CERTFin

Il quadro normativo dell'incident reporting: stato dell'arte

BANCHE & SICUREZZA

16 maggio 2023

TLP GREEN

Maria Ferrucci

Cyber security and fraud analyst

CERTFin

Agenda

- Principali definizioni di «incidente»
- Stato dell'arte del framework normativo di riferimento
- Verso un reporting «integrato»: la proposta del FSB
- Conclusioni

Principali definizioni di «incidente»

Circolare 285

- **<u>Incidenti di sicurezza (cyber)</u>:** *«incidenti causati da attività volontaria e malevola riguardanti l'accesso, l'uso, la divulgazione, l'interruzione, la modifica o la distruzione non autorizzati delle risorse della banca o incidenti che comunque producono, anche involontariamente, diffusione e/o alterazione di dati riservati della clientela e/o dell'intermediario» → vi rientrano anche le **frodi informatiche***
- **<u>Incidenti operativi</u>:** *«incidenti derivanti da processi inadeguati o malfunzionanti, persone e sistemi o eventi di forza maggiore. Tra tali eventi sono inclusi quelli naturali, errori software/hardware, eventi accidentali, malfunzionamenti di processo, sabotaggio (attacco fisico). **La diffusione e/o l'alterazione involontaria (ad esempio, per errore umano o software) di dati riservati della clientela e/o dell'intermediario ricade nella categoria degli incidenti cyber**»*

Cyber lexicon

<u>Cyber incident</u>: *«cyber event that adversely affects the cyber security of an information system or the information the system processes, stores or transmits **whether resulting from malicious activity or not**»*

Direttiva NIS2

<u>Incidente di sicurezza</u>: *«un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi»*

Stato dell'arte del framework normativo di riferimento (1/3)

Norma	Entrata in vigore / applicazione	Rif. articolo	Europea / Italiana	Soggetti obbligati	Soggetti destinatari	Oggetto della notifica	Tempistiche	Soglie / Criteri	Modalità Operative
PSD2 - Direttiva (UE) 2015/2366	13/1/2016 13/1/2018 (D. lgs.15 dicembre 2017, n. 218)	Art. 96	Europea	PSP	ANC / se l'incidente incide sugli interessi finanziari degli utenti, questi vengono informati	Gravi incidenti operativi o di sicurezza	Senza indugio / Almeno annuale, in caso di frodi connesse ai diversi mezzi di pagamento	Si rimanda a specifici Orientamenti dell'ABE	Si rimanda a specifici Orientamenti dell'ABE
Orientamenti in materia di segnalazione dei gravi incidenti ai sensi della PSD2 (EBA/GL/ 2021/03)	1/1/2022	-	Europea	PSP	ANC	Gravi incidenti operativi o di sicurezza	La segnalazione consiste nell'invio di 3 report: • *Iniziale*: entro 4 ore dalla classificazione (da fare entro 24 h dalla rilevazione); • *Intermedio*: quando le attività sono ripristinate, al più entro 3 giorni dal report iniziale; • *Finale*: entro 20 gg dalla chiusura dell'incidente	L'incidente è classificato come grave se soddisfa: • uno o più criteri al «livello di impatto maggiore», o • tre o più criteri al «livello di impatto minore»	Allegato - Modello di segnalazione per i prestatori di servizi di pagamento
Circolare 285/2013 (Comunicazione del 29 ottobre 2021)	29/10/2021	Parte Prima – Capitolo 4 – Sezione IV	Italiana	SI italiane e banche autorizzate in Italia appartenenti a SI straniere	Banca d'Italia (laddove previsto, inoltra a ABE / BCE)	Gravi incidenti operativi o di sicurezza	La segnalazione consiste nell'invio di 3 report: • *First: entro 2 ore dalla classificazione (da fare entro 24 h dalla rilevazione);* • *Interim: quando le attività sono ripristinate, al più entro 3 giorni dal first;* • *Final: entro 20 gg dalla chiusura dell'incidente*	L'incidente è classificato come grave se: • è soddisfatta una sola delle soglie «qualitative», per almeno una entità del gruppo • per le soglie «quantitative» deve essere effettuata una valutazione a livello consolidato / individuale	Notifica da effettuare con appositi moduli reperibili presso il sito web di Banca d'Italia
				LSI italiane e succursali di banche extracomunitarie			La segnalazione consiste nell'invio di 3 report: • *Iniziale: entro 4 ore dalla classificazione (da fare entro 24 h dalla rilevazione);* • *Intermedio: quando le attività sono ripristinate, al più entro 3 giorni dal first;* • *Finale: entro 20 gg dalla chiusura dell'incidente*	L'incidente è classificato come grave se soddisfa: • uno o più criteri al «livello di impatto maggiore», o • tre o più criteri al «livello di impatto minore»	Notifica da effettuare con appositi moduli reperibili presso il sito web di Banca d'Italia
				IP, IMEL e succursali di banche extracomunitarie con sede in Svizzera, Giappone, USA, Canada			La segnalazione consiste nell'invio di 3 report • *Iniziale: entro 4 ore dalla classificazione (da fare entro 24 h dalla rilevazione);* • *Intermedio: quando le attività sono ripristinate, al più entro 3 giorni dal first;* • *Finale: entro 20 gg dalla chiusura dell'incidente*	L'incidente è classificato come grave se soddisfa: • uno o più criteri al «livello di impatto maggiore», o • tre o più criteri al «livello di impatto minore»	Notifica da effettuare con appositi moduli reperibili presso il sito web di Banca d'Italia

Stato dell'arte del framework normativo di riferimento (2/3)

Norma	Entrata in vigore / applicazione	Rif. Articolo	Europea / Italiana	Soggetti obbligati	Soggetti destinatari	Oggetto della notifica	Tempistiche	Soglie / Criteri	Modalità Operative
Direttiva NIS - Direttiva (UE) 2016/1148	26/7/2016	Art. 14 e art.16	Europea	Operatori di Servizi Essenziali (OSE) e Fornitori di servizi digitali (FSD)	Autorità competente o CSIRT	Incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati / sulla fornitura dei servizi elencati all'Allegato III (es. cloud)	Senza indebito ritardo	3 criteri per gli OSE: a) il numero di utenti interessati dalla perturbazione del servizio essenziale b) la durata dell'incidente c) la diffusione geografica relativamente all'area interessata dall'incidente 5 criteri per i FSD: → ai precedenti si aggiungono: d) la portata della perturbazione del funzionamento del servizio e) la portata dell'impatto sulle attività economiche e sociali	Si rimanda a specifici Orientamenti del Gruppo di Cooperazione NIS
D. lgs. 18 maggio 2018, n.65	24/6/2018	Art. 12 e art. 14	Italiana	Operatori di Servizi Essenziali (OSE) e Fornitori di servizi digitali (FSD)	CSIRT e, per conoscenza, Autorità Competente NIS	Incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati / sulla fornitura dei servizi elencati all'Allegato III (es. cloud)	Senza ingiustificato ritardo	3 criteri per gli OSE: a) il numero di utenti interessati dalla perturbazione del servizio essenziale b) la durata dell'incidente c) la diffusione geografica relativamente all'area interessata dall'incidente 5 criteri per i FSD: → ai precedenti si aggiungono: d) la portata della perturbazione del funzionamento del servizio e) la portata dell'impatto sulle attività economiche e sociali.	Notifica da effettuare attraverso gli appositi canali predisposti (sito web dello CSIRT)
DPCM 81/2021	26/6/2021	-	Italiana	Soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica	CSIRT Italiano	Incidenti aventi un impatto sui beni ICT (Tabelle 1 e 2 dell'Allegato A, rispettivamente incidenti meno gravi e più gravi)	• Entro 1 ora dalla detection (incidenti più gravi) • Entro 6 ore dalla detection (incidenti meno gravi)	-	Notifica da effettuare attraverso gli appositi canali predisposti (sito web dello CSIRT)
Determina 3 gennaio 2023 ACN	18/1/2023	-	Italiana	Soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica	CSIRT Italiano	Incidenti aventi impatto su reti, sistemi informativi e servizi informatici diversi dai beni ICT di pertinenza dei soggetti inclusi nel perimetro (le categorie di incidenti sono elencate nell'Allegato A)	Entro 72 ore dalla detection	-	Notifica da effettuare attraverso gli appositi canali predisposti (sito web dello CSIRT)

Stato dell'arte del framework normativo di riferimento (3/3)

Norma	Entrata in vigore / applicazione	Rif. Articolo	Europea / Italiana	Soggetti obbligati	Soggetti destinatari	Oggetto della notifica	Tempistiche	Soglie / Criteri	Modalità Operative
GDPR - Regolamento (UE) 2016/679	25/5/2018	Art. 33	Europea	Titolari del Trattamento di Dati Personali	Garante della Privacy	Violazione di dati personali (*Data breach*)	Senza ingiustificato ritardo e, ove possibile, entro 72 ore da quando si è venuti a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche	Vanno notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali (chiarimento contenuto nelle EDPB Guidelines)	Notifica da effettuare accedendo al servizio telematico dedicato presso il sito web del Garante della Privacy
Direttiva NIS2 – Direttiva (UE) 2022/2555	18/10/2024	Art. 23	Europea	Soggetti essenziali o importanti	- CSIRT o, se opportuno, Autorità Competente - Se opportuno, i destinatari dei loro servizi	Incidenti significativi, ovvero che hanno un impatto significativo sulla fornitura dei servizi offerti	• Preallarme, senza indebito ritardo e al più entro 24 ore dalla detection • Valutazione iniziale (notifica), senza indebito ritardo e al più entro 72 ore dalla detection • Relazione finale, entro un mese dalla notifica Eventuali: • Relazione intermedia se richiesta dal CSIRT/ANC • Relazione sui progressi + relazione finale, se incidente in corso dopo un mese dalla notifica.		Si rimanda a eventuali atti di esecuzione della Commissione su formato / procedura di invio
DORA – Regolamento (UE) 2022/2554	17/1/2025	Art. 17-23	Europea	«Entità finanziarie»	Autorità competente interessata	Gravi incidenti TIC e gravi incidenti operativi o relativi alla sicurezza dei pagamenti (in caso di enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti e istituti di moneta elettronica)	• Notifica iniziale • Relazione intermedia (seguita da eventuali aggiornamenti), non appena cambi in maniera significativa lo stato dell'incidente • Relazione finale, quando è stata conclusa l'analisi delle cause dell'incidente	• Numero e/o rilevanza di transazioni / clienti o controparti interessate • Impatto reputazionale • Durata incidente • Estensione geografica • Impatti sui dati • Criticità dei servizi colpiti • Impatto economico	Si rimanda a specifici RTS per ulteriori dettagli quali ad esempio criteri e soglie per la determinazione della rilevanza e formati di segnalazione
Cyber Resilience Act	Proposta: 15/9/2022	Art. 11	Europea	«Fabbricanti» (sviluppano o fabbricano prodotti con elementi digitali e li commercializzano con il proprio nome o marchio)	• ENISA • Utilizzatori del prodotto con elementi digitali (in caso di incidente) • Persona o soggetto che si occupa della manutenzione della componente (in caso di vulnerabilità in un componente)	• Qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto con elementi digitali • Qualsiasi incidente che abbia un impatto sulla sicurezza del prodotto con elementi digitali.	• ENISA: senza indebito ritardo e, comunque, entro 24 ore dalla detection • Utilizzatore del prodotto: senza indebito ritardo		Si rimanda a eventuali atti di esecuzione della Commissione su formato / procedura di invio

Verso un reporting «integrato»: la proposta del Financial Stability Board

Alcune date salienti delle iniziative del FSB in ambito cyber resilience:

- Novembre 2018 → Cyber lexicon
- Ottobre 2021 → Cyber incident reporting: existing approaches and next steps for broader convergence
- Ottobre 2022 → Achieving greater convergence in incident reporting – Consultative document
- Aprile 2023 →
  - ***Recommendations to achieve greater convergence in cyber incident reporting*** (identificazione di issues e challenges nell'armonizzazione del reporting e raccomandazioni per il settore);
  - ***Aggiornamento Cyber lexicon*** (specifico per il settore finanziario, set limitato di termini «core», esclusione di termini «tecnici», utilizzo di fonti esistenti);
  - ***Format for Incident Reporting Exchange (FIRE)*** (entro due anni definizione del modello, sottoposto a consultazione pubblica).

Conclusioni

- È opportuno **presidiare le evoluzioni normative** che impattano su ambiti che si intersecano tra loro, al fine di ottenere benefici complessivi in termini di costi e di effort;

- Una **maggiore armonizzazione nella segnalazione** degli incidenti potrebbe produrre importanti benefici, tra cui:
  - sviluppare una visione comune e monitorare più efficacemente gli incidenti;
  - rafforzare la regolamentazione e la supervisione dei rischi cyber;
  - facilitare il coordinamento e la condivisione cross-authority e cross-border.

- Fatte salve le necessità di comunicazione istituzionale, i **meccanismi di condivisione delle informazioni** saranno tanto più efficaci quanto più i diversi soggetti coinvolti riusciranno a condividere esperienze e lesson learned.