filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Data breach: quanto mi costi

09 Febbraio 2021
Roberto Louhichi, Marco Dettori

Il report nel data breach

IBM security, con la recente pubblicazione del Cost of Data Breach Report 2020 – ricerca condotta dal Ponemon Institute su un campione di 524 organizzazioni in 17 Paesi (il 4% italiane) – ha analizzato i **costi derivanti dai data breach che, tra l'agosto 2019 e l'aprile 2020, hanno interessato le organizzazioni**.

Il report ha prodotto statistiche che, soprattutto alla luce di avvenimenti recenti (vedi il data breach che ha coinvolto Ho.Mobile), meritano di essere richiamate.

Considerazioni preliminari sul data breach

Volendo anticipare gli elementi rilevanti che emergono dai dati di seguito riportati, è evidente come la violazione dei dati personali sia un **aspetto sempre più cruciale nelle dinamiche aziendali**, al quale le imprese, siano esse grandi, medie o piccole, iniziano ad essere sempre più sensibili, anche e soprattutto per i **costi**, in termini **economici** e **reputazionali**, che la violazione comporta.

È in questo clima che si inserisce anche il nuovo servizio lanciato dal Garante privacy per gli adempimenti Data Breach, volto ad istruire e supportare titolari e responsabili del trattamento nell'individuazione e nella gestione di una violazione di dati.

Al di là di tutte le linee guida, statistiche e servizi istituzionali sulla materia, resta il fatto che la vera "arma in più" nelle mani dell'imprenditore non potrà che essere (come sempre) la **prevenzione**, da raggiungersi mediante l'adozione di specifiche procedure, costruite sulla singola realtà aziendale considerata, per la gestione di potenziali violazioni. D'altronde, **prevenire è meglio (e costa meno) che curare**!

I dati sul data breach

Il primo macro-dato da considerarsi riguarda il fatto che, nonostante un lieve decremento dell'1,5% rispetto al 2019, il **costo medio totale di una violazione dei dati continua ad assestarsi intono a 4 milioni di dollari** (per la precisione, 3.86 milioni). Importante sottolineare come la serie storica del report dei sette anni precedenti mostri un **incremento totale del 10%** di tale costo dal 2014 ad oggi.

In questo scenario, l'Italia si colloca al di sotto della media totale, con un costo medio totale pari a 3,19 milioni. Il dato non deve però autorizzare a sottostimare il problema poiché, come ha ricordato il Garante nella propria Relazione Annuale 2019, le **violazioni di dati personali notificate** all'Autorità nell'anno 2019 sono state **circa 4 al giorno**, per un totale di 1443 notifiche, rispetto alle 650 dell'anno precedente.

Quali i **fattori incidenti sull'ammontare del costo**? La risposta è fornita dalla **Figura 26** del report che fotografa l'impatto di 25 fattori chiave, sia in funzione di mitigazione che di amplificazione dei costi.

Tra i **fattori di mitigazione** vengono ricordati un piano di risposta agli incidenti e della gestione della continuità aziendale, la formazione dei dipendenti e la crittografia completa mentre hanno avuto un ruolo di **amplificazione del costo medio** lo smart working, la migrazione a sistemi in cloud e la complessità del sistema di sicurezza, specialmente perché accompagnata dalla mancanza di competenze interne.

Importante considerare anche quanto emerge dalla **Figura 29**, il cui istogramma mostra come le organizzazioni che hanno formato un **team di risposta agli incidenti** e che hanno sottoposto ampiamente a test il loro piano di risposta agli incidenti, hanno registrato un costo medio per una violazione dei dati pari a 3,29 milioni di dollari. **Al contrario, le organizzazioni che non hanno intrapreso nessuna di queste azioni, hanno registrato un costo medio totale pari a 5,29 milioni di dollari, una differenza di 2 milioni di dollari.**

Veniamo ora alle **cause delle violazioni**, rintracciate:

1. nell'errore umano per il 23% dei casi;
2. in un problema tecnico per il 25%; e
3. in un attacco malevolo per il restante 52%.

Con specifico riferimento alla parte di campione italiano, le percentuali restano pressochè immutate rispetto alla media generale, vedendosi solo un modesto incremento percentuale della voce "errore umano", che sale al 29%.

> **Di centrale interesse per le imprese il dato relativo al tipo di informazioni coinvolte nelle violazioni registrate. Infatti, ben nell'80% dei casi, la violazione interessa informazioni che rendono identificabili i clienti dell'impresa colpita.**

La percentuale è impressionante se paragonata a quella relativa alle altre categorie di dati. Le violazioni che hanno interessato altre tipologie di informazioni sono infatti pari al:

1. 32% dei casi per dati relativi alle **proprietà intellettuali**:
2. 24% dei casi per **dati anonimizzati dei clienti**:
3. 21% dei casi per informazioni di **identificabilità dei dipendenti** dell'impresa colpita.

In ultimo, tristemente sorprendente anche la statistica relativa ai **tempi per l'identificazione della violazione**, i quali si assestano, in conformità con i report degli anni antecedenti, in un lasso di tempo pari a **280 giorni**. La significatività di quest'ultimo è tanto più evidente se si richiama alla memoria il ben più breve intervallo temporale di 72 ore dalla presa coscienza della violazione che il GDPR concede al titolare per la notifica della stessa all'Autorità.

Ai dati del report appena analizzato possono accompagnarsi le risultanze del Allianz Risk Barometer 2021, studio dell'omonimo gruppo assicurativo che raccoglie le statistiche di oltre 2.700 esperti del risk management di 92 differenti Paesi, il quale colloca al primo posto della classifica dei rischi percepiti dalle imprese italiane i cyber-incidenti, quasi sempre coincidenti nella pratica con violazioni di dati personali, a discapito delle interruzioni di produzioni e della pandemia Covid-19 , che si piazzano rispettivamente al secondo e al terzo posto.

TAG: *data breach, violazione della privacy, clientela*
