BANCA D'ITALIA
EUROSISTEMA

I test di tipo TLPT: dalle esperienze del TIBER-IT alle regole di DORA

Introduzione all'evento di Chiara Scotti
Vice Direttrice Generale della Banca d'Italia*

Centro Congressi "C.A. Ciampi"
Roma, 27 febbraio 2025

Autorità, rappresentanti delle istituzioni finanziarie, esperti di cybersicurezza, signore e signori,

penso che nessuno possa mettere in discussione l'importanza della resilienza digitale del sistema finanziario, in particolare alla luce del forte aumento, a livello globale, di attacchi informatici, cresciuti sia in numero che gravità: tra la metà del 2023 e quella del 2024 sono stati registrati circa 11.000 incidenti, di cui più della metà in Europa[1]. Secondo il Fondo Monetario Internazionale, il 20 per cento degli incidenti riguarda il settore finanziario[2]. Sono inoltre cresciuti gli incidenti classificabili come gravi, in termini di impatto economico, scala di diffusione, durata o grado di compromissione di dati sensibili o infrastrutture critiche. I settori più colpiti sono la sanità (con circa il 18 per cento), la difesa (13 per cento) e l'industria finanziaria e assicurativa (8 per cento)[3]. Il settore finanziario presenta un rischio elevato a causa dell'alta profittabilità degli attacchi e della quantità di dati sensibili custoditi dagli operatori. In un'economia digitale questi dati costituiscono una risorsa strategica.

Anche in Italia si è registrato un aumento considerevole degli incidenti, secondo i dati dell'Agenzia per la Cybersicurezza Nazionale (ACN): da 126 nel 2022 a 303 nel 2023[4]. Parallelamente, le segnalazioni raccolte dalla Banca d'Italia su gravi incidenti *cyber*, sono

---

* Per i contributi al testo di questo intervento si ringraziano Luca De Angelis e Antonino Fazio.

1 Agenzia Europea per la Cybersicurezza (ENISA), *ENISA Threat Landscape 2024* (2024).

2 Fondo Monetario Internazionale (FMI), *Global financial stability report* (2024).

3 Secondo il rapporto 2024 dell'Associazione italiana per la sicurezza informatica (Clusit), dal 2019 al 2024 il numero medio mensile di incidenti è raddoppiato, da 139 a 273. Ogni giorno si registrano mediamente 9 gravi incidenti informatici, di cui circa il 90 per cento motivati da obiettivi economici (cybercrime e/o frodi). Le principali tipologie di minacce cyber sono rappresentate da: (*i*) *malware* e *ransomware* (34 per cento); (*ii*) sfruttamento di vulnerabilità tecnologiche (14 per cento); (*iii*) *phishing* (8 per cento).

4 Agenzia per la Cybersicurezza Nazionale (ACN), *Relazione annuale al Parlamento* (2023).

cresciute del 160 per cento nel 2023 rispetto all'anno precedente[5] e, secondo prime stime, del 30 per cento nel 2024.

Questi numeri dimostrano quanto sia urgente investire nelle attività di testing, inclusa la valutazione dell'efficacia delle difese adottate dagli operatori. Di particolare rilevanza in questo ambito sono i test avanzati di cybersicurezza guidati dall'analisi della minaccia – i c.d. *Threat-Led Penetration Testing* (TLPT) – che il Regolamento europeo sulla resilienza operativa digitale (DORA)[6] rende obbligatori per le istituzioni finanziarie classificate come 'critiche'. La metodologia per i TLPT sviluppata dall'Eurosistema, nota come *Threat Intelligence Based Ethical Red-Teaming-EU* (TIBER-EU)[7], è stata declinata in Italia dalla Banca d'Italia, Consob e IVASS con il TIBER-IT[8].

A testimonianza della rilevanza di questo impegno condiviso, abbiamo oggi invitato rappresentanti delle autorità, dell'industria finanziaria e del mercato dei servizi di cybersicurezza. Insieme ci confronteremo sull'applicazione dei TLPT/TIBER-IT negli ultimi due anni, ragionando sulle esperienze fatte e sui possibili sviluppi prospettici. Prima dell'avvio dei lavori odierni, desidero però soffermarmi su tre aspetti: il ruolo trasversale svolto dalle attività di testing nei presidi a tutela della cybersicurezza, alcune delle lezioni apprese dai test TIBER-IT in Italia e la crescente rilevanza del rischio di terze parti.

1. Le attività di testing come fattore trasversale della cybersicurezza

Le Autorità europee hanno da tempo raccolto la sfida di rafforzare la cybersicurezza dell'Unione. A tal fine sono state definite linee guida che stabiliscono presidi specifici da applicare agli operatori finanziari, tra cui banche, istituti di pagamento e di moneta elettronica[9]. Di recente, il Regolamento DORA ha introdotto un quadro normativo armonizzato, articolato su cinque pilastri:

1. la gestione del rischio ICT;
2. la segnalazione degli incidenti *cyber*;
3. i test di resilienza operativa, tra cui i TLPT;

---

5 Quando si verifica un evento, gli operatori classificano gli incidenti come "gravi" se soddisfano criteri e soglie definiti dalla Banca d'Italia (in base al tipo e alle dimensioni degli intermediari) e li segnalano in modo tempestivo. Cfr. Banca d'Italia, *Digital resilience in the Italian financial sector: evidences from the supervisory incident reporting framework*"(2024). Cfr. Paolo Angelini, *La cybersicurezza del settore finanziario: ruolo delle autorità e valore della cooperazione* (2024).

6 Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011.

7 Cfr. la pagina dedicata sul sito della Banca Centrale Europea al seguente link.

8 Cfr. la pagina dedicata sul sito della Banca d'Italia al seguente link.

9 Cfr. European Banking Authority (EBA), *EBA Guidelines on ICT and security risk management* (2019), da tempo recepiti nelle istruzioni di vigilanza emanate dalla Banca d'Italia. Cfr. European Insurance and Occupational Pensions Authority (EIOPA), *Guidelines on information and communication technology security and governance* (2020). Cfr. European Securities and Markets Authority (ESMA), *Guidelines on outsourcing to cloud service providers* (2020).

4. la gestione del rischio legato alle terze parti ICT, incluso il nuovo quadro di sorveglianza europeo sui fornitori critici di servizi ICT;
5. la condivisione delle informazioni, in primo luogo quelle relative alle minacce significative.

In particolare, DORA prevede che gli operatori adottino un programma di test quale elemento integrato del loro *framework* di resilienza operativa digitale includendo diverse tipologie di strumenti, ad esempio valutazioni delle vulnerabilità e della sicurezza delle reti, analisi del *software* e *penetration tests*. Per un sottoinsieme di soggetti critici identificati dalle autorità secondo criteri quali-quantitativi, è prevista inoltre l'obbligatorietà, con cadenza almeno triennale, dell'esecuzione di test di sicurezza più avanzati, ossia i TLPT. Indipendentemente dalla dimensione, seppure con la dovuta proporzionalità, DORA richiede comunque che tutte le entità finanziarie adottino standard minimi di protezione cibernetica e una maggiore capacità di risposta alle situazioni di crisi dei sistemi informatici.

In questo sistema organico di presidi, i test servono a verificare l'efficacia delle misure di sicurezza e dei relativi processi gestionali, migliorando nel tempo la capacità di rilevamento, preparazione e risposta agli incidenti operativi e agli attacchi *cyber*. Nell'ambito dei test di resilienza operativa, i TLPT non si limitano alla semplice verifica di vulnerabilità tecniche, ma mettono alla prova l'intera resilienza digitale di un'organizzazione, coinvolgendo sistemi, processi, persone e fornitori. Svolgendo una funzione trasversale a tutti i pilastri di DORA, favoriscono un approccio proattivo e sistemico alla sicurezza, contribuendo alla stabilità dell'intero settore finanziario.

L'attuazione di DORA ha richiesto in Europa un articolato percorso cooperativo per definire gli standard tecnici regolamentari. Recentemente quelli sui test TLPT, fondamentali per il tema che trattiamo oggi, sono stati adottati dalla Commissione europea e sono ora allo scrutinio del Parlamento europeo e del Consiglio. Ad oggi non ci aspettiamo impedimenti o modifiche sostanziali, per cui l'iter legislativo dovrebbe concludersi entro fine maggio.

2. Il quadro metodologico italiano TIBER-IT: le prime esperienze

Come accennato, l'Eurosistema ha sviluppato la metodologia TIBER-EU per lo svolgimento di test di tipo TLPT già nel 2018. Ciò ha garantito un approccio armonizzato nella conduzione dei test per l'attuazione della strategia di resilienza *cyber* per le infrastrutture di mercato[10]. Ad oggi, il TIBER-EU è stato adottato da 16 Paesi europei[11] e utilizzato in più

---

10 La Banca d'Italia ha significativamente contribuito allo sviluppo della strategia e degli strumenti ad essa connessi. Dal 2022, la Banca ha assunto il coordinamento della *Task Force* incaricata di aggiornare la strategia, che è stata recentemente pubblicata. Cfr. la pagina dedicata sul sito della Banca Centrale Europea al seguente link.

11 Austria, Belgio, Danimarca, Finlandia, Francia, Germania, Islanda, Irlanda, Italia, Lussemburgo, Paesi Bassi, Norvegia, Portogallo, Romania, Spagna, Svezia. Inoltre, la Banca Centrale Europea (BCE) applica il *framework* a livello sovranazionale.

di 100 test. Questo dimostra l'interesse degli operatori che riconoscono il suo valore nel verificare la sicurezza dei loro sistemi. La previsione del Regolamento DORA di effettuare test TLPT obbligatori adottando la metodologia TIBER-EU non rappresenta dunque una novità assoluta in Europa.

Anche l'Italia si è mossa in questa direzione da tempo e con decisione: nel 2022 l'adozione della "Guida nazionale TIBER-IT" ha offerto alle istituzioni finanziarie italiane la possibilità di sottoporsi a test avanzati di cybersicurezza su base volontaria[12]. Finora la Banca d'Italia ha supervisionato lo svolgimento di test volontari su 12 soggetti di diverse tipologie, tra cui banche, assicurazioni e altri operatori attivi nel sistema dei pagamenti. Questi primi test hanno confermato la validità dello strumento e il suo valore. Le verifiche condotte hanno permesso di identificare elementi importanti di vulnerabilità delle singole istituzioni, di natura tecnica, procedurale e organizzativa.

A livello tecnico, ad esempio, i test hanno evidenziato la capacità di bloccare azioni malevole sul perimetro esterno di difesa e, al contrario, la difficoltà di contrastare le intrusioni una volta avvenuta la violazione, sottolineando la necessità di integrare la sicurezza fin dalla progettazione dei sistemi e di adottare i principi della "difesa in profondità". Sono inoltre emersi margini di miglioramento nella gestione delle identità e degli accessi[13].

A livello di processo, sono emerse indicazioni utili per il corretto bilanciamento tra la numerosità delle funzioni critiche da sottoporre a test e le risorse da allocare da parte degli operatori e dei fornitori.

A livello organizzativo, i test hanno rivelato come la composizione del c.d. *Control Team,* responsabile dell'intero processo di test, debba essere accuratamente ponderata per assicurare l'efficacia, la riservatezza e il controllo del test. In tal senso è necessario che il *team* sia partecipato almeno dai responsabili delle principali funzioni aziendali coinvolte: sicurezza informatica, continuità operativa e gestione dei rischi.

L'entrata in vigore di DORA ha reso necessario procedere all'aggiornamento della metodologia TIBER-EU[14] per allinearla ai nuovi standard tecnici sui TLPT, soprattutto nelle componenti relative all'utilizzo di tester interni e alle tempistiche del processo – in particolare per la fase di preparazione e per la fase di chiusura del test. Coerentemente, si sta ora procedendo a rivedere le versioni nazionali del TIBER, quindi anche del nostro TIBER-IT. L'esperienza e i risultati dei test condotti finora saranno sicuramente utili in questa prospettiva. In particolare, sarà fondamentale continuare a garantire la possibilità di eseguire verifiche su base volontaria per tutti gli operatori non soggetti all'obbligo di DORA, in un'ottica di resilienza *cyber* del sistema nel suo complesso.

---

12 Cfr. Luigi Cannari, *La resilienza cibernetica del sistema finanziario italiano: il ruolo dei test TIBER-IT* (2022).

13 Ad esempio, attraverso un utilizzo più esteso dell'autenticazione multifattoriale.

14 Cfr. la pagina dedicata sul sito della Banca Centrale Europea al seguente link.

3. La rilevanza del rischio di terze parti, anche per i test di tipo TLPT

Un aspetto finale su cui vorrei soffermarmi è la crescente rilevanza del rischio di terze parti. La digitalizzazione del sistema finanziario ha portato un forte aumento di funzioni, attività e procedure tecnico-operative che gli intermediari vigilati affidano a operatori tecnologici, le c.d. terze parti o *third-party providers*. Secondo la recente analisi delle autorità di supervisione europee in preparazione di DORA, circa 3.500 operatori hanno segnalato 25.000 contratti con circa 10.000 fornitori[15]. Nell'ambito delle attività di vigilanza della Banca d'Italia, gli intermediari italiani hanno segnalato oltre 5.000 contratti di esternalizzazione di funzioni essenziali[16]. Questi fornitori sono spesso completamente esterni al perimetro finanziario, offrono servizi a una pluralità di settori economici, manifatturieri e del terziario e, in molte giurisdizioni, sono sottoposti a forme di supervisione più debole, se non inesistenti, rispetto agli operatori da essi serviti[17].

La resilienza *cyber*, quindi, dipende anche dalla solidità dei fornitori di tecnologia. Essi rappresentano uno snodo che richiede particolare attenzione, come mostrato da alcuni episodi anche recenti, di matrice malevola e non. Tra quelli malevoli ricordiamo gli attacchi *ransomware* su un fornitore italiano di servizi di gestione documentale e comunicazione, utilizzato da molti soggetti finanziari e su un fornitore internazionale di servizi a supporto della negoziazione e regolamento titoli. A questi si aggiungono alcuni recenti e rilevanti incidenti operativi non legati ad attacchi *cyber*, come i casi Crowdstike e Worldline dell'anno scorso.

Un aspetto innovativo di DORA è proprio l'attenzione del Regolatore alla gestione del rischio derivante dalle terze parti, in particolare da quelle definite come 'critiche' in base a indicatori quali-quantitativi e alle interdipendenze nel settore finanziario.

Un caso peculiare è costituito dai fornitori esterni coinvolti nello svolgimento dei TLPT, segnatamente per due tipologie specifiche di servizi di cybersicurezza: le c.d. *threat intelligence*[18] e *red teaming*[19]. Per minimizzare i rischi insiti in attività di test sui sistemi in produzione è necessario assicurare la qualità e l'affidabilità di questi fornitori. A tal proposito, la metodologia TIBER-EU e il Regolamento DORA prevedono requisiti per l'acquisizione dei citati servizi da parte degli operatori: la valutazione delle esperienze pregresse, delle competenze tecniche, di eventuali certificazioni, la sottoscrizione di assicurazioni professionali e l'aderenza a codici etici. Ai fornitori si chiede anche di adottare misure di sicurezza rigorose, perché essi stessi sono potenziali bersagli di attaccanti interessati ad accedere a informazioni sensibili.

---

15 Cfr. EBA, EIOPA, ESMA, *ESAs workshop on DORA dry run lessons learnt and data quality* (2024).

16 Cfr. Banca d'Italia, Relazione annuale (2024).

17 Cfr. Financial Stability Board (FSB), *Enhancing Third-Party Risk Management and Oversight* (2023).

18 Informazioni sulle minacce che sono state aggregate, trasformate, analizzate, interpretate o arricchite per fornire il contesto necessario ai processi decisionali. Cfr. FSB, *Cyber lexicon* (2023).

19 Si tratta di una simulazione controllata di un attacco condotta da un gruppo indipendente (*red team*) utilizzando le tattiche, le tecniche e le procedure degli attori della minaccia reali.

Nel corso del convegno odierno presenteremo i risultati di un'indagine sull'offerta di servizi di cybersicurezza in Italia, condotta lo scorso anno e volta a delineare le principali caratteristiche delle imprese attive in questo comparto, con un *focus* specifico sui servizi relativi ai TLPT. I risultati mostrano il grande dinamismo di questo comparto dell'industria, caratterizzato da una sensibile espansione del fatturato, dalla presenza di numerose nuove imprese e da frequenti cambi di assetto societario. È interessante notare che circa il 70 per cento dei rispondenti ha dichiarato di offrire o di voler offrire servizi per lo svolgimento dei TLPT, con una incidenza più elevata delle imprese di maggiori dimensioni.

4. Conclusioni

I test TLPT rappresentano un'opportunità unica per rafforzare la resilienza del settore finanziario. È in questo spirito che tutti i soggetti, anche quelli che non rientrano specificatamente nel perimetro delle disposizioni di DORA, dovrebbero adottare un approccio proattivo alla gestione delle minacce *cyber*, ricorrendo su base volontaria al *framework* TIBER-IT reso disponibile dalle Autorità. Questi strumenti non devono essere considerati un mero requisito regolamentare, ma un vero e proprio investimento nella resilienza digitale delle organizzazioni e dell'intero sistema finanziario.

A tal proposito, in un'ottica prospettica, vorrei richiamare tre punti di attenzione: il costo dei test, la disponibilità di risorse qualificate e l'opportunità di un coordinamento sovranazionale.

Lo sviluppo del mercato di questi servizi contribuirebbe a una maggiore concorrenza, ottimizzazione dei costi e qualità dei test, rendendo i TLPT accessibili a un numero maggiore di operatori.

La collaborazione tra Autorità, accademia, industria finanziaria e dei servizi ICT favorirebbe lo sviluppo di personale con competenze nella cybersicurezza, ampliando così la disponibilità di professionisti specializzati nei servizi necessari ai TLPT[20].

Infine, un miglior coordinamento tra le autorità finanziarie europee aiuterebbe ad evitare che i TLPT diventino eccessivamente gravosi, soprattutto per gli operatori paneuropei o quelli che forniscono servizi finanziari a più soggetti. Ove opportuno e come previsto dalla normativa, andrà favorita la realizzazione di test congiunti tra più operatori (c.d. *joint test*).

---

20 Cfr. Alessandra Perrazzelli, *Cyber sicurezza: Una continua sfida per l'economia e per la società* (2023).

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