Panoramica sulla soluzione

Previeni le fughe dei dati dalla tua azienda

La maggior parte delle aziende è vittima di fughe di dati. A volte i dati spariscono sottratti da personale interno ma più spesso vengono rubati da aggressori esterni, in modi diversi e per mezzo di canali differenti. Le aziende stanno tentando di mettere un freno a questo flusso in uscita, per motivi diversi e con maggiore o minore successo. Intel Security ha commissionato l'*Intel Security 2016 Data Protection Benchmark Study* (Analisi di benchmarking sulla protezione dei dati 2016) per comprendere a fondo le persone responsabili di questi furti, i tipi di dati che vengono sottratti e il modo in cui escono dalle aziende.

Nel *Report McAfee Labs sulle Minacce: settembre 2016*, abbiamo analizzato i dati del sondaggio ed elencato i risultati, fra cui:

- Il divario fra la perdita dei dati e il rilevamento della violazione è sempre più ampio.
- Gli operatori del settore sanitario e le industrie sono dalle mercé degli aggressori.
- L'approccio tipico alla prevenzione della fuga di dati è sempre meno efficace contro i nuovi obiettivi dei furti.
- La maggior parte delle imprese tende a sottovalutare il secondo metodo più comune di fuga di dati.
- La prevenzione delle fughe di dati viene implementata per le giuste motivazioni.
- La visibilità è fondamentale.

Policy e procedure raccomandate per un'efficace prevenzione delle fughe di dati

È essenziale per le aziende creare policy e procedure di prevenzione delle fughe di dati per prevenire i trasferimenti involontari o volontari di dati sensibili a terzi non autorizzati. Un'efficace iniziativa di prevenzione delle fughe di dati inizia con la fase di pianificazione durante la definizione dei requisiti aziendali. Ad esempio, l'allineamento della classificazione dei dati e delle policy sulla fuga di dati alle policy sulla privacy e agli standard di condivisione dei dati dell'azienda deve essere effettuato nella fase di pianificazione. Fissare dei solidi requisiti aziendali consente di mettere a fuoco l'iniziativa di prevenzione delle fughe di dati e di incentivare la protezione.

intel Security

Panoramica sulla soluzione

Un ulteriore passaggio importante in un'iniziativa di prevenzione delle fughe di dati è l'identificazione dei dati sensibili all'interno dell'azienda. Le tecnologie di scansione di server ed endpoint consentono la classificazione dei file basata su espressioni regolari, dizionari e tipi di dati non strutturati. I prodotti di prevenzione delle fughe di dati assicurano in genere classificazioni incorporate per categorie tipiche di dati sensibili come i dati delle carte di pagamento o le informazioni sanitarie personali, che possono accelerare il processo di identificazione. È anche possibile creare classificazioni personalizzate per identificare i tipi di dati univoci per l'azienda.

A complicare questo passaggio ci si mettono sia le applicazioni omologatee non omologate dal reparto IT e i relativi dati di supporto nel cloud. Per i dati omologati dal reparto IT nel cloud, l'identificazione dei dati sensibili può e deve far parte del processo quando ci si abbona al servizio cloud. Quando ciò avviene, la classificazione di questo tipo di dati può essere relativamente semplice.

Tuttavia, i gruppi funzionali all'interno delle aziende aggirano spesso il reparto IT per soddisfare i propri obiettivi aziendali abbonandosi a servizi cloud per proprio conto. Se il reparto IT non è a conoscenza di questi servizi e dei dati che li supportano, si verifica un incremento del potenziale per fughe di dati. Di conseguenza, durante questo passaggio è essenziale collaborare con i gruppi funzionali per identificare le posizioni dei dati nel cloud e per utilizzare il processo precedente per classificare tali dati.

Una volta completato il processo di rilevamento dei dati sensibili, l'implementazione dei prodotti di prevenzione delle fughe di dati all'interno della rete affidabile e su tutti gli endpoint può assicurare la visibilità e il controllo su importanti dati a riposo e dati in fuga. È essenziale implementare le policy per rilevare l'accesso o lo spostamento imprevisto di dati sensibili. Eventi come il trasferimento di dati sensibili sui dispositivi USB o tramite la rete in una posizione esterna potrebbe far parte di un normale processo aziendale o potrebbe invece essere un'azione intenzionale o involontaria che comporta una fuga di dati.

Una formazione correttamente sviluppata sulla consapevolezza della sicurezza può consentire di ridurre la probabilità di violazioni dei dati. Schermate giustificate possono addestrare gli utenti sulle azioni appropriate riguardo al trasferimento di dati sensibili e permettere loro di essere formati sulle policy di protezione dei dati nel corso della loro normale giornata di lavoro. Ad esempio, una schermata giustificata può notificare agli utenti che il trasferimento dati che stanno effettuando è contrario alle policy e fornire alternative al completamento del trasferimento, come l'oscuramento dei dati sensibili prima di tentare di nuovo il trasferimento.

I titolari dei dati sono in genere a conoscenza di come vengono usati i loro dati rispetto ad altre persone all'interno dell'azienda. Ai titolari dei dati deve essere assegnato il compito di smistare gli incidenti di fughe di dati. Separare i doveri tra i titolari dei dati e il team di sicurezza riduce la possibilità che un unico team aggiri le policy di protezione dei dati.

Una volta che gli spostamenti di dati approvati sono stati stabiliti e che le policy che disciplinano tali spostamenti sono state incorporate nei prodotti per la prevenzione delle fughe di dati, è possibile attivare le policy per il blocco dei trasferimenti non approvati di dati sensibili. Con il blocco attivato, agli utenti viene impedito di eseguire azioni che contravvengono alle policy. Le policy possono essere perfezionate per garantire la flessibilità in base ai requisiti dell'azienda per assicurare che gli utenti siano in grado di compiere le loro mansioni e di essere al contempo protetti.

Man mano che l'iniziativa per la prevenzione delle fughe di dati procede, è importante convalidare e perfezionare le policy a intervalli pianificati. Talvolta le policy sono troppo restrittive o troppo blande, con conseguente impatto sulla produttività o sui rischi per la sicurezza.

Cosa può fare Intel Security per aiutarti a proteggerti dall'esfiltrazione dei dati

McAfee DLP Discover

Il primo passo per proteggere correttamente i dati è capire dove risiedano le informazioni e quale sia esattamente la natura di quei dati. McAfee DLP Discover protegge contro l'esfiltrazione dei dati semplificando il primo passaggio mediante le seguenti funzionalità:

- Identifica le classificazioni per svolgere il rilevamento nell'ambiente affidabile usando le categorie predefinite (per esempio HIPAA, PCI, SOX) oppure creandone di personalizzate.
- Esegue una scansione e revisione dell'inventario usando le classificazioni identificate per capire quali tipi di dati risiedono nell'ambiente affidabile dove. Esamina le violazioni della policy esistente nell'interfaccia di McAfee DLP Discover.
- Esegue una scansione di remediation per trovare i dati memorizzati in siti non autorizzati e spostarli in una posizione autorizzata.
- Le scansioni di inventario e remediation possono essere svolte sulle risorse locali, come le condivisioni di rete, oppure sulle risorse nel cloud, come Box.
- Crea nuove policy di protezione dati basate sui risultati delle scansioni di McAfee DLP Discover.

McAfee DLP Endpoint

McAfee DLP Endpoint monitora e previene il trafugamento dei dati in sede, fuori sede e nel cloud. Monitora rapidamente gli eventi in tempo reale, applica le policy di sicurezza gestite centralmente e genera analisi dettagliate e report sulla proliferazione senza compromettere le operazioni quotidiane.

- Dopo il completamento della fase di scoperta, crea delle policy di protezione dati e ne segnala le violazioni. Ciò fornisce i dati necessari a capire meglio i movimenti dei dati all'interno dell'aziendae consente l'imposizione delle regole di blocco. McAfee DLP incorpora delle classificazioni (per esempio HIPAA, SOX, PCI e ITAR) che possono essere usate per identificare i dati all'interno dell'organizzazione.
- Crea delle schermate che guidano gli utenti verso una migliore comprensione delle policy di protezione dei dati, durante i loro trasferimenti quotidiani. Queste finestre a comparsa personalizzabili sono estremamente utili e riducono i trasferimenti rischiosi dei dati da parte dei dipendenti.
- Esaminando il Gestore eventi si possono identificare le proprietà dei dati in trasferimento alle posizioni non autorizzate, ad esempio la modalità del trasferimento e l'autore dello stesso.
- Dopo che le policy di protezione dei dati sono state create e affinate in base ai requisiti dell'azienda, viene abilitato il blocco dei trasferimenti non autorizzati dei dati.
- Attivando le classificazioni manuali si consente agli utenti di classificare i documenti che sono stati creati. Potenzialmente i titolari dei dati sono in grado di capire meglio la sensibilità dei documenti, nel caso in cui il motore di classificazione automatizzata non riesca a rilevare alcun dato strutturato. Ciò è integrato in McAfee DLP Endpoint senza alcuno strumento aggiuntivo di terzi.
- Per maggior protezione, si crea e implementa una Regola di protezione dell'accesso all'applicazione che utilizzi McAfee Threat Intelligence Exchange per impedire alle applicazioni sconosciute di accedere ai dati sensibili. In tal modo si consente il trasferimento dei dati sensibili alle applicazioni autorizzate ma vi si impedisce l'accesso a quelle non verificate oppure ostili.

McAfee DLP Monitor

McAfee DLP Monitor raccoglie, tiene traccia e crea report sui dati in movimento nell'intera rete. Scopri facilmente le minacce sconosciute ai dati e prendi delle misure per proteggerli.

- Attiva le policy integrate pertinenti per rilevare le potenziali violazioni nella rete.
- Crea ulteriori policy e regole personalizzate, come il monitoraggio dei trasferimenti di dati sensibili nel cloud.
- Conduci un'analisi forense per correlare gli eventi di rischio attuali e passati, individuare le tendenze di rischio e identificare le minacce. McAfee DLP Monitor consente agli esperti della sicurezza di comprendere rapidamente la situazione e di sviluppare regole e policy per affrontarla.
- Crea ulteriori filtri di acquisizione per escludere i dati non rilevanti e per affinare le regole al fine di ridurre i falsi positivi.
- Configura gli allarmi per inviare le notifiche di un'avvenuta violazione delle policy a mittenti, destinatari, titolari dei dati e amministratori di sistema.

McAfee DLP Prevent

McAfee DLP Prevent protegge contro la perdita dei dati garantendo l'uscita dei dati dalla rete solo quando è corretta, tramite email, webmail, messaggistica immediata, wiki, blog, portali, HTTP/HTTPS o trasferimenti via FTP. Spesso la rapidità dell'identificazione e mitigazione dei tentativi di trafugamento fa la differenza tra mantenere al sicuro i dati importanti e il finire sulle prime pagine dei giornali.

- Integra McAfee DLP Prevent con i proxy web o gli agent di trasferimento dei messaggi, usando le policy incorporate per impedire i trasferimenti di dati non autorizzati tramite i gateway di posta o i proxy web.
- Crea delle regole in McAfee DLP Prevent per consentire o bloccare i documenti sensibili in base alla percentuale di corrispondenza.
- Usa i modelli DLP integrati per impedire il trasferimento dei dati sensibili nel cloud.
- Leggi i report degli eventi di sicurezza e regola le policy per ridurre i falsi positivi e massimizzare la continuità aziendale.
- Configura gli allarmi per inviare le notifiche di un'avvenuta violazione delle policy a mittenti, destinatari, titolari dei dati e amministratori di sistema.

Ulteriori letture

Comunità Intel Security Expert Center

- McAfee Data Loss Prevention

914_0816_brf_preventing-data-leak-organization

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com