DSGVO-Compliance auf AWS

September 2018

Hinweise

Dieses Dokument wird nur zu Informationszwecken zur Verfügung gestellt. Es stellt das aktuelle Produktangebot und die Praktiken von AWS zum Erstellungsdatum dieses Dokuments dar. Änderungen vorbehalten. Kunden sind verantwortlich für ihre eigene Interpretation der in diesem Dokument zur Verfügung gestellten Informationen und für die Nutzung der AWS-Produkte oder -Services. Diese werden alle ohne Mängelgewähr und ohne jegliche Garantie, weder ausdrücklich noch stillschweigend, bereitgestellt. Dieses Dokument gibt keine Garantien, Gewährleistungen, vertragliche Verpflichtungen, Bedingungen oder Zusicherungen von AWS, seinen Partnern, Zulieferern oder Lizenzgebern. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Bestandteil der Vereinbarungen von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Inhalt

Die Datenschutz-Grundverordnung im Überblick 1

Durch die DSGVO hervorgerufene Veränderungen für in der EU tätige Organisationen 1

Ist AWS auf die DSGVO vorbereitet? 1

AWS Data Processing Addendum (DPA) 2

Rolle von AWS im Rahmen der DSGVO 2

CISPE-Verhaltenskodex 2

Datenzugriffskontrollen 3

Überwachung und Protokollierung 5

Schutz Ihrer Daten auf AWS 6

Verschlüsselung: Datenverschlüsselung auf AWS 6

Striktes Compliance-Framework und hohe Sicherheitsstandards 12

Modell der gemeinsamen Verantwortung für die Sicherheit 12

AWS-Compliance-Programm 13

Anforderungskatalog Cloud Computing (C5 – ein vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickeltes Prüfungsschema) 14

Dokumentversionen 15

Kurzbeschreibung

Ziel dieses Dokuments ist es, Antworten auf Fragen wie „Wie unterstützt AWS seine Kunden dabei, die Datenschutz-Grundverordnung (DSGVO) einzuhalten?“ zu liefern. Amazon Web Services (AWS) unterstützt seine Kunden mit Services und Ressourcen dabei, die Richtlinien der DSGVO einzuhalten, die möglicherweise auf deren Geschäftsbetrieb zutreffen. Dies beinhaltet die Einhaltung des Verhaltenskodex für Cloud Infrastructure Services Providers in Europe (CISPE) durch AWS, präzise Steuerungsmöglichkeiten für den Datenzugriff, Protokollierungs- und Überwachungstools, die Verschlüsselung, die Schlüsselverwaltung, Prüfungsmöglichkeiten, die Einhaltung von IT-Sicherheitsstandards, insbesondere die Bestätigungen der Anforderungen Cloud Computing Compliance Controls Catalogue (C5) des BSI.

Die Datenschutz-Grundverordnung im Überblick

Die Datenschutz-Grundverordnung (DSGVO) ist ein neues europäisches Datenschutzgesetz. Die DSGVO bringt die innerhalb der Europäischen Union (EU) geltenden Datenschutzgesetze in Einklang, indem sie als einzige Verordnung zum Thema Datenschutz für jeden Mitgliedsstaat bindend ist.
Die DSGVO gilt für sämtliche Unternehmen, die über eine Niederlassung in der EU verfügen oder die Waren und Dienstleistungen an Personen liefern und dabei die "personenbezogenen Daten" von EU-Bürgern verarbeiten. Unter personenbezogenen Daten sind alle Informationen zu verstehen, die sich auf eine identifizierte natürliche Person beziehen oder anhand derer eine natürliche Person identifiziert werden kann.

Durch die DSGVO hervorgerufene Veränderungen für in der EU tätige Organisationen

Einer der wichtigsten Aspekte der Datenschutz-Grundverordnung ist die angestrebte Harmonisierung der Verarbeitung und Nutzung personenbezogener Daten und ihr sicherer Austausch in den EU-Mitgliedsstaaten. Organisationen müssen die Sicherheit der verarbeiteten Daten sowie ihre Einhaltung der Datenschutz-Grundverordnung kontinuierlich nachweisen. Dazu sind die Implementierung und regelmäßige Prüfung nachhaltiger technischer und organisatorischer Maßnahmen sowie Richtlinien für die Einhaltung erforderlich. Aufsichtsbehörden können Strafen von bis zu 20 Millionen Euro oder 4 % des jährlichen weltweiten Umsatzes (je nachdem, was höher ausfällt) verordnen.

Ist AWS auf die DSGVO vorbereitet?

Unsere Experten für Compliance, Datensicherheit und Sicherheit arbeiten mit Kunden aus aller Welt zusammen und beraten sie zur Ausführung von Workloads in der AWS Cloud nach dem Inkrafttreten der Datenschutz-Grundverordnung. Es sind bereits sämtliche bisherigen Aktivitäten von AWS geprüft worden, um sicherzustellen, dass die neue Datenschutz-Grundverordnung eingehalten wird.

Wir bestätigen, dass die AWS-Services die Datenschutz-Grundverordnung erfüllen.

Gemäß Art. 32 sind Verantwortliche und Auftragsverarbeiter verpflichtet, "angemessene technische und organisatorische Maßnahmen" umzusetzen, und zwar "unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen". Die DSGVO bietet konkrete Vorschläge zur Durchführung möglicherweise erforderlicher Sicherheitsmaßnahmen wie etwa:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

AWS Data Processing Addendum (DPA)

Der AWS-Vertragsanhang zur DSGVO-konformen Datenverarbeitung (AWS GDPR Data Processing Addendum – GDPR DPA) unterstützt Sie dabei, die vertraglichen Verpflichtungen im Rahmen der DSGVO einzuhalten. Das AWS GDPR DPA ist in den Nutzungsbedingungen der AWS-Services integriert und gilt automatisch für alle Kunden weltweit, die sich an die DSGVO halten müssen.

Rolle von AWS im Rahmen der DSGVO

AWS wird entsprechend der DSGVO sowohl als Datenauftragsverarbeiter als auch als Datenverantwortlicher gesehen.

- **AWS als Datenauftragsverarbeiter –** Wenn Kunden und APN-Partner (AWS Partner Network) die AWS-Services zur Verarbeitung personenbezogener Daten verwenden, agiert AWS als Datenauftragsverarbeiter. Kunden und APN-Partner können die Steuermöglichkeiten, die wir in den AWS-Services zur Verfügung stellen – etwa die für Sicherheitskonfigurationen – für die Verarbeitung personenbezogener Daten nutzen. In diesen Fällen kann der Kunde oder APN-Partner selbst als Datenverantwortlicher oder Datenauftragsverarbeiter und AWS als Datenauftragsverarbeiter oder untergeordneter Datenauftragsverarbeiter agieren. Im AWS-Vertragsanhang zur DSGVO-konformen Datenverarbeitung sind die Verpflichtungen von AWS als Datenauftragsverarbeiter dargelegt.
- **AWS als Datenverantwortlicher –** Wenn AWS direkt personenbezogene Daten erhebt und die Zwecke und Verfahren für ihre Verarbeitung bestimmt – wenn AWS z. B. Kontoinformationen für die Kontoregistrierung, die Verwaltung und den Zugriff auf Services oder Kontaktinformationen für das AWS-Konto speichert, um über den Kunden-Support Unterstützung anzubieten – agiert das Unternehmen als Datenverantwortlicher und sichert die Einhaltung der DSGVO vertraglich zu.

CISPE-Verhaltenskodex

Die DSGVO liefert eine Grundlage für die Genehmigung von Verhaltenskodizes, anhand derer Verantwortliche und Auftragsverarbeiter Compliance und bewährte Methoden nachweisen können. Einer solcher Kodex, dessen offizielle Zulassung noch aussteht, ist der CISPE (Code of Conduct for Cloud Infrastructure Service Providers – Verhaltenskodex für Anbieter von Cloud-Infrastrukturdiensten [im Folgenden: der „Verhaltenskodex"]). Kunden von Cloud-Anbietern, die diesen Code of Conduct bestätigen, erhalten dadurch ein vertragliche Zusicherung auf die Einhaltung der DSGVO.
Zu den wichtigsten Vorteilen dieser Verhaltensregeln gehören:

- Es wird klar festgelegt, wer beim Datenschutz für welche Aspekte verantwortlich ist: Im Verhaltenskodex werden die Rollen von Anbieter und Kunden gemäß der

Datenschutz-Grundverordnung erläutert, insbesondere für Cloud-Infrastrukturdienste.

- Der Verhaltenskodex gibt die Prinzipien vor, an die sich Anbieter halten müssen: Der Verhaltenskodex stellt in Übereinstimmung mit der Datenschutz-Grundverordnung Grundprinzipien für Aktionen und Verpflichtungen auf, die seitens der Anbieter einzuhalten sind, um Kunden bei der Erfüllung der Vorgaben zu unterstützen. Kunden können sich bei ihren eigenen Strategien zur Einhaltung und zum Datenschutz auf diese verbindlichen Zusagen verlassen.
- Der Verhaltenskodex stattet Kunden mit allen nötigen Informationen aus, die sie bei den Entscheidungen bezüglich der Einhaltung benötigen: Laut dem Verhaltenskodex müssen Anbieter die Schritte, mit denen sie ihren Sicherheitsverpflichtungen nachkommen, transparent darlegen. Diese Schritte umfassen z. B. Benachrichtigungen bei Datenpannen, Datenlöschung, Datenverarbeitung durch Drittanbieter und Anfragen von Strafverfolgungsbehörden und anderen Behörden. Kunden können mithilfe dieser Informationen die gebotenen hohen Sicherheitsniveaus nachvollziehen.

Am 13.02.2017 gab AWS die Erklärung ab, dass Amazon EC2, Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), AWS Identity and Access Management (IAM), AWS CloudTrail, Amazon Elastic Block Store (Amazon EBS), VPC, KMS und Cloud HSM alle Punkte in diesem Kodex erfüllen (siehe https://cispe.cloud/publicregister). Unsere Kunden erhalten dadurch eine weitere Zusicherung von AWS: Mit AWS haben sie die Kontrolle über ihre Daten in einer sicheren, geschützten Umgebung, in der die Vorschriften eingehalten werden. Wir verhalten uns nicht nur im Einklang mit dem o. g. Kodex, sondern erfüllen auch Anforderungen von verschiedenen international anerkannten Zertifikaten und Akkreditierungen, darunter ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2, SOC 3 und PCI DSS Level 1.

Datenzugriffskontrollen

Artikel 25 der DSGVO sieht vor, dass der Verantwortliche "geeignete technische und organisatorische Maßnahmen" treffen soll, "die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden". Die im Folgenden benannten Verfahren zur Zugriffssteuerung von AWS helfen Ihnen, diese Vorgaben zu erfüllen, indem sie nur autorisierten Administratoren, Benutzern und Anwendungen den Zugriff auf AWS-Ressourcen und -Kundendaten gewähren:

- **Detailliert abgestimmter Zugriff auf AWS-Objekte in S3-Buckets/SQS/SNS usw. –** Sie können einzelnen Personen für verschiedene Ressourcen unterschiedliche Berechtigungen gewähren. So können Sie z. B. einigen Benutzern vollständigen Zugriff auf die Amazon Elastic Compute Cloud (Amazon EC2), den Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift und andere AWS-Services gewähren. Anderen Benutzern können Sie schreibgeschützten Zugriff auf nur einige S3-Buckets oder aktiven Verwaltungszugriff auf nur einige EC2-Instances oder ausschließlich Zugriff auf Ihre Rechnungsdaten gewähren.
- **Multi-Factor-Authentication (MFA) –** Als zusätzliche Sicherheitsmaßnahme

können Sie Ihrem Konto sowie bestimmten Benutzern eine Multi-Faktor-Authentifizierung zuordnen. Hierbei geben Sie (bzw. die Benutzer) zum Zugriff auf Ihr Konto nicht nur ein Passwort oder einen Zugriffsschlüssel ein, sondern z. B. auch einen Code, der an ein eigens dafür vorgesehenes Gerät gesandt wird.

- **Authentifizierung von API-Anforderungen –** Mit IAM-Funktionen können Sie Anwendungen, die auf EC2-Instances ausgeführt werden, sicher mit den Anmeldedaten ausstatten, die sie für den Zugriff auf andere AWS-Ressourcen wie S3-Buckets, RDS oder DynamoDB-Datenbanken benötigen.
- **Geografische Einschränkungen –** Durch die Technik des so genannten "Geoblocking" können Sie Benutzern, die sich außerhalb der von Ihnen festgelegten geografischen Regionen befinden, den Zugriff verwehren. Dies erfolgt durch eine CloudFront-Webdistribution. Hierzu stehen Ihnen zwei Optionen zur Auswahl:
  - Machen Sie von der Funktion CloudFront (geografische Einschränkung) Gebrauch. Hiermit verwehren Sie den Zugriff auf Dateien mit bestimmten Distributionsmerkmalen und schränken den Zugriff auf Länderebene ein.
  - Machen Sie von den Diensten Dritter zur Standortnutzungsbeschränkung Gebrauch. Mit dieser Option können Sie den Zugriff auf einen Teil der Dateien einer Distribution bzw. noch detaillierter als auf Länderebene einschränken.
- **Token für den vorübergehenden Zugriff (über STS) –** Der AWS Security Token Service (AWS STS) ermöglicht Ihnen, vertrauenswürdigen Benutzern temporäre, gesicherte Zugangsdaten bereitzustellen, mit denen ein steuerbarer Zugriff auf Ihre AWS-Ressourcen erfolgt. Temporäre Zugangsdaten verhalten sich zu langfristig gültigen Zugangsdaten (Ihrer IAM-Benutzer) nahezu identisch. Folgende Unterschiede bestehen:
  - Temporäre, gesicherte Zugangsdaten ermöglichen den Zugriff nur über einen kurzen Zeitraum hinweg. Dieser Zeitraum kann wenige Minuten, aber auch einige Stunden betragen. Nach dem Gültigkeitsablauf der Zugangsdaten werden sie von AWS nicht mehr als solche erkannt. Ein Zugang, der per API angefordert wird, ist danach nicht mehr möglich.
  - Temporäre Zugangsdaten werden nicht in Zusammenhang mit dem Benutzer gespeichert, sondern dynamisch generiert und dem Benutzer auf Abfrage bereitgestellt. Vor dem Gültigkeitsablauf der temporären Zugangsdaten kann ein Benutzer bei entsprechenden Rechten neue Zugangsdaten anfordern.

  Somit haben temporäre Zugangsdaten die folgenden Vorteile:
  - Es müssen keine langfristigen, gesicherten AWS-Zugangsdaten im Rahmen einer Anwendung bereitgestellt oder integriert werden.
  - Sie können Benutzern Zugriffsrechte auf Ihre AWS-Ressourcen gewähren, ohne ihnen eine AWS Identity zuordnen zu müssen. Vorübergehende Anmeldedaten bilden die Basis für Rollen und den Identitätsverbund.
  - Diese sind nur kurzfristig gültig, somit ist deren Rotation oder ihr ausdrücklicher Widerruf nach Ablauf ihrer Notwendigkeit nicht erforderlich. Danach ist eine Wiederverwendung ausgeschlossen. Sie können bis zu einer maximalen Grenze bestimmen, wie lange die Anmeldedaten gültig bleiben.

Überwachung und Protokollierung

Die DSGVO schreibt vor: "Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen". In diesem Artikel werden auch die aufzuzeichnenden Details aufgeführt. Anders ausgedrückt schreibt die DSGVO die Überwachung der Verarbeitung derjenigen Daten vor, anhand derer Personen identifiziert werden können (personenbezogene Daten, PII). Zusätzlich erfordern es die Anzeigepflichten in Bezug auf die zeitnahe Benachrichtigung über Datenpannen, dass entsprechende Vorfälle nahezu in Echtzeit erkannt werden. Zur Erfüllung dieser Auflage bietet Ihnen AWS verschiedene Überwachungs- und Protokollierungsdienste:

- **Asset-Management und -Konfiguration mit AWS Config –** AWS Config bietet Ihnen einen detaillierten Überblick über die Konfiguration der AWS-Ressourcen unter Ihrem AWS-Konto. Hierzu zählt auch, wie die Ressourcen zueinander in Verbindung stehen und wie sie in der Vergangenheit konfiguriert wurden. So können Sie erkennen, wie sich die Konfigurationen und Beziehungen mit der Zeit ändern.
  Bei AWS-Ressourcen handelt es sich um bestimmte Einheiten, mit denen Sie im Rahmen von AWS arbeiten können, etwa eine Amazon Elastic Compute Cloud (EC2)-Instance, ein Amazon Elastic Block Store (EBS)-Volume, eine Sicherheitsgruppe oder eine Amazon Virtual Private Cloud (VPC). Eine vollständige Liste der von AWS Config unterstützten AWS-Ressourcen finden Sie unter „Unterstützte AWS-Ressourcentypen“.
  AWS Config ermöglicht Ihnen Folgendes:
  - Sie können Ihre AWS-Ressourcenkonfigurationen im Hinblick auf erwünschte Einstellungen auswerten.
  - Sie können eine Momentaufnahme der aktuellen Konfigurationen der unterstützten, mit Ihrem AWS-Konto verknüpften Ressourcen abfragen.
  - Sie können Konfigurationen von in Ihrem Konto befindlichen Ressourcen wiederherstellen.
  - Sie können in der Vergangenheit festgelegte Konfigurationen von Ressourcen wiederherstellen.
  - Sie können bei der Erstellung, Konfigurationsänderung oder Löschung von Ressourcen benachrichtigt werden.
  - Sie können die Beziehungen verschiedener Ressourcen prüfen. Sie können beispielsweise nach allen Ressourcen suchen, die eine bestimmte Sicherheitsgruppe verwenden.
- **Compliance-Auditing und Sicherheitsanalysen mit AWS CloudTrail –** Mit AWS CloudTrail können Sie Ihre AWS-Bereitstellungen in der Cloud in einem Protokoll der AWS API-Aufrufe Ihres Kontos überwachen (z. B. der API-Aufrufe über die AWS Management Console, die AWS SDKs, die Befehlszeilen-Tools und AWS-Services einer höheren Ebene). Außerdem können Sie erkennen, welche Benutzer und Konten AWS-APIs für Services, die CloudTrail unterstützen, aufgerufen haben, ebenso wie die Quell-IP-Adresse, von der die Aufrufe ausgingen, und wann die Aufrufe stattgefunden haben. Sie können CloudTrail

mithilfe der API in Anwendungen integrieren, die Trail-Erstellung für Ihre Organisation automatisieren, den Status Ihrer Trails prüfen und steuern, wie Administratoren die CloudTrail-Protokollierung aktivieren bzw. deaktivieren.

- **Aufzeichnung von Konfigurationsänderungen durch TrustedAdvisor –** Durch Protokollierung erhalten Sie detaillierte Zugriffsprotokolle für die in einem S3-Bucket gespeicherten Daten. Diese Zugriffsprotokolle enthalten Details zu den Datenabrufen, wie beispielsweise die Art des Abrufs, die bei dem Abruf verwendeten Dateien oder Datum und Uhrzeit des Abrufs. Weitere Informationen zu den Inhalten eines Protokolls finden Sie im Abschnitt „Server Access Log Format“ (Format des Serverzugriffsprotokolls) im Entwicklerhandbuch zu Amazon Simple Storage Service.
- Serverzugriffsprotokolle sind für viele Anwendungen nützlich, da sie S3-Bucket-Eigentümern Einblick in die Art der Anfragen bieten, die von Clients erstellt werden, die sich ihrer Kontrolle entziehen. Standardmäßig erfasst Amazon S3 keine Servicezugriffsprotokolle. Wenn Sie die Protokollierung jedoch aktivieren, liefert Amazon S3 stündlich kumulierte Zugriffsprotokolle an Ihren S3-Bucket.
- Detaillierte Protokollierung des Zugriffs auf S3-Objekte
- Ausführliche Informationen zu Abläufen im Netzwerk mit VPC-FlowLogs
- Regelbasierte Konfigurationsprüfungen und -aktionen mit AWS Config-Regeln
- Filterung und Überwachung von HTTP-Zugriffen auf Anwendungen mit WAF-Funktionen in CloudFront

Schutz Ihrer Daten auf AWS

Die DSGVO fordert, "geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: (…) die Pseudonymisierung und Verschlüsselung personenbezogener Daten (…)". Darüber hinaus müssen Organisationen personenbezogene Daten vor unbefugter Weitergabe und unbefugtem Zugriff schützen. Eine Benachrichtigung des Datensubjektes oder eine Meldung an die Behörden kann unterbleiben (wodurch Verwaltungskosten und Reputationsschäden vermieden werden), wenn durch bereits vor der Datenpanne ergriffene "adäquate technische und organisatorische Maßnahmen (…), wie Verschlüsselung", eine unbefugte Kenntnisnahme der Daten durch Dritte ausgeschlossen werden kann. AWS bietet verschiedene hochgradig skalierbare und sichere Datenverschlüsselungsmechanismen zum Schutz der auf AWS gespeicherten und verarbeiteten Kundendaten an:

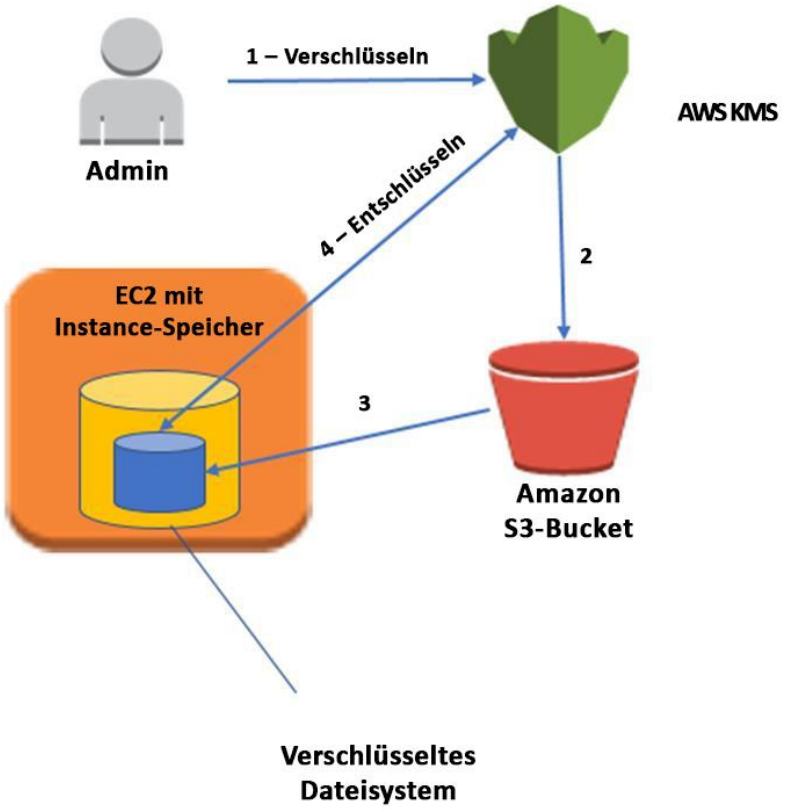
Verschlüsselung: Datenverschlüsselung auf AWS

- **Verschlüsselung ruhender Daten mit AES256 (EBS/S3/Glacier/RDS) –** Die Verschlüsselung ruhender Daten ist für die Einhaltung gesetzlicher Vorgaben entscheidend; dadurch soll gewährleistet werden, dass sensible, auf Datenträgern gespeicherte Daten für Benutzer oder Anwendungen ohne gültige Zugriffsschlüssel nicht lesbar sind. AWS stellt Optionen und Verfahren für ruhende Daten und für die Verwaltung von Zugriffsschlüsseln zur Verfügung, um die Verschlüsselung für den Kunden zu vereinfachen. Beispielsweise können Sie Amazon EBS-Volumes verschlüsseln und Amazon S3-Buckets für die serverseitige Verschlüsselung (SSE) konfigurieren. Hierbei kommt AES-256-

Verschlüsselung zum Einsatz. Zusätzlich unterstützt Amazon RDS die transparente Datenverschlüsselung (TDE).
Durch die Instance-Speicherung werden Amazon EC2-Instances vorübergehend auf Block-Ebene abgelegt. Diese Speicherung erfolgt auf Datenträgern, die physisch an einen Hostrechner angeschlossen sind. Die Instance-Speicherung ist ideal für die vorübergehende Speicherung von Daten, die sich häufig ändern, z. B. Puffer, Caches und Entwurfsdaten. Standardmäßig werden die auf diesen Datenträgern gespeicherten Daten nicht verschlüsselt. Eine Methode zum Verschlüsseln von Daten auf Linux-EC2-Instance-Speichern sind in Linux integrierte Bibliotheken. Diese Methode verschlüsselt Dateien transparent und schützt so vertrauliche Daten. Anwendungen, die die Daten verarbeiten, können diese Verschlüsselung auf Datenträgerebene nicht erkennen.

- **Verschlüsselung von Datenträgern und Dateisystemen –** Zur Verschlüsselung der Dateien in Instance-Speichern stehen zwei Methoden zur Verfügung. Die erste Methode besteht in der Verschlüsselung des Datenträgers, wobei der gesamte Datenträger bzw. der betreffende Datenträgerblock durch mindestens einen Zugriffsschlüssel verschlüsselt wird. Diese Methode wirkt unterhalb der Dateisystemebene, funktioniert betriebssystemübergreifend und verbirgt Verzeichnis- und Dateiinformationen wie Name und Größe. Bei Encrypting File System handelt es sich z. B. um eine Microsoft-Erweiterung zu New Technology File System (NTFS), das zum Betriebssystem Windows NT gehört. Sie sorgt für eine Verschlüsselung des Datenträgers.
  Die zweite Methode besteht in der Verschlüsselung auf Dateisystemebene. Es werden Dateien und Verzeichnisse verschlüsselt, jedoch nicht der gesamte Datenträger bzw. die gesamte Partition. Die Verschlüsselung auf Dateisystemebene ist dem Dateisystem übergeordnet und somit auf verschiedene Betriebssysteme übertragbar.
- **Dm-crypt-Infrastruktur von Linux –** Bei dm-crypt handelt es sich um einen Verschlüsselungsmechanismus für Linux auf Kernelebene, mit dem Benutzer ein verschlüsseltes Dateisystem bereitstellen können. Unter Bereitstellung eines Dateisystems versteht man den Prozess, bei dem ein Dateisystem einem Verzeichnis (Bereitstellungspunkt) zugeordnet wird, wodurch es für das Betriebssystem verfügbar wird. Nach dem Bereitstellen sind sämtliche Dateien eines Dateisystems für Anwendungen (ohne zusätzlichen Interaktionsbedarf) verfügbar; diese Dateien werden verschlüsselt, wenn sie auf Datenträgern gespeichert werden.
  Der Device Mapper ist eine Infrastruktur im Linux 2.6- und 3.x-Kernel, mit der in generischer Weise virtuelle Schichten von Block Devices erstellt werden können. Der Device Mapper liefert eine transparente Verschlüsselung der Block Devices unter Anwendung der Crypto-API des Kernels. In der Lösung in dieser Veröffentlichung wird dm-crypt in Verbindung mit einem datenträgergestützten System verwendet, das mithilfe des Logical Volume Manager (LVM) einem logischen Volume zugewiesen wird. LVM ermöglicht die Verwaltung des logischen Volumes für den Linux-Kernel.

- **Überblick über die Architektur –** Das folgende allgemeine architektonische Diagramm veranschaulicht das Konzept, mit dem EC2-Instances verschlüsselt werden können. Ein detaillierter Implementierungsplan folgt im nächsten Abschnitt.



1. Der Administrator verschlüsselt ein geheimes Passwort unter Anwendung von KMS. Das verschlüsselte Passwort wird in einer Datei gespeichert.
2. Der Administrator legt die Datei mit dem verschlüsselten Passwort in einem S3-Bucket ab.
3. Wird die Instance gestartet, kopiert diese die verschlüsselte Datei auf einen internen Datenträger.
4. Die EC2-Instance entschlüsselt die Datei per KMS und stellt das Passwort in reiner Textform wieder her. Mit diesem Passwort kann das durch Linux verschlüsselte Dateisystem über LUKS konfiguriert werden. Alle auf ein verschlüsseltes Dateisystem geschriebenen Daten werden durch einen AES-256-Algorithmus verschlüsselt.

- **Zentralisiertes (nach Region) verwaltetes Schlüsselmanagement –** AWS Key Management Service (KMS) ist ein verwalteter Service, der Ihnen die Erstellung und Kontrolle der für die Datenverschlüsselung verwendeten Verschlüsselungsschlüssel erleichtert und zum Schutz der Sicherheit Ihrer Schlüssel Hardware-Sicherheitsmodule (HSMs) einsetzt. Der AWS Key Management Service ist in verschiedene AWS-Services integriert, um Ihnen

beim Schutz der mit diesen Services gespeicherten Daten zu helfen. AWS Key Management Service ist auch in AWS CloudTrail integriert und stellt für Sie Protokolle der gesamten Schlüsselnutzung bereit, um Sie bei der Einhaltung Ihrer gesetzlichen und Compliance-Anforderungen zu unterstützen.

- **Zentralisierte Schlüsselverwaltung –** AWS Key Management Service bietet Ihnen eine zentrale Kontrolle Ihrer Verschlüsselungsschlüssel. Sie können auf einfache Weise Schlüssel erstellen, importieren und rotieren sowie Verwendungsrichtlinien und Audit-Nutzung über die AWS-Managementkonsole oder mit dem AWS SDK oder der AWS CLI definieren. Die Masterschlüssel in KMS, ob von Ihnen importiert oder durch KMS für Sie erstellt, werden in sehr robusten Speichern verschlüsselt gespeichert, um sicherzustellen, dass sie bei Bedarf abgerufen werden können. Sie können festlegen, dass KMS die in KMS erstellten Masterschlüssel einmal im Jahr automatisch rotiert. Sie müssen in diesem Fall bereits mit Ihrem Masterschlüssel verschlüsselte Daten nicht nochmals verschlüsseln. Sie müssen ältere Versionen Ihrer Masterschlüssel nicht im Auge behalten, KMS hält sie für die Entschlüsselung früher verschlüsselter Daten verfügbar. Sie können neue Masterschlüssel erstellen und jederzeit steuern, wer darauf Zugriff hat und mit welchen Services sie verwendet werden können. Sie können auch Schlüssel aus Ihrer eigenen Schlüsselverwaltungsinfrastruktur importieren und in KMS verwenden.
- **AWS-Service-Integration –** AWS Key Management Service ist nahtlos in verschiedene andere AWS-Services integriert. Diese Integration bedeutet, dass Sie zum Verschlüsseln der Daten, die Sie in diesen Services speichern, einfach AWS KMS-Masterschlüssel verwenden können. Sie können einen Standard-Masterschlüssel verwenden, der entweder automatisch für Sie erstellt wird und nur innerhalb des integrierten Services verwendbar ist, oder einen benutzerdefinierten Masterschlüssel auswählen, den Sie in KMS erstellt oder aus Ihrer eigenen Schlüsselverwaltungsinfrastruktur importiert haben.
- **Audit-Fähigkeiten –** Wenn Sie AWS CloudTrail für Ihr AWS-Konto aktiviert haben, wird jede Verwendung eines Schlüssels, den Sie in KMS speichern, in einer Protokolldatei aufgezeichnet, die an den von Ihnen bei der Aktivierung von AWS CloudTrail festgelegte Amazon S3-Bucket geliefert wird. Die aufgezeichneten Informationen enthalten Details zu Benutzer, Zeit, Datum und verwendetem Schlüssel.
- **Skalierbarkeit, Beständigkeit und Hochverfügbarkeit –** AWS Key Management Service ist ein verwalteter Service. Bei zunehmender Nutzung von AWS KMS-Verschlüsselungsschlüsseln müssen Sie keine Schlüsselverwaltungsinfrastruktur zukaufen. AWS KMS wird automatisch Ihrem Verschlüsselungsschlüssel-Bedarf entsprechend skaliert.
  Die von AWS KMS für Sie erstellten oder von Ihnen importierten Masterschlüssel können vom Service nicht exportiert werden. AWS KMS speichert mehrere Kopien verschlüsselter Versionen Ihrer Schlüssel in Systemen, die für eine Beständigkeit von 99,999999999 % konzipiert sind. So wird sichergestellt, dass Ihre Schlüssel verfügbar sind, wenn Sie darauf

zugreifen müssen. Wenn Sie jedoch Schlüssel in KMS importieren, müssen Sie eine Kopie Ihrer Schlüssel sicher aufbewahren, damit Sie sie jederzeit erneut importieren können, da KMS keine Kopien von importierten Kundenschlüssel anfertigen kann.
AWS KMS wird in mehreren Availability Zones in einer AWS-Region bereitgestellt, um eine hohe Verfügbarkeit für Ihre Verschlüsselungsschlüssel zu bieten.

- **Sicher –** AWS KMS ist so konzipiert, dass niemand auf Ihre Masterschlüssel Zugriff hat. Der Service baut auf Systemen auf, die für den Schutz Ihrer Masterschlüssel konzipiert wurden. Dabei werden umfassende Härtungsmethoden eingesetzt: Es werden niemals Klartext-Masterschlüssel auf einem Datenträger gespeichert, sie werden nicht dauerhaft im Arbeitsspeicher gespeichert und es gibt Beschränkungen, welche Systeme auf Hosts zugreifen können, die Schlüssel verwenden. Jeder Zugriff zum Aktualisieren von Software im Service wird über einen Genehmigungsprozess mit mehreren Teilnehmern kontrolliert, der durch eine unabhängige Gruppe bei Amazon überwacht und geprüft wird.
  Weitere Informationen über die Funktionsweise von AWS KMS finden Sie im Whitepaper zum AWS Key Management Service.

- **Bildung eines IPsec-Tunnels in AWS mithilfe von VPN-Gateways –** Amazon VPC ermöglicht die Bereitstellung eines logisch isolierten Bereichs der Amazon Web Services (AWS)-Cloud, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk ausführen können. Sie haben die vollständige Kontrolle über Ihre virtuelle Netzwerkumgebung, u. a. bei der Auswahl Ihres eigenen IP-Adressbereichs, dem Erstellen von Subnetzen und der Konfiguration von Routing-Tabellen und Netzwerk-Gateways. Darüber hinaus können Sie eine sichere hardwarebasierte VPN-Verbindung (Virtual Private Network) zwischen Ihrem Unternehmensrechenzentrum und Ihrer VPC einrichten und die AWS Cloud als Erweiterung Ihres Unternehmensrechenzentrums einsetzen.
  Die Netzwerkkonfiguration für Ihre Amazon VPC kann auf einfache Weise angepasst werden. Sie können beispielsweise ein öffentlich zugängliches Subnetz für Ihre Webserver einrichten, das Zugriff auf das Internet hat, und Ihre Backend-Systeme, etwa Datenbanken oder Anwendungsserver, in einem privaten Subnetz ohne Internetzugang betreiben. Sie können mehrere Sicherheitsebenen einrichten, darunter Sicherheitsgruppen und Netzwerk-Zugriffskontrolllisten, die den Zugriff auf Amazon EC2-Instances in den einzelnen Subnetzen steuern.

- **Dedizierte HSM-Module in der Cloud mit CloudHSM –** Der AWS CloudHSM-Service unterstützt Sie mithilfe dedizierter Hardware-Sicherheitsmodul-Appliances (HSM) bei der Einhaltung gesetzlicher, regulatorischer und vertraglicher Vorschriften für die Datensicherheit in der AWS-Cloud. Mit CloudHSM können Sie die Verschlüsselungsschlüssel und die vom HSM durchgeführten kryptografischen Vorgänge steuern.
  AWS und AWS Marketplace-Partner bieten eine Vielzahl von Lösungen zum Schutz sensibler Daten auf der AWS-Plattform. Doch für Anwendungen und

Daten, die strengen vertraglichen oder regulatorischen Vorschriften für die Verwaltung kryptografischer Schlüssel unterliegen, ist mitunter zusätzlicher Schutz erforderlich. Bislang war Ihre einzige Option das Speichern der sensiblen Daten (bzw. der Verschlüsselungsschlüssel zum Schutz der sensiblen Daten) in Ihren lokalen Rechenzentren. Dies verhinderte leider entweder das Migrieren dieser Anwendungen in die Cloud oder führte zum starken Performance-Einbußen. Der AWS CloudHSM-Service ermöglicht Ihnen das Schützen Ihrer Verschlüsselungsschlüssel in HSMs, die zur sicheren Schlüsselverwaltung entwickelt und bestätigt wurden, um gesetzlichen Standards zu entsprechen. Sie können die zur Verschlüsselung von Daten verwendeten kryptografischen Schlüssel sicher so erstellen, speichern und verwalten, dass nur Sie Zugriff darauf haben. AWS CloudHSM unterstützt Sie beim Einhalten strenger Vorschriften für die Schlüsselverwaltung, ohne die Anwendungsleistung zu beeinträchtigen.
Der AWS CloudHSM-Service funktioniert in Amazon Virtual Private Cloud (VPC). CloudHSM-Instances werden in Ihrer VPC mit einer von Ihnen angegebenen IP-Adresse bereitgestellt und ermöglichen eine einfache und private Netzwerkanbindung an Ihre Amazon Elastic Compute Cloud (EC2)-Instances. Durch Platzieren von CloudHSM-Instances in der Nähe Ihrer EC2-Instances verkürzen Sie die Netzwerklatenz, wodurch sich die Anwendungsleistung verbessern lässt. AWS bietet einen dedizierten und exklusiven (Einzelmandanten-) Zugriff auf CloudHSM-Instances, der von anderen AWS-Kunden isoliert ist. AWS CloudHSM ist in mehreren Regionen und Availability Zones (AZs) verfügbar und ermöglicht Ihnen das Hinzufügen eines sicheren und dauerhaften Schlüsselspeichers für Ihre Anwendungen.

- **Integriert –** Sie können CloudHSM mit Amazon Redshift, Amazon Relational Database Service (RDS) for Oracle oder Anwendungen anderer Anbieter wie SafeNet Virtual KeySecure als Vertrauensanker (Root of Trust), Apache (SSL-Terminierung) oder Microsoft SQL Server (transparente Datenverschlüsselung) nutzen. Sie können auch CloudHSM verwenden, wenn Sie eigene Anwendungen schreiben, und die standardmäßigen kryptografischen Bibliotheken wie PKCS#11, Java JCA/JCE und Microsoft CAPI und CNG, mit denen Sie vertraut sind, weiterverwenden.
- **Auditierbar –** Wenn Sie aus Sicherheits- oder Compliance-Gründen Ressourcenänderungen nachverfolgen oder Aktivitäten überwachen müssen, können Sie über CloudTrail alle Aufrufe der CloudHSM-API überprüfen, die in Ihrem Konto erfolgt sind. Darüber hinaus können Sie Vorgänge auf der HSM-Appliance mithilfe von SYSLOG überwachen oder SYSLOG-Protokollmeldungen an Ihren eigenen Collector senden.

Striktes Compliance-Framework und hohe Sicherheitsstandards

Gemäß DSGVO müssen angemessene technische und organisatorische Maßnahmen gewährleisten, "die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Beständigkeit der Verarbeitungssysteme und -services auf Dauer sicherzustellen". Gleichzeitig müssen Wiederherstellungen, Prüfungen und generelle Risikomanagement-Verfahren möglich sein. AWS bietet Ihnen ein leistungsfähiges Compliance-Framework unter Wahrung moderner Sicherheitsstandards.

Modell der gemeinsamen Verantwortung für die Sicherheit

Bevor wir ausführlicher darauf eingehen, wie AWS Ihre Daten schützt, sollte angemerkt werden, wie sich Sicherheit in der Cloud von der Sicherheit Ihrer Rechenzentren vor Ort unterscheidet. Wenn Sie Computersysteme und Daten in die Cloud umziehen, teilen Sie sich die Verantwortung für Sicherheit mit Ihrem Cloud-Dienstanbieter. In diesem Fall ist AWS für den Schutz der zugrunde liegenden Infrastruktur zuständig, die die Cloudumgebung ermöglicht, und Sie sind für alles verantwortlich, was Sie in die Cloud stellen oder mit der Cloud verbinden. Dieses Modell der gemeinsamen Verantwortung für die Sicherheit kann Ihren Betriebsaufwand in vielerlei Hinsicht reduzieren und in einigen Fällen sogar Ihre Standard-Sicherheitsposition verbessern, ohne dass Sie zusätzliche Maßnahmen ergreifen müssen.

Verantwortlichkeiten von AWS für die Sicherheit

Amazon Web Services ist für den Schutz der globalen Infrastruktur verantwortlich, auf der alle in der AWS-Cloud angebotenen Services betrieben werden. Diese Infrastruktur umfasst die Hardware, Software, Netzwerke und Einrichtungen, in bzw. auf denen AWS-Services ausgeführt werden. Der Schutz dieser Infrastruktur hat bei AWS höchste Priorität. Es ist zwar nicht möglich, dass Sie unsere Rechenzentren oder Standorte besuchen, um sich persönlich von diesem Schutz zu überzeugen, wir stellen aber mehrere Berichte von Drittprüfern zur Verfügung, die untersucht haben, inwieweit wir verschiedene Standards und Vorschriften zur Computersicherheit erfüllen (weitere Informationen siehe aws.amazon.com/compliance). Neben dem Schutz dieser globalen Infrastruktur fällt in den Verantwortungsbereich von AWS auch die Sicherheitskonfiguration seiner Produkte, der verwalteten Services. Beispiele für diese Arten von Services sind Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce und Amazon WorkSpaces. Diese Services bieten die Skalierbarkeit und Flexibilität cloudbasierter Ressourcen mit dem zusätzlichen Vorteil, dass sie qualifiziert verwaltet werden. Für diese Services übernimmt AWS grundlegende Sicherheitsaufgaben wie das Patching von Gastbetriebssystemen und Datenbanken, die Firewall-Konfiguration sowie die Notfallwiederherstellung. Für die meisten dieser verwalteten Services müssen Sie lediglich logische Zugriffskontrollen für die Ressourcen konfigurieren und die Anmeldeinformationen für Ihre Konten schützen. Einige Services erfordern unter Umständen die Durchführung weiterer Aufgaben, z. B. die Einrichtung von

Benutzerkonten für Datenbanken. Im Allgemeinen wird aber die Sicherheitskonfiguration durch den Service durchgeführt.

Verantwortlichkeiten der Kunden für die Sicherheit

Mit der AWS-Cloud können Sie virtuelle Server, Speicher, Datenbanken und Desktops innerhalb von Minuten anstatt Wochen bereitstellen. Sie können auch cloud-basierte Analyse- und Workflow-Tools verwenden, um Daten nach Bedarf zu verarbeiten und sie dann in Ihren eigenen Rechenzentren oder in der Cloud zu speichern. Der Umfang des Konfigurationsaufwands im Rahmen Ihrer Zuständigkeiten für Sicherheit hängt von den AWS-Services ab, die Sie verwenden.

AWS-Produkte, die in die sehr verbreitete Kategorie "Infrastructure as a Service (IaaS)" fallen – wie Amazon EC2, Amazon VPC und Amazon S3 – stehen vollständig unter Ihrer Kontrolle. Für diese müssen Sie alle erforderlichen Aufgaben im Zusammenhang mit der Sicherheitskonfiguration und -verwaltung selbst durchführen. Bei EC2-Instances sind Sie zum Beispiel verantwortlich für die Verwaltung des Gastbetriebssystems (einschließlich Updates und Sicherheits-Patches), für die auf diesen Instances installierten Anwendungen oder Dienstprogrammen sowie auf jeder Instance für die Konfiguration der von AWS bereitgestellten Firewall (bezeichnet als "Sicherheitsgruppe"). Dies sind im Grunde genommen die gleichen Sicherheitsaufgaben, die Sie seit jeher ausführen, unabhängig vom Standort Ihrer Server.

AWS Managed Services wie Amazon Relational Database Service (RDS) oder Amazon Redshift bieten alle Funktionen, die Sie benötigen, um eine bestimmte Aufgabe zu erledigen – nur ohne den zugehörigen Konfigurationsaufwand. Bei verwalteten Services müssen Sie sich nicht um das Starten und Warten von Instances, das Patchen von Gastbetriebssystemen oder Datenbanken oder das Replizieren von Datenbanken kümmern, denn dies wird von AWS für Sie erledigt. Wie bei allen Services sollten Sie jedoch die Anmeldedaten für Ihr AWS-Konto schützen und individuelle Benutzerkonten mit Amazon Identity and Access Management (IAM) einrichten, damit alle Benutzer über eigene Anmeldedaten verfügen und Sie eine Aufgabentrennung sicherstellen können. Darüber hinaus empfehlen wir für jedes Konto die Verwendung einer Multi-Factor Authentication (MFA). Diese setzt den Einsatz von SSL/TLS für die Kommunikation mit Ihren AWS-Ressourcen sowie die Einrichtung der Protokollierung der API-/Benutzeraktivitäten mit AWS CloudTrail voraus. Weitere Informationen zu zusätzlichen Maßnahmen, die Sie treffen können, finden Sie im Whitepaper AWS Security Best Practices und in den folgenden Literaturempfehlungen auf der Website zu AWS-Sicherheitsressourcen.

AWS-Compliance-Programm

Amazon Web Services Compliance ermöglicht AWS-Kunden, sich mit den zuverlässigen Kontrollmöglichkeiten in AWS vertraut zu machen, die der Sicherheit und dem Datenschutz in der Cloud dienen. Da die Systeme auf der AWS Cloud-Infrastruktur aufbauen, werden Compliance-Verantwortlichkeiten geteilt. Da die Systeme auf der AWS Cloud-Infrastruktur aufbauen, werden Compliance-Verantwortlichkeiten geteilt. Durch die Kombination Governance-zentrierter, auf einfache Prüfung ausgelegter Servicefunktionen mit den geltenden Compliance- oder Prüfungsstandards bauen die AWS Compliance-Assistenten auf herkömmlichen Programmen auf. Sie unterstützen Kunden bei der

Erstellung einer AWS-Sicherheitskontrollumgebung und deren Betrieb. Die IT-Infrastruktur, die AWS für Kunden bereitstellt, wird gemäß der bewährten Methoden für die Sicherheit und einer Reihe von IT-Sicherheitsstandards entwickelt und verwaltet. Dazu gehören:

- C5 (der Cloud Computing Compliance Control Catalogue des BSI), SOC 1/SSAE 16/ISAE 3402 (zuvor SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP und FedRAMP
- DoD SRG
- PCI DSS Stufe 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Tier 3

Außerdem können Kunden aufgrund der Flexibilität und Kontrollfunktion der AWS-Plattform Lösungen bereitstellen, die eine Reihe von branchenspezifischen Standards erfüllen. Dazu gehören:

- Criminal Justice Information Services (CJIS)
- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Motion Picture Association of America (MPAA)

AWS bietet Kunden bezüglich der IT-Kontrollumgebung umfangreiche Informationen in Form von Whitepapers, Berichten, Zertifizierungen, Akkreditierungen und weiteren Bescheinigungen Dritter. Weitere Informationen finden Sie im Whitepaper Risiko und Compliance.

Anforderungskatalog Cloud Computing (C5 – ein vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickeltes Prüfungsschema)

Der Anforderungskatalog Cloud Computing (C5) ist ein Prüfungsschema, das in Deutschland durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet wurde. Anhand dieses Prüfungsschemas stellen Cloud-Anbieter abgeleitet aus dem Eckpunktepapier "Sicherheitsempfehlungen für Cloud Computing-Anbieter" des BSI ihre operative Sicherheit unter Beweis.

Das C5-Prüfungsschema kann von AWS-Kunden und deren Compliance-Beratern verwendet werden, um den Umfang der AWS-Sicherheitsmaßnahmen sowie der von AWS zur Verfügung gestellten IT-Sicherheitsservices zu verstehen. C5 baut auf dem IT-Grundschutz nach ISO 27001 auf und stellt ein vergleichbares IT-Sicherheitsäquivalent mit zusätzlichen Cloud-spezifischen Kontrollfunktionen dar.

C5 bietet zusätzliche Kontrollfunktionen, die Informationen zum Datenspeicherort, der Servicebereitstellung, dem Gerichtsstand, den existierenden Zertifizierungen, den Offenlegungsverpflichtungen von Informationen und eine ausführliche Beschreibung der Services enthalten. Mittels dieser Informationen können Kunden bewerten, wie

rechtlichen Vorgaben (z. B. zum Datenschutz), ihren eigenen Richtlinien oder dem Bedrohungsumfeld im Rahmen der Nutzung der AWS Cloud Computing-Services entsprochen werden kann.

Dokumentversionen

Datum	Beschreibung
September 2018	Kleinere Updates
November 2017	Erstveröffentlichung