TAS: «DORA non ci ha colto di sorpresa»

Grazie a data center e centri di disaster recovery distribuiti in Europa, tra Italia e Francia, TAS ha rafforzato i servizi di business continuity a favore degli istituti clienti

Anche all'interno della catena di fornitura delle banche, l'effetto DORA è assicurato. L'applicazione del Regolamento porta in primo piano la resilienza operativa digitale, che comporta una richiesta crescente da parte delle banche ai propri fornitori di informazioni per valutare la compliance delle attività legate alla business continuity e al disaster recovery. Da una parte, quindi, la messa in atto di tutte le procedure e dei meccanismi che consentano la continuità delle funzioni essenziali o importanti; dall'altra, l'insieme di strategie per rispondere in modo rapido ed efficace agli incidenti ICT. Ma i tanti investimenti portati avanti negli anni, hanno permesso ad alcuni fornitori di non farsi cogliere impreparati di fronte alle nuove sfide regolamentari. «DORA stabilisce alle entità finanziarie standard tecnici ai quali si devono adeguare, di conseguenza, anche i fornitori, dato che fanno parte della catena di fornitura delle banche. Non è una novità: da sempre gli istituti di credito sono iper regolamentati e i vendor ICT sono quindi chiamati a innalzare gli standard di sicurezza e qualità per rispondere alle loro richieste – racconta Fabrizio Brintazzoli, CISO

Crediti immagine: SaskiaAcht/shutterstock

IL RISCHIO DI NON INVESTIRE

Per quale motivo DORA non ha colto di sorpresa alcuni fornitori ICT? «Andando ad analizzare le specifiche tecniche identificate dal Regolamento si trovano best practice che in realtà sono note da tempo in ambito IT, magari già da decenni e ritenute per di più corrette e necessarie – premette Brintazzoli. Ma siccome richiedono investimenti e sforzi non indifferenti, questi elementi vengono spesso tralasciati da molte imprese, che restano in attesa fino all'arrivo di norme cogenti e regolamenti che costringono all'azione».

@ *Fabrizio Brintazzoli, CISO di TAS*

di TAS. DORA non ci ha quindi colto di sorpresa, né tanto meno lontani dagli obiettivi fissati dal regolamento per le procedure di chi opera in ambito finanziario».

La gap analysis sugli obiettivi DORA

Negli anni TAS ha infatti raggiunto varie certificazioni per rispondere ai requisiti delle copiose normative che hanno impattato sul mercato, in particolare in ambito protezione dei dati e gestione delle informazioni. «Abbiamo condotto una gap analysis per capire a quale punto ci trovavamo e quali erano le mancanze per raggiungere gli obiettivi nelle diverse aree da coprire, così da trovarci pronti alle richieste dei clienti bancari e degli istituti di pagamento – spiega Brintazzoli. Il percorso è iniziato internamente e in autonomia ma, con l'applicazione del regolamento è entrato in vigore l'obbligo per le banche di controllare la catena di fornitura e sono quindi stati i clienti stessi a richiedere meeting, questionari e informazioni per valutare la nostra aderenza al DORA».

La collaborazione interna

L'assessment sui fornitori è in corso e spesso richiede ai vendor di mettere insieme varie funzioni, dalla compliance al dipartimento risk e a quello legal, «che devono collaborare in maniera congiunta per dare risposte complete ed esaustive ai clienti – chiarisce Brintazzoli. D'altronde spesso viene richiesto di modificare gli accordi quadro, inserendo delle integrazioni sul rispetto dei requisiti DORA».

La strategia per business continuity e disaster recovery

TAS, che presenta due anime, una da software vendor in ambito monetica per istituti di pagamento e istituti finanziari, e l'altra da fornitore di servizi in SaaS, ha già irrobustito la sua strategia di disaster recovery e business continuity, in linea con i requisiti normativi. «L'infrastruttura della fabbrica software è stata ideata per essere efficiente sotto questi due importanti ambiti – precisa Brintazzoli. Il data center primario è in Francia, presso la nostra controllata d'oltralpe, e il disaster recovery è situato in Italia. Per quanto riguarda i servizi erogati in SaaS, ci appoggiamo a due realtà, AWS e Aruba. DORA, così come NIS 2, sono regolamenti e direttive che aiuteranno a rafforzare la resilienza generale sistemica».

M.G.