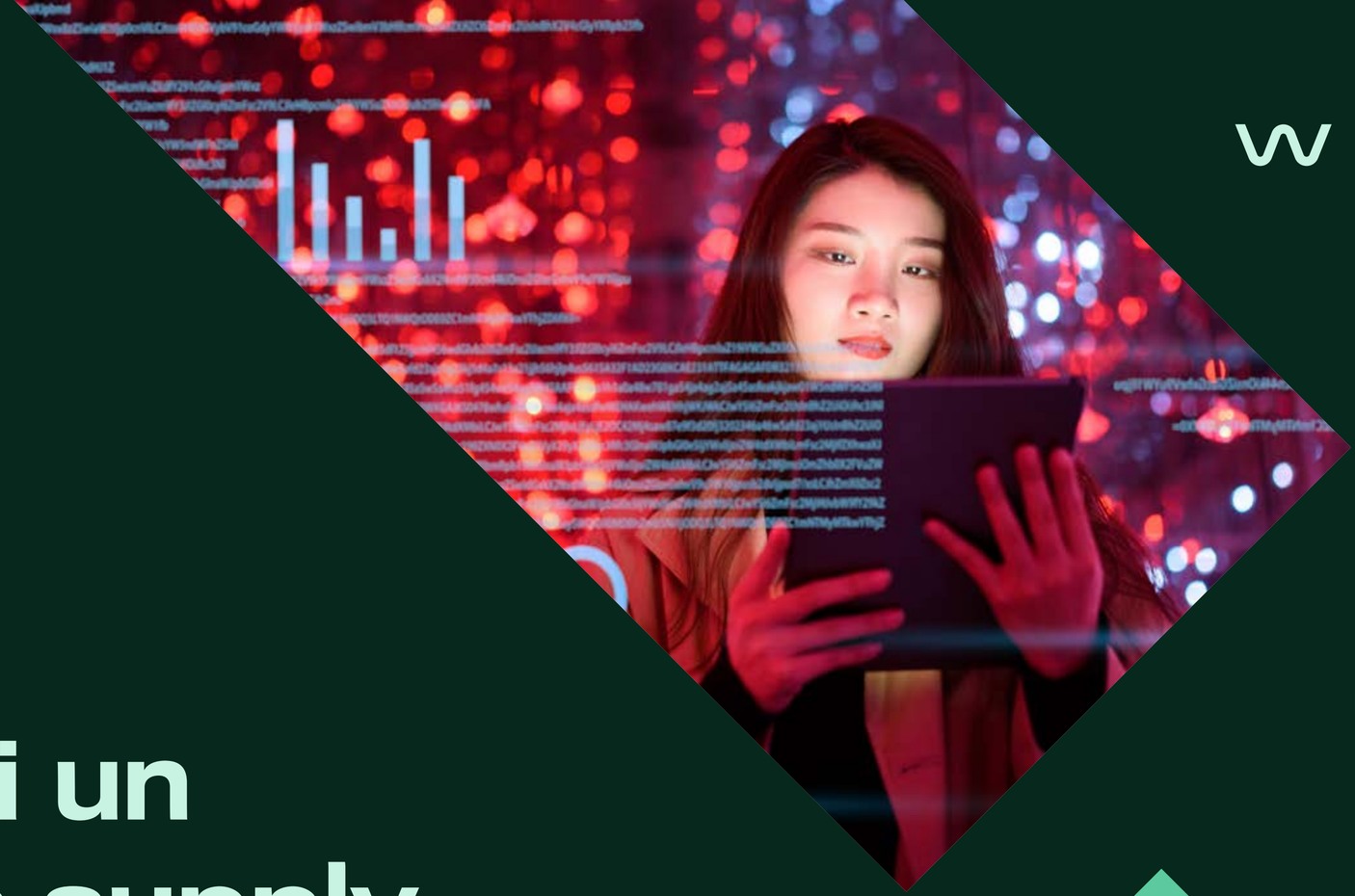
Report



Anatomia di un attacco alla supply chain Salesforce

Come evitare attacchi alla supply chain tramite integrazioni di terze parti con Salesforce

Sommario

1.Introduzione - Stato dell'arte
sul rischio per la supply chain digitale ..3
2.In che modo le integrazioni
di terze parti introducono
nuove minacce per Salesforce 6
3.Anatomia di un attacco alla
supply chain Salesforce 8
4.Best practice per mitigare il rischio
per la supply chain digitale 11
5.Fronteggiare i rischi per la supply
chain digitale nel 2022 14

1. Introduzione
Stato dell'arte sul rischio per la supply chain digitale

Oggi, tutte le aziende moderne si trovano al centro di una vasta e complessa rete di fornitori digitali. Grazie a connessioni Internet ad alta velocità e a un prezzo contenuto e all'ampio mercato cloud globale in rapida crescita, le organizzazioni hanno la possibilità di esternalizzare facilmente tutto ciò di cui hanno bisogno per far crescere il business. Possono accedere a soluzioni software specializzate tramite i modelli SaaS oppure acquisire componenti e plug-in per personalizzare a fondo l'infrastruttura aziendale.

La supply chain digitale offre una flessibilità e una libertà senza pari, che permettono di acquisire nuove capacità e cogliere le opportunità con grande rapidità. Lo scotto da pagare per tutto questo, però, è una maggiore esposizione al cyber rischio.

Introducendo una rete di migliaia di componenti mobili, risulta estremamente difficile mantenere una visibilità efficace sul patrimonio IT e identificare le potenziali vulnerabilità.

Queste connessioni, tuttavia, rappresentano un bersaglio di interesse per i threat actor. L'attacco a connessioni di terze parti come i fornitori SaaS o gli sviluppatori di plug-in software consente ai cyber criminali di bypassare le difese di sicurezza e magari colpire al cuore la rete di un'organizzazione.

Questa connettività può essere sfruttata per implementare malware, compreso ransomware mirato altamente distruttivo, all'interno dell'azienda target, sottrarre dati preziosissimi o acquisire il comando e controllo.

Gartner® ha citato il rischio di attacco alla supply chain come una delle tendenze più significative nella gestione della sicurezza e del rischio per il 2022, prevedendo che "entro il 2025, il 45% delle organizzazioni di tutto il mondo avrà subito attacchi ai danni della propria supply chain software, con un aumento del 300% rispetto al 2021".[1]

In realtà, è stato rilevato che gli attacchi alla supply chain sono triplicati già solo nel 2021. Alcune delle più grandi violazioni di dati avvenute lo scorso anno hanno avuto come oggetto le supply chain digitali.

1. Comunicato stampa di Gartner, "Top Trends in Cybersecurity 2022", pubblicato il 18 febbraio 2022

A cura degli analisti: Peter Firstbrook, Sam Olyaei, Pete Shoard, Katell Thielemann, Mary Ruddy, Felix Gaehtgens, Richard Addiscott e William Candrick. GARTNER è un marchio registrato e un marchio di servizio di Gartner, Inc. e/o delle sue affiliate negli Stati Uniti e in altri Paesi e viene qui utilizzato dietro autorizzazione. Tutti i diritti riservati.

Log4Shell

Questo exploit di alto profilo ha coinvolto la famosa libreria Java Apache Log4j 2 utilizzata per la registrazione dei messaggi di errore. La vulnerabilità, denominata ufficialmente CVE-2021-44228, ha permesso a un attaccante di ottenere l'accesso remoto a un dispositivo con determinate versioni di Log4j 2 tramite messaggi di testo. La falla è stata scoperta e rapidamente corretta con patch nel dicembre 2021, ma potrebbe essere stata in circolazione già dal 2013. Si ritiene che circa la metà di tutte le organizzazioni sia stata presa di mira utilizzando questa vulnerabilità nel tempo.

Okta

A marzo 2022, Okta, un fornitore di soluzioni MFA, ha annunciato di avere subito una massiccia violazione della sicurezza nel mese di gennaio, che ha coinvolto centinaia di clienti. La violazione ha dimostrato come le connessioni di terze parti vengano prese di mira e sfruttate, essendo di fatto iniziata con la compromissione di un sub-appaltatore di Okta. Gli attaccanti, un gruppo di hacker noto come Lapsus$, sono riusciti a penetrare nelle reti dei clienti e ad accedere ai dati utilizzando uno strumento di desktop remoto.

Office 365

L'ambiente Office 365 esteso è sempre più nel mirino dei threat actor per attacchi di phishing mirati. Prima di tutto, le vittime ricevono un'email in cui viene chiesto di accedere al proprio account 365 e verificare una nuova applicazione. Questa email include un link alla pagina di accesso a Office 365 effettiva dell'utente, anziché al consueto sito di phishing contraffatto. La minaccia è costituita proprio dall'applicazione, che fornirà l'accesso ai file e alle email dell'utente. Dato che si trova già all'interno dell'ambiente, l'applicazione fraudolenta può sottrarsi al requisito di autenticazione a più fattori (MFA).

SolarWinds

Sebbene sia avvenuto nel 2020, l'attacco SolarWinds rimane l'esempio più eclatante di attacco a una supply chain digitale di alto livello. Questo incidente, da molti ritenuto opera di agenti russi, ha coinvolto il fornitore di software SolarWinds in un sofisticato attacco su più fronti mirato alla sua nota soluzione Orion. Attraverso l'inserimento di codice malevolo in un aggiornamento del software, gli attaccanti sono riusciti ad accedere alle reti di migliaia di utenti, tra cui anche enti governativi come i Ministeri del Tesoro e della Giustizia degli Stati Uniti.

Questi attacchi dimostrano perché tutte le organizzazioni dovrebbero prendere sul serio i rischi per la supply chain digitale. Una sola applicazione compromessa può avere conseguenze su migliaia di organizzazioni in tutto il mondo. È importante che le aziende comprendano l'entità del pericolo e si adoperino per aggiornare le proprie capacità di sicurezza man mano che crescono le proprie connessioni digitali.

Il rischio per la supply chain è un problema che riguarda trasversalmente tutte le aree di business che hanno effettuato una trasformazione digitale e integrano software di terze parti. Più è rilevante la funzione di business, maggiore sarà il rischio.

Per questo motivo, Salesforce, il sistema CRM a cui si affidano oltre 150.000 organizzazioni in tutto il mondo, è uno degli ambienti software maggiormente a rischio su questo fronte. Sebbene l'infrastruttura Salesforce non sia ancora stata oggetto di un grave incidente ai danni della supply chain, non si possono escludere attacchi di questo genere in futuro.

Rapporto ENISA:

Secondo le stime del rapporto Threat Landscape for Supply Chain Attacks di ENISA, tra tutti gli attacchi alla supply chain analizzati tra il 2020 e il 2021:

- circa il 50% è stato attribuito a noti gruppi APT
- circa il 62% ha fatto leva sulla fiducia nei confronti del proprio fornitore
- il 62% ha visto l'impiego di malware
- il 66% ha sfruttato il codice dei fornitori per arrivare ai clienti
- circa il 58% mirava ad accedere ai dati, come dati personali o proprietà intellettuale

2. In che modo le integrazioni di terze parti introducono nuove minacce per Salesforce

Salesforce è un asset fondamentale per molte organizzazioni e spesso svolge un ruolo determinante nella loro strategia complessiva riguardante l'esperienza digitale e la gestione dei clienti. Non stupisce quindi l'enorme richiesta del mercato di poter personalizzare e configurare l'ambiente in base alle diverse esigenze operative.

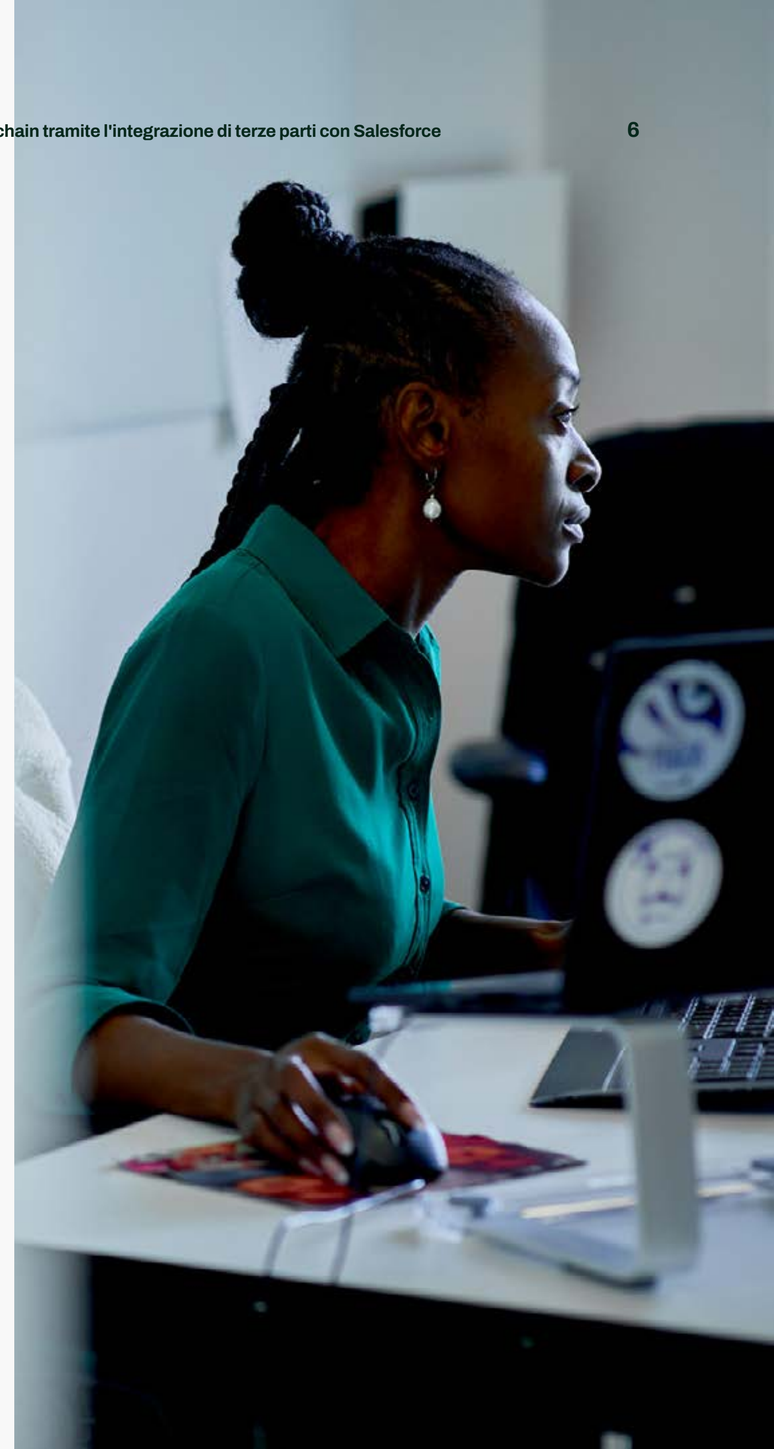
La piattaforma Salesforce può essere ampiamente personalizzata ed estesa con applicazioni, componenti e servizi cloud di terze parti. Salesforce AppExchange, l'app store ufficiale della piattaforma, offre più di 3.400 app e le organizzazioni possono collegare i propri ambienti Salesforce ad applicazioni o sistemi esterni tramite API SOAP o REST. Questi sistemi possono essere ospitati in diversi ambienti cloud e utilizzare tutta una serie di software proprietari o open-source. Inoltre, la piattaforma Salesforce supporta l'integrazione tradizionale basata su email o moduli web.

Con così tante opzioni a disposizione, le aziende troveranno sicuramente un supporto di terze parti per qualsiasi adattamento ed estensione desiderino implementare nel proprio ambiente Salesforce. Ogni nuova aggiunta, tuttavia, aumenta l'esposizione dell'organizzazione al rischio per la supply chain digitale.

In questo contesto esistono svariate minacce possibili:

Impostori malintenzionati

Nello scenario peggiore, le risorse di terze parti possono essere state create appositamente come vettori di attacco. Gruppi criminali organizzati scaricano applicazioni legittime ed effettuano il reverse engineering di cloni compromessi che nascondono il codice malevolo, per poi ripubblicarle per il download. Sebbene non siano stati segnalati casi su AppExchange di Salesforce, si tratta di un problema sempre più diffuso su Android, Google e altre fonti. Grazie ai rigorosi requisiti di sicurezza di Salesforce, AppExchange è una fonte ragionevolmente sicura, ma non può dirsi lo stesso per le molte altre risorse software online. È anche difficile controllare ciò che un'applicazione fa dopo l'installazione, per cui non è escluso che applicazioni precedentemente approvate vengano utilizzate per scopi malevoli.



Software compromesso

Come ampiamente dimostrato dalle violazioni di SolarWinds e Kaseya, i cyber criminali possono anche cercare di sfruttare la supply chain digitale prendendo di mira innanzitutto il fornitore di software. Questo permette loro di utilizzare applicazioni legittime e precedentemente approvate come vettore di attacco efficace, in grado di aggirare molte difese di sicurezza tradizionali. Questi attacchi prevedono l'utilizzo di molte risorse e quindi solitamente sono di pertinenza di gruppi organizzati che mirano a organizzazioni di alto valore o che cercano di colpire un numero considerevole di vittime con attacchi sofisticati come il ransomware. È quindi possibile che i singoli utenti di Salesforce non siano i target più redditizi, al contrario di Salesforce e dei suoi integratori di alto profilo.

Codice vulnerabile

Tutti gli asset digitali possono naturalmente introdurre cyber rischi senza l'intervento di un threat actor. Le vulnerabilità del software sono un rischio onnipresente per il business nell'era digitale: nel 2021 è stato raggiunto il record di 19.733 segnalazioni. È inevitabile che anche un'applicazione ultra-testata di un vendor con una reputazione impeccabile contenga qualche vulnerabilità.

Qualunque sia la fonte, anche una singola applicazione o un solo componente di terze parti non sicuro può essere sufficiente a veicolare una grave violazione della sicurezza.

Un ambiente complesso con centinaia di app aggiuntive e plug-in diventa presto estremamente difficile da gestire. Con così tante formichine brulicanti alle prese con compiti diversi, anche i migliori amministratori faranno fatica a vedere cosa succede dall'altra parte del formicaio.

Esiste però la tendenza preoccupante a non mettere in discussione la sicurezza dell'ambiente solo perché si tratta di Salesforce. Mentre gli amministratori di sistema e i team di gestione dello sviluppo e dell'infrastruttura sono sempre più consapevoli delle sfide legate alla protezione di altri ambienti come AWS, la natura più snella di Salesforce fa sì che spesso sia considerato autosufficiente e intrinsecamente sicuro. Le piattaforme IaaS (Infrastructure-as-a-Service) più complesse come AWS coinvolgeranno i team IT, di rete e di sicurezza fin dall'inizio, ma è improbabile che a Salesforce si dedichi la stessa attenzione.

Minaccia interna

Come qualsiasi altro ambiente digitale, Salesforce può diventare molto vulnerabile se non viene configurato correttamente.

Le applicazioni mal configurate e la gestione inefficace delle identità possono esporre rapidamente l'ambiente al rischio. I threat actor sono abili nel rilevare gli account utente e le applicazioni con una protezione inadeguata, in cui sono state lasciate le impostazioni predefinite. Controlli degli accessi deboli permettono ai cyber-attaccanti di infiltrarsi molto più facilmente nell'ambiente.

È un grave problema, anche al netto dell'introduzione di centinaia di nuovi elementi attraverso applicazioni e componenti di terze parti. Può essere particolarmente rilevante per le grandi organizzazioni, dove la mancanza di coordinamento tra filiali e reparti fa sì che l'ambiente sia intasato da applicazioni e plug-in ridondanti che svolgono le stesse attività. Le aziende più piccole possono essere più snelle, ma è più probabile che aggiungano nuovi componenti al volo, senza misure di protezione efficaci.

Si noti che Salesforce ha fatto in modo di rendere più visibili le regole di condivisione mal configurate per ridurre il rischio e ha pubblicato aggiornamenti delle versioni che applicano impostazioni più sicure al posto di quelle predefinite.
Ad esempio, è possibile usare Salesforce Optimizer, un'applicazione Lightning Experience, per effettuare controlli regolari e mettere in evidenza potenziali problemi correlati agli utenti guest.

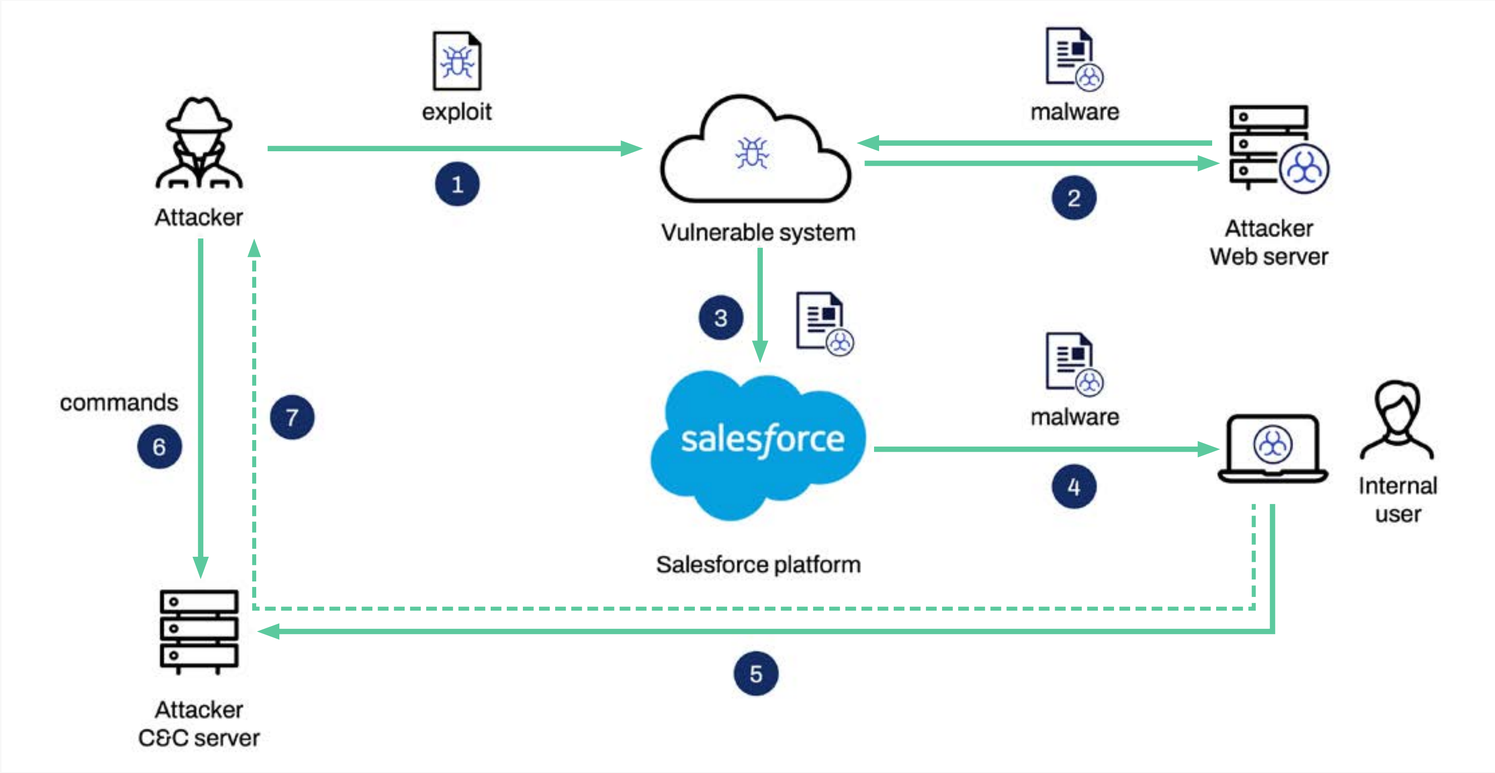
3. Anatomia di un attacco alla supply chain Salesforce

Data la sua ampiezza e complessità, l'ambiente Salesforce può essere preso di mira e sfruttato in diversi modi nell'ambito di un attacco alla supply chain digitale. Ecco due esempi di scenari di attacco.

Scenario 1: sistema di terze parti vulnerabile

In questo caso, l'attaccante identifica una vulnerabilità in un'applicazione software integrata con Salesforce, ad esempio uno strumento che recupera i dati per l'analisi, e la sfrutta per ottenere l'accesso remoto al sistema. L'applicazione vulnerabile è collegata a Salesforce tramite API e, poiché queste ultime sono generalmente considerate più attendibili di un utente umano, l'attaccante riesce ad accedere al sistema con relativa facilità.

L'attaccante può cercare di sottrarre o danneggiare i dati all'interno di Salesforce, ma può anche integrare le funzionalità della piattaforma nella sua catena di attacco. Può ad esempio inserire documenti e URL malevoli nell'ambiente perché vengano cliccati e scaricati da ignari utenti, quali dipendenti, clienti e altre connessioni. In seguito, potrà compromettere questi utenti e sfruttare il loro accesso al sistema per proseguire l'attacco nel resto dell'infrastruttura IT dell'azienda.



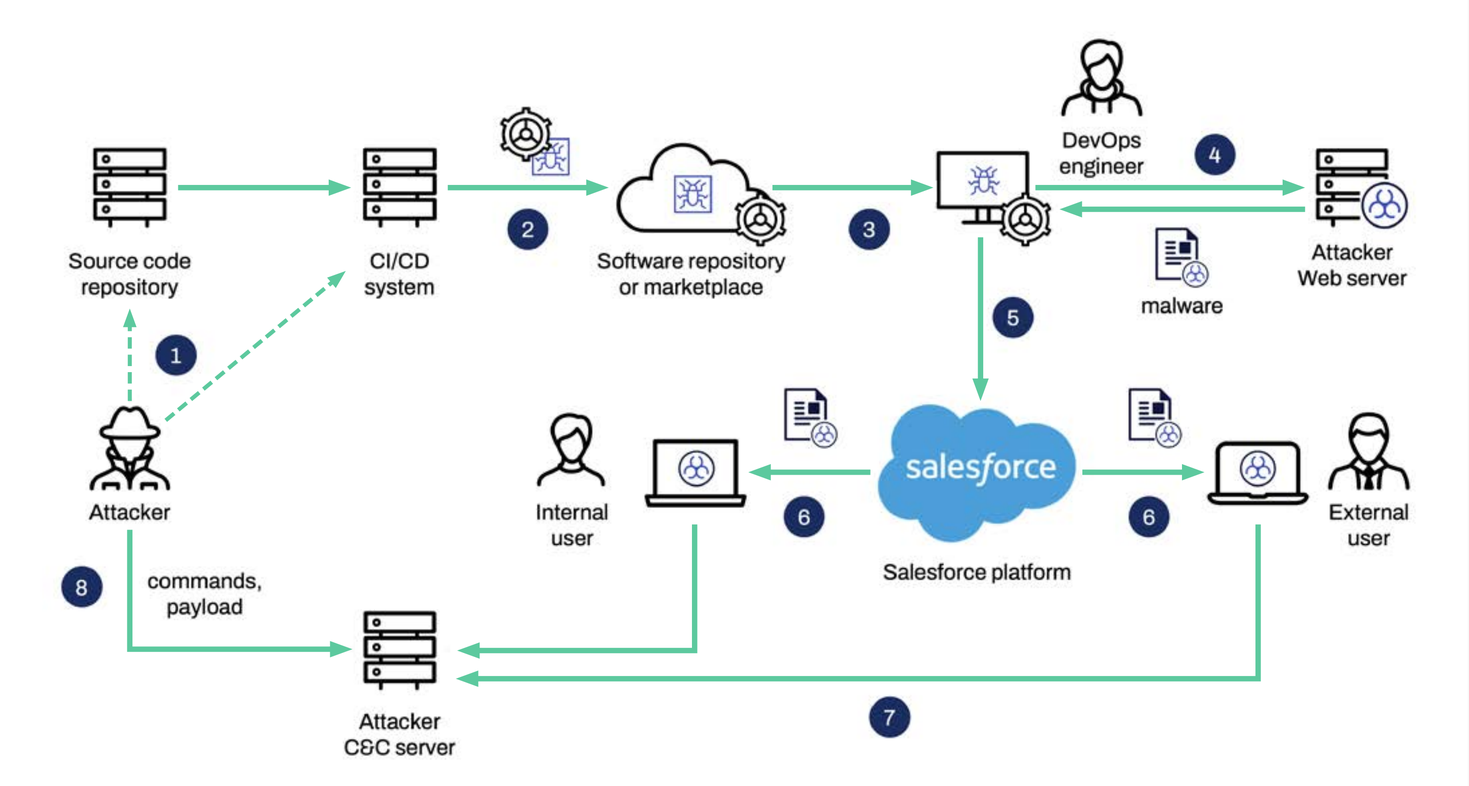
1. L'attaccante sfrutta la vulnerabilità nel sistema cloud di terze parti (o locale) connesso a Salesforce.
2. L'attaccante esegue il codice dell'exploit per ottenere l'accesso al sistema vulnerabile e scaricare malware dallo speciale server web.
3. L'attaccante "inietta" il malware nella piattaforma Salesforce. Ad esempio, il malware viene allegato a un caso, a un post di Chatter o caricato nella libreria di file comune.
4. L'utente interno scarica un file con il malware e lo apre sul proprio dispositivo. Non nota nulla di anomalo.
5. Il malware si connette al server C&C (command-and-control) ospitato dall'attaccante.
6. L'attaccante scopre che il malware è all'interno e si è connesso al server C&C. L'attaccante interagisce con il malware inviando altri comandi o payload.
7. L'attaccante sottrae dati sensibili dal computer dell'utente interno e/o da Salesforce.

Scenario 2: strumenti di sviluppo compromessi

In questo scenario, il threat actor prende di mira innanzitutto un repository di codice sorgente o il sistema CI/CD di un fornitore di software per introdurre codice malevolo nel suo prodotto. L'accesso iniziale al sistema può avvenire in vari modi; una delle tattiche più frequenti consiste nell'uso del phishing per acquisire le credenziali utente, come dimostrato da SolarWinds.

L'applicazione o il componente viene integrato nell'ambiente Salesforce e l'attaccante può sfruttare la sua connettività per compromettere altri utenti ed endpoint. Anche in questo caso, da qui può raggiungere gli scopi malevoli che si prefigge. Il processo può persino ripetersi, usando l'organizzazione target come ulteriore passaggio di un vasto attacco alla supply chain.

L'attaccante può accedere direttamente all'istanza Salesforce al primo passaggio oppure implementare una back-door e attendere che l'integratore acquisisca l'accesso in produzione successivamente. Gli sviluppatori tendono a fidarsi ciecamente della sicurezza dei loro strumenti, soprattutto se provengono da un fornitore noto. L'esperienza di SolarWinds, però, dimostra che anche un fornitore affermato può essere una fonte di rischio se viene compromesso da attaccanti organizzati.



1. L'attaccante scansiona il repository di codice sorgente pubblico e trova le credenziali del sistema CI/CD, a cui alla fine riesce ad accedere.
2. L'attaccante "inietta" un apposito payload nel pacchetto software creato dal sistema CI/CD e pubblicato nel repository di software o marketplace ufficiale.
3. L'ingegnere DevOps riceve il pacchetto dal repository/marketplace con il payload e lo esegue sul suo computer.
4. Il payload scarica il malware dal server web dell'attaccante.
5. Dato che l'ingegnere DevOps ha accesso a Salesforce, il malware viene caricato in Salesforce.
6. L'utente interno e/o esterno scarica il malware e lo apre sul suo computer.
7. Il malware si connette al server C&C (command-and-control) dell'attaccante.
8. L'attaccante invia comandi e ulteriore payload malevolo nel/i computer della vittima.

4. Best practice per la mitigazione del rischio per la supply chain digitale

La cyber security è un problema complesso che non può essere risolto con un'unica formula magica. Questo è particolarmente vero per un ambiente cloud vasto e denso come Salesforce. È per questo che la mitigazione del rischio di attacco alla supply chain digitale di Salesforce richiede un approccio multilivello che combini le giuste soluzioni di sicurezza con i giusti processi e criteri. Ecco alcuni degli elementi più importanti per una strategia di sicurezza Salesforce:

Implementazione della gestione APM (Application Portfolio Management)

Prima di introdurre applicazioni e componenti nell'ambiente Salesforce, è fondamentale eseguire una valutazione attenta che includa anche la ricerca delle vulnerabilità note e degli incidenti precedenti che hanno coinvolto l'asset e il suo fornitore, assicurandosi che quei problemi siano stati risolti. L'implementazione di un processo APM (Application Portfolio Management) coordinerà la verifica delle applicazioni future e l'inventario delle risorse esistenti. La due diligence si estende anche al fornitore stesso e le organizzazioni devono assicurarsi che tutte le terze parti dispongano di un livello di sicurezza adeguato per mitigare il rischio di attacco alla supply chain, incluso il rischio di implementazione accidentale di vulnerabilità negli aggiornamenti.

Le società con un profilo di rischio particolarmente elevato possono inserire requisiti di sicurezza nei loro contratti di servizio (SLA).

Nell'attuale clima geopolitico, le aziende devono anche prestare particolare attenzione all'origine del fornitore, per ridurre al minimo il rischio di operatori sostenuti da stati nazionali.

Rischio e potenziale impatto di una violazione

Oltre a valutare l'asset in sé, le organizzazioni devono analizzare a fondo anche il suo ruolo all'interno dell'ambiente Salesforce, considerando l'impatto che avrebbe se fosse coinvolto in una violazione. Ciò comporta la determinazione delle funzionalità del prodotto e il suo collegamento sia con Salesforce che con altre aree dell'infrastruttura IT.

L'introduzione di un rischio è un costo inevitabile per il business, ma le aziende devono essere sicure che il livello di rischio sia accettabile a fronte dei vantaggi offerti dal nuovo componente, integrando tutto ciò nella loro strategia di sicurezza.

Vista centralizzata degli asset di terze parti

Negli ambienti Salesforce più grandi, con centinaia di componenti di terze parti, può essere quasi impossibile tenere traccia di tutto. Tuttavia, gli amministratori devono cercare di ottenere la massima visibilità possibile per limitare la presenza di punti ciechi che possono portare a gravi incidenti.

Dovrebbero preferibilmente dare priorità all'acquisizione di un controllo e di una visibilità efficaci sugli elementi di terze parti più importanti e ad alto rischio, per poi procedere per gradi. Attraverso la definizione di norme strutturate riguardanti l'introduzione di nuove risorse, inoltre, sarà possibile mantenere la visibilità man mano che l'ambiente cresce, limitando l'aggiunta di applicazioni ridondanti.

Eliminare gli errori di configurazione e i problemi di accesso

Le aziende non devono solo guardare esternamente alla propria supply chain digitale, ma devono anche concentrarsi sui processi interni. Gli errori di configurazione delle applicazioni e una gestione inadeguata degli accessi possono spianare la strada ai cyber attaccanti, ancora prima dell'introduzione di terze parti.

Gli amministratori devono controllare l'ambiente Salesforce per assicurarsi che le applicazioni siano configurate correttamente con il livello appropriato di diritti di accesso. Tutti gli asset dovrebbero essere configurati sul livello minimo di accesso richiesto e con le funzionalità di condivisione disabilitate, se non sono strettamente necessarie.

Questo vale anche per gli utenti dell'organizzazione. Tanto i profili degli utenti umani quanto i sistemi automatizzati devono essere configurati secondo il principio del privilegio minimo, in modo che dispongano soltanto dei diritti di accesso di cui hanno bisogno per le loro mansioni. Questo è particolarmente importante per gli amministratori di sistema, poiché le aziende tendono spesso a concedere di default i diritti di amministratore a tutti gli utenti connessi al sistema.

Le best practice per l'accesso al sistema aiutano a ridurre la possibilità di sfruttamento dell'ambiente da parte di threat actor e a mitigare l'impatto di ciò che può accadere in caso di compromissione di un utente o di un'applicazione.

L'importante è capire che non si tratta di un'azione una tantum. Occorre esaminare periodicamente tutte le nuove funzionalità incluse in Salesforce consultando le note di rilascio fornite.

Nelle organizzazioni con ambienti particolarmente vasti, sarebbe preferibile eseguire regolarmente un'analisi approfondita delle configurazioni del sistema. Il servizio di consulenza cloud di WithSecure™ può fornire competenze specialistiche per assicurarsi che non venga tralasciato alcun dettaglio.

Bloccare contenuti malevoli su Salesforce

I threat actor useranno molti metodi diversi per iniziare l'attacco alla supply chain; uno degli approcci più comuni è l'utilizzo di credenziali sottratte. Per prevenire gli attacchi alla supply chain mediante phishing, furto di credenziali utente e malware, è necessario adottare un approccio olistico alla sicurezza che comprenda la protezione degli endpoint, della rete e del cloud.

WithSecure™ offre una gamma di soluzioni utili per prevenire, rilevare e rispondere agli attacchi moderni.

Bisogna comunque tenere conto del fatto che l'ambiente Salesforce stesso può essere sfruttato come vettore di attacco. Il supporto per l'upload e il download di contenuti è una caratteristica fondamentale per molte organizzazioni, ad esempio per consentire ai clienti delle compagnie di assicurazioni di caricare i documenti relativi ai sinistri e i propri documenti d'identità oppure alle società di selezione del personale di inviare e ricevere offerte di lavoro.

Questa funzionalità chiave può essere sfruttata per caricare file e URL malevoli in Salesforce come alternativa efficace al phishing basato su email. Un ambiente Salesforce compromesso può essere utilizzato anche per condividere contenuti malevoli con utenti e clienti.

Salesforce è responsabile della protezione dei dati all'interno del suo ambiente, ma non del controllo dei contenuti che vengono caricati o scaricati, che spetta invece all'organizzazione.

WithSecure™ Cloud Protection for Salesforce è uno dei modi più efficaci per bloccare questo percorso di attacco. Si tratta di una soluzione leader di mercato progettata per prevenire gli attacchi sferrati attraverso file e URL malevoli caricati in Salesforce da sofisticati gruppi criminali e utenti esterni al perimetro di cyber security dell'organizzazione.

Scansiona in tempo reale tutti i contenuti che vengono caricati e scaricati per identificare e bloccare i contenuti malevoli, grazie alla più recente threat intelligence di WithSecure™. Cloud Protection for Salesforce è stato sviluppato in collaborazione con Salesforce per offrire una protezione avanzata senza compromettere l'esperienza dei dipendenti e degli utenti.

Implementare un piano di risposta efficace

In ultimo, è importante capire che non bisogna più chiedersi se, ma quando, si presenterà la minaccia di un data breach. Anche le organizzazioni con strategie di sicurezza mature e sostenute da budget consistenti prima o poi dovranno fare in conti con un attaccante sufficientemente capace e determinato.

È quindi opportuno che tutte le aziende si preparino allo scenario peggiore di un attacco alla supply chain digitale ai danni del proprio ambiente Salesforce. La priorità in questo caso è implementare un piano efficace di risposta agli incidenti e correzione per identificare e bloccare rapidamente le minacce e ripristinare il prima possibile le normali attività di business.

Il servizio Salesforce Shield fornisce accesso a funzionalità come la registrazione dettagliata e la crittografia a livello di singoli campi. Questo può supportare esigenze chiave, come il monitoraggio delle attività, che sono utili per rilevare e analizzare gli incidenti.

Le organizzazioni hanno anche bisogno di accedere prontamente alle competenze e agli strumenti specializzati necessari per risalire all'origine della violazione e rimuovere eventuali minacce residue nell'ambiente, come dropper malware nascosti e programmi di comando e controllo. La collaborazione con un partner specializzato è uno dei modi più economici per acquisire queste capacità.

Le aziende devono anche pianificare la mitigazione dell'impatto di un ambiente Salesforce compromesso, che potrebbe causare l'arresto dell'intero processo CRM. Attraverso backup regolari del sistema e metodi di comunicazione alternativi è possibile assicurare la continuità di business durante la risoluzione della crisi.

5. Fronteggiare i rischi per la supply chain digitale nel 2022

- Il rischio per la supply chain cresce rapidamente, con threat actor alla ricerca di nuovi percorsi di attacco per eludere le difese
- L'ambiente Salesforce esteso è vulnerabile come percorso di attacco, a meno che le organizzazioni non adottino misure di precauzione
- Le aziende devono prepararsi ora, prima di subire un attacco

Il rischio per la supply chain è ormai parte integrante del business nell'era digitale. Le aziende devono essere consapevoli del fatto che la minaccia è in crescita, data l'espansione della loro supply chain e la presenza di threat actor sempre alla ricerca di nuove opportunità per eludere le difese di sicurezza.

Man mano che la loro digital footprint si allarga e si connette con un numero maggiore di terze parti, le organizzazioni devono rafforzare anche la loro capacità di monitorare e controllare la supply chain estesa.

Salesforce deve avere una posizione preminente in questi piani di sicurezza, sia come sistema CRM cruciale, sia come ambiente che può ospitare centinaia di elementi di terze parti.

In base al cosiddetto modello di responsabilità condivisa, Salesforce è responsabile della protezione della propria infrastruttura, ma la responsabilità per i componenti e i contenuti di terze parti che vengono introdotti nell'ambiente ricade sugli utenti.

Gli incidenti di alto profilo come SolarWinds, Kaseya e Log4J hanno fatto grande scalpore e hanno contribuito ad aumentare la consapevolezza in merito al rischio per la supply chain. Salesforce, tuttavia, rimane ancora esclusa da questo dibattito. Mettiti in contatto con il nostro team per scoprire in che modo WithSecure™ può aiutarti a proteggere questo percorso di attacco critico prima che venga scoperto e sfruttato.

Chi siamo

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 sicurezza informatica basata sui risultati, che protegge e consente le loro operazioni. La nostra protezione guidata dall'IA protegge gli endpoint e la collaborazione nel cloud e 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 portfolio per crescere insieme ai nostri partner attraverso modelli commerciali flessibili.

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

WITH secure