Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Comunicato stampa

Cyber-rischi: la FINMA pubblica una Comunicazione sulla vigilanza

Data:
07.06.2024

Embargo:
-

Contatto:
Patrizia Bickel, portavoce
Tel. +41 (0)31 327 93 19
patrizia.bickel@finma.ch

In una Comunicazione sulla vigilanza, l'Autorità federale di vigilanza sui mercati finanziari FINMA pubblica le conoscenze emerse dalla vigilanza sui cyber-rischi. Inoltre, precisa l'obbligo di notificare i cyber-attacchi e i cyber-esercizi basati su scenari.

Da diversi anni la FINMA indica i cyber-rischi come uno dei principali rischi per la piazza finanziaria svizzera (cfr. Monitoraggio FINMA dei rischi). In una Comunicazione sulla vigilanza, la FINMA informa in merito alle conoscenze emerse dalla vigilanza sui cyber-rischi e richiama l'attenzione sulle carenze ripetutamente individuate. Inoltre, precisa i requisiti concernenti l'obbligo di notificare i cyber-attacchi e specifica lo svolgimento di cyber-esercizi basati su scenari.

Le esternalizzazioni come fattore di rischio

Nel periodo 2022-2023, più della metà dei cyber-attacchi notificati riguardava servizi esternalizzati. Anche la FINMA, nel quadro della sua attività di vigilanza sui cyber-rischi, constata spesso lacune in questo ambito. Tuttavia, oltre all'*outsourcing*, anche altri temi sono oggetto di attenzione ricorrente, come la *governance* nella gestione dei cyber-rischi.

Ampliati gli strumenti di vigilanza

Inoltre, negli ultimi anni la FINMA ha introdotto ulteriori strumenti di vigilanza specifici in ambito cyber, come gli esercizi di *red teaming* o di *tabletop* con gli istituti assoggettati. Nel *red teaming*, gli esperti in materia di sicurezza assumono il ruolo di aggressori e cercano di aggirare le misure di sicurezza informatica di un'impresa copiando il metodo di attacco di un *hacker* «malintenzionato». Gli esercizi di *tabletop* consistono in una simulazione e riproduzione di uno scenario su carta. I rischi identificati vengono continuamente analizzati, valutati e sintetizzati in una mappa dei rischi.

Ampia attività di vigilanza in ambito cyber

Gli istituti assoggettati sono tenuti a notificare i cyber-attacchi alla FINMA. Inoltre, anche lo scorso anno la FINMA ha svolto più di una decina di controlli in loco specifici in ambito cyber. Le notifiche degli assoggettati o delle società di audit come pure i controlli in loco specifici in questo ambito consentono alla FINMA di valutare in maniera approfondita la qualità del

dispositivo di lotta contro i cyber-rischi messo a punto dagli istituti assoggettati alla vigilanza e, in caso di necessità, di adottare tempestivamente misure specifiche per i singoli istituti.