Audizione di Hewlett Packard Enterprise Italia sulla Comunicazione congiunta della Commissione 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) presso la XIV Commissione (Politiche dell'Unione Europea), Camera dei Deputati

17 maggio 2023

Egregio Presidente, Gentilissimi Onorevoli,

desidero innanzitutto ringraziarvi per l'opportunità offerta a Hewlett Packard Enterprise di essere audita sul tema della politica di cybersicurezza. Per noi è un onore e un piacere poter condividere il nostro posizionamento e il nostro contributo su un tema così importante come quello della cybersecurity che è sicuramente strategico a livello nazionale, europeo e internazionale. Considerando che l'azienda che ho l'onore di rappresentare potrebbe non essere conosciuta a tutte le persone presenti, prima di entrare nel merito della discussione, presenterò brevemente HPE:

Hewlett Packard Enterprise (HPE) è un'azienda leader globale nelle soluzioni di Cloud Ibrido e di Cybersicurezza con la sua sede principale a Houston, Texas e con un organico di circa 60 mila dipendenti nel mondo. Nel 1939 i due "padri" della

nostra azienda, Hewlett e Packard hanno fondato l'azienda nella Silicon Valley. Oggi, Hewlett Packard Enterprise è un'azienda globale che aiuta le organizzazioni pubbliche e private ad utilizzare i propri dati per far progredire il modo in cui le persone vivono e lavorano e costituisce una forza trainante nell'evoluzione della Cyber Security e nella convergenza di reti e sicurezza.

L'azienda offre una piattaforma che definiamo Edge-to-cloud con offerte che comprendono, oltre a quelle di Cybersicurezza, di cui vi parlerò brevemente oggi, anche servizi cloud, di elaborazione, HPC e AI, Storage e Data Management, Intelligent Edge, software che supportano le organizzazioni nell'accelerare i risultati sbloccando il valore di tutti i loro dati, ovunque si trovino. HPE propone soluzioni tecnologiche esclusive, aperte e intelligenti sia in modo "acquisto classico" e sia in modalità as-a-service con un fatturato a livello globale di 8B$. In questo modo l'azienda dà vita a un'esperienza coerente al modello cloud to the Edge, aiutando i clienti a sviluppare nuovi modelli di business e/o di servizio, interagire in nuovi modi e incrementare le prestazioni operative. Questo è quello che noi definiamo "Il Cloud che viene da te".

In Italia, siamo presenti da oltre 50 anni con circa 1000 dipendenti e collaboriamo con oltre tremila partner locali per mettere a punto soluzioni tecnologiche per Pubbliche amministrazioni e soggetti privati sostenendoli nello sviluppo di nuovi modelli e servizi digitali, sicuri e sostenibili.

Premessa e valutazioni generali: la politica di ciberdifesa dell'UE

Vorrei approfondire alcuni temi di particolare rilevanza che vengono menzionati nella Comunicazione su "*La politica di ciberdifesa dell'UE*", che mira a potenziare la capacità di ciberdifesa, **la capacità di prevenzione, rilevamento, difesa, recupero e deterrenza in relazione ad attacchi informatici rivolti contro l'UE e i suoi Stati Membri.**

Uno dei temi fondamentali che viene menzionato nella comunicazione (quale comunicazione?) è quello della **prevenzione e degli investimenti in capacità di ciberdifesa**. La prevenzione dev'essere vista da diversi punti di vista: *prevenzione nell'utilizzare delle tecnologie all'avanguardia* che includano sistemi di cybersicurezza di ultima generazione da fornitori di fiducia, *prevenzione nel fare valutazioni della vulnerabilità dei sistemi attuali* e *prevenzione nell'ambito delle competenze e di formazione.*

1. Le **capacità di computing, storage e networking** si sono evolute notevolmente negli ultimi anni. Le pubbliche amministrazioni hanno bisogno di adottare nuove capacità per sfruttare quanto più possibile il valore dei propri dati, per gestire la propria attività in modo efficace e competitivo e offrire i migliori servizi ai propri cittadini. Contemporaneamente, è aumentato anche il bisogno di soluzioni di sicurezza che aiutano le PA a comprendere e gestire i vari rischi che si presentano. Oggi questo significa navigare nella

complessità dei data center Multicloud e on-premise, insieme a dati in costante aumento all'Edge.

Proteggere le infrastrutture e i dati è possibile, ma **risulta necessario un approccio che includa l'intera vita di un'infrastruttura, dal silicio al cloud**. Anche prima che i server, lo storage e l'attrezzatura vengano assemblati, i materiali e i componenti devono essere attestati. Allo stesso modo, anche prima dell'avvio dell'infrastruttura, gli ambienti devono essere misurati e assicurati. E mentre i sistemi operativi e le applicazioni generano dati e producono risultati, la misurazione deve continuare e l'attestazione dell'ambiente sono fondamentali per mantenere l'integrità.

Per far fronte all'aumento della complessità ed essere un passo avanti con le minacce emergenti, c'è bisogno di integrare tecnologie e soluzioni Zero Trust per l'autenticazione dinamica di dati e applicazioni. Le funzionalità di sicurezza mantengono l'integrità dell'ambiente attraverso l'apprendimento, l'adattamento e l'evoluzione continui.

2. Un secondo aspetto della prevenzione è l'importanza di individuare nelle infrastrutture pubbliche e private quali sono le potenziali **vulnerabilità**. Questa valutazione permette di individuare i rischi interni ed esterni che le organizzazioni si trovano ad affrontare e permette di mettere in evidenza le

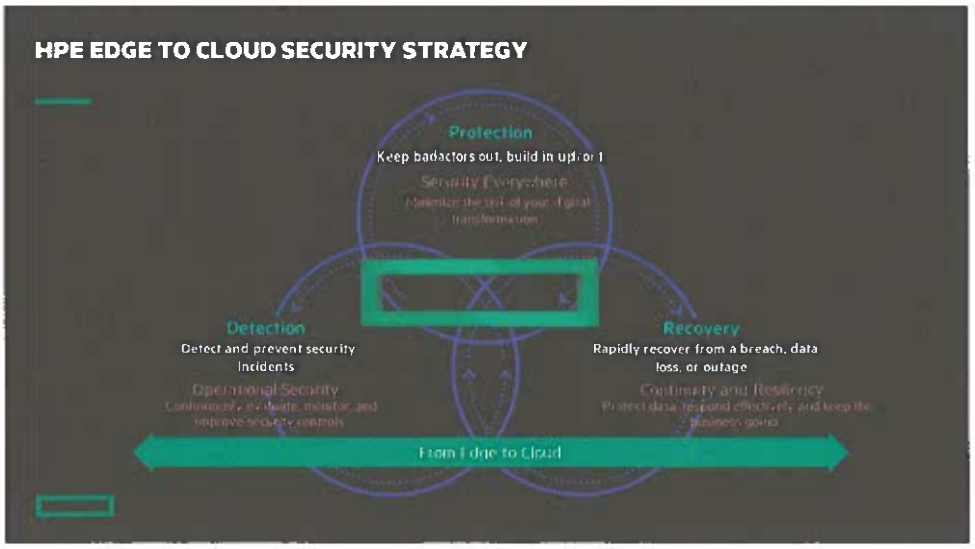
lacune. È di particolare importanza fare questi tipi di assessment per le infrastrutture critiche.

3. Ultimo aspetto, ma non per importanza, è quello delle **competenze**: la piena e integrata digitalizzazione sarà infatti possibile solo se, parallelamente all'implementazione delle infrastrutture e allo sviluppo delle nuove tecnologie, il Paese punterà sulla diffusione della cultura digitale tra la popolazione, versante sul quale scontiamo ancora un gap rilevante rispetto ai partner europei, come dimostrano i dati dell'Indice Desi 2022 della Commissione europea, che posizionano l'Italia al quart'ultimo posto nella classifica relativa alle competenze digitali di base.

A) CYBERSECURITY: Zero Trust Security Framework

- Grazie alle risorse del PNRR, uno degli obiettivi principali che l'Italia mira a raggiungere nei prossimi anni è sicuramente la **piena e integrata digitalizzazione dei servizi erogati dalle aziende e dalla PA.** La

conseguenza inevitabile è un aumento del rischio di attacchi informatici: secondo i dati dell'ultimo report dell'Osservatorio del Politecnico di Milano, l'Italia è passata dai 143 cyber attacchi nel 2018 a 2.553 nel 2020. Una tendenza confermata anche dal **Rapporto Clusit 2023**, che ha rilevato una crescita degli attacchi nell'ultimo anno pari all'8,4% rispetto all'anno precedente, ossia nel 2023, secondo il rapporto Clusit, si sono verificati in media 202 attacchi al mese. Ciò ha interessato in particolare il settore Finance/Insurance e la Pubblica Amministrazione, che rappresentano da soli circa il 50% dei casi. La nostra strategia in ambito sicurezza, che va dall'Edge al Cloud, copre 3 fasi fondamentali: il rilevamento e prevenzione della minaccia o dell'attacco, la protezione continua dei dati e la fase di Recovery in caso di attacco e ripristino in tempi rapidissimi del business aziendale.



- *Cyber security:* le minacce alla sicurezza di dati e servizi. La cyber security si occupa della protezione delle infrastrutture digitali e dei dati da esse ospitati: è uno degli elementi fondamentali della strategia di HPE. La sicurezza dei dati non dipende esclusivamente dalle tecnologie adottate per proteggerli dagli attacchi. Non basta affidarsi semplicemente alle soluzioni software disponibili - per quanto all'avanguardia – per assicurare la confidenzialità, l'integrità e la disponibilità delle informazioni. Assistiamo continuamente ad un rapido sviluppo di nuove minacce cyber con tecniche sempre più complesse. Le analisi a livello globale evidenziano come l'andamento relativo al numero di attacchi gravi superi le previsioni calcolate sulla media degli ultimi anni; Questo unito alla generale mancanza di consapevolezza dei rischi e delle conoscenze necessarie per gestirli, rendono indispensabile che le persone incaricate della sicurezza informatica sviluppino competenze specifiche e che le aziende adottino modelli organizzativi e procedure testate in situazione critiche. **All'interno di HPE esiste un Security Team** che, avvalendosi delle esperienze nella protezione delle infrastrutture e dei dati digitali dei propri clienti, fornisce le tecnologie, il know how e definisce i processi necessari a garantire una maggiore sicurezza informatica. HPE mette a disposizione un approccio completo alla cyber security basato sulla conoscenza del contesto, sulla cooperazione a livello italiano ed europeo per lo scambio di informazioni, sulla capacità di gestione della sicurezza informatica e su attività di promozione della cultura in oggetto. Gli esperti di HPE affiancano i clienti attraverso l'erogazione di servizi professionali per garantire l'allineamento

delle politiche di sicurezza alla strategia di migrazione al Cloud Ibrido attraverso attività di assessment, analisi del rischio e verifiche di conformità. Per garantire la sicurezza e il corretto accesso ai dati delle Amministrazioni, sono necessarie competenze e procedure per la definizione della migliore strategia di migrazione in sicurezza verso il Cloud computing. HPE fornisce strumenti a supporto dell'attività di valutazione e fattibilità della migrazione. Ciò avviene utilizzando un modello consolidato che prevede l'analisi dell'infrastruttura, l'identificazione di specifici obiettivi di performance e sicurezza, la definizione dello stato di adozione atteso, l'analisi dei gap attuali e l'identificazione e la pianificazione degli interventi da implementare. Nella prima fase viene valutata l'attuale postura in termini di sicurezza applicativa e infrastrutturale attraverso l'uso di specifici strumenti per identificare le vulnerabilità delle applicazioni web (Dynamic Application Security Testing) e condurre attività di Vulnerability Assessment sulle applicazioni esistenti. Durante tutte le altre fasi del progetto di migrazione viene effettuato il monitoraggio continuo delle attività e la valutazione del rischio, stilando e aggiornando un report che, in modo chiaro ed esaustivo, presenta gli indicatori relativi ai progressi compiuti. HPE ritiene che procedure specifiche e testate siano indispensabili, oltre che per una migrazione sicura verso il Cloud Ibrido, anche per la gestione dell'infrastruttura, dei dati e delle applicazioni.

- **HPE contribuisce ogni giorno e neutralizzare più di 250 miliardi di minacce** e ad emettere altrettanti aggiornamenti nei confronti dei clienti perché siamo qui oggi perché seguiamo con molto interesse la politica

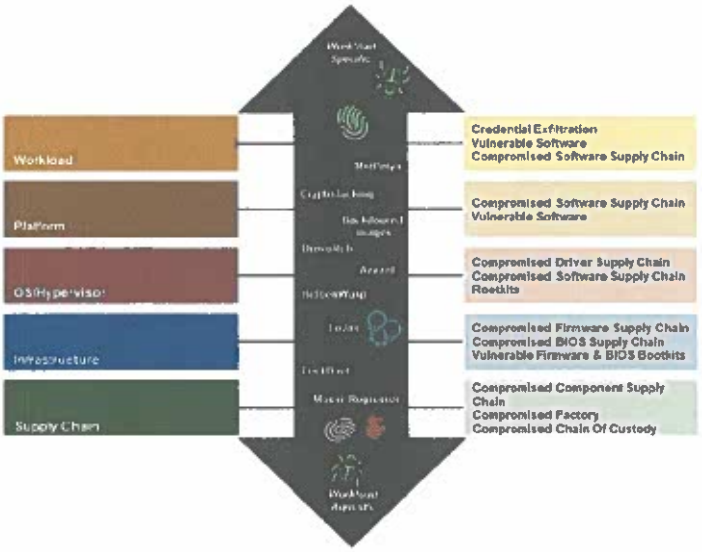
dell'Unione Europea ma soprattutto le evoluzioni del contesto normativo in ambito Nazionale questa attenzione nasce soprattutto al fatto che in Italia Siamo fortemente coinvolti nel processo di trasformazione digitale e nella costruzione del futuro digitale del paese insieme ai nostri partner e i nostri clienti; siamo infatti un produttore alla cui tecnologia servita al funzionamento delle principali infrastrutture ed aziende del paese. Inoltre, la nostra offerta è spesso integrata nella proposizione a valore dei maggiori fornitori di servizi digitali ed operatori di servizi essenziali. Quindi riteniamo di poter dare un contributo all'attuale dibattito dal nostro punto di vista di osservazione.

- Quello che notiamo e a cui stiamo assistendo oggigiorno è un aumento in velocità, in volume e in sofisticazione delle minacce: infatti c'è una superficie di attacco digitale in crescita in virtù dell'inevitabile e processo di digitalizzazione che non fa altro che aumentare il rischio Cyber. Le organizzazioni di tutto il mondo stanno espandendo e continueranno a espandere la propria rete con nuovi parametri definiti dal lavoro ubiquitario, dal lavoro da remoto e dai nuovi servizi Cloud dove si nota che i criminali stanno perfezionando le proprie strategie e stanno mettendo a punto nuove metodologie per sfruttare queste nuove aree di attacco. Sicuramente c'è il 5G che, come evidenzierò successivamente, è un elemento di attacco per la Cybersicurezza, ma c'è anche tutto l'ambiente domestico, gli attacchi Ransomware, tutta la rete internet satellitare, che sono altresì sempre più oggetto di attenzione dei criminali cibernetici.
- Questi elementi evidenziano quanto oggi sia importante per le Pubbliche

Amministrazioni, anche quelle locali, dotarsi di piani strutturali di cybersecurity e utilizzare tecnologie avanzate che garantiscono i massimi standard di sicurezza **mantenendo sul territorio italiano la gestione e la conservazione dei dati dei cittadini**, soprattutto quelli più sensibili.

- **Necessità di una Zero Trust Framework: HPE con il progetto Aurora porta avanti la strategia integrata nella piattaforma HPE As A Service GreenLake, che è stata interamente concepita per la sicurezza, a partire dalla supply chain, con funzionalità di protezione incorporate e integrate sin dal BIOS e dalle componenti elettroniche dell'infrastruttura a livello di circuito.** La piattaforma HPE GreenLake è infatti protetta da un'architettura "*zero trust*" progettata per verificare in modo automatico e continuativo l'integrità di hardware, sistemi operativi, piattaforme e carichi di lavoro, al fine di attestarne la sicurezza. Questa combinazione garantisce l'integrità dei

componenti, dalla fase di produzione e lungo tutta la supply chain, fino alla delivery, con una conferma basata sui principi "*zero trust*" al momento dell'avvio iniziale, prima di stabilire qualsiasi connessione alla rete aziendale. L'applicazione dei principi "*zero trust*" prosegue anche durante la delivery dei servizi, richiedendo un'attestazione regolare e persistente delle identità per tutte le attività, attraverso una componente software Open Source denominata SPIFFE/SPIRE. L'uso di una continua attestazione dello stato di sicurezza riduce notevolmente ad esempio problemi di furto biometrico e quindi il rischio di bypassare il riconoscimento facciale e le impronte digitali.



Source: Moor Insights & Strategy/HPE

B) a soluzione di HPE (Zerto) per risolvere in tempi rapidissimi gli attacchi Ransomware

- ***Rilevamento e recupero ransomware in tempo reale:*** ora che la stessa infrastruttura di ripristino di emergenza è un obiettivo di attacco, il

rilevamento in tempo reale è un must per qualsiasi moderna strategia di ripristino di emergenza. Qualsiasi soluzione che protegga i dati e i meccanismi di ripristino dovrebbe includere analisi comportamentali in tempo reale e analisi delle minacce in tempo reale. Le varianti di ransomware note condividono elementi comuni nel comportamento; pertanto, un rilevamento efficace in tempo reale non dovrebbe solo rilevare il ransomware in modo esplicito, ma dovrebbe anche rilevare comportamenti sospetti, che suggeriscono implicitamente l'attività del ransomware. L'analisi comportamentale può sfruttare l'apprendimento automatico per osservare comportamenti che assomigliano a trigger di ransomware, crittografia dei dati imprevista, tecniche di offuscamento e così via. Allo stesso modo, l'analisi delle minacce in tempo reale serve a mitigare le minacce, monitorando costantemente i perimetri della rete e intercettando il traffico, testando l'attività contro varianti note di ransomware e isolando e rimuovendo strategicamente le minacce sospette. Una soluzione che includa queste funzionalità è superiore a quelle che rilevano una minaccia solo nel momento in cui viene eseguito un backup. Il ransomware può facilmente provocare il caos in poche ore, paralizzando interi ambienti di produzione e garantendo che tutti i dati generati dall'ultimo backup giornaliero siano irrecuperabili.

- ***Protezione continua dei dati:*** mentre le minacce devono essere rilevate in tempo reale, i dati devono essere protetti continuamente, vale a dire 24 ore su 24. **I modelli di protezione continua dei dati (CDP) garantiscono alle organizzazioni la possibilità di monitorare e replicare**

continuamente tutte le modifiche ai dati, indipendentemente dalla granularità. In altre parole, ogni volta che un dato viene alterato in qualsiasi modo, una copia di quel dato viene immediatamente replicata per essere conservata al sicuro. I dati scritti in una posizione vengono scritti immediatamente e in modo asincrono in un journal. Grazie a questa replica finemente granulare e sempre immediata, qualsiasi dato può essere ripristinato in qualsiasi momento, indipendentemente dalla modalità e dai tempi in cui potrebbe essere stato compromesso da un utente malintenzionato. Una volta che i dati sono stati inizialmente sincronizzati, da quel momento in poi vengono replicate solo le modifiche apportate a tali dati. Nel contesto di un attacco ransomware, ciò significa che i dati compromessi possono essere ripristinati facilmente e rapidamente subito prima dell'attacco, rendendo inutili gli sforzi di crittografia dell'attaccante.

C) Connettività sicura anche nel 5G privato

In un mondo post-pandemico dove il lavoro ibrido è diventato la nuova normalità, è necessario un approccio differente alla sicurezza Edge di rete per proteggere le applicazioni SaaS critiche. **La piattaforma SSE (Security Service Edge) è un complemento naturale alle offerte SD-Wan, firewall di rete e segmentazione dinamica di HPE Aruba.** Insieme realizziamo una piattaforma SSE unificata, progettata per estendere la connettività dall'Edge attraverso una combinazione di servizi di accesso moderni, che lavorino tutti insieme in armonia. Gli operatori telco sono alla ricerca di soluzioni più semplici per implementare reti private 5G, così da soddisfare le crescenti esigenze dei loro clienti nell'ambito

dell'Edge connesso. Allo stesso tempo, i clienti Enterprise ci chiedono un'esperienza 5G personalizzata con bassa latenza, risorse criptate, copertura e sicurezza nei campus e negli ambienti industriali, a integrazione delle reti wireless esistenti. Con l'acquisizione di Athonet, HPE dispone di uno dei portfolio 5G e wi-fi privati più completi sul mercato, rivolto ai clienti Csp (Communication Service Provider) ed enterprise – che viene offerto in modalità as-a-service attraverso HPE GreenLake. HPE integrerà la tecnologia di Athonet nelle sue offerte per le Pubbliche Amministrazioni e per le Aziende Private per realizzare una architettura convergente che acceleri la trasformazione digitale Edge-to-cloud.

- **I vantaggi del 5G privato sicuro e aperto:** alle aziende che devono affrontare sfide complesse di connettività in ambiti vasti e in zone remote, il 5G privato offre livelli elevati di copertura, affidabilità e mobilità in particolare per campus e siti industriali. Inoltre, offre alle imprese nuove funzionalità ultrasicure, facili da implementare e gestire, pronte per applicazioni altamente specializzate come la robotica e l'IoT industriale, le reti e le canalizzazioni di dati e la semplificazione dei sistemi di sicurezza. L'integrazione della tecnologia di Athonet consentirà ad HPE – che si consoliderà così in un mercato che, secondo le previsioni di Idc, crescerà di oltre 1,6 miliardi di dollari entro il 2026 – di fornire funzionalità di rete privata per le imprese all'interno del portfolio di soluzioni di connettività di HPE Aruba.
- **La prospettiva di HPE sullo sviluppo delle reti 5G:** l'infrastruttura aperta garantisce più alti standard di sicurezza e di flessibilità. In particolare, il 5G aperto consente i più elevati livelli di sicurezza: per quanto riguarda gli

elementi di rete, la principale preoccupazione è rappresentata dalla possibilità di un data leakage verso entità straniere o di attacchi provenienti dall'interno della rete. L'architettura 5G di HPE assicura la piena trasparenza grazie all'architettura aperta, con tutte le Network Function implementate come componenti modulari, raggruppati a livello logico e costantemente monitorati e tracciati. Non avendo la nostra architettura delle "black box", gli operatori possono monitorare costantemente le prestazioni di ogni singolo componente ed i flussi di traffico che li attraversano, identificando ogni tentativo di sottrazione di informazioni o deviazione dalle solite prestazioni, dove il tutto avviene in real time. L'elemento della sicurezza è inoltre garantito dalle certificazioni dell'infrastruttura e dai software di gestione dei dati che sono open source, attestati da terze parti riconosciute a livello internazionale. Per i vendor, gli operatori mobili saranno liberi dal tradizionale lock-in che può causare problemi di sicurezza. Nel caso in cui una qualsiasi Network Function creasse sospetti, la disarticolazione della core network consentirà lo swap con una Network Function simile fornita da un altro vendor e ciò in tempi estremamente rapidi. Il 5G aperto interoperabile può essere complementare e sinergico con il Wi-Fi 6. Il 5G aperto consente di integrare, implementare e gestire le Radio Access Network utilizzando componenti, sottosistemi e software provenienti da più fornitori ORAN

D) CONCLUSIONI: Gaia-X e la sovranità del dato, la visione di HPE

- In linea con la nuova strategia europea sui dati, annunciata dalla

Hewlett Packard Enterprise

Commissione Europea a dicembre, HPE ha accolto con favore l'ambizione europea di beneficiare del valore generato dai dati industriali, contribuendo anche alla realizzazione del modello Gaia-X - un modello di cloud federato - in collaborazione con il governo tedesco.

- La **sovranità del dato** è un tema cruciale da non confondere col **concetto di autosufficienza**: il punto non è - chi - gestisce l'infrastruttura IT, ma, il potere di contrattazione che ha il fornitore digitale, specialmente in quei mercati altamente consolidati, come quello del mercato cloud pubblico. Il modello Gaia-X potrebbe costituire secondo HPE un modello valido per promuovere le 4 linee prioritarie promosse dal Consiglio Europeo
- Infatti, il **Consiglio europeo** nella riunione del **15 dicembre 2022** ha adottato delle **conclusioni** nelle quali, in particolare, ha **chiesto:**

  a) la definizione di una **politica forte dell'UE in materia di ciberdifesa**;

  b) **investimenti** per la cybersicurezza e la connettività spaziale, nonché per la resilienza delle infrastrutture critiche. La comunicazione congiunta delinea **quattro linee di azione prioritarie**:

  1. **promuovere un'azione comune** per rafforzare la ciberdifesa dell'UE rafforzando i **meccanismi di coordinamento fra attori nazionali e dell'UE**;
  2. **mettere in sicurezza l'ecosistema di difesa dell'UE**;
  3. **aumentare gli investimenti** in capacità di ciberdifesa;

4. promuovere **partenariati con Paesi terzi** per superare le sfide comuni.

D1) CONCLUSIONI in ambito Normativo e Legislativo

I suggerimenti relativi agli interventi normativi devono essere intesi come distribuiti tra le varie componenti delle legislazioni di pertinenza ed includono quindi proposte in merito ad attività in corso a **livello europeo** come pure a **livello nazionale**, incluse aree che possono essere di competenza della **normazione tecnica realizzata dalla ACN**.

Legislativo

- **Creazione di un coordinamento della messa in sicurezza delle infrastrutture critiche che appartengono a settori diversi, ma che possono essere collegati** (es. impatto di incidenti nel settore energetico sulle TLC, nelle TLC su altre reti, ecc.), anche in ottica di recepimento delle Direttive NIS2 e CER e in collegamento con future iniziative da adottare a livello comunitario sulla base della Policy on Cyber Defence
- **Individuazione e adozione a livello nazionale di KPI sulle tematiche di sicurezza Cyber ed analisi del rischio** che possano contribuire a fornire indicatori omogenei per le varie aziende/settori (iniziative già avviate con i decreti istitutivi della ACN)
- **Valutare la possibilità / necessità di intervenire sulla legislazione**

vigente **per favorire iniziative di bug bounty, vulnerability assessment** (attività che dovrà comunque essere svolta a fronte delle ultime evoluzioni delle norme europee)

- **Proporre la creazione del ruolo di responsabile della cyber security all'interno delle organizzazioni** (in analogia a quanto fatto per la sicurezza o per la protezione dei dati personali)

Norme tecniche per il PNSC (Perimetro Nazionale Sicurezza Cibernetica) e regole di procurement pubblico

- **Accelerare la realizzazione di un Knowledge DB sulle tematiche di sicurezza Cyber a cura di ACN** (attività in corso presso l'Agenzia della Cybersicurezza Nazionale)
- **Definire regole per maggiore uniformità nell'applicazione della Strategia di Cybersicurezza Nazionale sul materiale ICT acquisito per la P.A.** (*Quanto previsto sul tema Cybersicurezza nel decreto legislativo 31 marzo 2023, n. 36 è un passo nella giusta direzione; ma ACN dovrebbe definire dei requisiti di cybersicurezza, uniformi, chiari e facilmente implementabili per l'acquisizione di tutte le forniture in ambito ICT per la P.A., in modo che le centrali di acquisto pubbliche abbiano requisiti di gara allineati e consistenti)*
- **Normare più chiaramente e prioritizzare i processi di manutenzione evolutiva degli apparati e dei sistemi ICT critici al fine di mantenerli allo stato dell'arte verso le minacce più**

recenti. Definire regole chiare per le modalità di gestione e sostituzione di sistemi in esercizio dopo la data di fine supporto da parte del produttore al fine di ridurre / limitare nel tempo le vulnerabilità da questi generate.

- **Proporre principi condivisi / indicare priorità o criteri di validità dei principi per la protezione di reti, applicazioni, *endpoint* ecc.** *(ad es. Zero Trust, micro-virtualizzazione, ...)*

Verifiche e Certificazioni

- **Accelerare l'approvazione da parte del Parlamento e della Commissione Europea delle Certificazioni Europee di Cybersecurity EUCC (per gli apparati di rete) ed EUCS (per i servizi cloud)** al fine di ridurre il carico amministrativo e tecnico dei produttori di sistemi ICT / fornitori di servizi cloud che devono essere contemporaneamente conformi alle regolamentazioni dei 27 paesi dell'Unione ed a quelle di altri Paesi nel Mondo.
- **Promuovere le attività di standardizzazione di ENISA, CEN, ETSI,** ecc. e le relazioni con gli omologhi enti internazionali per razionalizzare e fare convergere standard e certificazioni ICT /cloud.
- **Uniformare le norme e le procedure di qualificazione, screening e di auditing di affidabilità' e sicurezza dei fornitori di servizi e sistemi ICT**, almeno per settore di mercato allo scopo di evitare l'inutile ripetizione di queste attività, con un notevole risparmio di tempo e risorse e la velocizzazione nel processo di acquisizione di sistemi ICT aggiornati.

- **Continuare il processo di valutazione ed ottimizzazione delle attività di certificazione (a cura CVCN) per renderle snelle, essenziali ed orientate al business,** definendo, in particolare, una versione semplificata del processo per i prodotti che sono dotati di certificazione di cybersicurezza in base ad uno schema di certificazione già approvato a livello nazionale o europeo
- **Promuovere, attraverso l'azione ed il coordinamento dell'ACN, lo sviluppo degli ISAC (Information Sharing Analysis Center) settoriali**, da utilizzare anche come piattaforme per la creazione di piani di confronto tra gli operatori di settore e tavoli di lavoro settoriali / intersettoriali per il co-investimento pubblico privato su tecnologie specifiche di difesa, continuità operativa e risposta agli incidenti (v. anche para. 2)

D2) Conclusioni in ambito di investimenti ed incentivi

Prevedere opportune forme di incentivazione / finanziamento *(a titolo di esempio: deduzioni e/o detrazioni fiscali; riduzione IVA su acquisti; finanziamenti a tasso o e/o agevolato; contributi a fondo perduto totali e/o parziali; tassazione agevolata sul costo del lavoro e sugli stipendi)* per l'implementazione di azioni di miglioramento della cybersicurezza, a seconda del tipo di attività e del destinatario.

Di seguito una proposta di aree prioritarie / rilevanti per la definizione di politiche / strumenti del tipo indicato:

- **Definire incentivi per il rafforzamento della cybersicurezza di**

imprese e pubbliche amministrazioni, concentrandosi soprattutto sui settori più sensibili (ad es. il settore sanitario) anche ad estensione degli interventi previsti in ambito PNRR. *(ad esempio, definire sistemi di incentivazione per gli investimenti necessari ad incrementare il livello di riservatezza, confidenzialità e il controllo degli accessi alle informazioni aziendali e personali e per soluzioni di difesa dagli attacchi cibernetici più frequenti, es. protezione anti-ransomware ma anche sistemi di backup)*

- **Includere nelle categorie per investimenti in beni materiali e immateriali previste da Transizione 4.0 anche i beni strumentali alla sicurezza informatica di macchine, computer, reti e infrastrutture.**

- **Includere nelle categorie previste da Transizione 4.0 anche tutti i servizi di cybersecurity (progettazione, implementazione, servizi gestiti, ...) necessari per la messa in sicurezza delle soluzioni realizzate**

- Definire incentivi a sostegno dei costi sostenuti dalle aziende per l'acquisizione di strumenti e risorse finalizzate a migliorare e rendere sempre più efficaci le attività di esercitazioni e test svolti al fine di migliorare la risposta in caso di incidente di sicurezza

Nello specifico ambito dei soggetti appartenenti al PNSC e/o al perimetro NIS2/CER, **individuare progetti di carattere nazionale, da finanziare con fondi pubblici e incentivi alle imprese per contribuire alla copertura degli oneri necessari per adeguare le operazioni alle normative nazionali ed europee, garantendo il livello di sicurezza da queste atteso.**

Gli ambiti di intervento potrebbero essere, a titolo di esempio: **formazione ed esercitazioni virtuali, piattaforma nazionale per la *threat intelligence*, ambienti di test simulati e condivisi, federazione di SOC (eventualmente in collegamento alle iniziative europee) e supporto alla gestione di crisi (eventualmente in collegamento a EU-Cyclone), utilizzo di tecnologie nazionali in vari ambiti** *(es. protezione endpoint, sandbox, crittografia, . ..)*, protezione delle infrastrutture di telecomunicazione[1], interventi sui costi del personale (interno o esterno) per le figure professionali particolarmente critiche *(ad esempio Analista Cyber, Ethical Hacker, Cyber Engineer, security Architect),* "rottamazione" di prodotti obsoleti e/o particolarmente critici *(es. di provenienza da paesi segnalati come a rischio),*

D3) CONCLUSIONI sul Finanziamento della Ricerca e sovranità tecnologica

Hewlett Packard Enterprise

Prevedere il finanziamento di attività volte alla costruzione del livello di indipendenza atteso nell'ambito delle tecnologie cyber e desiderato (da definire a cura delle istituzioni e in collaborazione con l'industria) sia mediante contributi all'attività di ricerca, sia mediante un utilizzo mirato della leva offerta dal procurement pubblico e/o dalle normative di compliance per i settori critici.

Di seguito una proposta di aree prioritarie / rilevanti che dovranno essere affrontate, avendo individuato i temi da approfondire / le tecnologie da sviluppare:

- **Finanziare l'attività di Ricerca e Sviluppo in ambito cyber, a partire dagli incubatori universitari,** anche intervenendo sulla legislazione per favorire le attività di test *(es. sandbox etc.)* allo scopo di creare proprietà intellettuale italiana da utilizzare per applicazioni sensibili a livello nazionale, ma anche per avviare un percorso di posizionamento a livello globale rispetto ai maggiori player di mercato

- **Definire politiche di procurement che richiedano, nel perimetro PNSC e/o NIS2/CER, un contributo nazionale, non necessariamente esclusivo,** in termini di tecnologie e/o di fonti dati, e orientare gli investimenti pubblici anche verso lo sviluppo di nuove soluzioni tecnologiche che consentano all'Europa di rafforzare la propria autonomia digitale *(es. Open RAN, architettura tecnologica delle reti TLC che consente di non dover dipendere da un unico fornitore integrato*

verticalmente) (siamo sicuri che tutta l offerta hpe sia nis2 READY?)

- **Sostenere gli investimenti privati e incentivare l'utilizzo delle tecnologie avanzate come l'intelligenza artificiale** e il *Quantum Computing* che potranno garantire un rafforzamento della cybersicurezza dell'intero sistema Paese, inclusi i soggetti più fragili ed esposti come le PMI

- **Promuovere una strategia comune dell'Unione Europea sulla localizzazione dei servizi cloud e dei dati**, anche alla luce delle attività di normazione e di discussione con i paesi alleati (es. Data Act, DMA, DSA, EU-U.S. Data Privacy Framework, EU/US TTC)

- **Creare un catalogo delle soluzioni tecnologiche e servizi a supporto UE** (i.e. tecnologie sviluppate da aziende europee e ospitate in paesi occidentali della UE)
- **Favorire la diffusione di tecnologie e soluzione cyber UE attraverso incontri dedicati**
- **Introdurre incentivi per lo sviluppo di start-up in ambito cybersecurity**, incluso l'avvio di un fondo strategico o di un piano di co-investimento pubblico privato per lo sviluppo di soluzioni tecnologiche destinate alla sicurezza cyber (attività in corso da parte di ACN e da supportare / finanziare)

- **Promuovere il ruolo dei centri di competenza / centri di innovazione in ambito cybersecurity**, al fine di mettere a sistema le competenze del settore privato, del mondo dell'università e della ricerca e di istituzioni pubbliche quali l'Agenzia per la Cybersecurity

D4) CONCLUSIONI per migliorare le competenze in ambito cybersicurezza

Prevedere azioni coordinate e significative per l'educazione diffusa (tutti i cittadini), di base (sistema scolastico), specialistica (università) e professionale (aziende, cyber academy), coordinando le azioni anche con le analoghe attività in sviluppo a livello Europeo *(es.* Cyber Skills Academy https://digital-skills-jobs.europa.eu/en *promossa nell'ambito della piattaforma europea di skill building).*

Di seguito una proposta di aree prioritarie / rilevanti che dovranno essere sviluppate:

- **Approfittare delle iniziative dell'anno europeo delle skills 2023,** e delle iniziative connesse come il Pact for Skills, per ammodernare il parco di conoscenze sia nell'ambito scolastico che imprenditoriale, ideando e sostenendo percorsi di formazione strutturati a tutti i livelli, dalla scuola dell'obbligo alle università, anche in collaborazione pubblico-privato, favorendo

un approccio sistemico quale, ad esempio, la creazione di esercitazioni congiunte

- **Incrementare, nel generale quadro mondiale di attacchi alla componente umana della cybersecurity**, la ricerca di soluzioni che mitighino il problema *(ad es. istituire, in connessione ai fondi del PNRR ed in collaborazione con i centri di ricerca e competenza sul territorio, un solido e trasversale programma di alfabetizzazione dei cittadini verso le nuove tecnologie e la relativa necessità di cybersicurezza)*

- **Estendere le risorse dei voucher PMI per la formazione in ambito cyber al fine di aumentare il livello di competenze nelle imprese italiane** ed ampliare il novero dei soggetti a cui è possibile commissionare attività di formazione ammissibili al credito d'imposta, includendo le aziende che sviluppano possono erogare corsi in materia di cybersecurity, al fine di colmare il gap di conoscenza presente nel mercato del lavoro, contribuendo agli obiettivi di Formazione 4.0

- **Istituire finanziamenti e/o ridurre le imposte per percorsi formativi sia a livello ISS sia a livello universitario** per nuovo personale e per attività di upskilling trasversali rispetto ai settori industriali per il personale già in forza

- **Promuovere campagne di cyber awareness e cyber hygiene destinate ai non addetti ai lavori** (o direttamente gestite da ACN o in PPP).