DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Cybersicurezza: i nuovi obblighi di notifica degli incidenti

17 Gennaio 2023

Stefano Mele, Partner, Gianni & Origoni

DB non solo diritto bancario

Stefano Mele, Partner, Gianni & Origoni

Stefano Mele

Stefano Mele è Partner dello studio Gianni & Origoni. Responsabile del Dipartimento di Cybersecurity e co-Responsabile del Dipartimento Privacy dello studio Gianni & Origoni. Esperto in materia di ICT, Privacy & Cybersecurity Law. Ha maturato venti anni di esperienza su questioni relative al proprio ambito di operatività e ha prestato la propria assistenza per importanti operazioni riguardanti questioni legali complesse e su più giurisdizioni in materia di nuove tecnologie e privacy, nonché su sicurezza cibernetica e crisis management a seguito di attacchi cyber. È membro del Consiglio Direttivo e Presidente della Commissione Sicurezza Cibernetica del Comitato Atlantico Italiano, oltre che Presidente del "Gruppo di lavoro sulla Cybersecurity" della Camera di Commercio americana in Italia (AmCham).

Dal prossimo 25 gennaio, i soggetti pubblici e privati inclusi all'interno dell'impianto normativo del Perimetro di Sicurezza Nazionale Cibernetica (di seguito, anche "Perimetro") avranno l'obbligo di notificare allo CSIRT Italia – organo oggi collocato all'interno dell'Agenzia per la Cybersicurezza Nazionale – gli incidenti aventi un impatto sulle reti, sui sistemi informativi e sui servizi informatici di propria pertinenza diversi dai beni ICT.

Questo nuovo obbligo discende dal combinato disposto dell'art. 1, comma 3-*bis*, del decreto-legge n. 105 del 2019 (comma inserito dall'art. 37-*quater*, comma 1, del decreto-legge 9 agosto 2022, n. 115, convertito con modificazioni dalla Legge 21 settembre 2022, n. 142) e dalla recentissima determina del 03 gennaio 2023 del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, pubblicata all'interno della Gazzetta Ufficiale del 10 gennaio 2023.

Per inquadrare correttamente tale obbligo, però, occorre fare un passo indietro e contestualizzare questa nuova richiesta del legislatore. Infatti, l'art. 3 del DPCM 81/2021, ovvero il secondo decreto attuativo del Perimetro di Sicurezza Nazionale Cibernetica, prevede da tempo che i soggetti pubblici e privati da cui dipenda l'esercizio di una funzione essenziale dello Stato o la prestazione di un servizio per gli interessi dello Stato, così come definiti nell'art. 2, comma 1, lett. *a)* e *b)*, del DPCM 131/2021, che abbiano ricevuto la comunicazione di inclusione all'interno del Perimetro, provvedano a notificare le tipologie di incidenti previste nell'allegato A del DPCM 81/2021. Questa imposizione, tuttavia, è relativa solo ai beni ICT di propria pertinenza, ovvero a quell'"*insieme di reti, sistemi informativi e servizi informatici, o parti di essi, di qualunque natura, considerato unitariamente ai fini dello svolgimento di funzioni essenziali dello Stato o per l'erogazione di servizi essenziali*" (art. 1, comma 1, lett. *m)*, del DPCM 131/2020), che siano stati comunicati nell'elenco dei beni ICT effettuato ai sensi dell'articolo 1, comma 2, lettera *b)*, del decreto-legge n. 105 del 2019.

Il legislatore, inoltre, all'art. 3, comma 3, del DPCM 81/2021, prevede anche che i soggetti inclusi nel Perimetro procedano comunque alla notifica nei casi in cui "*uno degli incidenti individuati nelle tabelle di cui all'allegato A* [del DPCM 81/2021] *si verifichi a carico di un sistema informativo o un servizio informatico, o parti di essi, che* [...] *condivida con un bene ICT funzioni di sicurezza, risorse di calcolo o memoria, ovvero software di base, quali sistemi operativi e di virtualizzazione*". Tale ulteriore previsione, quindi, estende l'obbligo di notifica anche a quelli che potremmo chiamare i 'beni contigui ai beni ICT', partendo dalla

vedi l'articolo online

concreta – e condivisibile – esigenza che un incidente che colpisca tali beni potrebbe velocemente "scalare" verso i beni ICT e comportare, quindi, ben presto un pregiudizio per la sicurezza nazionale.

Delineata sinteticamente la situazione ad oggi vigente, occorre evidenziare come l'inserimento del comma 3-*bis* all'interno dell'art. 1 del decreto-legge n. 105 del 2019, a cui ha fatto seguito – come accennato in precedenza – la recentissima determina del 03 gennaio 2023 del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, nasca dall'esigenza di estendere la conoscenza delle informazioni relative agli incidenti anche ai casi in cui questi non colpiscano solo i beni ICT o i 'beni contigui ai beni ICT'. Il legislatore, infatti, richiede che i soggetti pubblici e privati inclusi nel Perimetro di Sicurezza Nazionale Cibernetica, dal 25 gennaio 2023, notifichino allo CSIRT Italia anche quegli incidenti aventi un impatto sulle reti, sui sistemi informativi e sui servizi informatici di propria pertinenza "diversi" dai beni ICT.

Tale notifica dovrà essere effettuata entro 72 ore dal momento in cui il soggetto colpito sia venuto a conoscenza, a seguito delle evidenze ottenute, che l'incidente subìto faccia parte di una delle categorie indicate all'interno della tassonomia di cui all'allegato A, Sezione 1, della determina del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale (*i.e.*, accesso iniziale, esecuzione, installazione, movimenti laterali, azioni sugli obiettivi). Tuttavia, se quelle della Sezione 1 sono da considerarsi come notifiche obbligatorie, le categorie presenti nella Sezione 2 dell'allegato A sono, invece, facoltative e sono tese a fornire all'Agenzia per la Cybersicurezza Nazionale un quadro di valutazione della minaccia più completo. Esse si sostanziano, tuttavia, almeno per il momento, nella sola 'ricognizione riferita ad attività di *spearphishing*'.

Per completezza, occorre sottolineare anche come il legislatore – correttamente – abbia utilizzato essenzialmente la stessa tassonomia prevista in precedenza per gli incidenti legati ai beni ICT, contenendo però il numero delle categorie previste, in considerazione della potenziale minore gravità degli effetti di tali incidenti per la sicurezza nazionale.

Nella novella normativa in analisi resta fermo anche il concetto di incidente, che continua ad essere definito come "*ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici*", facendo intendere, quindi, come debbano essere prese in considerazione tutte le tipologie di incidenti e non solo quelli *cyber*.

Unica eccezione a questo obbligo è per gli incidenti aventi un impatto sulle reti, sui sistemi informativi e sui servizi informatici del Ministero della difesa, per i quali si applicano solo i principi e le modalità di cui all'art. 528, comma 1, lettera *d)*, del Codice dell'Ordinamento Militare (Decreto Legislativo 15 marzo 2010, n. 66), ovvero le norme del Codice dell'amministrazione digitale con le limitazioni di cui all'articolo 2, comma 6, e all'articolo 75, comma 2, nonché le facoltà di cui all'art. 17, comma 1-*bis*.

In ultimo, appare senz'altro opportuno evidenziare anche come, a differenza di ciò che avviene per gli incidenti relativi ai beni ICT e ai 'beni contigui ai beni ICT', il legislatore non abbia previsto alcuna sanzione per il mancato adempimento di tale ulteriore obbligo di notifica.

In conclusione, appare evidente come il novellato quadro normativo in materia di notifiche degli incidenti implichi per i soggetti pubblici e privati inclusi nel Perimetro di Sicurezza Nazionale Cibernetica – ivi comprese, quindi, anche le banche – un'urgente attività di aggiornamento dei processi interni di rilevazione, analisi e condivisione delle informazioni. Tale attività dovrà essere compiuta in tempi strettissimi, ovvero entro il 25 gennaio 2023. Essa comporterà la necessità non solo di adeguare i propri processi interni alle nuove tempistiche stabilite (72 ore), armonizzandoli con quanto già delineato per gli incidenti che abbiano un impatto sui beni ICT e sui loro 'beni contigui', ma anche e soprattutto di mappare e categorizzare a 'tempo di record' tutti gli eventi di sicurezza in relazione alla tassonomia prevista nell'allegato A della determina del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale (basata sulla classificazione del "Mitre Att&ck"), utilizzando la descrizione – abbastanza generica – fornita dal legislatore.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it