White Paper

Data Loss Prevention e Data Leak Prevention

Perdite di dati, un problema che si può evitare 2

Una sigla, due significati 2

Scacco alle perdite di dati in cinque mosse, per cominciare 3

Come fare tutto questo nella pratica 5

La sesta mossa 5

Una necessità per pochi? 6

Glossario 7

Perdite di dati, un problema che si può evitare

Quanto valgono i tuoi dati? Te lo sei mai chiesto? Parliamo dei dati relativi alla tua azienda o attività professionale, quelli che quotidianamente generi o utilizzi per portare a termine il tuo lavoro nei diversi ambiti in cui svolge: produttivo, commerciale/marketing, contabile/amministrativo, finanziario, fiscale/legale e così via. Dati senza i quali resteresti irrimediabilmente fermo al palo, dal momento che oggi l'IT non viene più utilizzato esclusivamente per recuperare efficienza o favorire l'innovazione, bensì per portare a termine letteralmente qualsiasi operazione di business, banale o complessa che sia. E, nel fare ciò, **il dato assume un ruolo centrale**: ogni operazione parte infatti da un'informazione, la trasforma e ne produce di nuove lungo una catena che crea valore – il valore della tua azienda.

Torniamo alla domanda iniziale: come fare per quantificare il valore dei tuoi dati? Potresti rispondere che i tuoi dati valgono tanto quanto il fatturato annuale della tua attività, ma sarebbe una stima incompleta. Più realisticamente, **i tuoi dati valgono infatti l'intero giro d'affari** che prevedi di totalizzare lungo tutta la vita del tuo business. In altre parole, dai tuoi dati dipende l'esistenza, lo sviluppo, il successo e la vita stessa della tua azienda.

Un patrimonio così importante deve ovviamente essere **gestito** in maniera opportuna, tenuto sotto controllo e **protetto** esattamente come qualsiasi altro oggetto prezioso. Anzi, con un po' di accortezza in più, dal momento che la stessa tecnologia avanzata che così tante cose ti permette di fare è anche la stessa causa di innumerevoli **vulnerabilità** e possibilità di perdita dei dati intorno a cui ruota il tuo lavoro.

Per fortuna esiste un'intera disciplina informatica dedicata a salvaguardare il tesoro rappresentato dalle tue informazioni. Gli specialisti la chiamano **DLP**, ed è una sigla che faresti bene a conoscere se vuoi metterti al riparo da sgradevoli sorprese.

Una sigla, due significati

Se ci rifletti un attimo, le strade che i tuoi dati possono prendere per uscire dalla tua legittima disponibilità sono davvero tantissime, ma alla fine è semplicemente questione di capire qual è l'effetto ultimo di un tale percorso:

- **Caso n. 1**, i dati vengono effettivamente perduti. Può essere perché un guasto ha reso irrecuperabile un intero database e i suoi backup, può darsi che un tuo collaboratore abbia inavvertitamente sovrascritto o cancellato file di informazioni, o può essere anche la conseguenza di un attacco deliberato per rendere indisponibili i tuoi dati richiedendo un riscatto per (forse) ridarteli indietro – quello che è noto con il nome di ransomware.
- **Caso n. 2**, i dati non scompaiono veramente ma, che tu ne sia consapevole o meno, finiscono con l'essere accessibili anche a soggetti non autorizzati, internamente e/o esternamente alla tua azienda. Le cause possono essere diverse: una vulnerabilità software, l'errata configurazione di un server o di un'applicazione, un dipendente che si copia dei file su una chiavetta per portarseli a casa senza autorizzazione e così via.

Appassionato di sigle, il settore informatico è riuscito a inventare un unico acronimo per esprimere le soluzioni che permettono di affrontare entrambe le casistiche. Sotto l'ombrello della sigla DLP si ritrovano infatti gli strumenti dedicati alla **Data Loss Prevention**, o prevenzione delle perdite di dati (il caso n. 1 appena visto), così come quelli studiati per la **Data Leak Prevention**, o prevenzione delle fughe di dati (caso n. 2 sopra).

Perdite o fughe che siano, la DLP ti mette a disposizione un **approccio completo alla protezione dei dati** in grado di evitare o minimizzare eventuali situazioni che possono andare dal semplicemente imbarazzante fino al penalmente rilevante.

Se non è proprio il massimo lasciar filtrare all'esterno tutte quelle informazioni competitive relative a clienti, contratti, listini, fatture e piani di sviluppo che possono fornire un vantaggio ai concorrenti, va decisamente peggio quando le fuoriuscite riguardano dati sensibili che ricadono nell'orbita del GDPR o di altre normative sulla privacy come quelle in vigore nel settore sanitario e in quello dei servizi finanziari. In questi casi la legge impone azioni correttive ben precise – a iniziare dalla tempestiva comunicazione alle parti interessate e all'autorità nazionale responsabile della materia – facendo scattare la possibilità di **sanzioni** anche significative che raggiungono, nei casi più gravi, la cifra di 20 milioni di euro o il 4% del fatturato.[1]

1 dataprogdpr.com/sanzioni-non-conformita-gdpr

Senza parlare del fatto che la pubblicità che scaturisce intorno a eventi del genere distrugge in un istante tutta la **reputazione** che un brand ha faticosamente conquistato nel tempo presso clienti e mercati con la potenzialità di azzerare l'avviamento di un'azienda e portarla alla chiusura. Non è un'esagerazione: la società di consulenza Price Waterhouse Coopers ha fatto delle analisi in quest'ambito scoprendo che ben 7 PMI su 10 cessano di esistere entro un anno da un evento di perdita significativa di dati.[2]

Scacco alle perdite di dati in cinque mosse, per cominciare

Una strategia DLP ben pianificata e coordinata non nasce per caso ma è frutto di esperienza e continuo aggiornamento sull'evoluzione del settore informatico. In genere una soluzione DLP si concentra su cinque aree principali:

Comprensione dei dati

Il patrimonio informativo di un'azienda non è tutto uguale e i dati non hanno tutti le stesse caratteristiche. Il primo passo è quello dunque di tracciare una "mappa del tesoro" che permetta di capire quali categorie di dati vengono trattate e dove, sia nei sistemi interni dell'azienda (server, applicazioni, messaggistica) che in quelli dei relativi fornitori di servizi come cloud provider e operatori SaaS esterni. In fondo non è possibile proteggere quello che non si sa di possedere o dove si trova effettivamente.

Si tratta di un'attività fondamentale – svolta anche attraverso il ricorso a sistemi automatizzati – che consente di **assegnare la giusta priorità** alle varie tipologie di dati: come è sbagliato lasciare le informazioni della tua azienda prive di una qualsiasi protezione, infatti, è altrettanto inopportuno "blindare" allo stesso modo ogni singolo dato indipendentemente dalla sua effettiva importanza. La protezione comporta infatti un costo non solo finanziario ma anche operativo, dal momento che ogni procedura di sicurezza introduce una sorta di frizione all'interno delle normali procedure di lavoro. Per questo è utile accertarsi di attivare meccanismi di protezione in linea con l'effettivo grado di sensibilità di ciascun dato.

Mappare i dati comporta tuttavia un ulteriore vantaggio. Nella maggior parte delle aziende, infatti, l'ambiente IT esistente tende a essere il risultato di un'evoluzione non sempre pianificata e pilotata adeguatamente. Sarà capitato anche a te: una situazione di urgenza lavorativa impone di implementare rapidamente nuove tecnologie e nuovi sistemi senza che vi sia tempo e modo di riflettere sull'impatto che i nuovi ingressi possono avere sullo scenario esistente. Si creano quindi vere e proprie isole di funzionalità e di informazioni (i cosiddetti "silos di dati") che frammentano l'IT aziendale rischiando oltretutto di sfuggire a una corretta gestione omogenea.

Ecco allora che l'avvio di un progetto DLP può essere considerato come un'occasione per mettere ordine scattando un'istantanea della situazione effettiva che potrà essere proficuamente utilizzata anche per altri scopi, come magari una razionalizzazione dei sistemi stessi con conseguenti risparmi di spazio e di consumi energetici, una revisione delle politiche di backup, una verifica delle licenze software effettivamente necessarie, un adeguamento alle policy normative come il GDPR e così via.

Consapevolezza delle fuoriuscite di dati

Certo, è facile accorgersi di una perdita di dati quando questi spariscono improvvisamente impedendo il normale lavoro degli utenti; è più difficile farlo quando l'esfiltrazione avviene sotto traccia o riguarda dati che vengono consultati solo raramente.

Spesso i dati sfuggono in maniera **inconsapevole**, essendo sufficiente una banale disattenzione nell'allegare i documenti ai messaggi di posta elettronica in uscita o nel copiare una cartella su una chiavetta USB che finisce poi dimenticata chissà dove e in mano a chissà chi. La recente diffusione di servizi e applicazioni in **cloud** ha inoltre introdotto tutta una serie di considerazioni sui temi della effettiva riservatezza e protezione delle informazioni. I file che copi su uno spazio di archiviazione online sono effettivamente al sicuro o potrebbero essere consultati da terzi? Gli utenti con cui condividi determinate cartelle continuano a essere autorizzati a farlo? Cosa succede ai numeri delle carte di credito che vengono utilizzate per gli ormai immancabili acquisti online?

2 www.unitrends.com/blog/what-are-the-consequences-of-data-loss

Per questo motivo un progetto DLP prevede l'attivazione di **processi automatici** che tengono sotto controllo gli spostamenti delle informazioni allertando in caso di movimenti sospetti o imprevisti. Può essere sufficiente ad esempio lo spostamento di determinati file su un servizio di storage esterno come Google Drive o Dropbox per attivare una serie di procedure come avvertire l'utente del tentativo di eseguire un'operazione non ammessa, dirottare l'operazione verso una destinazione appropriata (ad esempio uno spazio di sincronizzazione simile ma gestito su un server interno all'azienda) e **segnalare** l'accaduto agli amministratori IT per eventuali controlli più approfonditi.

Protezione dei dati in transito

Difficilmente le informazioni sono statiche, tutt'altro: la loro valorizzazione ne richiede spesso il trasferimento da un sistema all'altro o da un'applicazione all'altra, sia all'interno che all'esterno del perimetro fisico aziendale (come avviene nel caso del cloud). Quello che raramente si conosce invece è **l'intreccio degli spostamenti** che i dati compiono nell'arco della loro vita utile prima della cancellazione o dell'archiviazione definitiva.

Tracciare i movimenti dei dati è un'attività che completa la mappa delle tipologie delle informazioni che abbiamo visto al primo punto della nostra strategia DLP. Sapere quali categorie di dati intraprendono determinati percorsi i è utile per **ottimizzare** l'ambiente IT, evitare colli di bottiglia e rendere più resiliente l'intera struttura informatica; ma ti permette anche di attivare le misure opportune per salvaguardare il percorso dei dati critici dalla sorgente alla destinazione evitando che possano essere sottratti, copiati o modificati senza che qualcuno se ne possa accorgere.

Anche in questo caso il monitoraggio degli spostamenti dei dati è un'attività che va seguita **costantemente** in modo da riflettere in tempo reale i cambiamenti che intervengono man mano nel flusso delle informazioni. Questo non solo assicura la puntuale efficacia delle misure di protezione previste, ma contribuisce anche a ottimizzare le misure DLP sulla base delle necessità e delle specificità del momento.

Protezione dei dati in uso

Sarebbe facile proteggere i dati rendendoli semplicemente inaccessibili a chiunque, ma si tratterebbe di un controsenso dal momento che, per avere valore, un dato deve essere utilizzabile. La vera questione è che occorre accertarsi che il suo utilizzo avvenga in maniera **legittima** secondo le modalità previste e per le finalità ammesse.

Dunque, a seconda della **categoria** nella quale ricade e del ruolo attribuito all'utente che la manipola, un'informazione può aver bisogno di essere protetta da modifiche e cancellazioni, involontarie o meno che siano. Ci sono informazioni per cui deve essere inibita la stampa su carta piuttosto che la copia o la trasmissione via email; in certi casi può essere opportuno disabilitare persino la copia dello schermo (il cosiddetto screenshot).

Una strategia DLP si fa carico di salvaguardare i dati da azioni errate o indebite di questo tipo attraverso blocchi preimpostati; è inoltre possibile dotarsi di sistemi intelligenti che monitorano automaticamente i comportamenti degli utenti per segnalare eventuali schemi di attività sospette o meritevoli di approfondimento. In questo senso una soluzione DLP contribuisce anche a rafforzare le difese dai sempre più diffusi cyberattacchi, il che non fa mai male – anzi!

Protezione dei dati a riposo

Il termine "a riposo" indica, per esclusione rispetto a quanto visto sinora, i dati nel momento in cui non vengono trasferiti né utilizzati, quindi generalmente tutti quelli che sono **archiviati** da qualche parte a scopo storico oppure per impiego futuro. Candidati usuali a ricoprire questo ruolo sono database, repository, copie di backup, archivi di posta e così via, indipendentemente dal fatto che risiedano su storage locale, in cloud, su nastro, su dischi esterni o altro ancora.

Le tecniche DLP adottate in questo ambito comprendono per esempio la **cifratura crittografica** delle informazioni o il trasferimento su storage immutabile ("write-once"), e anche in questo caso i vantaggi si estendono oltre gli scopi immediati permettendoti di dimostrare l'affidabilità dei dati conservati in azienda nei casi di discovery legale, opposizione a terzi o dimostrazione della conformità normativa.

Come fare tutto questo nella pratica

Va da sé che l'attuazione di un progetto DLP non può prescindere dall'implementazione di una o più **soluzioni tecnologiche** che prendano in esame le particolarità dell'ambiente e delle necessità del singolo cliente.

Il settore offre un ricco ventaglio di opzioni in questo senso, anche se spesso si tratta di orchestrare insieme ed eventualmente completare prodotti che sono già presenti nell'IT aziendale. Un esempio possono essere i prodotti **per il backup e il disaster recovery**, che magari utilizzi già da tempo ma in modo a se stante, fuori da una strategia coerente come quella che un progetto DLP può procurarti.

Altri componenti software possono essere introdotti gradualmente, magari all'inizio in ambiti circoscritti per poi estendersi man mano alla totalità dei sistemi: sono i prodotti che si occupano della **cifratura** crittografica di dischi, file e documenti, i programmi che gestiscono l'utilizzo delle chiavette USB sul parco dispositivi dell'azienda, i tool che permettono di rilevare la presenza di **informazioni sensibili** (come numeri di carte di credito, dati personali, codici IBAN ecc.) all'interno dei messaggi di posta elettronica, delle chat o di altri documenti. Tutti strumenti che, per l'appunto, possono essere incasellati in una strategia DLP rafforzandosi a vicenda.

Se desideri invece una soluzione ancora più solida e strutturata, puoi ricorrere alternativamente a un **sistema DLP completo** intorno al quale potrai riarchitettare categorie e flussi di informazioni e utenze. Soluzioni di questo tipo fanno solitamente perno intorno a uno o più server dedicati, tecniche profonde di monitoraggio del traffico di rete e sistemi di memorizzazione specifici per ogni tipologia di dato trattata: ovviamente non allo scopo di "spiare" il personale, quanto di proteggere il patrimonio informativo contribuendo oltretutto a rendere più sereno il lavoro di tutti.

Una scelta del genere impone la **revisione** dell'ambiente esistente, la **sostituzione** di soluzioni che gli utenti sono abituati ad adoperare da tempo e un certo grado di **cambiamento** nei processi quotidiani, ma di contro guadagnerai la **certezza** di sapere che nessun angolo dell'IT rischia di rimanere fuori dalla strategia DLP. Specie se la tua attività ha certe dimensioni o deve rispettare particolari vincoli normativi e di compliance, questa opzione merita assolutamente di essere valutata con attenzione.

La sesta mossa

Si dice sempre che la tecnologia è uguale per tutti e che il vero elemento di differenziazione delle aziende è il suo **personale**. Verissimo: il mondo digitale ci mette a portata di mano tanti strumenti un tempo appannaggio di pochi esperti e ci consente di "fare di più con meno e in meno tempo" esplorando strade che non avremmo mai immaginato; ma alla fine il valore della creatività e dell'ingegno umano continua a essere al vertice di ogni impresa.

Esiste tuttavia un rovescio della medaglia, e cioè che **l'elemento umano** corrisponde spesso e volentieri anche all'anello debole della catena stesa a protezione del perimetro IT aziendale. Una disattenzione, mancanza di consapevolezza su quanto si sta facendo, un semplice errore possono provocare danni di vasta portata. La tecnologia ci aiuta sì a minimizzare le possibilità che si concretizzino queste casistiche e le eventuali ricadute, ma non a eliminarle del tutto.

Per questo una strategia DLP, come tanti altri aspetti legati all'impiego della tecnologia nelle aziende, deve essere affiancata da un **valido programma di formazione e sensibilizzazione** dei dipendenti. Un errore che si compie spesso infatti è quello di ritenere scontata la conoscenza di certe informazioni da parte di chiunque, mentre la realtà è che non tutto il personale arriva con la medesima esperienza nell'uso degli strumenti digitali né possiede le stesse capacità nel mantenersi aggiornato (per non parlare dell'interesse a farlo) su quanto accade in un settore in velocissima evoluzione come quello informatico.

Fornire una buona formazione di base e irrobustirla con periodici "ripassi" che tengano conto degli immancabili mutamenti di scenario è quindi essenziale se non vuoi che la soluzione DLP messa in piedi con tanta cura abbia un'efficacia ridotta rispetto alle sue piene potenzialità.

Sensibilizza i tuoi collaboratori sull'opportunità di prestare la giusta attenzione alle tematiche che circondano l'uso dei dati, dal momento che anche dalla conformità dei loro comportamenti dipende il buon funzionamento – e nei casi estremi la sopravvivenza stessa – dell'azienda per cui lavorano.

Rendi disponibile un **supporto** adeguato che risponda in maniera tempestiva e qualificata a qualsiasi dubbio o richiesta d'aiuto che possa provenire dal tuo personale. Tante volte si compiono errori perché, di fronte a una situazione inaspettata, non c'è tempo né modo per trovare qualcuno in grado di offrire il giusto consiglio. Predisponi quindi un percorso per ottenere rapidamente l'assistenza necessaria: i tuoi dipendenti saranno più tranquilli sapendo di avere qualcuno su cui poter contare nell'esecuzione delle loro responsabilità quotidiane.

Una necessità per pochi?

Torniamo alla domanda da cui eravamo partiti. Valutare una strategia DLP non è più – se mai lo è stata – un'incombenza riservata a grandi realtà o settori di attività particolarmente sensibili. I dati, di qualunque genere siano e a qualsiasi scopo vengano prodotti e utilizzati, sono la preziosa essenza di **tutte le aziende**. Il loro corretto e adeguato trattamento è la base di un lavoro ben organizzato e senza sorprese.

C'è di più: in questi anni stiamo assistendo all'ingresso spesso incontrollato di smartphone e dispositivi personali all'interno degli ambienti IT aziendali, per non parlare dell'estrema facilità di accesso a servizi in cloud anche gratuiti come ad esempio quelli per la sincronizzazione di file e lo storage online, oppure la diffusione delle varie modalità di smartworking intorno alle quali molte organizzazioni hanno dovuto ristrutturarsi a seguito della pandemia.

Tutti questi fenomeni non fanno che rendere poroso il **perimetro IT aziendale** complicandone il controllo attraverso le tecniche e gli strumenti tradizionali che magari possono essere stati sufficienti fino a ieri. Una strategia DLP – una disciplina che, ricordiamo, si affina costantemente per tenere il passo dei mutamenti che avvengono a livello di infrastrutture, strumenti e processi tecnologici – rappresenta allora la tua miglior garanzia per stendere un cordone protettivo intorno ai tuoi dati ovunque essi si trovino e comunque vengano utilizzati.

Il tuo **Managed Service Provider** di fiducia, una figura che per propria natura è sempre particolarmente aggiornata sulle ultime evoluzioni sia dei pericoli dell'IT che delle soluzioni disponibili per contrastarli, è certamente l'interlocutore più adatto da cui avviare un approfondimento di questo argomento su misura della tua attività.

Glossario

Cloud – Un modello di erogazione di servizi informatici attraverso un'architettura distribuita. Le risorse che costituiscono un ambiente cloud vengono condivise tra i diversi utilizzatori e possono essere scalate in modo elastico senza provocare interruzioni operative. Vi sono differenti tipologie di cloud: *pubblico*, la cui infrastruttura non appartiene all'utente finale a differenza del cloud *privato*; *ibrido*, formato da un mix di ambienti cloud e tradizionali; e *multicloud*, composto da più servizi cloud di tipologie e fornitori differenti

GDPR – Il Regolamento Generale sulla Protezione dei Dati è il riferimento normativo europeo delle leggi che dal 2018 definiscono la possibilità di raccogliere, conservare e utilizzare dati sensibili e personali appartenenti a cittadini e residenti della Comunità Europea. L'entrata in vigore del GDPR ha costretto le aziende a implementare meccanismi di controllo e governance delle informazioni che devono essere regolarmente verificati per garantire il corretto rispetto della norma evitando violazioni che comportano sanzioni rilevanti.

Ransomware – Un particolare tipo di malware che crittografa i file residenti sul computer colpito (e spesso anche su tutti gli altri dispositivi collegati alla stessa rete) che diventano così inaccessibili a meno di non pagare un riscatto per ottenere la chiave di decifrazione necessaria. Non sono rari i casi in cui anche la disponibilità di questa chiave non consenta il ripristino corretto dei sistemi, con gravi conseguenze per le aziende.

SaaS – Acronimo di Software-as-a-Service, ovvero un tipo di soluzione cloud che mette a disposizione un'applicazione software sotto forma di servizio utilizzabile su abbonamento accedendovi tramite interfaccia web o apposite API.