BANCA D'ITALIA
EUROSISTEMA

La resilienza cibernetica del sistema finanziario italiano: il ruolo dei test TIBER-IT

Intervento di Luigi Cannari
Capo del Dipartimento Mercati e sistemi di pagamento

Banca d'Italia – Sede di Milano
Via Moneta, 3, e in video-conferenza
13 ottobre 2022

Gentili ospiti,

a nome della Banca d'Italia, di Consob e di IVASS ringrazio i presenti e chi è collegato da remoto per seguire il convegno di oggi, rivolto a intermediari finanziari, imprese assicurative e fornitori di servizi tecnologici di sicurezza. Tratteremo della metodologia di test di cybersicurezza TIBER-IT, pubblicata dalle tre autorità finanziarie lo scorso mese di agosto: in prima battuta potrebbe apparire un argomento squisitamente tecnico, ma in realtà esso riveste un'importanza centrale nelle strategie che le autorità e gli operatori finanziari stanno mettendo in campo per governare efficacemente i rischi connessi con la digitalizzazione dei servizi.

Il contesto: importanza dei test nel prevenire i rischi cyber

La digitalizzazione, l'interconnessione sociale ed economica sono ormai diventati un dato strutturale della nostra società, e in particolare del sistema finanziario. Ciò presenta vantaggi e opportunità innegabili, ma genera anche nuove insidie. Negli ultimi anni i governi, le autorità di supervisione, gli organismi internazionali hanno posto una crescente attenzione ai rischi di attacchi cyber; questa attenzione è stata accentuata dai rapidi cambiamenti delle abitudini in tempi di pandemia e, da ultimo, dal peggioramento del contesto geopolitico. Oggi i potenziali attori della minaccia sono molteplici: entità para-statuali, organizzazioni criminali, gruppi antagonisti o semplici attivisti, ognuno con proprie peculiarità nella motivazione, nel modus operandi, nelle risorse a disposizione.

In questo contesto, gli intermediari finanziari devono presidiare e rafforzare le proprie capacità di difesa e il livello di resilienza operativa digitale, e devono farlo nel continuo; ciò vale in modo particolare per gli operatori a rilevanza sistemica, cioè i maggiori istituti di credito e imprese assicurative, le infrastrutture di mercato e tutti gli operatori che offrono servizi vitali per il settore. È dunque importante verificare l'efficacia delle capacità di difesa attraverso strumenti evoluti che consentano di simulare realisticamente i comportamenti e le tecniche messe in campo da chi mira a colpire il settore finanziario.

Il ruolo delle autorità finanziarie e della cooperazione nella promozione dei test

In questo contesto, Banca d'Italia, Consob e IVASS mettono a disposizione degli operatori finanziari la Guida Nazionale TIBER-IT, una metodologia per la conduzione dei test di sicurezza avanzati guidati dall'analisi della minaccia – anche comunemente noti con i termini *Red Teaming* o *Threat-Led Penetration Testing* (TLPT).

L'emanazione della Guida è stata il frutto di un percorso delle tre autorità avviato ad inizio 2020 con la pubblicazione della strategia congiunta Banca d'Italia-Consob per rafforzare la cyber resilienza del settore finanziario. Tra gli altri strumenti, lì si faceva già riferimento alla futura adozione del TIBER-IT: il recepimento nazionale del framework di testing TIBER-EU sviluppato in ambito Eurosistema – con un contributo di primo piano della Banca d'Italia – e diventato *de facto* un modello di riferimento non solo europeo ma mondiale.

L'adozione di una metodologia avanzata per i test di cybersicurezza è un esempio di come le strategie di intervento delle autorità finanziarie si stiano adeguando ad un contesto in rapida evoluzione: esse devono esser capaci di comprendere più rapidamente le minacce emergenti e promuovere lo sviluppo di buone prassi e di nuove forme di cooperazione e di scambio informativo, idonee a creare una cultura della sicurezza diffusa e condivisa.

L'adozione del TIBER-IT – che come vedremo meglio oggi si ispira a logiche distanti dai tradizionali metodi regolamentari e di supervisione – non è l'unico esempio di questa evoluzione. In Italia da diversi anni abbiamo avviato positive iniziative di cooperazione nel campo della cybersicurezza, come il CERTFin, l'organismo cooperativo tra autorità e operatori finanziari in tema di cyber resilience, attraverso il quale la Banca, insieme ad ABI e in collaborazione con le altre autorità e associazioni del settore finanziario e assicurativo, promuove la condivisione delle informazioni e di buone prassi tra gli aderenti. Tra le varie iniziative, anche il CERTFin si è occupato di metodologie per lo svolgimento di test, per l'analisi delle minacce e la prevenzione dei rischi informatici, stimolando competenze ed esperienze tra gli aderenti che potranno essere ben valorizzate con l'avvio del TIBER-IT.

Obiettivo dei test e futuri sviluppi regolamentari

Come nella stragrande maggioranza delle altre giurisdizioni che hanno recepito il TIBER-EU, i test TIBER-IT sono svolti su base volontaria e non costituiscono uno strumento di supervisione. Essi mirano ad individuare possibili lacune nelle capacità di rilevamento, protezione e risposta agli attacchi cyber, e non si configurano come esercizi di compliance di tipo *pass or fail*. La Guida TIBER-IT specifica in dettaglio quali sono i ruoli e le responsabilità di tutti gli attori del processo, con particolare riferimento al personale delle entità finanziarie e dei fornitori dei servizi di cybersicurezza. Un test TIBER segue un iter ben strutturato, volto a prevenire possibili rischi insiti in qualsiasi test che viene effettuato sugli ambienti di produzione e senza preventiva conoscenza da parte delle funzioni di sicurezza dell'entità testata, deputate alla protezione degli assetti aziendali. Dalle lezioni sin qui apprese dalla conduzione di questi test in Europa, per massimizzare i risultati dei test TIBER è di fondamentale importanza l'impegno attivo dell'entità finanziaria che svolge il test, a partire dalla sua Alta Dirigenza.

In tale contesto, pur ribadendo la volontarietà dei test TIBER-IT, anche a nome di Consob e IVASS, le autorità di vigilanza si aspettano un'ampia partecipazione delle entità finanziarie, a partire da quelle a rilevanza sistemica, soprattutto alla luce dei futuri sviluppi regolamentari. Il regolamento UE DORA, di ormai prossima pubblicazione, richiederà alle entità finanziarie di prevedere piani di test che includano diversi strumenti e metodologie. Tra questi, per gli operatori che saranno indicati dalle autorità competenti i test di tipo TLPT diverranno obbligatori. È quindi raccomandabile che le entità finanziarie, da qui ad allora, sfruttino questo lasso di tempo utilizzando il TIBER-IT, strumento a loro disposizione, per prepararsi in vista dell'entrata in vigore del Regolamento.

Rapporti con altri settori e ruolo dei fornitori di servizi di cybersicurezza

Il TIBER-EU e di conseguenza il TIBER-IT sono strumenti ideati per il settore finanziario, ma per definizione sono agnostici e pertanto, con i necessari aggiustamenti, la loro adozione può essere estesa ad altri settori critici, come ad esempio l'energia, le telecomunicazioni e la sanità. Questo già avviene in altre giurisdizioni, per esempio nei Paesi Bassi. Ecco perché un altro fattore importante è lo sviluppo di un mercato interno per i servizi di cybersicurezza erogati al sistema finanziario (e non solo), vista la sensibilità dei dati trattati e dei sistemi testati, anche alla luce delle tensioni geopolitiche. Ciò risponde all'esigenza di rafforzare l'indipendenza tecnologica del sistema Paese, uno degli obiettivi chiave della strategia nazionale di cybersicurezza.

* * *

In conclusione, desidero rimarcare l'importanza della collaborazione tra tutti gli attori dell'ecosistema finanziario per rafforzarne la resilienza operativa digitale nel suo complesso. Banca d'Italia, Consob e IVASS hanno pubblicato la Guida nazionale TIBER-IT come un ulteriore tassello di un percorso congiunto per la resilienza cyber sia italiano che europeo. Essa si collega idealmente alla riforma introdotta di recente in Italia per dotarsi di strategie, mezzi e strutture dedicate alle sfide della cybersicurezza, che vede al centro la creazione della Agenzia per la cybersicurezza nazionale. Oggi ascolteremo il Direttore dell'Agenzia, il prof. Baldoni, che potrà darci il suo punto di vista sulle sfide che dobbiamo affrontare e su come raccordare efficacemente le strategie settoriali con le azioni governative per la sicurezza dei cittadini, delle imprese e delle istituzioni del nostro Paese.

Ringrazio nuovamente tutti i partecipanti, ognuno portatore di interessi diversi, ma tutti convergenti verso l'obiettivo del rafforzamento della sicurezza delle nostre infrastrutture finanziarie. Su temi così trasversali il confronto e la condivisione delle informazioni tra le autorità e il mercato sono essenziali per impostare le azioni di prevenzione e contrasto nei confronti della crescente minaccia cibernetica. Confido in una proficua discussione e un aperto dibattito.

Auguro a tutti buon lavoro.

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