L’86% dei CISO italiani intervistati ammette che l’implementazione di DORA ha avuto un impatto sulla sua salute mentale

- Implementare DORA è costato ad oltre il 70% delle aziende italiane più di 500 mila euro e ad un terzo (37%) oltre 1 milione di euro
- Il ransomware rimane la principale minaccia informatica per il settore finanziario e bancario italiano.
- Il costo della compliance non è solo economico: il 71% dei CISO italiani si sente messo sotto pressione.

Milano, 18 marzo 2025 – Garantire conformità alle normative internazionali può avere un costo significativo per le aziende e per i dipendenti. Lo rivela una nuova ricerca di Rubrik che ha preso in esame i costi e le problematiche che le diverse organizzazioni hanno dovuto affrontare per rispettare i più recenti standard, come il Digital Operational Resilience Act (DORA).

Commissionato da Rubrik (NYSE: RBRK) e in collaborazione con Wakefield Research, la ricerca dei Rubrik Zero Labs rileva come più di un terzo (37%) delle organizzazioni finanziarie e bancarie in Italia ammetta di aver speso più di un milione di euro negli ultimi due anni per implementare normative come DORA, con un altro terzo (34%) che ha dichiarato una spesa compresa tra 501.000 e 1.000.000 euro. Nonostante le iniziative adottate dalle aziende, la componente di rischio resta ben presente, con il ransomware indicato come la minaccia maggiore (34%) per le organizzazioni finanziarie. Inoltre, un CISO su cinque (20%) ha citato le compromissioni di terze parti e il 26% le catene di fornitura del software come minacce significative alla sicurezza.

Il prezzo della compliance non è però soltanto economico. Un aspetto preoccupante messo in evidenza dalla ricerca è il fatto che l'86% di questi professionisti ammette un impatto sulla propria salute mentale, evidenziando la necessità generale di adottare un approccio più empatico a queste sfide. Quello italiano è il dato più alto tra i paesi intervistati, dove la media si attesta all'80%, con il 71% dei CISO italiani che dichiara come DORA ha messo sotto pressione il proprio ruolo.

Entrata in vigore a gennaio 2025, DORA ha introdotto un quadro normativo universale, con particolare attenzione alla gestione dei rischi legati alle tecnologie dell'informazione e della comunicazione (ICT). Questo quadro potrebbe trasformare il settore dei servizi finanziari e bancari, dato che detiene alcuni dei dati più sensibili di tutti i mercati.

“Data la crescente minaccia rappresentata dal ransomware e dalle compromissioni di terze parti, implementare normative dedicate è un passaggio necessario anche se costoso”, ha dichiarato James Hughes, VP of Solutions Engineering e Enterprise CTO di Rubrik. “Capire quali sono i dati più critici, dove risiedono e chi vi ha accesso, è essenziale per identificare, valutare e mitigare i rischi ICT. Se non vengono seguite buone pratiche igieniche come queste, le organizzazioni possono ricevere multe ingenti.”

La ricerca dei Rubrik Zero Labs mostra anche un evidente scollamento con il resto della C-suite quando si tratta di dare priorità alla resilienza informatica, dato che quasi tre quarti (71%) dei CISO italiani ritengono che il loro budget IT non sia completamente rispecchiato dagli obiettivi del loro consiglio di amministrazione per soddisfare i requisiti normativi.

“Esiste un divario critico tra la comprensione a livello di consiglio di amministrazione e la realtà. Mentre le autorità di regolamentazione operano in modo sempre più severo, molti CISO ritengono che i loro budget non riflettano adeguatamente l'impegno del consiglio di amministrazione per la conformità. Questo scollamento mette a rischio non solo la sicurezza delle organizzazioni, ma anche la loro capacità di soddisfare le richieste normative in continua evoluzione”, ha aggiunto Hughes.

DORA impone una serie di disposizioni chiave, come garanzie contrattuali e piani di emergenza, per ridurre al minimo le dipendenze e per mitigare i rischi dei partner. Per garantire le migliori pratiche in materia di

resilienza operativa, i test regolari della resilienza digitale e le simulazioni di attacco, come previsto da DORA, alimenteranno i piani di resilienza informatica e rassicureranno i CISO.

Nonostante ciò, i CISO italiani mostrano di avere fiducia nel cloud, con il 60% che ritiene che le informazioni personali di clienti, partner e dipendenti siano sostanzialmente al sicuro negli ambienti cloud. I CISO, i consigli di amministrazione e le altre parti interessate devono collaborare per garantire che le priorità di resilienza informatica siano chiaramente definite, adeguatamente finanziate e implementate in modo efficace per soddisfare il panorama normativo in evoluzione e salvaguardare il futuro del settore.

Metodologia della ricerca

La ricerca è stata commissionata da Rubrik e condotta da Wakefield Research su 350 CISO che lavorano in aziende con un minimo di 500 dipendenti, nei settori finanziario e bancario, escluse le holding. Sono stati presi in esame cinque mercati: Regno Unito, Germania, Francia, Italia e Paesi Bassi, tra il 21 novembre e il 3 dicembre 2024.

Rubrik

Rubrik (NYSE: RBRK) è in missione per proteggere i dati del mondo. Con la Zero Trust Data Security™, aiutiamo le organizzazioni a raggiungere la resilienza aziendale contro i cyberattacchi, gli insider malintenzionati e le interruzioni operative. Rubrik Security Cloud, basato sul machine learning, protegge i dati nelle applicazioni aziendali, cloud e SaaS. Aiutiamo le organizzazioni a mantenere l'integrità dei dati, a garantire una disponibilità dei dati che resista a condizioni avverse, a monitorare costantemente i rischi e le minacce ai dati e a ripristinare le aziende con i loro dati quando l'infrastruttura viene attaccata. Per maggiori informazioni visitate il sito www.rubrik.com e seguite @rubrikInc su X (conosciuto precedentemente come Twitter) e Rubrik su LinkedIn.