ANGOLO LEGALE

SICUREZZA INFORMATICA E DATA BREACH

Avv. Annalisa Callarelli

I fenomeni di data breach, la violazione della sicurezza informatica, sono in aumento. Oltre ai rischi dirompenti per l'azienda colpita, il titolare e il responsabile del trattamento dei dati possono incorrere in responsabilità civili, penali o amministrative

Secondo il report Clusit sulla sicurezza informatica 2021, la crescita degli attacchi hacker gravi di pubblico dominio nel triennio 2018-2020 è stata del 20% (da 1.552 a 1.871), a fronte di una crescita registrata nel precedente triennio 2015-2017 di "solo" +11% (da 873 a 1.127).
Security Operations Center (Soc) di Fastweb riferisce inoltre che, nel primo semestre del 2021, ci sarebbero stati 36 milioni di eventi malevoli "in forte aumento rispetto allo stesso periodo dell'anno precedente (registrando addirittura un +180%) e in cui il fenomeno più preoccupante è l'incremento dell'attività dei ransomware", anche conosciuti come "virus del riscatto", che attaccano i server delle aziende, criptando i dati e rendono quindi inaccessibili i file, se non previo pagamento di un ammontare a titolo, appunto, di riscatto.
Quanto sopra fa il paio con i recenti casi di data breach che hanno interessato grandi aziende italiane, pubbliche o private (la Regione Lazio, SIAE, San Carlo, Ferrari, Enel ecc.) e che hanno occupato le prime pagine di tutti i quotidiani.
Senza considerare gli episodi di PMI che non finiscono sui giornali, ma che si stanno moltiplicando.

COS'È IL DATA *BREACH*

Il data breach consiste in una violazione di sicurezza informatica, che può avvenire in modo accidentale (incidenti o

L'AUTORE

Avv. Annalisa Callarelli

Avvocato specializzato nel settore della contrattualistica d'impresa, nazionale e internazionale, con particolare riguardo a contratti di vendita/fornitura con o senza posa in opera, appalto e subappalto, distribuzione, agenzia e procacciamento d'affari, contratti con i consumatori. In tale contesto assiste committenti, fornitori e appaltatori sia in sede di redazione e negoziazione dei contratti sia durante l'esecuzione della commessa, gestendo anche eventuali reclami o contestazioni. Ha inoltre una significativa esperienza in sede di contenzioso, ove offre assistenza in eventuali controversie giudiziali oltre che per il recupero del credito.
È titolare dello studio legale SCLA con sede a Bologna.
a.callarelli@scla.it

errori umani o gusti) oppure illecita, ad esempio in caso di sottrazione dei dati da parte di un dipendente o, peggio ancora, a mezzo di attacchi hacker, che comporta la distruzione, la perdita, la modifica o la divulgazione di dati personali, anche sensibili, trattati dall'impresa colpita (dati dei dipendenti, dei clienti, dei fornitori ecc.).
I rischi per l'azienda, in caso di data breach, sono molteplici e di portata in alcuni casi dirompente.
In proposito, un ulteriore dato statistico parla da solo: il 60% delle piccole imprese fallisce entro sei mesi da un attacco informatico (National Cyber Security Alliance Stati Uniti).
In caso di attacco hacker o, comunque, di perdita o sottrazione dei dati, le aziende sono infatti spesso costrette a dover pagare ingenti somme per il loro rispristino.
Qualora, poi, la predetta perdita o sottrazione sia dovuta a un inadempimento dell'operatore rispetto ai propri obblighi in materia di trattamento dei dati personali, le conseguenze pregiudizievoli per il medesimo operatore e per il suo legale rappresentante aumentano in maniera esponenziale.

Come noto, ciascuna impresa risulta, in conformità alla normativa privacy, titolare del trattamento dei dati dalla medesima raccolti, gestiti e conservati; dati che possono essere anche sensibili (convinzioni religiose, origini razziali, religiose, politiche, appartenenza sindacale, sussidi ecc.).
In alcuni casi di collaborazione con soggetti terzi si potrà, al contempo, operare come responsabile del trattamento, ad esempio quando si utilizzano dati di clienti del terzo.
Poiché il fulcro del Reg. UE 679/16 (c.d. GDPR) è, appunto, la responsabilizzazione (traduzione di "accountability") del titolare e dei responsabili del trattamento, l'obiettivo di ciascuna impresa deve essere quello di porre in essere tutti i comportamenti proattivi a dimostrazione del concreto (e non meramente formale) rispetto del GDPR medesimo. Tanto vale anche rispetto alla sicurezza informatica.

COSA ACCADE IN CASO DI MANCATO ADEGUAMENTO AL GDPR
Nel caso in cui i dati personali non trovino adeguata protezione:
1) i soggetti interessati possono proporre un reclamo alle autorità competenti;
2) le autorità competenti possono svolgere controlli presso le imprese anche d'ufficio.

LA SICUREZZA INFORMATICA SI INTERSECA CON IL TEMA DEL TRATTAMENTO DATI. CON RISCHI PENALI E CIVILI

Le autorità preposte ai controlli sono il Garante per la protezione dei dati personali, la Polizia di Stato nonché la Guardia di Finanza - nucleo specializzato Privacy.
Nell'ambito degli accertamenti, i predetti organi hanno ampi poteri istruttori, potranno richiedere documentazione e svolgere tutti i controlli che riterranno utili.
Non solo.

LE RESPONSABILITÀ
Il titolare e il responsabile del trattamento potranno inoltre incorrere, a seconda dei casi, in gravi responsabilità civili, penali o amministrative.

Responsabilità civile
Secondo il GDPR (art. 82) chiunque subisca un danno materiale o immateriale causato da una violazione delle disposizioni del medesimo regolamento ha diritto a ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
In particolare:
- il titolare risponderà del danno cagionato nel caso in cui non riesca a dimostrare di aver predisposto tutte le misure idonee a prevenire il danno.
- l responsabile del trattamento risponderà se non ha adempiuto gli obblighi previsti dal GDPR o se non ha seguito le legittime istruzioni del titolare del trattamento.

In caso di data breach l'impresa non sarà, pertanto, ritenuta responsabile solo nel caso in cui riesca a dimostrare che l'evento dannoso non è alla medesima imputabile.

Responsabilità penale
Il c.d. Codice della Privacy (D.Lgs. 196/2003) prevede una serie di fattispecie di reato derivanti dall'inosservanza delle prescrizioni in materia di trattamento dati, come ad esempio: trattamento illecito dei dati (art. 167); comunicazione e diffusione illecita di dati personali (Art. 176 bis); acquisizione fraudolenta di dati personali (art. 167 ter); violazione delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (art. 171).

Responsabilità amministrativa
Il GDPR prevede inoltre delle gravose sanzioni amministrative (art. 83 GDPR) da infliggersi ai responsabili della violazione dei dati, che variano a seconda della natura e della durata della violazione, dell'oggetto o della finalità del trattamento e del carattere doloso o colposo della violazione, ma che possono arrivare fino a un importo di 20 milioni di euro o pari al 4% del fatturato annuo della società.

Quanto riportato deve rappresentare uno stimolo per le imprese affinché comprendano l'importanza di operare il più possibile in compliance con la normativa esistente in tema di privacy, adottando tutti i necessari presidi (inclusi quelli volti a garantire la sicurezza informatica) ed effettuando controlli periodici e formazione sul personale, affinché le predette misure vengano effettivamente rispettate e mantenute nel tempo. ■