PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 5012 di Giovedì 23 settembre 2021

Garantire la sicurezza dei dati attraverso un gestionale HSE

La sicurezza dei dati aziendali è garantita tramite il monitoraggio degli accessi, la tracciabilità delle operazioni e le tecnologie di data protection: requisiti indispensabili per un gestionale

La gestione e la protezione dei dati aziendali è ormai diventata una priorità assoluta nell'attuale contesto di digital transformation, in cui il patrimonio informativo aziendale è composto da dati personali, progetti e proprietà intellettuali, che hanno un valore inestimabile.

Infatti, nell'infrastruttura IT vengono salvate importanti informazioni come dati sensibili di dipendenti, fornitori, clienti attuali e potenziali, analisi, report e molto altro, per cui è facile intuire come il rischio di perdita e/o manomissione di questi dati può costituire un grave danno di entità non facilmente quantificabile, sia in termini economici sia in termini di immagine e reputation.

I dati oggi sono esposti a minacce esterne di ogni tipo, con attacchi che stanno diventando sempre più sofisticati, difficili da intercettare e da bloccare a causa di tecnologie sempre più evolute.

Questo ha aumentato la consapevolezza della necessità di garantire la sicurezza dei dati nelle imprese, esigenza già emersa con l'entrata in vigore del GDPR, che ha rappresentato una pietra miliare nell'ambito del trattamento dei dati personali.

In questo contesto le Aziende, prima di effettuare investimenti per l'implementazione di sistemi informativi, devono realizzare delle attente valutazioni al fine di selezionare soluzioni in grado di assicurare la sicurezza dei dati, attraverso il monitoraggio degli accessi e la storicizzazione puntuale di qualsiasi operazione di modifica, inserimento e cancellazione sugli stessi.

Tali caratteristiche sono fondamentali, tanto da essere incluse nel testo dell'**art. 53 del D. Lgs 81/08**, che declina tutti i requisiti che un sistema informativo deve possedere al fine di garantire la memorizzazione sicura dei dati aziendali, in ambito HSE.

In particolare, l'**art. 53**, al comma 2, prevede che la soluzione gestionale debba consentire:

1. L'accesso ai soli soggetti abilitati dal datore di lavoro
2. La validazione dei dati solo da parte dei responsabili
3. La riconducibilità delle operazioni di validazione all'utente responsabile
4. La storicizzazione di tutte le eventuali modifiche, in modo che siano solo aggiuntive a quelle già memorizzate

5. La riproduzione su supporti a stampa delle informazioni contenute nei supporti di memoria
6. La conservazione su almeno due distinti supporti informatici di memoria
7. La redazione della procedura descrittiva per la gestione del sistema medesimo, riportante i codici di accesso.

Ma, per garantire la data security a 360° dagli attacchi e dai reati informatici ? sempre più in crescita ? un sistema che soddisfi solo questi requisiti, non è sufficiente.

I cyber crimini contro Aziende, istituzioni e privati sono in forte aumento da diversi anni e molte organizzazioni non sono ancora preparate ad affrontarli: l'attacco informatico contro la Regione Lazio, che ha bloccato tutti i servizi digitali regionali compresi quelli legati alla campagna vaccinale, ha solo messo in evidenza e portato all'attenzione di tutti un problema che per gli esperti è già noto da diverso tempo.

Secondo il **Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche** (CNAIPIC), il numero degli attacchi contro infrastrutture critiche in Italia, ad esempio le aziende che erogano servizi, sono più che raddoppiati in un anno, passando dai 239 attacchi del 2019 ai 507 del 2020.

Il **Clusit**, Associazione Italiana per la Sicurezza Informatica, lancia l'allarme evidenziando, che dal 2014 al 2019 la crescita dei crimini informatici è stata pari al 91,2%.

Alla luce di questi allarmanti trend, le Aziende rispondono investendo maggiormente nel campo della sicurezza e protezione dei dati, come conferma l'**Osservatorio Cybersecurity & Data Protection** 2021 raggiungendo un valore di circa 1,37 miliardi di euro.

Ma, quando parliamo di sicurezza informatica, cosa si intende?

Per rispondere occorre fare riferimento ai concetti di disponibilità, integrità dei dati e riservatezza degli accessi:

- Disponibilità dei dati, ossia la salvaguardia del patrimonio informativo aziendale nell'ambito della usabilità e nel rispetto della confidenzialità dei dati;
- Integrità dei dati, volta ad assicurare che l'informazione non subisca modifiche e/o cancellazioni. In tale direzione si pone la scelta delle Aziende di impiegare sistemi di "log management";
- Riservatezza, ossia gestione della sicurezza al fine di limitare i rischi connessi all'accesso o all'uso delle informazioni in forma non autorizzata (data privacy), in conformità al GDPR.

Dunque, appare evidente che per garantire la data security è necessario adottare un approccio strutturato e strategico ed avere la visibilità a 360° di quello che avviene all'interno del proprio perimetro aziendale. Infatti, solo una efficace ed efficiente governance aziendale consente di valutare i rischi informatici associati alla propria realtà, attivando le giuste contromisure per assicurare che gli asset aziendali abbiano sempre dei livelli di sicurezza adeguati.

È in tale direzione che si muove **Wolters Kluwer** nel realizzare per le Aziende, la soluzione **SIMPLEDO** per la gestione dei processi HSE in grado di offrire le migliori garanzie in termini di dati, tecnologia e workflow in esso custoditi.

SIMPLEDO, in linea con l'**art. 53 del D. Lgs 81/08** e attraverso la funzionalità di **Data & Access Tracing**, consente di tenere traccia di tutte le attività svolte, storicizzare tutti i dati modificati e/o cancellati e monitorare puntualmente gli accessi, permettendo di ricondurre le singole azioni di inserimento, modifica e cancellazione agli utenti abilitati che le hanno predisposte.

In particolare, attraverso il **Data tracing** è possibile tracciare in modo completo, tutte le azioni effettuate sui dati in **SIMPLEDO**, riportando tutte le eventuali eliminazioni o sovrascritture di dati precedenti. Il sistema consente di esplorare i dati e quindi di analizzare le azioni effettuate dagli utenti che le hanno predisposte.

Allo stesso modo **SIMPLEDO** offre un ulteriore strumento, **Access tracing,** che consente il completo monitoraggio degli accessi effettuati sui dati, consentendo di conoscere su quali gli utenti hanno avuto accesso.

Ma la garanzia offerta da **SIMPLEDO** nell'ambito di sicurezza e protezione dei dati, non si limita a questo.

Infatti, la soluzione adotta tutte le misure volte a proteggere le risorse informatiche ed i dati ospitati: crittografia dei dati sensibili dei lavoratori (encryption at rest and in transit) come quelli sanitari, produzione di statistiche anonime, gestione sicura di dati, documenti e contratti dei fornitori, gestione delle password GDPR compliant e sicurezza degli accessi (autenticazione a due fattori e/o SSO), sono solo alcuni esempi.

Infine, la piattaforma utilizzata per l'erogazione dei servizi di **SIMPLEDO** è **Microsoft Azure**, il più innovativo e certificato servizio cloud che garantisce massimi livelli di performance, sicurezza e protezione dati, in conformità al GDPR.

Bisogna accelerare il più possibile la digital transformation partendo dal top management, adottando contromisure per proteggere adeguatamente gli asset aziendali con tecnologie avanzate che ne garantiscano un miglioramento continuo e sicuro di processi e dati.

La tua azienda garantisce livelli di sicurezza e data protection adeguati?

Per richiedere maggiori informazioni e/o una presentazione DEMO, invia una e-mail al seguente indirizzo: info.simpledo@wolterskluwer.com e/o compila il form con i tuoi dati

Leonarda Cornacchia

HSE Software Marketing Manager

Wolters Kluwer Italia