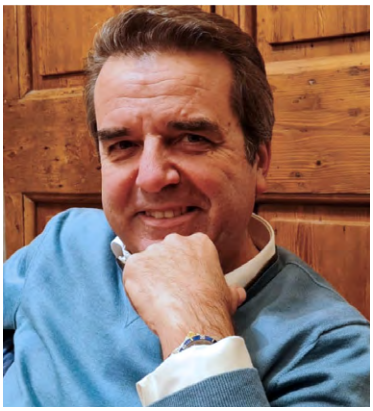
Attacchi cyber e attacchi sui social, la posizione di AIPSA

intervista ad Andrea Chittaro, presidente AIPSA



Come si può commentare il recente attacco cyber subito dalle Ferrovie dello Stato sul piano della prevenzione e delle capacità di reazione della struttura?
Da quello che leggo e dalle informazioni che sono girate nel network di settore, la struttura di security, assieme alle altre funzioni aziendali coinvolte, ha reagito tempestivamente e con efficacia. I danni al core business, in questo caso il trasporto ferroviario, sono stati estremamente contenuti. Se l'obiettivo degli attaccanti era quello di fermare un'infrastruttura critica nazionale, direi che non è stato conseguito.
Nemmeno sul fronte del pagamento di un eventuale riscatto, peraltro.
La strategia di segmentare opportunamente la rete ha consentito di isolare un'area ben definita, dove operare in fase di response e recovery.

Cosa sta alla base, invece, delle pesanti critiche lanciate sui social alle Ferrovie dopo l'attacco?
I social, per loro natura, sono praterie dove si esercitano in libertà commentatori di ogni genere. Ad ogni attacco subito da un'azienda o da un'Istituzione va in scena il solito copione "del giorno dopo". Io mi limito a rilevare le parole del Capo della Polizia Postale, il Dott. Ivano Gabrielli che ha, sostanzialmente, confermato l'impressione di un intervento rapido ed efficace da parte della struttura preposta.
Chiunque abbia solo una lontana idea di come oggi è complesso il mondo infrastrutturale ed applicativo di una qualsiasi realtà, sa bene che è impossibile chiudere ogni porta, blindarsi in una sorta di castello che ricorda i paradigmi della sicurezza di 40 anni fa. Un margine di esposizione resterà sempre anche a fronte di modelli di prevenzione particolarmente maturi. Allora, prima di lanciarsi in facili quanto approssimativi giudizi, sarebbe bene approfondire e capire, oltre alle cause, anche quanto un'azienda abbia investito in tecnologie e competenze. La security è un'attività da praticare con umiltà e con la consapevolezza che non esiste un modello perfetto.

Riprendendo invece i risultati della recente indagine realizzato per conto di Everbridge e Spike Reply in collaborazione con AIPSA sul livello di resilienza delle imprese italiane, quali azioni si potrebbero adottare per migliorare i livelli di preparazione alla gestione di eventi critici?
Innanzitutto, già dotarsi di un'organizzazione preposta alla gestione di questi eventi sarebbe un'ottima base di partenza. Sembra quasi banale dirlo ma, nella realtà, non sempre c'è una struttura di processo dedicata e dotata della giusta autonomia, del necessario budget e delle altrettanto essenziali competenze.
La storia recente ci ha insegnato come il mondo possa cambiare nel giro di poco. Come le certezze a cui ci eravamo ancorati possano venire meno. Due crisi di portata globale come la pandemia e il conflitto Russia-Ucraina non hanno memoria recente. Ed hanno sconvolto radicalmente abitudini, progetti, annullando ogni comfort zone. Credo che ci aspettino anni complicati, dove la percezione di insicurezza globale crescerà e dove strutturarsi per affrontare le sfide discendenti non sarà più un optional ma una ineludibile necessità.

Cosa farà AIPSA in questo senso?
Continuerà nella sua instancabile opera di sensibilizzazione, a tutti i livelli, e di promozione culturale della security e della consapevolezza verso questi temi. Credo sia venuto il momento per affermare definitivamente il ruolo delle funzioni di security aziendale e la loro rilevanza strategica rispetto ad ogni business.