# Data Breach o Data leak: qual è la differenza?

Non è molto facile oggi tenere traccia di tutte le notizie che riguardano le fughe di dati (Data leak) o le brecce nei database (Data Breach) delle grandi compagnie o degli istituiti di credito, anche considerando che il loro numero è in esponenziale aumento (+54% su base annua secondo alcune recenti stime).

In questo turbinio d’informazioni capita che nella stampa più generalista i termini Data Breach e Data Leak vengano usati come sinonimo l’uno dell’altro. Ma, in realtà, ci sono delle differenze tra i due fenomeni.

## Questione di parametri

Perché fare questa distinzione innanzitutto? In fondo in entrambi in casi sembra scontato che la conseguenza sia comunque l’esposizione di dati sensibili o possibili frodi con furto d’identità.

Curiosamente, però, prendendo in analisi il periodo di 12 mesi che va dal luglio 2017 a luglio 2018 possiamo tracciare un pattern abbastanza netto: un terzo degli incidenti di Cyber Security rilevati sono stati Data Leak, mentre il 40% erano costituiti da Data Breach. Una dicotomia abbastanza netta tra Breach e Leak tale da giustificare una discussione sulle due modalità.

Per comprendere al meglio cosa distingue un Data leak da un Data Breach vediamo cosa distingue il secondo.

In sintesi, si tratta di violazione di sistemi portate avanti da un Criminal hacker (o da un gruppo organizzato) al fine di estrarre informazioni, causare disservizio o semplicemente danno economico. Di contro i Data leak sono incidenti informatici in cui le informazioni sensibili vengono esposte per errore a causa di vulnerabilità, errore umano o errati processi aziendali in materia di protezione e conservazione del dato.

## Una definizione incerta

A questo punto è giusto anche osservare come non esista una definizione ufficiale e universale per il termine Data leak. Alcune fonti scartano a prescindere la parola Leak e parlano di Data Breach accidentale. A volte le perdite possono anche essere semplicemente indicate come “esposizione involontaria di dati”.

Nonostante l'uso variegato del linguaggio, la deduzione più importante da fare è proprio sulla differenza tra gli incidenti che comportano minacce attive che compromettono un sistema e gli incidenti in cui i dati sono stati involontariamente resi pubblici a seguito di un incidente o di un errore.

## Perché questa distinzione è importante?

Anche se in qualità di consumer non possiamo prevenire violazioni o fughe di informazioni, comprendere la differenza ci insegna le seguenti lezioni. Le perdite di dati sono talvolta il risultato di come sono progettati i servizi.

Alcuni Data leak che hanno fatto notizia, come Exactis o Panera, sono il risultato di un problema diffuso che si traduce in database mal configurati che a volte sono facilmente ricercabili su Google o attraverso altri strumenti estremamente accessibili.

In altri casi, però, le perdite sono il risultato diretto di come un servizio è stato progettato.

Basti a pensare ai casi di Facebook e di Polar Fitness. Nel primo caso sembra proprio che le incoerenze nelle politiche di sviluppo di Facebook abbiano permesso a società dubbie come Cambridge Analytica di scivolare attraverso le crepe. Non è fuori dal mondo speculare che sia Cambridge Analytica che gli scandali del Nametest siano solo la punta dell'iceberg. In altre parole, questi sono solo gli abusi di cui siamo a conoscenza.

Se in passato la piattaforma social era così aperta e indifesa come questi casi arcinoti ci portano a credere, allora ci sono probabilmente decine di altre applicazioni che per progettazione hanno avuto accesso a più dati del necessario per funzionare.

## I Data Leak potrebbero non sempre essere divulgati

In tutti gli Stati, per legge, le aziende devono divulgare le violazioni dei dati; tuttavia, quando si tratta di Data Leak, queste leggi possono essere difficili da applicare. In primo luogo, la divulgazione richiede il riconoscimento e la consapevolezza di un problema, ma in molti casi, la conoscenza delle fughe di dati proviene da professionisti della sicurezza di terze parti e talvolta da informatori (come nel caso di Cambridge Analytica).

Inoltre, in un piccolo numero di casi, come nel caso della perdita che ha colpito l’americana Polar Fitness, i ricercatori di Cyber Security hanno rilevato la presenza di vulnerabilità sfruttabili su una piattaforma, ma poiché non è possibile dimostrare l’effettiva perdita di dati e l'azienda non ha trattato l'incidente come una violazione.

Per questo motivo, ci sono forse decine di Data Leak che regolarmente passano in sordina.

Questo, naturalmente, mette i consumatori in una posizione in cui non sono in grado di ricevere un risarcimento o anche solo di adottare misure per proteggersi dai danni, motivo per cui gli esperti suggeriscono spesso di presumere che i nostri dati siano già stati compromessi anche se non abbiamo mai ricevuto una notifica di violazione.

## Come considerare la gravità delle due

Dovreste reagire al Data Leak con la stessa preoccupazione di un Data Breach. Anche se le aziende rassicurano che i dati esposti non sono stati compromessi.

In molti casi, il difetto o la vulnerabilità che causa la perdita è presente per un periodo di tempo indeterminato e strumenti come Shodan rendono estremamente facile la ricerca di reti esposte.

Poiché tali strumenti esistono, è difficile credere che i sistemi non siano già stati compromessi molto prima che gli sviluppatori vengano a conoscenza del problema.

Siate attenti a tutti i siti web a cui aderite, specialmente i social network che usano il vostro vero nome o dati di localizzazione in tempo reale.

Da Fitbit a Facebook, servizi come questi hanno l'incentivo a inghiottire tutti i dati possibili su di voi e, quindi, potrebbero aumentare involontariamente o involontariamente il rischio di una violazione o perdita.

Infine, l'incertezza che circonda le Data Leak evidenzia la necessità di proattività. Uno dei modi per essere proattivi è investire nella protezione dei furti di identità, che controlla il web (compresi i siti del mercato nero) per l'utilizzo delle vostre informazioni personali.

Anche se non è possibile prevenire perdite, violazioni di dati o furti di identità, la conoscenza degli incidenti di sicurezza informatica può aiutare a reagire correttamente alle minacce del mondo di oggi. Continuate a leggere il nostro blog sulla violazione dei dati per essere sempre al passo con le storie che contano.

## Come reagire, lato business

Ovviamente se lato utente ci sono particolari accortezze da rispettare, lato business, ogni incidente informatico, che sia Data breach o Data leak deve essere gestito nel modo più efficiente e accurato per evitare ulteriori perdite e rispettare quanto normato nel GDPR.

Per questo è fondamentale approntare un Cyber Data Incident Response Pack, in grado di:

* Gestire l’incident e supportare l’azienda nelle attività;
* Analizzare la natura della violazione;
* Identificare le evidenze, prove e informazioni tecniche;
* Determinare la tipologia dei dati compromessi;
* Stabilire quali dati sono stati compromessi:
* Formalizzare lo stato delle misure di sicurezza in essere;
* Predisporre in piano di Remediation.

Nello specifico il servizio di Cyber Data Breach Incident Response permette di essere compliant alla normativa vigente di Data Protection normata, appunto, nel GDPR.

L’attività di Cyber Security Framework Checkup è strutturata solamente in 5 fasi:

* **Cyber Security Investigation:** In questa fase avviene l’analisi dell’attacco, dei target vittima e dei dati compromessi;
* **Forensic Investigation:** Cristallizza legalmente le evidenze e le prove;
* **ICT Integrity Checkup:** Verifica l’integrità dell’infrastruttura;
* **Vulnerability Checkup:** Verifica le eventuali vulnerabilità dell’infrastruttura;
* **Reporting/Remediation Plan:** Documentazione per la notifica al Garante e Remediation Plan.

## Il pericolo in agguato, il fake data breach

## Ma se non bastassero i problemi creati da Data Leak e Data Breach, si sta palesando un nuovo spauracchio per i business, particolarmente per quelli quotati in borsa: il Fake Data Breach.

## Non è passato molto tempo dal caso di Nexi, dove quasi 18mila records erano stati pubblicati sul sito Pastebin e attribuiti all’istituto finanziario Italiano.

## Ma, a prescindere dalle evidenze circostanziali, i dati pubblicati potrebbero essere stati usati per arrecare danno a qualsiasi tipo di azienda, non essendo sempre ricollegabili a Nexi.

## In quel caso, anche se il presunto bersaglio al tempo ha rassicurato “il mondo” negando serenamente l’accadimento (un approccio alla gestione delle cosidette “Cyber Crisis” assolutamente errato, che causa piu’ danni che soluzioni), chi non è atto a cimentarsi nel mondo della Cyber Security, naturalmente, stenta a credere a chi è sotto i riflettori.

## Il pericolo è che questo sia solo il primo esempio di una nuova strategia diffamatoria che potrebbe diventare standard: utilizzare dati non descrittivi per screditare i propri competitor o, perché no, i propri avversari politici agli occhi del pubblico, così come per svolgere azioni illegali proprie del c.d. “Insider Trading”, ma senza la necessità di avere, appunto, insider all’interno dell’organizzazione vittima

## Il caso ha però aperto anche un altro filone di criticità, se vogliamo più ‘alto’, ovvero la mancanza di azione ed autorevolezza da parte di quegli organismi che dovrebbero tutelare le parti coinvolte – sia consumer sia azienda – in casi come questo.

## Se il data breach c’è stato, non mancano gli strumenti – GDPR docet –per sanzionare adeguatamente chi non ha adottato le misure di sicurezza e per attivare ogni utile procedura di emergenza a salvaguardia dei cittadini, le cui informazioni personali indebitamente fuoriuscite dagli archivi elettronici possono essere adoperate in modo illegale. In caso contrario, se la news si rivelasse priva di qualsiasi frammento di verità il compito del Garante e della Consob dovrebbe essere quello di comunicare urbi et orbi la falsità della notizia e del conseguente allarme. Il risultato, mancando queste garanzie, l’abbiamo già visto con Nexi – stante che la notizia è ancora in divenire – e le conseguenze sulla brand reputation e sul titolo si sono già fatte sentire.