MalpensaNews

Come garantire la privacy e la sicurezza dei dati sensibili in azienda

divisionebusiness · Monday, July 29th, 2024

Nell'era digitale, per tutte le aziende la **protezione dei dati sensibili** rappresenta un aspetto di fondamentale importanza. Sono numerose le strategie che possono essere implementate dalle imprese al fine di garantire la sicurezza delle informazioni e al tempo stesso la loro privacy: essenziale è, per esempio, la formazione del personale; ma non si può prescindere dal controllo degli accessi e da altre soluzioni come la crittografia avanzata. Le **politiche di sicurezza** meritano di essere studiate in modo meticoloso, ma soprattutto aggiornate con il passare del tempo, vista la rapidità con la quale le tecnologie si evolvono. Aziende specializzate come Boolebox mettono a disposizione diversi strumenti utili ad assicurare una protezione efficace dei dati aziendali, ma quel che ci vuole è anche un cambio di passo dal punto di vista culturale.

Un tesoro da proteggere

Non è un caso se, in occasione di una delle campagne pubblicitarie commissionate dal **Garante per la protezione dei personali** in seguito all'entrata in vigore del GDPR, i dati venivano definiti un tesoro da proteggere. In che modo? Il primo passo potrebbe essere quello di procurarsi (e mettere a disposizione dei propri dipendenti) degli **strumenti avanzati**, a cominciare da software che consentano di adattare al GDPR il sistema di gestione della privacy. Si può optare, per esempio, per un software in cloud, non vincolato all'utilizzo di specifici device.

Privacy dei dati: strategie di prevenzione e di protezione

Come si è accennato, è indispensabile che il personale venga formato in maniera completa in materia di privacy dei dati. Tutti i lavoratori, infatti, devono essere consci delle **policy applicate in azienda** in tema di riservatezza dei dati, ma anche delle best practices che devono essere messe in pratica per raggiungere i più elevati standard di sicurezza. Al contempo, è molto importante eseguire un monitoraggio costante, anche per riuscire a reagire in maniera tempestiva alle eventuali violazioni che si dovessero riscontrare. Se si verificano degli **incidenti di sicurezza**, è bene poter contare su un piano di risposta: il che vuol dire definire delle procedure che permettano di identificare il più velocemente possibile gli "accident" e gli "incident" che si possono verificare, così che le misure di disaster recovery più appropriate possano essere adottate di conseguenza.

Il valore della conoscenza

Può sembrare superfluo metterlo in evidenza, ma non lo è: per garantire la sicurezza dei dati è bene

avere una conoscenza completa delle norme vigenti in materia di **privacy dei dati**. Questo implica avere una comprensione approfondita di tutti gli obblighi legali che è necessario rispettare, anche per essere certi che le politiche che vengono applicate siano conformi alla legge. Dopodiché si potrà pensare a quali misure di sicurezza scegliere, con il ricorso a **software antivirus, firewall, tecnologie di crittografia** e non solo.

Gli obblighi per le aziende

Il titolare e responsabile del trattamento dei dati all'interno di un'azienda ha l'obbligo di provvedere alla raccolta degli stessi, alla loro conservazione e al loro trattamento in maniera da rispettare i diritti dei soggetti interessati. Tra le mansioni di cui si devono occupare **i titolari e responsabili del trattamento** c'è la tenuta del registro di trattamento, ma anche la redazione delle informative sulla privacy da mettere a disposizione dei dipendenti, dei clienti e dei soci. Molto importante è anche il **registro data breach**: si tratta del registro delle violazioni, che permette di tenere traccia degli eventuali accessi ai dati personali che vengono effettuati in maniera imprevista. Compito dei titolari e responsabili del trattamento è anche quello di provvedere all'analisi dei rischi e alla loro valutazione.

Il ripristino dei dati

È indispensabile che, in seguito a un incidente tecnico o fisico, l'accesso ai dati personali e la loro disponibilità possano essere ripristinati in maniera tempestiva. Il **backup dei dati** è il primo passo da compiere in tal senso: una soluzione che può essere implementata senza difficoltà da parte di qualunque azienda. Il backup è uno strumento che può essere definito quasi salvavita, ma solo a condizione che venga eseguito su **dispositivi sicuri** e in maniera frequente. Non può mancare, d'altro canto, una procedura che consenta di testare la reale efficacia delle misure di carattere organizzativo e tecnico che si è scelto di adottare.

Le misure organizzative

Quali sono, dunque, queste misure di carattere organizzativo? Una è la **formazione del personale**, a cui abbiamo già fatto cenno; ma occorre menzionare anche tutte quelle procedure specifiche grazie a cui è possibile rappresentarsi in anticipo le attività che devono essere svolte in varie evenienze. Non si tratta di pensare solo a come agire quando vengono violate delle informazioni, ma anche più semplicemente alle modalità con le quali devono essere gestite le **richieste di accesso ai dati** da parte di varie tipologie di utenti. Sono tutte decisioni che devono essere prese a monte e non possono essere improvvisate.

This entry was posted on Monday, July 29th, 2024 at 10:30 am and is filed under Scienza e Tecnologia
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.