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

Comunicazione FINMA sulla vigilanza 03/2024

Conoscenze emerse dalla vigilanza sui cyber-rischi, precisazioni concernenti la Comunicazione FINMA sulla vigilanza 05/2020 e i cyber-esercizi basati su scenari

7 giugno 2024

Laupenstrasse 27, 3003 Berna, Tel. +41 (0)31 327 91 00, www.finma.ch

Indice

1 Introduzione

Da diversi anni i cyber-rischi si annoverano fra i rischi principali che la FINMA tratta nel suo Monitoraggio dei rischi, pubblicato con frequenza annuale. Al riguardo, il numero delle segnalazioni pervenute alla FINMA in merito ai cyber-attacchi andati a segno o parzialmente andati a segno aumenta ogni anno.

Con la Comunicazione FINMA sulla vigilanza 05/2020 «Obbligo di notificare i cyber-attacchi secondo l'art. 29 cpv. 2 LFINMA» è stato descritto con maggiore precisione il corrispondente obbligo di notifica. Le notifiche da allora pervenute mostrano differenti sviluppi per quanto concerne la situazione di minaccia, i metodi degli attacchi e i relativi obiettivi. Attraverso la sua attività di vigilanza, la FINMA ottiene un quadro dettagliato della gestione dei cyber-rischi da parte degli istituti assoggettati alla vigilanza. In particolare, i controlli in loco specifici in ambito cyber consentono alla FINMA di effettuare una valutazione approfondita della maturità del dispositivo di lotta contro i cyber-rischi messo a punto dagli istituti assoggettati alla vigilanza. I risultati ottenuti e le constatazioni specifiche agli istituti sono stati pubblicati su base aggregata nel Monitoraggio FINMA dei rischi e nel Rapporto annuale della FINMA.

Nella presente Comunicazione sulla vigilanza, la FINMA fornisce agli assoggettati, sulla base di tali risultati, indicazioni specifiche concernenti la gestione dei cyber-rischi. Tali indicazioni sono rilevanti per tutti gli istituti assoggettati. Per determinati aspetti si fa esplicitamente riferimento alla Circolare FINMA 23/1 «Rischi operativi e resilienza – banche». Le presenti indicazioni sono rivolte principalmente agli istituti ai quali si applica la predetta circolare, tuttavia possono fungere da linee guida anche per gli altri istituti.

A questo proposito vengono affrontate anche domande ricorrenti sulla Comunicazione FINMA sulla vigilanza 05/2020 «Obbligo di notificare i cyber-attacchi secondo l'art. 29 cpv. 2 LFINMA».

Infine, viene trattato e precisato il nm. 70 della Circolare FINMA 23/1.

2 Conoscenze emerse dalla vigilanza sui cyber-rischi

2.1 Esternalizzazioni

Già nel Monitoraggio FINMA dei rischi 2020 la FINMA aveva riferito in merito a un aumento degli attacchi messi a segno nelle catene di fornitura degli istituti assoggettati alla vigilanza, il che rappresentava circa il 25% di tutti gli attacchi. Negli anni successivi, la quota è salita già a oltre il 50%, mantenendosi stabile in questo ambito. Pertanto, la FINMA ha esaminato in maniera più approfondita il tema dei cyber-rischi nelle esternalizzazioni[1], facendone una priorità della vigilanza. Lo scopo della FINMA era determinare il motivo per cui gli attacchi ai fornitori di servizi andassero a segno con frequenza superiore alla media. Dai controlli in loco è emerso che ciò era ascrivibile, fra le altre cose, al fatto che gli istituti assoggettati alla vigilanza avessero formulato in maniera poco chiara i requisiti di cyber-sicurezza nei confronti dei fornitori esterni di servizi incaricati o alla mancata o discontinua verifica di tali requisiti.

- In seguito all'identificazione di gravi falle nella sicurezza, solo pochissimi istituti hanno interagito proattivamente con i loro principali fornitori esterni di servizi per garantire che questi potessero porvi rimedio rapidamente e prima che si verificasse un danno.
- La FINMA ha di frequente constatato che gli istituti direttamente assoggettati alla vigilanza hanno posto rimedio in modo rapido alle gravi vulnerabilità, evitando danni diretti. Tuttavia, alcuni fornitori esterni di servizi spesso non hanno reagito con la stessa efficacia e non erano sufficientemente preparati per affrontare le conseguenze di cyber-attacchi andati a segno.
- In molti casi gli istituti non disponevano di un inventario completo dei loro fornitori di servizi: mancavano informazioni che indicassero se presso il fornitore di servizi sono salvati dati critici o se esso è incaricato di erogare una funzione critica. Pertanto, presso tali fornitori di servizi spesso veniva svolto un controllo lacunoso o non veniva effettuato alcun controllo regolare da parte degli istituti assoggettati.
- Presso gli istituti analizzati, dall'inventario dei principali subdelegati nelle esternalizzazioni sono emerse notevoli differenze nel grado di maturità della registrazione, della documentazione e delle possibilità di accesso ai dati critici[2].
- Perlopiù gli istituti interessati non avevano definito in modo chiaro i dati critici. Ciò ha ostacolato non solo la protezione interna di questi dati, ma anche l'adeguata classificazione dei fornitori esterni e la determinazione delle necessarie misure di controllo per ridurre i rischi identificati.

[1] Cfr. al riguardo anche il nuovo rischio principale «esternalizzazione» *(outsourcing)* indicato nel Monitoraggio dei rischi 2023 e nel Rapporto annuale 2023 della FINMA.

[2] Cfr. al riguardo anche il nm. 14 Circ. FINMA 18/3.

Se un istituto esternalizza funzioni essenziali a un fornitore di servizi (in particolare per quanto concerne funzioni critiche o dati critici in misura rilevante), devono essere garantiti presso tali fornitori gli stessi requisiti regolamentari previsti per l'istituto assoggettato. Parimenti, tali requisiti sono applicabili anche ad eventuali subdelegati coinvolti. Pertanto, la FINMA considera che un inventario aggiornato delle principali esternalizzazioni, comprese quelle dei subdelegati, sia uno strumento essenziale.

L'istituto rimane responsabile in qualsiasi momento del rispetto dei requisiti prudenziali. Un'esternalizzazione o il trasferimento di tale responsabilità a un altro fornitore di servizi non è possibile.

2.2 *Governance* e identificazione

Un altro aspetto centrale è la *governance* nella gestione dei cyber-rischi. In passato, la FINMA ha constatato di frequente che i cyber-rischi sono stati presentati come un mero problema tecnologico e pertanto non è stata conferita loro la necessaria priorità a livello di direzione o di consiglio di amministrazione. Di conseguenza, nella nuova Circolare FINMA 23/1 sono state chiaramente definite, per esempio per le banche, le responsabilità dell'organo preposto all'alta direzione e della direzione (cfr. nm. 61). Inoltre, presso molti istituti assoggettati alla vigilanza la FINMA ha constatato le seguenti ulteriori carenze in materia di *governance*:

- Presso gli istituti di medie dimensioni, spesso non era stata effettuata una chiara delimitazione fra la gestione operativa dei cyber-rischi e l'istanza di controllo indipendente. È essenziale che l'efficacia della gestione operativa venga verificata in maniera continua da un'istanza di controllo indipendente[3].
- L'identificazione delle potenziali minacce dovute a cyber-rischi specifiche all'istituto era spesso lacunosa. Inoltre, spesso non si sapeva quali collaboratori avessero accesso a dati critici, in quanto mancava un sistema centralizzato per le autorizzazioni. Ciò ha reso più difficile per l'organo preposto alla sicurezza del corrispondente istituto approntare un dispositivo di protezione dei dati critici.
- Numerosi istituti assoggettati alla vigilanza non hanno esplicitamente integrato i cyber-rischi nella loro gestione trasversale dei rischi operativi. Per questo motivo non è stato possibile garantire una gestione sistematica e completa dei cyber-rischi.

[3] Cfr. sezioni sulle funzioni di controllo e sulle istanze di controllo indipendenti nella Circolare 2017/1 «*Corporate governance* – banche» e nella Circolare 2017/2 «*Corporate governance* – assicuratori».

- Inoltre, alcuni istituti assoggettati alla vigilanza hanno definito in modo insufficiente i cyber-rischi come pure la loro propensione e la loro tolleranza al rischio. Questi aspetti costituiscono tuttavia componenti centrali di un efficace dispositivo di protezione dai cyber-rischi.

Stando al Monitoraggio FINMA dei rischi, da anni i cyber-rischi si annoverano fra i rischi principali, motivo per cui riveste un'importanza centrale il fatto che gli istituti assoggettati li rilevino come un rischio a sé stante nella gestione dei rischi operativi qualitativi e definiscano una corrispondente propensione al rischio nonché una tolleranza al rischio.

Inoltre, è fondamentale che, in riferimento ai cyber-rischi, le funzioni chiave vengano integrate nel sistema di controllo interno (SCI) in conformità a standard o *practices* riconosciuti a livello internazionale e che la loro efficacia venga regolarmente esaminata, valutata e documentata da un'istanza di controllo indipendente. Occorre valutare regolarmente anche la separazione dei compiti, delle competenze e delle responsabilità al fine di garantire l'indipendenza e di prevenire i conflitti d'interesse.

2.3 Dispositivo di protezione

Per quanto concerne il dispositivo di protezione, nella vigilanza continua nel corso degli scorsi anni si è potuta constatare una tendenza positiva. Per esempio, nell'ambito del contrasto agli attacchi di interruzione distribuita del servizio (*Distributed Denial of Service*, DDoS)[4] gli istituti assoggettati alla vigilanza hanno adottato misure di protezione sempre migliori e maggiormente efficaci. Tuttavia, anche in questo ambito sono state effettuate importanti constatazioni in merito alle carenze in essere:

- Spesso le misure di protezione in materia di *Data Loss Prevention* (DLP) si sono limitate solo alle caratteristiche di identificazione del cliente o ai numeri delle carte di credito. Altri dati critici, come i dati personali degni di protezione, segreti d'affari, proprietà intellettuale ecc., non rientravano nelle misure di protezione in materia di DLP.
- Quasi tutti gli istituti sottoposti al controllo avevano definito una direttiva e processi concernenti la sicurezza dei dati *(back-up)* come pure piani di ripristino. Presso alcuni istituti mancava però un test di tali processi in caso di un grave cyber-attacco, p.es. un *malware* di crittografia *(ransomware)*.
- Presso un numero elevato di istituti assoggettati sussiste anche un potenziale di miglioramento negli ambiti della formazione e della consapevolezza informatica. Per un efficace dispositivo di protezione è indispensabile che il personale a tutti i livelli gerarchici sia formato e aggiornato

[4] Attacchi DDoS: un numero elevato di richieste, basate sulla potenza di calcolo distribuita, provoca un sovraccarico dei sistemi (ad esempio, un sito internet).

regolarmente sui cyber-rischi, conosca i metodi di attacco più comuni, tra cui il *phishing*, e sappia a quali interlocutori rivolgersi all'interno dell'azienda nel momento in cui sussistono indizi di un cyber-attacco. Questo obiettivo può essere perseguito in particolare mediante test regolari da parte dei collaboratori.

Per gli istituti ai quali si applica la Circolare FINMA 23/1, i requisiti concernenti la formazione e la consapevolezza in materia di cyber-rischi sono fissati esplicitamente nella circolare (cfr. nm. 26).

Inoltre, è indispensabile che tutti gli istituti si confrontino criticamente con uno scenario in cui le loro misure di protezione possano essere superate e un aggressore possa riuscire a causare il maggior danno possibile all'impresa. Al riguardo è importante che le attuali strategie di *back-up* e di ripristino vengano verificate, per esempio per chiarire se, nel quadro di una crittografia completa dei dati (critici), tali dati possano essere ripristinati entro i termini fissati e con la tempestività, l'integrità, la qualità e la completezza desiderate. Per le banche, al riguardo si rimanda in particolare ai nuovi requisiti prudenziali concernenti l'osservanza della resilienza operativa in conformità alla Circolare FINMA 23/1.

2.4 Individuazione, reazione e ripristino

La capacità di registrare, riconoscere e reagire tempestivamente ai cyber-attacchi è un elemento centrale nella maggior parte dei controlli della FINMA incentrati sui cyber-rischi e spesso costituisce anche il tema di accertamenti approfonditi.

Nel corso di tali controlli in loco, la FINMA ha constatato in particolare i seguenti schemi ricorrenti presso gli istituti assoggettati alla vigilanza:

- Alcuni degli assoggettati alla vigilanza non avevano allestito piani di reazione ai cyber-incidenti oppure tali piani erano incompleti o non erano stati verificati in termini di efficacia.
- Nell'individuazione e nella registrazione dei cyber-attacchi è inoltre emerso che alcuni istituti non avevano monitorato in modo tempestivo e sistematico la propria tecnologia della comunicazione. In alcuni casi mancava una valutazione dei dati log critici oppure questa veniva effettuata soltanto durante gli orari di ufficio.
- La maggior parte degli istituti aveva adottato misure volte a garantire il ripristino tempestivo del normale esercizio in seguito ad eventi straordinari. Tuttavia, al riguardo spesso mancavano specifiche misure di ripristino in seguito ai cyber-attacchi.

La preparazione in funzione dei rischi e basata su scenari da parte degli istituti assoggettati ai cyber-incidenti e alle crisi in ambito cyber riveste un'importanza centrale. In tale contesto, l'allestimento di piani di reazione realistici e testati costituisce un fattore essenziale di successo per gestire in modo efficace situazioni di stress causate da cyber-attacchi. In particolare, in seguito a un cyber-attacco andato a segno, è fondamentale trarre i dovuti insegnamenti e apportare immediatamente le necessarie migliorie.

3 Precisazioni concernenti la Comunicazione FINMA sulla vigilanza 05/2020

In seguito alla precisazione, nella Comunicazione FINMA sulla vigilanza 05/2020, dell'obbligo da parte di tutti gli istituti assoggettati di notificare i cyber-attacchi, la FINMA ha ricevuto varie domande concernenti la relativa interpretazione.

Per questa ragione, di seguito vengono precisati alcuni punti:

- A partire dal momento in cui viene individuato un cyber-attacco, l'istituto ha 24 ore di tempo per notificarlo alla FINMA.
- Entro questo lasso di tempo ci si attende che l'istituto proceda a una prima valutazione del grado di gravità, per poter giudicare se l'attacco soddisfa i criteri per una notifica alla FINMA[5].
- Per la prima notifica, la FINMA si attende che venga effettuata una comunicazione in via informale tramite e-mail, telefono ecc. al *Key Account Manager* responsabile per il corrispondente istituto assoggettato alla vigilanza. La prima notifica deve contenere una prima valutazione della gravità e descrivere sinteticamente la situazione. In questa fase non è richiesto l'inoltro di un modulo compilato integralmente sulla Piattaforma di rilevamento e di richiesta della FINMA (EHP) basata sul web.
- Gli istituti che sottostanno parimenti all'obbligo di notifica secondo la Legge sulla sicurezza delle informazioni (LSIn; RS *128*) possono inoltrare la loro notifica entro 24 ore utilizzando l'apposito modulo dell'Ufficio federale della cibersicurezza (UFCS) e selezionare l'opzione che prevede l'inoltro della notifica alla FINMA, purché il rispetto del termine possa essere garantito. La notifica completa entro 72 ore deve comunque essere effettuata tramite l'EHP.
- Se un istituto deve scegliere se completare la valutazione della gravità per una prima valutazione o rispettare il termine di 24 ore, la priorità deve essere accordata al rispetto del termine.

[5] Cfr. Comunicazione sulla vigilanza 05/2020, allegato 1.

- Una prima notifica già inoltrata alla FINMA entro 24 ore può essere ritirata in qualsiasi momento se l'istituto, nel quadro delle ulteriori determinazioni del grado di gravità e della relativa valutazione, giunge alla conclusione che il cyber-attacco non ha raggiunto la soglia di rilevanza.
- Se il fornitore di servizi di un istituto (p. es. ospedale, gestore patrimoniale, studio legale) non costituisce un partner essenziale in materia di *outsourcing* in conformità alla Circolare FINMA 18/3 «*Outsourcing*», l'istituto – in particolare in conformità all'art. 22 LSA, al nm. 68 della Circ. FINMA 23/1 e alla Comunicazione FINMA sulla vigilanza 05/2020, deve assicurarsi di essere stato informato da tale fornitore in merito ai cyber-incidenti verificatisi presso di esso. Se, in tal caso, l'istituto classifica il cyber-incidente come rilevante in conformità alla Comunicazione FINMA sulla vigilanza 05/2020, allora deve effettuare anche le necessarie notifiche alla FINMA.
- I termini per la notifica di 24 o 72 ore si applicano solo nei giorni lavorativi ufficiali della banca. Costituiscono un'eccezione i cyber-attacchi con grado di gravità «grave». Tali attacchi devono essere notificati entro 24 ore alla FINMA anche al di fuori dei giorni lavorativi della banca.
- L'obbligo di notifica per le esternalizzazioni si configura nel modo seguente: in conformità al nm. 23 della Circolare FINMA 18/3, gli assoggettati continuano ad avere nei confronti della FINMA la stessa responsabilità che avrebbero se non ricorressero all'esternalizzazione. Per converso, ciò significa che il termine per la notifica inizia a decorrere non appena l'istituto o, in caso di funzioni esternalizzate, l'offerente terzo, ha individuato un cyber-incidente. Ciò garantisce anche la parità di trattamento secondo il diritto in materia di vigilanza degli istituti che non hanno esternalizzato alcuna funzione.
- In conformità alla Comunicazione FINMA sulla vigilanza 05/2020, per le notifiche relative a cyber-attacchi con un grado di gravità «*medio*» viene redatto un rapporto conclusivo sulle cause che comprende almeno il rapporto d'indagine interno o esterno o il rapporto forense. Per le notifiche relative ai cyber-attacchi con grado di gravità «*elevato*» o «*grave*», il rapporto sulle cause dovrebbe comprendere i seguenti elementi:
  - il motivo per cui il cyber-attacco è andato a buon fine;
  - le ripercussioni dell'attacco sul rispetto delle disposizioni del diritto in materia di vigilanza, sull'esercizio dell'istituto e sui clienti;
  - le misure attuate per ridurre le conseguenze dell'attacco.

  Per i cyber-attacchi con grado di gravità «*grave*» devono inoltre essere presentate le comprove e le analisi concernenti il buon funzionamento dell'organizzazione per la gestione delle crisi.

4 Cyber-esercizi basati su scenari

Negli istituti ai quali si applica la Circolare FINMA 23/1 devono essere svolti cyber-esercizi in funzione dei rischi e basati su scenari. L'ampiezza e il contenuto di tali esercizi sono stabiliti in base al principio di proporzionalità. Per gli istituti di rilevanza sistemica, la FINMA considera che gli esercizi di *red teaming*[6] (simulazione avversaria) costituiscano una componente necessaria dei cyber-esercizi. Gli istituti privi di rilevanza sistemica dovrebbero svolgere un esercizio *tabletop* almeno una volta all'anno[7].

Gli istituti delle categorie di vigilanza 4 e 5 possono adempiere tale obbligo partecipando agli esercizi del Swiss Financial Sector Cyber Security Centre (Swiss FS-CSC)[8]. Al riguardo, per ogni istituto partecipante occorre garantire che la minaccia potenziale di questi esercizi specificatamente per l'istituto sia documentata in modo chiaro e che venga allestito un rapporto con i risultati specifici per l'istituto derivanti da questi esercizi. Se la minaccia specifica per l'istituto non può essere desunta dal cyber-esercizio svolto dal Swiss FS-CSC, per esempio perché lo scenario non ha una rilevanza marcata per il profilo di rischio di un istituto, tale istituto deve comunque svolgere un cyber-esercizio individuale riferito allo scenario in questione ai fini dell'osservanza del nm. 70.

La FINMA si riserva il diritto di far svolgere o di accompagnare da vicino tali esercizi in funzione dei rischi e basati su scenari in maniera selettiva nel quadro della verifica prudenziale o di una verifica supplementare. I quadri normativi esistenti dovrebbero essere usati come riferimento in questo caso[9].

[6] *Red teaming*: gli esperti in materia di sicurezza assumono il ruolo di un aggressore e cercano di attaccare e aggirare le misure di sicurezza informatica di un'impresa copiando il metodo di attacco di un *hacker* "malintenzionato".

[7] *Tabletop*: simulazione e riproduzione di uno scenario su carta (esercitazione teorica).

[8] Vgl. https://fscsc.ch/

[9] Cfr. p.es. TIBER-EU, CBEST Threat Intelligence-Led Assessments