## Adozione della Guida nazionale del TIBER-IT

La crescente sofisticazione e pervasività della minaccia cibernetica nelle economie moderne, anche come conseguenza della loro rapida digitalizzazione e della profonda interconnessione tra diversi attori e paesi, ha posto la resilienza cibernetica[1] tra le priorità di azione per i governi, gli organismi internazionali e le autorità. Le evoluzioni più recenti hanno dimostrato come sia necessario presidiare in misura crescente, ai vari livelli, la resilienza cibernetica delle infrastrutture vitali e dei maggiori operatori, per assicurare la continuità delle attività economiche e dei servizi alla collettività e la loro sicurezza e affidabilità, di pari passo con lo sviluppo digitale dell'economia e della società.

La minaccia cibernetica è particolarmente accentuata per il settore finanziario, in ragione delle motivazioni economiche degli attaccanti, della numerosità e diversificazione dei soggetti che vi operano, della stretta interconnessione tra i diversi nodi del sistema: è molto elevata la possibilità che un malfunzionamento o un grave attacco a un singolo operatore possa trasmettersi ad altri e che, per tale via, possa essere compromessa la stabilità e l'efficienza del sistema finanziario, la continuità dei servizi finanziari, bancari e assicurativi, la sicurezza del sistema dei pagamenti e la fiducia di cittadini e imprese.

Gli organismi di regolamentazione e standardizzazione a livello internazionale ed europeo e le autorità del sistema finanziario hanno adottato e stanno perfezionando numerose misure per rafforzare la capacità di prevenzione, difesa e reazione dei singoli operatori e del sistema finanziario nel suo complesso alla minaccia cibernetica.

In tale ambito, rileva in particolar modo l'obiettivo di rafforzamento della capacità di difesa proattiva delle entità finanziarie, anche attraverso lo svolgimento di *penetration test* avanzati, commisurati alla rilevanza e complessità degli scenari di rischio e ai modelli di business e operativi di ciascuna entità finanziaria. In tale direzione muovono le guide metodologiche, le raccomandazioni e la regolamentazione emanate a livello internazionale ed europeo[2], volte anche a favorire l'applicazione di metodologie armonizzate e comparabili per la realizzazione di tali test, in ragione dei collegamenti tra i vari comparti del sistema finanziario e delle sue interconnessioni a livello internazionale. A livello europeo, il modello di riferimento per la conduzione di test della specie è costituito dalla metodologia *Threat Intelligence-based Ethical Red Teaming* o TIBER-EU, adottata dalla BCE[3] nel 2018.

Al fine di dotare il sistema finanziario italiano di una metodologia di riferimento per la conduzione, su base volontaria, da parte delle singole entità finanziarie di test avanzati di sicurezza guidati dallo

---

[1] "*The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.*" (FSB Cyber Lexicon, 2018).

[2] G7 *Fundamental Elements for Threat-Led Penetration Testing* (G7FE-TLPT), G7 Cyber Expert Group, 2018; *G7 Fundamental elements for cyber security in the financial s*ector (G7FE), G7 Cyber Expert Group, 2016; *Guidance of Cyber Resilience for Financial Market Infrastructures*, CPMI-IOSCO, 2016. A livello europeo rilevano: i) la proposta del *Digital Operational Resilience Act,* ii) le *Guidelines on information and communication technology security and governance dell'* EIOPA (*EIOPA-BoS-20/600*); iii) le *Guidelines on ICT and security risk management* dell'EBA (EBA/GL/2019/04); iv) le *Guidelines on outsourcing to cloud service providers dell*' ESMA (ESMA50-164-4285); v) il *Joint Advice on the costs and benefits of a coherent cyber resilience testing framework* delle tre ESAs.

[3] La BCE ha reso obbligatoria la conduzione di test di tipo TIBER-EU per i sistemi di pagamento di rilevanza sistemica europei; a livello nazionale è stata lasciata facoltà alle autorità competenti di adottare metodologie analoghe su base obbligatoria o volontaria.

scenario della minaccia, il framework TIBER-EU è recepito tramite l'allegata Guida nazionale TIBER-IT, che è stata adottata dalla Banca d'Italia, dalla Consob e dall'IVASS.

In continuità con le finalità della strategia congiunta per la sicurezza cibernetica del settore finanziario italiano emanata dalla Banca d'Italia e dalla Consob[4], l'adozione della Guida consente di migliorare la resilienza cibernetica del sistema finanziario italiano e, per tale via, la sua stabilità complessiva.

Il TIBER-IT si rivolge a più tipologie di entità finanziarie italiane: le infrastrutture di mercato, i gestori di sistemi di pagamento e di infrastrutture strumentali tecnologiche o di rete, le sedi di negoziazione, le banche, gli istituti di pagamento e gli istituti di moneta elettronica, gli intermediari finanziari ex art. 106 TUB, le imprese di assicurazione e gli intermediari assicurativi. I test potranno essere condotti dalle entità finanziarie su base volontaria, tenuto conto del livello di maturità cibernetica raggiunto da ciascuna; l'entità finanziaria mantiene la decisione finale di sottoporsi al test ed è responsabile della gestione di tutti i rischi correlati alla sua esecuzione, che avviene a cura di società scelte dall'entità che si sottopone al test. Le tre Autorità indirizzano la programmazione dei test in linea con l'evoluzione degli scenari di rischio e la rilevanza delle entità finanziarie per la continuità di servizio del settore.

In particolare, la Guida nazionale TIBER-IT: a) definisce la metodologia e il modello operativo per la conduzione di test di tipo TLPT da parte delle entità finanziarie italiane; b) individua le fasi in cui si articola il processo di test; c) definisce i ruoli e le attività dei diversi attori coinvolti (Autorità, soggetto che effettua il test e fornitori esterni).

Per supportare le entità finanziarie nell'utilizzo della nuova metodologia e nelle attività di test, le tre Autorità mettono a disposizione un centro di competenza dedicato: il TIBER Cyber Team Italia (TCT), il cui funzionamento è assicurato da esperti della Banca d'Italia, in collaborazione con quelli della Consob e dell'IVASS.

Il TCT è raggiungibile tramite l'indirizzo email: tiber-it@bancaditalia.it.

Si confida sull'adesione da parte delle maggiori entità finanziarie italiane alla nuova metodologia TIBER-IT e sul loro svolgimento proattivo di test di tipo TLPT, come ulteriore tassello del proprio percorso di rafforzamento nella gestione delle principali ed emergenti tipologie di rischio.

La presente nota e la Guida nazionale TIBER-IT sono pubblicate sui siti internet della Banca d'Italia, della Consob e dell'IVASS.

| per la CONSOB<br>Il Presidente | per l'IVASS<br>Il Presidente | per la BANCA D'ITALIA<br>Il Governatore |
|---|---|---|
| *Paolo Savona* | *Luigi Federico Signorini* | *Ignazio Visco* |

[4] https://www.bancaditalia.it/media/comunicati/documenti/2020-01/cs_BIConsob_20200116_ST.pdf.