Incontro con l’Area Chief Security Officer

Il 15 aprile 2026 si è svolto un importante incontro tra le Organizzazioni Sindacali e i vertici dell'Area Chief Security Officer (CSO) del Gruppo Intesa Sanpaolo. Al centro del confronto, la presentazione della nuova struttura organizzativa e le linee guida del Piano Industriale 2026-2029, un percorso che punta a ridefinire radicalmente il concetto di sicurezza all'interno della nostra Banca in un panorama globale caratterizzato da crescenti tensioni geopolitiche e da un'evoluzione tecnologica senza precedenti. L'incontro ha permesso di approfondire la riorganizzazione avviata nell'ottobre 2024 sotto la guida dell’Area da parte del Generale Antonio De Vita.

L'evoluzione dei rischi odierni impone il **superamento della vecchia distinzione tra sicurezza fisica e digitale**, muovendosi verso una visione strategica e integrata che metta a fattor comune le competenze di Cybersecurity, Antifrode e Sicurezza Fisica, garantendo al contempo una netta segregazione tra chi implementa le soluzioni informatiche e chi ha il compito di monitorarle.

Questo cambio di paradigma trova la sua espressione nel progetto del Global Defence Center Integrato, un'evoluzione naturale dei presidi esistenti che mira anche a internalizzare attività storicamente delegate a fornitori esterni. **In questo scenario, assume particolare rilievo la scelta di Napoli come nuova sede operativa strategica**. Questa decisione non risponde solo a criteri logistici, ma punta a valorizzare l'ecosistema territoriale del Mezzogiorno attraverso partnership con poli universitari di eccellenza, affiancandosi al rafforzamento delle sedi storiche di Milano e Torino. Il piano prevede un investimento significativo sul capitale umano: **sono previste 60 nuove assunzioni e il reskilling di 40 colleghe e colleghi**, con l'obiettivo di riappropriarsi di competenze chiave e tutelare il know-how aziendale.

Sul fronte della protezione dei dati, il Gruppo sta adottando **l'approccio "Zero Trust"**, un modello che non concede fiducia “informatica” implicita a nessun dispositivo o credenziale, ma introduce la verifica esplicita e continuativa dell’identità e dei dispositivi. Se da un lato questo comporta l'introduzione di misure stringenti come il blocco delle porte USB o controlli più rigidi sugli accessi remoti — con un impatto inevitabile sull'esperienza d'uso quotidiana — dall'altro è dichiarato dall’azienda fondamentale per tutelare i dipendenti stessi da potenziali responsabilità derivanti, ad esempio, da fughe di dati.

Parallelamente, la **Travel Security** si conferma un presidio di eccellenza, con oltre 19.200 trasferte gestite nel triennio precedente e un ulteriore potenziamento previsto per garantire la massima assistenza h24 ai colleghi operanti all'estero.

L'introduzione dell'Intelligenza Artificiale nella gestione di compiti di "primo livello" rappresenta una sfida che il Gruppo dichiara di voler governare per gestire i grandi volumi di minacce, permettendo ai colleghi specializzati di concentrarsi sulle situazioni di reale emergenza.

Infine, l'azienda afferma che **la cultura della sicurezza diventerà un patrimonio diffuso** attraverso simulazioni, podcast dedicati come "L'arte della difesa digitale" e programmi di formazione che coinvolgeranno tutti i livelli, dai vertici aziendali alle fasce più vulnerabili della clientela.

Come Organizzazioni Sindacali riteniamo positivo che l'azienda abbia sottolineato come la sicurezza non debba mai essere vista come un costo ma semmai come un investimento; e accogliamo con estremo interesse il **processo di internalizzazione delle competenze** e delle attività di Security Operations Center. **Riappropriarsi delle professionalità e investire in nuove assunzioni** è la strada corretta per garantire solidità al Gruppo e dignità alle altissime professionalità delle colleghe e dei colleghi.

Tuttavia, vigileremo con estrema attenzione su alcuni punti che riteniamo critici per il benessere dei lavoratori:

- **Qualità del Reskilling**: i 40 percorsi di riconversione interna non devono essere semplici passaggi burocratici, ma devono poggiare su una formazione di alto livello che fornisca alle colleghe e ai colleghi strumenti reali per affrontare la complessità del nuovo ruolo.
- **Impatto Operativo dello "Zero Trust"**: comprendiamo la necessità di proteggere i dati, ma le misure di sicurezza non devono trasformarsi in un ostacolo insormontabile alla produttività quotidiana. Chiediamo che l'azienda monitori costantemente il "carico cognitivo" e i rallentamenti operativi che queste procedure possono generare, intervenendo per fluidificare i processi dove necessario.
- **Valorizzazione del Mezzogiorno**: il progetto sulla sede di Napoli è un'occasione d'oro per il territorio, che auspichiamo possa ripetersi anche altrove. Chiediamo che questo impegno si traduca in reali percorsi di crescita e che le partnership universitarie portino a un inserimento stabile sempre maggiore di giovani professionisti.

La sicurezza è un bene comune che, per essere veramente efficace, necessita di fiducia: non può essere perseguita a discapito della qualità della vita lavorativa delle colleghe e dei colleghi, ma deve essere a supporto dei processi operativi garantendo protezione attiva anche a tutela della corretta operatività quotidiana in temi di privacy e accesso alle risorse e ai dati aziendali e, a questo proposito, serve anche maggiore chiarezza e semplificazione delle normative. Continueremo a presidiare attivamente questi temi affinché l'Area CSO diventi davvero un modello di eccellenza non solo tecnologica, ma anche di protezione e tutela delle colleghe e dei colleghi del Gruppo.

Milano, 28 aprile 2026

Delegazioni trattanti Gruppo Intesa Sanpaolo
FABI - FIRST/CISL - FISAC/CGIL - UILCA - UNISIN