COVID-19: la resilienza del sistema bancario e finanziario

Author : Redazione

Date : 20 Maggio 2020

Il diffondersi del COVID-19 in Italia ha costretto molti settori a divenire una trincea per fronteggiare questo nuovo e sconosciuto avversario.

Nell'ambito delle varie decretazioni emanate dalla Presidenza del Consiglio dei Ministri si sono via via individuati una pluralità di **settori considerati essenziali** per il funzionamento del Paese.
Tra questi, possiamo annoverare il settore bancario e finanziario.

Nelle prime "zone rosse" individuate dal Governo si trovavano quasi il 40% del totale di tutte le filiali bancarie: queste, in larga misura, hanno continuato a garantire il servizio alla clientela.

Sin dai primi giorni dell'emergenza, prima in ordine sparso poi grazie alla concertazione tra ABI (Associazione Bancaria Italiana) e le sigle sindacali si è arrivati a **standard di operatività** per garantire alla clientela il minore disservizio possibile e uniformità di servizio in tutta Italia.

Questa gestione straordinaria, con diverse declinazioni per ogni singolo Istituto, si basa fondamentalmente sull'accesso alle filiali su prenotazione e solo per operazioni urgenti o non eseguibili con altri canali (virtuali, ATM evoluti...), la fornitura di opportuni presidi al ridotto personale presente (mascherine, disinfettanti per le mani, pannelli in plexiglass) e il rafforzamento delle attività di pulizia degli ambienti di lavoro.

Anche negli Uffici Centrali, dove molto spesso il *layout* degli ambienti è quello dell'open space, viene disposta la turnazione del personale e il decentramento in diversi siti, anche per evitare l'interruzione delle attività qualora se ne debba procedere alla disinfezione in caso di accertato caso COVID19 positivo.

Un altro fondamentale strumento per garantire la funzionalità è il ***remote working*** di quanto più personale possibile, in alcune realtà si è arrivati anche al 70% del personale. Ciò ha ovviamente messo sotto stress le piattaforme ICT, in larga misure in *outsourcing*, ma l'alta specializzazione di questi fornitori ha permesso in breve tempo di garantire la normale operatività.

L'incremento di operatività sui canali virtuali da parte della clientela non poteva passare

inosservato ai sempre attivi criminali informatici.

Fin dall'inizio di febbraio iniziano una serie di campagne di false email che vengono prontamente individuate dal **Centro Nazionale Anticrimine Informatico per la protezione delle infrastrutture critiche (CNAIPIC),** nucleo della Polizia Postale e delle Comunicazioni della Polizia di Stato.

In larga misura queste email, con il pretesto di fornire informazioni sulla diffusione del Coronavirus, invogliavano ad aprire un allegato "malevolo" contenente un virus, dai più "banali" in grado di carpire alcuni dati personali o le credenziali di accesso ai siti di banca virtuale, a quelli *ransomware* per "tenere in ostaggio" il computer a quelli - ancora più complessi - in grado di "impossessarsi" della macchina per utilizzarla a sua volta per perpetrare ulteriori attacchi.

A contribuire a questa attività difensiva in una fase preventiva opera il **CERTFin – CERT Finanziario Italiano** - la cui Presidenza è condivisa tra Banca d'Italia e ABI è operato da ABI Lab, una cooperazione pubblico-privata finalizzata alla *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.

Anche in questo momento di emergenza a vegliare sul sistema bancario e finanziario italiano c'è **Banca d'Italia**.

Tra i tanti aspetti oggetto dell'attività di vigilanza operata da Banca d'Italia nei confronti delle banche o dei gruppi bancari c'è proprio la cosiddetta Continuità Operativa, questa rientra nel governo dei rischi dell'operatore per garantire il raggiungimento degli obiettivi aziendali.

Attraverso apposite circolari, l'ultima delle quali è n. 285 del 17 dicembre 2013 *"Disposizioni di vigilanza per le Banche",* più volte aggiornata, vengono individuati i requisiti comuni per tutti gli operatori e quelli particolari per i processi a rilevanza sistemica.

La circolare riepiloga alcuni **scenari di crisi** che devono essere tenuti in considerazione in sede di predisposizione del piano di continuità operativa:

- distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche per fattori naturali (sisma, dissesto idrogeologico, allagamento, eruzione vulcanica) o antropici (interdizione dell'area per motivi di sicurezza o ordine pubblico, guerra, terrorismo, sabotaggio, incendio, rischio chimico-industriale);

- indisponibilità di sistemi informativi critici, anche con riferimento ai sistemi funzionali alla prestazione dei servizi di pagamento (indisponibilità dei sistemi e delle applicazioni, accesso non autorizzato/incidenti alla sala server, infiltrazione nelle reti, virus e attacchi esterni);

- indisponibilità di personale essenziale per il funzionamento dei processi aziendali (dimissioni, blocco dei trasporti, pandemia, malattia, eventi catastrofici naturali o antropici);

- interruzione del funzionamento delle infrastrutture tra cui energia elettrica, reti di

telecomunicazione (Connettività dati, connettività voce, Internet), reti interbancarie, mercati finanziari;

- alterazione o perdita di dati e documenti critici (dati elettronici e documenti cartacei).

Il **piano di continuità operativa** deve indicare le procedure per le modalità della dichiarazione di crisi, l'attivazione della struttura dedicata (ad es. comitato di crisi), la gestione della fase emergenziale, le modalità di comunicazione, le tempistiche per il ripristino dei processi critici e l'iter per la ripresa della normale operatività.

Gli operatori devono individuare i "processi critici" cioè quei processi o funzioni di rilievo che necessitano di elevati livelli di continuità operativa a causa dell'impatto dei danni conseguenti ad una loro indisponibilità

Per individuare il livello di rischio di ogni processo aziendale e le conseguenze dell'interruzione del servizio si ricorre all'analisi d'impatto come procedura preliminare alla predisposizione del piano di continuità.

Questa analisi viene annualmente aggiornata sulla base delle verifiche svolte, in caso di cambiamenti organizzativi o in presenza di nuovi rischi o minacce.

Il 20 marzo 2020 Banca d'Italia, in un suo comunicato stampa, raccomanda a tutte le banche di rivedere i propri piani di emergenza e continuità operativa considerando le azioni da compiersi per minimizzare gli effetti negativi della diffusione del COVID-19.

Il sistema finanziario poggia sul corretto funzionamento dei maggiori operatori e sulla loro capacità di erogare i servizi essenziali nei comparti dei sistemi di pagamento e dell'accesso ai mercati finanziari che vengono pertanto denominati "processi a rilevanza sistemica" quali ad esempio:

- servizi di pagamento al dettaglio a larga diffusione tra il pubblico (bollettini postali, pagamento delle pensioni sociali, erogazione del contante);

- servizi strettamente funzionali al soddisfacimento di fondamentali esigenze di liquidità degli operatori economici, il cui blocco ha rilevanti effetti negativi sull’operatività degli stessi.

Banca d'Italia provvede a individuare questi operatori, chiedendo loro requisiti di continuità operativa più stringenti rispetto a quelli previsti per la generalità degli operatori e ne verifica le soluzioni adottate.

Per gestire il coordinamento delle crisi operative della piazza finanziaria italiana nel 2003 nasce il **CODISE (Coordinamento della continuità operativa del sistema finanziario).**

Esso è presieduto dalla Banca d'Italia e vi partecipano la CONSOB (Commissione Nazionale per le Società e la Borsa) e gli operatori del settore finanziario rilevanti sul piano sistemico.

Il suo ruolo in ambito di Continuità operativa è statuito nella Circolare n. 263 del 27 dicembre 2006, *"Disposizioni di vigilanza prudenziale delle banche",* e dalle Linee Guida in materia di continuità operativa delle infrastrutture di mercato del maggio 2014.

La struttura ha lo scopo di facilitare lo **scambio di informazioni** e l'adozione delle misure necessarie per fronteggiare eventi che possono mettere a rischio la continuità operativa del sistema, il funzionamento delle infrastrutture finanziarie nonché la fiducia del pubblico nella moneta.

Il CODISE promuove esercitazioni per verificare l'adeguatezza delle procedure delle banche coinvolte, svolge compiti di analisi e di confronto sull'evoluzione delle minacce alla continuità operativa nonché sulle emergenti tematiche quali per esempio la *cyber security*. In caso di incidenti che possono avere impatti rilevanti la dichiarazione dello stato di crisi prevede l'immediata richiesta di attivazione del CODISE.

Per superare il limite del CODISE che non estende la sua area di azione a tutti gli attori del contante nel maggio 2015 viene istituito il **COBAN (Comitato per la continuità operativa della distribuzione di banconote in euro).**

Il comitato è composto da quattro membri, uno ciascuno in rappresentanza di Banca d'Italia, ABI, Poste Italiane e Ministero dell'Interno - Dipartimento della Pubblica Sicurezza.

Tra i compiti del Comitato ci sono: la promozione dello scambio di conoscenze, il coinvolgimento degli altri attori del circuito del contante (tra cui gli Istituti di Vigilanza con i loro servizi di trasporto valori e sale conta), l’organizzazione di esercitazioni per verificare l'efficacia delle procedure e l’analisi dell'evoluzione delle minacce tenendo anche conto i nuovi orientamenti in materia muturati a livello di Eurosistema.

Vari sono gli **eventi critici** analizzati: di tipo naturale (calamità naturali, catastrofi, disastri ambientali), operativo (scioperi di lunga durata, blocco dei trasporti, attacchi criminali e terroristici, incidenti industriali, attacchi cibernetici) e settoriali (interruzioni anche temporanee dell'operatività di un Istituto di Vigilanza privata).

A seguito delle numerose richieste sollevate da sindacati e associazioni di categoria per tutelare il personale della **vigilanza privata**, il 19 marzo scorso il COBAN ha definito delle nuove modalità di esecuzione dei servizi di trasporto valori concentrandoli su tre giorni settimanali per permettere di sospenderli in alcune giornate. In ottemperanza alle indicazioni fornite dal COBAN, Banca d’Italia ha ordinato un numero consistente di mascherine e ha preso contatti con gli uffici regionali della Protezione Civile, scongiurando di fatto il blocco della distribuzione del contante.

In questo momento di grave emergenza, il sistema bancario e finanziario è in grado di continuare a garantire il suo fondamentale supporto per il funzionamento del Sistema Paese: è imprescindibile, tuttavia, il supporto di tutta la collettività.

Articolo a cura di **Marco Missaglia**