4 Dinge, die jeder Salesforce-Administrator über Cloud-Sicherheit wissen sollte

WITH secure

Was bedeutet Cloud-Sicherheit?

Mit der zunehmenden Nutzung von Cloud-Infrastrukturen, -Plattformen, -Anwendungen und -Diensten steigt auch die Zahl von Angriffspunkten, über die böswillige Angreifer in Systeme eindringen könnten. Ohne wirksamen Schutz steigt das Risiko von Datendiebstahl, Ransomware- und anderen Angriffen. Störungen im Betriebsablauf, Imageschäden und Verstöße gegen Compliance-Regeln und Datenschutzbestimmungen könnten die Folgen sein. Cloud-Sicherheit bezieht sich auf die Technologien, Prozesse und Ressourcen, die Sie einsetzen, um Ihr Unternehmen vor Cloud-basierten Angriffen zu schützen – und in vielen Fällen sind diese gefährlich unzureichend.

Mit zunehmender Cloud-Nutzung sicher bleiben

Es gibt viele zwingende Gründe, warum Unternehmen auf die Cloud umsteigen: niedrigere Betriebskosten, mehr Flexibilität und die Notwendigkeit, Mitarbeitern die Möglichkeit zu geben, aus der Distanz zusammen zu arbeiten. In der Tat hat das Erfordernis von Social Distancing während der Pandemie in den letzten zwei Jahren cloudbasiertes Arbeiten normal werden lassen. Salesforce gehört dabei zu den beliebtesten Plattformen.

Dieser Trend wird sich fortsetzen. Eine kürzlich von Gartner durchgeführte CFO-Umfrage zeigte, dass 74 % der Unternehmen davon ausgehen, ein Teil der Mitarbeiter werde dauerhaft außerhalb des Büros arbeiten. 17 % von diesen gehen davon aus, dass das auf mindestens jeden fünften Beschäftigten[1] zutreffen wird. Cloud-Plattformen kommen außerdem zunehmend für geschäftskritische Aufgaben zum Einsatz - vom Austausch sensibler Daten bis hin zur Zusammenarbeit mit Kunden und Partnern.
Die Cloud beitet eindeutig ein Plus an Produktivität und Komfort. Zu wenige Unternehmen erkennen jedoch die Sicherheitsrisiken der neuen Arbeitsweise, und sorgen für deren wirksame Eindämmung - während Cyberkriminelle zunehmend geschickter darin werden, solche Lücken auszunutzen.Mit der zunehmenden Nutzung von Cloud-Software-as-a-Service-Angeboten (SaaS) wie Salesforce, Microsoft 365, Google Workspace und anderen werden diese Dienste zu einem immer lukrativeren und attraktiveren Ziel.

Wenn Angreifer nicht vorhaben, in der Cloud gespeicherte Daten zu stehlen, nutzen sie Cloud-Dienste als "Sprungbrett", um in andere interne und externe Systeme einzudringen.
So haben wir etwa bereits Beispiele für Phishing- und Ransomware-Angriffe gesehen, die über Cloud-Dienste durchgeführt wurden.

Unsere Experten haben vier wohlgehütete Geheimnisse gelüftet, die Ihnen helfen, Salesforce und andere Cloud-Dienste sicher zu nutzen.

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

Verborgene Wahrheit 1

Mehr Sicht-barkeit, mehr Kontrolle

Wenn Sie Daten in einen Cloud-Service wie Salesforce verschieben, stellen Sie volle Transparenz und Kontrolle sicher. Sie müssen jederzeit wissen, welche Art von Daten Sie speichern, wie sie klassifiziert sind, woher sie kommen, wer auf sie zugreifen kann und wohin sie gehen. Stammen Daten aus nicht vertrauenswürdigen Quellen, etwa aus E-Mails, müssen Sie in der Lage sein, schädliche Inhalte zu blockieren, bevor sie interne oder externe Benutzer erreichen.

Außerdem müssen Sie sicherstellen, dass Sie nicht gegen Vorschriften oder Compliance-Anforderungen verstoßen, die in den Ländern, Branchen und Märkten gelten, in denen Sie tätig sind - wie etwa die DSGVO in der EU oder den Sicherheitsstandard für Zahlungskarten PCI-DSS. Dazu müssen Sie jeden Zugriff auf alle sensiblen Daten überwachen und das auch dokumentieren. Außerdem müssen Sie in der Lage sein, nicht autorisierte Zugriffe auf Daten zu erkennen. Es kommt also darauf an, Aktivitäten und Verhalten überwachen, statt nur nach bekannten Bedrohungen Ausschau zu halten.

Verborgene Wahrheit 2

Zuständigkeiten kennen, Lücken schließen

Eine Hauptursache für Sicherheitslücken in der Cloud ist ein unzureichendes Verständnis, wer für welche Sicherheitsaspekte in den Clouds Dritter verantwortlich ist. Die Anbieter garantieren in der Regel die Sicherheit ihrer Plattformen und weisen oft beeindruckende Akkreditierungen und Zertifikate vor. Einige ihrer Kunden wiegen sich darauf in der falschen Sicherheit, sie bräuchten sich um keinen Aspekt der Cloud-Sicherheit zu sorgen.

Wenn Sie Cloud-Dienste wie Salesforce nutzen, willigen Sie in ein Modell der geteilten Verantwortung ein. Während die Anbieter vertraglich sicherstellen, dass ihre Systeme auf Infrastruktur- und Plattformebene sicher sind, bleiben Sie für die allgemeine Sicherheitshygiene, die korrekte Konfiguration der von Ihrem Anbieter bereitgestellten Cloud-Sicherheitskontrollen und den Schutz Ihrer Daten im System verantwortlich. Die genauen Verantwortlichkeiten können von Vertrag zu Vertrag variieren, aber die meisten folgen einer weitgehend ähnlichen Aufteilung.

Verborgene Wahrheit 3

Sichere Konfiguration bei zuneh-mender Komplexität

Cloud-Dienste und -Anwendungen werden schnell sehr komplex. Daraus resultieren häufig Fehlkonfigurationen oder schwache Zugangskontrollen, die zu Datenschutzverletzungen führen können. Über Software-Interfaces, APIs, können andere Anwendungen und Dienste ebenfalls auf Daten in der Cloud zugreifen. Wenn diese falsch konfiguriert sind oder mehr Berechtigungen als nötig erhalten, können auch sie einen Verstoß begünstigen.

Dies gilt insbesondere für Salesforce-Administratoren, die einem ständigen Strom von Änderungswünschen ihrer Organisationen ausgesetzt sind. Wahlweise sollen sie neue Funktionen hinzufügen, erweiterte Möglichkeiten der Plattform nutzen oder Apps, Services und Add-ons von Drittanbietern aus Salesforce AppExchange bereitstellen. Verringern Sie die Komplexität, indem Sie Tools wie Cloud Threat Detection und Cloud Security Posture Management (CSPM) einsetzen, um möglicherweise gefährliche oder nicht konforme Konfigurationen automatisch zu erkennen.

Verborgene Wahrheit 4

Angriffe aus der Lieferkette abfangen

Selbst wenn Ihre Cloud-Plattform oder Ihr Cloud-Dienst korrekt konfiguriert ist, besteht ein Risiko bei Integrationen von Drittanbietern oder Anwendungen, die über APIs verbunden sind. Rechnen Sie damit, dass Systeme, die mit Ihrer Cloud verbunden sind, auf Grund von Sicherheitslücken oder Fehlkonfiguration angreifbar sind. Angreifer könnten sich gezielt Zugang zu Organisationen verschaffen, die Systeme für Dritte bereitstellen, und deren Vertriebskanäle ausnutzen - bekannt als "Supply-Chain-Attacke".

So wurde 2019/20 eine Hintertür im beliebten Netzwerkverwaltungssystem SolarWinds ausgenutzt. Über die konnten Angreifer in die Systeme mehrerer US-Behörden eindringen. Kürzlich wurde eine Schwachstelle im Java-Logging-Framework Log4j entdeckt, die schätzungsweise 93 % der Cloud-Umgebungen von Unternehmen angreifbar machte (Quelle: Wiz/EY). Log4j ist derart weit verbreitet, dass die Log4j-Schwachstelle wohl noch einige Zeit ein Problem bleiben wird. Oft wird das Framework unsichtbar von anderen Paketen installiert, die für ihre Funktion bestimmte Java-Komponenten benötigen.

Wenn Sie eine Integration Ihrer Salesforce-Cloud mit einem Partner-, Kunden- oder Drittanbietersystem haben, das unwissentlich über eine Schwachstelle wie Log4j kompromittiert wurde, könnte sich ein Angreifer darüber Zugang zur Ihrer Cloud verschaffen. Daher ist es wichtig, dass Sie sowohl auf bekannte Malware-Bedrohungen als auch auf ungewöhnliche Aktivitäten achten, die auf eine unbekannte Bedrohung hinweisen könnten.

Wer braucht zusätzliche Sicherheit für Salesforce?

WithSecure™ Cloud Protection for Salesforce[8] bietet Echtzeitschutz vor Viren, Trojanern und Ransomware und scannt alle Inhalte, die in die Cloud hochgeladen werden. Es vervollständigt die integrierten Sicherheitskontrollen der Salesforce-Cloud-Plattform. Damit werden Sie Ihrer Verantwortung, alle über Salesforce gespeicherten oder freigegebenen Daten zu schützen.

Die Lösung bietet Ihnen die Möglichkeit, Angriffe über bösartige Dateien oder Phishing-Links zu verhindern oder zu abzubrechen. Außerdem bietet sie vollständige Transparenz und Analysen - samt Details zu allen Inhalten, auf die interne oder externe Benutzer zugreifen.

Zusätzliche Schutzmaßnahmen wie WithSecure™ Cloud Protection for Salesforce einzusetzen, wird für viele Unternehmen zunehmend entscheidender. Im Folgenden stellen wir drei typische Anwendungsfälle vor.

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

Anwendungsfall 1: **Der proaktive Suchende**

Immer mehr Salesforce-Administratoren erkennen, dass sie mit der zunehmenden Nutzung von Cloud-Systemen und -Services für einen umfassenden Schutz der Plattform sorgen müssen. Sie sind sich der wachsenden Cloud-Bedrohungen wie Ransomware und Datenschutzverletzungen bewusst. Sie sind sich auch über ihre geteilten Verantwortlichkeiten für die Sicherheit im Klaren. Allerdings wissen sie vielleicht nicht genau, welche Tools von Drittanbietern verfügbar sind, um sie dabei zu unterstützen. Sie beginnen also, relevante Fragen zu Schutz und Sicherheit der Salesforce-Umgebung[3] zu stellen. Sie erfahren schnell von Lösungen wie WithSecure™ Cloud Protection for Salesforce, indem sie über AppExchange nach Sicherheitsanwendungen suchen. Sie erfahren auch, dass die WithSecure™-Lösung die Lücken in der Salesforce-Sicherheit schließen kann. Anschließend beginnen sie mit einer Bewertung und Beschaffung, nachdem sie bereits einen soliden Business Case für die Investition erstellt haben.

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

Anwendungsfall 2: **Der Portal-Verantwortliche**

Ein Unternehmen dehnt die Nutzung von Salesforce aus, um sich mit Partnern und/oder Kunden zu vernetzen - zum Beispiel über Experience Cloud (früher bekannt als Community Cloud). Es kann jedoch nicht sicher sein, dass externe Drittparteien über angemessene Sicherheitsvorkehrungen an ihren Endpunkten verfügen, also auf den Systemen und Geräten, die sie für die Verbindung mit dem Portal des Unternehmens verwenden. Wenn sie externen Benutzern erlauben, Inhalte wie Dokumentation, Formulare oder Links in Salesforce hochzuladen, müssen sie sicherstellen, dass dabei keine Bedrohungen wie Malware oder Phishing-Links verwendet werden. Dabei geht es auch um ihren Ruf. Sie können es sich nicht leisten, zu riskieren, dass etwas Schädliches eingeschleust und anschließend von einem Partner oder Kunden heruntergeladen wird. Ebenso wenig können sie sich einen Systemausfall leisten, da ihr Portal möglicherweise das Kernstück ihres Geschäftsmodells ist - wie es bei Finanzunternehmen, Personalvermittlungsfirmen, Reisebüros und anderen professionellen Dienstleistungsunternehmen häufig der Fall ist.

Anwendungsfall 3: **Der Compliance-Verantwortliche**

Ein großes Unternehmen - oder eines, das in einem stark regulierten Sektor wie dem Gesundheitswesen, den Finanzdienstleistungen oder der Regierung tätig ist - hat oft strenge Compliance-Regeln, etwa gesetzliche und behördliche Regeln zu Datenschutz und Privatsphäre, oder auch interne Compliance-Verfahren, die sich an best practices orientieren, wie z. B. dem Sicherheitsstandard ISO 27001. Ein leitender Manager, vielleicht ein CISO oder CIO oder sogar der CEO, verlangt, sicherzustellen, dass Cloud-Plattformen, -Anwendungen und -Dienste völlig konform zu den Datensicherheitsrichtlinien des Unternehmens sind. Administratoren wird klar, dass sie zusätzliche Tools benötigen, um Salesforce angemessen zu schützen. Dazu gehört wahrscheinlich die Implementierung von Content Security mit Lösungen wie Cloud Protection von WithSecure™, aber auch eine Cloud Security Posture Management (CSPM)-Lösung, um die Compliance im gesamten Unternehmen sicherzustellen.

Über WithSecure

WithSecure 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 Endpoints 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 ist Teil der 1988 gegründeten F-Secure Corporation, die an der NASDAQ OMX Helsinki Ltd. gelistet ist.

W / T H
secure