BANCA D'ITALIA
EUROSISTEMA

Cyber sicurezza:
Una continua sfida per l'economia e per la società

Intervento di Alessandra Perrazzelli
Vice Direttrice Generale della Banca d'Italia

10 febbraio 2023

Scenario evolutivo della minaccia cyber

La digitalizzazione, l'interconnessione sociale ed economica sono ormai diventati un elemento strutturale del contesto in cui viviamo. Lo scoppio della pandemia ha accelerato l'adozione di tecnologie informatiche all'interno di infrastrutture critiche, di processi produttivi e, in ultima analisi, della vita privata dei cittadini.

Se da un lato l'evoluzione tecnologia determina rilevanti benefici, dall'altro introduce nuovi rischi: il cyberspazio diventa quindi il luogo dove organizzazioni talvolta anche governative possono attuare proprie strategie anche con fini criminali**.** La massiccia campagna di attacchi informatici – basati su "ransomware" – che la scorsa settimana è stata diretta verso organizzazioni di diversi Paesi, inclusa l'Italia, ci conferma i potenziali e dirompenti effetti di questi rischi, oltre all'urgenza di interventi forti, efficaci e globali. Il tema che affrontiamo oggi è dunque di grande attualità e rilevanza.

Alla luce di questi eventi, osserviamo come il cyber-spazio diventi spesso strumentale al perseguimento di interessi di tipo statuale e criminale.

- Il cyber-spazio è la quinta dimensione della conflittualità – dopo terra, mare, aria e spazio extra-atmosferico – e costituisce uno degli elementi dello scenario in cui si innesta la politica internazionale.

- L'alta profittabilità degli attacchi informatici condotti con finalità economica[1] favorisce la costante crescita del cyber-crime, che si evolve adottando strumenti e tecniche di attacco sempre più sofisticati e modelli di business progressivamente

---

1 Solamente negli Stati Uniti, si stima che il cyber-crime abbia prodotto nel 2021 danni a aziende e cittadini per circa 6,9 miliardi di dollari, mentre gli attacchi *ransomware* avrebbero generato profitti pari ad almeno 1,2 miliardi di dollari (ref. https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2021-internet-crime-report e https://www.fincen.gov/news/news-releases/fincen-analysis-reveals-ransomware-reporting-bsa-filings-increased-significantly).

più efficienti[2]. Le frodi informatiche, spesso realizzate attraverso forme sofisticate di raggiro, rappresentano un fenomeno in continua evoluzione, che colpisce anche i cittadini[3].

La creazione di catene di fornitura sempre più lunghe e complesse, unitamente al moltiplicarsi e diversificarsi degli operatori, si è riflessa in un aumento considerevole della superficie di esposizione. Se nel 2020, in Europa, solo l'1% di compromissioni informatiche erano causate da attacchi cyber a terze parti, nel 2021 questo numero era già salito al 17%[4].

Il sistema finanziario, in cui operiamo, risulta particolarmente esposto alla minaccia cyber. La centralità del suo ruolo per il funzionamento di un'economia di mercato lo rende un bersaglio privilegiato per attori malevoli. A ciò si aggiunge che l'interconnessione con altre infrastrutture strategiche, tra le quali quelle energetiche e di telecomunicazioni, ne estende indefinitamente i confini. Inoltre, la stessa digitalizzazione del settore finanziario ha avuto come effetto benefico la disponibilità sempre maggiore di servizi innovativi di facile accesso e a costi decrescenti promuovendo così l'inclusione finanziaria, ma ne ha anche aumentato la vulnerabilità complessiva.

La minaccia cyber e il ruolo delle autorità finanziarie: regolamentazione, supervisione e cooperazione

Alla luce di queste osservazioni, la resilienza operativa digitale[5] è un elemento centrale della stabilità finanziaria: lo abbiamo evidenziato anche nel piano strategico per il triennio 2023-25 della Banca d'Italia appena pubblicato. Nella complessa rete di nodi e interconnessioni – che comprende gli istituti di credito, i prestatori di servizi di pagamento, le infrastrutture di mercato, gli investitori istituzionali, le compagnie assicurative, le imprese e i cittadini – le banche centrali svolgono un ruolo cruciale per assicurare la stabilità dell'intero sistema. La continuità operativa dei servizi finanziari è una precondizione indispensabile per tutti gli obiettivi assegnati alla Banca d'Italia ed in

---

2 La diffusione del paradigma del *Crime-As-a-Service*, per esempio, ha contribuito alla creazione di una catena del valore a supporto della criminalità, che consente anche a soggetti con limitate capacità tecniche, finanziarie o organizzative di condurre efficaci attività illegali nel cyber-spazio acquistando o appaltando i servizi necessari Inoltre, gli attacchi *ransomware* continuano a costituire una costante e diffusa minaccia per le organizzazioni pubbliche e private di tutto il mondo, generando rilevanti perdite economiche per le entità colpite e portando alla diffusione di ingenti volumi di dati sensibili, sia di tipo industriale che personale.

3 Dagli esposti presentati alla Banca d'Italia rileviamo che circa la metà delle truffe a danno della clientela di servizi finanziari è realizzata attraverso il furto di credenziali, con il ricorso a tecniche che sfruttano vulnerabilità tecnologiche dei sistemi informativi e di comunicazione, oltre che forme di ingegneria sociale. Lo confermano i reclami all'Arbitro bancario e finanziario, che, in un caso su quattro e con una casistica molto variegata, hanno per oggetto perdite e frodi subite nell'utilizzo di bonifici, carte e altri strumenti di pagamento elettronici.

4 https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends.

5 La resilienza operativa digitale attiene alla capacità degli operatori di assicurare nel tempo – anche in caso di incidenti di natura malevola o legati a malfunzionamenti interni – affidabilità e integrità operativa garantendo l'offerta dei propri servizi, attraverso i sistemi informatici e di rete.

particolare per la sana e prudente gestione degli intermediari, l'efficienza e l'affidabilità dei sistemi di pagamento, la fiducia nella moneta e la tutela degli utenti.

Nel percorso intrapreso la regolamentazione è un elemento cardine per assicurare una trasformazione digitale sostenibile e preservare la cyber-sicurezza. La fiducia del mercato nel corretto operato degli intermediari è perseguita anche attraverso un articolato e complesso sistema di regole e controlli. Quando questo sistema è ben tarato, i benefici per la collettività – specificatamente in termini di stabilità del sistema finanziario – sono indubbi. Tuttavia, dal punto di vista degli intermediari, essere assoggettati a questo corpus di regole e controlli rappresenta un costo significativo di *compliance*, che può incidere sulla stessa sostenibilità del modello di business. Rispetto ad altre fattispecie di rischio, quello cyber pone alle autorità ulteriori sfide di notevole complessità. In primo luogo è necessario ricercare il corretto equilibrio tra innovazione e sicurezza, ponendo attenzione agli impatti della regolamentazione e alla necessità di non inibire lo sviluppo di servizi finanziari più innovativi, inclusivi e competitivi. In secondo luogo è necessario dotarsi di strumenti di intervento adeguati, sul fronte regolamentare e della supervisione: una cassetta degli attrezzi che, pur fornendo un quadro di riferimento sufficientemente stabile, sia capace di adattarsi nel tempo all'evoluzione dei rischi, secondo principi di flessibilità e proporzionalità. Ciò al fine di mantenerne la validità nel tempo, contenere le complessità e assicurare l'appropriato raccordo con altre normative settoriali ed inter-settoriali e con gli standard internazionali.

È proprio a questi criteri che si ispira lo sforzo dei legislatori nazionali ed europei che negli ultimi anni sono intervenuti ampiamente sul tema della sicurezza dei servizi finanziari e della resilienza operativa digitale. A livello europeo abbiamo diversi esempi: la Direttiva sui servizi di pagamento (PSD 2)[6], la Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS)[7] e da ultimo il regolamento sulla resilienza operativa digitale (DORA)[8]: si tratta di norme che si pongono in una linea di continuità con l'azione regolamentare svolta nel tempo dalla Banca d'Italia nella sua veste di supervisore di intermediari e infrastrutture ma che offrono il vantaggio di introdurre un quadro armonizzato a livello europeo. A livello nazionale rileva anche la legge sul perimetro nazionale di sicurezza cibernetica e quella che ha istituito l'Agenzia Nazionale di Cybersicurezza[9], assegnando

---

6 Direttiva UE 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno.

7 Direttiva UE 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

8 Per assicurare livelli uniformi ed elevati di sicurezza informatica e la continuità di servizio in tutti gli ambiti e i settori dell'Unione Europea è in corso, da parte del legislatore europeo, uno sforzo imponente di produzione di norme. Il Regolamento DORA (2554) introduce requisiti armonizzati in tutta Europa per la resilienza operativa di tutte le categorie di operatori, anche quelli più innovativi come le piattaforme di *crowdfunding*. Il Regolamento introduce principi diretti a contenere i rischi derivanti dall'interconnessione del sistema finanziario con le terze parti (i providers tecnologici) e dalla concentrazione in capo ad uno stesso provider di tanti rapporti di esternalizzazione; darà anche avvio ad un nuovo regime di sorveglianza nei confronti dei fornitori tecnologici sistemici che sarà esercitato dalle tre autorità di europee di settore (EBA, EIOPA, ESMA) in base al settore finanziario prevalentemente servito dal provider. Inoltre, la norma intende favorire la condivisione delle informazioni tra comunità di operatori e introduce una nuova cornice di sorveglianza sui fornitori di servizi attribuendone la competenza alle autorità di vigilanza europee.

9 Decreto legge n. 82/2021, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

alla stessa competenze esclusive e un ruolo di punto di raccordo unico tra tutti i portatori di interesse, incluse le autorità finanziarie.

Affinché il controllo dei nuovi rischi cyber sia efficace, alla regolamentazione vanno affiancate altre forme di intervento, come quelle basate sulla cooperazione tra autorità e con gli operatori privati del settore finanziario nazionale e internazionale. La collaborazione tra tutti i soggetti del settore finanziario è cruciale per sviluppare una visione comune e un approccio di sistema che sia in grado di favorire la convergenza di policy, regole e standard per la gestione del rischio cyber, sviluppare competenze e coordinare azioni di risposta alle minacce emergenti.

Avendo presenti questi obiettivi, come Banca d'Italia contribuiamo attivamente ai lavori in diverse sedi di cooperazione europee e internazionali (es. Sistema Europeo delle Banche Centrali, G7, G20) e condividiamo le strategie per il presidio dei rischi cyber con altre autorità nazionali[10]. In questa strategia si inserisce anche la promozione di spazi di compartecipazione pubblico-privato in cui le diverse organizzazioni si scambiano informazioni sulle minacce cyber attraverso unità specializzate e mutuamente riconoscibili, i *Computer Emergency Response Team* (CERT).

Penso, come esempio di proficua interazione tra regole e cooperazione, all'azione di prevenzione delle frodi informatiche nei servizi di pagamento: in ambito europeo e nazionale sono state introdotte specifiche previsioni normative per l'accesso sicuro ai servizi finanziari; tra queste rileva l'introduzione dell'obbligo di autenticazione a più fattori per i pagamenti[11], che tutti noi come utenti abbiamo imparato a gestire negli ultimi anni; ma è fondamentale anche l'azione svolta, di concerto con altre istituzioni e con gli operatori finanziari privati, per la sensibilizzazione di cittadini e imprese attraverso iniziative di comunicazione mirate, anche all'interno dei programmi di educazione finanziaria.

L'impegno della Banca d'Italia nella prevenzione e protezione dalla minaccia cyber

Come Banca d'Italia siamo da sempre impegnati nella fornitura di servizi al sistema finanziario che richiedono il dispiegamento di infrastrutture e tecnologie all'avanguardia. Mi riferisco ad esempio alle infrastrutture di pagamento al dettaglio e all'ingrosso: nodi nevralgici del sistema finanziario nazionale ed europeo[12]. Nelle banche dati dell'Istituto sono conservati inoltre importanti dati sensibili, quali ad esempio quelli sui prestiti bancari

---

10 Un esempio di cooperazione istituzionale è stata la recente adozione congiunta, con Consob e IVASS, di un quadro di riferimento per l'esecuzione di test avanzati di sicurezza, il cd. TIBER-IT (basato su un analogo modello europeo, lo European threat intelligence-based ethical red teaming, TIBER-EU) con l'obiettivo comune di rafforzare le capacità di prevenzione, preparazione e risposta agli attacchi cyber dei principali operatori finanziari. Un ulteriore esempio è la costituzione di una struttura, operativa sin dal 2003, per il coordinamento di eventuali crisi operative del sistema finanziario nazionale, il cd. Codise (che sta per 'Continuità di servizio'), presidiato dalla Banca d'Italia e partecipato dalle altre autorità di settore e dalle istituzioni finanziarie di rilevanza sistemica.

11 Ai sensi della già citata Direttiva UE 2015/2366.

12 Ricordiamo in particolare i sistemi TARGET 2 e TARGET 2 Securities, BI-Comp e il Centro Applicativo della Banca d'Italia (CABI).

erogati a livello individuale nell'area dell'euro e le informazioni sui debiti di famiglie e imprese verso il sistema bancario e finanziario.

Siamo quindi costantemente impegnati nelle attività di prevenzione e contrasto della minaccia cyber a tutela dei servizi erogati in ambito nazionale ed europeo e per assicurare il corretto svolgimento dei compiti istituzionali dell'Istituto. In tale ambito, abbiamo promosso l'evoluzione del tradizionale modello di difesa basato sulle capacità individuali e di tipo reattivo, attingendo a modelli proattivi e cooperativi derivanti dal settore dell'intelligence. L'azione della Banca d'Italia è stata ed è cruciale nel costruire relazioni di fiducia tra tutte le parti coinvolte e sviluppare spazi e forme di cooperazione pubblico-privato per favorire lo scambio informativo sulla minaccia cyber tra controparti qualificate e mutualmente riconosciute. Si tratta di attività alla base del principio di sicurezza partecipata, che permette di contrastare in maniera più efficace la naturale asimmetria[13] della minaccia cyber. Questa è infatti non convenzionale, difficilmente individuabile, caratterizzata da elevate capacità, alta intensità e pone i difensori in una condizione di costante svantaggio rispetto agli attaccanti.

Coerentemente con questo principio, nel 2017 abbiamo istituito il CERT con lo scopo di partecipare allo sforzo collettivo di risposta alle minacce cyber e contribuire alla definizione di strategie di difesa adeguate alla prevenzione e mitigazione del rischio cyber. In collaborazione con l'ABI, la Banca ha inoltre dato vita al CERTFin, tavolo permanente nel quale gli operatori finanziari (a oggi circa 70 aderenti) condividono informazioni e analisi delle minacce cyber, collaborano nella risposta agli incidenti, promuovono iniziative per migliorare la consapevolezza dei rischi cyber da parte degli utenti dei servizi finanziari. Nella stessa logica, la Banca d'Italia partecipa a iniziative di cooperazione con il settore privato nell'ambito del Sistema Europeo delle Banche Centrali e di altri consessi internazionali.

Abbiamo inoltre sviluppato accordi e protocolli specifici con istituzioni nazionali e sovranazionali, al fine di ricondurre a fattor comune competenze e informazioni sulle minacce osservate nell'interesse nazionale e per la sicurezza del settore finanziario. L'ultimo in ordine di tempo è quello con la già menzionata Agenzia per la Cybersicurezza Nazionale (ACN) finalizzato allo scambio di informazioni idonee a prevenire e contrastare incidenti cyber che, anche potenzialmente, possano riguardare gli ambiti di interesse di ciascuna Istituzione.

Conclusioni e sfide per il futuro

Concludendo il mio intervento, voglio sottolineare che la minaccia cyber non riguarda solo vulnerabilità di tipo tecnologico, bensì anche e soprattutto quelle umane.

Anche nei sistemi meglio difesi, l'elemento umano può rappresentare l'anello debole della catena: ciò vale sia all'interno delle organizzazioni finanziarie, sia nella prospettiva degli utenti finali, cittadini, imprese e pubbliche amministrazioni. È dunque fondamentale continuare a investire sul capitale umano, che sia o meno direttamente impegnato

13 Con il termine contrasto asimmetrico ci si riferisce ad un conflitto non dichiarato, con notevole disparità di risorse militari o finanziarie e nello status dei due contendenti. Il contendente militarmente ed economicamente più forte deve difendersi da un avversario difficilmente individuabile, trovandosi in situazione di svantaggio.

nella prevenzione delle minacce cyber, per una diffusione più capillare possibile della consapevolezza dei rischi connessi con la nostra vita digitale.

La capacità di reclutamento e di mantenimento all'interno della propria compagine di personale specializzato è un fattore chiave di successo nella prevenzione delle minacce cyber per tutte le organizzazioni, siano esse pubbliche o private. Per questo è necessario che vengano affinati gli strumenti più idonei a questi scopi, nel riconoscimento delle peculiarità degli ambienti normativi nel quale ciascuno opera. In questo, la Banca d'Italia si è attivata nel favorire la selezione all'interno delle istituzioni pubbliche di risorse altamente qualificate.

Le autorità di supervisione dei mercati finanziari si trovano inoltre ad affrontare la sfida dell'aggiornamento continuo delle conoscenze per analizzare e valutare attentamente i rischi e le opportunità legate all'adozione di modelli di offerta e tecnologie emergenti. Mi riferisco ad esempio al campo delle cripto-attività, degli *smart contract* e delle componenti infrastrutturali sottostanti, come quelle basate su *cloud computing*, *blockchain* e altre tecnologie decentralizzate (le cd. *distributed ledger technologies*). Sul fronte della *governance e delle strategie per la difesa cyber*, la nascita dell'Agenzia per la Cybersicurezza Nazionale dotata di ampia autonomia e risorse rappresenta indiscutibilmente un importante passo avanti. Tramite essa, infatti, si potranno mettere a sistema più agevolmente le numerose competenze ed esperienze maturate in Italia sul tema della sicurezza cyber.

Gli eventi recenti ci hanno dimostrato che in uno spazio digitale sempre più interconnesso in un contesto caratterizzato da crescenti tensioni geopolitiche la comprensione e la gestione sistemica delle vulnerabilità e delle minacce cyber, richiedono una visione comune e uno sforzo condiviso da parte di tutti gli attori del sistema economico e dell'intero ecosistema, a partire dal livello locale, sino a quello nazionale e internazionale. Lungo questa direttrice, si inserisce il convegno di oggi, auguro quindi a voi tutti un proficuo e costruttivo confronto.

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