Guida completa alla protezione dei dati

Forcepoint

Brochure

Panoramica

Per certi aspetti, il rapporto tra sicurezza dei dati e performance aziendali è una storia vecchia quanto il business. Dopotutto, la forma più semplice di vantaggio competitivo è la capacità che ha un'azienda di proteggere il suo "ingrediente segreto", che si tratti di un processo esclusivo, una proprietà intellettuale critica o una ricetta nel senso letterale del termine.

Oggi però la questione è molto più complessa. Si calcola che il 90% dei dati mondiali sia stato creato in appena due anni.[1] A ciò si aggiungano fattori come la proliferazione di dispositivi mobili, i rapporti tra clienti e fornitori a distanza, i dipendenti in remoto e in roaming e tanti altri ancora, per cui i dati sono conservati e accessibili in più luoghi, da più persone e in qualsiasi momento.

Sulla scia di questo cambiamento di ruolo dei dati sul posto di lavoro, le violazioni dei dati di alto profilo hanno contribuito a creare un nuovo business case per la sicurezza dei dati. L'impatto finanziario è un fattore importante, naturalmente; il costo medio di una violazione di dati è di 3,26 milioni di dollari.[2] In termini meno drastici, gli eventi imprevisti relativi alla sicurezza dei dati possono causare danni critici al marchio aziendale e alla fiducia dei clienti.

I settori fortemente regolamentati, come l'assistenza sanitaria e i servizi finanziari, sono da tempo soggetti a obblighi di legge per la protezione dei dati sensibili. Più di recente, tuttavia, la crescente attenzione del pubblico e una maggiore sensibilizzazione in fatto di sicurezza dei dati hanno portato all'emissione di nuove normative che disciplinano le modalità con cui le aziende possono raccogliere, trattare e conservare i dati: la legge malese sulla protezione dei dati personali, il regolamento generale sulla protezione dei dati dell'UE, i principi sulla privacy australiani, la legge californiana sulla privacy dei consumatori... L'elenco non finisce qui ed è sufficiente per indurre qualsiasi organizzazione, soggetta o meno alle normative vigenti, a pensare seriamente alla protezione dei dati.

3,26 milioni di dollari

Costo medio di una violazione dei dati[2]

2.600 - 10.000

Numero di dati sensibili persi in una violazione media[2]

68%

Percentuale di violazioni dei dati che non vengono scoperte per mesi[2]

In questa situazione, una cosa è ormai chiara: per consentire alle aziende e ai dipendenti di operare nel mondo del business oggi è necessario cambiare la logica con cui osserviamo la sicurezza dei dati. Nello stato di incessante evoluzione che è diventato la nuova norma, dei criteri reattivi non sono più sufficienti per proteggerci. Vediamo come adottare un atteggiamento proattivo verso la protezione dei dati e per quale motivo questa è una scelta sicura per le aziende moderne.

Si calcola che il 90% dei dati mondiali sia stato creato in appena due anni.[1]

Elevazione del ruolo della protezione dei dati

Per molti team di sicurezza dei dati, la giornata di lavoro è scandita dall'arrivo di un allarme, l'indagine successiva e i processi di remediation del danno. E il ciclo si ripete senza sosta. Il problema? Delle policy rigide spesso lanciano l'allarme per attività a basso rischio, generando una serie di "falsi positivi". Questi vanno comunque analizzati, creando così un onere enorme per i team di sicurezza dei dati, già gravati da compiti e responsabilità da adempiere con una larghezza di banda limitata.

Una tecnologia di protezione dei dati in grado di interpretare il contesto in cui si svolge l'attività informatica può alleggerire il lavoro dei team di sicurezza dei dati, aiutandoli a concentrare le indagini sugli eventi imprevisti che costituiscono una minaccia reale e lasciar perdere quelli che non rappresentano un rischio effettivo per l'azienda. Definendo le giuste priorità, questa tecnologia consente a un team di sicurezza di modificare il proprio ruolo all'interno di un'azienda, passando dalla semplice applicazione delle regole a diventare una guida proattiva verso un futuro più sicuro ed efficiente.

Accelerazione della crescita professionale

Gli esperti in sicurezza dei dati, alleggeriti del carico dei falsi allarmi, possono dedicarsi ad addestrare e guidare altri dipendenti, contribuendo alla loro crescita professionale e indirizzandone la carriera.

Accelerazione della crescita aziendale

Tramite un utilizzo più intelligente dei dati, i professionisti della sicurezza che sono in grado di individuare le efficienze nel loro carico di lavoro possono mettere in luce le opportunità di crescita aziendale oppure segnalare quei comportamenti di dati che possono ostacolare la crescita aziendale.

Accelerazione della trasformazione digitale

La semplificazione delle indagini realizzata grazie alla contestualizzazione degli eventi di compromissione dei dati consente ai team di guadagnare tempo che potranno poi dedicare all'ottimizzazione dei criteri e delle procedure, per adattarli a una cultura dei dati basata su cloud, accelerando la trasformazione digitale e acquisendo così un vantaggio competitivo per l'azienda.

Protezione dei dati ovunque si lavora

La tradizionale prevenzione della perdita dei dati protegge i dati in tre punti di accesso: sulla rete, negli endpoint e, sempre di più, nel cloud. Questa soluzione potrebbe essere sufficiente, se le persone che accedono a questi dati rimanessero entro tali perimetri. In realtà, invece, li travalicano sempre di più e, appena al di fuori del perimetro, i criteri di protezione dei dati non valgono più. Ecco perché attenersi alle regole non basta! Vediamo com'è possibile superare questo ostacolo.

Implicazioni della trasformazione cloud

La migrazione al cloud non è questione di "se", ma di "quando". Le richieste di lavoratori in remoto, clienti e partner strategici non fanno altro che accelerare i tempi, premendo per l'adozione di un cloud più rapido. Un esempio? Oggi, nell'87% delle imprese i dipendenti accedono alle app aziendali mobili usando i loro smartphone[3], fenomeno noto come bring-your-own-device o BYOD. Inoltre, quasi un quarto dei lavoratori millennial affermano di aver scaricato file aziendali su quei dispositivi e di aver installato applicazioni cloud di terze parti (bring-your-own-cloud o BYOC) senza notificarlo all'IT o alla direzione esecutiva. Questi comportamenti creano il cosiddetto "IT shadow" e dimostrano che un'azienda non detiene sempre il controllo su quando e come i suoi operatori si muovono nel cloud. Quale che sia il ritmo del cambiamento, le policy di sicurezza tradizionali faticano ad adeguarsi per soddisfare le nuove richieste.

Uno dei motivi è che i provider di applicazioni cloud tendono a dare priorità a portabilità, accessibilità e facilità di utilizzo e non necessariamente alla sicurezza dei dati che vengono resi portatili, accessibili o facili da usare. Si concentrano su un modello di responsabilità condivisa in cui proteggono l'infrastruttura, ma lasciano ai clienti il compito di proteggere i dati condivisi che sono al suo interno. Ciò significa che, data la natura transitoria e mobile del lavoro odierno, spetta all'azienda mettere in atto una protezione dei dati che segua i dipendenti ovunque essi vadano.

Le persone, il nuovo perimetro

In che modo è possibile proteggere i dati se le persone che li utilizzano oltrepassano le linee di difesa? È necessario un nuovo perimetro: le persone stesse.

La protezione dei dati di tipo human-centric consente di conservare i dati in un ambiente protetto a cui le persone possono accedere ovunque lavorino. Inoltre, se la sicurezza dei dati viene abbinata all'identità di un individuo è possibile adottare dei criteri che tengono in considerazione il livello di rischio personale, fornendo una visione dettagliata degli intenti. Ad esempio: un evento imprevisto che coinvolge un dipendente di lunga data e fidato può causare meno preoccupazioni di uno che riguarda un venditore sospetto o un ex dipendente scontento. Infine, il monitoraggio della sicurezza dei dati a livello umano fornisce visibilità su come tali dati vengono utilizzati nei vari dispositivi e applicazioni, procurando un contesto che può aiutare i team di sicurezza a meglio identificare le minacce e a trarne degli insegnamenti.

Sviluppo del business case per la protezione dei dati

La protezione dei dati di tipo human-centric è adatta alla realtà dinamica delle aziende moderne, ma che valore ha per la tua? Per rispondere a questa domanda, sfatiamo il mito che affligge i team di sicurezza dei dati ovunque: la protezione è nemica della produttività. Con i giusti strumenti e gli opportuni processi, una può favorire l'altra.

Risposte specifiche

Le tattiche tradizionali per la prevenzione della perdita dei dati possono semplicemente bloccare le azioni rischiose, ad esempio, impedire di salvare su un'unità flash personale un file aziendale sensibile. Tutto questo avrebbe senso se una tale operazione venisse compiuta da un ex dipendente scontento o da un lavoratore a breve termine. Il più delle volte, però, non è così; magari si tratta di un dirigente d'azienda che cerca semplicemente di fare il backup di un file importante o vuole spostarlo su un nuovo computer. Ma le policy di sicurezza dei dati tradizionali non riconoscono la differenza, quindi bloccano regolarmente attività informatiche del tutto innocue, ostacolando così la produttività dell'azienda.

L'individuazione dei rischi a livello umano permette di tenere in considerazione il contesto e l'intento alla base di un'azione, consentendo risposte di sicurezza specifiche e non assolute. Ciò non solo riduce le interruzioni dei flussi di lavoro dei dipendenti, ma alleggerisce anche l'onere delle indagini per i team di sicurezza, consentendo loro di agevolare il progresso piuttosto che bloccarlo.

Mitigazione della vulnerabilità

Anche un dipendente senza cattive intenzioni può scoraggiarsi se il suo lavoro viene ostacolato da policy di sicurezza globali. Quindi (seppur mosso da buone intenzioni) potrebbe cercare uno stratagemma per aggirare il problema, infrangendo le regole quanto basta per superare il blocco di sicurezza. Ritornando all'ultimo esempio, potrebbe dividere il file in segmenti più piccoli e inviarli via e-mail a un personal computer in modo da poterli salvare sull'unità.

Questo crea due problemi. In primo luogo, questa sequenza di azioni può generare un allerta ancora più urgente rispetto a un tentativo di salvare un file su un'unità rimovibile, perché indica che una persona sta cercando di aggirare le misure di sicurezza. Probabilmente sarà necessario indagare, impegnando tempo e risorse. Più preoccupante, però, è forse il fatto che simili espedienti, per quanto innocenti, possono introdurre nuove vulnerabilità che compromettono quelle stesse policy di sicurezza che li hanno causati. La protezione dei dati di tipo human-centric consentirebbe di adottare criteri più flessibili e più adeguati, arrestando questa spirale discendente prima che inizi.

Atteggiamento proattivo

Come può confermare chiunque, da un medico a un professionista della sicurezza dei dati, prevenire è meglio che curare.

Con gli indizi contestuali e le informazioni comportamentali forniti dai dati di tipo human-centric, è possibile bloccare le minacce reali prima che causino danni, mentre l'azienda può continuare a operare ai massimi livelli. I dipendenti possono svolgere il proprio lavoro senza essere ostacolati da criteri di sicurezza inflessibili. Gli oberati team di sicurezza dei dati possono smistare accuratamente le allerte e concentrarsi sulla risoluzione degli eventi imprevisti che costituiscono un rischio effettivo. Questa è la sicurezza dei dati, senza compromessi.

Il nuovo standard per la protezione dei dati

Il carattere evolutivo delle minacce alla sicurezza ci impone di adeguare la nostra mentalità rispetto alla protezione dei dati, accettando l'idea che i cambiamenti sono e saranno sempre una costante. Ecco perché i nostri principi fondamentali per la protezione dei dati prendono forma considerando le esigenze future:

1. Una cultura preventiva e non punitiva della sicurezza dei dati

Dal ruolo di supervisori che imponevano l'adozione retroattiva delle policy di sicurezza, i team di sicurezza dei dati si trasformeranno in guide che condurranno aziende e collaboratori ad acquisire comportamenti più sicuri nell'utilizzo dei dati.

2. Valutazione del rischio di tipo human-centric

L'utilizzo mobile e dinamico dei dati richiede una sicurezza che tenga conto dell'unica costante: l'utente. In questo modo la sicurezza diventa flessibile e adattiva, cioè cambia quando cambiano i comportamenti delle persone e il livello di rischio.

3. Visione olistica dei dati

Una visibilità piena e costante dei dati quando si spostano fuori dalla rete aziendale, tra gli endpoint o nel cloud fornisce indizi contestuali sull'intento, contribuendo a formulare delle risposte di sicurezza adeguate.

4. Politiche coerenti a prescindere dall'ambiente

La definizione del perimetro di sicurezza a livello di individuo garantisce la protezione dei dati indipendentemente da dove sono archiviati o utilizzati.

Sei pronto per il prossimo passo verso la protezione proattiva dei dati?

› **Consulta la nostra infografica,** 9 passi verso il successo con la Data Protection.

1. IBM Marketing Cloud, "10 Key Marketing Trends for 2017"
2. Ponemon Institute, "U.S. Cost of a Data Breach Study," 2017
3. Syntonic, "BYOD Usage in the Enterprise," 2016

Forcepoint

forcepoint.com/contact

Informazioni su Forcepoint

Forcepoint è l'azienda leader nel settore della sicurezza informatica per la protezione degli utenti e dei dati. La sua missione è tutelare le aziende e guidare la trasformazione digitale e la crescita. Le soluzioni armonizzate di Forcepoint si adattano in tempo reale al modo in cui le persone interagiscono con i dati, forniscono un accesso sicuro e, allo stesso tempo, consentono ai dipendenti di creare valore. Dalla sua sede ad Austin, Texas, Forcepoint crea ambienti sicuri e affidabili per migliaia di clienti in tutto il mondo.