Verifica della vigilanza sulla cibersicurezza dei fornitori di servizi finanziari

Autorità federale di vigilanza sui mercati finanziari

L'essenziale in breve

Il Controllo federale delle finanze (CDF) ha effettuato una verifica presso l'Autorità federale di vigilanza sui mercati finanziari (FINMA) allo scopo di esaminare l'efficienza e l'efficacia della vigilanza in materia di cibersicurezza dei fornitori di servizi finanziari.

L'8 dicembre 2017 il Consiglio federale ha varato la Strategia nazionale per la protezione delle infrastrutture critiche (PIC) per il periodo 2018–2022. Due dei 27 settori parziali definiti sono sottoposti alla vigilanza della FINMA: i servizi finanziari e i servizi assicurativi.

Il dispositivo complessivo in Svizzera procede a rilento

Le direttive obbligatorie per le banche e i commercianti di valori mobiliari emanate dalla FINMA nel 2017 sono adeguate. Tuttavia, esistono da anni lacune nel dispositivo complessivo sui ciber-rischi. Le misure concrete stanno tuttavia procedendo a rilento a causa di responsabilità e competenze poco chiare. Ad esempio, è ancora in fase di costituzione un'organizzazione di crisi funzionante e le esercitazioni intersettoriali contro i ciberattacchi, che dovrebbero svolgersi regolarmente, sono state effettuate soltanto una volta.

La vigilanza dipende dalle risorse disponibili

La vigilanza sui ciber-rischi, uno dei sei rischi principali per la FINMA, è stata sviluppata ulteriormente in modo costante con le risorse disponibili. In questo settore non sono ancora state realizzate o attuate tutte le attività pianificate. Ciò è stato riconosciuto dalla FINMA, che ha provveduto ad apportare adeguamenti organizzativi e formali all'inizio del 2020. Tuttavia, sussiste ancora il rischio che la vigilanza non segua le attività pianificate, ma si orienti alle risorse disponibili. Si potrebbero ottenere guadagni in termini di efficienza nel rilevamento e nella valutazione dei risultati delle verifiche.

Le banche non hanno sufficientemente rispettato l'obbligo di notifica dei ciberincidenti

Le banche non hanno rispettato a sufficienza l'obbligo di notifica di ciberincidenti. La mancata notifica non ha avuto conseguenze per gli istituti sottoposti alla vigilanza, sebbene sarebbero disponibili adeguati strumenti a tal fine. La FINMA non dispone quindi di una fonte significativa per individuare i ciber-rischi a livello di istituti.

Questa circostanza è accentuata dal fatto che le banche rifiutano l'accesso diretto della FINMA a MELANI (Centrale d'annuncio e d'analisi per la sicurezza dell'informazione). L'intensificazione dei controlli in loco raccomandata dal CDF potrebbe in parte colmare queste lacune.

Testo originale in tedesco