2023: Wie schützen Sie Ihre Salesforce-Cloud?

Einschätzung der Bedrohungen und Herausforderungen

WITH secure

Einführung

2022 war erneut ein turbulentes Jahr für die Cybersicherheit. Bekannte Tätergruppen wie Lapsus$ und Conti haben mit umfangreichen Angriffen auf führende Unternehmen und nationale Infrastrukturen für Aufsehen gesorgt. Auch weniger bekannte kriminelle Organisationen stellen durch Taktiken wie gezielte Ransomware eine zunehmende Gefahr dar.

Cyberangriffe erfolgen vorwiegend über herkömmliche IT-Systeme und Endgeräte. Da aber immer mehr Unternehmen ihre Infrastruktur und ihre Betriebsabläufe in die Cloud verlagern, passen sich Gefährder schnell an und verlagern ihren Fokus auf cloudbasierte Umgebungen wie Salesforce.

Mehr als 150.000 Unternehmen verlassen sich bei ihren entscheidenden CRM-Aktivitäten (d. h. beim Customer Relationship Management) auf die Salesforce-Plattform, die entsprechend große Mengen an wertvollen und sensiblen Kundendaten enthält. Salesforce ist außerdem in hohem Maße kollaborativ und adaptierbar, und es unterstützt eine Vielzahl von Plug-ins von Drittanbietern und Optionen für die Konnektivität.

Die Kombination dieser Faktoren macht Salesforce zu einem verlockenden Ziel für Angreifer. Obwohl bisher keine größeren Fälle gemeldet wurden, glauben wir, dass dies nur eine Frage des Wann und nicht des Ob ist.

Salesforce ist an sich eine sehr sichere Plattform, die über zahlreiche Kontrollen verfügt, um einen sicheren Speicherort für Ihre Daten zu gewährleisten. Viele Kontrollen müssen jedoch von den Kunden selbst korrekt konfiguriert werden, um ihre Daten sicher zu halten - genau das ist die Idee des Modells der gemeinsamen Verantwortung.

In diesem Bericht teilen drei Salesforce-Sicherheitsexperten ihre Erkenntnisse, worauf man sich im kommenden Jahr beim Thema Salesforce-Sicherheit konzentrieren sollte. Ihre Erfahrungen werden durch die neuesten Daten der WithSecure™-Marktforschung zur Cloud- und Salesforce-Sicherheit im Jahr 2022* ergänzt.

Lesen Sie im Folgenden mehr über die Ergebnisse der Untersuchung und die wichtigsten Prioritäten für die Salesforce-Sicherheit im Jahr 2023 – und was Sie tun können, um Vorsprung zu gewinnen und das Risiko zu minimieren.

Die wichtigsten Sicherheits-themen im Jahr 2022:

- Die bedeutendsten Sicherheitsprobleme laut IT-Experten und Salesforce-Administratoren
- Die Bedrohung durch Fehlkonfigurationen und nicht überwachte Assets
- Die Zunahme von schädlichen Dateien und URLs in Salesforce
- Ermittlung der richtigen Sicherheitskontrollen
- Unsere acht wichtigsten Empfehlungen zur Absicherung von Salesforce im Jahr 2023

*WithSecure™ Marktforschung: B2B-Marktforschung mit 3.072 IT-Entscheidungsträgern und Meinungsführern in 12 Ländern im Zeitraum von April bis Mai 2022: Großbritannien, Frankreich, Deutschland, Belgien/Niederlande, Finnland, Norwegen, Schweden, Dänemark, USA, Kanada und Japan.

Unsere Experten:

Dmitriy Viktorov
Head of Product and Technology, Cloud Protection bei WithSecure™

Dmitriy ist ein erfahrener Produkt- und Sicherheitsprofi, der leidenschaftlich gerne komplexe Probleme löst und Kunden dabei hilft, ihre Cloud und ihre digitalen Dienste sicher und geschützt zu halten. Er hatte verschiedene Positionen in den Bereichen Forschung und Entwicklung, Produktmanagement und Technology Office inne und leitet derzeit die Produktentwicklung von Cloud Protection für Salesforce.

Pankaj Paryani
Salesforce Technical Lead bei WithSecure™

Pankaj ist kompetenter Salesforce-Entwickler und -Berater und hat mehrere Projekte für Kunden in den USA, Großbritannien und der APAC-Region entwickelt. In seiner aktuellen Funktion leitet er das CRM-Entwicklungsteam bei WithSecure™, um zu gewährleisten, dass Vertrieb und Service die Anforderungen der Kunden sicher erfüllen.

Doug Merrett
Salesforce Security, Compliance, Privacy and Resilience Specialist bei Platinum7

Doug ist ein leidenschaftlicher Fürsprecher der Sicherheit. Er war 13 Jahre lang für Salesforce als Plattform- und Sicherheitsspezialist in Großbritannien und Australien gearbeitet. In dieser Zeit hat er vielen Kunden geholfen, den Salesforce-Ansatz für Sicherheit und Infrastruktur zu verstehen und sie bei der Optimierung der Sicherheit ihrer auf der Salesforce-Plattform gespeicherten Daten beraten. Im Juni 2021 gründete Doug sein eigenes Beratungsunternehmen, Platinum7, das sich ausschließlich auf Salesforce Security, Compliance und Resilience konzentriert.

Die bedeutendsten Sicherheitsprobleme laut IT-Experten und Salesforce-Administratoren

Die 5 größten Sicherheitsherausforderungen

1. Verhinderung von Datenpannen
2. Gewährleistung des Schutzes vor Malware und Ransomware
3. Erkennung von Angriffen, die möglicherweise andere Sicherheitsmaßnahmen unterlaufen haben
4. * Verhinderung hochentwickelter E-Mail-basierter Bedrohungen, wie Phishing oder Kompromittierung von Geschäfts-E-Mails (BEC).
5. Gewährleistung der Sicherheit von Cloud-basierten Anwendungen für die Zusammenarbeit, wie Office 365 und Salesforce

* Cloud and Zusammenarbeit

Cloud-Plattformen wie Salesforce sind für die Umsetzung von Remote- und Hybrid-Arbeitsstrategien, die durch die Pandemie beschleunigt wurden, unverzichtbar geworden. Darüber hinaus bieten sie Vorteile aufgrund verbesserter Effizienz und Agilität sowie geringerer Kosten und Ressourcen. Cloud-Umgebungen schaffen jedoch auch Lücken und veränderliche Elemente, von denen viele außerhalb einer direkten Kontrolle liegen.

“Jahrzehntelang war alles direkt vor Ort unter Ihrer Kontrolle, und Sie mussten sich nur um eine begrenzte Anzahl externer Verbindungen kümmern. Heute liegt alles oder vieles in der Cloud, und viele kritische Systeme sind einer direkten Kontrolle entzogen.”

Pankaj Paryani, Salesforce Technical Lead, WithSecure™

Was waren in den letzten 18 Monaten Ihre drei größten Probleme bei der Verwaltung der Datensicherheit?

(Aus dem Salesforce-Bericht zu Top Security Trends für 2022)

*59% Sicherheitsverwaltung durch Drittanbieter

**53% Einhaltung von Compliance-Vorschriften

49% Sicherheit bei mobilen Geräten

38% Ressourcenbeschränkungen

37% Schwachstellenmanagement

28% Verwaltung proaktiver Maßnahmen zur Verhinderung von Hackerangriffen

15% Revision

5% Nutzerverhalten

*Sicherheitsverwaltung durch Drittanbieter

Salesforce ist so angelegt, dass es hochgradig adaptierbar ist, damit neue Funktionen bei Bedarf leicht gefunden und implementiert werden können. Allein auf Salesforce AppExchange gibt es mehr als 3.400 Anwendungen sowie unzählige APIs und Plug-ins von Drittanbietern, die online zugänglich sind. Das ist zwar von Vorteil für die Integration und Zugänglichkeit, bringt aber auch eine umfangreiche Lieferkette von Drittanbietern mit sich, die schnell außer Kontrolle geraten kann. Jedes Add-on erhöht die potenzielle Anfälligkeit für Angriffe auf die Lieferkette. Angesichts der Tatsache, dass Angriffe auf die Lieferkette in den letzten Jahren die allgemeine Cybersicherheitslandschaft dominiert haben, ist es kein Wunder, dass hier ein Hauptproblem für die Sicherheit von Salesforce liegt. Lesen Sie mehr in unserem neuesten Bericht über das Management von Drittanbietern in Salesforce.

**Regulierung und Compliance

Das regulatorische Umfeld hat sich weiterentwickelt, und die Einhaltung von Sicherheits- und Datenschutzbestimmungen ist mit zunehmender Digitalisierung und Cloud-Migration immer komplexer geworden. Da verschiedene Regionen ihre eigenen Rechtsvorschriften und Aufsichtsbehörden haben, müssen Unternehmen genau wissen, wohin ihre Daten übertragen, wo sie gespeichert und verarbeitet werden sowie wer Zugriff auf diese Daten hat. Außerdem müssen sie auf die branchenspezifischen Vorschriften achten, z. B. im Gesundheits- und Finanzwesen.

Mit der Einführung neuer und der Aktualisierung anderer Vorschriften stehen weitere Änderungen vor der Tür. Die Europäische Kommission veröffentlicht demnächst die neue Richtlinie NIS2 (Netz- und Informationssysteme), die voraussichtlich innerhalb der nächsten 18 Monate in Kraft treten wird.

Was sind Ihre drei größten Probleme in der IT-Sicherheit?

Ransomware und Phishing

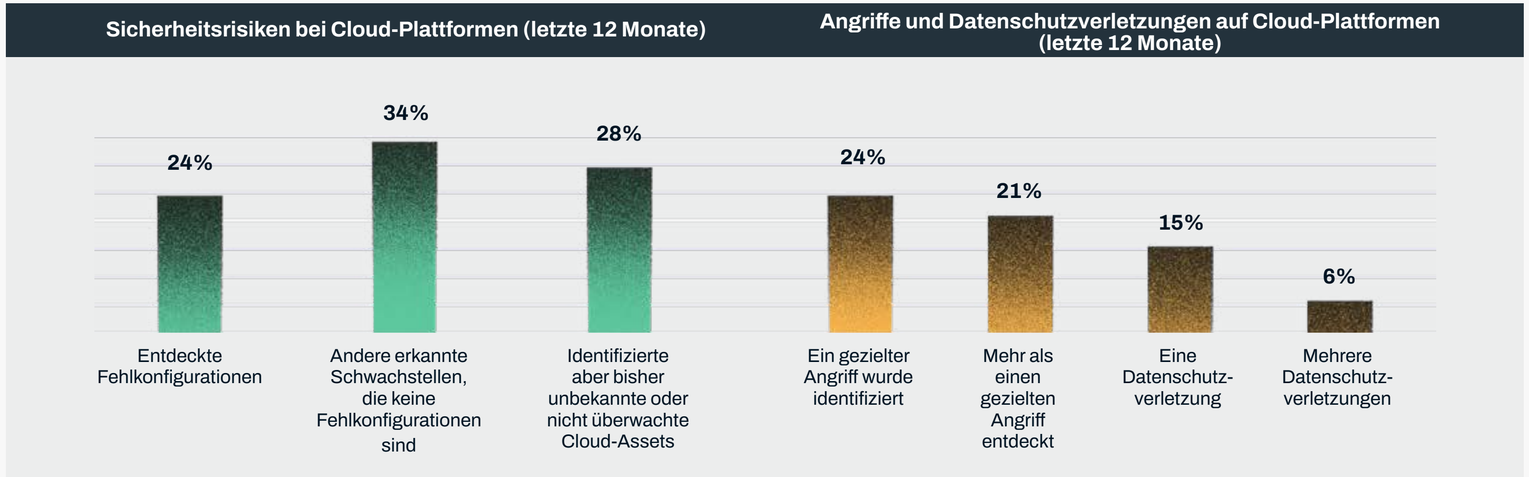
Phishing wird in der Regel als eine durch E-Mails übertragene Bedrohung betrachtet, und Angreifer nutzen auch weiterhin E-Mails für Phishing-Angriffe. Leider ist aber auch Salesforce nicht immun gegen Phishing-Angriffe, da die Plattform verschiedene E-Mail-basierte Abläufe wie E-Mail-to-Case oder E-Mail-to-Chatter umfasst. Darüber hinaus bietet Salesforce mit Slack, Chatter und anderen Optionen von Drittanbietern eine Reihe von Kommunikations- und Kollaborationskanälen, die ebenfalls für Phishing-Angriffe missbraucht werden können.

Auch wenn die Salesforce-Umgebung selbst für gängige Ransomware relativ unzugänglich ist, kann sie zur Übertragung schädlicher Dateien und Links auf Zielsysteme ausgenutzt werden. Man muss auch bedenken, dass sich Ransomware und andere Schadprogramme schnell weiterentwickeln. Die hochflexiblen Kommunikationsfunktionen von Salesforce könnten potenziell Ansatzpunkte für solche Bedrohungen der nächsten Generation bieten.

Sichtbarkeit und Kontrolle des Zugangs

Aus eigener Erfahrung haben unsere Experten auch die Sichtbarkeit und Kontrolle von Netzwerkverbindungen als ein wichtiges Thema hervorgehoben. Unternehmen müssen genau wissen, wie interne und externe Benutzer auf wichtige Daten und Systeme zugreifen können und wie ihre Salesforce-Plattform mit anderen Systemen verbunden ist und interagiert.

Die Bedrohung durch Fehlkonfigurationen und nicht überwachte Assets



Ein Viertel der Befragten glaubt, in den letzten 12 Monaten Opfer eines gezielten Angriffs geworden zu sein. Das zeigt, dass die Angreifer immer raffinierter und organisierter vorgehen. Allerdings machen viele Unternehmen den Angreifern das Leben leicht, indem sie ihre Cloud-Umgebungen nicht richtig konfigurieren und überwachen.

Fehlkonfigurationen sind besonders häufig, da die Optionen für die durchschnittliche Cloud-Umgebung sehr umfangreich sind. Die häufigsten von uns festgestellten Salesforce-Konfigurationsprobleme haben mit dem Zugriff zu tun. Benutzer wie Anwendungen verfügen oft über Standardberechtigungen, die ein hohes Maß an privilegiertem Zugriff auf die Plattform zulassen. Das erhöht das Risiko durch externe Angreifer und böswillige Insider beträchtlich und führt auch zu mehr Anfälligkeit für menschliche Fehler.

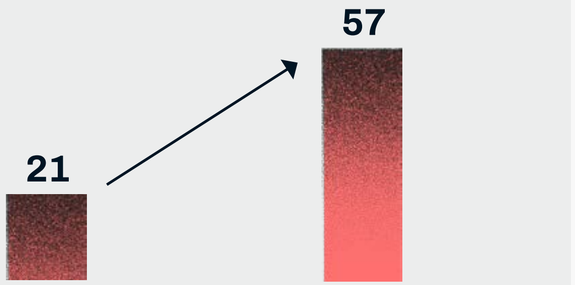
Darüber hinaus kämpfen Unternehmen oft damit, den Überblick über ihre Systeme zu behalten. Das Software-as-a-Service (SaaS)-Modell hat zur Folge, dass es für die Mitarbeiter nur allzu leicht ist, neue Add-ons und Anwendungen zu beschaffen und zu implementieren, während die IT-Abteilung nichts davon mitbekommt. Folglich ist Salesforce oft mit Elementen gespickt, die nicht ausreichend geprüft wurden und nicht auf Schwachstellen oder verdächtige Aktivitäten überwacht werden.

“Komplexität ist der Feind der Sicherheit. Je komplexer die Umgebung, desto eher wird etwas übersehen und nicht richtig konfiguriert. Als hochgradig adaptierbare Plattform bietet Salesforce viele Möglichkeiten für Fehlkonfigurationen.”

Dmitriy Viktorov, Head of Product and Technology, Cloud Protection, WithSecure™

Schädliche Dateien und URLs in Salesforce sind auf dem Vormarsch

Datei-/URL-Erkennungen pro Kunde und Monat



In den letzten 6 Monaten stieg das Erkennungsvolumen von schädlichen Dateien und URLs auf 250 %.

Es ist bekannt, dass sich die Anzahl der Angriffsversuche stetig erhöht hat. Dieser Trend wird durch WithSecures eigene Daten aus der Überwachung von Salesforce-Umgebungen eindeutig bestätigt. In den letzten sechs Monaten haben wir durchschnittlich 57 schädliche Dateien oder URLs pro Kunde und Monat entdeckt. Dies entspricht einem Anstieg auf 250 Prozent gegenüber dem Durchschnitt der vorangegangenen sechs Monate.

Schädliche HTML-Dateien sind die gängigste Angriffsart und machen über die Hälfte der von uns entdeckten Dateien aus.

Die 5 häufigsten Erkennungen von Schadprogrammen und Dateitypen

1. HTML Dateien 49 %
2. Archiv rar/zip-Dateien 23 %
3. Microsoft-Office-Dateien 10%
4. Exe-/com-Dateien 4 %
5. PDF-Dateien 3%

*letzte 6 Monate

Die Top 5 Malware Typen:

1. Trojaner 54%
2. Adware 15%
3. Exploit 12%
4. Andere 12%
5. Downloader 2%

*letzte 6 Monate

Bei den von uns identifizierten Malware-Angriffen handelte es sich mehrheitlich um Malware vom Typ Trojaner.

Wir haben auch verschiedene Tendenzen dahingehend festgestellt, dass Angreifer gezielt nach Salesforce-Assets suchen, um sie anzugreifen. Wenn ein Kunde z. B. Salesforce Experience Cloud implementiert und ein Portal für das Hochladen von Inhalten einrichtet, steigt die Anzahl der erkannten Dateien und URLs kurz darauf rasant an.

Bemerkenswert ist auch, dass mehr schädliche URLs als Dateien entdeckt werden. Die Angreifer haben erkannt, dass immer mehr Unternehmen ihre Strategien auf das Scannen von Dateien ausgerichtet haben, und sind zu dem komplexeren und schwieriger zu entdeckenden URL-Ansatz übergegangen.

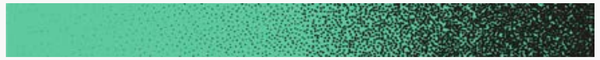
“Jeder weiß, dass nach Schaddateien gescannt werden muss, aber das Scannen von URLs ist immer noch nicht Standard, vor allem außerhalb von E-Mails.”

Doug Merrett, Salesforce Security, Compliance, Privacy and Resilience Specialist, Platinum7

Ermittlung der richtigen Sicherheitskontrollen

Welche der folgenden Aussagen zur Sicherheit von Cloud-Anwendungen treffen am ehesten auf Ihr Unternehmen/Ihre Organisation zu?

(z. B. Office 365, Google Workspace, Salesforce)



27.6%

Wir verwenden integrierte Standard- und erweiterte Sicherheitsfunktionen desselben Anbieters.

22%

Wir verwenden, wo immer es möglich ist, Cloud Access Security Broker (CASB/SASE) für allgemeine Zwecke sowie anwendungsspezifische Sicherheit.

18.2%

Wir verwenden integrierte Standardsicherheit und erweiterte Sicherheit von anderen spezialisierten Sicherheitsanbietern.

14.4%

Wir verwenden den Cloud Access Security Broker (CASB/SASE) für allgemeine Zwecke und haben nicht die Absicht, anwendungsspezifische Sicherheit hinzuzufügen.

14.3%

Wir verwenden nur integrierte Standardsicherheit und haben nicht die Absicht, erweiterte Sicherheit hinzuzufügen.

Unsere Untersuchung fand eine große Bandbreite an Cloud-Sicherheitsfunktionen vor. Während die meisten Befragten eine Mischung aus spezialisierten Sicherheitsanwendungen nutzen, verlässt sich eine beträchtliche Anzahl nur auf die nativen Sicherheitsfunktionen der Anwendung bzw. Plattform.

Diese eingebauten Funktionen sind ein guter Anfang, und sie haben oft den Vorteil, dass sie vom Hersteller der Anwendung entwickelt wurden. Allerdings weisen sie in der Regel auch einige gravierende Lücken auf. So bietet Salesforce beispielsweise keine Sicherheit für unstrukturierte Daten und verfügt über keine systemeigenen Funktionen zum Scannen von Up- und Downloads von Inhalten.

Idealerweise sollten Unternehmen die systemeigenen Sicherheitsfunktionen und internen Salesforce-Services mit spezialisierten Sicherheitstools von mindestens einem Anbieter kombinieren, um bestehende Lücken zu schließen. Unternehmen sollten außerdem versuchen, möglichst alle Bereiche mit Lösungen eines einzigen Anbieters abzudecken. Die Verwendung von Lösungen verschiedener Anbieter kann sich als schwierig erweisen, da die Teams mit verschiedenen getrennten Datenströmen und Warnmeldungen zurechtkommen müssen.

Bei der Auswahl eines Cloud Access Security Brokers (CASB) können Proxy-Lösungen schwieriger zu implementieren sein, da sie speziell für jedes SaaS-Produkt konfiguriert werden müssen und sehr empfindlich sein können. API-basierte CASBs oder nativ integrierte Lösungen erweisen sich als vielseitiger und nützlicher.

“Integrierte Hersteller-Tools decken selten alles ab, aber sie können sehr effektiv sein, da die Entwickler das System genau kennen. Ein zusätzliches spezialisiertes Tool sorgt für Ausgewogenheit und deckt eventuelle Lücken ab.”

Pankaj Paryani, Salesforce Technical Lead, WithSecure™

Unsere wichtigsten Empfehlungen für die Absicherung von Salesforce im Jahr 2023

Der Rückblick auf die zentralen Punkte des Jahres 2022 schafft die Basis für die wichtigsten Sicherheitsprioritäten des kommenden Jahres. Im Folgenden finden Sie die Empfehlungen unserer Experten für 2023 und darüber hinaus.

1. Verwalten Sie Identitäten und Zugänge

Einer der zuverlässigsten Erfolgsfaktoren ist es, sich auf die Verwaltung des Systemzugangs zu konzentrieren. Die Multifaktor-Authentifizierung (MFA) reduziert das Risiko von Sicherheitsverstößen augenblicklich signifikant. Da MFA jetzt standardmäßig Bestandteil von Salesforce ist, lässt sie sich schnell und ohne zusätzliche Kosten implementieren. Zugleich wird die Angriffsfläche durch die Einführung eines Ansatzes der geringsten Privilegien für den Systemzugang sowohl für Benutzer als auch für die API-Integration erheblich reduziert. Dies ist zwar ein etwas längerer Prozess, dafür aber extrem wichtig.

2. Überwachen Sie eintreffende Bedrohungen für Salesforce

Angreifer erweitern ihr Instrumentarium über E-Mail hinaus. Die Funktion zum Hochladen von Inhalten und die integrierten Kommunikationskanäle von Salesforce wie Chatter können für Malware- und Phishing-Angriffe ausgenutzt werden. Allerdings fehlt es der Plattform an nativen Funktionen zur Überwachung von Inhalten. WithSecure™ Cloud Protection for Salesforce wurde in Zusammenarbeit mit Salesforce entwickelt, um alle ein- und ausgehenden Inhalte in Echtzeit zu scannen und schädliche Dateien und URLs zu identifizieren und zu blockieren.

3. Halten Sie Datenschutz- und Compliance-Vorschriften ein

Die rechtlichen Rahmenbedingungen ändern sich ständig, und bei so vielen veränderlichen Elementen in der Salesforce-Umgebung kann es eine komplexe Aufgabe sein, die Einhaltung aller Vorschriften zu überwachen. Das ist am besten durch die Einhaltung eines strikten Ansatzes der geringsten Privilegien mit standardmäßig minimalem Zugriff gewährleistet. Bei Vorschriften, die sich auf Dritte erstrecken, sollte eine strenge Überprüfung durchgeführt werden, um Verbindungen und Verantwortlichkeiten abzudecken.

4. Lassen Sie die integrierten Tools nicht links liegen

Salesforce enthält standardmäßig eine Reihe sehr nützlicher Tools. Stellen Sie also sicher, dass Sie das Beste daraus machen, bevor Sie in Lösungen von Drittanbietern investieren. Health Check und Optimizer sind zwei Tools, mit denen Sie schnell mögliche Fehlkonfigurationen oder verlorene Zugriffskontrollen aufdecken können. Diese Tools bieten Ihnen nicht nur einige schnelle Sicherheitsvorteile, sondern können auch den Kauf unnötiger zusätzlicher Tools vermeiden helfen.

“Obwohl Salesforce sich bemüht, seine Infrastruktur sicher zu halten, müssen auch die Benutzer ihre Verantwortung für die Sicherung ihrer Instanzen wahrnehmen. Es vergeht kaum ein Tag, an dem Salesforce nicht angegriffen wird - es ist also keine Zeit zu verlieren.”

Doug Merrett, Salesforce Security, Compliance, Privacy and Resilience Specialist, Platinum7

“Effektive Benutzerüberwachung ist ein Muss. Sie hilft nicht nur, Angreifer und böswillige Insider zu erkennen, sondern auch Zwischenfälle und Fehlkonfigurationen.”

Doug Merrett, Salesforce Security, Compliance, Privacy and Resilience Specialist, Platinum7

5. Sichern Sie Ihre Sicherungskopien

Zuverlässige Backups sind eine Ihrer wertvollsten Ressourcen zur Verbesserung der Resilienz. Wenn Sie in der Lage sind, Ihre Salesforce-Instanz wiederherzustellen, reduziert das erheblich die Auswirkungen von Angriffen wie Ransomware, die darauf abzielen, Ihre CRM-Daten zu beschädigen oder zu zerstören. Backups bieten auch eine weitere Schutzebene gegen menschliches Versagen und ermöglichen es ihnen, den Reset-Knopf zu drücken, wenn Fehlkonfigurationen oder eine schlechte App-Integration zu Problemen führen.

6. Erfüllen Sie Ihre Sorgfaltspflicht

Wenn Ihre Salesforce-Umgebung weiterwächst, ist es wichtiger denn je, bei der Due-Diligence-Prüfung gründlich zu sein. Wenn Sie sich für die Implementierung einer neuen Anwendung oder eines Plug-ins von Drittanbietern entscheiden, müssen Sie den Anbieter überprüfen und sicherstellen, dass er zuverlässig und vertrauenswürdig ist. Die Community ist gut darin, genaue Berichte im AppExchange-Store zu hinterlassen, so dass dies ein geeigneter Ansatzpunkt ist. Die Bewertungen können aktualisiert werden. Es lohnt sich also zu prüfen, ob sich im Laufe der Zeit etwas geändert hat.

7. Aktivieren Sie die Ereignisüberwachung

Die Ereignisüberwachung ist entscheidend, um zu verstehen, was in Ihrer Salesforce-Umgebung geschieht. So können Sie sehen, wie Benutzer und Anwendungen auf Ihre kritischen Daten zugreifen und mit ihnen interagieren. Diese Transparenz ist entscheidend für den Schutz Ihrer Salesforce-Plattform sowohl vor externen Angriffsversuchen als auch vor Risiken, die von innen kommen, sei es durch böse Absicht oder aus Versehen.

Diese forensischen Daten sind nur dann nützlich, wenn sie richtig verarbeitet und verstanden werden können. Daher sind Tools wie Splunk und Imprivata FairWarning nützlich, um sich einen Überblick zu verschaffen.

8. Schützen Sie sensible Daten

Geschäftsdaten sind lebenswichtig und jedes Bit und Byte ist schützenswert. Achten Sie jedoch besonders auf Kunden- und andere sensible Daten. Verwenden Sie Salesforce Shield oder andere Lösungen von Drittanbietern, um sensible Daten zu finden, zu verschlüsseln, zu überwachen und zu speichern.

“Salesforce verbessert seine Ressourcen zum Schutz vor Bedrohungen wie Phishing kontinuierlich mit neuen integrierten Funktionen. Die Anwender müssen jedoch ihren Teil dazu beitragen, diese Tools richtig zu implementieren und zu nutzen.”

Pankaj Paryani, Salesforce Technical Lead, WithSecure™

“Angriffe auf die Lieferkette waren in den letzten zwei Jahren ein großes Thema, und sie werden auch im kommenden Jahr nicht nachlassen. Unternehmen müssen sich vorrangig damit befassen, ihre erweiterten digitalen Umgebungen zu verstehen und zu sichern.”

Dmitriy Viktorov, Head of Product and Technology, Cloud Protection, WithSecure™

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

Kontakt aufnehmen

salesforce PARTNER SINCE 2016

Quellen

Die WithSecure™ 2022 B2B Market Research Studie erreichte 3.072 Befragte mit einer Online-Umfrage, die im Mai 2022 in 12 Ländern durchgeführt wurde, darunter 9 europäische Länder: Großbritannien, Frankreich, Deutschland, Belgien, Niederlande, Dänemark, Finnland, Norwegen, Schweden: in Nordamerika: USA und Kanada; außerdem Japan. Alle Befragten waren Entscheidungsträger im Bereich IT-/Netzwerk-/Cloud-Sicherheit, die den Kauf von IT-/Netzwerk-/Cloud-Sicherheitsprodukten und -dienstleistungen in ihren Unternehmen mitbestimmen.

Die Zahlen und Trends der Erkennungen schädlicher Dateien und URLs wurden von WithSecure™ aus internen, anonymisierten Daten von Bedrohungsanalyseanfragen gesammelt, die aus geschützten Salesforce-Umgebungen eingegangen sind.

Salesforce's Top Data Trends for 2022 – Basierend auf einer Umfrage unter 300 InfoSec- und IT-Führungskräften, die von Salesforce und Pulse durchgeführt wurde.

Über WithSecure™

WithSecure™, ehemals F-Secure Business, ist der zuverlässige Partner für Cybersicherheit. IT-Dienstleister, Managed Security Services Provider und andere Unternehmen vertrauen WithSecure™ – wie auch große Finanzinstitute, Industrieunternehmen und führende Kommunikations- und Technologieanbieter. Mit seinem ergebnisorientierten Ansatz der Cybersicherheit hilft der finnische Sicherheitsanbieter Unternehmen dabei, die Sicherheit in Relation zu den Betriebsabläufen zu setzen und Prozesse zu sichern sowie Betriebsunterbrechungen vorzubeugen. WithSecure™ nennt diesen Ansatz „Outcome-based Cyber Security“. KI-gesteuerte Sicherheitsmaßnahmen sichern Endgeräte und die Zusammenarbeit in der Cloud mit intelligenten Erkennungs- und Reaktionsmechanismen. Die Detection & Response-Experten von WithSecure™ identifizieren Geschäftsrisiken, indem sie proaktiv nach Bedrohungen suchen und bereits laufende Angriffe abwehren – dabei arbeiten sie eng mit Instituten, großen Unternehmen und innovativen Tech-Firmen zusammen. Sie haben mehr als 30 Jahre Erfahrung in der Entwicklung von Technologien, die sich an den Bedürfnissen der Unternehmen orientieren. Das Portfolio von WithSecure™ eröffnet durch flexible Vertriebsmodelle die Möglichkeit, gemeinsam mit Partnern zu wachsen.

WithSecure™ Corporation wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd. gelistet.

W / T H®
secure