

Profili di responsabilità nei data breach



Nel contesto digitale odierno, all'interno della grande categoria dei **security breach**, le violazioni della sicurezza dei dati, comunemente note come "**data breach**" rappresentano una minaccia significativa per le organizzazioni o società di ogni dimensione e grado. Questi incidenti non solo compromettono la riservatezza, l'integrità e la disponibilità delle informazioni, ma sollevano anche questioni critiche riguardo ai profili di responsabilità. Comprendere chi è responsabile in caso di una violazione dei dati è fondamentale per garantire una gestione efficace degli attacchi e per conformarsi alle normative vigenti.

Cos'è il data breach all'interno del Gdpr

Il **Data Breach**, noto in italiano come **violazione dei dati personali**, è infatti una tipologia di security breach e si riferisce più specificatamente a un incidente di sicurezza che, accidentalmente o in modo illecito, provoca la distruzione, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trattati, sia durante la trasmissione che nella fase di archiviazione o gestione.

I data breach, possono verificarsi a causa di vari tipologie di attacchi informatici, come: hacking, insider leaks, frodi con carte di pagamento, attacchi malware, perdita o furto di dispositivi fisici, divulgazione non intenzionale o altre ragioni sconosciute.

Le tipologie di dati rubati a seguito di un data breach

possono includere: numeri di carte di credito, dati dei clienti, segreti commerciali, cartelle cliniche, informazioni finanziarie, informazioni di identificazione personale (PII) o questioni di sicurezza nazionale. Le violazioni di dati possono colpire aziende di ogni dimensione, settore e area geografica e si verificano con una frequenza allarmante.

I data breach si suddividono sostanzialmente in tre principali categorie, in base al tipo di criticità che colpisce i dati personali: **confidentiality breach**, **availability breach** e **integrity breach**.

Il **confidentiality breach** riguarda la violazione della riservatezza. Questo avviene quando i dati personali vengono divulgati senza autorizzazione, sia intenzionalmente che accidentalmente.

L'**availability breach** si riferisce alla compromissione della disponibilità dei dati. In questo caso, le informazioni personali vengono perse o distrutte senza il consenso dell'utente, anche in modo involontario.

L'**integrity breach** indica una violazione dell'integrità dei dati. Ciò accade quando le informazioni personali vengono modificate senza autorizzazione, indipendentemente dal fatto che l'alterazione sia intenzionale o accidentale.

Tutte queste violazioni compromettono la sicurezza informatica degli utenti e possono avere conseguenze significative. Inoltre, la perdita di riservatezza può esporre dati sensibili, inclusi quelli protetti dal segreto professionale.

In conformità al **GDPR (Regolamento Generale sulla Protezione dei Dati, Regolamento UE 2016/679)**, eventuali violazioni devono essere notificate **all'autorità di controllo competente** nella singola nazione di riferimento, senza **ingiustificato ritardo** e, se possibile, **entro 72 ore** dalla scoperta dell'incidente, secondo **l'articolo 33** dello stesso, a meno che non sia dimostrato che il rischio per i diritti e le libertà

delle persone fisiche sia irrilevante. Qualora la comunicazione avvenga oltre il termine previsto, è necessario fornire una giustificazione per il ritardo.

L'**articolo 34** invece, del regolamento GDPR disciplina la parte della comunicazione della violazione dei dati personali all'interessato, prevedendo che:

La comunicazione non è necessaria se:

- Sono state adottate misure di protezione adeguate (es. crittografia).
- Sono state prese azioni per eliminare il rischio.
- La comunicazione richiederebbe sforzi sproporzionati (in tal caso, si può optare per una comunicazione pubblica).

Paradigmi di attribuzione della responsabilità nei data breach

La violazione delle disposizioni previste dal GDPR può comportare conseguenze sia materiali che immateriali. Tali effetti possono variare da disagi minori, come la necessità di ripristinare un dato erroneamente cancellato, fino a situazioni estremamente gravi, come la compromissione della salute di una persona a causa della modifica non autorizzata di dati sanitari prima di un intervento medico. In questi casi, l'interessato ha diritto a un risarcimento da parte del Titolare del trattamento responsabile del danno, a meno che quest'ultimo non dimostri di non avere alcuna colpa nell'accaduto.

Se più soggetti sono coinvolti nel trattamento dei dati, sia con la stessa qualifica (ad esempio, Contitolari o più Responsabili del trattamento) che con ruoli diversi (ad esempio, un Titolare e un Responsabile), la responsabilità sarà solidale. Questo significa che chi ha subito il danno potrà chiedere l'intero risarcimento a uno qualsiasi dei

soggetti coinvolti, che avrà poi diritto di rivalersi sugli altri in base alla loro quota di responsabilità.

In altre parole, all'interno del rapporto tra i vari soggetti coinvolti, ciascuno sarà chiamato a rispondere solo nella misura della propria effettiva responsabilità.

Il risarcimento del danno avviene previa dimostrazione e quantificazione in sede civile, ed è distinto dalle eventuali sanzioni amministrative imposte dal Garante per la protezione dei dati personali e dalle possibili condanne penali previste dalla normativa nazionale. Poiché il diritto penale è di competenza degli Stati membri, il legislatore europeo non può prevedere direttamente sanzioni di questo tipo, ma può lasciare agli Stati la facoltà di introdurle, come stabilito dall'articolo 25, comma 2, della Costituzione italiana e dall'articolo 83 del Trattato sul funzionamento dell'Unione Europea. Questo sistema mira a garantire una tutela il più possibile completa contro le violazioni dei dati personali.

La responsabilità può essere suddivisa riassumendo quindi in diverse categorie, tra cui:

- **Responsabilità legale:** Riguarda l'obbligo di conformarsi alle leggi e alle normative sulla protezione dei dati, come il Regolamento Generale sulla Protezione dei Dati (GDPR) nell'Unione Europea. Le organizzazioni sono tenute a implementare misure di sicurezza adeguate a proteggere i dati personali e possono essere ritenute legalmente responsabili in caso di mancata conformità. Rientra in questa categoria la **responsabilità civile** in quanto deriva dall'obbligo di conformarsi alle normative sulla protezione dei dati, come il **GDPR**. Se un'organizzazione non adotta misure adeguate a proteggere i dati personali e questo causa un danno agli interessati, questa può essere chiamata a risponderne in sede civile, con conseguente obbligo di risarcimento.

Il danneggiato potrà eventualmente agire per chiedere il risarcimento del danno, che potrà essere sia patrimoniale che non patrimoniale, nei confronti dei titolari del trattamento, i contitolari, i responsabili del trattamento dei dati personali. Tuttavia, si sottolinea che li stessi soggetti vanno esonerati da tale responsabilità se dimostrano che l'evento dannoso non gli è in alcun modo imputabile.

- **Responsabilità contrattuale:** si riferisce agli obblighi definiti nei contratti con terze parti, come fornitori o partner. In caso di violazione dei dati derivante da una terza parte, l'organizzazione potrebbe essere ritenuta responsabile se non ha garantito che il partner rispettasse gli standard di sicurezza concordati. La responsabilità civile discende quindi anche dalla responsabilità contrattuale, tutte le volte in cui un'organizzazione ha stipulato accordi con terze parti (come fornitori di servizi IT o cloud) e una violazione dei dati avviene per negligenza o mancato rispetto degli standard di sicurezza previsti nel contratto.
- **Responsabilità professionale:** coinvolge i singoli dipendenti o professionisti che, attraverso negligenza o comportamento doloso, causano o contribuiscono a una violazione dei dati. In tali casi, sia l'individuo che l'azienda possono essere ritenuti responsabili.
- **Responsabilità etica:** oltre agli obblighi legali e contrattuali, le organizzazioni hanno una responsabilità etica nei confronti dei loro clienti e stakeholder di proteggere le informazioni sensibili e di agire con trasparenza in caso di violazione.

L'attribuzione della responsabilità va detto, dipende spesso dalla natura della violazione, dalle circostanze specifiche e dalle misure preventive adottate dall'organizzazione.

Metriche sanzionatorie nella non-compliance

La non conformità alle normative sulla protezione dei dati può

comportare sanzioni pecuniarie amministrative notevoli per le organizzazioni. La fonte giuridica su cui si basano, è l'art. 83 del GDPR. È compito delle autorità di controllo, infatti, fare in modo che le **sanzioni GDPR** siano effettive, proporzionate e dissuasive. Le metriche sanzionatorie variano in base alla giurisdizione e alla gravità della violazione. Ad esempio, secondo il GDPR, le multe possono raggiungere fino al 4% del fatturato annuo globale dell'azienda o 20 milioni di euro, a seconda di quale sia l'importo maggiore.

Un'organizzazione che riceve una **sanzione per violazione del GDPR** non subisce solo un **danno economico significativo**, ma rischia anche un impatto negativo sulla propria **reputazione** e sulla **fiducia** da parte degli stakeholder.

Le ripercussioni finanziarie possono estendersi nel tempo, influenzando il **fatturato** e limitando le possibilità di crescita e di sviluppo di nuove opportunità di business.

Negli ultimi 25 anni, la **protezione dei dati personali** è diventata sempre più centrale sia in Italia che a livello internazionale. Da semplice tutela di un diritto fondamentale, si è evoluta fino a diventare un elemento strategico essenziale per affrontare le sfide tecnologiche attuali e future.

Le autorità di controllo, (per l'Italia, **il Garante per la protezione dei dati personali**) dispongono di poteri correttivi in grado di incidere sulle attività di titolari e responsabili, come avvertimenti, ammonimenti, limitazioni e divieti del trattamento o sospensione di flussi extraeuropei.

Le sanzioni previste dal GDPR vengono applicate caso per caso, tenendo conto delle specifiche circostanze dell'infrazione. Inoltre, possono essere combinate con altri provvedimenti correttivi adottati dall'autorità di controllo, come già illustrato in precedenza.

Nel determinare se imporre una sanzione pecuniaria e nel

definirne l'importo, vengono valutati diversi elementi, tra cui:

- **Natura e gravità della violazione:** Include il tipo di dati compromessi, il numero di persone coinvolte e l'entità del danno causato.
- **Durata della violazione:** Il periodo durante il quale la violazione è rimasta non rilevata o non affrontata può influire sull'entità della sanzione.
- **Misure preventive adottate:** L'implementazione di misure di sicurezza adeguate prima della violazione può attenuare la condanna.
- **Cooperazione con le autorità:** Una collaborazione proattiva con le autorità di controllo durante le indagini può influire positivamente sulla determinazione dei provvedimenti.
- **Precedenti violazioni:** Un history di non conformità può portare a pene più severe.

È quindi essenziale che le organizzazioni comprendano queste metriche e adottino misure proattive per garantire la conformità e la tempestività, riducendo così il rischio di sanzioni onerose.

Protocolli di incident response e rimedi giuridici

Una risposta tempestiva ed efficace a una violazione dei dati è cruciale per mitigare i danni e per adempiere agli obblighi legali. La **priorità principale** per un'organizzazione in caso di violazione dei dati è quella di **bloccare gli effetti negativi** dell'incidente. Questo intervento può essere **temporaneo**, attraverso soluzioni provvisorie (**workaround**), oppure **definitivo**, eliminando le cause che hanno generato il problema.

Allo stesso tempo, o comunque nel minor tempo possibile, è fondamentale procedere al **ripristino dei dati personali compromessi**.

Le modalità di intervento variano in base al tipo di impatto subito dai dati, che può riguardare la loro **riservatezza, integrità o disponibilità**. Ad esempio, se un guasto tecnico provoca la **corruzione dei dati**, sarà necessario ricorrere al **ripristino da backup**.

Nel caso di una violazione della **riservatezza**, invece, le possibilità di contenere il danno sono più limitate. Tuttavia, esistono strumenti in grado di recuperare, almeno in parte, dati rubati e diffusi, ad esempio nel **dark web**.

I protocolli di incident response dovrebbero includere:

1. **Identificazione dell'Incidente:** Rilevare rapidamente la violazione attraverso sistemi di monitoraggio e segnalazione.
2. **Contenimento:** Isolare i sistemi compromessi per prevenire ulteriori danni.
3. **Valutazione dell'Impatto:** Determinare l'entità della violazione, inclusi i dati coinvolti e le potenziali conseguenze.
4. **Notifica:** Informare le autorità competenti e, se necessario, le persone interessate entro i termini stabiliti dalle normative.
5. **Remediation:** Implementare misure correttive per risolvere le vulnerabilità e prevenire future violazioni.
6. **Documentazione:** registrare dettagliatamente tutte le azioni intraprese durante la gestione dell'incidente per scopi giuridici e di audit.

Oltre ai protocolli di risposta, le organizzazioni e/o le aziende devono essere consapevoli dei rimedi giuridici disponibili in caso di violazione dei dati. Questi già affrontati sopra, possono includere:

- **Azioni legali:** Le persone i cui dati sono stati compromessi possono intentare cause legali per danni,

come abbiamo visto sopra.

- **Sanzioni amministrative:** Le autorità di controllo possono infliggere multe e altri provvedimenti per non conformità.
- **Obblighi di risarcimento:** Le organizzazioni potrebbero essere tenute a risarcire le persone per le perdite subite a causa della violazione.

Digital Forensics nei procedimenti legali

La **digital forensics**, o informatica forense, svolge un ruolo cruciale nei procedimenti legali legati ai data breach. Questa disciplina si occupa dell'analisi, della raccolta e della preservazione delle prove digitali per stabilire la dinamica di una violazione dei dati e attribuire le responsabilità.

Le indagini di digital forensics seguono un processo formale e una rigida catena di custodia per tracciare la raccolta e la gestione delle evidenze. Questo sistema garantisce l'integrità delle stesse, consentendo agli investigatori di dimostrare che non sono state alterate. Di conseguenza, le prove forensi digitali possono essere utilizzate ufficialmente nelle richieste di risarcimento assicurativo o verifiche di conformità normativa.

Fasi del processo di digital forensics

L'analisi forense segue un flusso rigoroso per garantire l'integrità delle prove, la loro ammissibilità in sede legale e prevede:

1. Identificazione delle prove

Gli esperti di digital forensics individuano dispositivi e sistemi compromessi per raccogliere informazioni utili. Questi possono includere server, database, log di accesso e dispositivi mobili.

2. Acquisizione delle prove

Le evidenze digitali vengono duplicate attraverso tecniche di **imaging forense** per garantire che

l'originale rimanga inalterato.

3. Analisi e correlazione dei dati

Gli investigatori esaminano file, registri di sistema, metadati e tracce digitali lasciate dagli attaccanti per ricostruire l'attacco. Tecniche avanzate come **reverse engineering** e **memory forensics** vengono utilizzate per identificare malware e vettori d'attacco.

4. Documentazione e reporting

Ogni fase dell'analisi viene documentata con report dettagliati che possono essere utilizzati come prova in tribunale. Le relazioni devono essere comprensibili sia per esperti tecnici che per giudici e avvocati.

5. Testimonianza forense

Gli specialisti possono essere chiamati a testimoniare in tribunale per spiegare le loro scoperte e validare l'autenticità delle prove raccolte.

La digital forensics e la risposta agli incidenti (**DFIR**) uniscono due ambiti della cybersecurity per rendere più efficiente la gestione delle minacce, garantendo al contempo la conservazione delle prove utili contro i cybercriminali.

La digital forensics, si concentra sull'analisi delle minacce informatiche per raccogliere evidenze digitali a fini legali, e la risposta agli incidenti, che riguarda il rilevamento e la neutralizzazione degli attacchi in corso. L'unione, come detto, di questi due approcci consente ai team di sicurezza di reagire più rapidamente alle minacce, evitando che prove cruciali vadano perse nel processo di mitigazione.

In particolare, possiamo riassumere che le funzioni e gli scopi perseguiti sono:

- **Attribuzione della colpa**

La digital forensics aiuta a determinare se un data breach è stato causato da negligenza aziendale, attacco informatico esterno o attività dolosa interna.

- **Conformità normativa**

I risultati delle indagini forensi possono essere utilizzati per dimostrare la conformità (o la non conformità) alle normative sulla protezione dei dati, come il GDPR o il NIST Cybersecurity Framework.

- **Supporto alle indagini penali e civili**

In caso di procedimenti giudiziari, le prove digitali possono essere utilizzate per perseguire criminali informatici o per difendersi da richieste di risarcimento danni.

L'informatica forense è quindi essenziale e fondamentale per garantire un'efficace gestione dei data breach, proteggere i diritti delle parti coinvolte e assicurare la giustizia.

Conclusioni

La gestione della responsabilità nei casi di **data breach** è un tema di cruciale importanza per le organizzazioni di ogni settore. La crescente digitalizzazione e l'aumento delle minacce informatiche rendono essenziale un approccio strutturato e conforme alle normative per prevenire, gestire e mitigare gli effetti delle violazioni dei dati.

L'attribuzione della responsabilità dipende da molteplici fattori, tra cui il rispetto delle normative vigenti (come il **GDPR**), le clausole contrattuali, la condotta dei dipendenti e la governance aziendale. Le **metriche sanzionatorie** dimostrano che la non-compliance può avere conseguenze economiche e reputazionali severe, incentivando le aziende a implementare **robusti protocolli di sicurezza**.

L'adozione di un efficace **incident response plan** è invece fondamentale per minimizzare i danni in caso di attacco e per adempiere agli obblighi normativi, tra cui la notifica tempestiva alle autorità competenti. Inoltre, la **digital forensics** svolge un ruolo determinante nel supporto alle indagini legali, consentendo di raccogliere prove utili per l'attribuzione delle responsabilità e l'eventuale avvio di

azioni giuridiche.

Per mitigare i rischi e garantire la sicurezza dei dati, le aziende devono investire in tecnologie avanzate, formazione del personale e strategie di **cyber resilience**. Solo un approccio proattivo e multidisciplinare può ridurre l'esposizione alle minacce e garantire una gestione efficace delle violazioni, proteggendo sia l'organizzazione che i suoi stakeholder.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/responsabilita-da-ta-breach/>