Comunitario e Internazionale

Il Regolamento europeo DORA per l'individuazione e la gestione dei rischi informatici

di Cristina Rabazzi *
04 Luglio 2023

Il Regolamento (UE) DORA (Digital Operational Resilience Act) 2022/2554, relativo alla resilienza operativa digitale per gli operatori del settore finanziario ed i loro fornitori di servizi ICT, è divenuto operativo lo scorso mese di gennaio e sarà vincolante a partire dal 17 gennaio 2025.

NT+ Contenuto esclusivo Norme & Tributi Plus

Il Regolamento (UE) DORA (Digital Operational Resilience Act) 2022/2554, relativo alla resilienza operativa digitale per gli operatori del settore finanziario ed i loro fornitori di servizi ICT, è divenuto operativo lo scorso mese di gennaio e sarà vincolante a partire dal 17 gennaio 2025.
Per resilienza digitale operativa si intende "*la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi tlc, l'intera gamma delle capacità connesse alle tlc necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità anche in occasione di perturbazioni*" (cfr. art. 3).In altre parole, viene prescritta la capacità dei sistemi informatici e di rete, che sostengono i processi commerciali degli operatori finanziari, di continuare a operare regolarmente anche durante un attacco informatico sia esso localizzato o su vasta scala.
La necessità di tale regolamento emerge dal ruolo essenziale che l'uso dei sistemi informatici interconnessi ha assunto nella fornitura di servizi finanziari, al punto da raggiungere oggi un'importanza critica e strategica per il mantenimento dell'efficienza di tutti gli operatori del settore.
In ambito bancario, infatti, ormai quasi la totalità delle operazioni avviene in forma digitale mediante potenti infrastrutture ICT, come ad esempio pagamenti, compensazione e regolamento dei titoli, negoziazione elettronica e algoritmica, prestiti e finanziamenti, finanza peer to peer, gestione del credito. In maniera analoga, anche nel settore assicurativo con l'emergere di intermediari che offrono servizi online e che operano esclusivamente per via telematica risulta strategica una idonea infrastruttura ICT e la sua sicurezza.
L'intervento normativo europeo ha, tra gli altri, lo scopo di mitigare la disomogeneità legislativa e di vigilanza dei singoli Stati membri, che possono intralciare la libertà di stabilimento, di prestazione di servizi e possono causare disparità in ambito concorrenziale tra player che operano nello stesso settore finanziario ma in territori differenti.

Nello specifico, il Regolamento DORA disciplina la gestione dei rischi informatici sia interni che derivanti da terzi, per poi definire la classificazione e la segnalazione degli incidenti informatici, delineando le procedure che gli Organi di Gestione devono attuare per la prevenzione, l'identificazione, la risposta ed il ripristino dell'operatività. Fornisce inoltre indicazioni circa i test di resilienza operativa digitale che devono essere eseguiti ed i meccanismi di condivisione delle informazioni tra le entità finanziarie.

Gestione dei rischi informatici

Nell'esaminare gli adempimenti principali, troviamo innanzitutto quello relativo all'adozione di un sistema di gestione dei rischi informatici. L'articolo 5 impone, infatti, all'Organo di Gestione dell'entità finanziaria di applicare un sistema di controllo interno volto a garantire la gestione dei rischi informatici attraverso politiche e procedure per la tutela dei dati, la definizione dei ruoli e delle responsabilità per tutte le funzioni connesse all'infrastruttura ICT, la definizione della strategia di resilienza operativa digitale, l'approvazione ed il riesame periodico dei piani interni di audit e le modalità per l'uso dei servizi ICT, prestati da fornitori terzi.

Il sistema stesso, come definito all'articolo 6, deve comprendere strategie, politiche, procedure, protocolli e strumenti necessari per proteggere software, hardware, server, locali, centri di elaborazione dati ed aree designate come sensibili, in modo che tutta l'infrastruttura ICT risulti adeguatamente mappata e protetta.

La tempestività dell'individuazione di attività anomale, prevista all'articolo 10, deve essere attuata prevedendo molteplici livelli di controllo che definiscano soglie di allarme e criteri per l'attivazione e l'avvio dei processi di risposta agli incidenti, compresi meccanismi di allarme automatico per il personale incaricato.

Al fine della corretta e rapida individuazione dei rischi informatici sarà necessario, da parte dell'entità finanziaria, dedicare risorse al monitoraggio.

Nell'ambito della gestione del rischio, l'entità finanziaria dovrà poi prevedere, all'interno del quadro di gestione, i piani di risposta e di ripristino che garantiscano la continuità dei servizi erogati.

Test di resilienza operativa digitale

L'articolo 24 fornisce le indicazioni per la valutazione della capacità di resilienza operativa digitale dell'entità finanziaria in modo da identificarne eventuali punti deboli ed attuare le necessarie misure correttive.

Viene quindi introdotta una nuova procedura di monitoraggio costante dell'infrastruttura ICT, aggiungendosi a quelle già esistenti di intervento in caso di incidenti informatici. Nello svolgimento del test dovranno essere presi in considerazione i rischi aggiornati ed eventuali rischi specifici a cui l'operatore potrebbe risultare essere esposto a causa della propria attività.

Tali test dovranno essere svolti all'interno dell'organizzazione almeno una volta all'anno o in concomitanza di eventuali modifiche apportate all'infrastruttura ICT.

Il programma di test di resilienza operativa digitale dovrà comprendere, come indicato negli articoli 25 e 26, l'esecuzione di adeguati test quali scansione delle vulnerabilità, analisi open source,

valutazione della sicurezza di rete e della sicurezza fisica, esami del codice sorgente, test basati su scenari, test di penetrazione (anche TLPT) ed end-to-end.

Gli operatori finanziari italiani già possono svolgere test avanzati di cybersicurezza di tipo Threat-Led Penetration Testing (TLPT), su base volontaria, al fine di rafforzare la resilienza cibernetica delle singole entità finanziarie. Tali test sono peraltro stati accolti anche da Banca d'Italia, Consob e l'IVASS nella Guida nazionale TIBER IT, con cui è stato recepito il framework TIBER-EU, che rappresenta il modello di riferimento per la conduzione di test avanzati di cybersicurezza a livello europeo.

Gestione dei rischi derivanti da terzi

Il Legislatore europeo ha voluto dedicare una ampia sezione alla gestione dei rischi derivanti da terzi, disciplinando dettagliatamente gli aspetti di responsabilità, di due diligence nella scelta degli operatori ICT, nella formulazione e gestione del contratto e nelle procedure da adottare per il monitoraggio e la comunicazione agli organi di vigilanza.

Condivisione delle informazioni

Il regolamento DORA definisce, all'articolo 45, i meccanismi di condivisione delle informazioni e delle analisi delle minacce informatiche che dovranno tutelare la protezione dei dati condivisi e sensibili. Tali meccanismi sono disciplinati da norme di condotta, dal Regolamento (UE) 2016/679 (GDPR) e della disciplina in materia di concorrenza.

Questo aspetto risulta essere di grande importanza, in quanto lo scambio di informazioni sulle minacce informatiche consente di incentivare la cooperazione delle entità finanziarie volta ad un costante monitoraggio e aggiornamento tecnico condiviso.

Conclusioni

Con il Regolamento DORA il legislatore europeo ha voluto armonizzare a livello normativo un settore molto tecnico e complesso, puntando sulla sicurezza e la resilienza dell'area più strategica e sensibile che ciascuna entità finanziaria possa avere. Del resto, nell'attuale contesto di mercato, sempre più digitale e sempre più bersaglio di avanzati attacchi informatici, è necessario fare leva su politiche ed azioni all'interno della propria organizzazione, che producano effetti amplificati su tutta la comunità, fortificando l'operatività dell'intera struttura finanziaria.

**a cura dell' Avv. Cristina Rabazzi, Gebbia Bortolotto Penalisti Associati*

Il Sole 24 ORE aderisce a The Trust Project

P.I. 00777910159 | © Copyright Il Sole 24 Ore Tutti i diritti riservati

Il Sole 24 ORE