BANCA D'ITALIA
EUROSISTEMA

La cybersicurezza del settore finanziario: ruolo delle autorità e valore della cooperazione

Intervento di apertura di Paolo Angelini
Vice Direttore Generale della Banca d'Italia

Convegno "La cooperazione pubblico-privato per la resilienza cyber del settore finanziario italiano - Le opportunità per gli operatori e il ruolo del CERTFin"

Roma, 4 luglio 2024

Signore e signori,

è per me un piacere darvi il benvenuto in Banca d'Italia per questo convegno, che affronta temi la cui rilevanza è venuta rapidamente crescendo negli ultimi anni.

La digitalizzazione dei servizi, e delle stesse relazioni sociali, è ormai un elemento strutturale del contesto in cui viviamo. Nel campo dei servizi finanziari il fenomeno si è sviluppato in anticipo rispetto ad altri mercati. Ha comportato benefici rilevanti, ma anche nuovi rischi operativi, cresciuti rapidamente di recente. Vi hanno contribuito sia l'aumento della fruizione online di certi servizi finanziari indotto dalla pandemia sia la tendenza a usare il cyber-spazio come luogo di aggressione con finalità politiche, economiche o puramente criminali, anche per effetto del recente inasprimento delle tensioni internazionali.

Le autorità, le associazioni, gli intermediari presenti a questa giornata di studio sono tutti in prima linea, ciascuno nel proprio ambito di competenza, per definire regole, strategie e strumenti per contrastare questi rischi e contribuire a uno sviluppo sicuro dell'ecosistema digitale.

In questo intervento accennerò ai recenti sviluppi in materia di incidenti cyber, illustrerò alcune novità regolamentari in arrivo, sottolineerò l'importanza della cooperazione tra istituzioni e intermediari ai fini del contrasto alla cybercriminalità.

Gli attacchi cyber aumentano e si diversificano le azioni di risposta

La cybercriminalità si evolve rapidamente. Adotta tecniche e strumenti sempre più sofisticati, prende molteplici forme (dal *ransomware* alle frodi informatiche), aggredisce soggetti eterogenei (cittadini, imprese, organizzazioni pubbliche e private).

La diffusione del paradigma del *Crime-As-a-Service* consente anche a soggetti con limitate capacità tecniche, finanziarie o organizzative di acquistare o appaltare i servizi necessari

per condurre efficaci attività illegali nel cyber-spazio. I cyber criminali beneficiano essi stessi del progresso tecnologico: gli sviluppi in materia di intelligenza artificiale e, in prospettiva, di computer quantistici, sono in grado di offrire nuove opportunità di sviluppo economico e sociale, ma anche di scardinare i meccanismi di sicurezza oggi prevalenti.

Secondo un'indagine della Banca d'Italia sulle imprese industriali e dei servizi private non finanziarie con oltre 20 addetti (INVIND 2023 sui dati del 2022), quasi il 90 per cento delle imprese è consapevole della possibilità di subire un attacco informatico. Quelle che sono state vittima di un attacco percepiscono un rischio più elevato, cui si associa un maggiore investimento in prevenzione. Le imprese più piccole, con un numero di addetti compreso tra 20 e 49, risultano meno consapevoli dei rischi cibernetici: quelle che ritengono per nulla probabile che un attacco cibernetico possa interessare un'impresa con le loro stesse caratteristiche sono il 14 per cento del campione, contro il 7 per centro tra le imprese con oltre 50 addetti[1]. Non sorprende quindi che gli attacchi ai sistemi informatici delle imprese prendano prevalentemente di mira quelle più grandi, che hanno maggiore capacità economica, ma sfruttino anche il minor grado di preparazione che caratterizza le imprese di dimensioni medie o piccole (PMI).

Dalla relazione annuale dell'Agenzia per la Cybersicurezza Nazionale (ACN) emerge un fortissimo aumento degli incidenti segnalati nel 2023 (303, contro 126 nel 2022), che ha interessato tutti i settori economici[2]. Il numero di attacchi di tipo *ransomware*, che costituisce il fenomeno più allarmante, è aumentato del 27 per cento, interessando sia le PMI sia le grandi imprese. Per le PMI il fenomeno è verosimilmente sottostimato, tenuto conto che tali imprese sono spesso sprovviste di presidi di cybersicurezza adeguati e tendono a non segnalare gli incidenti. Tendenze analoghe sono state registrate anche a livello europeo e internazionale[3].

Il settore finanziario è un obiettivo privilegiato dei cybercriminali, per l'alta intensità tecnologica, la forte interdipendenza tra gli operatori della comunità finanziaria, nazionale e globale, e per il valore economico e strategico delle funzioni da esso svolte.

Le segnalazioni inviate alla Banca d'Italia dalle banche e dai prestatori di servizi di pagamento confermano la forte accelerazione del numero di incidenti cyber l'anno scorso: 30 segnalazioni di attacchi, contro 13 nel 2022 (fig. 1.a). I casi più frequenti hanno riguardato la disponibilità di servizi offerti alla clientela (cosiddetti attacchi *Denial Of Service*; fig. 1.b), talvolta attuati da soggetti che appaiono riconducibili a governi di paesi extraeuropei.

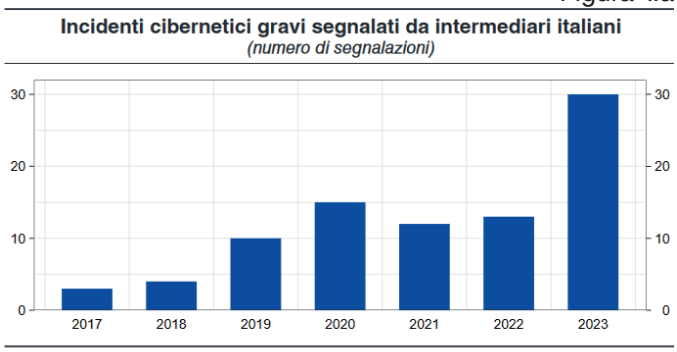
---

1 Cfr. L. Bencivelli e M. Mongardini, La sicurezza cibernetica delle imprese italiane: percezione dei rischi e pratiche di mitigazione, Banca d'Italia, Questioni di economia e finanza, 852, giugno 2024.

2 Cfr. Agenzia per la cybersicurezza nazionale (ACN), "Relazione annuale al Parlamento, 2023".

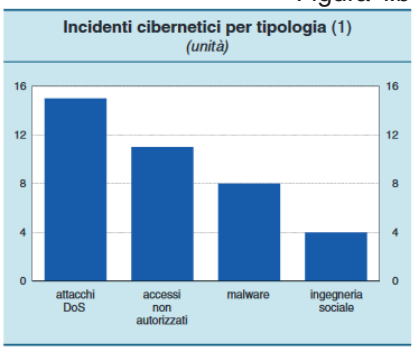
3 Cfr. Agenzia dell'Unione europea per la cybersicurezza (ENISA), "ENISA Threat Landscape 2023"; Fondo Monetario Internazionale, "Global Financial Stability Report, April 2024".

Figura 1.a



Fonte: segnalazioni di vigilanza.

Figura 1.b



Fonte: elaborazioni su segnalazioni di vigilanza.
(1) Un incidente può essere classificato secondo più tipologie. I dati si riferiscono al 2023.

Alla crescita della criminalità cibernetica si contrappone quella dell'azione di contrasto, che tipicamente si svolge su due piani. Da un lato, sono fondamentali le misure difensive che ciascuna delle vittime potenziali pone in essere, adeguando strategie, assetti di governo e investimenti in tecnologia, risorse, processi e formazione. Dall'altro, è in atto uno sforzo cooperativo che vede coinvolte Forze dell'ordine, autorità di controllo e potenziali vittime della minaccia – imprese, ma anche soggetti pubblici di vario tipo (l'incontro odierno è parte di questo sforzo). Le Autorità finanziarie cooperano anche a livello internazionale, promuovendo l'adozione di regole, politiche, strumenti di controllo e iniziative condivisi.

La Banca d'Italia è attiva in questo percorso sia per il suo ruolo istituzionale di tutela della stabilità del sistema finanziario sia in quanto gestore di una infrastruttura critica per il Paese e per l'Eurosistema. La nostra pianificazione strategica comprende piani d'azione che coprono entrambi i fronti.

Prepararsi alle novità regolamentari

La principale novità in arrivo in ambito legislativo è rappresentata dal DORA (*Digital operations Resilience Act*), che entrerà in vigore a gennaio 2025 e disciplinerà a tutto tondo la resilienza operativa digitale nel settore finanziario.

Pur introducendo vari elementi di novità, per numerosi aspetti DORA si muove in continuità col passato. Ad esempio, alcune disposizioni previste nel regolamento erano già applicate al settore finanziario sotto forma di linee guida[4]. Inoltre il rischio IT è già da tempo parte integrante dello SREP (*Supervisory review and evaluation process*), che prevede approfondimenti e verifiche ispettive mirate e include la fissazione dei requisiti di capitale degli intermediari.

Anche le previsioni sulle cosiddette "terze parti" (soggetti che forniscono tecnologie e servizi digitali al settore finanziario) introdotte da DORA non sono completamente nuove. Alcuni poteri delle autorità di vigilanza e di supervisione nei confronti questi soggetti

4 Cfr. ad esempio Autorità Bancaria Europea (EBA), "Guidelines on ICT and Security Risk Management".

erano presenti nell'ordinamento nazionale già da diversi anni[5]. Il Regolamento estende e rafforza tali poteri con l'introduzione di un nuovo regime di sorveglianza sui fornitori critici a livello europeo, che saranno individuati in base a criteri quali-quantitativi.

DORA introduce previsioni specifiche in materia di TLPT, i *Threat Led Penetration Test*, esercizi che dovranno essere condotti da tutte le principali banche, infrastrutture di mercato e assicurazioni europee, e che consentono all'intermediario di verificare il proprio grado di resistenza e resilienza a fronte di uno specifico scenario di minaccia cyber. Anche questo strumento era già noto in molte giurisdizioni, compresa l'Europa, ma il regolamento ne struttura l'utilizzo in modo più organico, prevedendo un processo articolato su cicli pluriennali, con la partecipazione delle autorità e di specialisti anche esterni.

Infine, DORA promuove la partecipazione di entità finanziarie e autorità di vigilanza a meccanismi di condivisione delle informazioni, valorizzando la cooperazione e lo sviluppo di iniziative pubblico-private come il nostro CERT di settore, il CERTFin.

È in fase di conclusione la stesura della regolamentazione di secondo livello collegata alla normativa primaria. La Banca d'Italia ha partecipato con le altre Autorità competenti, italiane ed europee, alla messa a punto dei testi e si sta ora concentrando sugli impatti in termini di processi, metodologie e risorse necessarie per l'attuazione.

Un aspetto che stiamo presidiando è la coerenza di questo *corpus* normativo con le regole in tema di sicurezza delle reti e dei sistemi informativi, oggetto anch'esse di una significativa revisione con la prossima attuazione della Direttiva NIS2. Lavoriamo con le istituzioni interessate, tra cui il MEF, l'ACN e la Presidenza del Consiglio dei Ministri, per evitare incertezze applicative e duplicazioni di oneri per gli operatori.

L'importanza della cooperazione

Contromisure individuali, regolamentazione, supervisione, pur potenziate, non bastano a proteggere il settore da minacce sempre più sofisticate e insidiose. La cooperazione tra i vari attori coinvolti consente di promuovere la consapevolezza dei rischi connessi con le tecnologie più innovative, individuare tempestivamente le minacce e attivare le azioni di rimedio più efficaci.

In questo ambito la cooperazione tra gli intermediari finanziari, lungi dal rappresentare una minaccia per la concorrenzialità del mercato, costituisce un indispensabile strumento di contenimento del rischio. La Banca d'Italia ha da sempre promosso queste forme di cooperazione nei campi in cui le decisioni dei singoli intermediari non sono in grado di conseguire risultati ottimali. Tramite il proprio CERT (CERTBI), la Banca intrattiene

---

5 Dal 2015 le autorità di vigilanza e supervisione hanno specifici poteri sui soggetti non vigilati ai quali le diverse tipologie di entità finanziarie hanno esternalizzato funzioni aziendali. La Banca d'Italia può richiedere informazioni (in alcuni casi sulla base di contratti stipulati tra il soggetto vigilato e il fornitore) nonché effettuare ispezioni, convocare amministratori e altro personale e infine applicare sanzioni in caso di inottemperanza alle richieste.

rapporti di collaborazione con i diversi attori che operano nell'architettura nazionale di cybersicurezza, in primo luogo l'ACN, ma anche la Polizia di Stato, l'Arma dei Carabinieri, la Guardia di Finanza. Ugualmente attraverso il CERT del settore finanziario, il CERTFin, avviato nel 2017 insieme all'ABI, facciamo fronte comune nella prevenzione e nel contrasto dei nuovi rischi[6]. L'esperienza di questi sette anni di funzionamento è ampiamente positiva, come testimoniato dalla crescita del numero di partecipanti (passati da circa 20 agli odierni 70), dal significativo aumento degli scambi informativi e dal potenziamento della rete di collaborazione con organismi simili a livello internazionale.

Anche la cooperazione con soggetti esterni al mondo della finanza è assai importante. Il cyber-spazio non ha confini, e le tecniche di attacco dei cybercriminali non differenziano la vittima in funzione del settore di appartenenza. Nel nostro Paese, da qualche anno, un approccio di sistema è reso possibile dall'adozione di una Strategia di cybersicurezza nazionale e dal ruolo trasversale assegnato alla ACN. Anche il legislatore europeo ha tracciato, con la direttiva NIS, un percorso di collaborazione tra le istituzioni dei settori essenziali della società e dell'economia.

A fronte di questi progressi, non vanno nascoste alcune difficoltà. La pluralità delle iniziative che si sono venute sviluppando in materia evidenzia un quadro di riferimento complesso e a tratti frammentato, con conseguenti accresciute esigenze di raccordo informativo e operativo tra tutte le istituzioni coinvolte. Questo assetto comporta difficoltà di coordinamento e costi relativamente elevati.

Questo è uno dei temi che saranno oggetto del confronto di oggi, dal quale contiamo di poter trarre utili spunti di miglioramento.

A tal proposito, ho il piacere di anticipare che oggi, dopo la prima tavola rotonda, verrà sottoscritto il Protocollo di intesa per la collaborazione per la prevenzione dei crimini informatici nel settore finanziario tra il CERTFin e la Direzione centrale per la polizia scientifica e la sicurezza cibernetica del Ministero dell'Interno, a testimonianza del comune impegno per rendere più sicuro l'ecosistema dei servizi finanziari digitali per il Paese e per i cittadini.

---

6 Cfr. https://www.certfin.it/

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia