BANCA D'ITALIA
EUROSISTEMA

Comunicazione al mercato in materia di sicurezza ICT[1]

Il prossimo 17 gennaio 2025 sarà applicabile il Regolamento sulla resilienza operativa digitale del settore finanziario (Digital Operational Resilience Act, DORA), che introduce norme armonizzate a livello europeo volte a rafforzare la gestione dei rischi ICT[2].

La Banca d'Italia, in linea con l'approccio della Vigilanza unica europea, segue da tempo la tematica della sicurezza ICT attraverso iniziative di supervisione che riguardano sia i singoli operatori finanziari sia il sistema nel suo complesso. Nel fare riserva di emanare una specifica comunicazione al mercato sull'attuazione nazionale del Regolamento DORA, si richiama fin d'ora l'attenzione degli intermediari vigilati direttamente dalla Banca d'Italia sulle evidenze emerse dalle analisi di supervisione.

I dati relativi alle segnalazioni dei gravi incidenti operativi o di sicurezza, come riportato nel recente documento di analisi della Banca d'Italia "Digital resilience in the Italian financial sector: evidences from the supervisory incident reporting framework", segnalano che nell'ultimo triennio vi è stato un aumento delle segnalazioni di incidenti sia operativi sia cibernetici (per questi ultimi l'aumento è stato maggiore nel 2023).

Le analisi evidenziano che gli incidenti operativi sono spesso causati da inadeguatezze nel processo di modifica dei sistemi (cd. *ICT change management*), mentre per quelli di natura cibernetica rilevano maggiormente gli accessi non autorizzati, che nella gran parte dei casi comportano violazioni della riservatezza dei dati e/o dei servizi offerti dall'entità finanziaria. Tra questi ultimi eventi rientrano le azioni condotte da personale interno e/o da fornitori di servizi autorizzati che abusano dei diritti di accesso ai sistemi loro concessi.

Alcuni punti di attenzione sono emersi dall'indagine condotta dalla Banca d'Italia per migliorare la conoscenza dei processi e delle prassi di aggregazione e reportistica dei dati di rischio adottati dalle banche italiane ("Indagine Risk Data Aggregation"). In particolare, le possibili carenze nella capacità di gestire e aggregare i dati sui rischi e le eventuali inadeguatezze dei sistemi ICT utilizzati per

[1] La presente comunicazione è destinata ai seguenti soggetti vigilati dalla Banca d'Italia: banche (escluse le banche significative), imprese di investimento, gestori, istituti di pagamento, istituti di moneta elettronica, emittenti di token collegati ad attività, prestatori di servizi per le cripto-attività, fornitori di servizi di *crowdfunding*. Non è destinata a quei soggetti a cui non si applica il Regolamento DORA.

[2] Il Regolamento DORA, richiamando anche parte del contenuto delle linee guida per la gestione dei rischi ICT e di sicurezza emanati dall'EBA, definisce un quadro organico per la gestione del rischio ICT che comprende politiche, procedure, protocolli e strumenti che le entità devono implementare per far fronte a tali rischi. Il regolamento, come integrato dai connessi atti di normativa secondaria, disciplina vari aspetti della gestione del rischio nelle sue diverse fasi, ivi inclusi quelli relativi alle misure di protezione della confidenzialità dei dati e al processo di gestione del cambiamento.

supportare i processi decisionali e le attività di gestione dei rischi possono compromettere la solidità del processo decisionale e l'efficacia del governo dei rischi da parte degli intermediari.

Analoghe evidenze emergono dagli approfondimenti condotti nell'ambito del Meccanismo di Vigilanza Unico (MVU) sulle banche significative. Ci si riferisce in particolare ai risultati dell'analisi orizzontale condotta dall'MVU *"Key observations from the 2024 horizontal analysis of IT and cyber risk"*, che combina le informazioni fornite dalle banche significative tramite il questionario sul rischio ICT (*IT Risk Questionnaire*) e le evidenze emerse dagli accessi ispettivi sulla sicurezza cibernetica degli ultimi anni.

È pertanto essenziale che gli intermediari presidino adeguatamente il profilo del rischio ICT, che sta ormai travalicando i confini del rischio operativo e assumendo natura trasversale all'intera operatività aziendale, dati il crescente ricorso alla tecnologia e gli impatti che eventuali debolezze nella gestione delle risorse informatiche possono avere sulla reputazione degli intermediari.

L'evoluzione regolamentare di imminente applicazione richiede di rafforzare il presidio del rischio ICT. Infatti, il Regolamento DORA introdurrà obblighi per le entità finanziarie in materia di gestione del rischio ICT, riguardanti tra l'altro i presidi di protezione e prevenzione del rischio ICT e di rilevamento delle attività anomale[3].

Alla luce di quanto sopra, si richiede a tutti gli intermediari direttamente vigilati dalla Banca d'Italia di valutare, su base consolidata per i gruppi e individuale per i soggetti non appartenenti a gruppi[4], il proprio posizionamento rispetto ai requisiti introdotti dal Regolamento DORA, con particolare riferimento alle seguenti aree: i) strategie sul rischio di terza parte, sul rinnovo dei contratti di fornitura e sulla trasmissione all'Autorità del Registro delle Informazioni; ii) adattamento di presidi e politiche interne; iii) attività e programma di test di resilienza operativa digitale.

Si richiede inoltre ai suddetti intermediari di effettuare una autovalutazione del proprio sistema di gestione dei rischi ICT, al fine di assicurare che le politiche, le procedure, i protocolli e gli strumenti in materia di rischio ICT siano adeguati a:

- prevenire, ovvero rilevare tempestivamente, violazioni alla riservatezza dei dati e/o dei servizi forniti. Tali approfondimenti devono comprendere:

  - una valutazione delle misure adottate per prevenire la perdita di integrità, disponibilità e riservatezza dei dati, incluse le eventuali fughe di dati (cd. *data leakage*);

  - una valutazione delle misure relative al controllo degli accessi, inclusi eventuali abusi dei diritti di accesso concessi al proprio personale e/o al personale dei propri fornitori di servizi;

  - una valutazione delle attività di controllo e monitoraggio dei sistemi ICT adottate anche al fine di individuare attività anomale che possano avere impatti sulla riservatezza dei dati e/o dei servizi[5];

[3] Cfr. Art. 9, 10 e 16 del Regolamento DORA.

[4] Sono esclusi gli intermediari non bancari di gruppi significativi.

[5] Cfr. art. 10 del Regolamento DORA (ovvero l'art.16 per i soggetti di cui al primo comma di tale articolo).

- ridurre il rischio derivante dai cambiamenti ICT. A tale proposito, si richiede agli intermediari di valutare che il proprio quadro di *ICT change management* sia in linea con quanto richiesto dal Regolamento DORA e dalle relative norme attuative in termini di prassi, politiche, attribuzione di responsabilità e meccanismi di presidio della sicurezza[6].

L'organo di amministrazione dovrà approvare l'autovalutazione, condotta con il coinvolgimento delle funzioni di controllo di secondo e terzo livello, e trasmetterla alla Banca d'Italia entro il 30 aprile 2025.

[6] Cfr. art. 9.4 punto e) del Regolamento DORA (ovvero l'art.16 per i soggetti di cui al primo comma di tale articolo), come integrato dall'art. 17 (ovvero l'art. 38 per i soggetti di cui al primo comma dell'art.16 del regolamento DORA) del Regolamento delegato relativo alla gestione dei rischi informatici (Regolamento delegato UE 2024/1774).