ATTUALITÀ

Data breach: se lo conosci lo eviti? Non sempre

di **Fondazione AIDR** · 7 ottobre 2021, 00:01

di Federica De Stefani, avvocato e responsabile Aidr Regione Lombardia

Sentiamo (sempre più) spesso parlare di data breach e la richiesta che ne deriva, quasi naturalmente, riguarda la possibilità di evitarlo o, quanto meno, di contenerlo. La risposta, purtroppo, è negativa, non è possibile evitare un data breach poiché il "rischio zero" non esiste.

È certo possibile limitare le occasioni per cadere nella "trappola" dell'incidente informatico ed è altrettanto possibile limitare le conseguenze che ne derivano, ma questo è un discorso diverso. Per comprendere il fenomeno del data breach, molto spesso identificato esclusivamente con un attacco hacker, è necessario comprendere di cosa si tratti.

Che cos'è il data breach

Con il termine "data breach" si indica una violazione di sicurezza che comporta – accidentalmente o in modo illecito – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Come si vede un data breach può comportare la perdita di dati che non derivano da un attacco hacker, ma può derivare anche dalla perdita della diponibilità degli stessi, così come avviene nell'ipotesi in cui ci sia, per esempio, un furto di un device.

Quando si verifica il data breach.

Le tipologie di data breach sono piuttosto varie e quindi, a mero titolo esemplificativo, possiamo indicare come rientranti nella casistica l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati, il furto o la perdita di dispositivi informatici contenenti dati personali, l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc, la deliberata alterazione di dati personali, la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità, la divulgazione non autorizzata dei dati personali.

Dove si può verificare un data breach

Un data breach, inteso, come detto, come violazione che incide sulla disponibilità, integrità e riservatezza dei dati, può riguardare qualsiasi ambito, sia fisico sia digitale. Si pensi, per esempio, alla distruzione di un archivio cartaceo, o al furto di documenti o, ancora, alla manomissione e all'alterazione degli stessi.

*I s***oggetti interessati da un data breach**

Un data breach rappresenta un evento che, a seconda delle caratteristiche specifiche del singolo caso, può coinvolegere soggetti diversi.

Il titolare del trattamento è colui che, a norma dell'art. 33 GDPR, si deve attivare senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, per notificare la violazione al Garante per la protezione dei dati personali, salva l'ipotesi in cui sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Al contrario, qualora la violazione presenti rischi elevati per i diritti e le libertà delle persone fisiche, il titolare, sempre senza ritardo, deve anche provvedere a informare gli interessati. Nel caso in cui sia stato nominato un Responsabile del trattamento quando questi venga a conoscenza di una violazione, è tenuto a informare tempestivamente il titolare in modo che possa attivarsi.

Le cause di un data breach

Come detto il data breach è violazione di sicurezza che comporta – accidentalmente o in modo illecito – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati trattati e questo significa, nella pratica, che le misure di sicurezza adottate non hanno funzionato. Non bisogna tuttavia cadere nell'errore di associare automaticamente il data breach all'adeguatezza delle misure adottate per farne derivare sic et simplicter una responsabilità (oggettiva) del titolare del trattamento. La questione è ben più complessa, posto che il GDPR non prevede una responsabilità di questo genere in capo al titolare, ma prevede la possibilità per lo stesso di dimostrare di aver fatto tutto quanto in suo potere per proteggere i dati trattati.

Il fattore umano e l'importanza della formazione

Se da un lato l'evento data breach non può essere totalmente eliminato, in quanto, come anticipato, il rischio zero non esiste, dall'altro è necessario interrogarsi sulle strategie e sulle misure da adottare per limitare al massimo il rischio.

Al di là delle misure tecniche e organizzative “adeguate”, così nella terminologia del Regolamento europeo, una parte importante della prevenzione è rappresentata dalla formazione del personale. Ad oggi il fattore umano rappresenta ancora un tallone d’Achille piuttosto diffuso in moltissime realtà, anche strutturate e di grandi dimensioni. La mancanza di adeguata e specifica formazione, l’assenza di policy adeguate sull’utilizzo degli strumenti informatici e sulle procedure, sono ancora oggi cause piuttosto diffuse di data breach.

Il nodo della questione è rappresentato non solo dalla tipologia di protezione adottata, ma anche dalle modalità di applicazione delle stesse, dall’aggiornamento e dalla formazione specifica data ai soggetti che trattano i dati.

Non si deve infatti dimenticare che la compliance deve svolgersi a più livelli, deve essere trasversale e non può riguardare solo il lato tecnico e la cybersecurity, ma anche l’aspetto organizzativo e procedurale per quanto attiene al c.d. fattore umano.

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2021/10/07/data-breach-se-lo-conosci-lo-eviti-non-sempre/

© 2026 Istituzioni24