Le 4 cose che ogni amministratore Salesforce deve sapere sulla sicurezza nel cloud

W / T H
secure

Che cos'è la sicurezza nel cloud?

Man mano che aumenta l'utilizzo di infrastrutture, piattaforme, applicazioni e servizi cloud, aumentano anche le opportunità per i malintenzionati di infiltrarsi nei sistemi. In assenza di difese efficaci, cresce il rischio di furto di dati, ransomware e altri attacchi che potrebbero compromettere gravemente le attività, danneggiare la reputazione ed esporre l'azienda a violazioni delle norme di conformità e dei regolamenti sulla protezione dei dati. La sicurezza nel cloud è quell'insieme di tecnologie, processi e risorse messo in campo per proteggere l'organizzazione da attacchi basati sul cloud e in molti casi si rivela pericolosamente inadeguata.

Restare al sicuro mentre cresce l'uso del cloud

Le organizzazioni stanno passando al cloud per tutta una serie di ottime ragioni, tra cui costi di gestione più bassi, la maggiore flessibilità operativa e la necessità di consentire il lavoro e la collaborazione da remoto. Con il distanziamento sociale imposto dalla pandemia, il lavoro basato sul cloud è diventato di fatto la normalità negli ultimi due anni e Salesforce è una delle piattaforme più diffuse.

E la tendenza non sembra destinata a scemare. Da un recente sondaggio di Gartner sui CFO è emerso che il 74% delle aziende prevede che una parte dei dipendenti lavorerà fuori sede in modo permanente e il 17% stima che i dipendenti remoti rappresenteranno non meno del 20% della loro forza lavoro[1]. Le piattaforme cloud sono sempre più utilizzate per attività business-critical, dalla condivisione di materiali sensibili e la gestione della documentazione alla collaborazione con clienti e partner.

Eppure, anche se il cloud è chiaramente una manna in termini di produttività e comodità, sono troppo poche le organizzazioni che comprendono e mitigano in modo efficace i rischi per la sicurezza introdotti da questo nuovo modo di lavorare e i cyber criminali sono sempre più abili a sfruttare qualsiasi falla nelle difese delle organizzazioni. Con il maggiore ricorso a offerte software as-a-service (SaaS) nel cloud, come Salesforce, Microsoft 365, Google Workspace e altri, questi servizi diventano un obiettivo sempre più allettante e redditizio per gli attaccanti.

Se anche non avessero intenzione di sottrarre i dati memorizzati nel cloud, gli attaccanti sfruttano comunque i servizi cloud come "trampolini" per entrare in altri sistemi interni ed esterni. Ad esempio, abbiamo già assistito ad alcuni attacchi di phishing e ransomware condotti attraverso i servizi cloud.

I nostri esperti hanno evidenziato quattro verità nascoste che ti aiuteranno a utilizzare Salesforce e altri servizi cloud in tutta sicurezza.

1. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

Verità nascosta 1

Aumentare la visibilità per avere più controllo

Quando si spostano i dati in un servizio cloud come Salesforce, è necessario mantenere la piena visibilità e il controllo totale. Questo significa che devi sapere quali tipi di dati hai archiviato, come sono classificati, da dove provengono, chi può accedervi o dove sono diretti. Se i dati provengono da fonti esterne, sconosciute o non attendibili, ad esempio l'email, devi bloccare i contenuti dannosi e non consentiti prima che raggiungano gli utenti interni o esterni.

Devi anche assicurarti che non violino regolamenti o requisiti di conformità vigenti nelle giurisdizioni, nei settori e nei mercati in cui operi, ad esempio il GDPR, la normativa UE per la protezione dei dati, o lo standard PCI-DSS per la sicurezza delle carte di pagamento. Questo significa che devi essere in grado di monitorare e controllare l'accesso ai dati sensibili e conservare un audit trail completo. Devi anche poter rilevare gli insider malintenzionati e qualsiasi accesso non autorizzato ai dati e questo significa monitorare le attività e il comportamento anziché cercare semplicemente le minacce note.

Verità nascosta 2

Comprendere le responsabilità e colmare le lacune della sicurezza

Una delle cause principali dei gap di sicurezza è un malinteso diffuso sulla divisione delle responsabilità per la sicurezza dei vari aspetti nei cloud di terze parti.

I provider in genere garantiscono la sicurezza delle proprie piattaforme, spesso sfoggiando impressionanti accreditamenti e certificazioni. Questo genera in alcuni acquirenti la falsa idea di non doversi occupare di nulla per quanto riguarda la sicurezza nel cloud.

Quando si acquistano servizi cloud come Salesforce, si sottoscrive quello che è noto come modello di responsabilità condivisa per la sicurezza. Anche se i provider garantiscono per contratto che i propri sistemi sono sicuri a livello di infrastruttura e piattaforma, la responsabilità in merito ai controlli basilari per la sicurezza dei dati, alla corretta configurazione dei controlli forniti dal provider e alla protezione dei dati nel sistema resta sempre in capo all'organizzazione. Le responsabilità esatte possono variare in base al contratto, ma nella maggior parte dei casi il modello ricalca una suddivisione di questo tipo.

Verità nascosta 3

Tenere i cloud ben configurati in mezzo alla complessità crescente

I servizi e le applicazioni cloud possono diventare molto complessi, aprendo la strada a errori di configurazione o controlli di accesso inadeguati che possono portare a violazioni dei dati. Ai dati possono accedere altre applicazioni e altri servizi connessi alle piattaforme cloud tramite interfacce software note come API. Se sono configurate in modo errato o concedono autorizzazioni inappropriate, anche queste potrebbero essere il veicolo di una violazione.

Questo è di particolare interesse per gli amministratori di Salesforce, che devono far fronte a un flusso costante di richieste di cambiamento da parte delle proprie organizzazioni per aggiungere nuove funzionalità, sfruttare le capacità avanzate della piattaforma o implementare app, servizi e componenti aggiuntivi di terze parti da Salesforce AppExchange. Per ridurre la complessità, implementa strumenti come il rilevamento delle minacce cloud e CSPM (Cloud Security Posture Management) per evidenziare automaticamente le configurazioni potenzialmente pericolose o non conformi.

Verità nascosta 4

Mitigare gli attacchi alla supply chain

Anche quando la piattaforma o il servizio cloud è configurato correttamente, le integrazioni o le applicazioni di terze parti connesse tramite API rappresentano un rischio. Devi tenere conto del fatto che i sistemi connessi al cloud possono essere compromessi attraverso una vulnerabilità o un'errata configurazione software. Gli attaccanti possono anche utilizzare le tecniche di movimento laterale per ottenere l'accesso alle organizzazioni che forniscono sistemi di terze parti e sfruttare il loro canale di distribuzione (il cosiddetto "attacco alla supply chain").

Nel 2019-20, ad esempio, la compromissione di una backdoor nel noto sistema di gestione di rete SolarWinds ha consentito agli attaccanti di infiltrarsi nei sistemi di varie agenzie governative USA. Più di recente, una vulnerabilità nel framework di logging Java Log4j ha esposto al rischio di attacco circa il 93% degli ambienti cloud aziendali (fonte: Wiz/EY). Anche se molti sistemi sono stati corretti tramite patch, Log4j è talmente diffuso, e spesso installato in modo invisibile da altri pacchetti che richiedono particolari componenti Java ("dipendenze"), che la vulnerabilità Log4j rimarrà probabilmente un problema per diverso tempo.

Se hai un'integrazione tra il cloud Salesforce e un partner, cliente o sistema di terze parti che è stato compromesso inconsapevolmente attraverso una vulnerabilità come Log4j, quella connessione potrebbe essere sfruttata da un attaccante per infiltrarsi nell'organizzazione, quindi è fondamentale monitorare sia le minacce malware note che le attività anomale che potrebbero essere il segno di una minaccia sconosciuta.

A chi serve una sicurezza aggiuntiva per Salesforce?

WithSecure™ Cloud Protection for Salesforce[8] fornisce protezione in tempo reale da virus, trojan e ransomware, esaminando tutti i contenuti caricati nel cloud. Integra i controlli di sicurezza incorporati nella piattaforma cloud di Salesforce e ti permette di rispettare le tue responsabilità di sicurezza proteggendo tutti i dati che vengono archiviati o condivisi tramite Salesforce.

La soluzione permette di prevenire o fermare gli attacchi condotti tramite file malevoli o link di phishing. Offre inoltre visibilità completa e analisi dettagliata di tutti i contenuti a cui accedono gli utenti interni o esterni.

Molte organizzazioni che utilizzano Salesforce hanno la necessità sempre più urgente di implementare difese supplementari come WithSecure™ Cloud Protection for Salesforce per la piattaforma. Qui di seguito puoi trovare tre casi di utilizzo tipici.

2. https://www.withsecure.com/en/solutions/software-and-services/cloud-protection-for-salesforce

Caso di utilizzo 1: **il cercatore proattivo**

Sempre più amministratori di Salesforce si rendono conto del fatto che all'aumento dell'utilizzo dei sistemi e servizi cloud si accompagna la necessità di assicurare la protezione completa della loro piattaforma Salesforce. Sono consapevoli delle crescenti minacce cloud come il ransomware e le violazioni di dati. Sono anche consapevoli delle loro responsabilità condivise per la sicurezza, ma potrebbero non sapere esattamente su quali tipi di strumenti di terze parti possono contare per far fronte a quelle responsabilità. Quindi iniziano a porre domande pertinenti sulla sicurezza e sulla protezione dell'ambiente Salesforce[3] dai cyber attacchi. Trovano rapidamente informazioni sulle soluzioni come WithSecure™ Cloud Protection for Salesforce cercando con AppExchange per scoprire quali app di sicurezza sono disponibili. Scoprono anche che la soluzione WithSecure™ può colmare le lacune nella sicurezza di Salesforce. Quindi avviano una fase di valutazione e approvvigionamento, avendo già costruito un solido business case per l'investimento.

3. https://help.salesforce.com/s/articleView?id=000318378&type=1#FileUpload?

Caso di utilizzo 2: **il protettore del portale**

Un'organizzazione sta espandendo l'utilizzo di Salesforce per collegarsi ai partner e/o clienti, ad esempio tramite Experience Cloud (in precedenza Community Cloud). Tuttavia, non può garantire che le terze parti esterne abbiano una sicurezza adeguata sui propri endpoint, ovvero i sistemi e dispositivi che utilizzano per connettersi al portale dell'organizzazione. Se consente agli utenti esterni di caricare contenuti su Salesforce, ad esempio documentazione, moduli o link, dovrà essere in grado di garantire che questi endpoint potenzialmente compromessi non vengano utilizzati per introdurre minacce come malware o link di phishing. Teme i danni che potrebbero derivarne, sia per i suoi sistemi che per la sua reputazione. Non può permettersi di correre il rischio che qualcosa di pericoloso penetri nei sistemi e venga poi scaricato da un partner o cliente. E non può neanche permettersi un'interruzione delle attività dei propri sistemi perché il portale potrebbe essere il fulcro della sua offerta di business, come spesso accade per le società finanziarie, agenzie di selezione del personale, agenzie di viaggio e altre società di servizi professionali.

Caso di utilizzo 3: **il supervisore della conformità**

Una grande organizzazione o una società che opera in un settore altamente regolamentato come la sanità, i servizi finanziari o la pubblica amministrazione, spesso deve seguire rigorose norme di conformità. Queste norme possono includere impegni contrattuali previsti dalla legge o dalle normative in materia di protezione dei dati e privacy oppure possono essere semplicemente procedure di conformità interne basate su best practice, come lo standard di sicurezza ISO 27001. Un dirigente di alto livello, magari un CISO o CIO o addirittura un CEO, fissa come obiettivo quello di garantire che le piattaforme, le applicazioni e i servizi cloud siano pienamente conformi alle politiche generali di sicurezza dei dati dell'organizzazione. Di conseguenza, gli amministratori si rendono conto di avere bisogno di strumenti aggiuntivi per proteggere adeguatamente i loro ambienti Salesforce. Questa strategia includerà probabilmente l'implementazione della sicurezza dei contenuti con soluzioni come WithSecure™ Cloud Protection, ma potrebbe richiedere una soluzione Cloud Security Posture Management (CSPM) per garantire la conformità in tutta l'azienda.

Informazioni su WithSecure™

WithSecure™ è il partner di riferimento per la cyber security. Provider di servizi IT, MSSP e aziende, insieme alle più importanti istituzioni finanziarie, imprese manifatturiere e migliaia di fornitori dei più avanzati sistemi di comunicazione e tecnologie nel mondo si affidano a noi per conseguire una cyber security basata sui risultati, che protegge e consente le loro operazioni. La nostra protezione guidata dall'IA mette al sicuro gli endpoint e la collaborazione su cloud, il nostro sistema di intelligent detection and response è alimentato da esperti che identificano i rischi aziendali tramite threat hunting proattivo e affrontando gli attacchi in tempo reale. I nostri consulenti collaborano con imprese e tech challenger per costruire la resilienza attraverso una consulenza sulla sicurezza basata su prove concrete. Con oltre 30 anni di esperienza nella costruzione di tecnologie che soddisfano gli obiettivi aziendali, abbiamo costruito il nostro portafoglio per crescere con i nostri partner attraverso modelli commerciali flessibili.

WithSecure™, parte di F-Secure Corporation, è stata fondata nel 1988 ed è quotata sul listino NASDAQ OMX Helsinki Ltd.

WITH secure