Checklist:
cinque segnali che indicano la necessità di aggiungere la prevenzione della perdita dei dati alla tua attività di MSP

Perché i Service Provider dovrebbero occuparsi di prevenire la perdita dei dati?

Per anni, le organizzazioni hanno avuto difficoltà a proteggere i dati sensibili dagli accessi non autorizzati, dalla sottrazione dei dati perpetrata tramite attacchi esterni o dai rischi interni, come le configurazioni IT errate e gli errori umani. Le conseguenze di queste difficoltà sono sotto gli occhi di tutti: titoli imbarazzanti sui giornali, clienti danneggiati, sfiducia dei partner, perdite azionarie e sanzioni normative.

Con l'avvento delle tecnologie di prevenzione della perdita di dati basate sull'analisi comportamentale, gli MSP possono finalmente offrire e gestire i servizi DLP ottenendo il massimo valore con un impegno minimo e riducendo i rischi per i loro clienti.

È il momento di capitalizzare questa tendenza e garantire sonni tranquilli ai tuoi clienti, sapendo che i loro dati sono protetti nel pieno rispetto della conformità normativa.

"L'80% delle organizzazioni a livello mondiale riferisce di temere una potenziale violazione dei dati con conseguenze dirette sui dati dei clienti nei prossimi 12 mesi."

Fonte: Ponemon Institute, Cyber Risk Index Report, 2021

Verifica questi cinque segnali che indicano la necessità di aggiungere servizi DLP alla tua attività

1 Tramite i propri endpoint i dipendenti dei clienti possono accedere a dati sensibili (ad esempio, ai dati soggetti a normative)

Anche se i clienti archiviano i propri dati sensibili nel cloud, questi restano accessibili dalle workstation dei dipendenti e possono essere facilmente sottratti tramite i dispositivi periferici o i canali di rete, come l'e-mail e la messaggistica istantanea.

Secondo l'analisi di Verizon "Data Breach Investigation Report 2022", oltre l'80% delle violazioni dei dati avviene per motivi finanziari. Per questo gli attacchi mirano principalmente a dati di valore: informazioni soggette a normative, segreti commerciali o dati di proprietà intellettuale, che garantiscono ai criminali un profitto economico.

Se i collaboratori dei tuoi clienti creano, archiviano o lavorano con dati di questo tipo sui propri endpoint, è indispensabile che questi siano protetti dall'accesso da parte di utenti non autorizzati, per evitare che i clienti incorrano in gravi rischi finanziari, normativi e di reputazione.

2 Sei alla ricerca di nuove fonti di profitto per far crescere la tua azienda

Dal report di Acronis "Pulse of the MSP 2021" emerge che gli MSP individuano nella Cyber Security la loro principale fonte di profitto futura. Tuttavia, la maggior parte dei Service Provider che offre servizi di sicurezza gestiti si trova di fronte a un'agguerrita concorrenza.

L'avvento delle tecnologie DLP basate sull'analisi comportamentale rappresenta un fattore di differenziazione che ti consente di offrire servizi DLP fino a poco tempo fa non disponibili agli MSP e alle organizzazioni di piccole dimensioni. Erano infatti molto complessi, costosi da erogare e con lenta realizzazione del valore, perché difficili da associare ai processi aziendali in costante evoluzione e specifici di ogni cliente.

Le tecnologie DLP ti offrono oggi nuove fonti di profitto e la possibilità di erogare un servizio DLP interessante per organizzazioni di ogni dimensione, riducendo il rischio che i dati dei clienti finiscano nelle mani di persone non autorizzate.

3 I tuoi clienti appartengono a settori altamente regolamentati (healthcare, bancario e finanziario, pubblica amministrazione)

I clienti che trattano o archiviano informazioni di identificazione personale (PII), informazioni sanitarie (PHI), dati di carte di credito o qualsiasi altro tipo di dati sensibili in settori con alto grado di regolamentazione, richiedono un livello di protezione dei dati superiore al semplice backup.

La maggior parte delle normative, come GDPR, HIPAA e PCI-DSS, impone di segnalare violazioni e perdite di dati entro breve tempo dal loro verificarsi; nel caso di perdita di dati sensibili, le sanzioni economiche per i clienti possono essere molto elevate.

Le soluzioni di prevenzione della perdita di dati sono l'unica tecnologia in grado di monitorare i flussi di dati interni all'organizzazione e di prevenirne le perdite, incrementando la visibilità e facilitando le indagini sugli eventi DLP.

4 I tuoi clienti appartengono a settori molto soggetti al rischio di attacco e perdita di dati

Da sempre, alcuni settori presentano vulnerabilità di sicurezza più alte e al contempo archiviano dati sensibili di grande valore, il che li pone direttamente nel mirino dei criminali informatici. Ne sono esempi il settore dell'istruzione, dell'healthcare e altri settori pubblici nei quali l'accessibilità dei dati è un requisito ma, allo stesso tempo, serve una protezione efficace che ne impedisca la sottrazione.

Le tecnologie DLP basate sull'analisi comportamentale ti consentono di fornire un servizio DLP molto competitivo a un prezzo conveniente, per proteggere queste organizzazioni dai rischi di mancata conformità e di fuga dei dati.

5 I clienti stanno valutando e/o sottoscrivendo assicurazioni digitali per ridurre la responsabilità civile

Le assicurazioni digitali sono uno dei temi del momento in ambito di Cyber Security. I clienti si rivolgono agli assicuratori digitali per limitare la responsabilità civile della propria azienda in caso di violazioni dei dati.

Il costo di queste assicurazioni dipende da vari elementi, tra cui il fatturato annuale, il settore di appartenenza, il tipo e il volume di dati conservati e il livello di sicurezza dell'azienda. Considera l'aggiunta dei servizi di DLP alla tua offerta, per tutelare i requisiti di salvaguardia dei dati per le assicurazioni digitali e ridurre le spese dei tuoi clienti.

Advanced DLP

Advanced DLP per Acronis Cyber Protect Cloud aiuta i tuoi clienti a dormire sonni tranquilli, sapendo che i propri dati sensibili sono al sicuro dall'esportazione verso destinazioni non autorizzate. La sua tecnologia esclusiva, basata sull'analisi comportamentale, consente la creazione e la continua estensione di policy DLP conformi alle specifiche esigenze di ogni cliente, permettendoti di avviare i servizi con una semplicità mai vista prima e di generare valore con un impegno minimo.

Acronis

Per saperne di più visita www.acronis.com