Comunicazione al mercato in materia di resilienza operativa digitale e modelli avanzati di Intelligenza Artificiale

Le tecnologie emergenti, e in particolare i sistemi di intelligenza artificiale, stanno trasformando il panorama della cybersicurezza e ponendo nuove sfide per le loro possibili implicazioni per la riservatezza, l'integrità e la resilienza dei sistemi informatici e delle informazioni da essi gestite, anche nel settore finanziario.

In particolare, i modelli di ultima generazione hanno la capacità di identificare le vulnerabilità dei sistemi *software* e generare contemporaneamente le relative modalità di sfruttamento in tempi estremamente ridotti e senza la necessità di specifiche competenze tecniche. Ciò comporta una sensibile riduzione dell'intervallo temporale tra l'individuazione delle vulnerabilità e il loro sfruttamento, con conseguente incremento dei rischi di subire attacchi *cyber* efficaci.

Le nuove tecnologie di intelligenza artificiale potrebbero, quindi, accrescere l'asimmetria fra attaccanti e difensori, a scapito di questi ultimi, tale da rendere necessario un adattamento rapido da parte delle entità finanziarie[1]. In questo nuovo contesto, il rafforzamento della resilienza operativa digitale non rappresenta soltanto un'esigenza di conformità, ma una condizione essenziale per assicurare la continuità aziendale e la capacità di offrire servizi finanziari affidabili.

Alla luce di tali evoluzioni, la Banca d'Italia, in coerenza con l'impostazione della Vigilanza unica europea, e tenendo presente i requisiti previsti dal Digital Operational Resilience Act (DORA) che mantengono piena valenza anche in questo contesto, invita gli intermediari a individuare e realizzare con tempestività le misure necessarie per potenziare i processi e i

[1] La presente comunicazione è rivolta ai seguenti soggetti direttamente vigilati dal Dipartimento Vigilanza Bancaria e Finanziaria della Banca d'Italia: banche e gruppi bancari meno significativi (compresa Bancoposta), istituti di pagamento, istituti di moneta elettronica, imprese di investimento, fornitori di servizi per le cripto-attività, gestori di fondi di investimento alternativi, società di gestione, fornitori di servizi di *crowdfunding*, intermediari finanziari (ex. 106).

presidi di sicurezza a protezione dei propri sistemi al fine di rafforzare la propria resilienza operativa e cibernetica.

Si segnala la necessità che gli intermediari pongano in essere misure per rafforzare i presidi nelle seguenti aree:

- ***Governance***: gli organi con funzione di amministrazione e di gestione devono rivedere il quadro di riferimento per la determinazione della propensione al rischio (RAF) per incorporare i rischi derivanti dalle tecnologie di frontiera, in maniera coerente con le decisioni strategiche, incluse quelle concernenti gli investimenti in ambito ICT e l'allocazione delle risorse[2]. Ad essi spetta promuovere il rafforzamento dei sistemi di governo e di controllo, nonché assicurare una chiara e puntuale attribuzione delle responsabilità, anche con riferimento alla gestione e sicurezza dei dati. Essi sono altresì tenuti a definire presidi appropriati per il governo degli eventuali fornitori esterni di servizi informatici; tali presidi comprendono, in particolare, adeguati requisiti contrattuali, volti ad assicurare efficaci misure di monitoraggio della sicurezza e di gestione degli aggiornamenti (*patch*) da parte del fornitore, nonché criteri rigorosi per la valutazione ex-ante e la selezione dei fornitori. A tal fine, è importante che l'organo di amministrazione e di gestione annoveri al proprio interno componenti dotati di adeguate competenze tecnologiche, anche in materia di intelligenza artificiale, e che preveda un *budget* adeguato a garantire la propria formazione nel continuo.
- **Igiene informatica:** anche alla luce delle minacce connesse ai modelli di intelligenza artificiale di frontiera, occorre integrare nella propria strategia i principi della difesa in profondità (*defence-in-depth*)[3] e dell'igiene informatica, che prevedono processi di autenticazione e autorizzazione rigorosi, una gestione granulare degli accessi e un monitoraggio costante delle attività. A tali modelli dovrebbero essere affiancate strategie di segmentazione delle reti e degli ambienti operativi, al fine di limitare la propagazione di eventuali compromissioni.

[2] Qualora gli intermediari decidano di avvalersi di strumenti di difesa basati sull'intelligenza artificiale (cfr. infra), il loro impiego dovrà essere coerente con la strategia in materia di IA e accompagnato da un adeguata valutazione dei rischi specifici associati a tali tecnologie, nonché dall'adozione di idonei presidi (i.e. monitoraggio delle prestazioni e del deterioramento, supervisione umana, ecc.).

[3] Si intende una strategia applicata alla cybersicurezza che utilizza più livelli sovrapposti di misure di sicurezza. Se un livello viene superato, i successivi intervengono per bloccare l'attacco, rilevare l'intrusione e proteggere i dati sensibili.

- **Gestione delle risorse informatiche e della potenziale superficie d'esposizione**: occorre disporre di inventari completi, aggiornati e affidabili, anche in considerazione delle minacce emergenti. Si tratta di un prerequisito essenziale sia per individuare e gestire correttamente le vulnerabilità sia per mappare la propria potenziale superficie di attacco e intervenire in modo efficace. La classificazione delle risorse informatiche in funzione della criticità deve tenere conto della loro eventuale esposizione diretta su internet, nonché del ricorso a soluzioni basate su infrastrutture *cloud*. Allo stesso tempo, occorre procedere alla modernizzazione delle infrastrutture, anche mediante la sostituzione o l'aggiornamento di tecnologie non più supportate o giunte a fine vita (*legacy*).
- **Gestione delle vulnerabilità e degli aggiornamenti (*patch*)**: si rende necessario individuare rapidamente le vulnerabilità dei propri sistemi ICT, anche attraverso l'evoluzione delle tecniche di scansione delle vulnerabilità (e ove opportuno[4] anche avvalendosi di sistemi di intelligenza artificiale) per ridurre il divario con eventuali attaccanti. Inoltre, è necessario rendere più efficiente il processo per la gestione delle vulnerabilità attraverso l'applicazione più tempestiva delle azioni di rimedio, dando precedenza a quelle considerate più critiche. Occorre intervenire prioritariamente per mettere in sicurezza i *software open source* e, più in generale, i sistemi direttamente accessibili dall'esterno, le cui vulnerabilità (specialmente quelle per le quali non è ancora disponibile una correzione, cd vulnerabilità *zero-day*) possono essere sfruttate da attaccanti malevoli.
- **Monitoraggio, rilevazione e misure di difesa**: si rende necessario rafforzare i sistemi di monitoraggio e difesa delle applicazioni, degli accessi e del traffico di rete (compreso quello da e verso i fornitori terzi di servizi informatici), integrandoli, ove opportuno, con strumenti basati sull'intelligenza artificiale, per analizzare grandi volumi di dati e identificare anomalie in tempo reale, specie con riferimento alle risorse informatiche critiche. È altresì fondamentale che tali sistemi di monitoraggio siano sincronizzati con l'inventario delle risorse informatiche per garantire che queste ultime siano monitorate in base alla loro classificazione di criticità.

[4] La valutazione deve tenere in considerazione i costi e i benefici, nonché il profilo di rischio complessivo dell'intermediario, la complessità dei servizi, l'attività e l'operatività (cfr. art.4.1 del DORA).

- **Attività di test**: occorre rafforzare i test di resilienza operativa digitale[5] e quelli dei processi di risposta e recupero, includendo in modo strutturato anche le attività di gestione delle crisi, attraverso il test periodico delle procedure operative in linea con i requisiti previsti dal regolamento DORA. Tali attività dovrebbero prevedere la simulazione di scenari realistici e progressivamente più complessi, adeguati alla continua evoluzione del panorama delle minacce *cyber* a seguito dei cambiamenti nel contesto tecnologico. Le attività di test assumono un ruolo ancora più cruciale per valutare la preparazione dell'entità in un contesto dove la probabilità che si verifichi un incidente ICT è aumentata.

Il crescente ricorso a fornitori esterni amplia le vulnerabilità collegate alla gestione della leva tecnologica: catene di fornitura articolate su più livelli e concentrate in pochi operatori possono trasformare criticità circoscritte in problemi di ampia portata. Pertanto, le iniziative degli intermediari devono essere supportate anche dai fornitori esterni, sui quali ricadono le medesime responsabilità di assicurare la salvaguardia e la continuità dei sistemi[6].

Ci si attende che il Consiglio di Amministrazione, nel corso di una seduta congiunta con il Collegio Sindacale, esamini il contenuto della presente Comunicazione. Nel corso della medesima seduta, dovrà essere dato avvio ai lavori per la stesura di una Relazione che, distintamente per ciascuna delle aree richiamate, rappresenti il livello attuale di esposizione al rischio e l'adeguatezza dei presidi esistenti, individui le principali carenze e le relative priorità di intervento nonché definisca un piano di lavoro con l'indicazione delle azioni, dei tempi e degli investimenti necessari, proporzionato al profilo di rischio, alla complessità dei servizi, all'attività e all'operatività dell'intermediario; tale piano dovrà altresì definire le modalità con cui il Consiglio di Amministrazione verificherà l'avanzamento dello stesso. Ogni entità finanziaria dovrà individuare e comunicare all'Organo di Vigilanza uno specifico punto di responsabilità aziendale (ad esempio, la funzione di controllo dei rischi

[5] Si fa riferimento in particolare: i) all'articolo 24.1 di DORA, che prevede che le entità finanziarie abbiano un programma di test di resilienza operativa digitale aggiornato, solido ed esaustivo quale parte integrante del quadro per la gestione dei rischi informatici; ii) all'art 25.1, che prevede che "*Il programma di test di resilienza operativa digitale … prevede l'esecuzione di test adeguati, tra cui valutazione e scansione delle vulnerabilità, analisi open source, valutazioni della sicurezza delle reti, analisi delle carenze, esami della sicurezza fisica, questionari e soluzioni di scansione del software, esami del codice sorgente, ove fattibile, test basati su scenari, test di compatibilità, test di prestazione, test end-to-end e test di penetrazione*". Oltre a tali requisiti validi per tutti gli intermediari, restano salvi i requisiti in materia di test di penetrazione guidati dalla minaccia (TLPT) per quei soggetti individuati da parte delle Autorità di Vigilanza competenti.

[6] Banca di Italia, Considerazioni Finali del Governatore sul 2025.

ICT di secondo livello). La Relazione, con allegato il piano di lavoro, deve essere trasmessa alla Vigilanza entro il 31 dicembre 2026.