Einführung in die AWS-Sicherheit

Januar 2020

Hinweise

Kunden sind eigenverantwortlich für die unabhängige Bewertung der Informationen in diesem Dokument zuständig. Dieses Dokument: (a) dient rein zu Informationszwecken, (b) spiegelt die aktuellen Produktangebote und Verfahren von AWS wider, die sich ohne vorherige Mitteilung ändern können, und (c) impliziert keinerlei Verpflichtungen oder Zusicherungen seitens AWS und dessen Tochtergesellschaften, Lieferanten oder Lizenzgebern. AWS-Produkte oder -Services werden im vorliegenden Zustand und ohne ausdrückliche oder stillschweigende Gewährleistungen, Zusicherungen oder Bedingungen bereitgestellt. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden wird durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Teil der Vereinbarungen zwischen AWS und seinen Kunden und ändert diese Vereinbarungen auch nicht.

Inhalt

Überblick

Amazon Web Services (AWS) bietet eine skalierbare Cloud-Computing-Plattform für hohe Verfügbarkeit und Zuverlässigkeit. Sie finden hier Tools, um eine Vielzahl von Anwendungen auszuführen. Die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme und Daten zu schützen, hat für AWS höchste Priorität. Ebenso wichtig ist es uns, Ihr Vertrauen zu bewahren. Dieses Dokument bietet eine Einführung in das Sicherheitskonzept von AWS. Dabei werden auch die Kontrollmechanismen in der AWS-Umgebung sowie einige der Produkte und Funktionen erörtert, die AWS Kunden zur Verfügung stellt, damit diese ihre Sicherheitsziele erreichen können.

Sicherheit der AWS-Infrastruktur

Die AWS-Infrastruktur ist eine der flexibelsten und sichersten Cloud-Computing-Umgebungen, die heute verfügbar sind. Sie stellt eine hochgradig skalierbare, zuverlässige Plattform zur Verfügung, über die Kunden Anwendungen und Daten rasch und sicher bereitstellen können. Beim Aufbau und bei der Verwaltung dieser Infrastruktur werden nicht nur bewährte Sicherheitsmethoden und -standards, sondern auch die besonderen Anforderungen der Cloud berücksichtigt. AWS sorgt mithilfe von redundanten und mehrschichtigen Kontrollen, fortlaufenden Validierungen und Tests sowie einer hochgradigen Automatisierung dafür, dass die zugrunde liegende Infrastruktur rund um die Uhr überwacht und geschützt ist. Dabei stellt AWS sicher, dass diese Kontrollen in jedem neuen Rechenzentrum oder Service repliziert werden.

Alle AWS-Kunden profitieren von einer Rechenzentrums- und Netzwerkarchitektur, die eingerichtet wurde, um den Ansprüchen unserer Kunden mit höchsten Sicherheitsanforderungen gerecht zu werden. Somit erhalten Sie eine resiliente Infrastruktur, die für die höchsten Sicherheitsansprüche konzipiert ist, ohne die Kosten und den betrieblichen Aufwand eines herkömmlichen Rechenzentrums.

Bei AWS gilt ein Modell der geteilten Verantwortung für Sicherheit. Entsprechend ist AWS für die Sicherheit der zugrunde liegenden Cloud-Infrastruktur verantwortlich, während Sie für die Sicherheit der Workloads zuständig sind, die Sie in AWS bereitstellen (*Abbildung* 1). Damit erhalten Sie die notwendige Flexibilität und Agilität, um die am besten geeigneten Sicherheitskontrollen für Ihre Geschäftsfunktionen in der AWS-Umgebung implementieren zu können. Sie können den Zugriff auf Umgebungen, in denen vertrauliche Daten verarbeitet werden, stark beschränken und für Informationen, die öffentlich verfügbar sein sollen, weniger strenge Kontrollen einrichten.

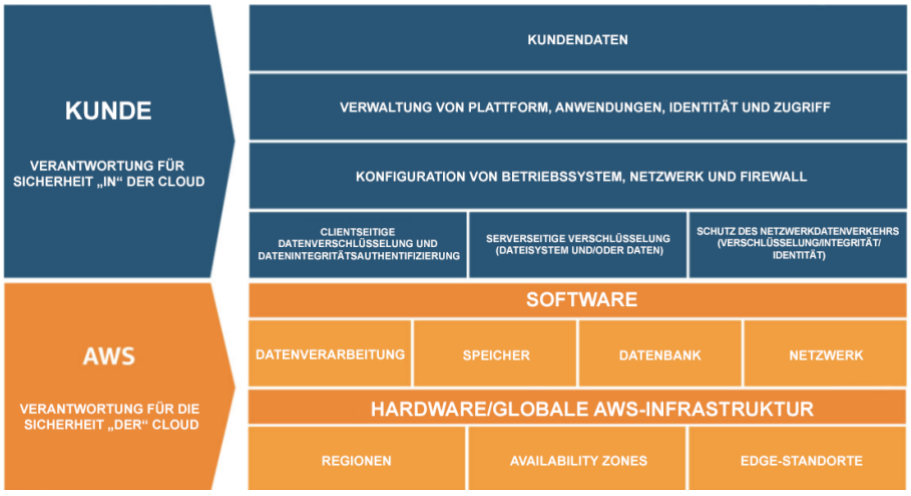

Abbildung 1: Das Modell der geteilten Verantwortung für Sicherheit von AWS

Sicherheitsprodukte und -funktionen

AWS und seine Partner bieten eine Vielzahl von Tools und Funktionen, mit deren Hilfe Sie Ihren Sicherheitsanforderungen gerecht werden. Diese Tools ähneln den vertrauten Kontrollmechanismen, die Sie in Ihren On-Premises-Umgebungen bereitstellen. AWS bietet sicherheitsspezifische Tools und Funktionen für die Netzwerksicherheit, das Konfigurationsmanagement, die Zugriffssteuerung und die Datensicherheit. Darüber hinaus stellt AWS Tools für die Überwachung und Protokollierung bereit, um Ihnen umfassende Einblicke in die Vorgänge in Ihrer Umgebung zu ermöglichen.

Sicherheit der Infrastruktur

AWS bietet mehrere Sicherheitsfunktionen und -services zur Verbesserung des Datenschutzes und zur Kontrolle des Netzwerkzugriffs. Hierzu gehören:

- Die Möglichkeit, private Netzwerke zu erstellen und den Zugriff auf Ihre Instances oder Anwendungen zu kontrollieren, dank der in die Amazon VPC integrierten Netzwerk-Firewalls; Kunden können die TLS-Verschlüsselung von Daten bei der Übertragung AWS-Service-übergreifend kontrollieren;

- Konnektivitätsoptionen, die private oder dedizierte Verbindungen von Ihrem Büro oder Ihrer On-Premises-Umgebung ermöglichen;

- Technologien zur Abmilderung von DDoS-Angriffen, die auf Ebene 3 oder 4 sowie auf Ebene 7 angewendet werden. Diese können als Teil von Strategien zur Bereitstellung von Anwendungen und Inhalten angewendet werden;

- Automatische Verschlüsselung des gesamten Datenverkehrs in den globalen und regionalen AWS-Netzwerken zwischen Einrichtungen, die von AWS gesichert werden.

Bestands- und Konfigurationsverwaltung

AWS bietet eine Vielzahl von Tools, die ein schnelles Vorgehen ermöglichen, wobei Sie gleichzeitig sicherstellen können, dass Ihre Cloud-Ressourcen den Standards und bewährten Methoden Ihres Unternehmens entsprechen. Hierzu gehören:

- Bereitstellungstools zur Verwaltung der Erstellung und Außerbetriebnahme von AWS-Ressourcen gemäß den Unternehmensstandards;

- Tools für die Bestands- und Konfigurationsverwaltung, mit deren Hilfe AWS-Ressourcen ermittelt und anschließend Änderungen an diesen Ressourcen im Laufe der Zeit verwaltet werden können;

- Tools zur Definition und Verwaltung von Vorlagen, mit denen standardmäßige, vorkonfigurierte, gehärtete virtuelle Maschinen für EC2-Instances erstellt werden können.

Datenverschlüsselung

AWS bietet Ihnen die Möglichkeit, Ihren ruhenden Daten in der Cloud eine zusätzliche Sicherheitsebene hinzuzufügen. Zu diesem Zweck werden skalierbare und effiziente Verschlüsselungsfunktionen zur Verfügung gestellt. Hierzu gehören:

- Möglichkeiten zur Verschlüsselung von ruhenden Daten in den meisten AWS-Services, wie z. B. Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon ElastiCache, AWS Lambda und Amazon SageMaker;

- Flexible Optionen für die Schlüsselverwaltung, einschließlich AWS Key Management Service, sodass Sie selbst entscheiden können, ob AWS die Verschlüsselungsschlüssel verwalten soll oder ob Sie die komplette Kontrolle über Ihre Schlüssel behalten möchten;

- Speicherung dedizierter hardwarebasierter Verschlüsselungsschlüssel unter Verwendung von AWS CloudHSM, damit Sie Ihren Compliance-Anforderungen gerecht werden;

- Warteschlangen für verschlüsselte Nachrichten für die Übertragung vertraulicher Daten unter Verwendung der serverseitigen Verschlüsselung (Server-side Encryption, SSE) für Amazon SQS.

Darüber hinaus bietet AWS APIs, damit Sie Verschlüsselung und Datenschutz in alle Services integrieren können, die Sie in einer AWS-Umgebung entwickeln oder bereitstellen.

Identitäts- und Zugriffskontrolle

AWS bietet Ihnen Möglichkeiten, Benutzerzugriffsrichtlinien für alle AWS-Services zu definieren, zu erzwingen und zu verwalten. Hierzu gehören:

- AWS Identity and Access Management (IAM) – Mit diesem Service können Sie einzelne Benutzerkonten mit Berechtigungen für mehrere AWS-Ressourcen definieren. AWS Multi-Factor Authentication für privilegierte Konten beinhaltet Optionen für software- und hardwarebasierte Authentifikatoren. Mithilfe von IAM können Sie Ihren Mitarbeitern und Anwendungen unter Verwendung Ihrer bestehenden Identitätssysteme wie Microsoft Active Directory oder anderer Angebote von Partnern Verbundzugriff auf die AWS-Managementkonsole und die AWS-Service-APIs gewähren.

- AWS Directory Service – Dieser Service ermöglicht Ihnen eine Integration und einen Verbund mit Unternehmensverzeichnissen, um den Verwaltungsaufwand zu verringern und eine bessere Erfahrung für die Endbenutzer zu bieten.

- AWS Single Sign-On (AWS SSO) – Dieser Service ermöglicht die zentrale Verwaltung des SSO-Zugriffs und der Benutzerberechtigungen für alle Ihre Konten in AWS Organizations.

AWS bietet eine native Integration von Identity and Access Management für viele AWS-Services sowie eine API-Integration in Ihre eigenen Anwendungen oder Services.

Überwachung und Protokollierung

AWS bietet Tools und Funktionen, die Ihnen einen Einblick in die Vorgänge in Ihrer AWS-Umgebung ermöglichen. Hierzu gehören:

- AWS CloudTrail – Mit diesem Service können Sie Ihre AWS-Bereitstellungen in der Cloud anhand eines Protokolls der AWS-API-Aufrufe für Ihr Konto überwachen. Dabei werden auch die API-Aufrufe über die AWS-Managementkonsole, die AWS-SDKs, die Befehlszeilen-Tools und AWS-Services einer höheren Ebene berücksichtigt. Außerdem können Sie erkennen, welche Benutzer und Konten AWS-APIs für Services, die CloudTrail unterstützen, aufgerufen haben. Sie sehen, von welcher Quell-IP-Adresse die Aufrufe ausgingen und wann die Aufrufe stattgefunden haben.

- Amazon CloudWatch – Dieser Service bietet eine zuverlässige, skalierbare und flexible Überwachungslösung, die innerhalb weniger Minuten einsatzbereit ist. Sie müssen keine eigenen Überwachungssysteme und -infrastrukturen mehr einrichten, verwalten und skalieren.

- Amazon GuardDuty – ein Service zur Bedrohungserkennung, der Ihre AWS-Konten und -Workloads fortlaufend auf böswillige oder unbefugte Verhaltensweisen überwacht und so schützt. Amazon GuardDuty stellt über Amazon CloudWatch Benachrichtigungen bereit. Sie können dann eine automatisierte Antwort auslösen oder jemanden über den Vorfall informieren.

Diese Tools und Funktionen bieten Ihnen die notwendige Transparenz, um Probleme zu erkennen, bevor sich diese auf Ihre Geschäfte auswirken. Auf diese Weise können Sie Ihre Sicherheitslage und das Risikoprofil Ihrer Umgebung verbessern.

Sicherheitsprodukte in AWS Marketplace

Durch die Verlagerung ihrer Produktions-Workloads zu AWS können Unternehmen Verbesserungen in puncto Agilität, Skalierbarkeit, Innovation und Kosteneinsparungen erzielen und dabei gleichzeitig die Sicherheit der Umgebung aufrechterhalten. AWS Marketplace bietet branchenführende Sicherheitsprodukte an, die mit vorhandenen Kontrollen in Ihren On-Premises-Umgebungen gleichwertig oder identisch sind oder sich in diese integrieren lassen. Diese Produkte ergänzen die vorhandenen AWS-Services, sodass Sie eine umfassende Sicherheitsarchitektur bereitstellen und eine nahtlosere Erfahrung in Ihrer Cloud und Ihren On-Premises-Umgebungen ermöglichen können.

Sicherheitsberatung

AWS stellt seinen Kunden Beratung und Know-how in Form von Online-Tools, Ressourcen, Support und professionellen Services von AWS und seinen Partnern zur Verfügung.

AWS Trusted Advisor ist ein Online-Tool, das die Funktion eines individuellen Cloud-Experten übernimmt und Ihnen hilft, Ihre Ressourcen den bewährten Methoden entsprechend zu konfigurieren. Trusted Advisor überprüft Ihre AWS-Umgebung, um Ihnen zu helfen, Sicherheitslücken zu schließen, Möglichkeiten für Kosteneinsparungen zu finden, Ihre Systemleistung zu verbessern und die Zuverlässigkeit zu erhöhen.

AWS-Account-Teams sind Ihr erster Ansprechpartner. Sie geben Ihnen Anleitungen für die Bereitstellung und Implementierung und verweisen Sie bei eventuell auftretenden Sicherheitsproblemen an die entsprechenden Ressourcen.

Die Mitarbeiter des **AWS Enterprise Support** bieten Ihnen innerhalb von 15 Minuten Antworten und sind rund um die Uhr telefonisch, im Chat oder per E-Mail erreichbar. Darüber hinaus ist ein Technical Account Manager (TAM) Ihr fest zugeordneter Ansprechpartner. Dieser Concierge-Service sorgt dafür, dass die Anliegen der Kunden möglichst schnell bearbeitet werden können.

Das **AWS-Partnernetzwerk** bietet Hunderte branchenführende Produkte an, die mit vorhandenen Kontrollen in Ihren On-Premises-Umgebungen gleichwertig oder identisch sind

oder sich in diese integrieren lassen. Diese Produkte ergänzen die vorhandenen AWS-Services, damit Sie eine umfassende Sicherheitsarchitektur bereitstellen und eine nahtlosere Erfahrung in Ihrer Cloud und Ihren On-Premises-Umgebungen bieten können. Darüber hinaus stehen Ihnen Hunderte zertifizierte AWS-Beratungspartner weltweit bei Ihren Sicherheits- und Compliance-Fragen beratend zur Seite.

AWS Professional Services ist auf Sicherheit, Risiken und Compliance spezialisiert. Das Team unterstützt Sie gerne bei der Migration Ihrer hochsensiblen Workloads zur AWS Cloud und hilft Ihnen so, Vertrauen und technische Kompetenzen aufzubauen. Die Mitarbeiter von AWS Professional Services helfen Kunden, auf der Grundlage bewährter Designs Sicherheitsrichtlinien und -verfahren zu entwickeln, und sorgen dafür, dass das Sicherheitsdesign der Kunden den internen und externen Compliance-Anforderungen genügt.

AWS Marketplace ist ein digitaler Katalog mit Tausenden von Softwarelisten unabhängiger Softwareanbieter. Hier ist es leicht möglich, Software, die in AWS ausgeführt werden kann, zu finden, zu testen, zu kaufen und bereitzustellen. Die Sicherheitsprodukte von AWS Marketplace ergänzen die vorhandenen AWS-Services, damit Sie eine umfassende Sicherheitsarchitektur bereitstellen und eine nahtlosere Erfahrung in Ihrer Cloud und Ihren On-Premises-Umgebungen bieten können.

AWS Security Bulletins stellt Sicherheitsberichte zu aktuellen Schwachstellen und Bedrohungen zur Verfügung und ermöglicht den Kunden eine Zusammenarbeit mit AWS-Sicherheitsexperten, um Aspekte wie z. B. Missbrauchsmeldungen, Schwachstellen und Penetrationstests anzugehen. Wir bieten auch Onlineressourcen für die Meldung von Schwachstellen.

In der **AWS-Sicherheitsdokumentation** erfahren Sie, wie Sie die AWS-Services so konfigurieren können, dass sie Ihren Sicherheits- und Compliance-Anforderungen entsprechen. AWS-Kunden profitieren von einer Rechenzentrums- und Netzwerkarchitektur, die eingerichtet wurde, um die Anforderungen der Organisationen mit den höchsten Sicherheitsanforderungen zu erfüllen.
Das **AWS Well-Architected Framework** unterstützt Cloud-Architekten beim Aufbau einer sicheren, leistungsstarken, resilienten und effizienten Infrastruktur für ihre Anwendungen. Das AWS Well-Architected Framework umfasst die Säule der Sicherheit, die auf den Schutz von Informationen und Systemen ausgerichtet ist. Zu den wichtigsten Themen zählen die Vertraulichkeit und Integrität von Daten, die Ermittlung und Verwaltung der Benutzerberechtigungen mithilfe der Berechtigungsverwaltung, der Schutz der Systeme und die Festlegung von Kontrollen zur Erkennung von Sicherheitsereignissen. Kunden können über die Konsole auf den Well-Architected-Service zugreifen oder sich Unterstützung von einem der APN-Partner holen.

Mit dem **AWS Well-Architected Tool** können Sie den Status Ihrer Workloads überprüfen und mit den neuesten bewährten Methoden für die AWS-Architektur vergleichen. Dieses kostenlose Tool ist in der AWS-Managementkonsole verfügbar. Zunächst müssen Sie einige Fragen zu operativer Exzellenz, Sicherheit, Zuverlässigkeit, Leistungseffizienz und Kostenoptimierung

beantworten. Daraufhin erstellt das AWS Well-Architected Tool einen Plan für die Entwicklung einer Cloud-Architektur unter Verwendung bewährter Methoden.

Compliance

Über AWS Compliance können sich Kunden mit den zuverlässigen Kontrollmöglichkeiten in AWS für die Sicherheit und den Datenschutz in der AWS Cloud vertraut machen. Bei Systemen, die in der AWS Cloud erstellt werden, sind AWS und die Kunden gemeinsam für die Compliance verantwortlich. AWS-Computing-Umgebungen werden fortlaufend geprüft und von Akkreditierungsstellen verschiedener Regionen und Branchen zertifiziert (z. B. SOC 1/SSAE 16/ISAE 3402 (ehemals SAS 70), SOC 2, SOC 3, ISO 9001/ISO 27001, FedRAMP, DoD SRG und PCI DSS Level 1). Darüber hinaus verfügt AWS über Programme zur Bestätigung der Sicherheit, die Vorlagen und Kontrollzuordnungen bieten, damit Kunden die Compliance ihrer in AWS ausgeführten Umgebungen sicherstellen können. Eine umfassende Liste der Programme finden Sie unter AWS-Compliance-Programme.

Alle AWS-Services können in Einklang mit der DSGVO verwendet werden. Somit können Kunden nicht nur von allen Maßnahmen profitieren, die AWS bereits zur Aufrechterhaltung der Sicherheit der Services ergreift, sondern auch AWS-Services im Rahmen ihrer Pläne zur Einhaltung der DSGVO bereitstellen. Der AWS-Vertragsanhang zur DSGVO-konformen Datenverarbeitung (AWS GDPR Data Processing Addendum – GDPR DPA) hilft Ihnen, die vertraglichen Verpflichtungen im Rahmen der DSGVO einzuhalten. Der AWS-Vertragsanhang zur DSGVO-konformen Datenverarbeitung ist in die Nutzungsbedingungen der AWS-Services integriert und gilt automatisch für alle Kunden weltweit, die sich an die DSGVO halten müssen. Amazon.com, Inc. ist unter dem EU-US Privacy Shield zertifiziert. AWS fällt unter diese Zertifizierung. Dies macht es für Kunden, die personenbezogene Daten in die USA übertragen möchten, leichter, ihren Datenschutzverpflichtungen gerecht zu werden. Die Zertifizierung von Amazon.com Inc. ist auf der Website des EU-US Privacy Shield unter folgendem Link zu finden: https://www.privacyshield.gov/list.

Durch den Betrieb in einer akkreditierten Umgebung verringern sich die notwendigen Prüfungen und die damit verbundenen Kosten für die Kunden. Die zugrunde liegende Infrastruktur von AWS wird kontinuierlich Bewertungen unterzogen. Diese beziehen sich auch auf die physische Sicherheit und die Umgebungssicherheit der Hardware und der Rechenzentren. Kunden können diese Zertifizierungen nutzen und diese Kontrollen einfach übernehmen.

In einem herkömmlichen Rechenzentrum werden allgemeine Compliance-Aktivitäten oft in regelmäßigen Abständen manuell durchgeführt. Diese Aktivitäten beinhalten die Prüfung der Asset-Konfigurationen und Berichte über Verwaltungsaktivitäten. Diese Berichte sind bereits veraltet, noch bevor sie überhaupt veröffentlicht werden. Durch den Betrieb in einer AWS-Umgebung können Kunden zur Prüfung der Compliance integrierte, automatisierte Tools wie AWS Security Hub, AWS Config und AWS CloudTrail nutzen. Mit diesen Tools verringert sich der Aufwand bei der Durchführung von Prüfungen, da diese Aufgaben routinemäßig, kontinuierlich und automatisiert durchgeführt werden. Wenn Sie weniger Zeit mit manuellen Aktivitäten

verbringen müssen, können Sie dazu beitragen, dass Compliance in Ihrem Unternehmen keinen notwendigen Verwaltungsaufwand mehr bedeutet, sondern eine Maßnahme zur Bewältigung der Risiken und zur Verbesserung Ihrer Sicherheitslage darstellt.

Weitere Informationen

Zusätzliche Informationen finden Sie in folgenden Ressourcen:

Für Informationen über ...	Siehe
Wichtige Themen, Forschungsbereiche und Trainingsmöglichkeiten zur Cloud-Sicherheit in AWS	AWS-Cloud-Sicherheit – Lernen
Das AWS Cloud Adoption Framework, in dem die Beratung in sechs Schwerpunktbereichen organisiert ist: Business, Mitarbeiter, Governance, Plattform, Sicherheit und Betriebsablauf	AWS Cloud Adoption Framework
Spezielle Kontrollen in AWS, Integration von AWS in Ihr bestehendes Framework	Amazon Web Services: Risiko und Compliance
Bewährte Methoden für die Bereitstellung von Sicherheitskontrollen in einer AWS-Umgebung	Bewährte Methoden für die Sicherheit in AWS
Säule für Sicherheit des AWS Well-Architected Framework	Säule für Sicherheit des AWS Well-Architected Framework

Dokumentversionen

Datum	Beschreibung
Januar 2020	Aktualisierung mit den neuesten Services, Ressourcen und Technologien
Juli 2015	Erstveröffentlichung