250.000 studenti attraverso le Cisco Academy nei prossimi 3 anni per rafforzare le competenze di cibersicurezza nell' Unione Europea[9].

6. Cisco Cybersecurity Readiness Index e il divario di preparazione

Sebbene ci sia un ampio consenso sul fatto che il passaggio al lavoro ibrido sia destinato a rimanere, il suo successo a lungo termine dipende in larga misura dalla capacità delle organizzazioni di salvaguardarsi dalle nuove minacce in rapida evoluzione. A fronte di ciò, abbiamo voluto capire quanto le aziende di tutto il mondo siano pronte ad affrontare queste sfide. A tal fine, abbiamo sviluppato il Cisco Cybersecurity Readiness Index. L'indagine è stata condotta su un campione di **6.700 professionisti** che operano nell'ambito della cybersecurity, distribuiti su **4 continenti e in 27 paesi, fra cui l'Italia,**

Al termine dell'indagine le aziende sono state classificate secondo 4 gradi di maturità: da Iniziale, a Formativo, a Progressivo infine Maturo, sulla base della loro preparazione e adozione sui 5 pilastri fondamentali della protezione della cybersecurity: identità, dispositivi, rete, carichi di lavoro delle applicazioni e dati.

I risultati sono evidenti: secondo l'indice, **solo il 15% delle organizzazioni a livello globale è ritenuto in possesso di un livello maturo di preparazione** per gestire i rischi di sicurezza del lavoro ibrido. **In Italia, il livello di preparazione è ancora più basso, con solo il 7%** delle organizzazioni che rientrano nella fase di preparazione matura.

Come colmare il divario di preparazione in materia di sicurezza informatica?

La buona notizia è che i responsabili della sicurezza sono consapevoli dei rischi e sono desiderosi di investire nella loro preparazione in materia di cybersecurity: **l'87% delle organizzazioni italiane ha in programma di aumentare il proprio budget per la cybersecurity di almeno il 10% nei prossimi 12 mesi, rispetto all'86% a livello globale**. È fondamentale che questi aumenti di budget avvengano al più presto.

Nelle aree critiche, sono stati compiuti passi significativi per la sicurezza delle organizzazioni contro le minacce alla cybersecurity. Tuttavia, le organizzazioni di tutto il mondo – e forse anche i governi – devono riconoscere che la strada da percorrere è ancora lunga.

L'implementazione di alcune soluzioni, in particolare quelle per l'identità, i dispositivi e le reti, non sono state implementate con la rapidità che potrebbero, lasciando alcune organizzazioni vulnerabili agli attacchi.

Colmare il gap di preparazione deve diventare un imperativo globale e una priorità assoluta per i leader aziendali. Le organizzazioni hanno bisogno di resilienza in materia di sicurezza, concentrandosi su ciò che conta di più e anticipando ciò che sta per accadere.

Per costruire organizzazioni sicure e resilienti, i leader aziendali devono stabilire una base di riferimento per valutare quanto sono "pronti" nei cinque principali pilastri delle soluzioni di sicurezza.

[9] https://digital-skills-jobs.europa.eu/en/inspiration/pledges/bridging-cyber-skills-gap-cisco-networking-academy

Considerando l’ambiente in cui operano le aziende e l’attuale divario di preparazione, un’attesa di dodici mesi potrebbe rivelarsi troppo lunga. Ciò di cui le organizzazioni hanno bisogno è la resilienza della sicurezza, considerare cioè la sicurezza come fondamentale per la strategia aziendale e priorità collettiva in tutta l’organizzazione. La resilienza consiste nella verifica delle minacce, nella comprensione delle connessioni all’interno dell’organizzazione e nel vedere il contesto completo di ogni situazione, in modo che i team possano stabilire le priorità e assicurarsi di prendere la miglior decisione possibile.

7. Visibilità e automazione per una sicurezza più efficace

Cisco mantiene la su leadership di mercato attraverso quattro ambiti di interesse quali: Cloud, Cybersecurity, Reti, Sostenibilità, Futuro del lavoro grazie ad un processo di innovazione che passa da incrementale a essere basato sull’open innovation.

Nella cybersecurity nasce Cisco Security Resilience, con l’intento di garantire una gestione dinamica della sicurezza tramite una piattaforma aperta e completa, realizzata con il contributo del gruppo Cisco Talos, e dei specialisti e ricercatori.

La nostra visione in Cisco si basa sull’adozione di una piattaforma di sicurezza che chiamiamo Cisco Security Cloud. Astraiamo i controlli di sicurezza dall'infrastruttura sottostante e forniamo una visione completa dal momento in cui un utente fa clic su un'e-mail, lungo l'intera catena fino a quando un'applicazione accede ai dati. E quando disponiamo di questa visione della piattaforma end-to-end, possiamo fermare gli attacchi come il ransomware molto meglio di queste singole soluzioni per i punti di sicurezza. Ricordiamo infine le ultime due recentissime acquisizioni del 2023 quali Valtix e Lightspin per aumentare la sicurezza in ambito Cloud.