Audizione di Hewlett Packard Enterprise Italia sull'esame del disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (AC 1717)

Commissioni riunite, I Commissione Affari Costituzionali e II Giustizia, Camera dei Deputati

26 marzo 2024

Presentazione di HPE

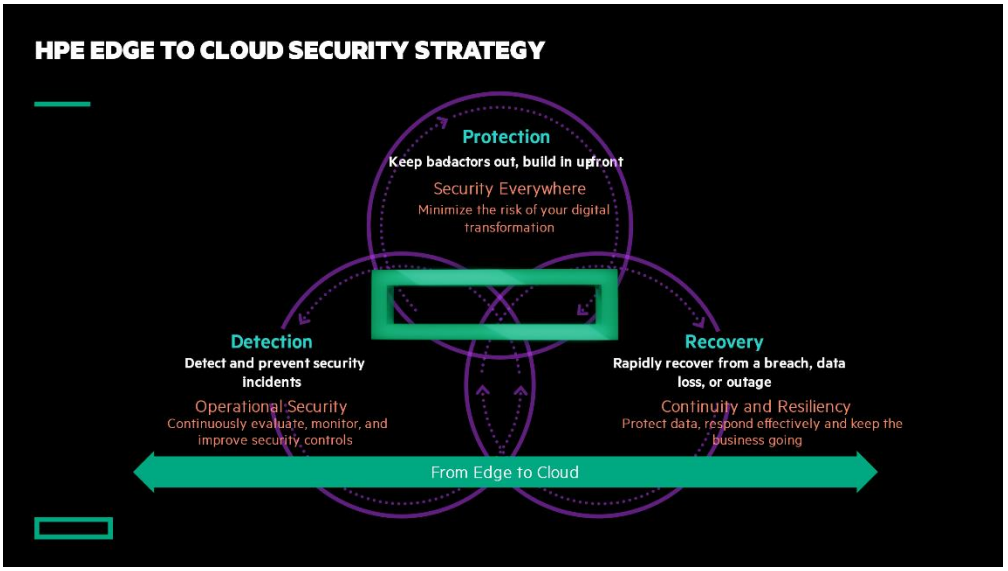
Hewlett Packard Enterprise (HPE) è un'azienda leader globale nelle soluzioni di Cloud Ibrido, Supercomputing e Artificial Intelligence, Networking e Cybersicurezza con sede principale a Houston, Texas e con un organico di circa 60 mila dipendenti nel mondo. Nel 1939 i due "padri" dell'azienda, Hewlett e Packard, l'hanno fondata nella Silicon Valley. Oggi, HPE è un'azienda globale che aiuta le organizzazioni pubbliche e private a utilizzare i propri dati per far progredire il modo in cui le persone vivono e lavorano e costituisce una forza trainante nell'evoluzione della cybersecurity e nella convergenza di reti e sicurezza.

L'azienda offre una piattaforma definita **Edge-to-cloud** con offerte che comprendono, oltre a quelle di cybersicurezza, anche servizi cloud, HPC e AI, Storage e Data Management, Intelligent Edge e 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" 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 con il modello cloud to the Edge, aiutando i clienti a sviluppare nuovi modelli di business e/o di servizio, a interagire in nuovi modi e a incrementare le prestazioni operative. Questo è quello che viene definito "Il Cloud che viene da te".

In Italia, HPE è presente da oltre 50 anni con circa 1000 dipendenti e collabora con oltre tremila partner sul territorio per mettere a punto soluzioni tecnologiche per Pubbliche

amministrazioni e soggetti privati, sostenendoli nello sviluppo di nuovi modelli e servizi digitali, sicuri e sostenibili.

La strategia di HPE sulla Cybersecurity



La strategia di HPE in ambito sicurezza, che va dall'Edge al Cloud, copre 4 fasi fondamentali:

a) Prevenzione degli attacchi

b) Protezione continua dei dati

c) Ripristino rapido del servizio (in caso di attacchi andati a buon fine)

d) Connettività sicura.

Considerazioni relative all'art. 10 del disegno di legge

Riteniamo molto importante l'attenzione dedicata, all'interno del disegno di legge, alla definizione di **criteri di cybersicurezza da tenere in considerazione in relazione alle attività di approvvigionamento di beni e servizi informatici** impiegati in settori connessi alla tutela degli interessi nazionali strategici.

Per fare in modo che questi criteri siano efficaci e utilizzabili per tutti i diversi casi d'uso che

riguardano la sicurezza informatica è fondamentale, nella fase di attuazione del ddl - che prevede l'adozione di un decreto del Presidente del Consiglio dei ministri, entro centoventi giorni dalla data di entrata in vigore della legge, su proposta dell'Agenzia per la cybersicurezza nazionale, previo parere del Comitato interministeriale per la cybersicurezza - tenere in considerazione tutte le quattro fasi della strategia di cybersecurity:

a) **Prevenzione degli attacchi**

   È prioritario adottare una normativa specifica che riguardi **la sicurezza in caso di acquisizione di beni** e che preveda di:

   - acquisire infrastrutture che prevedano in fase di produzione una **supply chain sicura e certificata** in modo da evitare che il sistema arrivi già compromesso in termini di sicurezza ancora prima di essere collegato alla rete,

   - **incentivare l'adozione di architetture "Zero trust",** attraverso l'utilizzo dell'Intelligenza Artificiale per monitorare il cambio di identità IT, automatizzare azioni di prevenzione e blocco del servizio e ripristino dell'identità iniziale ("Fingerprint");

   - **prioritizzare i processi di manutenzione evolutiva degli apparati e dei sistemi ICT critici**, al fine di mantenerli sempre aggiornati verso delle minacce più recenti (es. 1 cybersecurity audit all' anno);

   - **definire regole chiare per la sostituzione di apparati dichiarati in fine supporto da parte del produttore** (hardware/ software), poiché dopo il fine supporto non vengono più rilasciati aggiornamenti di sicurezza.

b) **Protezione dei dati**

   Nel caso di acquisizione di servizi IT in contesti nazionali strategici, **è fondamentale prevedere che i dati restino di proprietà dell'ente**, in linea con la strategia dell'Unione Europea.

c) **Ripristino rapido del servizio** (in caso di attacchi andati a buon fine)

   È molto importante che la nuova normativa ponga l'accento sulla necessità di adottare soluzioni di **Disaster Recovery**, che permettono di ripristinare rapidamente ed

efficientemente il servizio. Tali soluzioni devono essere il più possibile aperte in modo da evitare lock-in.

d) Connettività sicura

Grande attenzione deve essere posta anche sull'utilizzo, da parte di tutti gli attori che operano in settori connessi alla tutela degli interessi nazionali strategici, di **infrastrutture digitali che garantiscano i massimi standard di sicurezza**. La connettività sicura rappresenta infatti un elemento fondamentale perché le reti sono il punto di ingresso di tutti i possibili attacchi.

Raccomandazioni di carattere generale

Come HPE, riteniamo fondamentale **favorire maggiormente la collaborazione tra attori pubblici e privati per rafforzare tutti insieme la sovranità tecnologica e digitale del nostro Paese**, attraverso una serie di misure finalizzate a implementare i sistemi di sicurezza di aziende e PA e a potenziare le *soft skills* del capitale umano diffondendo la cultura digitale. In particolare, è prioritario:

- **finanziare attività di ricerca e sviluppo in ambito cyber**, a partire dagli incubatori universitari e le startup, in modo da garantire una maggiore indipendenza nazionale sulla cybersicurezza. Sotto questo profilo, il nostro Paese potrebbe prendere spunto da una serie di best practice internazionali, come ad esempio il modello di Israele;

- **definire un coordinamento relativo alla 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 europeo sulla base dell'EU Cyber Defence Policy Framework;

- **individuare dei KPI, a livello nazionale, sulla sicurezza cyber e sull'analisi del rischio** che possano contribuire a fornire indicatori omogenei per le varie aziende e i diversi settori (iniziative già avviate con i decreti istitutivi della ACN);

- **adottare 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.