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 05/2020

Obbligo di notificare i cyber-attacchi secondo l'art. 29 cpv. 2 LFINMA

7 maggio 2020

Laupenstrasse 27
3003 Bern
Tel. +41 (0)31 327 91 00
Fax +41 (0)31 327 91 01
www.finma.ch

1 Introduzione

La FINMA continua a ritenere che il pericolo rappresentato dai cyber-attacchi[1] sulla piazza finanziaria svizzera sia molto elevato. Gli istituti assoggettati alla vigilanza della FINMA sono nel mirino dei cyber-criminali che, oltre a perseguire interessi pecuniari, puntano a compromettere la disponibilità, la confidenzialità e l'integrità dell'infrastruttura tecnologica di importanza critica come pure di informazioni sensibili. Il pericolo di cyber-attacchi è ancora più accentuato soprattutto in particolari situazioni di stress, come l'attuale pandemia di COVID-19. I cyber-criminali sfruttano la fase di incertezza e adeguano le loro strategie di attacco all'attuale situazione, mettendo ancora più sotto pressione le imprese già fortemente sollecitate.

Lo scopo della presente comunicazione sulla vigilanza è rammentare a tutti gli istituti assoggettati alla vigilanza della FINMA il requisito legale vigente che prevede di notificare senza indugio tutti gli eventi di grande importanza ai fini della vigilanza (art. 29 cpv. 2 LFINMA). Ciò comprende gli eventi di grande importanza in relazione con i cyber-attacchi andati a buon fine o in parte falliti.[2] La FINMA verificherà successivamente, sulla base delle ulteriori esperienze maturate in relazione all'obbligo di notifica, la necessità di integrare le seguenti precisioni in una circolare.

2 Cyber-attacchi di grande importanza ai fini della vigilanza

L'importanza di un cyber-attacco è determinata dal fatto che esso compromette, direttamente o indirettamente[3], da un lato la protezione individuale, ossia la tutela dei creditori, degli investitori e degli assicurati e, dall'altro, la funzionalità dei mercati finanziari.

Ciò riguarda principalmente i cyber-attacchi, indipendentemente dal fatto che siano andati a buon fine o siano in parte falliti, perpetrati a danno delle funzioni di importanza critica[4] per gli assoggettati, il cui dissesto o malfunzionamento avrebbe considerevoli ripercussioni sulla protezione individuale e la

[1] S'intendono gli attacchi perpetrati a partire da Internet e reti affini a danno dell'integrità, della disponibilità e della confidenzialità dell'infrastruttura tecnologica, in particolare per quanto riguarda i dati critici e/o sensibili e i sistemi informatici.

[2] Per le imprese di assicurazione, l'obbligo di notifica deriva inoltre dall'impatto mediatico nonché dal potenziale danno di reputazione o di solvibilità provocato dai cyber-attacchi. Cfr. Circolare FINMA 08/25 «Obbligo di informazione – assicuratori», nm. 1 e 5.

[3] Per esempio, mediante attacchi a infrastrutture di importanza critica per gli assoggettati alla vigilanza della FINMA (p. es. fornitore di servizi internet, fornitore di energia elettrica, ecc.).

[4] Prodotti e servizi forniti dagli assoggettati e relativi processi operativi soggiacenti (p. es. traffico dei pagamenti, approvvigionamento in numerario, negoziazione in borsa, allestimento e gestione di contratti di assicurazione, trattamento dei sinistri ed elaborazione delle prestazioni, gestione dei dati personali degni di particolare protezione nel comparto delle assicurazioni contro le malattie e sulla vita; gestione di titoli e investimenti, ecc.) e dei relativi attivi critici.

compromettterebbe fortemente. Ciò comprende segnatamente l'obiettivo di protezione della disponibilità. D'altro canto, questi attacchi possono tuttavia compromettere anche gli obiettivi di protezione dell' integrità dell'infrastruttura tecnologica e della confidenzialità delle informazioni e dei dati. Se sono interessati istituti di rilevanza sistemica o più istituti contemporaneamente che forniscono prestazioni integrate di importanza critica, in determinate circostanze gli attacchi sono suscettibili di compromettere anche la funzionalità dei mercati finanziari in Svizzera.

Di norma, i cyber-attacchi sono direttamente rivolti alle risorse di supporto di tali funzioni critiche. Sono segnatamente considerate risorse di supporto designate come critiche il personale, l'infrastruttura tecnologica, le informazioni e gli edifici, come pure i fornitori di importanza critica[5] che supportano i processi operativi di tali funzioni critiche. Ogni assoggettato è tenuto a identificare in modo autonomo le proprie funzioni critiche, i corrispondenti processi operativi nonché le attività critiche di supporto[6].

Se in seguito a un cyber-attacco ad attività critiche vengono compromessi uno o più obiettivi di protezione di funzioni critiche e i loro processi operativi, occorre notificarlo senza indugio alla FINMA.

[5] Se un istituto delega funzioni essenziali ad altre persone fisiche o giuridiche, esso è sottoposto all'obbligo di notificare i cyber-attacchi perpetrati ai danni dei suoi fornitori, se tali attacchi incidono sulle funzioni essenziali che sono state esternalizzate. Cfr. al riguardo l'art. 47 cpv. 2 della Legge sulla sorveglianza degli assicuratori (LSA; RS 961.01).

[6] Per esempio il nm. 135.2 e il nm. 135.7 e segg. della Circ. FINMA 08/21 «Rischi operativi – banche» e gli standard minimi Business Continuity Management dell'ASA, Circolare FINMA 17/2 «*Corporate governance* – assicuratori», nm. 28 segg.

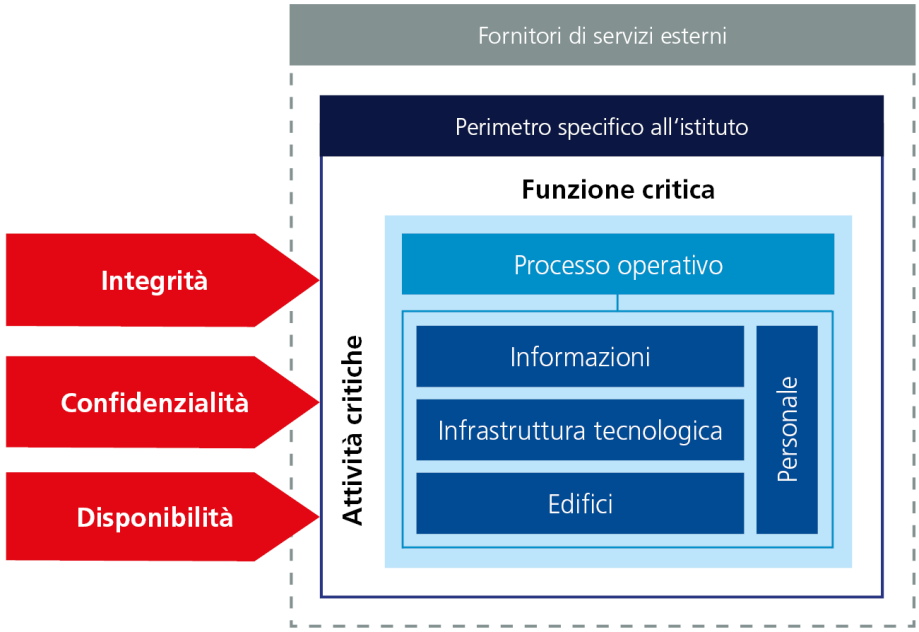

Figura 1: Rappresentazione schematica di un cyber-attacco alla funzione critica di un assoggettato.

Nell'allegato 2 è riportato un elenco non esaustivo di esempi di attivi critici e possibili cyber-attacchi a essi rivolti.

3 Notifica immediata alla FINMA

Per notifica immediata alla FINMA s'intende che, in caso di constatazione di un cyber-attacco, il competente (Key) Account Manager dell'istituto interessato informa la FINMA entro 24 ore e dopo aver effettuato una prima valutazione del livello di criticità. La notifica deve essere effettuata in base al seguente elenco, entro 72 ore, tramite la Piattaforma di richiesta e di rilevamento (EHP) della FINMA[7][8].

Il seguente elenco fornisce un'indicazione del contenuto della notifica alla FINMA:

- Nome dell'istituto

[7] https://www.finma.ch/it/finma/extranet/piattaforma-di-rilevamento-e-di-richiesta-ehp/ (disponibile a partire dall'1° giugno 2020)

[8] Sulla Piattaforma EHP: ~~"EHP" – "Dichiarazioni" – pulsante: "Nuova dichiarazione" – Modello di dichiarazione: "Dichiarazioni cyber-attacchi"~~
"EHP" – "Dati trasmessi" – Pulsante: "Dati Trasmessi +" – Modello di dichiarazione: "Dichiarazioni cyber-attacchi"

- Persona di contatto, inclusi dati di contatto (numero di telefono e indirizzo e-mail)
- Data / Orario di notifica alla FINMA
- Data / Orario di constatazione dell'attacco
- Data / Orario in cui è avvenuto l'attacco (se noto)
- Descrizione dei cyber-attacchi e situazione attuale
- Prima valutazione del grado di gravità del cyber-attacco (v. allegato 1) *(opzioni: medio, elevato, grave)*
- Evoluzione del grado di gravità *(opzioni: decrescente, stabile, crescente)*
- Entità interessate (unità organizzativa(e) presso l'istituto o il fornitore)
- Obiettivi di protezione interessati (*scelta multipla: confidenzialità, integrità, disponibilità)*
- Funzioni di importanza critica interessate, processi operativi e attività (informazioni, infrastruttura tecnologica, edifici o personale interessati)
- Numero di clienti interessati (stato attuale)
- Vettori di attacco *(scelta multipla: e-mail, attacco tramite web, attacco di forza bruta, furto dell'identità, supporti esterni rimovibili, perdita/furto di apparecchi, sfruttamento delle vulnerabilità del software, sfruttamento delle vulnerabilità dell'hardware, altro [indicare]).*
- Tipo di attacco (descrizione) (p. es. DDoS, accesso non autorizzato, malware, abuso/uso improprio delle infrastrutture tecnologiche, ecc.).
- Contromisure amministrative, operative e/o tecniche con indicazione della scadenza prevista
- Misure di comunicazione (cosa, a chi, quando)

Se, dopo che l'obbligo di notifica è stato integralmente adempiuto, si verificano nuovi sviluppi o nuove valutazioni sul medesimo attacco, occorre effettuare un'ulteriore notifica entro il termine menzionato di 72 ore.

Per i cyber-attacchi con grado di gravità elevato o grave (v. allegato 1), la FINMA si attende che l'istituto, dopo aver terminato il trattamento del caso, rediga un rapporto conclusivo sulle cause (analisi *root cause*), che includa segnatamente un'analisi, le ragioni per cui l'attacco è andato a buon fine, le ripercussioni degli attacchi sul rispetto delle disposizioni regolamentari, sull'esercizio e sui clienti, nonché le misure volte a ridurre le conseguenze dell'attacco. Per i cyber-attacchi con grado di gravità grave (v. allegato 1) devono inoltre essere presentate le comprove e le analisi concernenti il buon funzionamento dell'organizzazione per la gestione delle crisi.

Per i cyber-attacchi con grado di gravità medio (v. allegato 1) è sufficiente un rapporto conclusivo sulle cause.

La FINMA si attende dagli assoggettati che il contenuto della presente Comunicazione sulla vigilanza concernente l'obbligo di notifica per i cyber-attacchi sia attuato al più tardi entro il 1° settembre 2020, o anche prima sulla base del *best effort*.

Allegato 1: Determinazione del grado di gravità di un cyber-attacco

Per determinare il grado di gravità di un cyber-attacco, possono essere utilizzati i criteri seguenti.

Grado di gravità	Definizione	Criteri
Grave	Danni presenti o attesi di grande entità e duraturi agli obiettivi di protezione (disponibilità, integrità, confidenzialità) delle attività di importanza critica.	– Disponibilità: le attività di importanza critica non sono disponibili sul medio-lungo periodo (*default* > 200 % del RTO[9]) – Confidenzialità / integrità: informazioni sensibili (quasi) pienamente interessate – Ripercussioni finanziarie o danni alla reputazione che compromettono l'esistenza dell'istituto – La gestione dei cyber-attacchi comporta l'attivazione dell'organizzazione per la gestione delle crisi (BCM).
Elevato	Gli obiettivi di protezione (disponibilità, integrità, confidenzialità) delle attività di importanza critica sono seriamente danneggiati o in pericolo.	– Disponibilità: gli attivi di importanza critica non sono disponibili sul medio periodo (*default* >= RTO) – Confidenzialità / integrità: informazioni sensibili interessate in larga misura e/o informazioni di importanza critica per il processo operativo. – Considerevoli ripercussioni finanziarie o danni alla reputazione – La gestione dei cyber-attacchi comporta il ricorso a risorse esterne.
Medio	Gli obiettivi di protezione (disponibilità, integrità, confidenzialità) delle attività di importanza critica sono direttamente danneggiati o in pericolo.	– Disponibilità: le attività di importanza critica non sono disponibili sul breve periodo (*default* > 50 % del RTO) – Confidenzialità / integrità: informazioni sensibili interessate in misura considerevole[10] – Notevoli ripercussioni finanziarie o danni alla reputazione – I cyber-attacchi possono essere gestiti internamente con le risorse a disposizione.

[9] *Recovery time objective*: tempo previsto per la riattivazione degli attivi di importanza critica.

[10] Al di fuori del normale corso degli affari (*business as usual*)

Allegato 2: Esempi di attività di importanza critica e cyber-attacchi ai relativi obiettivi di protezione

	Esempi di attività di importanza critica	Esempi di cyber-attacchi
Informazioni	Informazioni sensibili / confidenziali come dati sull'identificazione dei clienti, contratti di assicurazione, dati in relazione con la liquidazione dei danni e l'elaborazione delle prestazioni, protocolli delle sedute del consiglio di amministrazione e della direzione, informazioni sulla strategia, dati concernenti le Risorse umane, ecc.	Attacchi agli obiettivi di protezione mediante l'accesso non autorizzato ai dati all'interno ma anche all'esterno dell'impresa, deflussi di dati, furto di dati, modifica dei dati, ecc.
Infrastruttura tecnologica	Infrastruttura tecnologica necessaria per lo svolgimento di una funzione d'importanza critica (p. es. *hardware*, *software*, infrastruttura, ecc.).	Attacchi agli obiettivi di protezione mediante (D)DoS, perdita / furto di supporti per l'archiviazione di informazioni confidenziali, *ransomware*, ecc.
Edifici	Edifici essenziali per l'erogazione di funzioni di importanza critica (p. es. centri di ricerca, filiali, uffici di *back office*, ecc.).	Attacchi agli obiettivi di protezione mediante malfunzionamento o disattivazione delle misure di protezione che regolano l'accesso agli ambiti sensibili.
Personale	Collaboratori che svolgono funzioni di importanza critica o vi contribuiscono in misura significativa, come la direzione, i commercianti, i consulenti alla clientela ecc. e i collaboratori che rivestono un ruolo chiave (p. es. collaboratori con privilegi elevati, amministratori del sistema, personale addetto alla sicurezza, contabilità, ecc.).	Attacchi agli obiettivi di protezione mediante *social engineering* (p. es. *spear phishing*), minacce d'*insider*, furto d'identità, estorsione, ecc.