protiviti®
Risk & Business Consulting.
Internal Audit.

Insight

N. 50 – Maggio 2016

Prevenzione dai Data Leak e protezione dei dati sensibili aziendali

A partire dal caso Snowden, il termine *Data Leak* è entrato nel vocabolario comune ad indicare il trasferimento non autorizzato - volontario o involontario - di informazioni riservate.

Nonostante il continuo sviluppo delle tecnologie di sicurezza informatica e gli sforzi delle aziende volti a proteggere i propri dati, i casi di *data leak* sono sempre più frequenti e di dimensioni sempre più ingenti, sia dal punto di vista economico/finanziario, sia dal punto di vista reputazionale.

Malgrado gli impatti siano generalmente significativi, vi è ancora poca attitudine da parte delle aziende a gestire preventivamente il rischio legato alla diffusione di dati riservati e le attività di mitigazione troppo spesso vengono affrontate con un approccio focalizzato quasi esclusivamente sugli aspetti tecnici (IT), trascurando gli interventi necessari a livello organizzativo, di processo e, più in generale, di business.

Per alcune aziende che trattano dati altamente riservati e relativi ai propri clienti, che costituiscono un bersaglio particolarmente appetibile per numerosi soggetti interessati al patrimonio informativo che custodiscono, la tendenza assume ancor più rilevanza. Si pensi alle aziende fornitrici di servizi professionali, come ad esempio società di consulenza, boutique di M&A, società di revisione, studi legali. In tali realtà, l'elevata criticità e sensibilità delle informazioni trattate si abbina spesso alla non adeguatezza delle competenze e delle strutture organizzative necessarie a gestire in maniera coerente i rischi di *data leak*.

È opportuno che tutte le aziende prendano consapevolezza della necessità di utilizzare un *framework* di protezione dei dati, procedendo in modo sistematico al fine di ridurre, al di sotto del livello ritenuto accettabile dal management, i rischi di violazione delle informazioni sensibili. Nell'affrontare questa sfida, è necessario anche che il management abbia la consapevolezza che, a meno di non ricorrere a soluzioni estreme che comporterebbero un ingessamento dei processi aziendali non accettabile, le misure di mitigazione che si mettono in atto non potranno mai garantire l'assoluta certezza di prevenire i *data leak* di tutto il patrimonio informativo aziendale: i casi recenti hanno dimostrato come anche le realtà più avanzate - e con maggiori investimenti in sicurezza - possano essere violate se l'attaccante ha sufficienti risorse tecniche, economiche, temporali ed è in possesso di adeguate competenze.

Per questo motivo è ancora più importante identificare, sin dall'inizio, **il livello di rischio effettivamente accettabile**, per mettere in atto le opportune azioni di protezione dei dati più rilevanti per il business.

Con il presente Insight, Protiviti mira ad offrire alcuni spunti di riflessione sul tema della prevenzione e della gestione dei *data leak*, proponendo il proprio approccio per un governo efficace della sicurezza aziendale.

Nel 2015, globalmente, il numero totale di record sottratti illecitamente alle aziende ha toccato i 736 milioni, comunque inferiore al picco raggiunto nel 2014 con ben 1,1 miliardi di record sottratti.

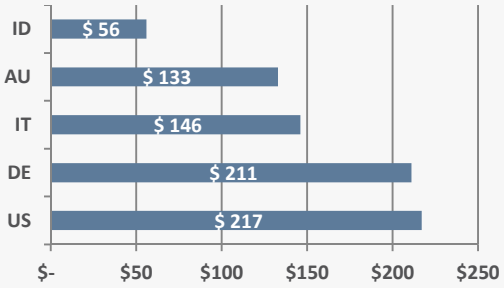
Fonte: Risk Based Security - Data Breach QuickView (2016)

A livello mondiale, il costo del singolo data leak ha raggiunto nel 2015 un valore medio di 3,79 milioni di dollari, con un incremento del 7,67% rispetto al 2014, e del 23% su base triennale. Anche il costo di ciascun record sottratto è aumentato a $ 154, rispetto ai $ 145 del 2014.

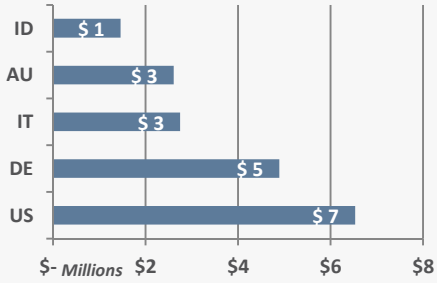
Fonte: IBM & Ponemon - Cost of Data Breach Study: Global Analysis (Maggio 2015)

La situazione in Italia a confronto

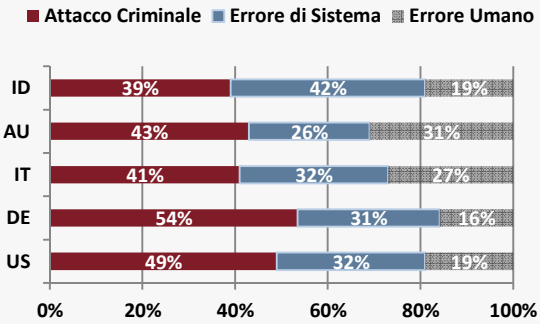
Costo medio di ciascun record sottratto



Costo medio di ciascun data leak



Ripartizione dei record sottratti in base alle cause di leakage



Legenda

ID = India
AU = Australia
IT = Italia
DE = Germania
US = Stati Uniti

Fonte: IBM & Ponemon - Cost of Data Breach Study: Global Analysis (Maggio 2015)

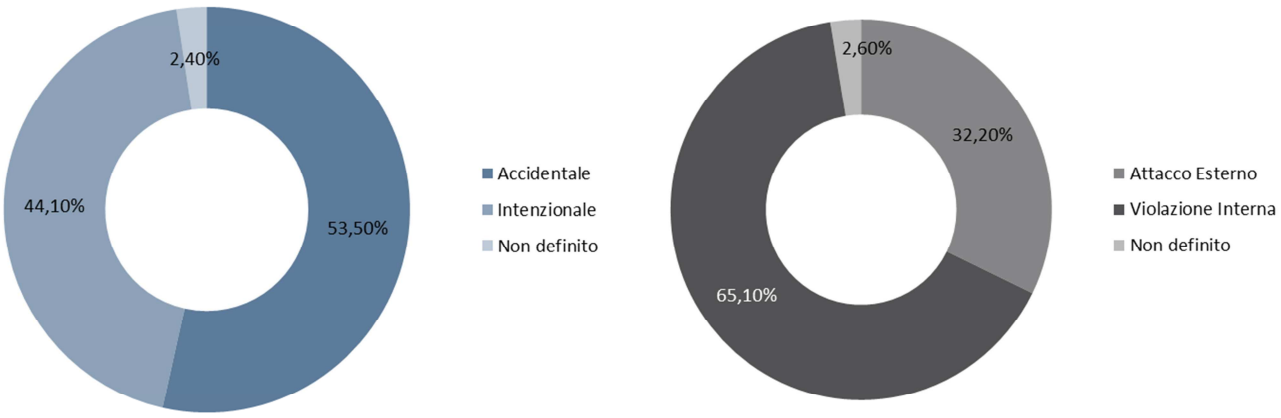
Data Leak Management (DLM)

Per ***Data Leak Management*** si intende l'implementazione di processi e strumenti finalizzati a prevenire, rilevare e interrompere la fuoriuscita di informazioni sensibili all'esterno del perimetro aziendale.[1]

Il concetto di *data leak* risulta essere molto ampio e comprende una serie di casistiche con peculiarità tali da renderle estremamente eterogenee. È infatti possibile che le informazioni trapelino a causa di un'**azione malevola** da parte di un ***hacker* esterno**, oppure per azione di personale interno (***insider***) che diffonde l'informazione per molteplici possibili ragioni (ideologia, corruzione, vendetta, ricatto, etc.).

Eppure, per quanto possa sorprendere, la circostanza più frequente di diffusione di informazioni riservate è di origine involontaria; è infatti sufficiente che il dato venga accidentalmente esposto (per errore umano o di sistema) in ambienti non protetti, per perdere la possibilità di governo dello stesso.

Figura 1. Tipologia e origine degli attacchi[3].



Per questo motivo Protiviti propone un approccio che ha come snodo fondamentale un'analisi del rischio, che pone in relazione gli impatti che un'azienda può subire a seguito di un *data leak* sulle diverse tipologie di dato sensibile - e sui sistemi che le trattano - con i possibili soggetti che possono determinarli.

A questo scopo, si considerano **4 tipologie di soggetti**:

1. **Well Meaning User**: utenti che non hanno intenzioni malevole, ma inconsapevolmente (spesso per ignoranza delle procedure di sicurezza) rappresentano essi stessi una fonte di rischio di esposizione di dati aziendali riservati.
2. **Opportunistic Insider**: utenti che dispongono di privilegi di accesso superiori a quelli che sarebbero necessari. Non metterebbero in atto azioni fraudolente per ottenere tali privilegi, ma disponendone già li considerano acquisiti. Il loro accesso non autorizzato può esporre l'azienda a rischi di *data leak*.
3. **Unsophisticated Attacker**: soggetti malevoli che mirano a sfruttare falle banali e ben note, usando metodi di attacco semplici e poco sofisticati. Anche senza successo nella sottrazione, possono comunque recare a danni ai sistemi IT.
4. **Sophisticated Attacker**: criminali con elevate competenze, fortemente motivati e con un ottimo livello di conoscenza di un bersaglio specifico e appositamente scelto. Spesso dispongono di rilevanti risorse per i loro attacchi.

Data l'ampiezza del problema, è ragionevole ipotizzare un approccio di tipo **olistico**, che non si limiti a proteggere separatamente i singoli elementi a rischio (ad esempio i database) ma che **si estenda a tutto l'ambiente aziendale**, integrando le misure tecnologiche con *policy*, procedure, cultura aziendale e consapevolezza degli attori coinvolti. Un approccio così esteso e pervasivo dovrebbe permettere di conseguire una protezione adatta ad affrontare il rapido cambiamento tecnologico.

L'approccio proposto si struttura su **4 fasi principali**:

Data Classification

Il primo passo per un'efficace sistema di *Data Leak Management* consiste nel collocare i dati all'interno di categorie immediatamente identificabili e gestibili. La classificazione avviene tramite schemi tassonomici che sfruttano caratteristiche direttamente riconoscibili, tra cui, in particolare: sensibilità del dato, valore intrinseco del dato, grado di confidenzialità, strategia di archiviazione.

In questo modo risulta più semplice l'attività di assegnazione della priorità di intervento: i dati con maggiore impatto potenziale saranno posti in sicurezza in modo prioritario e saranno trattati con misure più stringenti, riducendo rapidamente e significativamente il rischio complessivo.

Essendo infatti impossibile, per insufficienza di risorse (umane, economiche, etc.), proteggere tutte le tipologie di dato allo stesso modo, è necessario identificare quelli effettivamente critici.

Durante la classificazione è necessario inoltre identificare i dati che sono sottoposti a specifiche prescrizioni normative, ad esempio quelli soggetti a tutela della legge sulla *privacy*.

Tuttavia, è bene ricordare che il livello di sicurezza desiderato dovrebbe in parte prescindere dal livello di *compliance* (esterna od interna) richiesto. Infatti, i dati strategicamente rilevanti non sempre sono soggetti a prescrizioni particolari, per cui il rischio loro associato prescinde dalle richieste normative.

Nel concreto, accade spesso che vi sia una certa coincidenza tra il valore di business del dato e le richieste normative. In tal caso è fondamentale non limitarsi ad attuare le misure minime di protezione richieste dalla normativa applicabile, ma occorre valutare se esse siano effettivamente adeguate al livello di rischio accettabile dall'organizzazione.

Data Discovery

Nonostante il contesto fortemente "data-centrico" dell'azienda moderna, spesso non si ha piena consapevolezza di quanti e quali dati si trovino nei vari sistemi informativi, nonché di quali politiche di sicurezza si applichino.

Spesso i *data leak* sono causati dal fatto che una copia "dimenticata" di dati critici si trovi su un sistema secondario non protetto adeguatamente, o sia accessibile da esso, il che la rende facilmente violabile.

Questa dispersione deve essere prontamente indirizzata da attività di ricerca (**Data Discovery**), al fine di individuare, mappare e poi classificare il patrimonio informativo aziendale, a prescindere dalla collocazione della singola informazione.

Analisi del Rischio

Una volta identificate le tipologie e la collocazione dei dati sensibili, è necessario procedere alla valutazione dei rischi di *data leak*.

In particolare, i rischi devono essere analizzati in funzione delle 4 differenti tipologie di soggetti, indicati precedentemente, che possono determinarli (***Well Meaning User***, ***Opportunistic Insider***, ***Unsophisticated Attacker*** e ***Sophisticated Attacker***).

In questo modo è possibile inquadrare le casistiche in specifici scenari reali, ai quali saranno associate le contromisure più idonee che, anziché rimanere generiche, potranno essere calate sugli scenari stessi.

Data Defense

L'attività di protezione vera e propria del dato avviene con la predisposizione delle linee di difesa. Tra i diversi meccanismi di difesa da adottare, segnaliamo i seguenti:

- **Controllo degli Accessi**: molto spesso le aziende, per semplificare il processo di assegnazione e gestione dei privilegi, tendono a garantire accessi estesi a tutti, a prescindere dall'effettiva necessità del singolo dipendente. Al contrario, le regole di controllo degli accessi dovrebbero essere configurate sulla base del "*Principle of Least Privilege",* ovverossia attribuendo a ciascun utente l'insieme minimo di privilegi necessari allo svolgimento del suo compito. Utilizzando regole restrittive, è possibile limitare notevolmente il rischio di comportamento fraudolento o perdite accidentali ad opera degli *insider*.
- **Monitoraggio**: il monitoraggio dell'utilizzo dei dati consente di individuare eventuali abusi e di intervenire prontamente interrompendo tale attività. L'attività di controllo dovrebbe essere il più granulare e dettagliata possibile, e dovrebbe includere sia i *data in use* (quando memorizzati in un sistema di archiviazione), sia i *data at rest* (quando acceduti dagli utenti), sia i *data in motion* (quando trasmessi).
- **Data disposal**: uno degli aspetti meno curati (ma più efficaci) per mitigare il rischio di *data leak* consiste nella distruzione in modo irrecuperabile delle informazioni sensibili non più necessarie, andando così a limitare la quantità di informazioni che si decide di mantenere. Ad esempio, limitandosi a custodire solamente quanto richiesto per *compliance*, per normativa, o per tutela legale, è possibile rimuovere dal perimetro aziendale tutte quelle informazioni potenzialmente critiche, che però non sono più utili a fini di business.
- **Gestione documentazione cartacea**: così come è importante mettere al sicuro i dati digitalizzati, altrettanto rilevante è proteggere i dati presenti in forma fisica, come ad esempio quelli in formato documentale cartaceo. La loro gestione deve essere regolamentata tramite *policy* e procedure, come ad esempio quelle di *clean desk*, di gestione delle stampe e di distruzione al termine dell'utilizzo.
- **Policy fuori ufficio**: rendere sicuro il trattamento dei dati quando ci si trova in un ambiente protetto come l'ufficio non è sufficiente. Nel momento in cui i dati sensibili sono trattati in ambienti pubblici (in viaggio, presso le sedi di altre aziende, in trasferta, mediante dispositivi personali come smartphone e tablet, etc.) è necessario fare sì che siano adeguatamente protetti, ad esempio mediante strumenti di crittografia della memoria e di autenticazione forte per l'accesso agli strumenti di lavoro.
- **Gestione degli incidenti**: la gestione degli incidenti di sicurezza, in questo caso i *data leak*, deve essere supportata da procedure e piani di azione immediatamente implementabili. Non solo la risposta deve essere tempestiva, ma la gestione degli incidenti e delle eventuali crisi derivanti in caso di incidenti di vasta portata deve seguire schemi predefiniti che consentano sia di risolvere immediatamente la falla di sicurezza, sia di gestirne le conseguenze all'interno e all'esterno dell'organizzazione, nonché di apprendere e migliorare il sistema di sicurezza sulla base dell'esperienza maturata con gli incidenti.
- **Valutazione e analisi delle terze parti**: molti dei recenti *data leak* sono stati causati da terze parti, coinvolte nel trattamento delle informazioni, che non hanno adottato misure di sicurezza in linea con quanto fatto dall'azienda titolare. E' pertanto necessario estendere la prospettiva di messa in sicurezza a tutto l'ecosistema aziendale, definendo misure per il trattamento delle informazioni che si applichino a tutte le terze parti coinvolte.
- **Awareness**: è di massima rilevanza assicurarsi che tutti i soggetti aziendali coinvolti siano consapevoli delle implicazioni date dal rischio di *data leak* e di come determinati comportamenti possano rendere inefficaci le misure definite. Molto spesso, tale consapevolezza è assente, in quanto manca la relativa istruzione. Solo un adeguato training del personale, compreso il top management, che gestisce le informazioni più critiche, può far sì che le misure di mitigazione non siano vanificate da una scarsa consapevolezza del personale.

Altri strumenti di difesa

Le misure sopra descritte possono inoltre essere affiancate da strumenti di ***cyberinsurance***.

Nonostante l'assicurazione sui *data leak* sia ancora una pratica poco diffusa - e l'offerta di servizi sia ancora in fase di sviluppo e maturazione - è di sicuro un ambito in crescita negli ultimi anni. I prodotti di *cyberinsurance* possono essere un valido strumento per coprire i costi di natura legale e regolatoria, di comunicazione, di analisi forense, di ripristino dei dati, di responsabilità verso terzi e di estorsione da parte degli *hacker*.

Essi tuttavia non devono essere assolutamente considerati come una soluzione per l'assenza di un programma di gestione della sicurezza, in quanto le debolezze nei programmi di sicurezza possono condurre a dei premi assicurativi particolarmente elevati o addirittura all'impossibilità di stipula della polizza. Il rischio reputazionale (i.e. immagine), tuttavia, non è assicurabile.

Considerazioni finali

Le conseguenze di una violazione del patrimonio informativo possono essere estremamente critiche per un'azienda e comprometterne in maniera rilevante la reputazione o la possibilità di continuare ad operare sul mercato. È pertanto necessario definire ed attuare un programma di sicurezza delle informazioni effettivamente commisurato alle proprie caratteristiche e peculiarità che, partendo dalla valutazione del patrimonio informativo e dei rischi ai quali è esposto, identifichi le misure più adatte, che si coniughino con le esigenze operative e di investimento.

Protiviti ha numerosi anni di esperienza nel dare supporto alle attività di *Data Leak Management*, sviluppando solide competenze e metodologie di comprovato successo. Attraverso numerosi progetti abbiamo messo a punto un approccio omnicomprensivo in grado di aiutare i nostri Clienti a proteggersi all'interno di un ambiente di rete sempre più pericoloso e complesso.

***

Contatti:

Hernan Gabrieli – *Managing Director*
hernan.gabrieli@protiviti.it

Antonio Pantaleo – *Manager*
antonio.pantaleo@protiviti.it

Enrico Ferretti – *Director*
enrico.ferretti@protiviti.it