Il Ruolo del Backup e del Disaster Recovery nel contesto del nuovo regolamento Privacy

(GDPR: General Data Protection Regulation- Regolamento UE 2016/679)

Il General Data Protection Regulation (GDPR) è alle porte. Imporrà numerose responsabilità alle aziende per quanto riguarda la raccolta e la gestione dei dati personali dei cittadini dell'UE.

A seguito delle nuove disposizioni introdotte dal Regolamento GDPR, le impresse saranno obbligate ad implementare in modo specifico i ruoli, i processi e le tecnologie che assicurano la sicurezza dei dati personali dei cittadini dell'UE.

Dovranno inoltre garantire che questi siano accessibili, usati appropriatamente e forniti con il consapevole consenso degli interessati.

Per capire cosa questo significhi per le aziende, è utile comprendere come la nuova regolamentazione estenda la definizione di dato personale. **Con il concetto di dato personale non si intende più solamente la documentazione finanziaria, governativa e medica.** In accordo con le nuove regolamentazioni dovranno essere **considerati dati personali anche tutte le informazioni genetiche, culturali e sociali** (es. indirizzo email, indirizzo IP, cookies, post sui social media, informazioni genetiche, informazioni mediche ecc...).

Inoltre il GDPR rende requisito obbligatorio per ogni azienda l'ottenimento dell'esplicito consenso da ogni individuo per l'utilizzo dei propri dati personali e di garantire il "Diritto all'Oblio".

Cosa devi tenere a mente:

Tutti i cittadini dell'UE hanno **il diritto legale di accedere ai dati che un'azienda ha raccolto su di loro** – durante un acquisto online, accedendo a servizi statali online, servizi sanitari o dopo acquisiti da applicazioni mobile. È responsabilità dell'azienda garantire di essere in grado di fornire queste informazioni su richiesta del soggetto. Le imprese **devono fornire informazioni dettagliate sul modo in cui stanno usando i dati dei consumatori.**

I consumatori **ottengono il diritto di richiedere alle aziende di trasferire i propri dati ad terze parti.**

“E’ responsabilità dell’azienda avvertire un soggetto colpito e l’Autorità Nazionale per la Privacy di ogni violazione dei dati entro 72 ore”

I clienti **hanno il diritto di richiedere la cancellazione dei dati alle aziende, alle organizzazioni e agli enti alle quali hanno, anche in precedenza, autorizzato la raccolta e la gesione dei dati personali.** L'azienda dovrà assicurare che ogni traccia delle informazioni personali del richiedente venga cancellata dai data system aziendali.

Le imprese dovranno informare gli utenti nel caso in cui i dati personali vengano immagazzinati fuori dai confini dell'UE.

E' responsabilità dell'azienda **avvertire entro le 72** (dalla scoperta dell'evento) i soggetti colpiti e l'Autorità Nazionale di Garanzia della Privacy **in caso di violazione dei dati** (perdite e danni accidentali, furti o accessi non autorizzati a dati personali).

DIZIONARIO:

Data Controller: premesso che il Data Controller è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o con altri, determina le finalità e i mezzi del trattamento di dati personali, è tale un'azienda operante dentro o fuori l'UE ma che tiene rapporti con cittadini dell'UE e raccoglie dati sensibili di residenti nell’UE durante la propria attività. Alcuni esempi: un’azienda che processa ordini online, pagamenti da consumatori o fornitori, struttura di assistenza sanitaria che conserva dati del paziente ecc.

Data Processor: premesso che il Data Processor è la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del Trattamento, è tale un'azienda che opera come appaltatrice del Data Controller: storage provider, SaaS, BaaS o DraaS provider ecc.

"Le aziende devono essere in grado di proteggere e mantenere la privacy dei dati anche in caso di attacchi ransomware. Le aziende che non soddisfano i requisiti GDPR potranno essere soggetto a ingenti multe (fino a € 20 milioni o il 4% delle entrate complessive annue)."

Una delle sfide più grandi che le aziende devono considerare per soddisfare il GDPR è **la gestione dei dati.** Basti pensare a **quante copie dei dati personali di un solo individuo potrebbero essere diffuse all'interno della stessa azienda.** Questa è la ragione per la quale è così importante **creare una mappa che mostri come l'azienda processi, immagazzini e metta in sicurezza i dati.** Potrebbe sembrare difficile all'inizio, ma è compito dell'azienda avere piena coscienza su come i dati personali vengano trattati. Solo dopo questo tipo di analisi sarà possibile derivare tutte le informazioni necessarie per la raccolta e il trattamento dei dati personali.

Un altro problema cruciale è **la sicurezza dei dati.** Impostare e mantenere **sia un solido Backup sia un piano di Disaster Recovery (DR) efficace**, sono ormai due accorgimenti necessari per una seria policy riguardante la protezione dei dati.

Incidenti come attacchi ransomware, malware o "server failure" (diversamente originati) provano il fatto che le aziende possono facilmente perdere accesso ai dati raccolti.

Perciò, in conformità con il GDPR, un'azienda deve **assicurare una solida protezione dei dati e disporre un piano di Disaster Recovery affidabile** non solo in termini di implementazione di una soluzione di backup, ma anche di una soluzione di recupero dei dati testata regolarmente.

Le aziende devono essere in grado di proteggere e mantenere la privacy dei dati anche in caso di attacchi ransomware: quelle che non soddisfano i requisiti GDPR potranno, infatti, essere soggette a ingenti multe (€ 20 milioni o il 4% delle entrate complessive annue).

"Perché il backup sia veramente in grado di fornire la sicurezza dei dati contro ogni possibile downtime, non dovrebbe essere modificabile. Allora come si relaziona al Diritto all'Oblio?"

Il Diritto all'Oblio è un **nuovo diritto riconosciuto ad ogni cittadino dell'UE: prevede il diritto di richiedere che i propri dati personali vengano cancellati e non più processati da alcun soggetto.** Per esempio, un tuo cliente potrebbe richiedere la cancellazione di tutti i suoi dati personali immagazzinati nel tuo server o in altre applicazioni.

Ma se il backup deve garantire realmente la sicurezza dei dati contro ogni possibile downtime (tempo morto del sistema, magari successivo ad attacco o incidente) non dovrebbe, in teoria, essere modificabile.

Allora come si relaziona il backup al diritto all'oblio?
Per soddisfare il GDPR, le aziende devono assicurare che i propri dati siano facilmente ripristinabili. Allo stesso tempo il Diritto all'Oblio obbliga alla cancellazione di quei dati per i quali l'utente abbia richiesto con apposita documentazione la rimozione.

Una soluzione possibile è una configurazione appropriata delle impostazioni di conservazione e backup. In questo scenario, la memorizzazione dei dati è relativamente breve – i dati sono sovrascritti ogni 72h.

Step 1: **Analisi**

Step 2: **Requisiti**

Step 3: **Testing**

Determina il tuo RTO e RPO

Inizia dalle basi. Il **Recovery Time Objectives** (RTO - é il tempo necessario per il pieno recupero dell'operatività di un sistema o di un processo organizzativo in un sistema di implementazioni di policy di Disaster Recovery) e il **Recovery Point Objective** (RPO - uno dei parametri usati nell'ambito delle policy di Disaster Recovery per descrivere la tolleranza ai guasti di un sistema informatico) sono i due principali parametri nella pianificazione di un piano di Disaster Recovery e per la protezione dei dati.

Guarda ad ogni dispositivo (postazioni lavoro, server, virtual machine ecc...) e decidi quanto ognuno di questi sia critico per la tua azienda: quanto velocemente hai bisogno che quel dispositivo torni online e funzionante? **Se non è così importante, non spendere soldi e risorse per recuperarlo per primo.**

Tieni presente che i dati sono importanti, ma non tutti sono fondamentali per le operazioni aziendali. **Pensa per quanto tempo i tuoi dati potrebbero essere inaccessibili senza che vi sia un impatto negativo sulla tua azienda**; dall'altra parte, quali dati sarebbero veramente costosi o potenzialmente pericolosi da ricreare per la tua azienda?

Mentre ricerchi la soluzione di Disaster Ricovery appropriata, verifica, per prima cosa, se quelle che stai vagliando saranno in grado di garantire i parametri RTO e RPO.

STRONGBOX

Step 1: **Analisi**

Step 2: **Requisiti**

Step 3: **Testing**

Determina le tue necessità di Backup

Ripensa il tuo ambiente informatico
Decidi tenendo di conto quali sistemi e tecnologie il tuo sistema di Backup dovrà supportare: protezione image-based, accesso veloce ai dati, massima sicurezza, la certezza che i tuoi dati di Backup non vengano corrotti, una soluzione affidabile che possa eseguire il backup dell'intero ambiente aziendale, uffici remoti, applicativi, dispositivi mobili degli impiegati.

Step 1: **Analisi**

Step 2: **Requisiti**

Step 3: **Testing**

Gestione delle policy di Testing e Backup

Qual è la soluzione di Disaster Recovery adatta per il tuo business? È semplice: quella che funziona. Ma come si può sapere se la tua soluzione è affidabile, come puoi stimare se i tuoi parametri RTO e RPO possono essere raggiunti?

La tua soluzione di Disaster Recovery deve poter recuperare i tuoi dati in ogni momento. Per questo devi provvedere a testare la soluzione DR regolarmente. Per fare ciò senza sprechi di tempo e risorse, la tua soluzione DR deve offrire un sistema di gestione semplice, centralizzato, con accesso remoto, con sistema di report avanzato, con monitoraggio dei log ecc.

COME STRONGBOX PUÒ RISOLVERE I TUOI PROBLEMI GDPR CON I DATI PERSONALI?

Strongbox è un prodotto globale che copre endpoint (PC, postazioni lavoro e dispositivi mobili), server (Windows Server, Linux Server, database, location di rete ecc...). Con il suo aiuto si possono proteggere 21 diverse piattaforme.

Senza alcun modulo aggiuntivo puoi mettere in sicurezza l'intero ambiente informatico e preparare semplicemente la tua azienda per il GDPR.

Backup in cloud privato

È un'idea innovativa per creare un'infrastruttura di backup in una location di fiducia e sicura per un ambiente con una grande quantità di dati.

Basterà ottenere un software per il backup per salvare in locale i tuoi dati: in altri termini, un cloud privato.
Tuttavia il resto delle funzionalità e possibilità andrebbe revisionato.

Sicurezza End-to-End

Non dovrai preoccuparti se il backup dei dati sia stato eseguito correttamente o meno. Ogni file è controllato con SHA1 per garantire che ci sia esattamente lo stesso dato nel backup. Tutti i dati sulla macchina vengono criptati con l'algoritmo AES 256 CBC prima di essere inviati alla destinazione di backup. Con l'algoritmo di criptazione AES 256 CBC ogni blocco successivo viene criptato utilizzando i dati dell'elemento precedente. Quello stesso processo si verifica durante la decripta-zione. E sì, il trasferimento è crittografato, inoltre, anche grazie al Protocollo SSL.

Autenticità e integrità

Strongbox verifica l'autenticità e integrità del dato quando si tratta del file originale.

Verifica anche se l'integrità del dato è stata mantenuta al completamento del ripristino.

Gestione centralizzata delle policy di backup

Insieme alle funzionalità di protezione dei dati, ottieni una console di gestione centralizzata che semplifica la gestione delle policy di backup. Con il suo aiuto, puoi gestire e monitorare in modo completo i backup eseguiti su tutti i dispositivi assegnati alla licenza, configurare le applicazioni client, le impostazioni, creare nuovi utenti, aggiungere nuovi host e gestire tutti i servizi di backup.