Bericht

So funktioniert ein Angriff auf die Salesforce-Lieferkette

So verhindern Sie Angriffe auf Lieferketten bei der Integration von Drittanbietern in Salesforce

Inhalt

1. Einleitung
Der Status quo bei den Gefahren für digitale Lieferketten

Jedes moderne Unternehmen steht heute im Mittelpunkt eines riesigen komplexen Gefüges digitaler Anbieter. Günstiges High Speed Internet und der enorme, rasant wachsende globale Cloud-Markt bedeuten, dass Unternehmen einfach auslagern können, was sie für ihr Wachstum brauchen. Spezialisierte Softwarelösungen erhält man über SaaS-Modelle, oder man erwirbt Komponenten und Plugins, um die eigene Infrastruktur individuell anzupassen.

Digitale Lieferketten bieten einzigartige Flexibilität und Freiheit. Unternehmen können dadurch schnell neue Ressourcen erschließen und Geschäftsfelder erschließen. Damit verbunden sind aber auch erhöhte Cyberrisiken.

Die Einrichtung eines Netzes aus tausenden beweglichen Teilen erschwert es erheblich, den IT-Bestand effektiv zu überblicken und potenzielle Schwachstellen zu ermitteln.

Angreifer versuchen allerdings ständig, diese Verbindungen zu nutzen. Sie zielen auf Verbindungen bei Drittanbietern von SaaS-Lösungen oder Software-Plugins ab, um Sicherheitsmaßnahmen zu umgehen und den Kern eines Unternehmens-Netzwerks zu treffen. Diese Konnektivität lässt sich ausnutzen, um Malware, inklusive hochgradig schädlicher gezielter Ransomware, im Unternehmen zu installieren, hochwertige Daten zu extrahieren oder die Kontrolle zu übernehmen.

Gartner® nennt die Risiken für digitale Lieferketten einen der stärksten Trends im Bereich Sicherheit und Risikomanagement für 2022 und erwartet, dass "bis 2025 45 % der Unternehmen weltweit Angriffe auf ihre digitalen Lieferketten erleben – eine Verdreifachung gegenüber 2021."1

Tatsächlich wurde die Zunahme von Angriffen auf Lieferketten allein für 2021 schon auf das Dreifache geschätzt. Einige der größten Datenpannen des letzten Jahres betrafen digitale Lieferketten.

1. Gartner Press Release, “Top Trends in Cybersecurity 2022”, veröffentlicht 18 Februar 2022

Von Analysten: Peter Firstbrook, Sam Olyaei, Pete Shoard, Katell Thielemann, Mary Ruddy, Felix Gaehtgens, Richard Addiscott, William Candrick. GARTNER ist eine eingetragene Marke und Service-Marke von Gartner, Inc. und/oder seinen Tochtergesellschaften in den USA und international und wird hier mit freundlicher Genehmigung verwendet. Alle Rechte vorbehalten.

Log4Shell

Diese auffällige Sicherheitslücke betraf die beliebte Apache Log4j 2 Java-Bibliothek für die Protokollierung von Fehlermeldungen. Über die Schwachstelle, offiziell CVE-2021-44228, konnte ein Angreifer über Textnachrichten Remotezugriff auf ein Gerät mit bestimmten Versionen von Log4j 2 erlangen. Die Schwachstelle wurde im Dezember 2021 entdeckt und schnell gepatcht, war aber wohl schon seit 2013 bekannt. Vermutlich wurde fast die Hälfte aller Unternehmen bereits über diese Schwachstelle attackiert.

Okta

Im März 2022 meldete der MFA-Anbieter Okta eine große Sicherheitsverletzung, die Hunderte Kunden betraf. Der Angriff zeigte, wie Verbindungen von Drittanbietern ausgenutzt werden: Er begann mit der Schädigung eines Subprozessors, der Okta beliefert. Die unter dem Namen Lapsus$ bekannte Hackergruppe konnte dann über ein Remote-Desktop-Tool in Kundennetzwerke eindringen und auf Daten zugreifen.

Office 365

Angreifer nutzen zunehmend die erweiterte Office 365-Umgebung für gezielte Phishing-Angriffe. Die Opfer erhalten zunächst eine E-Mail mit der Aufforderung, sich bei ihrem 365-Konto anzumelden und eine neue Anwendung zu bestätigen. Statt der üblichen gefälschten Phishing-Website verweist die E-Mail auf die echte Office 365-Anmeldeseite des Benutzers. Die Anwendung selbst verschafft dem Angreifer Zugang zu Dateien und E-Mails des Benutzers. Da die Anwendung bereits in der Umgebung liegt, umgeht sie die Multifaktor-Authentifizierung (MFA).

SolarWinds

Obwohl die SolarWinds Attacke schon 2020 stattfand, ist sie immer noch das bekannteste Beispiel für einen High-End-Angriff auf digitale Lieferketten. Der raffinierte, breit angelegten Angriff auf die beliebte Orion-Lösung des Softwareanbieters SolarWinds kam vermutlich von russischen Agenten. Die Täter injizierten heimlich Schadcode in ein Software-Update und verschafften sich so Zugang zu den Netzwerken tausender Nutzer, darunter auch Regierungsbehörden wie das US-Finanzministerium und das Justizministerium.

Diese Angriffe zeigen, wie ernst Unternehmen die Gefahren für digitale Lieferketten nehmen müssen. Eine einzige befallene Anwendung kann tausende Organisationen auf der ganzen Welt schädigen. Unternehmen müssen das Ausmaß der Gefahr erkennen und ihre Sicherheitstechnik auf den letzten Stand bringen, um für zunehmende digitale Verbindungen gerüstet zu sein.

Die Lieferkettenrisiken betreffen alle Geschäftsbereiche nach digitalen Veränderungen, die Drittanbieter-Software integrieren. Je wichtiger die Geschäftsfunktion ist, desto größer das Risiko.

Salesforce, das CRM-System für mehr als 150.000 Unternehmen weltweit, gehört zu den gefährdetsten Softwareumgebungen für solche Angriffe, und obwohl die Salesforce-Infrastruktur bisher noch nicht in einen größeren Supply-Chain-Vorfall verwickelt war, sind erfolgreiche Angriffe in Zukunft nicht auszuschließen.

Der ENISA-Report

Der ENISA-Report Threat Landscape for Supply Chain Attacks report schätzt, dass von den 2020 und 2021 analysierten Angriffen auf Lieferketten

- rund 50% bekannten APT-Gruppen zugeschrieben wurden
- rund 62 % das Vertrauen der Unternehmen in ihre Lieferanten ausnutzten
- in 62 % der Fälle Malware beteiligt war
- 66 % der Attacken den Code der Anbieter benutzten, um Kunden anzugreifen
- rund 58 % auf Daten wie Kundeninformationen oder IP-Adressen gerichtet waren

2. So verursacht die Integration von Drittanbietern neue Gefahren für Salesforce

Salesforce ist für viele Organisationen ein zentraler Faktor, der oft die gesamte Kundenmanagement- und Digital Experience-Strategie prägt. Daher gibt es am Markt eine große Nachfrage nach Möglichkeiten zur Anpassung und Konfiguration der Umgebung für unterschiedliche betriebliche Anforderungen.

Die Salesforce-Plattform lässt sich vielfach anpassen und mit Anwendungen, Komponenten und Cloud-Services von Drittanbietern erweitern. Salesforce AppExchange, der offizielle App-Store der Plattform mit mehr als 3.400 Apps, ermöglicht es Unternehmen, ihre Salesforce-Umgebungen über SOAP- oder REST-APIs mit externen Systemen oder Anwendungen zu koppeln. Diese Systeme lassen sich in verschiedenen Cloud-Umgebungen hosten und nutzen vielfältige proprietäre oder Open-Source-Software. Zudem unterstützt die Salesforce-Plattform die herkömmliche E-Mail- oder Webformular-basierte Integration

Angesichts so vieler Optionen finden Unternehmen sicher die Unterstützung von Drittanbietern für alle Anpassungen und Erweiterungen zu ihrer Salesforce-Umgebung. Allerdings erhöht jede neue Erweiterung auch das Risiko für die digitalen Lieferketten.

Hier gibt es eine Vielzahl potenzieller Gefahren:

Bösartige Betrüger

Schlimmstenfalls werden Drittanbieter-Assets gezielt als Angriffsvektoren eingesetzt. Kriminelle Gruppen laden reguläre Anwendungen herunter und erzeugen manipulierte Klone, in denen Schadcode versteckt ist, um sie dann erneut zum Download anzubieten. Bisher gab es zwar keine gemeldeten Fälle in AppExchange von Salesforce, aber dafür immer häufiger bei Android, Google und anderen Quellen. Die strikte Sicherheitsüberprüfung von Salesforce macht AppExchange zu einer durchaus sicheren Quelle, aber das gilt nicht für die vielen anderen Online-Software-Ressourcen. Außerdem ist es schwierig zu prüfen, was Anwendungen nach der Installation tun. Zuvor überprüfte Anwendungen können daher missbräuchlich verwendet werden.

Kompromittierte Software

Wie die Angriffe auf SolarWinds und Kaseya zeigen, können Cyber-Kriminelle auch auf digitale Lieferketten zugreifen, indem sie als erstes den Software-Anbieter attackieren. Dadurch können sie reguläre, bereits überprüfte Anwendungen als effektiven Angriffsvektor nutzen, der viele gängige Sicherheitssysteme umgeht. Solche Angriffe sind ressourcenintensiv und werden daher meist nur von organisierten Gruppen ausgeführt, die es auf bedeutende Organisationen abgesehen haben oder die eine große Anzahl von Opfern mit ausgefeilteren Angriffen wie Ransomware treffen wollen. Daher sind einzelne Salesforce-Nutzer zwar nicht die lohnendste Zielscheibe, aber Salesforce selbst und seine bekanntesten Integratoren werden es sein.

Schwachstellen im Code

Jeder digitale Inhalt kann auch ohne das Eindringen eines Angreifers Cyberrisiken mitbringen. Software-Schwachstellen sind ein ständiges Risiko bei Geschäften im digitalen Zeitalter. Im Jahr 2021 wurden unglaubliche 19.733 Schwachstellen gemeldet. Selbst die meistgetestete Anwendung eines renommierten Anbieters weist unweigerlich zumindest einzelne Schwachstellen auf.

Egal woher sie stammt, selbst eine einzige unsichere Anwendung oder Komponente eines Drittanbieters kann schon ausreichen, um eine schwerwiegende Sicherheitslücke zu erzeugen..

Eine komplexe Umgebung mit Hunderten zusätzlicher Anwendungen und Plugins ist schnell sehr schwierig zu verwalten. Bei so vielen herumlaufenden Ameisen mit unterschiedlichen Aufgaben können selbst die besten Administratoren kaum erkennen, was auf der anderen Seite des Ameisenhügels passiert.

Es gibt aber eine gefährliche Tendenz zu der Annahme, dass Umgebungen sicher bleiben, nur weil es sich um Salesforce handelt. Zwar erkennen Systemadministratoren sowie Entwicklungs- und Infrastrukturmanagement-Teams zunehmend die Probleme bei der Sicherung anderer Umgebungen wie AWS, doch die klarere Struktur von Salesforce bewirkt, dass es oft als in sich geschlossen und selbstsichernd gilt. Bei komplexeren Infrastructure-as-a-Service-Plattformen (IaaS) wie AWS sind IT-, Netzwerk- und Sicherheitsteams von Anfang an involviert, aber Salesforce erhält selten die gleiche Aufmerksamkeit.

Die Bedrohung aus dem Inneren

Wie andere digitale Umgebungen auch, kann Salesforce sehr anfällig sein, wenn es nicht richtig konfiguriert ist.

Falsche Anwendungskonfigurationen und ineffektive Identitätsverwaltung können Umgebungen schnell angreifbar machen. Angreifer sind versiert darin, wenig gesicherte Benutzerkonten und Anwendungen auszumachen, die mit Standardeinstellungen verwendet werden. Schwache Zugriffsrechte helfen Cyber-Angreifern, Umgebungen zu infiltrieren.

Das ist ein ernstes Problem – noch bevor Hunderte neuer Elemente durch Anwendungen und Komponenten von Drittanbietern eingeführt werden. Dies ist besonders problematisch für größere Unternehmen, wo ein Mangel an Koordination zwischen Filialen und Abteilungen dazu führt, dass Umgebungen durch redundante Anwendungen und Plugins für dieselben Aufgaben überladen sind. Kleine Unternehmen sind zwar schlanker, fügen aber eher spontan Komponenten ohne effektiven Schutz hinzu.

Salesforce hat nun Schritte zur Risikominimieerung und Verbesserung der Erkennung schlecht konfigurierter Freigaberegeln gesetzt und Release-Updates veröffentlicht, die die Standardeinstellungen in sicherere Einstellungen ändern. Salesforce Optimizer, eine Lightning Experience-Anwendung, eignet sich z. B. zur regelmäßigen Überprüfung und Aufdeckung potenzieller Probleme mit Gastbenutzern.

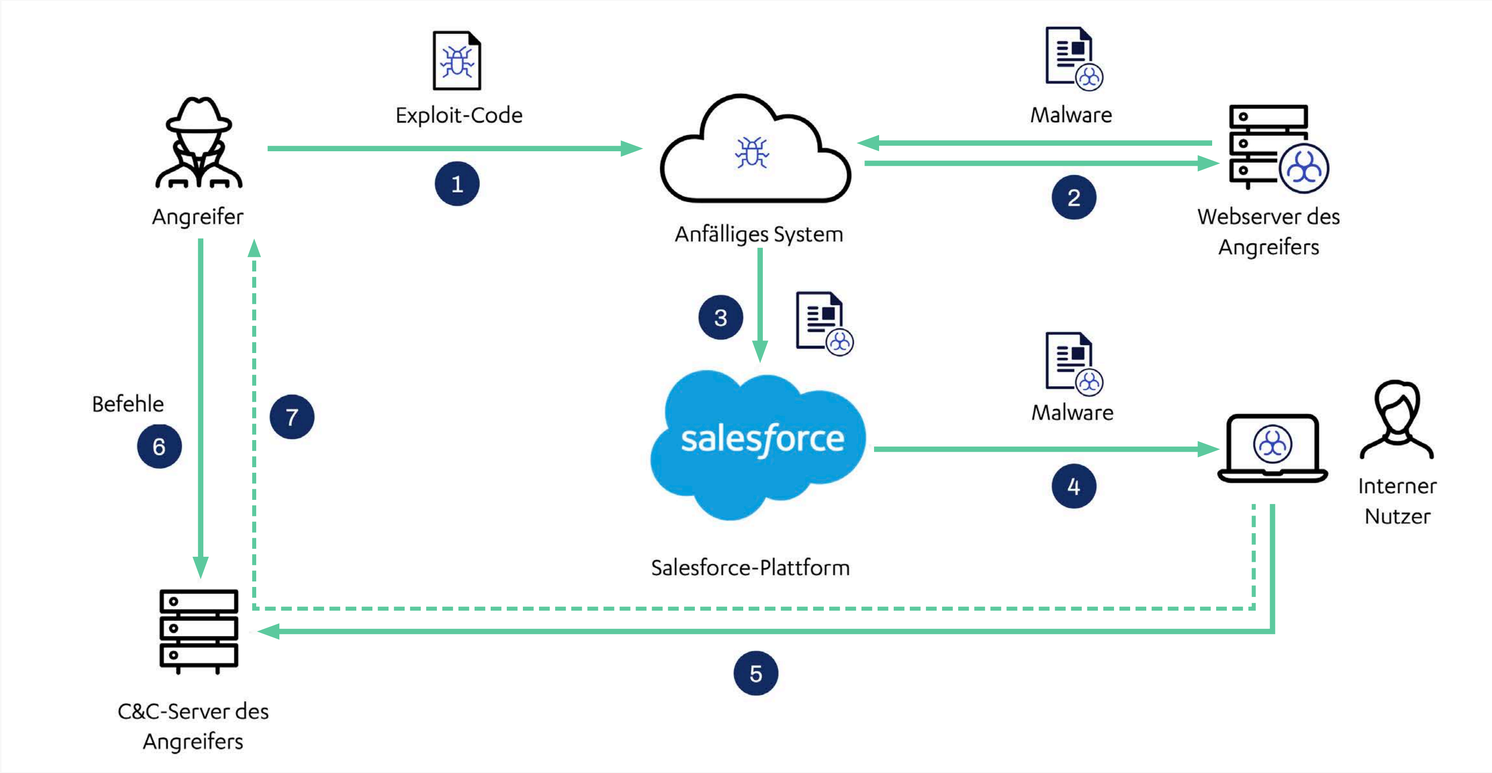
3. So funktioniert ein Angriff auf die Salesforce-Lieferkette

Wegen des großen Umfangs und der Komplexität der Salesforce-Umgebung gibt es eine Vielzahl von Möglichkeiten, wie diese im Rahmen eines Angriffs auf die digitale Lieferkette ins Visier genommen und ausgenutzt werden kann. Hier sind zwei Beispiele für Angriffsszenarien.

Szenario 1: Anfälliges Drittanbietersystem

Hier findet und benutzt der Angreifer eine Schwachstelle bei einer in Salesforce integrierten Softwareanwendung, z. B. einem Tool, das Daten für Analysen abruft, und erlangt so Remote-Zugriff auf das System. Die anfällige Anwendung ist über eine API mit Salesforce verbunden, und da APIs meist als vertrauenswürdiger gelten als ein menschlicher Benutzer, kann der Angreifer recht einfach auf das System zugreifen.

Der Angreifer kann versuchen, Daten in Salesforce zu stehlen oder zu schädigen, nutzt aber evtl. auch die Funktionen der Plattform für seine Angriffsstrategie. So. werden etwa Schad-Dokumente und -URLs in der ganzen Umgebung verteilt, damit arglose Nutzer inkl. Mitarbeiter, Kunden und andere Teilnehmer sie anklicken und herunterladen. Diese Nutzer werden dann missbraucht, indem ihr Systemzugang für die Fortsetzung des Angriffs auf die übrige IT-Infrastruktur des Unternehmens ausgenutzt wird.



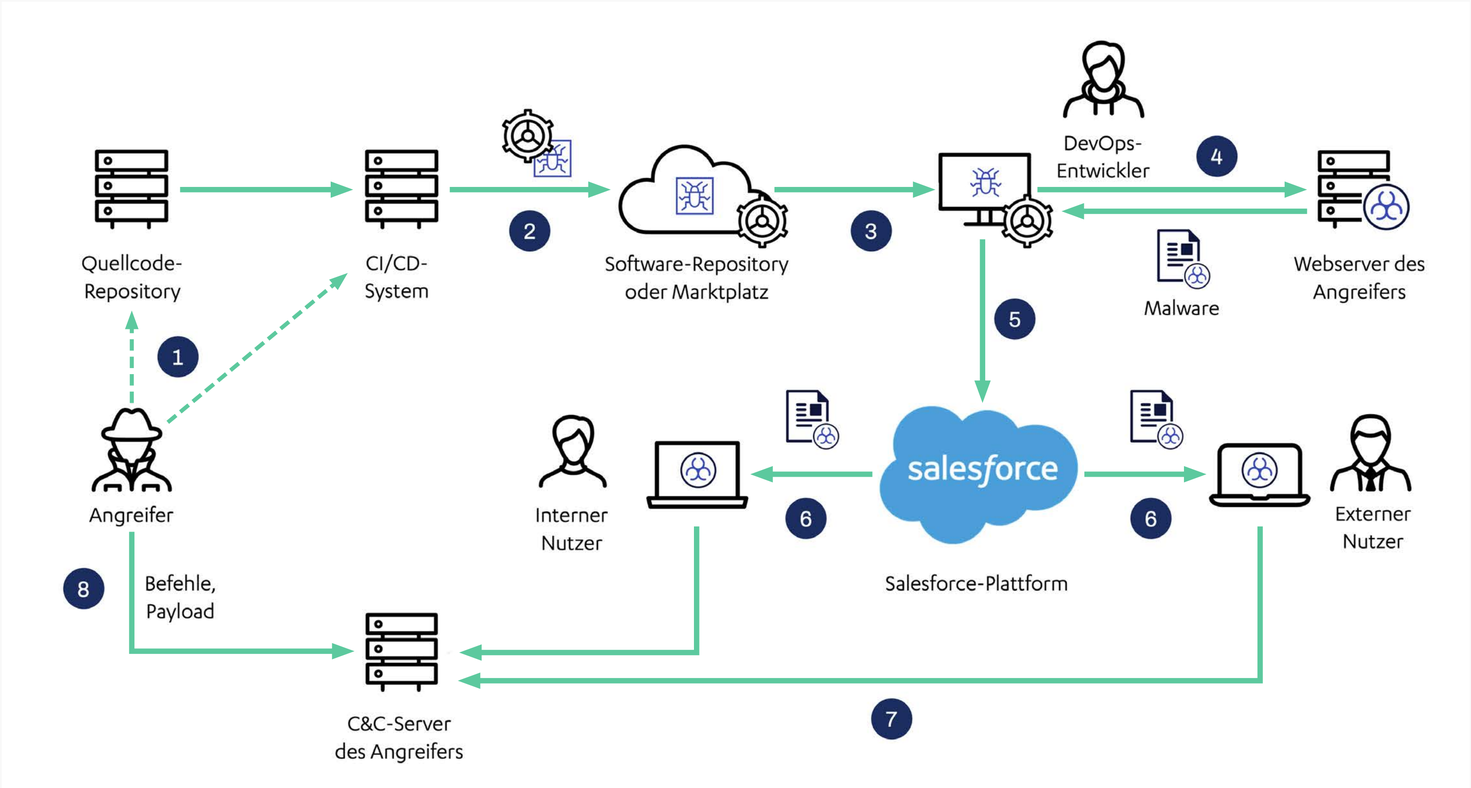
1. Der Angreifer nutzt eine Schwachstelle im Cloud- (oder On-Premise-) System eines Drittanbieters aus, das mit Salesforce verknüpft ist.
2. Der Angreifer startet den Exploit-Code, um sich Zugang zu dem anfälligen System zu verschaffen und Malware von dem speziellen Webserver herunterzuladen.
3. Der Angreifer "injiziert" Malware in die Salesforce-Plattform. und hängt sie z. B. an einen Fall oder einen Chatter-Post an oder lädt sie in die gemeinsame Dateibibliothek hoch..
4. Der interne Nutzer lädt eine Datei mit Malware herunter und öffnet sie auf seinem Gerät. Er bemerkt nichts Besonderes.
5. Die Malware ruft den vom Angreifer gehosteten Command-and-Control-Server (C&C) auf.
6. Der Angreifer sieht, dass die Malware im System ist und sich erfolgreich mit dem C&C-Server verbunden hat. Er sendet dann der Malware zusätzliche Befehle oder Nutzdaten.
7. Der Angreifer holt sich sensible Daten vom Computer des internen Nutzers und/oder von Salesforce..

Szenario 2: Kompromittierte Entwickler-Tools

In diesem Szenario attackiert der Angreifer zunächst ein Quellcode-Repository oder das CI/CD-System eines Softwareanbieters, um Schadcode in dessen Produkt einzuschleusen. Der erste Zugriff auf das System kann unterschiedlich erfolgen, wobei Phishing zur Erlangung von Benutzeranmeldedaten eine der häufigsten Taktiken ist, wie der Fall SolarWinds zeigt.

Die Anwendung bzw. Komponente wird dann in die Salesforce-Umgebung integriert, damit der Angreifer ihre Konnektivität nutzen kann, um andere Nutzer und Endpunkte zu gefährden. Von hier aus verfolgt er dann seine schädlichen Ziele weiter. Das kann sich sogar wiederholen, wobei das angegriffene Unternehmen als Sprungbrett für einen erweiterten Angriff auf die Lieferkette dient.

Der Angreifer kann beim ersten Mal direkt auf die Salesforce-Instanz zugreifen oder eine Backdoor einrichten und warten, bis der Integrator Zugang zur Produktion hat. Entwickler vertrauen gerne blind auf die Sicherheit ihrer Tools, vor allem solche von bekannten Anbietern. Wie SolarWind zeigt, kann auch ein guter Anbieter eine Gefahrenquelle werden, wenn er von organisierten Angreifern geschädigt wird.



1. Der Angreifer scannt das öffentliche Quellcode-Repository und findet Anmeldedaten für das CI/CD-System, auf das er dann Zugriff erhält.
2. Der Angreifer injiziert eigens erstellte Nutzdaten in das vom CI/CD-System erstellte und im offiziellen Software-Repository oder auf dem Marktplatz veröffentlichte Softwarepaket.
3. Der DevOps-Entwickler holt das Paket aus dem Repository/Marktplatz mit der Payload und startet es auf seinem Computer.
4. Die Payload lädt Malware vom Webserver des Angreifers herunter.
5. Da der DevOps-Entwickler Zugriff auf Salesforce hat, wird die Malware in Salesforce hochgeladen.
6. Der interne und/oder externe Nutzer lädt Malware herunter und öffnet sie auf seinem Computer.
7. Die Malware verbindet sich mit dem Command-and-Control-Server (C&C) des Angreifers.
8. Der Angreifer sendet Befehle und zusätzliche Schaddaten an den/die Computer des Opfers.

4. Best Practices zur Eindämmung digitaler Gefahren für die Lieferkette

Cybersicherheit ist komplex und kann nicht mit einem einzigen Allheilmittel erreicht werden. Das gilt besonders für eine so große und umfassende Cloud-Umgebung wie Salesforce. Daher ist zur Eindämmung der Gefahr von Angriffen auf die digitale Lieferkette von Salesforce ein mehrschichtiger Ansatz nötig, der die richtigen Sicherheitslösungen mit den richtigen Prozessen und Regeln kombiniert. Zu den wichtigsten Elementen einer Salesforce-Sicherheitsstrategie gehören:

Implementierung eines Application Portfolio Managements (APM)

Alle Anwendungen und Komponenten müssen vor der Integratioin in die Salesforce-Umgebung gründlich geprüft werden, einschließlich aller bekannten Schwachstellen und früherer Vorfälle, die mit der Anlage und ihrem Anbieter zu tun haben – und der Frage, ob diese Probleme behoben sind. Ein implementiertes Application Portfolio Management (APM) koordiniert die Prüfung zukünftiger Anwendungen und die Erfassung vorhandener Assets.Die Sorgfaltspflicht erstreckt sich auch auf den Anbieter selbst, und Unternehmen sollten prüfen, dass alle Drittanbieter über ein angemessenes Sicherheitsniveau für das Risiko eines Angriffs oder einer versehentlichen Implementierung einer Schwachstelle in Updates verfügen.

Unternehmen mit erhöhtem Risikoprofil können als Teil ihrer Service Level Agreements (SLAs) Sicherheitsauflagen einführen. Im aktuellen weltpolitischen Klima sollten sie auch besonders auf die Herkunft der Anbieter achten, um die Gefahr staatlich gelenkter Akteure zu minimieren.

Erfassung potenzieller Auswirkungen von Sicherheitslücken

Unternehmen sollten nicht nur die Assets selbst überprüfen, sondern auch ihren Ort in der Salesforce-Umgebung und die Folgen einer Sicherheitsverletzung. Das heißt, es ist zu prüfen, welche Funktionen das Produkt hat und wie es mit Salesforce sowie mit anderen Bereichen der IT-Infrastruktur verbunden ist.

Die Einbeziehung von Gefahren ist ein unvermeidlicher Kostenfaktor, aber Unternehmen müssen einfach sicher sein, dass das Risikolevel im Verhältnis zu den Vorteilen neuer Komponenten vertretbar ist und dass sie dies in ihre Sicherheitsstrategie einbeziehen.

Assets von Drittanbietern: So behalten Sie alles im Blick

Bei größeren Salesforce-Umgebungen mit hunderten Komponenten von Drittanbietern kann es praktisch unmöglich sein, alles im Blick zu behalten. Administratoren müssen jedoch unbedingt auf maximale Transparenz achten, um blinde Flecken zu vermeiden, die zu gravierenden Störungen führen können.

Im Idealfall sollten effektive Kontrolle und Sicht auf die wichtigsten und gefährdetsten Elemente von Drittanbietern Priorität haben, um sich dann schrittweise von dort aus vorzuarbeiten. Strukturierte Richtlinien für die Einführung neuer Ressourcen gewährleisten außerdem den Überblick über wachsende Umgebungen und verringern die Anzahl redundanter Anwendungen.

Beseitigen Sie Fehlkonfigurationen und Zugangsprobleme

Zusätzlich zum Blick nach außen auf die digitalen Lieferketten müssen Unternehmen auch auf ihre internen Prozesse achten. Falsch konfigurierte Anwendungen und eine fehlerhafte Zugriffsverwaltung können Cyber-Angreifern Tür und Tor öffnen, auch ohne dass Drittanbieter beteiligt sind.

Administratoren sollten ihre Salesforce-Umgebung auditieren, damit die Anwendungen korrekt mit den entsprechenden Zugriffsrechten konfiguriert sind. Im Idealfall sollten alle Assets auf die minimal erforderliche Zugriffsebene eingestellt und alle Freigabefunktionen deaktiviert sein, sofern dies nicht explizit erforderlich ist.

Dasselbe gilt für die Nutzer in der Organisation. Nutzerprofile wie auch automatisierte Systeme sollten nach dem Prinzip der minimalen Berechtigung konfiguriert, d. h. nur mit den für die jeweilige Rolle erforderlichen Zugriffsrechten ausgestattet werden. Das gilt besonders für Systemadministratoren, da Unternehmen oft dazu neigen, jedem Benutzer im System automatisch Administratorrechte zu geben.

Best-Practice-Verfahren für den Systemzugang verringern die Gefahr, dass ein Angreifer die Umgebung missbraucht, und mindern die Folgen bei kompromittierten Benutzern oder Anwendungen.

Denken Sie unbedingt daran, dass dies keine einmalige Maßnahme ist. Alle neuen Funktionen in Salesforce sollten periodisch mithilfe der beigefügten Versionshinweise überprüft werden.

Unternehmen mit besonders komplexen Umgebungen sollten ihre Systemkonfigurationen im Idealfall periodisch gründlich überprüfen. Der Cloud-Consulting-Service von WithSecure sorgt mit seinem Know-how dafür, dass hier nichts übersehen wird.

Blockieren schädlicher Informationen in Salesforce

Angreifer nutzen zahlreiche Methoden für ihre Angriffe auf Lieferketten, wobei die Nutzung gestohlener Anmeldedaten zu den häufigsten Verfahren gehört. Um Angriffe auf die Lieferkette mit Phishing, gestohlenen Benutzerdaten und Malware zu verhindern, brauchen Unternehmen einen umfassenden Security-Ansatz mit Endpunkt-, Netzwerk- und Cloud-basiertem Schutz.

WithSecure bietet verschiedene Lösungen für Kunden, um neuartige Angriffe zu verhindern, zu erkennen und darauf zu reagieren.

Zu beachten ist aber auch, dass Salesforce selbst als Angriffsvektor genutzt werden kann. Der Support für das Hoch- und Herunterladen von Inhalten ist eine wichtige Funktion, mit der etwa Versicherungskunden Schadensberichte und Identitätsnachweise hochladen oder Personaldienstleister Stellenprofile senden und empfangen können.

Diese Funktion kann auch missbraucht werden, um Schaddateien und -URLs in Salesforce hochzuladen - statt Phishing per E-Mail. Eine kompromittierte Salesforce-Umgebung lässt sich zudem nutzen, um Schadinhalte mit Benutzern und Kunden zu teilen.

Salesforce ist für die Sicherung der Daten in seiner Umgebung verantwortlich, nicht aber für hoch- oder heruntergeladene Inhalte - diese Verantwortung liegt beim Unternehmen..

WithSecure Cloud Protection for Salesforce ist eine der effektivsten Maßnahmen, um diesen Schwachpunkt zu beseitigen. Die Lösung ist marktweit führend und wurde entwickelt, um Angriffe über Schaddateien und -URLs zu verhindern, die von raffiniert vorgehenden kriminellen Gruppen und Nutzern außerhalb des Cybersicherheitsbereichs eines Unternehmens in Salesforce hochgeladen werden.

Die Lösung scannt alle hoch- und heruntergeladenen Inhalte in Echtzeit, um schädliche Inhalte mithilfe aktuellster Bedrohungsdaten von WithSecure zu erkennen und zu blockieren. Cloud Protection for Salesforce wurde gemeinsam mit Salesforce entwickelt, um einen leistungsstarken Schutz ohne Beeinträchtigung Benutzerfreundlichkeit zu bieten.

Einführung eines wirksamen Reaktionsplans

Schließlich ist noch etwas wichtig: Die Gefahr einer Datenpanne ist nicht mehr eine Frage des Ob, sondern des Wann. Selbst Unternehmen mit mit großen Budgets für bewährte Sicherheitsstrategien werden von entsprechend fähigen und entschlossenen Angreifern attackiert.

Daher sollten sich alle Unternehmen auf den Worst Case eines Angriffs auf die digitale Lieferkette mit Auswirkungen auf ihre Salesforce-Umgebung vorbereiten. Vorrangig ist hier die Implementierung eines effektiven Reaktions- und Bereinigungsplans, um Gefahren schnell zu erkennen und zu stoppen und den Normalbetrieb schnellstmöglich wiederherzustellen.

Der Salesforce Shield-Service bietet Zugriff auf Funktionen wie detaillierte Protokollierung und feldweise Verschlüsselung. So werden wichtige Anforderungen wie die Aktivitätsüberwachung unterstützt, die zur Erkennung und Analyse von Vorfällen nützlich sind.

Unternehmen brauchen auch Zugang zu speziellen Skills und Tools, um die Herkunft des Angriffs zu finden und weitere Gefahren in der Umgebung zu beseitigen, z. B. versteckte Malware-Dropper und Command-and-Control-Programme. Die Kooperation mit einem spezialisierten Partner ist hierfür eine der wirtschaftlichsten Möglichkeiten.

Unternehmen müssen auch planen, wie sie die Auswirkungen einer beeinträchtigten Salesforce-Umgebung auffangen, die zum Stillstand ihres gesamten CRM-Prozesses führen könnte. Die Implementierung regelmäßiger System-Backups und die Nutzung alternativer Kommunikationsmethoden können helfen, den Betrieb weiterzuführen, während die Krise gemeistert wird.

5. Den Gefahren für digitale Lieferketten im Jahr 2022 vorbeugen

- Das Risiko für Lieferketten wächst rapide, da Angreifer neue Wege suchen, um Schutzmaßnahmen zu umgehen.
- Die erweiterte Salesforce-Umgebung ist ohne Schutzmaßnahmen der Unternehmen als Angriffspunkt anfällig.
- Unternehmen sollten sich jetzt vorbereiten, bevor sie zu den Opfern zählen.

Risiken in der Lieferkette sind ein unvermeidlicher Teil der Geschäftstätigkeit im digitalen Zeitalter. Unternehmen müssen wissen, dass die Bedrohung wächst, da sich ihre eigenen Lieferketten ausweiten, aber auch Angreifer nach immer neuen Wegen suchen, um Sicherheitsmaßnahmen zu umgehen.

Unternehmen müssen sicherstellen, dass ihre Kapazitäten zur Überwachung und Kontrolle der erweiterten Lieferketten mit der Ausweitung ihres digitalen Fußabdrucks und der Vernetzung mit immer mehr Drittanbietern mithalten.

Salesforce muss in diesen Sicherheitskonzepten einen zentralen Platz einnehmen, da es nicht nur ein wesentliches CRM-System ist, sondern auch eine Umgebung, in der Hunderte verschiedener Elemente von Drittanbietern zu finden sein können.

Während Salesforce für die Sicherheit der eigenen Infrastruktur zuständig ist, sind die Benutzer für die Komponenten und Inhalte von Drittanbietern verantwortlich, die in die Umgebung gelangen - ein Ansatz, der als Modell der geteilten Verantwortung (Shared Responsibility) bekannt ist.

Markante Vorfälle wie SolarWinds, Kaseya und Log4J bestimmen weiterhin die Schlagzeilen und schärfen das Bewusstsein für Risiken in der Lieferkette. Salesforce ist aber noch nicht Teil dieser Diskussion. Kontaktieren Sie jetzt unser Team, um zu erfahren, wie Sie mit WithSecure diesen kritischen Angriffspunkt schützen können, bevor er entdeckt und für einen ernsten Cyberangriff ausgenutzt wird.

WithSecure™ Cloud Protection for Salesforce ergänzt die nativen Sicherheitsfunktionen von Salesforce, indem es Gefahren in hochgeladenen Dateien und URLs mildert.

Get in touch

available on AppExchange

salesforce

Wer wir sind

WithSecureTM ist Ihr zuverlässiger Partner für Cybersicherheit. IT-Dienstleister, MSSPs und Unternehmen sowie die größten Finanzinstitute, Hersteller und Tausende der weltweit avanciertesten Kommunikations- und Technologieanbieter vertrauen uns bei ergebnisorientierter Cybersicherheit, die ihren Betrieb schützt und verbessert. Unser KI-gesteuerter Schutz sichert Endpunkte und Cloud-Zusammenarbeit, und unsere intelligenten Erkennungs- und Reaktionsfunktionen werden von Spezialisten bereitgestellt, die Geschäftsrisiken aufdecken, indem sie proaktiv nach Bedrohungen suchen und Angriffe in Echtzeit abwehren. Unsere Berater arbeiten mit Unternehmen und Technologieanbietern zusammen, um durch faktenbasierte Sicherheitsberatung Resilienz zu gewährleisten. Mit über 30 Jahren Erfahrung in der Entwicklung von Technologien, die den Unternehmenszielen entgegenkommen, haben wir unser Portfolio so entwickelt, dass wir mit unseren Partnern durch flexible Geschäftsmodelle weiter wachsen können.

WithSecureTM ist Teil der F-Secure Corporation, die 1988 gegründet wurde und an der NASDAQ OMX Helsinki Ltd. notiert ist.

WITH secure