Infrastrutture IT robuste e cultura sulla sicurezza

Una infrastruttura IT solida e resiliente, soprattutto nei sistemi di storage e backup. Un nuovo processo di gestione del rischio in ottica di business continuity ma anche consulenza agli istituti finanziari per definire i piani di difesa

La resilienza, termine molto usato e fin troppo abusato nel periodo pandemico, si trova sul palcoscenico del Regolamento europeo Digital Operational Resilience Act. DORA definisce un insieme di regole volto a rafforzare la resilienza digitale delle istituzioni finanziarie europee, per gestire adeguatamente le interruzioni e le minacce legate ai sistemi informativi e di telecomunicazione.

@ Federico Passeri, IT Security & Risk Manager di Cabel Industry SpA

«Si tratta di un cambiamento epocale – racconta Federico Passeri, IT Security & Risk Manager in Cabel Industry SpA – perché non solo indica alle aziende del settore bancario come essere compliant alla normativa, ma soprattutto mette in atto un profondo cambiamento culturale verso il tema della sicurezza, per garantire un miglioramento continuo attraverso interventi procedurali e tecnici».

Una nuova offerta, compliant

Non solo gli istituti finanziari, ma anche i loro service provider sono inoltre chiamati a rafforzare ulteriormente le strategie di continuità aziendale e di ripristino dopo disastri. «La nuova normativa europea pone un'enfasi senza precedenti sull'importanza di mantenere operativi i servizi critici anche in situazioni di emergenza e da tempo abbiamo avviato il percorso di sviluppo e adattamento dell'offerta in termini di compliance – commenta Passeri. Abbiamo creato soluzioni flessibili e scalabili, tenendo conto dell'evoluzione delle architetture IT e delle esigenze di agilità di business, per rispondere velocemente ai cambiamenti dell'infrastruttura tecnologica».

Resilienza e continuità operativa

Il primo ambito di intervento è stata ovviamente la infrastruttura IT, con l'obiettivo di irrobustirla, attraverso soluzioni tecnologiche ancor più solide e resilienti. In particolar modo per quanto riguarda i sistemi di storage e di backup, così da protegge i dati critici e renderli facilmente recuperabili in caso di emergenza. Con un processo di vulnerability assessment interamente revisionato e potenziato. «Attraverso il nuovo processo di monitoraggio e gestione dei rischi sui progetti e sui change – premette Passeri –, ci siamo posti l'obiettivo di sviluppare strumenti che consentano di identificare e rispondere prontamente alle minacce sulla continuità operativa, migliorando così la capacità di prevenire o mitigare gli impatti derivanti da disservizi».

Accrescere la cultura sulla sicurezza

La DORA pone al centro dell'attenzione anche il rischio ICT legato alle terze parti. Nuovi indicatori e clausole contrattuali, ma anche requisiti minimi che diventano cruciali in tutte le fasi del rapporto delle terze parti, sono sotto la lente degli istituti finanziari. «Centrale è quindi il tema della formazione e della consulenza, per accrescere competenze e cultura in ambito security – conclude Passeri. Per questo motivo, offriamo consulenza avanzata per aiutare i nostri clienti a sviluppare e implementare piani di difesa e di continuità aziendale efficaci, in ottica di irrobustimento di tutto il network».

G.C.