BANCA D'ITALIA
EUROSISTEMA

Resoconto Esercitazione G7 CBCE

Codise

4-6 giugno 2019

Sommario

Introduzione

Il Codise, struttura deputata al coordinamento delle crisi operative della piazza finanziaria italiana, nell'ambito delle proprie funzioni, operando in raccordo con le analoghe strutture a livello internazionale, organizza e partecipa a test e simulazioni per consentire ai propri membri di esercitarsi ad affrontare problematiche operative con impatti sui processi a rilevanza sistemica.

In tale ambito, il Codise ha partecipato dal 4 al 6 giugno 2019, in qualità di punto di contatto per la comunità finanziaria italiana, alla prima esercitazione "cyber"[1] tra le autorità finanziarie dei paesi appartenenti al G7, con l'obiettivo di verificare le modalità di comunicazione e coordinamento tra le autorità, in caso di un attacco cyber rilevante ai danni del sistema finanziario internazionale.

Nell'occasione, si è svolta anche un'esercitazione locale che ha permesso agli operatori sistemici[2] della piazza finanziaria italiana, alle autorità finanziarie (MEF, Banca d'Italia e Consob) e ad altre organizzazioni aderenti al CERTFin[3] di esercitarsi individualmente e collettivamente a fronteggiare uno scenario cyber avverso, con impatti rilevanti sulla loro operatività e sul sistema dei pagamenti.

[1] G7 CBCE (Cross Border Coordination Exercise).

[2] 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.

[3] Il CERTFin – CERT Finanziario Italiano – è un'iniziativa cooperativa pubblico-privata finalizzata a innalzare la capacità di gestione dei rischi cyber degli operatori bancari e finanziari e la cyber resilience del sistema finanziario italiano attraverso il supporto operativo e strategico alle attività di prevenzione, preparazione e risposta agli attacchi informatici e agli incidenti di sicurezza. Il CERTFin è governato dall'Associazione Bancaria Italiana (ABI) e dalla Banca d'Italia, che ne condividono la Presidenza, ed è operato dal Consorzio ABI Lab. IVASS e ANIA hanno aderito nel dicembre 2018 al CERTFin e partecipano negli organi direttivi in rappresentanza del settore assicurativo. I servizi sono messi a disposizione dei partecipanti su base cooperativa, grazie al coinvolgimento degli operatori finanziari italiani.

1. Organizzazioni partecipanti e obiettivi dell'esercitazione

La partecipazione all'esercitazione è avvenuta su 3 livelli:

Livello 1: autorità finanziarie dei paesi del G-7: ministeri del Tesoro e delle Finanze, banche centrali, autorità di vigilanza sui mercati e autorità di supervisione bancaria;

Livello 2: altre autorità pubbliche o governative, che fanno parte delle strutture organizzative preposte alla gestione di crisi del settore finanziario a livello locale;

Livello 3: istituzioni private del sistema finanziario delle singole giurisdizioni. Intermediari finanziari, mercati, infrastrutture di mercato, fornitori tecnologici.

Tutti i paesi del G-7 hanno deciso di far partecipare le strutture organizzative preposte alla gestione delle crisi locali del settore finanziario, ma in differenti modalità:

- Italia, Francia, Germania e Giappone hanno coinvolto anche il settore privato. Per l'Italia, in particolare, il Codise è stato il punto di contatto tra comunità finanziaria locale e internazionale. Inoltre è stato coinvolto il CERTFin, con una parte della propria constituency, mentre non hanno partecipato autorità del secondo livello;

- Regno Unito, USA, Canada e Unione Europea hanno coinvolto solamente organizzazioni appartenenti ai livelli 1 e 2, simulando quini il coinvolgimento delle aziende del settore privato.

L'esercitazione G-7 CBCE ha consentito di testare le modalità di comunicazione e coordinamento tra le autorità finanziarie dei paesi del G-7 in caso di un grave incidente cyber con impatto globale. In particolare, l'esercitazione si poneva i seguenti obiettivi: :

• migliorare la mutua conoscenza delle strutture organizzative del settore finanziario preposte alla risposta agli incidenti cyber nelle singole giurisdizioni;

• individuare buone prassi e lezioni apprese sulla risposta agli incidenti cyber e sui meccanismi di coordinamento all'interno delle singole giurisdizioni, includendo eventualmente l'interazione con il settore privato;

• promuovere il coordinamento tempestivo tra le autorità finanziarie dei paesi del G-7 delle azioni di risposta a incidenti cyber rilevanti;

• verificare l'efficacia del protocollo di risposta agli incidenti cyber tra le autorità finanziarie dei paesi del G-7, in caso di un incidente cyber rilevante che interessi il sistema finanziario internazionale, mediante uno scenario verosimile sia per quanto riguarda gli aspetti tecnici sia per quelli economico/finanziari;

• identificare eventuali aree di potenziale miglioramento del coordinamento della risposta agli incidenti cyber del settore finanziario dei paesi del G-7.

Come detto, nell'ambito dell'esercitazione G7 CBCE, il **settore finanziario italiano**, ha svolto la periodica simulazione locale con l'obiettivo di comunicare e coordinarsi nell'ambito delle esistenti strutture di gestione delle crisi (Codise) e di risposta agli incidenti cyber (CERTFin).

I singoli partecipanti privati della comunità nazionale hanno così potuto esercitarsi rispetto ai seguenti aspetti:

- analisi e gestione di un evento anomalo secondo le procedure organizzative stabilite;
- uso dei piani di emergenza e continuità operativa, in una situazione potenzialmente critica con impatti sulla propria operatività (includendo tra l'altro gli eventuali processi di (a) notifica al Codise e al CERTFin; (b) segnalazione all'autorità di vigilanza; (c) notifica ai sensi della normativa NIS, Network Information Security Directive).
- definizione di eventuali comunicazioni interne ed esterne alla propria organizzazione;

Per riprodurre in modo realistico le azioni che si svolgerebbero in caso di una crisi cyber con impatti sul sistema finanziario internazionale, infine, sono state esercitate anche le modalità di coordinamento e i flussi delle comunicazioni tra la comunità locale, rappresentata dal Codise, e il tavolo delle autorità finanziarie dei paesi del G-7 (e viceversa).

2. Caratteristiche dell'esercitazione e scenario

Lo scenario[4] intendeva mettere alla prova la capacità del sistema finanziario di far fronte a un attacco cyber su larga scala, preparato da alcuni criminali nei mesi precedenti ed eseguito contemporaneamente a danno di alcuni importanti intermediari finanziari in Italia e in altri paesi del G7 e di uno dei maggiori fornitori di software per i pagamenti interbancari. Gli impatti hanno riguardato principalmente il sistema finanziario e non i cittadini.

Come in un evento reale i partecipanti, coinvolti con diversi livelli d'intensità, hanno avuto l'opportunità di collaborare e scambiarsi informazioni sia in ambito Codise sia attraverso il team virtuale del CERTFin. L'esercitazione non ha richiesto recovery tecnologico, non ha interessato i dati di produzione, non ha richiesto la disponibilità di ambienti tecnologici di collaudo dei servizi finanziari, fatta eccezione per gli apparati di comunicazione, è stata

[4] Lo scenario è stato progettato da un Task Force, coordinata dalla Banca d'Italia, cui hanno partecipato esponenti di alcune istituzioni finanziarie partecipanti all'esercitazione.

condotta dalle sedi dei partecipanti e gestita da un'unità di coordinamento presso la Banca d'Italia.

I partecipanti sono stati informati degli eventi in modo graduale, attraverso un set di informazioni (inject) sequenziali, inviati via mail. Dopo la ricezione di ogni inject, i giocatori hanno reagito come se l'evento descritto fosse reale (simulando, come detto, eventuali interventi sugli apparati informatici).

Le attività sono durate 3 giorni, dal 4 al 6 giugno 2019, quasi interamente in tempo reale. Solo il pomeriggio del 6 giugno è stato simulato un salto temporale al 18 giugno per rendere più realistica la discussione riguardo le modalità di rientro della crisi.

Alla chiusura dei lavori, nel pomeriggio del 6 giugno, esponenti del top management delle autorità e degli intermediari hanno partecipato ad una conferenza telefonica, per discutere gli spunti più rilevanti emersi e le possibili iniziative per prevenire e contrastare i nuovi rischi connessi con la digitalizzazione dei servizi finanziari.

3. Risultati

L'esercitazione ha riscontrato un forte coinvolgimento di tutti i partecipanti: hanno preso parte alle attività della sola esercitazione italiana circa 200 persone appartenenti a 20 diverse organizzazioni. È stato così possibile testare le capacità di collaborazione e comunicazione del sistema finanziario nelle 8 audio conferenze del Codise, cui sono seguiti 18 comunicati stampa (da parte di autorità e imprese private).

L'esercitazione inoltre ha permesso ai partecipanti di testare la rispondenza delle contromisure attuate rispetto ai requisiti normativi in caso di grave crisi operativa, dovuta a un attacco cyber, includendo anche le comunicazioni sugli incidenti: cinque banche hanno inviato il report dell'incidente alla Vigilanza (Banca d'Italia/SSM), tre organizzazioni hanno utilizzato l'apposito modulo per la segnalazione degli incidenti ai sensi della NIS al CSIRT Italia.

Dall'esercitazione sono emersi numerosi spunti di riflessione su miglioramenti possibili nel coordinamento e la comunicazione in caso di crisi operativa del settore finanziario.

I punti di maggior rilievo sono sinteticamente i seguenti:

Comunicazione: le modalità di comunicazione con soggetti esterni al Codise (altre istituzioni del sistema finanziario, soggetti non appartenenti al sistema finanziario, mercati, cittadini, etc.) sono state sempre un aspetto critico durante le crisi o le simulazioni. L'esercitazione CBCE ha mostrato che tale aspetto è ancora più rilevante in caso di crisi cyber, durante le quali occorre un coordinamento per la comunicazione non solo all'interno

del sistema finanziario ma anche ma anche con soggetti operanti nell'ambito governativo della sicurezza nazionale oltre che con le autorità finanziarie di altri paesi o sovranazionali.

Collaborazione tra Codise e CERTFin: uno degli obiettivi dell'esercitazione era testare le modalità di collaborazione tra CERTFin e Codise, secondo le modalità concordate. Sono emersi possibili profili di miglioramento in tale collaborazione, per consentire un efficace utilizzo delle analisi tecniche e dei report predisposti dal CERTFin.

Scenario: l'esercitazione ha mostrato che, in caso di crisi cyber, occorre tenere in adeguata considerazione le possibili reazioni dei mercati e della cittadinanza. In futuro sarebbe utile organizzare una simulazione il cui scenario sia focalizzato su questi aspetti. La tematica cyber inoltre ben si adatterebbe anche a scenari "cross-industry".

4. Prospettive

Il buon risultato dell'esercitazione G7 CBCE ha confermato la validità delle procedure di cooperazione tra operatori sistemici (banche, infrastrutture di mercato, fornitori di servizi) e autorità in un ambito più esteso del Codise, che comprendeva anche MEF, CERTFin e parte della propria constituency.

I risultati hanno mostrato l'utilità di alcuni approfondimenti, in particolare:

- valutare l'adozione di un protocollo per la comunicazione in caso di crisi di natura cyber tra membri del Codise e del CERTFin e le autorità finanziarie (MEF, Banca d'Italia e Consob);
- avviare le attività per la preparazione di un'esercitazione con uno scenario che includa effetti sui mercati e sugli utenti finali.