BANCA D'ITALIA
EUROSISTEMA

CODISE

Cyber Poison 2014

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

17 ottobre 2014

Introduzione

La sesta simulazione nazionale di continuità operativa organizzata dal CODISE si è svolta il 17 ottobre 2014; oltre alla Banca d'Italia e alla CONSOB, vi hanno partecipato gli operatori a rilevanza sistemica della piazza finanziaria italiana: Banco Posta, Cassa Compensazione e Garanzia, e-MID, Equens, ICBPI, ICCREA, Intesa San Paolo, Monte Paschi Siena, Monte Titoli, MTS, SIA, Unicredit. In relazione allo scenario è stata invitata a partecipare anche Borsa Italiana.

Nell'esercitazione, i partecipanti hanno operato presso le loro sedi; la normativa di riferimento ha richiesto la presenza degli internal auditors. Le risorse complessivamente impegnate sono state pari a oltre 600 giorni-uomo.

Obiettivi

L'esercizio intendeva verificare l'efficacia del processo di adeguamento degli operatori sistemici ai nuovi requisiti di continuità operativa e alla guida CODISE con riferimento a:

- la gestione di situazioni estreme caratterizzate da scenari di crisi estesa e blocchi prolungati delle infrastrutture dei mercati finanziari, che richiedano il ricorso a procedure a bassa integrazione nei processi aziendali per le esigenze di liquidità proprie e della clientela;
- le misure per la escalation, il processo per la dichiarazione e gestione dello stato di crisi, l'integrazione con il processo per la gestione degli incidenti;
- la gestione delle comunicazioni con le controparti rilevanti;
- il rientro dall'emergenza, con particolare attenzione alla rilevazione dei danni, alla gestione del le operazioni di rientro, alla verifica dell'operatività per i servizi ripristinati.

Caratteristiche della simulazione

L'esercitazione non richiedeva il recovery tecnologico, non interessava i dati di produzione né le procedure operative dei soggetti convolti, non richiedeva la disponibilità di particolari ambienti tecnologici di collaudo dei servizi finanziari, fatta eccezione per gli apparati di comunicazione, non coinvolgeva soggetti esterni al CODISE.

La simulazione si è svolta in tre sessioni: mattutina (08:00 - 13:00) dedicata al crisis management; pomeridiana (15:00 - 16:30) focalizzata sul rientro all'operatività ordinaria; serale (17:30 - 18:30) dedicata alla discussione, coordinata dal Vice Direttore Generale della Banca d'Italia (dr. Fabio Panetta), sull'andamento dell'esercitazione e sulle possibili aree di miglioramento.

Scenario

L'esercitazione, chiamata Cyber Poison 2014 e progettata da una task force di membri del CODISE, ha ipotizzato un evento di portata molto ampia con conseguenze diverse sui singoli partecipanti. Come in un evento reale i partecipanti sono stati coinvolti con diversi livelli d'intensità.

Cyber Poison 2014 ha simulato in un solo giorno l'attività di quattro giorni del mese di giugno 2014 (cosiddetta "tecnica dell'orologio accelerato"), prendendo a riferimento i dati finanziari reali di quelle giornate. Si è simulato che gli eventi si svolgessero in un contesto di elevata volatilità dei mercati, anche con giornate critiche in termini di liquidità a causa dei riversamenti fiscali e del

regolamento delle operazioni di rifinanziamento principale.

Lo scenario intendeva mettere alla prova la capacità del sistema finanziario di far fronte a un attacco informatico su larga scala – un'alterazione del software di due fornitori d'infrastruttura con impatto sull'integrità dei dati delle banche e delle infrastrutture di mercato – i cui impatti si sono propagati rapidamente all'intero sistema finanziario italiano e ai suoi utenti (i cittadini, le imprese, le pubbliche amministrazioni). Lo scenario prevedeva ricadute significative anche sui mercati esteri che, tuttavia, non sono stati coinvolti.

Risultati

L'esercitazione si è connotata per il forte coinvolgimento di tutti gli operatori sistemici e, pur con i limiti di una simulazione, ha permesso di mettere alla prova la capacità del settore finanziario di gestire crisi operative su larga scala. Essa ha consentito di verificare i processi per la comunicazione e il coordinamento settoriale e ha permesso agli operatori sistemici di testare la rispondenza delle contromisure attuate rispetto ai requisiti normativi in caso di grave crisi operativa, in particolare dovuta a un attacco informatico su larga scala.

Come in ogni esercitazione è stato necessario introdurre alcune schematizzazioni della realtà per consentire di concentrare in poche ore di simulazione eventi che si sarebbero svolti in quattro giorni. Sono emerse importanti aree di miglioramento che saranno oggetto d'intervento nei prossimi mesi.

I risultati dell'esercizio sono stati raccolti dalla Banca d'Italia durante l'esercitazione, discussi nel corso della sessione serale, rilevati dai partecipanti nei moduli di feedback, analizzati con l'internal audit all'interno delle singole aziende partecipanti. In termini complessivi i riscontri sono stati positivi e tutti i partecipanti hanno considerato molto utile la simulazione; in particolare va segnalata l'ampia soddisfazione per le attività di verifica dei meccanismi di escalation verso i vertici aziendali.

Dall'esercitazione sono emersi numerosi spunti di riflessione sui miglioramenti possibili nel sistema finanziario, nelle procedure e nelle funzionalità delle apparecchiature tecniche del CODISE, nelle caratteristiche della simulazione, nel livello di adeguamento degli operatori sistemici ai nuovi requisiti di continuità operativa. I punti di maggior rilievo sono sinteticamente i seguenti:

Profili relativi al sistema finanziario.

- Andrà approfondito il tema dell'arco di tempo massimo che il sistema finanziario è in grado di tollerare utilizzando i contingency payments di Target2 prima che gli impatti diventino non sostenibili.
- Ciascun operatore sistemico potrà valutare la possibilità di una gestione del collateral che permetta di ridurre la dipendenza da singole infrastrutture.
- Sono da verificare in maggiore dettaglio le procedure della Tesoreria dello Stato in caso di grave crisi operativa.
- Sono da approfondire in un'ottica sistemica i piani di crisi della Banca d'Italia e delle banche commerciali per la gestione del contante.

Adeguamento ai requisiti di continuità operativa.

- Per migliorare la resilienza del sistema, saranno rivisti i criteri per l'inclusione degli operatori nel gruppo delle aziende a rilevanza sistemica.

Caratteristiche della simulazione.

- La "tecnica dell'orologio accelerato" ha talvolta divaricato il trascorrere del tempo tra le diverse funzioni aziendali colpite dagli eventi rendendo più difficile mantenere una visione unitaria della crisi. Andrà valutata la possibilità di definire scenari meno diluiti nel tempo o prevedere tempi più lunghi per l'esercitazione, da svolgere eventualmente

anche in giorni non lavorativi.

- Il disegno degli scenari dovrà prestare maggiore attenzione alla verifica dei meccanismi per il coordinamento della comunicazione verso il pubblico e le autorità.
- Le esercitazioni future potranno focalizzarsi anche su aspetti tecnologici legati alla gestione dell'emergenza cyber e non solo sugli aspetti organizzativi.

Prospettive

Il buon risultato della simulazione Cyber Poison 2014 ha confermato la validità delle procedure di cooperazione tra operatori sistemici (banche, infrastrutture di mercato, fornitori di servizi) e autorità nel CODISE.

Nel medio termine l'efficacia delle simulazioni potrà essere aumentata prevedendo scenari con dimensione internazionale e/o test di disaster recovery simultanei con operatività da siti secondari in produzione per una o più settimane.