DSGVO-Compliance in AWS

November 2017

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 gehört, weder ganz noch teilweise, nicht zu den Vereinbarungen von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Inhalt

Übersicht

Die Datenschutz-Grundverordnung (DSGVO) tritt am 25.05.2018 in Kraft. AWS stellt Ihnen Dienste und Ressourcen zur Verfügung, die Ihnen die Erfüllung der DSGVO-Vorgaben erleichtern sollen, die ggf. für Ihren Betrieb zutreffen. Dies beinhaltet die Erfüllung des CISPE-Verhaltenskodex durch AWS, granulare Zugangskontrollen, Protokollierungs- und Überwachungstools, Verschlüsselung, Schlüsselverwaltung, Prüfungskapazitäten, Compliance mit IT-Sicherheitsstandards und die C5-Zertifikate von AWS.

Die Datenschutz-Grundverordnung Ein Überblick

Die Datenschutz-Grundverordnung (DSGVO) ist ein neues europäisches Datenschutzgesetz, das am 25. Mai 2018 in Kraft tritt. Die DSGVO soll innerhalb der EU geltende Datenschutzgesetze harmonisieren, 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, wenn sie die „personenbezogenen Daten“ von EU-Angehörigen 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.

Die Datenschutz-Grundverordnung ersetzt die bestehende Datenschutzrichtlinie der EU (Verordnung 95/46/EG). Ab dem 25. Mai 2018 sind diese Datenschutzrichtlinie und alle Gesetze, die sich auf sie beziehen, nicht mehr gültig.

Änderungen im Rahmen der Einführung der Datenschutz-Grundverordnung (DSGVO) für in Europa tätige Organisationen

Einer der wichtigsten Aspekte der Datenschutz-Grundverordnung ist die Harmonisierung des Vorgangs zur Verarbeitung, Verwendung und des sicheren Austauschs von personenbezogenen Daten zwischen EU-Mitgliedsstaaten. Organisationen müssen die Sicherheit der verarbeiteten Daten sowie ihre Compliance mit der Datenschutz-Grundverordnung kontinuierlich nachweisen. Dazu sind die Implementierung und regelmäßige Prüfung nachhaltiger technischer und organisatorischer Maßnahmen sowie Compliance-Richtlinien erforderlich. Aufsichtsbehörden werden Strafen von bis zu 20 Mio. EUR oder 4 % des jährlichen – weltweiten – Umsatzes (je nachdem was höher ausfällt) verordnen können.

Wie bereitet sich AWS auf die DSGVO vor?

Unsere Experten zur Richtlinien-Compliance, zum Datenschutz und für die Sicherheit haben bereits die Fragen vieler internationaler Kunden beantwortet und sie dahingehend beraten, was beim Ausführen von Rechenprozessen in der Cloud nach Inkrafttreten der Datenschutz-Verordnung zu beachten ist. Es sind bereits sämtliche bisherigen Aktivitäten von AWS geprüft worden, um sicherzustellen, dass die neue Datenschutz-Grundverordnung eingehalten wird.

> Wir können bestätigen, dass alle AWS-Dienste im Einklang mit der DSGVO stehen, wenn diese im Mai 2018 rechtskräftig wird.

Gemäß Art. 32 sind Verantwortliche und Auftragsverarbeiter verpflichtet, „geeignete technische und organisatorische Maßnahmen“ umzusetzen, und zwar „[u]nter 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 von möglicherweise erforderlichen Sicherheitsmaßnahmen, nämlich 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 physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

CISPE-Verhaltenskodex

Die DSGVO findet für die Zulassung von Verhaltenskodizes Anwendung, um Verantwortliche und Bearbeiter darin zu unterstützen, im Sinne der Compliance und bewährter Vorgehensweisen zu handeln. Einer solcher Kodizes, dessen Zulassung noch aussteht, ist der CISPE (Code of Conduct for Cloud Infrastructure Service Providers – Verhaltenskodex für Anbieter von Cloud-Infrastrukturdiensten (im Folgenden: der „Verhaltenskodex“)). Der Code vermittelt Kunden die Rückversicherung, dass ihr Cloud-Anbieter die angemessenen Datenschutzstandards befolgt, die im Einklang mit der DSGVO stehen.

Zu den wichtigsten Vorteilen dieser Verhaltensregeln gehören:

- **Es wird festgelegt, wer im Bereich des Datenschutzes für welche Aufgaben zuständig ist.** Im Verhaltenskodex werden die Rollen von Anbieter und Kunden gemäß der Datenschutz-Grundverordnung festgelegt, 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 Compliance- und Datenschutzstrategien auf diese verbindlichen Zusagen verlassen.
- **Die Kunden erhalten mit dem Verhaltenskodex die Sicherheitsinformationen, die sie für Compliance-Entscheidungen 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 Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), AWS Identity and Access

Management (IAM), AWS CloudTrail, und Amazon Elastic Block Store (Amazon EBS) alle Punkte in diesem Kodex erfüllen (s. https://cispe.cloud/publicregister). Dies gibt unseren Kunden die zusätzliche Gewissheit, dass sie im sicheren, geschützten und richtlinienkonformen Umfeld von AWS die vollständige Kontrolle über ihre Daten haben. Wir verhalten uns nicht nur im Einklang mit dem o. g. Kodex, sondern besitzen auch verschiedene international anerkannte Zertifikate und Akkreditierungen, darunter ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2, SOC 3 und PCI DSS Level 1.

Datenzugriffskontrollen

Art. 25 der DSGVO schreibt vor, der „Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden“. Die im Folgenden benannten Zugriffskontrollmechanismen von AWS helfen Ihnen, diese Vorgaben zu erfüllen, indem sie nur autorisierten Administratoren, Benutzern und Apps den Zugriff auf die AWS-Ressourcen und -Kundendaten gewähren:

- **Feingranulare Zugriffskontrolle auf AWS-Objekte in S3-Buckets/SQS/SNS und anderen –** Sie können jeder Person einen anderen Zugriff auf unterschiedliche Ressourcen gewähren. Z. B. können Sie bestimmten Benutzern vollständigen Zugriff auf Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift und andere AWS-Dienste gewähren. Anderen Benutzern können Sie schreibgeschützten Zugriff auf nur einige S3-Buckets oder den aktiven Verwaltungszugriff auf nur einige EC2-Instances oder nur und ausschließlich einen Zugriff auf Ihre Rechnungsdaten gewähren.
- **Multi-Factor-Authentication (MFA) –** Sie können als zusätzliche Sicherheitsmaßnahme Ihrem Konto sowie bestimmten Benutzern eine Zwei-Faktor-Authentifizierung zuordnen. Hierbei geben Sie (bzw. die Benutzer) zum Zugriff auf Ihr Konto nicht nur ein Passwort oder einen Zugangsschlüssel ein, sondern auch einen Code, der an ein eigens dafür konfiguriertes Gerät gesandt wird.
- **API-Anforderungs-Authentifizierung –** Sie können IAM-Funktionen einsetzen, um Anmeldedaten betriebssicher in Apps (die auf EC2-Instances ausgeführt werden) eingeben zu können, die für deren

Zugriff auf andere AWS-Ressourcen, wie z. B. S3-Buckets, RDS oder DynamoDB-Datenbanken, erforderlich sind.

- **Geografische Einschränkungen –** Sie können durch die Technik des sogenannten „Geoblocking“ Benutzern den Zugriff verwehren, die sich außerhalb der von Ihnen festgelegten geografischen Standorte befinden. Dies erfolgt durch eine CloudFront-Webdistribution. Dies wird durch zwei Optionen ermöglicht:
    - **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 schränken Sie den Zugriff auf Teilsätze der Daten mit Distributionsmerkmalen oder auf eine spezifischere Ebene als die Länderebene ein.
- **Token für den vorübergehenden Zugriff (über STS) –** Der AWS Security Token Service (AWS STS) ermöglicht es Ihnen, vertrauenswürdigen Benutzern vorübergehende, gesicherte Zugangsdaten zuzuordnen, mit denen ein kontrollierter Zugriff auf Ihre AWS-Ressourcen erfolgt. Vorübergehende Zugangsdaten verhalten sich zu langfristig gültigen Zugangsdaten (Ihrer IAM-Benutzer) nahezu identisch. Folgende Unterschiede bestehen:
    - **Vorübergehende, 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.
    - **Vorübergehende Zugangsdaten werden nicht in Zusammenhang mit dem Benutzer gespeichert, sondern werden dynamisch generiert und dem Benutzer auf Abfrage bereitgestellt.** Vor dem Gültigkeitsablauf der vorübergehenden Zugangsdaten kann ein Benutzer bei entsprechenden Rechten neue Zugangsdaten anfordern.

  Somit haben vorübergehende 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-Identität zuordnen zu müssen. Vorübergehende Anmeldedaten bilden die Basis für Rollen und das föderierte Identitätsmanagement.
- 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 die Gültigkeitsfrist im Rahmen eines maximalen Zeitraums definieren.

Überwachung und Protokollierung

Die DSGV schreibt vor: „ Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen“. In diesem Artikel werden die aufzuzeichnenden Details aufgeführt. Die GDPR fordert somit die Überwachung der Verarbeitung von PII-Daten. Zusätzlich erfordern es die Anzeigepflichten in Bezug auf die zeitnahe Benachrichtigung über Datenpannen, dass entsprechende Vorfälle nahezu in Echtzeit erkannt werden. Damit Sie diese Auflagen erfüllen können, bietet Ihnen AWS verschiedene Überwachungs- und Protokollierungsdienste an:

- **Asset-Management und -Konfiguration mit AWS Config** – Über AWS Config erhalten Sie eine detaillierten Ansicht der Konfiguration der AWS-Ressourcen in Ihrem AWS-Konto. Dies umfasst u. a. Informationen über die Ressourcenverknüpfung und über ihre bisherige Konfiguration, sodass Sie die im Laufe der Zeit erfolgten Änderungen der Konfigurationen und Verknüpfungen/Beziehungen nachvollziehen können.

  Bei AWS-Ressourcen handelt es sich um bestimmte Einheiten, mit denen Sie im Rahmen von AWS arbeiten können, nämlich 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 hier: 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, Änderung oder Löschung von Ressourcen benachrichtigt werden.
- Sie können die Beziehungen verschiedener Ressourcen abfragen. Beispielsweise wollen Sie möglicherweise alle Ressourcen derselben Sicherheitsgruppe abfragen.

- **Compliance-Prüfungen und Sicherheitsanalysen mit AWS CloudTrail** – Mit AWS CloudTrail können Sie Ihre AWS-Bereitstellungen in der Cloud überwachen, indem Sie einen Verlauf der AWS API-Aufrufe für Ihr Konto abrufen (z. B. der API-Aufrufe über die AWS Management Console, die AWS SDKs, die Befehlszeilen-Tools und AWS-Dienste auf einer höheren Ebene). Sie können außerdem identifizieren, welche Benutzer und Konten AWS-APIs für Services, die CloudTrail unterstützen, aufgerufen haben, die Quell-IP-Adresse, von der die Aufrufe ausgingen, und wann die Aufrufe aufgetreten sind. Sie können CloudTrail mithilfe der API in Anwendungen integrieren, können die Trail-Erstellung für Ihr Unternehmen automatisieren, können Sie Trail-Status überprüfen und steuern, wie Administratoren die CloudTrail-Anmeldung ein- und ausschalten.
- **Identifikation der Konfigurationsherausforderungen durch TrustedAdvisor –** Durch die Protokollierung können Sie detaillierte Zugriffsprotokolle abrufen, die an ein S3-Bucket geliefert werden. Ein Zugriffsprotokoll-Datensatz enthält Details über jede Anfrage, wie beispielsweise den Anfragetyp die in der Anfrage angeforderten Ressourcen sowie Uhrzeit und Datum der Anfrage. Weitere Informationen über die Inhalte eines Protokolls finden Sie im Abschnitt

„Server Access Log – Log-Format“[1] im Entwicklerhandbuch zu Amazon Simple Storage Service.

- Serverzugriffsprotokolle sind für viele Anwendungen nützlich, da sie Bucket-Eigentümern Einblick in die Art der Anfragen bieten, die von Clients erstellt werden, die sich ihrer Kontrolle entziehen. Standardmäßig erfasst Amazon S3 keine Dienstzugriffsprotokolle. Wenn Sie die Protokollierung jedoch aktivieren, liefert Amazon S3 stündlich Zugriffsprotokolle an Ihr Bucket.
- Individuell festgelegte 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 im AWS-System

Die DSGV fordert, „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: [...] die Pseudonymisierung und Verschlüsselung personenbezogener Daten [...]“ Zusätzlich müssen sich Organisationen gegen die unbefugte Offenlegung von bzw. den unbefugten Zugriff auf personenbezogene Daten absichern. Ist die Sicherheit personenbezogener Daten verletzt worden und wirkt sich dies aller Wahrscheinlichkeit nach negativ auf die Rechte und Freiheiten natürlicher Personen aus, obwohl der Verantwortliche „angemessene technische und organisatorische Schutzmaßnahmen (...), z. B. Verschlüsselung“ einsetzte, ist er nicht verpflichtet, die betroffenen Datensubjekte über diesen Vorgang zu unterrichten und kann somit Verwaltungskosten und Reputationsschäden vermeiden. AWS bietet verschiedene, hochskalierbare und sichere Datenverschlüsselungsmechanismen zum Schutz von auf AWS gespeicherten und bearbeiteten Kundendaten an.

- **Verschlüsselung ruhender Daten mit AES256 (EBS/S3/Glacier/RDS) –** Die Verschlüsselung ruhender Daten [2] ist für die Erfüllung gesetzlicher Vorgaben entscheidend; es soll

gewährleistet werden, dass sensible, auf Datenträgern gespeicherte Daten nicht durch Benutzer oder Anwendungen ohne gültige Zugangsschlüssel erfasst werden können. AWS stellt Optionen für ruhende Daten und für die Verwaltung von Zugangsschlüsseln zur Verfügung, um das Verschlüsselungsverfahren zu unterstützen. 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.

- **Verschlüsselung von Datenträgern und Dateien** – Es bestehen zwei Methoden zur Verschlüsselung von Dateien auf Instance-Speichern. Die erste Methode besteht in der Verschlüsselung des Datenträgers, wobei der gesamte Datenträger oder der Block auf dem Datenträger durch mindestens einen Zugangsschlüssel verschlüsselt wird. Diese Methode wirkt unterhalb der Dateisystemebene, funktioniert betriebssystemübergreifend und verbirgt Verzeichnis- und Dateiinformationen wie z. B. 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.

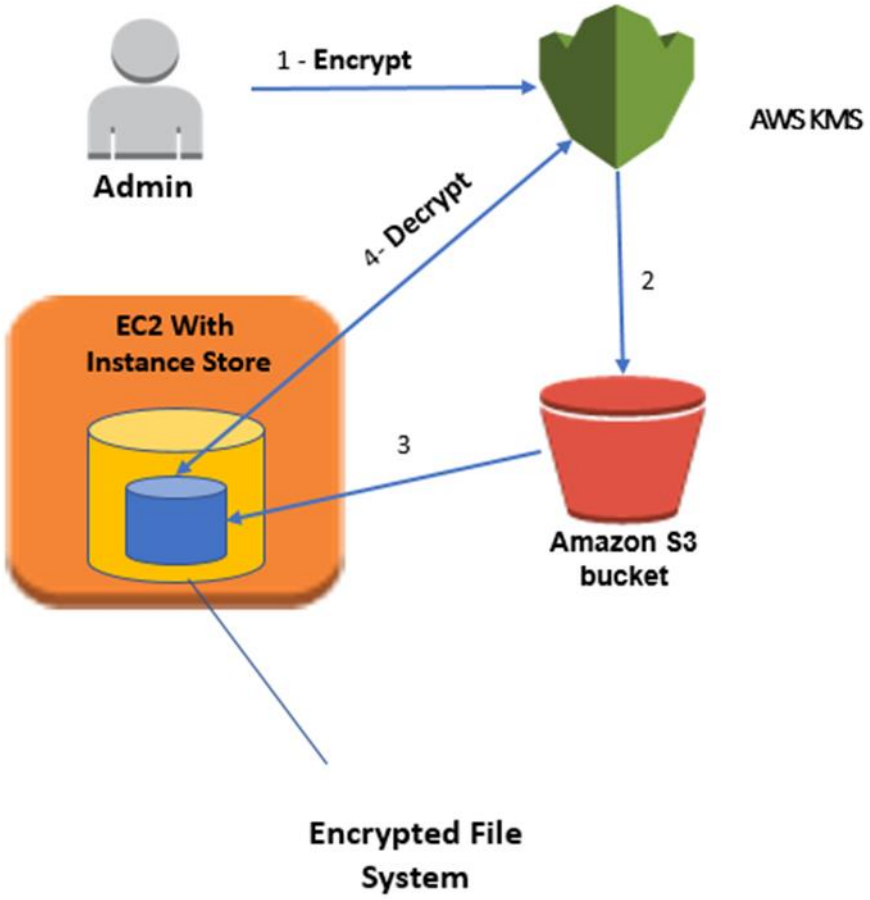
  Die zweite Methode besteht in der Verschlüsselung auf Dateisystemebene. Es werden Dateien und Verzeichnisse verschlüsselt, jedoch nicht der gesamte Datenträger bzw. die gesamte Partition. Die Verschlüsselung auf Dateisystemebene ist dem Dateisystem übergeordnet und somit auf verschiedene Betriebssysteme übertragbar.

- **Die Linux dm-crypt-Infrastruktur** – 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 jedoch 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.

- **Architektonischer Überblick** – Das folgende allgemeine architektonische Diagramm veranschaulicht das Konzept, mit dem EC2-Instances verschlüsselt werden können.



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 Gebiet) 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 bei mehreren anderen 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 Art Schlüssel erstellen, importieren und rotieren sowie Verwendungsrichtlinien und Audit-Nutzung aus der AWS Management Console oder mithilfe von AWS SDK oder 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 Infrastruktur für die Schlüsselverwaltung importieren und in KMS verwenden.
    - AWS-Service-Integration **– AWS Key Management Service ist nahtlos integriert in mehrere andere AWS-Services.** 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 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 Infrastruktur für die Schlüsselverwaltung importiert haben und zu dessen Verwendung Sie berechtigt sind.

- **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 das von Ihnen bei der Aktivierung von AWS CloudTrail festgelegte Amazon S3-Bucket geliefert wird.[3] Die aufgezeichneten Informationen enthalten Details zu Benutzer, Zeit, Datum und verwendetem Schlüssel.
- **Skalierbarkeit, Belastbarkeit und hohe Verfügbarkeit** – AWS Key Management ist ein verwalteter Dienst. Bei zunehmender Nutzung von AWS KMS-Verschlüsselungsschlüsseln müssen Sie keine zusätzliche Infrastruktur für die Schlüsselverwaltung kaufen. 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 Schlüssel nach KMS importieren, müssen Sie eine Kopie Ihrer Schlüssel sicher aufbewahren, sodass Sie sie jederzeit neu importieren können.

  AWS KMS wird in mehreren Availability Zones in einer AWS-Region bereitgestellt, um hohe Verfügbarkeit für Ihre Verschlüsselungsschlüssel zu bieten.
- Sicherheit – **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 in Amazon überwacht und geprüft wird.

Weitere Informationen über die Funktionsweise von AWS KMS finden Sie im Whitepaper zum AWS Key Management Service[4].

- **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 Virtual Private Network (VPN)-Verbindung 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, wie 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-(HSM-)Appliances beim Einhalten gesetzlicher, regulatorischer und vertraglicher Vorschriften für die Datensicherheit in der AWS Cloud.** Mit CloudHSM können Sie die Verschlüsselungsschlüssel und vom HSM durchgeführten kryptografischen Vorgänge kontrollieren.

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 Ausbremsen ihrer Leistung. Der AWS CloudHSM-Service ermöglicht Ihnen das Schützen Ihrer Verschlüsselungsschlüssel in HSMs, die gemäß gesetzlichen Standards zur sicheren Schlüsselverwaltung entwickelt und bestätigt wurden. 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 beständigen 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,

mit denen Sie vertraut sind, weiterverwenden, wie z. B. PKCS#11, Java JCA/JCE und Microsoft CAPI und CNG.

- **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 Ihr eigenen Sammler senden.

Striktes Compliance-Framework und hohe Sicherheitsstandards

Gemäß DSGVO müssen technische und organisatorische Maßnahmen es gewährleisten, „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;“. Gleichzeitig müssen Wiederherstellungen, Prüfungen und generelle Risikomanagement-Verfahren möglich sein. AWS bietet Ihnen ein leistungsfähiges Compliance-Framework unter Wahrung moderner Sicherheitsstandards.

Das Modell der geteilten Verantwortung für Sicherheit von AWS

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 geteilten Verantwortung für Sicherheit kann den Betriebsaufwand für Sie in vielerlei Hinsicht reduzieren. In manchen Fällen lässt sich dadurch sogar Ihre Sicherheitslage allgemein verbessern, ohne dass Sie zusätzliche Maßnahmen ergreifen müssen.

Verantwortlichkeiten von AWS für die Sicherheit

Amazon Web Services ist dafür verantwortlich, die globale Infrastruktur zu schützen, 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 finden Sie unter http://aws.amazon.com/compliance/.

Beachten Sie, dass AWS zusätzlich zum Schutz dieser globalen Infrastruktur auch für die Sicherheitskonfiguration seiner Produkte, der verwalteten Services, verantwortlich ist. Beispiele für diese Arten von Services sind Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, Amazon WorkSpaces und einige weitere Services. Diese Services bieten die Skalierbarkeit und Flexibilität cloudbasierter Ressourcen mit dem zusätzlichen Vorteil, dass sie 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, insgesamt wird die Sicherheitskonfiguration aber vom Service übernommen.

Verantwortlichkeiten des Kunden für die Sicherheit

Mit der AWS-Cloud können Sie virtuelle Server, Speicher, Datenbanken und Desktops innerhalb von Minuten anstatt Wochen bereitstellen. Sie haben auch die Möglichkeit, cloudbasierte Analyse- und Workflow-Tools zu nutzen, um Ihre Daten entsprechend Ihrem Bedarf zu verarbeiten, um 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 unter die hinlänglich bekannte Kategorie des Infrastructure as a Service (IaaS) fallen, z. B. Amazon EC2, Amazon VPC und Amazon S3, stehen vollkommen unter Ihrer Kontrolle. Für diese müssen Sie alle erforderlichen Aufgaben im Zusammenhang mit der Sicherheitskonfiguration und -verwaltung durchführen. Für EC2-Instances sind Sie z. B. verantwortlich für die Verwaltung des Gastbetriebssystems (einschließlich Updates und Sicherheits-Patches), für die auf diesen Instances installierten Anwendungen oder Dienstprogramme sowie für die Konfiguration der von AWS bereitgestellten Firewall (bezeichnet als "Sicherheitsgruppe") auf jeder Instance. Dies sind im Grunde genommen die gleichen Sicherheitsaufgaben, die Sie seit jeher ausführen, unabhängig vom Standort Ihrer Server.

Von AWS verwaltete Services wie Amazon RDS oder Amazon Redshift bieten alle Ressourcen, die Sie benötigen, um eine bestimmte Aufgabe zu erledigen – aber 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 müssen Sie aber die Anmeldeinformationen Ihres AWS-Kontos schützen und mit Amazon Identity and Access Management (IAM) individuelle Benutzerkonten einrichten, damit jeder Ihrer Benutzer über eigene Anmeldeinformationen verfügt und Sie eine Aufgabentrennung implementieren können. Darüber hinaus empfehlen wir für jedes Konto die Verwendung einer Multi-Factor Authentication (MFA). Dies 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 über zusätzliche Maßnahmen, die Sie treffen können, finden Sie im Whitepaper Optimale Vorgehensweisen für die AWS-Sicherheit und auf der Website zu AWS-Sicherheitsressourcen.

AWS-Compliance-Programm

Amazon Web Services Compliance ermöglicht unseren 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. 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 die Kunden beim Erstellen einer AWS-Sicherheitskontrollumgebung und deren Betrieb. Die IT-Infrastruktur, die AWS für Kunden bereitstellt, wird gemäß optimaler Vorgehensweisen für Sicherheit und einer Reihe von IT-Sicherheitsstandards entwickelt und verwaltet. Dazu gehören:

- SOC 1/SSAE 16/ISAE 3402 (zuvor SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP und FedRAMP
- DOD CSM Stufe 1 bis 5
- PCI DSS Stufe 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Stufe 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 anderen Nachweisen Dritter. Weitere Informationen finden Sie im Whitepaper „Risiko und Compliance“ unter: http://aws.amazon.com/compliance/.

Anforderungskatalog Cloud Computing (C5; von der Bundesregierung unterstütztes Zertifizierungsschema)

Der Anforderungskatalog Cloud Computing (C5)[5] ist ein regierungsgestütztes Prüfschema, das in Deutschland durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgestellt wurde. Anhand des Prüfschemas sollen Organisationen im Rahmen des Eckpunktepapiers "Sicherheitsempfehlungen für Cloud Computing Anbieter[6]" der deutschen Bundesregierung ihre operative Sicherheit gegen weit verbreitete Cyber-Angriffe unter Beweis stellen.

Das C5-Prüfschema kann von AWS-Kunden und deren Compliance-Beratern verwendet werden, um den Umfang der IT-Sicherheitsservices von AWS zu verstehen, die ihnen während der Übertragung von Arbeitslasten in die Cloud zur Verfügung stehen. C5 fügt dem IT-Grundschutz das gesetzlich festgelegte IT-Sicherheitsleveläquivalent mit zusätzlichen Cloud-spezifischen Kontrollfunktionen hinzu.

C5 bietet nun 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 rechtliche Vorgaben (z. B. zu Datenschutz), ihre eigenen Richtlinien oder das Bedrohungsumfeld ihre Cloud Computing-Services beeinflussen.

Am Dokument vorgenommene Änderungen

Datum	Beschreibung
November 2017	Erstveröffentlichung

Notes

[1] http://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html

[2] https://do.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

[3] https://aws.amazon.com/cloudtrail/

[4] https://do.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Anforderungskatalog-Cloud_Computing-C5.pdf?__blob=publicationFile&v=3

[6] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile&v=2