Sicherheit nach Maß: Anmelden bei AWS

Wie AWS CloudTrail Ihnen helfen kann, Compliance-Anforderungen durch Protokollieren von API-Aufrufen und Ressourcenänderungen einzuhalten

Oktober 2015

(Die neueste Version dieses Dokuments finden Sie unter

https://aws.amazon.com/compliance/aws-whitepapers/.)

Inhaltsverzeichnis

Kurzbeschreibung

Protokollierung und Überwachung von API-Aufrufen sind entscheidende Komponenten in den bewährten Methoden für Sicherheit und Betrieb. Es sind aber auch Anforderungen, um gesetzliche Bestimmungen und Branchenstandards zu erfüllen. AWS CloudTrail ist ein Web-Service, der API-Aufrufe an unterstützte AWS-Services in Ihrem AWS-Konto aufzeichnet und eine Protokolldatei an Ihren Amazon Simple Storage Service (Amazon S3)-Bucket überträgt. AWS CloudTrail entschärft die allgemeinen Herausforderungen, die lokale Umgebungen bergen können. Mit diesem Service können Sie nicht nur die Einhaltung von Richtlinien oder gesetzlichen Vorschriften einfacher nachweisen, sondern auch für mehr Sicherheit und optimalere betriebliche Prozesse sorgen.

Dieses Dokument gibt einen Überblick über allgemeine Compliance-Anforderungen im Bezug auf die Protokollierung und zeigt detailliert auf, wie AWS CloudTrail-Funktionen dazu beitragen können, diese Anforderungen zu erfüllen. Abgesehen von den Standardgebühren für S3 für die Protokollspeicherung und die Nutzung von SNS für optionale Benachrichtigungen fallen keine zusätzlichen Gebühren für die Verwendung von AWS CloudTrail an.

Einführung

Amazon Web Services (AWS) stellt eine Vielzahl von bedarfsorientierten IT-Ressourcen und -Services bereit, die Sie starten und verwalten können und die Sie nutzungsabhängig bezahlen. Die Aufzeichnung der AWS API-Aufrufe und entsprechenden Änderungen der Ressourcenkonfiguration ist ein entscheidender Faktor für IT-Governance, -Sicherheit und -Compliance. AWS CloudTrail bietet eine einfache Lösung, um AWS API-Aufrufe und Ressourcenänderungen aufzuzeichnen. Die Belastung durch die Herausforderungen einer lokalen Infrastruktur und Speicherung wird verringert, indem Sie die Möglichkeit erhalten, leistungsfähige präventive und nachträglich aufdeckende Sicherheitskontrollen für Ihre AWS-Umgebung zu schaffen. Für lokale Protokollierungslösungen müssen Agents installiert, Konfigurationsdateien und zentrale Protokollserver eingerichtet sowie teure und sehr robuste Datenspeicher aufgebaut und gepflegt werden, um Daten speichern zu können. AWS CloudTrail macht dieser mühsamen Infrastruktureinrichtung ein Ende und ermöglicht Ihnen, mit nur zwei Klicks die Protokollierungsfunktion zu starten und eine bessere Einsicht in alle API-Aufrufe in Ihrem AWS-Konto zu erhalten. API-Aufrufe von mehreren Servern werden von CloudTrail fortlaufend in einer hochverfügbaren Verarbeitungspipeline erfasst. CloudTrail können Sie aktivieren, indem Sie sich einfach bei AWS Management Console anmelden, zur CloudTrail-Konsole navigieren und die Protokollierungsfunktion mit einem Klick aktivieren. Weitere Informationen über Services und Regionen zur Verwendung mit AWS CloudTrail finden Sie auf der AWS CloudTrail-Website.

Für die Erstellung dieses Whitepapers wurden Protokollierungsanforderungen häufiger Compliance-Rahmenwerke (z. B. ISO 27001:2005, PCI DSS v2.0, FedRAMP etc.) erfasst und in allgemeinen Kontrollen und Protokollierungsbereichen zusammengeführt. Sie können es für eine Vielzahl von Szenarien nutzen, wie z. B. für bewährte Methoden für Sicherheit und Betrieb oder die Einhaltung interner Richtlinien, Branchen-standards und gesetzlicher Vorschriften. Das Whitepaper wurde allgemein gehalten, damit alle Leser verstehen können, wie AWS CloudTrail bestehende Protokollierungs- und Überwachungsaktivitäten optimieren kann.

Kontrollieren des Zugriffs auf Protokolldateien

Für die Erhaltung der Integrität Ihrer Protokolldaten ist es wichtig, Zugriffe rund um die Erstellung und Speicherung Ihrer Protokolldateien sehr sorgsam zu verwalten. Nur autorisierte Benutzer sollten Ihre Protokolldaten einsehen und ändern können. Für lokale Umgebungen ist es eine Herausforderung, gegenüber Behörden nachweisen zu können, dass der Zugriff auf Protokolldaten auf autorisierte Benutzer beschränkt ist. Es kann zeitaufwendig und schwierig sein, diese Kontrolle effektiv nachzuweisen, da die meisten lokalen Umgebungen nicht über eine einzelne Protokollierungslösung oder eine systemübergreifende einheitliche Protokollierungssicherung verfügen.

Mit AWS CloudTrail wird der Zugriff auf Amazon S3-Protokolldateien zentral in AWS gesteuert. Dadurch können Sie den Zugriff auf Ihre Protokolldateien problemlos kontrollieren und die Integrität und Vertraulichkeit Ihrer Protokolldateien aufzeigen.

	Allgemeine Protokollierungs-anforderungen	Wie AWS CloudTrail zur Einhaltung von Compliance-Anforderungen beiträgt
Kontrollieren des Zugriffs auf Protokolldateien	Gewährleisten von Kontrollen, um unbefugte Zugriffe auf Protokolle zu verhindern	Mit AWS CloudTrail können Sie den Zugriff auf Ihre Protokolldateien einschränken. Sie können den Zugriff auf Ihre Protokolldateien steuern und verhindern, dass diese geändert werden, indem Sie AWS Identity and Access Management (IAM)-Rollen und Amazon S3-Bucket-Richtlinien konfigurieren, um durchzusetzen, dass der Zugriff auf die Protokolldateien schreibgeschützt ist. Weitere Informationen Sie können Ihre Authentifizierungs- und Autorisierungskontrollen zudem noch verstärken, indem Sie AWS Multi Factor Authentication (AWS MFA) in Ihren Amazon S3-Buckets (den Speicherorten Ihrer AWS CloudTrail-Protokolle) aktivieren. Weitere Informationen
	Gewährleisten von Kontrollen, um sicherzustellen, dass der Zugriff auf Protokolleinträge rollenbasiert ist	Mithilfe von AWS CloudTrail können Sie den Benutzerzugriff auf Ihre Protokolldateien auf der Grundlage einer detaillierten und rollenbasierten Bereitstellung steuern. AWS Identity and Access Management (IAM) ermöglicht Ihnen, den Zugriff Ihrer Benutzer auf AWS CloudTrail sicher zu steuern. Außerdem können Sie anhand von IAM-Rollen und Richtlinien für Amazon S3-Buckets den rollenbasierten Zugriff auf das S3-Bucket, das Ihre AWS CloudTrail-Protokolldateien speichert, durchsetzen. Weitere Informationen

Abrufen von Warnungen bei Protokolldateierstellung und fehlerhafter Konfiguration

Besonders wichtig für eine effektive IT-Governance und die Einhaltung von internen oder externen Compliance-Anforderungen sind Warnungen nahezu in Echtzeit, wenn die Konfiguration von Protokollen, die Detailinformationen zu API-Aufrufen oder Ressourcenänderungen enthalten, fehlerhaft ist. Selbst aus betrieblicher Perspektive ist eine ordnungsgemäße Konfiguration der Protokollierung zwingend erforderlich, da Sie so die Möglichkeit erhalten, die Aktivitäten Ihrer Benutzer und Ressourcen zu überblicken. Variabilität und Umfang von Protokollierungsinfrastrukturen in lokalen Umgebungen erschweren jedoch eine aktive Überwachung und Warnung im Fall von fehlerhaften Konfigurationen oder Änderungen der Protokollierungskonfigurationen.

Sobald Sie AWS CloudTrail für Ihr Konto aktiviert haben, übermittelt der Service Protokolldateien an Ihr S3-Bucket. Wahlweise veröffentlicht CloudTrail Benachrichtigungen bei Bereitstellungen von Protokolldateien an ein SNS-Thema, sodass Sie dann entsprechend handeln können. Diese Warnungen enthalten die Amazon S3-Bucket-Protokolldateiadresse, damit Sie schnell auf die Objektmetadaten zum Ereignis über die Quell-protokolldateien zugreifen können. Darüber hinaus warnt Sie Ihre AWS Management Console, wenn Protokolldateien falsch konfiguriert sind und die Protokollierung folglich nicht länger ausgeführt wird.

	Allgemeine Protokollierung sanforderungen	Wie AWS CloudTrail zur Einhaltung von Compliance-Anforderungen beiträgt
Empfangen von Warnungen bei Protokolldateierstellung und fehlerhafter Konfiguration	Bereitstellen von Warnungen, wenn Protokolle erstellt werden oder fehlerhaft sind, und Befolgen von in der Organisation festgelegten Aktionen bei fehlerhafter Konfiguration	Über die AWS Management Console werden Sie von AWS CloudTrail sofort benachrichtigt, wenn Probleme mit der Protokollierungskonfiguration auftreten. Weitere Informationen
	Gewährleisten, dass Warnungen zu fehlerhaften Protokollkonfigurationen Benutzer zu relevanten Protokollen mit zusätzlichen Informationen leiten (keine Weitergabe unnötiger Details)	AWS CloudTrail erfasst die Amazon S3-Bucket-Protokolldatei-adresse bei jeder Erstellung einer neuen Protokolldatei. AWS CloudTrail veröffentlicht Benachrichtigungen bei der Erstellung einer Protokolldatei, sodass Kunden entsprechend und nahezu in Echtzeit handeln können. Die Benachrichtigung wird an Ihr Amazon S3-Bucket übermittelt und in der AWS Management Console angezeigt. Wahlweise können Amazon SNS-Mitteilungen mithilfe von Push an Mobilgeräte oder über API oder die AWS Management Console an verteilte Dienste übertragen werden. Die SNS-Nachricht bei Erstellung einer Protokolldatei enthält deren Adresse. Somit werden zwar nur die wirklich erforderlichen Informationen weitergegeben, aber gleichzeitig können problemlos weitere Ereignisdetails verknüpft werden. Weitere Informationen

Verwalten von Änderungen an AWS-Ressourcen und Protokolldateien

Für die IT-Governance und -Sicherheit ist es entscheidend, zu erkennen, welche Änderungen an Ressourcen vorgenommen werden. Das Verhindern von Änderungen an und von unbefugten Zugriffen auf Protokolldateien hat außerdem direkte Auswirkungen auf die Integrität Ihrer Änderungsverwaltungsprozesse und Ihre Fähigkeit, interne, branchenübliche und regulatorische Anforderungen rund um die Änderungsverwaltung einzuhalten. Eine große Herausforderung in lokalen Umgebungen besteht darin, Änderungen an Ressourcen oder Protokollen aufzeichnen zu können, da Ihnen nur begrenzte Ressourcen zur Verfügung stehen, um zu überwachen, was eine unerschöpfliche Datenmenge zu sein scheint.

AWS CloudTrail ermöglicht Ihnen, die Änderungen an einer AWS-Ressource nachzuverfolgen, einschließlich Erstellung, Modifizierung und Löschung. Durch Überprüfen des Protokollverlaufs zu API-Aufrufen unterstützt Sie AWS CloudTrail außerdem bei der Untersuchung eines Ereignisses, um zu bestimmen, ob es nicht autorisierte oder unerwartete Änderungen gegeben hat. Dazu können Sie überprüfen, wer die Änderungen initiiert hat, wann sie aufgetreten sind und woher sie stammen. Wahlweise veröffentlicht CloudTrail Benachrichtigungen an ein SNS-Thema, sodass Sie entsprechend handeln können, wenn die neue Protokolldatei in Ihrem Amazon S3-Bucket bereitgestellt wird.

Verwalten von Änderungen an IT-Ressourcen und Protokolldateien	**Allgemeine Protokollierungsanforderungen**	**Wie AWS CloudTrail zur Einhaltung von Compliance-Anforderungen beiträgt**
	Bereitstellen von Protokollen zu Systemkomponentenänderungen (einschließlich Erstellen und Löschen von Objekten auf Systemebene)	AWS CloudTrail erstellt Protokolldaten bei Systemänderungsereignissen, damit Sie Änderungen an Ihren AWS-Ressourcen nachverfolgen können. AWS CloudTrail bietet Einblicke in jegliche Änderung an Ihrer AWS-Ressource (von der Erstellung bis zur Löschung), indem es die mittels API-Aufrufen über die AWS Management Console, die AWS Command Line Interface (CLI) oder die AWS Software Development Kits (SDKs) durchgeführten Änderungen protokolliert. Weitere Informationen
	Gewährleisten von Kontrollen, um Änderungen an Änderungsprotokollen oder Fehler im Zusammenhang mit Protokollen zu verhindern	Standardmäßig werden die Protokolldateien zu den API-Aufrufen mit serverseitiger S3-Verschlüsselung (SSE) verschlüsselt und in Ihrem S3-Bucket gespeichert. Protokolldatenänderungen können mithilfe von IAM und MFA kontrolliert werden, um schreibgeschützten Zugriff auf Ihr Amazon S3-Bucket, dem Speicherort Ihrer AWS CloudTrail-Protokolldateien, zu erzwingen. Weitere Informationen

Speichern von Protokolldateien

Branchenstandards und gesetzliche Vorschriften erfordern möglicherweise die Speicherung von Protokolldateien für unterschiedlich lange Zeiträume. So verlangt z. B. PCI DSS die Speicherung von Protokollen für ein Jahr, HIPAA verlangt die Aufbewahrung von Aufzeichnungen für mindestens sechs Jahre und andere Vorschriften ordnen längere oder variable Speicherungszeiträume je nach protokollierten Daten an. Daher kann die Verwaltung der Anforderungen an die Speicherung von Protokolldateien für unterschiedliche Daten auf verschiedenartigen Systemen eine administrative und technologische Last sein. Darüber hinaus kann die dauerhafte und sichere Speicherung und Archivierung großer Protokolldatenmengen für viele Organisationen eine Herausforderung darstellen.

AWS CloudTrail ist auf eine nahtlose Integration in Amazon S3 und Amazon Glacier ausgelegt. Dies erlaubt Ihnen eine auf Ihre Speicherbedürfnisse ausgelegte Anpassung von S3-Buckets und -Lebenszyklusregeln. AWS CloudTrail bietet Ihnen einen unbegrenzten Ablaufzeitraum für Ihre Protokolle. Sie können also den Zeitraum für die Speicherung Ihrer Protokolle so anpassen, dass die Anforderungen Ihrer Regulierungsbehörde eingehalten werden.

	Allgemeine Protokollierungsanforderungen	Wie AWS CloudTrail zur Einhaltung von Compliance-Anforderungen beiträgt
Speichern von Protokolldateien	Speichern von Protokollen für mindestens ein Jahr	Sie können AWS CloudTrail so konfigurieren, dass Ihre Protokolldateien über alle Regionen und/oder mehrere Konten in einem einzelnen S3-Bucket zusammengeführt werden. Dies vereinfacht die Speicherung von Protokolldateien. Mit AWS CloudTrail können Sie den Zeitraum für die Speicherung Ihrer Protokolle anpassen, indem Sie den gewünschten Ablaufzeitraum für Protokolldateien, die in Ihr Amazon S3-Bucket geschrieben werden, entsprechend konfigurieren. Sie kontrollieren die Aufbewahrungsrichtlinien für Ihre CloudTrail-Protokolldateien. Sie können Protokolldateien für einen Zeitraum Ihrer Wahl oder unbegrenzt speichern. Standardmäßig werden Protokolldateien unbegrenzt gespeichert. Sie können Ihre Protokolldateidaten auch nach Amazon Glacier verlagern, um im Zusammenhang mit dem Archivspeicher noch von weiteren Kosteneinsparungen zu profitieren. Weitere Informationen.
	Speichern von Protokollen für einen von der Organisation festgelegten Zeitraum	
	Speichern von Protokollen in Echtzeit für mehr Stabilität	AWS CloudTrail sorgt für Stabilität der Protokolldateien durch die Nutzung von Amazon S3, einer sehr robusten Speicherinfrastruktur. Der Standardspeicher von Amazon S3 ist mit einer Jahreshaltbarkeit von 99,999999999 % und Jahresverfügbarkeit von Objekten von 99,99 % ausgelegt. Weitere Informationen.

Erstellen von benutzerdefinierten Protokolldatenberichten

Aus operativen und sicherheitsrelevanten Gesichtspunkten stellt die Protokollierung von API-Aufrufen die Daten und Zusammenhänge bereit, die Sie benötigen, um das Benutzerverhalten zu analysieren und bestimmte Ereignisse zu erkennen. Protokolle zu API-Aufrufen und Änderungen an IT-Ressourcen können zudem für den Nachweis genutzt werden, dass nur autorisierte Benutzer bestimmte Aufgaben in Ihrer Umgebung und in Übereinstimmung mit Compliance-Anforderungen durchgeführt haben. In Anbetracht des Umfangs und der Variabilität in Verbindung mit Protokolldaten von unterschiedlichen Systemen kann es in einer lokalen Umgebung schwierig sein, klar zu erkennen, welche Benutzeraktivitäten und IT-Ressourcenänderungen durchgeführt wurden.

AWS CloudTrail generiert Daten, die Sie verwenden können, um anormales Verhalten zu erkennen, Ereignisaktivitäten im Zusammenhang mit bestimmten Objekten abzurufen oder einen einfachen Prüfpfad für Ihr Konto bereitzustellen. Sie können Ihre aktuellen Protokollanalysen mit den mehr als 25 verschiedenen Feldern in den Ereignisdaten, die AWS CloudTrail bereitstellt, weiterentwickeln. Diese können Sie einsetzen, um Abfragen und individuelle Berichte beispielsweise zu internen Untersuchungen oder externer Compliance zu erstellen. AWS CloudTrail ermöglicht Ihnen, API-Aufrufe auf bestimmte bekannte unerwünschte Verhalten hin zu überwachen und Alarme mithilfe Ihrer Protokollverwaltungslösungen oder Sicherheitsvorfall- und Ereignisverwaltungslösungen (Security Incident an Event Management, SIEM) auszulösen. Die von AWS CloudTrail bereitgestellten angereicherten Daten können Ihre Untersuchungen beschleunigen und Ihre Reaktionszeit bei Vorfällen verkürzen. Außerdem können die von AWS CloudTrail bereitgestellten Daten möglicherweise dazu beitragen, API-Aufrufe einer tieferen Sicherheitsanalyse zu unterziehen, um verdächtiges Verhalten und latente Muster zu identifizieren, die nicht direkt einen Alarm auslösen, aber möglicherweise ein Sicherheitsproblem darstellen. Und schließlich arbeitet AWS CloudTrail mit einem umfangreichen Spektrum an Partnern, die gebrauchsfertige Sicherheits-, Analyse- und Alarmierungslösungen anbieten. Weitere Informationen zu unseren Partnerlösungen finden Sie auf der AWS CloudTrail-Website.

Erstellen von benutzerdefinierten Protokolldatenberichten	**Allgemeine Protokollierungsanforderung**	**Wie AWS CloudTrail zur Einhaltung von Compliance-Anforderungen beiträgt**
	Protokollieren von Zugriffen einzelner Benutzer auf Ressourcen, nach Zugriffen auf das System und durchgeführten Aktionen. "Zugriff einzelner Benutzer" schließt den Zugriff von Administratoren und Systemverwaltern ein;	AWS CloudTrail bietet die Möglichkeit, umfassende und detaillierte API-Aufrufberichte zu generieren. Es werden Aktivitäten protokolliert, die von allen Benutzern durchgeführt werden, die mit einer beliebigen Zugriffsmethode auf Ihre protokollierten AWS-Ressourcen zugreifen. Hierzu gehören root, IAM-Benutzer, verbundene Benutzer sowie alle Benutzer oder Services, die Aktivitäten für Benutzer ausführen. Weitere Informationen.
	Erstellen von Protokollen in einer von der Organisation festgelegten Häufigkeit	AWS CloudTrail bietet die Möglichkeit, Protokollanalysetools einzusetzen, um Protokolldateidaten in einer individuell festgelegten Häufigkeit abzurufen. Dazu werden Protokolle nahezu in Echtzeit erstellt und Protokolldaten binnen 15 Minuten nach dem API-Aufruf an Ihr Amazon S3-Bucket übermittelt. Sie können Protokolldateien als Input für branchenführende Protokollverwaltungs- und –analyse-lösungen nutzen, um Analysen durchzuführen. Weitere Informationen.

Allgemeine Protokollierung sanforderungen	Wie AWS CloudTrail zur Einhaltung von Compliance-Anforderungen beiträgt
Bereitstellen von Protokollen bei Initiierung der Protokollierungsaktivität	AWS CloudTrail protokolliert sämtliche API-Aufrufe, auch bei Aktivierung und Deaktivierung der AWS CloudTrail-Protokollierung. Sie können also nachverfolgen, wann CloudTrail selbst aktiviert bzw. deaktiviert wurde. Weitere Informationen.
Generieren von Protokollen, die für einheitliche Zeitstempelinformationen mit einer internen Systemuhr synchronisiert werden	AWS CloudTrail erstellt mit einer einzelnen internen Systemuhr synchronisierte Protokolle, indem Ereigniszeitstempel in Coordinated Universal Time (UTC) generiert werden, die mit dem Basisstandardformat der ISO 8601 für Datum und Uhrzeit übereinstimmen. Weitere Informationen.
Bereitstellen von Protokollen, aus denen ersichtlich wird, ob unangemessene oder ungewöhnliche Aktivitäten aufgetreten sind	AWS CloudTrail ermöglicht Ihnen, API-Aufrufe durch Aufzeichnen von Autorisierungsfehlern in Ihrem AWS-Konto zu überwachen. Somit können Sie versuchte Zugriffe auf gesperrte Ressourcen oder andere ungewöhnliche Aktivitäten nachverfolgen. Weitere Informationen.
Bereitstellen von Protokollen mit angemessenen Ereignisdetails	AWS CloudTrail liefert API-Aufrufe mit detaillierten Informationen, wie z. B. Typ, Datum und Uhrzeit, Standort, Quelle/Ursprung, Ergebnis (einschließlich Ausnahmen, Fehler und Sicherheitsereignis-informationen), betroffene Ressource (Daten, System etc.) und zugeordneter Benutzer. Mit AWS CloudTrail können Sie Folgendes identifizieren: den Benutzer, den Zeitpunkt des Ereignisses, die IP-Adresse des Benutzers, die Anforderungs-parameter, die vom Benutzer angegeben werden, die Antwortelemente, die vom Service zurückgegeben werden sowie optional den Fehlercode und die Fehlermeldung. Weitere Informationen.

Fazit

In AWS können Sie praktisch alles ausführen, was auch lokal ausgeführt werden kann: Websites, Anwendungen, Datenbanken, mobile Apps, E-Mail-Kampagnen, verteilte Datenanalysen, Medienspeicher und private Netzwerke. Die von AWS gebotenen Services sind auf Zusammenarbeit ausgelegt, sodass Sie Komplettlösungen entwickeln können. AWS CloudTrail bietet eine einfache Lösung zum Protokollieren von Benutzeraktivitäten, durch die der Aufwand des Betriebs eines komplexen Protokollierungssystems verringert wird. Die Migration der Arbeitslasten auf AWS bietet zudem den Vorteil eines höheren Sicherheitsniveaus nach Maß durch die Nutzung der vielen angebotenen Funktionen, die eine Kontrolle ermöglichen. Aus denselben Gründen, aus denen die Bereitstellung von Infrastruktur in der Cloud Vorteile gegenüber einer lokalen Bereitstellung hat, bietet cloudbasierte Governance geringere Einstiegskosten, einfachere Bedienung und höhere Agilität durch mehr Transparenz, Sicherheitskontrolle und zentrale Automatisierung. AWS CloudTrail ist einer der Services, den Sie nutzen können, um mit AWS Governance für Ihre IT-Ressourcen auf hohem Niveau zu erreichen.

Weitere Ressourcen

Im Folgenden finden Sie Links zu Antworten auf häufig gestellte Fragen in Zusammenhang mit der Protokollierung in AWS:

- Wozu kann ich AWS verwenden? Weitere Informationen.
- Erste Schritte mit AWS Weitere Informationen.
- Erste Schritte mit AWS CloudTrail Weitere Informationen.
- Verfügt AWS CloudTrail über eine Liste mit häufig gestellten Fragen? Weitere Informationen.
- Wie kann ich bei der Nutzung von AWS Compliance erreichen? Weitere Informationen.
- Wie kann ich bei der Nutzung von AWS eine Prüfung vorbereiten? Weitere Informationen.

Anhang: Index der Compliance-Programme

Die Informationen im Whitepaper oben wurden anhand von Protokollierungsanforderungsbereichen präsentiert. Zu Referenzzwecken werden die Protokollierungsanforderungen häufiger Compliance-Rahmenwerke in der folgenden Tabelle aufgeführt:

AWS-Compliance-Programm	Compliance-Anforderung
Payment Card Industry (PCI) Data Security Standard (DSS) Stufe 1 AWS erfüllt die Anforderungen von PCI DSS "Level 1". Sie können ihre Anwendungen auf unserer PCI-konformen Technologieinfrastruktur für die Speicherung, Verarbeitung und Übermittlung von Kreditkartendaten in der Cloud ausführen. Weitere Informationen.	**PCI 5.2:** Gewährleisten, dass alle Antivirenmechanismen aktuell sind, aktiv ausgeführt werden und in der Lage sind, Audit-Protokolle zu generieren
	PCI 10.1: Einrichten eines Prozesses zur Verknüpfung des gesamten Zugriffs auf Systemkomponenten (insbesondere des Zugriffs mit Administratorprivilegien wie root) mit den einzelnen Benutzern
	PCI 10.2: Implementierung automatisierter Audit-Trails für alle Systemkomponenten zur Rekonstruktion der folgenden Ereignisse: **10.2.1:** Alle individuellen Zugriffe auf Karteninhaberdaten **10.2.2:** Alle Aktivitäten von Personen mit Root- oder Administratorberechtigungen **10.2.3:** Zugriff auf alle Prüfpfade **10.2.4:** Ungültige logische Zugriffsversuche **10.2.5:** Verwendung von Identifikations- und Authentifizierungsmechanismen **10.2.6:** Initialisierung von Audit-Protokollen **10.2.7:** Erstellung und Löschung von Objekten auf Systemebene
	PCI 10.3: Aufzeichnen von mindestens den folgenden Audit-Trail-Einträgen für alle Systemkomponenten zu jedem Ereignis: **10.3.1:** Benutzer-ID **10.3.2:** Art des Ereignisses **10.3.3:** Datum und Uhrzeit **10.3.4:** Hinweis auf Erfolg oder Fehler **10.3.5:** Ursprung des Ereignisses **10.3.6:** Identität oder Name betroffener Daten, Systemkomponenten oder Ressourcen
	PCI 10.4.2: Zeitinformationen sind geschützt.
	PCI 10.5: Schützen der Audit-Trails vor Veränderungen
	PCI 10.5.1: Beschränken der Anzeige der Audit-Trails auf Personen mit arbeitsbedingtem Bedarf

AWS-Compliance-Programm	Compliance-Anforderung
Payment Card Industry (PCI) Data Security Standard (DSS) Stufe 1 AWS erfüllt die Anforderungen von PCI DSS "Level 1". Sie können ihre Anwendungen auf unserer PCI-konformen Technologieinfrastruktur für die Speicherung, Verarbeitung und Übermittlung von Kreditkartendaten in der Cloud ausführen. Weitere Informationen.	**PCI 10.5.2:** Schützen von Audit-Trail-Dateien vor nicht autorisierten Änderungen
	PCI 10.5.3: Sofortige Sicherung von Audit-Trail-Dateien auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen
	PCI 10.5.4: Erstellen von Protokollen für nach außen gerichtete Technologien auf einem Protokollserver im internen LAN
	PCI 10.5.5: Verwenden von Software zur Dateiintegritäts-überwachung und Änderungserfassung für Protokolle, damit bei der Änderung von bestehenden Protokolldaten ein Alarm ausgelöst wird (nicht jedoch bei der Eingabe neuer Daten)
	PCI 10.6: Mindestens einmal tägliche Überprüfung der Protokolle für alle Systemkomponenten. Protokollüberprüfungen müssen die Server mit Sicherheitsfunktionen wie Angriffserkennungsserver (intrusion-detection systems, IDS) und AAA-Protokollserver (Authentifizierung, Autorisierung und Kontoverwaltung, z. B. RADIUS) umfassen.
	PCI 10.7: Aufbewahren der Audit-Trail-Verlaufsdaten für mindestens ein Jahr, wobei ein mindestens dreimonatiger Zeitraum sofort für die Analyse bereitstehen muss (beispielsweise online, archiviert oder aus einer Sicherung wiederherstellbar)
	PCI 11.5: Bereitstellen von Software zur Überwachung der Dateiintegrität, die eine Warnung ausgibt, wenn es zu nicht autorisierten Änderungen an wichtigen System-, Konfigurations- oder Inhaltsdateien kommt, und Konfiguration der Software für einen mindestens wöchentlich durchzuführenden Vergleich wichtiger Dateien
	PCI 12.2: Entwickeln von täglichen Routineverfahren für die Betriebssicherheit, die den Anforderungen in dieser Spezifikation entsprechen (z. B. Benutzerkonto-Wartungsverfahren und Protokollüberprüfungsverfahren)
	PCI A.1.2.d: Beschränken des Zugriffs und der Berechtigungen aller Entitäten auf die jeweils eigene Umgebung mit Karteninhaberdaten
	PCI A.1.3: Aktivierung eindeutiger mit PCI DSS-Anforderung 10 konformer Protokollierungs- und Audit-Trails für die Karteninhaberdaten-Umgebung jeder Entität
	PCI 11.4: Nutzung von Systemen zur Erkennung und/oder Verhinderung von Eindringversuchen in das Netzwerk. Überwachen des gesamten Datenverkehrs in der Umgebung der Karteninhaberdaten-Umgebung sowie an kritischen Punkten innerhalb der Karteninhaberdaten-Umgebung und Alarmieren des Personals bei mutmaßlichen Sicherheitsverletzungen. Ständige Aktualisierung der Systeme zur Erkennung und Verhinderung von Eindringversuchen, der Basis und der Signaturen

AWS-Compliance-Programm	Compliance-Anforderung
Payment Card Industry (PCI) Data Security Standard (DSS) Stufe 1 AWS erfüllt die Anforderungen von PCI DSS "Level 1". Sie können ihre Anwendungen auf unserer PCI-konformen Technologieinfrastruktur für die Speicherung, Verarbeitung und Übermittlung von Kreditkartendaten in der Cloud ausführen. Weitere Informationen.	**PCI 11.5:** Bereitstellen von Software zur Überwachung der Dateiintegrität, die eine Warnung ausgibt, wenn es zu nicht autorisierten Änderungen an wichtigen System-, Konfigurations- oder Inhaltsdateien kommt, und Konfiguration der Software für einen mindestens wöchentlich durchzuführenden Vergleich wichtiger Dateien
Service Organization Controls 2 (SOC 2) Der SOC 2-Bericht ist eine Bescheinigung, für die die Bewertung der Kontrollfunktionen auf die Kriterien der American Institute of Certified Public Accountants (AICPA) Trust Services Principles ausgeweitet wird. Diese Grundsätze bestimmen für Serviceanbieter wie AWS maßgebliche Kontrollfunktionen für die Praxis hinsichtlich Sicherheit, Verfügbarkeit, Integrität der Verarbeitung, Vertraulichkeit und Datenschutz. Weitere Informationen.	**SOC 2 Security 3.2.g:** Vorliegen von Verfahren, um logischen Zugriff auf das definierte System zu beschränken. Hierzu gehört u. a. Folgendes: Beschränkung des Zugriffs auf Systemkonfigurationen, Superuser-Funktionalität, Masterpasswörter, leistungsstarke Dienstprogramme sowie Sicherheitsgeräte (z. B. Firewalls).
	SOC 2 Security 3.3: Vorliegen von Verfahren, um physischen Zugriff auf das definierte System zu beschränken. Hierzu gehören u. a. Einrichtungen, Sicherungsmedien und andere Systemkomponenten wie Firewalls, Router und Server.
	SOC 2 Security 3.7: Vorliegen von Verfahren, um Verstöße gegen die Systemsicherheit und andere Vorfälle zu identifizieren, zu melden und zu behandeln
	SOC 2 Availability 3.5.f: Vorliegen von Verfahren, um logischen Zugriff auf das definierte System zu beschränken. Hierzu gehört u. a. Folgendes: Beschränkung des Zugriffs auf Systemkonfigurationen, Superuser-Funktionalität, Masterpasswörter, leistungsstarke Dienstprogramme sowie Sicherheitsgeräte (z. B. Firewalls).
	SOC 2 Availability 3.6: Vorliegen von Verfahren, um physischen Zugriff auf das definierte System zu beschränken. Hierzu gehören u. a. Einrichtungen, Sicherungsmedien und andere Systemkomponenten wie Firewalls, Router und Server.
	SOC 2 Availability 3.10: Vorliegen von Verfahren, um Probleme der Systemverfügbarkeit und zugehörige Sicherheitsverstöße und andere Vorfälle zu identifizieren, zu melden und zu behandeln
	SOC 2 Confidentiality 3.3: Vereinbarkeit der Systemverfahren bezogen auf die Vertraulichkeit der Datenverarbeitung mit den dokumentierten Vertraulichkeitsrichtlinien

AWS-Compliance-Programm	Compliance-Anforderung
Service Organization Controls 2 (SOC 2) Der SOC 2-Bericht ist eine Bescheinigung, für die die Bewertung der Kontrollfunktionen auf die Kriterien der American Institute of Certified Public Accountants (AICPA) Trust Services Principles ausgeweitet wird. Diese Grundsätze bestimmen für Serviceanbieter wie AWS maßgebliche Kontrollfunktionen für die Praxis hinsichtlich Sicherheit, Verfügbarkeit, Integrität der Verarbeitung, Vertraulichkeit und Datenschutz. Weitere Informationen.	**SOC 2 Confidentiality 3.8.1:** Vorliegen von Verfahren, um logischen Zugriff auf das System und die vertraulichen Informationsressourcen im System zu beschränken. Hierzu gehört u. a. Folgendes: Beschränkung des Zugriffs auf Systemkonfigurationen, Superuser-Funktionalität, Masterpasswörter, leistungsstarke Dienstprogramme sowie Sicherheitsgeräte (z. B. Firewalls).
	SOC 2 Confidentiality 3.13: Vorliegen von Verfahren, um Verstöße gegen die Vertraulichkeit und Sicherheit des Systems und andere Vorfälle zu identifizieren, zu melden und zu behandeln
	SOC 2 Confidentiality 4.2: Vorliegen von Prozessen, um potenzielle Beeinträchtigungen der Fähigkeit der Entität zu identifizieren und zu beheben, kontinuierlich ihre Ziele gemäß der Vertraulichkeit ihres Systems und der zugehörigen Sicherheitsrichtlinien zu erreichen
	SOC 2 Integrity 3.6.g: Vorliegen von Verfahren, um logischen Zugriff auf das definierte System zu beschränken. Hierzu gehört u. a. Folgendes: Beschränkung des Zugriffs auf Systemkonfigurationen, Superuser-Funktionalität, Masterpasswörter, leistungsstarke Dienstprogramme sowie Sicherheitsgeräte (z. B. Firewalls)
	SOC 2 Integrity 4.1: Regelmäßige Überprüfung der Leistungsfähigkeit von Verarbeitungsintegrität und -sicherheit des Systems und Abgleich mit der definierten Systemverarbeitungsintegrität und zugehörigen Sicherheitsrichtlinien
	SOC 2 Integrity 4.2: Vorliegen eines Prozesses, um potenzielle Beeinträchtigungen der Fähigkeit der Entität zu identifizieren und zu beheben, kontinuierlich ihre Ziele gemäß ihrer definierten Systemverarbeitungsintegrität und der zugehörigen Sicherheitsrichtlinien zu erreichen

AWS-Compliance-Programm	Compliance-Anforderung
Internationale Organisation für Normung (International Organization for Standardization, ISO) 27001 DIN ISO/IEC 27001 ist ein weit verbreiteter globaler Sicherheitsstandard, der Sicherheitsanforderungen für Informationsmanagementsysteme beschreibt. Der Standard bietet eine systematische, auf regelmäßigen Risikobewertungen basierende Vorgehensweise zur Verwaltung von Unternehmens- und Kundendaten. Weitere Informationen.	*Aufgrund von Urheberrechtsgesetzen kann AWS keine Anforderungsbeschreibungen für ISO 27001 zur Verfügung stellen. Sie können eine Kopie des ISO 27001-Standards online von verschiedenen Quellen beziehen, u. a. von ISO.org.*
Federal Risk and Authorization Management Program (FedRAMP) FedRAMP ist ein US-Bundesprogramm zur Standardisierung der Sicherheitsbewertung, Autorisierung und laufenden Überwachung von Cloud-Produkten und -Services bis zur Einstufung "Moderate". Weitere Informationen.	**FedRAMP NIST 800-53 Rev 3 AU-2:** Die Organisation: a. bestimmt auf der Grundlage einer Risikobewertung und der Anforderungen der Aufgabe/des Unternehmens, dass das Informationssystem folgende Ereignisse prüfen können muss: [Zuweisung: von der Organisation festgelegte Liste prüffähiger Ereignisse]; b. koordiniert die Sicherheitsprüfungsfunktion mit anderen Entitäten der Organisation, für die prüfungsbezogene Informationen erforderlich sind, um gegenseitige Unterstützung zu fördern und die Auswahl prüffähiger Ereignisse zu leiten; c. begründet, warum die Liste prüffähiger Ereignisse für angemessen erachtet wird, um Ermittlungen nach Eintreten von Sicherheitsvorfällen zu unterstützen, und d. bestimmt auf der Grundlage aktueller Bedrohungsinformationen und kontinuierlicher Risikobewertung, dass die folgenden Ereignisse im Informationssystem geprüft werden müssen: [Zuweisung: die von der Organisation festgelegte Untermenge der in AU-2 a. definierten prüffähigen Ereignisse, die gemäß der Prüfungshäufigkeit für jedes identifizierte Ereignis (oder situationsbedingt) geprüft werden müssen].

AWS-Compliance-Programm	Compliance-Anforderung
Federal Risk and Authorization Management Program (FedRAMP) FedRAMP ist ein US-Bundesprogramm zur Standardisierung der Sicherheitsbewertung, Autorisierung und laufenden Überwachung von Cloud-Produkten und -Services bis zur Einstufung "Moderate". Weitere Informationen.	**FedRAMP NIST 800-53 Rev 4 AU 2:** Die Organisation: a. bestimmt, dass das Informationssystem folgende Ereignisse prüfen können muss: [Zuweisung: von der Organisation festgelegte prüffähige Ereignisse]; b. koordiniert die Sicherheitsprüfungsfunktion mit anderen Entitäten der Organisation, für die prüfungsbezogene Informationen erforderlich sind, um gegenseitige Unterstützung zu fördern und die Auswahl prüffähiger Ereignisse zu leiten; c. begründet, warum die prüffähigen Ereignisse für angemessen erachtet werden, um Ermittlungen nach Eintreten von Sicherheitsvorfällen zu unterstützen, und d. bestimmt, dass die folgenden Ereignisse im Informationssystem geprüft werden müssen: [Zuweisung: die von der Organisation festgelegte Untermenge der in AU-2 a. definierten prüffähigen Ereignisse, die gemäß der Prüfungshäufigkeit für jedes identifizierte Ereignis (oder situationsbedingt) geprüft werden müssen].
	FedRAMP NIST 800-53 Rev 3 AU-3: Das Informationssystem erstellt Auditdaten, die ausreichende Informationen enthalten, um mindestens Folgendes zu bestimmen: Ereignistyp, Ereigniszeitpunkt (Datum und Uhrzeit), Ereignisort, Ereignisquelle, Ergebnis des Ereignisses (Erfolg oder Fehler) sowie die Identität aller Benutzer/Subjekte im Zusammenhang mit dem aufgetretenen Ereignis.
	FedRAMP NIST 800-53 Rev 4 AU-3: Das Informationssystem erstellt Auditdaten, die Informationen enthalten, um mindestens Folgendes zu bestimmen: Ereignistyp, Ereigniszeitpunkt, Ereignisort, Ereignisquelle, Ergebnis des Ereignisses sowie die Identität aller Benutzer oder Subjekte im Zusammenhang mit dem aufgetretenen Ereignis.
	FedRAMP NIST 800-53 Rev 3 AU-4: Die Organisation weist Speicherkapazität für Auditdaten zu und konfiguriert die Überprüfung, um die Wahrscheinlichkeit einer Kapazitätsüberschreitung zu verringern.
	FedRAMP NIST 800-53 Rev 4 AU-4: Die Organisation weist Speicherkapazität für Auditdaten in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Speicheranforderungen für Auditdaten] zu.
	FedRAMP NIST 800-53 Rev 3 AU-5: Das Informationssystem: a. warnt bestimmte verantwortliche Organisationsmitarbeiter, wenn Fehler in überwachten Prozessen auftreten, und b. führt folgende zusätzliche Aktionen durch: [Zuweisung: von der Organisation festgelegte Aktionen, die durchzuführen sind (z. B. Informationssystem herunterfahren, die ältesten Auditdaten überschreiben, die Generierung von Auditdaten stoppen)].

AWS-Compliance-Programm	Compliance-Anforderung
Federal Risk and Authorization Management Program (FedRAMP) FedRAMP ist ein US-Bundesprogramm zur Standardisierung der Sicherheitsbewertung, Autorisierung und laufenden Überwachung von Cloud-Produkten und -Services bis zur Einstufung "Moderate". Weitere Informationen.	**FedRAMP NIST 800-53 Rev 4 AU-5:** Das Informationssystem: a. warnt [Zuweisung]: von der Organisation festgelegtes Personal], wenn Fehler in überwachten Prozessen auftreten, und b. führt folgende zusätzliche Aktionen durch: [Zuweisung: von der Organisation festgelegte Aktionen, die durchzuführen sind (z. B. Informationssystem herunterfahren, die ältesten Auditdaten überschreiben, die Generierung von Auditdaten stoppen)].
	FedRAMP NIST 800-53 Rev 3 AU-6: Die Organisation: a. überprüft und analysiert Auditdaten des Informationssystems [Zuweisung: von der Organisation festgelegte Häufigkeit] hinsichtlich Hinweisen auf unangemessene oder ungewöhnliche Aktivitäten und meldet bestimmten verantwortlichen Organisationsmitarbeitern die Ergebnisse und b. passt das Niveau für Auditprüfungen, -analysen und -berichte im Informationssystem an, wenn sich das Risiko für Abläufe und Werte der Organisation, für Personen, andere Organisationen oder den Staat ändert. Dies erfolgt auf der Grundlage strafverfolgungsrelevanter Informationen, nachrichtendienstlicher Informationen oder anderer zuverlässiger Informationsquellen.
	FedRAMP NIST 800-53 Rev 3 AU-6: Die Organisation: a. überprüft und analysiert Auditdaten des Informationssystems [Zuweisung: von der Organisation festgelegte Häufigkeit] hinsichtlich Hinweisen auf [Zuweisung: von der Organisation festgelegte unangemessene oder ungewöhnliche Aktivitäten] und b. meldet Ergebnisse an [Zuweisung: von der Organisation festgelegte/s Personal/Rollen].
	FedRAMP NIST 800-53 Rev 3 AU-8: Das Informationssystem verwendet interne Systemuhren, um Zeitstempel für Auditdaten zu generieren.
	FedRAMP NIST 800-53 Rev 4 AU-8: Das Informationssystem: a. verwendet interne Systemuhren, um Zeitstempel für Auditdaten zu generieren, und b. generiert die Zeit in den Zeitstempeln nach dem Schema der Coordinated Universal Time (UTC) oder der Greenwich Mean Time (GMT) und erfüllt [Zuweisung: von der Organisation festgelegte Granularität der Zeitmessung].
	FedRAMP NIST 800-53 Rev 3 AU-9: Das Informationssystem schützt die Prüfungsinformationen und -tools vor unbefugten Zugriffen, Änderungen und Löschungen.
	FedRAMP NIST 800-53 Rev 4 AU-9: Das Informationssystem schützt die Prüfungsinformationen und -tools vor unbefugten Zugriffen, Änderungen und Löschungen.
	FedRAMP NIST 800-53 Rev 3 AU-10: Das Informationssystem schützt vor Personen, die fälschlicherweise abstreiten, bestimmte Aktionen durchgeführt zu haben.

AWS-Compliance-Programm	Compliance-Anforderung
Federal Risk and Authorization Management Program (FedRAMP) FedRAMP ist ein US-Bundesprogramm zur Standardisierung der Sicherheitsbewertung, Autorisierung und laufenden Überwachung von Cloud-Produkten und -Services bis zur Einstufung "Moderate". Weitere Informationen.	**FedRAMP NIST 800-53 Rev 4 AU-10:** Das Informationssystem schützt vor Personen (oder Prozessen, die im Auftrag von Personen handeln), die fälschlicherweise abstreiten, [Zuweisung: von der Organisation festgelegte Aktionen, die der Nachweisbarkeit unterliegen] durchgeführt zu haben.
	FedRAMP NIST 800-53 Rev 3 AU-11: Die Organisation speichert Auditdaten für [Zuweisung: von der Organisation festgelegter Zeitraum gemäß der Richtlinie zur Aufbewahrungsdauer], um Ermittlungen nach Eintreten von Sicherheitsvorfällen zu unterstützen und die aufsichts-rechtlichen und organisationsspezifischen Anforderungen für die Informationsaufbewahrung zu erfüllen.
	FedRAMP NIST 800-53 Rev 4 AU-11: Die Organisation speichert Auditdaten für [Zuweisung: von der Organisation festgelegter Zeitraum gemäß der Richtlinie zur Aufbewahrungsdauer], um Ermittlungen nach Eintreten von Sicherheitsvorfällen zu unterstützen und die aufsichts-rechtlichen und organisationsspezifischen Anforderungen für die Informationsaufbewahrung zu erfüllen.