CyberGrant
SECURITY MADE EASY

WHITE PAPER

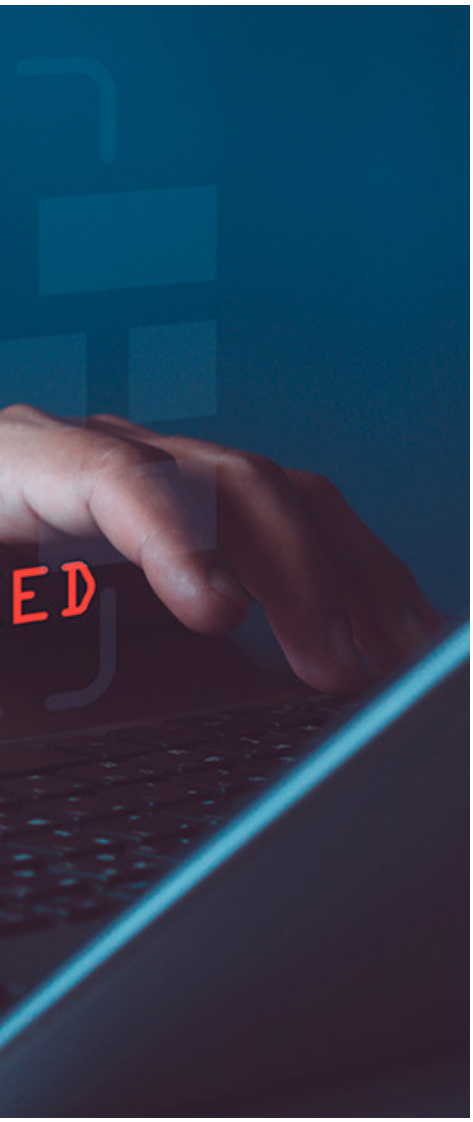
DATA LOSS PREVENTION. NEXT LEVEL

DLP: la sfida che le aziende evitano

Rischi economici e reputazionali

I dati della tua azienda sono al sicuro? La verità potrebbe sorprenderti.
Cos'è la data loss prevention e perché le aziende non la fanno? La difficoltà nella classificazione dei dati può essere risolta con soluzioni come FileGrant Enterprise o RemoteGrant, gestendo così i rischi economici e reputazionali della perdita di dati sensibili.

Sommario



Scenario

10.626 violazioni di dati nel 2024

Secondo il "**2024 Data Breach Investigation Report**" di Verizon, sono state confermate 10.626 violazioni di dati, quasi il doppio rispetto alle 5.199 violazioni del 2023. L'incremento significativo è attribuibile sia al potenziamento delle capacità degli aggressori sia all'espansione delle impronte digitali delle organizzazioni. Inoltre, il report rivela che:

- il **68%** dei data breach è dovuto all'elemento umano, ovvero, una **persona vittima di un attacco di ingegneria sociale o che ha commesso un errore.**
- Il **15% delle violazioni hanno coinvolto una terza parte o un fornitor**e, come catene di fornitura di software, infrastrutture di partner di hosting o custodi di dati

Fonte immagine - "2024 Data Breach Investigation Report" di Verizon

AI utilizzata come vettore d'attacco

È doveroso evidenziare che, nonostante i settori colpiti e le cause siano variabili, molti incidenti presentano elementi comuni, tra cui l'utilizzo dell'intelligenza artificiale come vettore d'attacco.

Le minacce includono **deepfake generati dall'IA e la creazione di malware** completamente automatizzato. Inoltre, lo scorso anno ha altresì registrato un **aumento degli attacchi ai servizi cloud**, che hanno colpito piattaforme SaaS come Snowflake e tutti i principali fornitori di servizi cloud.

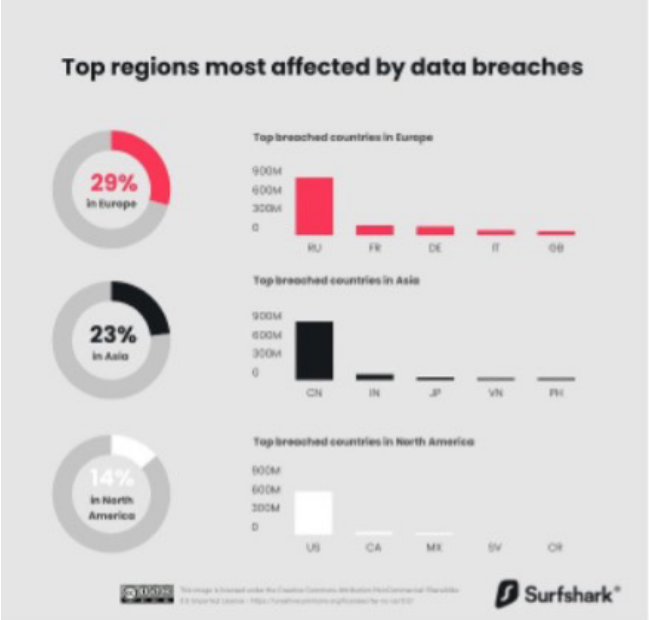
4,88 milioni di dollari

costo medio di una violazione

Il rapporto **“Cost of a Data Breach Report 2024” di IBM e Ponemon** Institute ci rivela che:

- Il costo medio globale di una violazione dei dati nel 2024 è pari a **4,88 milioni di dollari: un +10% rispetto al 2023** e il totale più alto di sempre.
- **1 su 3 è la percentuale che ha coinvolto i “dati shadow”**, a dimostrazione del fatto che la proliferazione dei dati sta rendendo più difficile il monitoraggio e la protezione.

  I ricercatori hanno rilevato che l’archiviazione dei dati in ambienti multipli è una pratica comune, responsabile del 40% delle violazioni. Queste violazioni richiedono inoltre più tempo per essere individuate e gestite. In confronto, i dati conservati in un singolo tipo di ambiente hanno subito meno violazioni: 25% nel cloud pubblico, 20% on-premise e 15% nel cloud privato.
- **2,22 milioni di dollari è il risparmio sui costi** derivanti dall’uso estensivo dell’AI nella prevenzione per le organizzazioni che hanno utilizzato ampiamente l’intelligenza artificiale e l’automazione della sicurezza nella prevenzione rispetto a quelle che non l’hanno fatto.
- +26,4% Aumento della carenza di competenze informatiche Più della metà delle organizzazioni vittime di violazioni si trovano ad affrontare elevati livelli di **carenza di personale addetto alla sicurezza**.
- 292 Giorni necessari per identificare e contenere le violazioni che coinvolgono credenziali rubate. Attacchi di phishing, hanno impiegato invece mediamente 261 giorni per essere contenuti, mentre gli attacchi di ingegneria sociale hanno richiesto circa 257 giorni.



Fonte immagine – Surfshark - “Data Breach Recap 2024”

A livello di distribuzione dei data breach, il report **“Data Breach Recap 2024” di Surfshark** rivela che **l’Europa ha registrato la quota più alta di violazioni di dati**, rappresentando il 29% degli account compromessi a livello globale, con oltre 1,6 miliardi di account violati, e la Russia in prima linea. Mentre l’Asia si posiziona come la seconda regione più colpita, con il 23% del totale globale, ovvero quasi 1,3 miliardi di account violati, con la Cina in testa. Il Nord America, invece, risulta occupare la terza posizione, rappresentando il 14% di tutte le violazioni, con quasi 770 milioni di account compromessi, principalmente negli Stati Uniti.

Qual è la causa principale delle violazioni dei dati?

Attacchi esterni e vulnerabilità interne

Le violazioni dei dati nel 2024 sono principalmente causate da una **combinazione di attacchi esterni e di vulnerabilità interne** e di seguito una panoramica delle cause principali scaturite dai report di IBM-Ponemon Institute e Verizon:

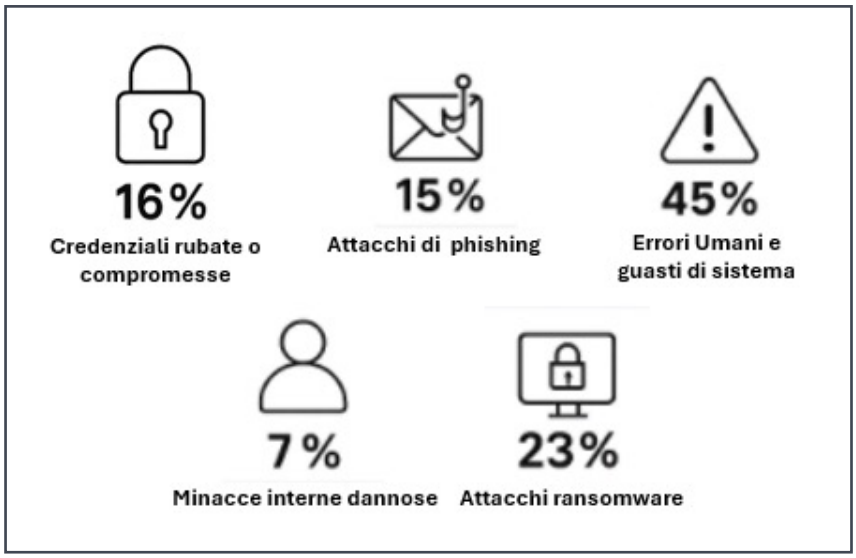


Immagine creata con icone e riflettente percentuali raccolte dai report IBM e Verizon

- **Credenziali rubate o compromesse (16% delle violazioni)** - Gli aggressori ottengono dettagli di accesso validi tramite metodi come phishing, ingegneria sociale o acquisto di credenziali dal dark web. Una volta all'interno, possono navigare nei sistemi senza essere rilevati. Inoltre, le password deboli o riutilizzate possono essere facilmente indovinate dagli aggressori e, se un dipendente usa la stessa password su più servizi, una violazione di un servizio può portare a una compromissione in un altro, inclusi i sistemi dell'organizzazione. Ancora, l'accesso a siti Web non attendibili può portare a violazioni dei dati.
- **Attacchi di phishing (15% delle violazioni)** - Il phishing rimane un metodo prevalente grazie alla sua efficacia nell'ingannare gli utenti inducendoli a rivelare informazioni sensibili o a installare malware

- **Errori umani e guasti di sistema (45% delle violazioni)** - Ciò può includere la condivisione accidentale di dati sensibili, la configurazione errata di database, l'invio di dati sensibili al destinatario sbagliato o persino la perdita di dispositivi contenenti dati sensibili, evidenziando l'importanza delle misure di sicurezza sia umane sia tecniche. È importante sottolineare che la perdita di dati può verificarsi anche attraverso i vari canali di comunicazione utilizzati dai dipendenti, inclusi i dispositivi mobili, per l'invio e l'archiviazione dei dati in diverse sedi. Inoltre, la mancata osservanza da parte dei dipendenti delle procedure per la prevenzione della perdita di dati e per l'uso corretto delle informazioni aziendali può consentire a parti non autorizzate di accedere a dati sensibili dell'organizzazione, provocando così perdite e violazioni di dati.
- **Minacce interne dannose (7% delle violazioni)** - Gli attacchi che coinvolgono attori dannosi all'interno di un'organizzazione comportano rischi sostanziali. Gli insider possono copiare o rubare i dati aziendali, compresi dati proprietari e informazioni riservate o sabotare sistemi. Ciò spesso comporta costi più elevati e tempi più lunghi per il rilevamento e il contenimento.
- **Attacchi ransomware (23% delle violazioni)** - Gli aggressori ransomware crittografano i dati critici e richiedono il pagamento di un riscatto per il loro rilascio, causando significative interruzioni operative e perdite finanziarie. La prevalenza del ransomware riflette lo spostamento degli aggressori verso metodi che massimizzano l'impatto e la redditività.

Inoltre, è doveroso ricordare che le vulnerabilità nel software possono essere, altresì, sfruttate dagli aggressori se non vengono prontamente corrette. Pertanto, le organizzazioni che non riescono a mantenere aggiornati i software e i sistemi sono a maggior rischio di violazioni dei dati.

Violazione dei dati per settore

I diversi settori affrontano sfide specifiche in materia di sicurezza informatica, in base alla natura delle loro attività, al valore dei dati che gestiscono e ai contesti normativi in cui operano. Vediamo i dati salienti riportati nel report di IBM.

Settore Sanitario

9,77 milioni di dollari

costo medio di una violazione nel settore

È il settore più costoso per quanto riguarda le violazioni dei dati. Nel 2024, il costo medio di una violazione nel settore sanitario è stato di **9,77 milioni di dollari**, segnando il tredicesimo anno consecutivo con i **costi di violazione più elevati tra tutti i settori**.

Le ragioni principali per cui il settore sanitario è particolarmente vulnerabile includono:

- **Dati sensibili dei pazienti** - Le organizzazioni sanitarie archiviano grandi quantità di informazioni personali, come anamnesi e diagnosi, che sono molto preziose sul mercato nero.
- **Conformità normativa** - La non conformità comporta pesanti multe e sanzioni, aumentando il costo delle violazioni.
- **Impatto operativo** - Gli attacchi informatici possono interrompere servizi sanitari critici, mettendo a rischio la vita dei pazienti. Ad esempio, gli attacchi ransomware possono ritardare i trattamenti e compromettere l'assistenza.

Settore Finanziario

È continuamente sotto assedio, rimanendo un obiettivo primario per i criminali informatici grazie all'accesso diretto ad asset monetari e informazioni finanziarie sensibili. Il costo medio di una violazione dei dati nel settore finanziario è stato di 6,08 milioni di dollari, superiore alla media globale nei vari settori. Di seguito i principali fattori di rischio e impatti per il settore finanziario:

6,08 milioni di dollari

costo medio di una violazione nel settore

- **Multe regolamentari** -Le varie normative (GDPR, NIS2, DORA, PCI-DSS, ecc.) aumentano l'onere finanziario post-violazione attraverso requisiti di applicazione severi.
- **Perdite finanziarie** - Furti, frodi e interruzioni operative causano impatti finanziari immediati e significativi.
- **Aumento del danno reputazionale** - La fiducia è cruciale nel settore finanziario, e le violazioni erodono questa fiducia, portando alla perdita di clienti e difficoltà nell'acquisizione di nuovi clienti.

Settore Industriale

Il settore - che include anche produzione e infrastrutture critiche - ha registrato il **più alto aumento dei costi di violazione dei dati**. Inoltre, la sempre maggiore convergenza dei sistemi IT (Information Technology) ed OT (Operation Technology) ha ampliato la superficie di attacco. Di seguito i dati più salienti del 2024:

Aumento del costo medio delle violazioni - Il settore ha visto un incremento medio di $830.000 per violazione rispetto all'anno precedente.

Tempo medio di identificazione e contenimento - Le violazioni hanno richiesto in media 219 giorni per essere identificate e 85 giorni per essere contenute, superando la media complessiva.

Inoltre, il settore industriale si caratterizza per vulnerabilità specifiche, quali:

- **Sensibilità ai tempi di inattività** - Le interruzioni possono bloccare le linee di produzione, causando perdite di fatturato significative e ritardi nella supply chain.
- **Dipendenze della supply chain** - Gli attacchi provocano effetti a cascata lungo la supply chain, amplificando il danno complessivo.
- **Sistemi legacy** - Vecchi sistemi di controllo industriale spesso mancano di funzionalità di sicurezza moderne, rendendoli vulnerabili.
- **Rischi cyber-fisici** - Gli attacchi possono avere conseguenze fisiche, inclusi danni alle apparecchiature e rischi per la sicurezza umana. Inoltre, i software e i sistemi sono a maggior rischio di violazioni dei dati.

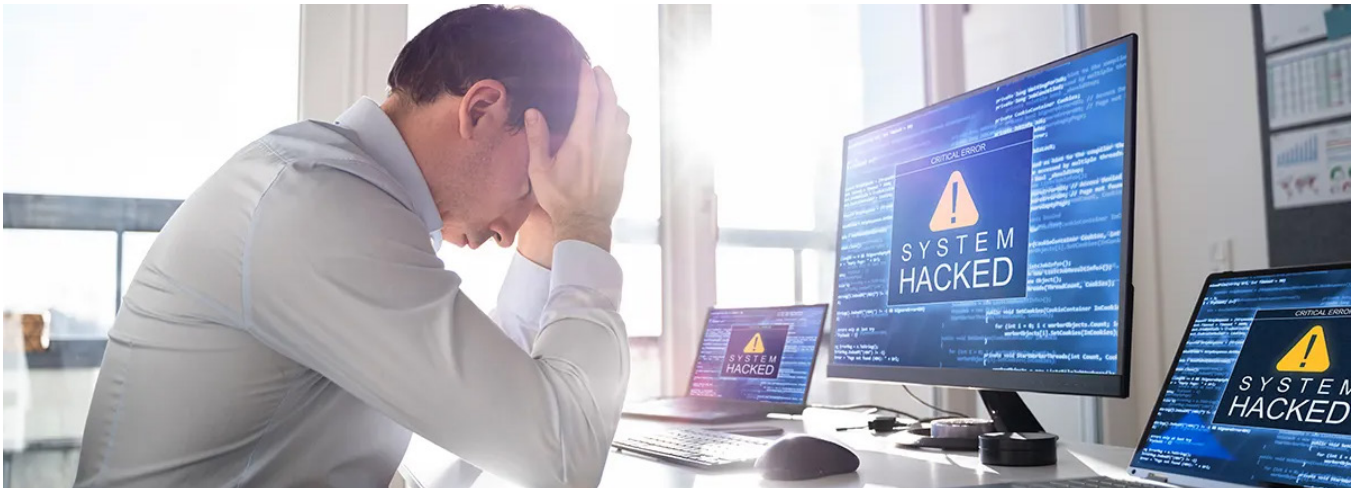
Perché è importante prevenire la perdita di dati?

Conseguenze dirette

Le violazioni dei dati comportano rischi significativi sia per le organizzazioni sia per gli individui, con conseguenze di vasta portata. Di seguito le principali motivazioni per cui è importante evitare la perdita di dati:

1. **Perdite finanziarie** - I costi diretti derivanti dalla risposta alle violazioni e i costi indiretti derivanti dall'interruzione delle attività possono essere sostanziali.
2. **Danni alla reputazione** - La perdita di fiducia dei clienti porta a una diminuzione dei ricavi e a danni al marchio a lungo termine.
3. **Conseguenze legali e normative** - Le sanzioni normative sono in aumento, con sanzioni più elevate per la non conformità. Inoltre, requisiti di reporting sempre più severi comportano controlli e costi aggiuntivi.
4. **Interruzione operativa** - Tempi di inattività significativi ostacolano la produttività e influiscono sulla fornitura del servizio.
5. **Rischi della supply chain** - Le violazioni di terze parti possono avere un impatto diretto sulla tua organizzazione, estendendo le vulnerabilità oltre il controllo immediato.

Pertanto, il riconoscere gli aspetti appena illustrati è il primo passo verso l'implementazione di strategie di prevenzione efficaci per proteggere i dati riservati o sensibili delle aziende.



Che cos’è la Data Loss Prevention (DLP)?

La DLP si riferisce a **strategie, strumenti e pratiche volte a rilevare e prevenire l’accesso non autorizzato**, il trasferimento o l’esposizione di dati aziendali sensibili. Le soluzioni DLP **aiutano le organizzazioni a rilevare e prevenire violazioni dei dati, esfiltrazioni o distruzioni indesiderate di dati sensibili**. È essenziale per le organizzazioni proteggere i propri dati sensibili e mantenere la conformità ai requisiti normativi.

Elementi chiave

Gli elementi chiave del DLP includono:

- **Identificazione dei dati**: classificazione e taggatura dei dati sensibili.
- **Visibilità dei dati:** monitoraggio dell’accesso e dello spostamento dei dati tra i sistemi.
- **Controllo degli accessi**: limitazione dell’accesso ai dati in base ai ruoli e alle autorizzazioni degli utenti.

Tipi di DLP

Endpoint, network o cloud

La DLP può essere di tre tipi, a seconda dei diversi ambienti aziendali a cui sono rivolte le soluzioni e le pratiche.

1. **Endpoint DLP** – I dati sui dispositivi degli utenti finali – quali laptop, smartphone e desktop – sono protetti, monitorando e controllando le attività che potrebbero portare a violazioni dei dati. Ad esempio, sono bloccati i trasferimenti di file non autorizzati da un laptop aziendale a un'unità esterna.

2. **Network DLP** – I dati in transito sulla rete, sono monitorati e protetti, impedendo trasferimenti di dati non autorizzati e assicurando che le informazioni sensibili non lascino la rete dell'organizzazione - quali la protezione delle comunicazioni e-mail, della messaggistica istantanea e dei trasferimenti di file. Ad esempio, si limitano gli allegati contenenti dati sensibili alle e-mail a destinatari esterni.

3. **Cloud DLP** - I dati archiviati nei servizi cloud sono salvaguardati applicando policy e controlli di sicurezza per impedire l'accesso non autorizzato e la perdita di dati da ambienti basati su cloud, quali: Google Drive, Dropbox e AWS. Ad esempio: si impediscono i download non autorizzati di file sensibili da una cartella cloud condivisa.

Come gestire le sfide di DLP

Implementazione della DLP

L'implementazione di una strategia efficace di DLP è cruciale per le organizzazioni al fine di proteggere i dati, soprattutto quelli sensibili come le informazioni di identificazione personale (PII – Personally Identifiable Information) e i dati finanziari. Tuttavia, ci sono diverse sfide che possono ostacolare tale obiettivo. Di seguito le principali sfide DLP e le relative strategie per superarle:

Identificazione dei dati sensibili

Sfida - Le organizzazioni devono sviluppare metodi per identificare accuratamente i dati sensibili - quali le informazioni personali identificabili (PII), i dati aziendali critici e le informazioni finanziarie - che necessitano di protezione.

Soluzione - Utilizzare strumenti DLP automatizzati che utilizzano l'apprendimento automatico per analizzare e classificare i dati. Tali strumenti possono essere addestrati a riconoscere varie

Gestione degli accessi

Sfida - Le organizzazioni devono garantire che i dipendenti abbiano l'accesso necessario ai dati aziendali, impedendo al contempo a utenti non autorizzati di accedere a informazioni sensibili.

Soluzione - È fondamentale stabilire rigorose politiche di controllo degli accessi per garantire che solo le persone autorizzate possano accedere ai dati sensibili. Alcune soluzioni DLP permettono di implementare policy di accesso basate sui ruoli e controllare regolarmente i log di accesso per garantire che solo il personale autorizzato abbia accesso ai dati sensibili, oltre a permettere di implementare l'autenticazione a più fattori e i principi del minimo privilegio. Ciò può portare a un'efficienza operativa e a una sicurezza bilanciate.

Monitoraggio e rilevamento

Sfida - È sempre più complesso monitorare lo spostamento e l'archiviazione dei dati quando sono distribuiti tra repository cloud, servizi di archiviazione cloud per i consumatori e server locali.

Soluzione - Le organizzazioni devono disporre di strumenti di Data Loss Prevention (DLP) in grado di offrire una copertura completa su tutte le piattaforme in cui i dati vengono archiviati o elaborati. È fondamentale che questi strumenti siano in grado di monitorare in tempo reale il trasferimento e l'archiviazione dei dati, garantendo visibilità su dove i dati sono collocati, come vengono utilizzati e chi vi accede.

Protezione dalle minacce interne

Sfida - Le minacce interne, ovvero i casi in cui dipendenti o collaboratori abusano dell'accesso a dati sensibili, rappresentano un rischio significativo.

Soluzione - Si possono implementare rigidi controlli di accesso e suddividere le responsabilità tra i dipendenti, oltre a condurre controlli approfonditi sui precedenti dei nuovi assunti. È altrettanto importante migliorare le misure di sicurezza fisica, mantenere un ambiente di lavoro positivo e stabilire procedure chiare sia per gli audit in corso che per la gestione dei dipendenti in uscita.

Mini Roadmap per implementare una soluzione di DLP

Di seguito una mini-roadmap con gli aspetti - in sequenza - che un'azienda deve considerare quando decide di implementare una soluzione di DLP. E, precisamente:

1. **Comprensione dei dati** - È essenziale che i team di sicurezza IT collaborino con i diversi reparti dell'organizzazione per identificare i tipi di dati da proteggere e i documenti riservati. Il dialogo facilita l'implementazione di politiche e regole efficaci per la classificazione dei dati.
2. **Sviluppo globale delle policy** - Le policy di DLP devono coprire ogni aspetto della protezione dei dati, inclusa la classificazione dei dati, i ruoli utente e i livelli di accesso, definendo chiaramente la gestione, la trasmissione e l'archiviazione dei dati. Le policy devono essere chiare, applicabili e riviste regolarmente per garantirne l'efficacia e la pertinenza.
3. **Formazione e consapevolezza dei dipendenti** - La formazione dei dipendenti è cruciale per il successo della soluzione DLP. I dipendenti devono essere istruiti sull'importanza della sicurezza dei dati e sul loro ruolo nella protezione delle informazioni sensibili. Sessioni di formazione regolari e programmi di sensibilizzazione assicurano che i dipendenti comprendano e rispettino le policy DLP. Dimostrazioni pratiche da parte del fornitore possono migliorare l'implementazione del prodotto.
4. **Monitoraggio e risposta agli incidenti** - È fondamentale implementare meccanismi solidi per il monitoraggio e la risposta agli incidenti. La soluzione DLP deve monitorare i flussi di dati e rilevare potenziali violazioni. Un piano efficace di risposta agli incidenti è altresì essenziale per affrontare rapidamente gli eventi di perdita di dati, mitigare i danni e prevenire futuri incidenti simili.
5. **Audit e aggiornamenti regolari** - Condurre audit e garantire aggiornamenti regolari è cruciale per mantenere un programma di DLP efficace. Gli audit identificano eventuali lacune nell'implementazione della strategia DLP, mentre gli aggiornamenti delle soluzioni e delle policy DLP, basati sui risultati degli audit e sulle minacce emergenti, aiutano a mantenere un programma solido e aggiornato.

Soluzioni di DLP: leve strategiche per la conformità alle normative regionali e internazionali

Le soluzioni di DPL sono essenziali per garantire la conformità alle normative regionali e internazionali.

Normative europee e standard internazionali richiedono l'adozione di **misure tecniche e organizzative adeguate**, in cui le soluzioni DLP giocano un ruolo cruciale. Tra questi, si annoverano lo standard ISO/IEC 27001, i regolamenti GDPR, DORA, PCI-DSS e la direttiva NIS 2, che prescrivono requisiti specifici. Ma vediamo più in dettaglio di cosa si tratta.

- **ISO 27001** - Lo standard definisce i requisiti per un Information Security Management System (ISMS). L'ALLEGATO A specifica controlli per prevenire la perdita di dati, come il controllo A.8.8 per la protezione delle informazioni sensibili e il controllo A.9.4.1 focalizzato sul monitoraggio degli accessi, elementi chiave delle soluzioni DLP.
- **GDPR** - Il regolamento impone alle organizzazioni di adottare misure rigorose per proteggere i dati personali dei cittadini dell'UE, con sanzioni severe per la non conformità. Le soluzioni DLP aiutano le aziende a identificare e proteggere i dati sensibili, monitorare i flussi di dati e documentare i processi di protezione, dimostrando la conformità durante gli audit.
- **PCI-DSS** - Stabilisce regole per garantire che le organizzazioni che gestiscono dati di carte di credito mantengano un ambiente sicuro, prevenendo la perdita di dati.
- **DORA** - Riguarda principalmente il settore finanziario e assicurativo, obbligando le organizzazioni a implementare controlli tecnici per prevenire l'esfiltrazione non autorizzata di dati, effettuare valutazioni di rischio, e mantenere elevati standard di sicurezza dei dati.
- **NIS 2** - Introduce un quadro normativo per la resilienza informatica delle infrastrutture critiche, richiedendo agli operatori di servizi essenziali di implementare sistemi di monitoraggio e prevenzione delle fughe di dati, e di rilevare tempestivamente incidenti di sicurezza.
- **AI ACT** - Stabilisce che la protezione dei dati deve essere garantita lungo l'intero ciclo di vita dei sistemi di AI, con misure allineate a quelle del GDPR per la protezione della privacy e la sicurezza dei dati personali.

Le soluzioni di CyberGrant per la DLP

Cyber Grant Inc., società con sede a Menlo Park (California), offre sul mercato le soluzioni avanzate **FileGrant Enterprise** e **RemoteGrant** che integrano la protezione degli endpoint e il monitoraggio delle applicazioni, prevenendo la perdita di dati attraverso il controllo degli accessi e la crittografia automatica dei file. Vediamo in dettaglio le caratteristiche di queste due soluzioni in termini di DLP:

FileGrant

È particolarmente adatto come soluzione di DLP per diversi motivi, quali:

- **È applicabile a diverse tipologie di file** - La crittografia avanzata utilizzata copre un'ampia gamma di formati, inclusi PDF, documenti Office, audio, video, immagini e testi.
- **Utilizza la crittografia standard AES-256** – Crittografia Leader di mercato per garantire la massima sicurezza nei documenti cifrati.
- **Utilizza la crittografia in modalità offline** - Assicura che i file rimangano protetti anche in modalità offline, grazie alla crittografia «a riposo».
- **Possiede la crittografia integrata nel PDF** - Permette di integrare i file crittografati direttamente nel PDF, consentendo un'anteprima sicura con qualsiasi lettore PDF.
- **Garantisce la sicurezza via API** - I file possono essere rapidamente crittografati e protetti con una semplice chiamata API.
- **Offre la crittografia manuale intuitiva** - La crittografia manuale è disponibile tramite un'interfaccia grafica intuitiva, rendendo la protezione accessibile a tutti gli utenti.
- **Garantisce il totale controllo dei documenti** - Offre la possibilità di terminare l'accesso ai contenuti immediatamente, impedendo copia, modifica e stampa per preservare l'integrità e la sicurezza.
- **Blocca il data scraping dell'IA** - Protegge da sistemi IA come CoPilot o ChatGPT per salvaguardare i diritti

d'autore e la proprietà intellettuale.

- **Garantisce il controllo utenti e condivisioni** - Gli amministratori possono monitorare i file e le condivisioni degli utenti per motivi di sicurezza, senza accedere ai contenuti.
- Offre alti livelli di protezione grazie al Viewer proprietario – Impedisce la cattura dello schermo durante le videoconferenze e l'uso di tool per il ritaglio e la proiezione dei documenti.

RemoteGrant

La soluzione di DLP RemoteGrant permette alle aziende di:

- **Bloccare l'esfiltrazione dei dati** - La funzionalità previene il trasferimento non autorizzato di dati dal dispositivo, assicurando che le informazioni sensibili rimangano protette.
- **Mitigare l'Errore Umano** - È ridotto il rischio di violazioni dei dati che possono derivare da un uso improprio o accidentale del contenuto del dispositivo.
- **Garantire limiti operativi senza frizioni** – Sono limitate le azioni senza compromettere l'esperienza dell'utente, mantenendo la produttività e migliorando la sicurezza.
- **Controllare l'accesso ai file sensibili** - Monitora e gestisce le applicazioni che possono accedere ai file sensibili, proteggendoli da utilizzi non autorizzati e bloccando l'accesso in assenza di un'autorizzazione chiara, oltre ad operare a livello di sistema operativo per proteggere gli ambienti di lavoro sia online sia offline

Inoltre, RemoteGrant si caratterizza per:

- Coniugare la DLP con l'approccio Zero Trust Application, fornendo una protezione completa e trasparente all'interno dell'organizzazione.
- Offrire un controllo granulare delle applicazioni, come PowerShell, e supportare ambienti virtuali e connessioni remote, proteggendo i dati in contesti di lavoro ibrido.
- Assicurare che i dati nei CRM non possano essere scaricati o manipolati senza autorizzazione, offrendo un livello di sicurezza superiore rispetto all'accesso tramite browser convenzionali.
- Offrire un funzionalità avanzata - brevettata da CyberGrant - per nascondere le porte RDP, aumentando la sicurezza delle connessioni remote.
- Essere dotata di un'avanzata tecnologia di rilevamento delle minacce che sfrutta ben 75 antivirus per identificare in tempo reale le attività di phishing e di altre minacce.
- Offrire policies di sicurezza on-demand, consentendo una personalizzazione flessibile per affrontare richieste di sicurezza uniche, creando template di protezione personalizzati che rispondono esattamente ai bisogni delle aziende.

FileGrant Enterprise & RemoteGrant: leve strategiche per la conformità normativa

Entrambe le soluzioni di CyberGrant facilitano la conformità normativa, offrendo alle aziende gli strumenti necessari per soddisfare e superare le rigorose esigenze delle normative sulla protezione dei dati, sulla privacy e sulla cyber resilience. Vediamo di seguito come.

- **GDPR** - Le soluzioni garantiscono la protezione dei dati personali e la privacy, supportando la conformità attraverso la crittografia dei dati, pratiche sicure di gestione dei dati e funzionalità incentrate sulla privacy.
- **NIS2** - Le soluzioni allineano le operazioni alla direttiva utilizzando misure di sicurezza, inclusi la registrazione di attività sensibili e controlli avanzati di accesso.
- **DORA** - Le soluzioni contribuiscono al rispetto dei requisiti attraverso la registrazione di attività sensibili, la crittografia dei dati e dei documenti finanziari e il controllo degli accessi.

In sintesi, FileGrant e RemoteGrant sono propedeutiche a garantire un approccio strutturato alla cybersecurity e alla gestione dei dati rivelandosi investimento strategico, oltre a generare un vantaggio competitivo e garantire l'adempimento agli obblighi normativi in materia di sicurezza dei dati e cybersecurity.

Conclusioni

Le tecnologie di DLP sono fondamentali per la **protezione delle informazioni sensibili**, con un'importanza accentuata dai requisiti normativi e dall'**evoluzione delle minacce cyber.** Queste soluzioni offrono nuove prospettive per una sicurezza proattiva ed efficace. Le soluzioni di DLP, di fatto, non solo migliorano la visibilità sui dati e prevengono le perdite, ma **ottimizzano la risposta agli incidenti e il ripristino, oltre a rafforzare le difese e aumentano la resilienza contro gli attacchi informatici**.

In sintesi, in un contesto normativo in continua evoluzione, focalizzato sulla sicurezza dei dati e la cybersecurity, **l'adozione di soluzioni DLP è essenzial**e. Non rappresenta solo una scelta strategica, ma diventa **un obbligo per assicurare la resilienza e la fiducia nell'economia digitale**.

A cura di **Federica Maria Rita Livelli**

www.cybergrant.net