

Cybersecurity, conclusi gli stress test su 109 banche. BCE: “Restano aree di miglioramento”



Una prova di stress che ha visto coinvolte 109 banche vigilate direttamente dalla **Banca Centrale Europea** chiamate a rispondere a un questionario e a sottoporre documentazione all'esame dei responsabili della vigilanza, mentre un campione di 28 banche è stato selezionato per verifiche più approfondite.

La Banca centrale europea ha concluso oggi la prova di stress sulla resilienza cibernetica, intesa a valutare la risposta e il ripristino da parte delle banche in caso di incidente di cibersecurity grave ma plausibile. Nel complesso, spiega

l'istituzione finanziaria dell'Unione europea, è emerso che le banche dispongono di sistemi di risposta e ripristino, ma restano aree di miglioramento. I risultati, che confluiranno nel processo di revisione e valutazione prudenziale (**Supervisory Review and Evaluation Process, SREP**) 2024, hanno contribuito a sensibilizzare le banche riguardo ai punti di forza e debolezza dei rispettivi sistemi di resilienza cibernetica.

“L’obiettivo del processo di selezione è stabilire accordi quadro con i fornitori esterni più idonei per garantire che l’Eurosistema sia pronto ad avviare lo sviluppo di un euro digitale in futuro, se giustificato”, aveva spiegato il membro del Comitato esecutivo della Bce, **Piero Cipollone**, lo scorso gennaio.

L’esercizio, avviato nel gennaio 2024, spiega la BCE in una nota, prevedeva uno scenario di prova fittizio nel cui ambito tutte le misure preventive fallivano e un attacco cibernetico si ripercuoteva gravemente sulle basi di dati dei sistemi fondamentali di ciascuna banca. La prova di stress si è quindi incentrata sulla risposta e sul ripristino da parte delle banche in caso di attacco cibernetico, anziché sui meccanismi di prevenzione. Individuare e affrontare le carenze nei sistemi di resilienza delle banche vigilate sul piano operativo, anche a seguito di rischi cibernetici, è una delle priorità di vigilanza dell'MVU per il periodo 2024-2026, alla luce del recente forte incremento degli incidenti cibernetici segnalati dai soggetti vigilati alla BCE, in parte riconducibile alle crescenti tensioni geopolitiche e alle sfide poste dalla digitalizzazione del settore bancario.

A queste ultime è stato chiesto di eseguire un test di ripristino informatico a tutti gli effetti e di fornire elementi comprovanti il successo di tale test, oltre ad accertamenti in loco da parte dei responsabili della vigilanza. Il campione includeva modelli imprenditoriali e aree geografiche differenti per essere rappresentativo del

sistema bancario dell'area dell'euro in senso più ampio e assicurare un sufficiente coordinamento con altre attività di vigilanza.

Per mettere alla prova la loro risposta allo scenario, le banche hanno dovuto dimostrare la capacità di:

- attivare i propri piani di risposta alle crisi, incluse le procedure interne di gestione delle crisi e i piani di continuità operativa;
- comunicare con tutte le parti interessate esterne, quali i clienti, i prestatori di servizi e le forze dell'ordine;
- effettuare un'analisi allo scopo di individuare quali sarebbero i servizi interessati e come;
- attuare misure di mitigazione, incluse soluzioni che aiuterebbero la banca a operare durante il periodo necessario per il pieno ripristino dei sistemi informatici.

Per mettere alla prova la capacità di ripristino in seguito allo scenario, le banche hanno dovuto dimostrare di poter:

- attivare i propri piani di ripristino, anche recuperando i dati dai back-up e allineandosi con i fornitori terzi di servizi essenziali nelle modalità di risposta all'incidente;
- assicurare di avere provveduto al ripristino e al buon funzionamento delle aree colpite;
- beneficiare degli insegnamenti tratti, ad esempio mediante il riesame dei piani di risposta e ripristino.

Anche in futuro la BCE si impegna a collaborare con le banche su cui vigila per il rafforzamento dei loro sistemi di resilienza cibernetica. A tal fine, le incoraggerà ulteriormente a continuare a lavorare per soddisfare le aspettative di vigilanza, assicurandosi tra l'altro che dispongano di piani di continuità operativa, comunicazione e

ripristino adeguati, con una gamma sufficientemente ampia di scenari di rischio cibernetico. Le banche dovrebbero inoltre essere in grado di conseguire i propri obiettivi di ripristino, valutare correttamente la dipendenza da fornitori terzi di servizi essenziali di tecnologia dell'informazione e della comunicazione (TIC) e stimare adeguatamente le perdite dirette e indirette derivanti da un attacco cibernetico.

I risultati dell'esercizio confluiranno nello SREP 2024, inteso alla valutazione dei profili di rischio individuali delle banche.

Leggi le altre notizie sull'home page di Key4biz

<https://www.key4biz.it/cybersecurity-conclusi-gli-stress-test-su-109-banche-dellue-bce-restano-aree-di-miglioramento/499787/>