Lookout

I cinque rischi principali quando si opera nel cloud

E cosa fare per evitarli

Il cloud porta con sé vantaggi significativi ma anche una nuova serie di rischi

Oggi la maggior parte delle organizzazioni opera nel cloud. Sfruttando la scalabilità e la facilità di utilizzo dei servizi cloud, è possibile migliorare la produttività e la collaborazione riducendo i costi operativi. Inoltre, quando si utilizzano le infrastrutture altrui, non ci si deve preoccupare della manutenzione, il che significa che è più facile espandere le proprie capacità e riprendersi da eventi disastrosi.

Se da un lato il cloud semplifica le operazioni in molti modi, dall'altro comporta una serie di rischi che possono avere un impatto sui profitti. Nel 2021, il costo medio delle violazioni dei cloud pubblici è stato di 4,8 milioni di dollari, mentre il costo delle violazioni dei cloud ibridi è stato di 3,61 milioni di dollari.1 Per continuare a operare nel cloud, la vostra organizzazione deve quindi essere consapevole di questi rischi e adottare misure appropriate per mitigarli.

Indice

4,8 MILIONI DI DOLLARI
costo medio delle violazioni dei cloud pubblici nel 2021

1. Reed, Jonathan, Security Intelligence, "The Cost of a Data Breach Goes Beyond the Bottom Line," novembre 2021

Rischio 1

Cloud ibridi e diversificati

Le configurazioni dei cloud sono estremamente flessibili e possono essere adattate alle vostre esigenze. Potete operare interamente su un cloud pubblico – come Amazon Web Services, Microsoft Azure o Google Cloud – oppure creare una configurazione multi-cloud che includa due o più di questi provider. Ma potreste anche voler mantenere alcune operazioni in sede con una configurazione cloud ibrida.

La personalizzazione comporta una certa complessità. E se non si è attrezzati per gestirla, può portare a problemi di configurazione. Insieme alle credenziali rubate o compromesse, le configurazioni errate del cloud sono state le principali cause delle violazioni nel 2020, con un costo medio per violazione di 4,41 milioni di dollari.2

A differenza degli scenari di hacking classici, in cui l'obiettivo viene scelto prima del vettore di attacco, le violazioni del cloud avvengono perché il malintenzionato trova la via più rapida per ottenere il maggior profitto. Spesso ciò avviene predisponendo sistemi automatizzati per scoprire velocemente le vulnerabilità. Sovente, la via di minor resistenza è una risorsa cloud mal configurata, una situazione che si verifica comunemente a causa della natura disarticolata della distribuzione dei servizi cloud. Con più sistemi cloud, è necessario gestire un mosaico di operazioni e controlli di sicurezza che probabilmente avranno diritti, capacità e requisiti diversi. Nel tentativo di proteggere tali infrastrutture disarticolate, le organizzazioni spesso impiegano strumenti specializzati man mano che emergono nuovi casi d'uso. Ma con agenti, console e processi multipli, questi prodotti disomogenei spesso aggiungono ulteriori oneri a team che sono già fin troppo stressati e aprono così la strada a lacune operative e di visibilità che possono essere sfruttate dai malintenzionati.

> Le configurazioni errate del cloud sono state una delle principali cause delle violazioni nel 2020

2. IBM Security, "Cost of a Data Breach 2020," luglio 2020

Rischio 2

Punti deboli delle soluzioni di gestione degli accessi

Mettendo a disposizione opzioni da configurare in base alle singole esigenze, il cloud moltiplica anche il numero di identità umane e di servizio da gestire. Le identità umane sono gli utenti finali, mentre le identità di servizio sono autorizzazioni e diritti che controllano gli accessi
o le operazioni disponibili per il servizio. Ogni risorsa nel cloud, come macchine virtuali, container e data store, ha un'identità di servizio.

Una buona soluzione di gestione degli accessi può contribuire a ridurre questa complessità con il single sign-on (SSO), che consente agli utenti di accedere alle applicazioni del sistema con un'autenticazione incrementale (la cd. "step-up authentication"). Il problema è che si tratta di un sistema binario, in cui
gli utenti ottengono l'accesso se forniscono la giusta credenziale. Lo strumento non protegge i dati contenuti in queste applicazioni e non monitora né controlla le azioni che un utente può compiere una volta entrato nel vostro ambiente.

La pandemia da COVID-19 ha portatod a un drastico aumento del numero di lavoratori remoti, una tendenza che continuerà nel 2023.3 Ciò significa che continuerete a dover affrontare il problema di endpoint e reti, come smartphone e Wi-Fi domestici, che non sono sotto il controllo diretto del vostro reparto IT. Dovrete inoltre bilanciare il controllo della sicurezza e la produttività, poiché i vostri lavoratori remoti probabilmente non sono abituati alle rigorose procedure di sicurezza e necessarie per tenere al sicuro le vostre reti.

L'implementazione di reti private virtuali, o VPN, per l'accesso in sede può introdurre una protezione tramite Basic Authentication. Tuttavia, poiché le VPN forniscono un accesso a livello di rete, se le credenziali di accesso di un utente vengono compromesse o se questi decide di agire in modo disonesto, il suo account può essere facilmente utilizzato per spostarsi lateralmente e compromettere i dati. Le VPN, inoltre, non hanno visibilità sulle attività relative ai dati e non sono strutturate per essere scalabili.

Il vostro cloud aziendale potrebbe trovarsi a gestire migliaia di identità e a disporre di migliaia di policy ed impostazioni di configurazione.

La gestione degli accessi da sola non è in grado di autenticare gli utenti o di assicurarsi che i criteri di protezione dei dati siano applicati correttamente in tutte queste applicazioni.4

La pandemia ha portato a un drastico aumento del lavoro a distanza, un trend che continuerà nel 2023.

3. "Secondo gli esperti il lavoro a distanza è destinato a rimanere e aumenterà nel 2023".
4. Faatz, Donald, Carnegie Mellon University, “Best Practices for Cloud Security,” marzo 2018

Rischio 3

Mancanza delle competenze e delle professionalità necessarie per il cloud

Alimentato dalle esigenze del lavoro a distanza, l'utilizzo del cloud è in costante aumento. Ciò, tuttavia, sta mettendo a dura prova la capacità dei team IT e di sicurezza, che già devono fare i conti con una carenza di personale qualificato. Le organizzazioni citano la mancanza di personale qualificato come uno dei maggiori ostacoli alla protezione dei lavoratori, dei dispositivi, delle applicazioni e dei dati aziendali. Secondo le stime, in tutto il settore della sicurezza mancano 3,1 milioni di professionisti (dati aggiornati al novembre 2021).5

In un sondaggio del 2020, solo il 27% delle organizzazioni ha dichiarato di essere fiduciosa nella propria capacità di affrontare gli alert di sicurezza nel cloud, mentre il 92% ha affermato di aver bisogno di migliorare le proprie competenze in materia di sicurezza del cloud. Per quanto riguarda la mancanza di competenze, l'84% ha dichiarato di dover aggiungere personale per colmare il deficit.6

Il rischio derivante dalla carenza di personale o dall'inesperienza è aggravato dalla tendenza delle organizzazioni ad implementare varie soluzioni specifiche, che richiedono una gestione quotidiana intensiva.

Queste attività di ordinaria amministrazione si traducono in team sovraccarichi di lavoro che non hanno l'opportunità di concentrarsi sullo sviluppo delle carriere e sulle iniziative strategiche. Ne conseguono un'elevata insoddisfazione sul lavoro e un alto turnover.

L'utilizzo di un modello basato sul cloud alleggerirà la pressione, eliminando il lavoro inutile e noioso richiesto dai prodotti specifici. In questo modo i vostri team IT e di sicurezza avranno la visibilità e il controllo necessari, oltre al tempo per concentrarsi sui progetti più importanti per il proprio sviluppo personale e per la protezione della vostra organizzazione.

> Solo il 27% delle organizzazioni è fiducioso nella propria capacità di gestire gli alert di sicurezza nel cloud

5. Hwang, Vince, Cloud Computing, “Breaking Through the Cloud Security Skills Gap,” novembre 2021
6. Ovcharenko, Dmytro, N-iX, “7 risks in cloud migration and how to avoid them”, aprile 2020

Rischio 4

Affidamento a strumenti tradizionali basati su appliance

Che si tratti di un'implementazione con un semplice cloud o di un ambiente multi-cloud, non avere una strategia chiara fin dall'inizio può portare ad uno spreco di risorse, ad un'operatività inefficiente e a un'insoddisfacente esperienza degli utenti che devono effettuare più login e ripetere i processi.

Delle falle possono spesso manifestarsi negli strumenti di sicurezza basati su appliance. Questi prodotti – come VPN, Secure Web Gateway (SWG) on-premises e Data Loss Prevention (DLP) – vengono tradizionalmente distribuiti in configurazioni stand-alone. Di conseguenza, le loro policy sono definite separatamente, hanno paradigmi di gestione diversi e non si integrano bene tra loro. Le soluzioni basate su appliance hanno la loro utilità, soprattutto quando la maggior parte delle entità risiede all'interno di perimetri, ma nel cloud possono essere difficili da scalare e non forniscono la visibilità e il controllo necessari.

Al contrario, un approccio basato su una piattaforma di sicurezza distribuita tramite cloud consente di raggruppare più soluzioni specifiche e di semplificare la sicurezza informatica. Così il cliente è in grado di applicare policy di protezione dei dati adattive che non ostacolano la produttività.

Le VPN non forniscono protezione contro il credential stuffing o il password spraying

Rischio 5

Minacce odierne in rapida evoluzione

Le minacce informatiche basate sul cloud stanno mettendo a nudo le debolezze critiche di molte soluzioni e metodologie di sicurezza esistenti.

Al giorno d'oggi, i malintenzionati non si limitano ad accedere ad un sistema. Si muovono lateralmente all'interno dell'ambiente, alla ricerca di dati sensibili o di altre risorse di alto valore.

Gli strumenti basati su appliance sono costosi e difficili da scalare, oltre ad avere una visibilità limitata sulle minacce basate sul cloud. Le VPN, ad esempio, non forniscono una protezione adeguata contro il credential stuffing o il password spraying. La gestione dell'identità e degli accessi (IAM, Identity and Access Management) prevede configurazioni e policy rigide che non sono in grado di valutare costantemente il livello di rischio di un utente al momento dell'accesso.

Gli attacchi DDoS (Distributed Denial of Service) sono diventati più facili grazie alla disponibilità di nuovi servizi DDoS a pagamento. Inoltre, le policy "fai-da-te" (DIY) e quelle create internamente sono poco efficaci e richiedono molto personale aggiuntivo addetto alla sicurezza.

Si scoprono nuove generazioni di malware sempre piu' evolute, come il ransomware, che viene facilmente distribuito tramite messaggi di phishing. Queste minacce informatiche hanno firme che cambiano frequentemente e non sempre vengono rilevate dai proxy web basati su appliance, i cui motori di threat intelligence sono spesso obsoleti.

Le soluzioni basate sul cloud, invece, si aggiornano costantemente e non richiedono ulteriori investimenti in personale addetto alla sicurezza. Sono inoltre scalabili e più efficaci nel proteggere da un attacco DDoS.

> Le minacce informatiche basate sul cloud stanno mettendo a nudo le debolezze di molte soluzioni e tecnologie di sicurezza esistenti

Cosa potete fare per mitigare i rischi del cloud

Il numero di misure che potete adottare per ridurre il rischio di violazione dei dati è quasi infinito. Per iniziare, ecco alcune delle più importanti:

Effettuare degli approfondimenti

Una delle cose più importanti che potete fare per assicurarvi che il vostro cloud risponda alle vostre esigenze e sia adeguatamente sicuro è informarvi. Non buttatevi sul cloud perché è la tendenza del momento o perché le statistiche appaiono buone nel report di un analista. Alcuni degli elementi da comprendere sono i costi operativi, le procedure di onboarding, la sicurezza, il disaster recovery, i termini di servizio, l'ubicazione dei data center e i termini e le procedure di offboarding. Dovreste anche assicurarvi che il servizio cloud sia implementato e configurato correttamente.

Proteggere i dati

Quando si tratta di mitigare i rischi del cloud, è necessario andare oltre le policy a livello di app. Indipendentemente dal fatto che le applicazioni risiedano in sede, in cloud privati o in cloud pubblici, ciò che conta è la protezione dei dati sensibili, come la proprietà intellettuale o le informazioni regolamentate. È necessario andare oltre alla semplice gestione degli accessi con policy che cambiano dinamicamente in base al livello di sensibilità dei dati. Ciò significa che agli utenti viene concesso un accesso adeguato ai livelli di rischio del loro comportamento e del loro endpoint.

Monitorare costantemente

Sebbene il lavoro nel cloud rappresenti un modello di responsabilità condivisa, siete voi i responsabili finali della sicurezza del vostro ambiente e dei vostri dati. Il monitoraggio continuo del comportamento del sistema, sia nel cloud che in sede, nonché di tutti i vostri endpoint, vi aiuterà a ridurre gli incidenti rischiosi e le vere e proprie minacce dannose. Ciò deve includere il monitoraggio in tempo reale del rischio degli utenti e dei dispositivi e l'applicazione dinamica del principio "zero trust".

Andare oltre la gestione degli accessi

È necessario andare oltre la gestione binaria degli accessi, garantendo l'applicazione del modello "zero trust" in modo preciso e dinamico. Prendetevi il tempo necessario per configurare programmi e policy di gestione degli accessi precisi, che proteggano i vostri dati e consentano agli utenti di accedere a ciò di cui hanno bisogno. Prestate particolare attenzione ai dispositivi perimetrali, ma non fermatevi qui. Gli strumenti di gestione degli accessi da soli non sono in grado di proteggere dalle minacce interne o dalle credenziali compromesse. È necessaria una piattaforma in grado di comprendere il contesto che circonda l'utente e di rilevare comportamenti dannosi o rischiosi.

Consolidare le operazioni IT e di sicurezza

La complessità delle operazioni in-the-cloud impone alle organizzazioni di cambiare la propria metodologia di sicurezza, passando da quella basata su appliance a quella basata su piattaforma. Un'unica piattaforma di sicurezza basata su cloud e perfettamente integrata può centralizzare l'applicazione delle policy e fornire un unico punto da cui gestire e monitorare i sistemi. In questo modo potete proteggere i dati in modo efficiente e fornire agli utenti ciò di cui hanno bisogno per rimanere produttivi.

Proteggete le vostre operazioni sul cloud con una piattaforma unificata

Operare nel cloud contribuisce a rendere le organizzazioni più produttive e a ridurre i costi, ma aggiunge complessità e nuovi rischi per la sicurezza. La Lookout Security Platform offre protezione contro questi ed altri rischi in un'unica soluzione integrata e facile da configurare. Comprendendo i rischi ed adottando le misure necessarie per ridurli, è possibile sfruttare i vantaggi del cloud riducendo al contempo i potenziali problemi.

Siamo in grado di offrirvi la valutazione gratuita del vostro rischio.

Lookout™

A proposito di Lookout

Lookout è una società specializzata in sicurezza integrata endpoint-to-cloud. La nostra missione è proteggere e potenziare il nostro futuro digitale in un mondo incentrato sulla privacy, in cui la mobilità e il cloud sono essenziali per ogni attività lavorativa e ricreativa. Consentiamo a consumatori e dipendenti di proteggere i dati e di rimanere connessi in modo sicuro senza violare la privacy e la fiducia. Lookout gode della fiducia di milioni di consumatori, delle più grandi aziende e agenzie governative e di partner come AT&T, Verizon, Vodafone, Microsoft, Google e Apple. Lookout ha sede a San Francisco e uffici ad Amsterdam, Boston, Londra, Sydney, Tokyo, Toronto e Washington D.C. Per saperne di più, visitate il sito www.lookout.com e seguite Lookout sul suo blog, LinkedIn, und Twitter.

Per maggiori informazioni
lookout.com

Richiedi una demo
lookout.com/demo