Contenuto dei dati utente Personali o Aziendali e la gestione dei rischi *di Christopher Shelton-Agar, Data Rover Director.*

In questo articolo evidenziamo le differenze tra l'approccio tradizionale della gestione delle quote di archiviazione rispetto alle esigenze che le aziende hanno oggi su come assumere il controllo, e trarre il massimo dei benefici in termini di Business, sull'enorme mole di dati generati dagli utenti che naturalmente non strutturati.

Sintesi

La realtà vissuta attualmente nelle aziende, indipendentemente dalle dimensioni, dal luogo di lavoro o dal settore di attività in cui operano, necessitano di uno spazio di storage prontamente disponibile e affidabile, per archiviare i dati in modo da gestire correttamente e sviluppare le proprie attività. Immaginate che solo pochi decenni fa i dati aziendali erano cartacei; ora invece tutto è memorizzato in file elettronici che possono essere facilmente spostati o consegnati, alla velocità della luce, in qualsiasi luogo e a qualsiasi destinatario. Questa forse può considerarsi come una meravigliosa evoluzione della tecnologia e della comunicazione, ma questa evoluzione si porta dietro un insieme completamente nuovo di pericoli e rischi.

Lo spazio di archiviazione è diventato essenzialmente molto più economico. Tuttavia, bisogna tenere conto che le esigenze e/o l'utilizzo dello spazio richiesto nelle aziende è in costante aumento. Quindi, in realtà, i costi per le aziende sono come in precedenza, se non maggiori. La gestione dei dati non strutturati e il suo contenuto è tutta un'altra storia. La stragrande maggioranza delle aziende ha poca o nessuna idea di quali dati possieda in realtà e di cosa è responsabile.

Mentre il mondo si muove progressivamente verso un ambiente molto sensibile alla proprietà dei dati, in cui privacy e protezione sono diventati la chiave contro l'ostilità proveniente da ransomware, virus, malware e terrorismo IT, vediamo chiaramente che la richiesta di gestione dello storage sta cambiando: da un controllo stretto sullo spazio puro consumato e un metodo per limitare lo spreco, ad un esame molto più raffinato di quello che si trova effettivamente all'interno dello spazio disponibile e dell'eventuale utilizzo dei suoi contenuti. Dunque, quello che è importante capire prima di ogni altra cosa è che, al giorno d'oggi, il rischio aumenta se questo contenuto viene lasciato incustodito...

Riassumiamo alcuni dei fattori di rischio più evidenti:

All'interno dell'azienda, chi detiene i diritti di accesso, a quali dati si riferiscono e come sono stati creati e mantenuti i relativi percorsi? Cosa succede ai diritti di accesso quando un dipendente parte, viene trasferito o viene cambiato il ruolo degli owner? Qualcuno può tracciare nel passato?
I dati contenuti nei file relativi all'impresa o l'ambiente di storage sono inquinati con contenuti personali, indesiderati o inutili? Quali politiche o azioni vengono messe in atto per ragguagliare l'utente?
Potrebbero esserci implicazioni giuridiche nei confronti del contenuto dei dati e della loro origine? Ad esempio, dati di concorrenti, indesiderati, rubati o non autorizzati presenti sui file server.
Potrebbero essere presenti informazioni Know-How o Sensibili, all'interno dei file, preziose per i concorrenti?
Potrebbero esserci dati abbandonati, obsoleti o più copie degli stessi dati andate dimenticate?
La posizione e la proprietà dei file che contengono dati sugli stipendi, le revisioni, le informazioni bancarie, le password, i registri sanitari e così via, sono realmente mappate e protette?
I dati personali sono protetti adeguatamente e collocati correttamente?
L'azienda mantiene ed applica le politiche di protezione dei dati per la conservazione e la perdita dei dati?
Esiste una politica efficace per la pulizia periodica dell'ambiente, per ottimizzare non solo l'utilizzo dello storage e il suo contenuto, ma anche i tempi di backup e il consumo di energia?
L'azienda dispone di una soluzione per la gestione dei dati correlata al rischio e in grado di identificare processi interrotti o flussi di lavoro instabili?
I responsabili di progetto e il personale sono consapevoli ed edotti sulle best practices nelle politiche di storage per scopi di compliance?
La Gestione dei dati ha un costo! Il servizio dell'azienda coinvolge se stesso e il proprio personale nel mantenimento dell'ambiente con la definizione di centri di costo?

Andare in "cloud" non risolverà automaticamente le problematiche legate all'archiviazione e decisamente non è così economico come pubblicizzato. Quindi, quale tipo di analisi di pre-lancio e dei rischi si potrebbero effettuare per evitare problemi di "spazzatura" e sicurezza?

Questi aspetti riguardo il possesso e la gestione dei dati sono solo la punta dell'iceberg del rischio. Se gestita correttamente, assicuratevi che l'azienda aumenti l'efficienza, la produttività, e anche la protezione contro ogni probabilità di essere accusati di gestione sconsiderata o di essere legalmente responsabili davanti alle autorità.

Una prospettiva sulla gestione tradizionale delle quote

A seconda di come un'azienda si evolve, i processi aziendali ed i flussi di lavoro vengono definiti, ed attorno ad essi viene creata e modellata la piattaforma dell'infrastruttura IT in base ai vari requisiti.

Quando un dipendente crea, condivide o riceve file, devono essere tutti salvati e registrati, ed infine bisogna eseguirne correttamente il backup o renderli continuativamente disponibili online. Questi file potrebbero risiedere nel disco rigido locale del computer, in un dispositivo di archiviazione esterno come un dongle, in un dispositivo aziendale di archiviazione di file come un file server Microsoft Windows, o un dispositivo di memorizzazione NAS o SAN avanzato, oppure addirittura un ambiente di storage basato sul cloud.

Se, per un qualunque motivo, i file divenissero inaccessibili, o nel caso in cui il dipendente non potesse salvare nuovi file di lavoro, causa la limitazione di quota per utente o gruppo, ci si chiede immediatamente quale impatto potrebbe avere sulla continuità aziendale di tutta l'organizzazione. Indubbiamente, il dito punterebbe sul contenuto del file, la possibile corruzione o la definizione inadeguata dei processi aziendali nella gestione dello storage. Alla fine della giornata sarà compito dell'amministratore dell'infrastruttura IT di garantire in ogni momento la disponibilità.

Un modo comune e semplice per gestire i dati che sommergono il file server, o SAN/NAS, è quello di porre un confine intorno ad utenti e condivisioni, applicando una limitazione "hard" o "soft" attraverso una dimensione di quota a quell'utente, gruppo o dipartimento. Quando la quota raggiunge una data soglia, il servizio blocca o avverte gli utenti che stanno esaurendo lo spazio disponibile. Inoltre, si può applicare indistintamente un blocco sul tipo di file. Ad esempio, proibire all'utente di salvare file video o multimediali.

L'amministratore IT risolve il problema dal proprio punto di vista, costruendo una recinzione intorno al campo, affinché la volpe non possa entrarvi! Oggi, questo approccio non è più una soluzione valida. Semplicemente, il motivo è che dovremmo preoccuparci di più del contenuto dei nostri dati, quanto di esso è effettivamente in uso, e chi potrebbe accedervi. Ad oggi, i media nei file sono oggetto di business effettivamente reali, li limitano, rendendoli impossibili da gestire.

La mancata osservanza e/o il mancato rispetto di appropriate pratiche di business in materia di storage potrebbero, in ultima analisi, mettere in pericolo l'intera azienda. Gli utenti danno per scontato che l'utilizzo del file server sia un loro diritto. Concepiscono lo spazio assegnato loro, esclusivamente come un archivio per il proprio lavoro, per alcuni dati personali, e, se lasciati indisturbati, anche per "spazzatura" assolutamente indesiderata. In breve tempo, questi file server traboccano di cose come foto o film personali del weekend, vecchie cartelle di progetto lasciate nel sistema che occupano soltanto spazio, insieme a file contenenti informazioni delicate quali password, dettagli di carte di credito o documenti di clienti/personale, e anche a qualcosa di ancora più assurdo come direttori che fanno backup multipli dei loro portatili sul file server. Oltre al problema del reale spazio consumato c'è il rischio nascosto sul contenuto e l'accessibilità.

Tuttavia, i sistemi di quote intelligenti che applicano alla cieca una barriera non sono una risposta per l'efficienza del business e certamente neanche alla compliance e alla governance. La tradizionale gestione delle quote può considerarsi come ultimo baluardo in organizzazioni in cui gli amministratori IT non sono in grado di ottenere adeguato controllo sui dati non strutturati generati dagli utenti. Infine queste aziende corrono un rischio molto elevato da qualsiasi punto di vista immaginabile.

L'approccio moderno al rischio correlato alla gestione dei dati

Il rischio correlato alla gestione dei dati prevede l'identificazione di una soluzione per processi interrotti o flussi di lavoro instabili e imperfetti. Il mondo degli affari di oggi sta spostando la sua attenzione sulla protezione del valore dell'individuo e della stessa organizzazione. A tal fine, si richiede di allinearsi alle leggi regolamentari internazionali, in cui la conformità e la governance dei dati stanno mettendo tutti sotto i riflettori. Per affrontare tutto ciò, l'azienda deve mettere se stessa sotto un vero e proprio "microscopio organizzativo", avvalendosi di strumenti e capacità tali da individuare processi interrotti, flussi di lavoro instabili o imperfetti.
Le parti interessate di queste società devono essere coinvolte ed informate sul contenuto dei dati per le quali sono responsabili, e sulla loro potenziale correlazione con le molte regolamentazioni messe in atto, come quelle delle norme GDPR in arrivo.

Siamo tutti consapevoli del fatto che il 60% o più dei file contenuti nelle aziende non siano legati ad attività lavorative o siano file non più utilizzati. Per una corretta gestione, necessitiamo di una soluzione che possa identificare, individuare e potenzialmente categorizzare tutti i file da quelli buoni/cattivi o sotto indagine, determinando chi potrebbe avere accesso a tutto questo.

L'intera azienda deve essere sensibile a tale questione e quindi istruita su come utilizzare gli strumenti per separare autonomamente ciò che va bene dalla "spazzatura", rimuovendo i dati delicati dopo l'uso. Con le giuste informazioni si ha una conoscenza tale per poter decidere cosa fare.

Altro argomento da sottolineare riguarda l'auditing. Quando un'azienda richiede l'esecuzione di verifiche di routine, o è stata sanzionata a seguito di indagine causa fughe di dati/furti o perdite, allora si deve anche sapere che queste problematiche potevano essere assolutamente evitate, se i diritti di accesso fossero stati impostati correttamente e resi monitorabili.

Bisogna essere consapevoli che Microsoft si dichiara chiaramente non in grado di garantire informazioni precise attraverso la propria soluzione. Troppo spesso, l'auditing è considerato come una richiesta di indagine da parte della polizia. Un terribile spreco di tempo e denaro ha fatto sì che l'azienda mettesse al primo posto una soluzione preventiva contro questo potenziale rischio. L'80% di tutte le intrusioni viene dall'interno. Così le varie azioni di protezione diventano una soluzione per curare delle perdite.

Conclusioni

Avere una soluzione che consenta di ottenere informazioni preziose sul contenuto e sullo stato di sicurezza in realtà sta evidenziando ciò che è produttivo in contrapposizione ad aree meno produttive dell'azienda stessa stessa. Non solo si impara ad avere maggior successo, ma si è in grado di prendere decisioni sempre più adeguate, in modo da evitare costi inutili. La prima conseguenza automatica che si ottiene è il controllo e la compliance. Porre restrizioni e incaricare la polizia di indagare è solo uno spreco di tempo e denaro. Considerate Data Rover come il Vostro consulente esperto sul contenuto dei dati utente e nella gestione dei rischi.