

Overview

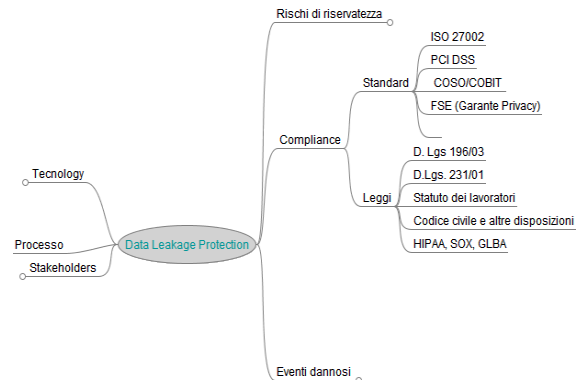


Recentemente la cronaca ha messo in luce diversi episodi che hanno evidenziato la vulnerabilità delle organizzazioni a fenomeni di perdita dei dati (**Data Leakage**).

Queste perdite hanno riguardato sia dati strutturati che non strutturati e sono avvenute in ogni fase del ciclo di vita delle informazioni.

Le procedure operative e la struttura tecnica dei sistemi informativi devono indirizzare questi rischi senza compromettere l'operatività della struttura

L'esigenza di rilevare e prevenire i fenomeni di perdita di dati aziendali nasce principalmente da vincoli di **compliance** a standard, leggi e regolamenti che mirano a tutelare la proprietà intellettuale e la privacy. Nello stesso tempo, tuttavia, bisogna evitare che i controlli di sicurezza adottati per far fronte a tali fenomeni risultino troppo pervasivi.



Definire ed implementare una *Strategia di Data Leakage Prevention (DLP)* significa identificare e controllare i rischi (*Risk Mitigation*) cui sono esposti i dati sensibili delle varie tipologie (**Strutturati, Non Strutturati**) nelle varie fasi del loro ciclo di vita (**Data At Rest, In Use, In Motion**), considerando le particolarità dei processi cui sono sottoposti.



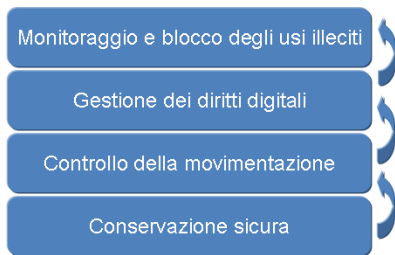
Matrice dei rischi per fase/tipologia del dato

La risk mitigation deve avvenire con la selezione ed implementazione di controlli di sicurezza efficaci ed economicamente sostenibili che si articolano in misure organizzative e di processo a cui seguono interventi di implementazione ed integrazione di soluzioni tecnologiche che supportano e agevolano i processi di rilevazione e prevenzione delle perdite di dati.

Present assiste il suo cliente in tutte le fasi di ideazione, implementazione ed esercizio di una strategia di data protection, dall'analisi del rischio ai managed services

La soluzione

L'approccio Present al DLP prevede una prima fase di indirizzo strategico focalizzata alla definizione del *Programma di Intervento* e basata sull'analisi dei processi, dell'organizzazione e delle tecnologie di protezione già in uso. I risultati di tale analisi vengono poi utilizzati per valutare i gap da colmare rispetto ad uno scenario ottimale, adeguato agli obiettivi e alle esigenze dell'organizzazione. Viene, alla fine, rilasciato un piano dettagliato di interventi di adeguamento per ciascun ambito.



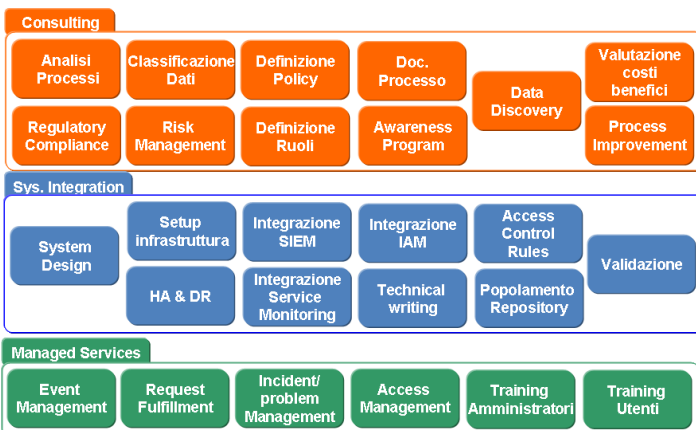
Per l'implementazione delle contromisure/ soluzioni di DLP Present suggerisce un approccio strutturato e graduale che prevede:

- l'individuazione di ambiti distinti di intervento, omogenei per tipologia di dati e/o Funzioni aziendali che li trattano; la scelta dell'ambito tiene conto di fattori di rischio (sensibilità del dato, livello di rischio), opportunità (costo economico, personale coinvolto, impatto organizzativo);
- un modello (vedi figura a fianco) che distingue quattro livelli di capability da consolidare in sequenza dal basso verso l'alto: dopo il completamento e consolidamento delle contromisure al livello inferiore si passa al livello successivo superiore.

Le Soluzioni di DLP che Present propone nel proprio portfolio di offerta sono evidenziate nello schema riportato a fianco, articolato sui quattro livelli di capability descritti sopra.

Tali soluzioni, prese singolarmente o integrate tra di loro, sono in grado di supportare, semplificare ed agevolare i processi organizzativi preposti al DLP.

Le soluzioni possono convivere in maniera integrata per affrontare sia i problemi dei dati strutturati che dei dati non strutturati.



L'offerta Present include:

- servizi di *Consulenza* finalizzati all'analisi e allo sviluppo del Programma di Intervento;
- servizi di *System Integration* per l'implementazione e l'integrazione della soluzione DLP con le infrastrutture del cliente ,
- *Managed Services*, per la gestione della soluzione DLP e l'assistenza al cliente diretta o tramite l'addestramento del personale.