BANCA D'ITALIA
EUROSISTEMA

Report Esercitazione Codise TP2018

Esercitazione di continuità operativa per gli operatori a rilevanza sistemica della piazza finanziaria italiana

11 dicembre 2018

BANCA D'ITALIA
EUROSISTEMA

Sommario

Introduzione

Il Codise, struttura deputata al coordinamento delle crisi operative della piazza finanziaria, nell'ambito delle proprie funzioni, promuove attività per esercitare i piani di continuità operativa dei partecipanti e la collaborazione tra gli attori del sistema finanziario italiano, utilizzando scenari che impattino i processi a rilevanza sistemica.

In tale ambito, l'esercitazione di continuità operativa TP2018, svolta l'11 dicembre 2018 presso il Centro Convegni della Banca d'Italia a Roma, ha rappresentato un'importante opportunità per testare l'utilizzo dei piani di continuità operativa e di comunicazione dei partecipanti.

L'esercitazione ha permesso agli operatori sistemici[1] della piazza finanziaria italiana di esercitarsi individualmente e collettivamente a fronteggiare uno scenario cyber avverso, con impatti rilevanti sulla propria operatività e sull'intero sistema dei pagamenti.

L'esercitazione proposta, di tipo "table top"[2], ha simulato un attacco cyber ai sistemi di pagamento al dettaglio, con compromissione dell'integrità dei dati di pagamento.

[1] Si tratta di soggetti, che, in caso di grave incidente operativo, potrebbero causare un impatto sistemico sulla piazza finanziaria italiana. A essi, quindi, la normativa impone requisiti rafforzati di continuità operativa e la partecipazione al Codise. Tali operatori sistemici vengono individuati dalla Banca d'Italia ogni tre anni applicando criteri oggettivi.

[2] Si tratta di un incontro durante il quale i partecipanti discutono le azioni da intraprendere nel caso di un evento avverso simulato, senza realmente attivare le procedure di emergenza né operare sui sistemi informativi.

Obiettivi dell'esercitazione

L'esercitazione ha offerto la possibilità ai partecipanti di esercitarsi a fronteggiare uno scenario avverso e di:

- analizzare un evento anomalo e indirizzarne la corretta gestione come previsto dalle proprie procedure organizzative;

- utilizzare i propri piani di continuità operativa, in una situazione potenzialmente critica che abbia impatti sulla propria operatività, includendo l'analisi dell'opportunità di notifica al Codise dell'evento e degli eventuali conseguenze sistemiche;

- definire eventuali comunicazioni interne ed esterne alla propria organizzazione;

- aumentare la consapevolezza sulle problematiche riguardanti le attività di pagamento e sugli impatti che esse possono avere non soltanto sui propri processi e sistemi ma anche sulle entità a loro connesse, sul sistema dei pagamenti e sulla piazza finanziaria nel suo complesso;

- collaborare e comunicare tra loro e con le autorità in caso di attivazione del Codise;

- identificare e analizzare eventuali misure che potrebbero essere attuate fra i partecipanti interessati per incrementare le loro capacità di risposta e di condivisione delle informazioni e dati utili.

Caratteristiche esercitazione

I partecipanti sono stati impegnati in una discussione, individuale e collettiva, riguardo alle decisioni da assumere e le azioni da intraprendere, sulla base di uno scenario teorico predefinito con impatto sulla propria operatività e su quella del sistema finanziario italiano nel suo complesso.

I processi, le applicazioni e i sistemi reali non sono stati interessati dalle attività dell'esercitazione. Non sono state, inoltre, simulate attività operative, comunicazioni tramite telefono, email o svolgimento di riunioni e teleconferenze o azioni di attori e autorità esterni al Codise.

I partecipanti sono stati informati degli eventi in modo graduale, attraverso un set di informazioni (*inject*[3]) sequenziali. Dopo la ricezione di ogni inject, gli operatori hanno avuto la possibilità di discutere individualmente le azioni da intraprendere e di confrontarsi, in seguito, con gli altri partecipanti, in una discussione moderata dai rappresentanti della Banca d'Italia.

Nella parte finale sono stati approfonditi gli elementi d'interesse emersi durante la giornata e si è discusso di possibili aree di miglioramento.

[3] Set di informazioni che descrivono, gradualmente e con maggiore dettaglio, gli eventi collegati all'anomalia riscontrata nel funzionamento del sistema dei pagamenti.

Scenario e Risultati

L'esercitazione ha simulato un attacco cyber al sistema finanziario italiano con impatto sull'integrità dei dati di alcuni operatori.

La discussione che ne è seguita ha rappresentato un importante momento di confronto e fornito spunti di riflessione che si ritiene opportuno approfondire, con l'obiettivo di rafforzare nel continuo l'efficacia del Codise e la resilienza della piazza finanziaria italiana.

L'argomento maggiormente discusso ha riguardato l'obiettivo di assicurare tempi di ripristino dell'operatività rapidi anche in caso di scenari estremi ma plausibili, in quanto l'indisponibilità prolungata dei processi a rilevanza sistemica potrebbe avere impatti di rilievo sulla piazza finanziaria italiana e minare la fiducia del pubblico negli strumenti alternativi al contante.

Si è discusso, inoltre, del potenziale impatto sistemico delle frodi sui pagamenti al dettaglio. Al momento in ambito internazionale, dopo i casi di frode effettuati tramite la rete SWIFT, l'attenzione delle autorità è focalizzata sui pagamenti all'ingrosso. L'esercitazione ha mostrato che un'eventuale frode cyber ai danni del sistema dei pagamenti al dettaglio, potrebbe avere implicazioni di natura sistemica.

Altri aspetti emersi dalla discussione sono stati:

- dipendenza da sistemi di compensazione esteri: circa tre quarti del numero totale dei pagamenti al dettaglio nazionali è elaborato da sistemi paneuropei, sotto la supervisione della BCE. Ciò pone problemi di comunicazione e coordinamento in caso di grave crisi di tali operatori, che non partecipano al Codise;

- possibile utilizzo di canali di regolamento alternativi: alcuni partecipanti hanno proposto come soluzione temporanea al problema previsto dallo scenario l'utilizzo di canali alternativi, per esempio i sistemi dei pagamenti "instant" o all'ingrosso. Andrebbero gestiti, in tal caso, la complessità dell'operazione di trasferimento dell'operatività e un eventuale aggravio di costi per gli utenti del servizio;

- rilevanza della comunicazione: tutti i partecipanti hanno concordato sulla necessità di assicurare un coordinamento a livello Codise delle comunicazioni verso l'esterno in caso di attacchi Cyber che, coinvolgendo diversi operatori abbiano natura sistemica.

I partecipanti hanno comunicato, sia durante lo svolgimento dell'esercitazione che nei moduli di feedback, un'ampia soddisfazione per le attività svolte, ritenendo altresì utile lo svolgimento di attività simili con maggior frequenza.

Prospettive

I risultati dell'esercitazione indicano l'opportunità di svolgere alcuni approfondimenti. In particolare con l'obiettivo di:

i. valutare come dare concreta attuazione alla "*Guidance on cyber resilience for financial market infrastructures*" attraverso l'istituzione di presidi adeguati alla rapida ripartenza dei servizi a seguito d'incidente "Cyber" anche in caso di scenario estremo ma plausibile[4];

ii. verificare la possibilità concreta di utilizzare canali alternativi in caso di problematica bloccante nei sistemi di pagamento al dettaglio;

iii. avviare una interlocuzione con gli operatori con sede al di fuori del territorio nazionale per facilitare un coinvolgimento dei sistemi di pagamento non italiani in casi analoghi a quello simulato nell'esercitazione.

[4] La "*CPMI/IOSCO Guidance on cyber resilience for financial market infrastructures*" del 2016 ha considerato l'eventualità che, in casi particolarmente gravi, una FMI non sia in grado di ripartire entro le 2 ore e ha raccomandato alle FMI di: a) prevedere un piano di emergenza per il contenimento dell'impatto e che, in ogni caso, garantisca una chiusura regolare della giornata operativa; b) sviluppare piani concreti entro 12 mesi dalla pubblicazione della guida al fine di accrescere le proprie capacità di resilienza cyber per essere in grado di rispettare il requisito delle 2 ore anche in caso di scenari estremi ma plausibili.