AWS Sicherheit Best Practices

Dob Todorov
Yinal Ozkan

September 2014

(Die neueste Version dieses Dokuments finden sie unter **http://aws.amazon.com/security**.)

Inhalt

Abstrakt 4

Überblick 4

Das AWS-Modell geteilter Verantwortung 5

Definieren und Kategorisieren von AWS-Komponenten 12

Entwerfen Sie Ihr eigenes ISMS zum Schutz Ihrer Komponenten auf AWS 13

Verwalten von AWS-Konten, IAM-Benutzern, Gruppen und Rollen 15

Verwalten des Zugriffs auf Amazon EC2-Instances auf Betriebssystemebene 21

Sichern Ihrer Daten 22

Schützen Ihrer Betriebssysteme und Anwendungen 36

Schützen Ihrer Infrastruktur 46

Verwaltung von Sicherheitsüberwachung, Alarmierung, Prüfpfaden und Vorfallreaktion 59

Zusammenfassung 63

Referenzen und weiterführende Literatur 64

Abbildungen

Abbildung 1: Das Modell geteilter Verantwortung für Infrastruktur-Services 8

Abbildung 2: Das Modell geteilter Verantwortung für Container-Services 10

Abbildung 3: Das Modell geteilter Verantwortung für abstrakte Services 11

Abbildung 4: Funktionsweise von EC2-Rollen 19

Abbildung 5: AWS-Identitätsverbund mit temporären Sicherheits-Anmeldeinformationen 20

Abbildung 6: Ebenenbezogener Netzwerkschutz in der Cloud 53

Tabellen

Tabelle 1: Beispiele für Komponenten 13
Tabelle 2: Phasen bei der ISMS-Erstellung 15
Tabelle 3: Strategien für AWS-Konten 16
Tabelle 4: Anmeldeinformationstypen 17
Tabelle 5: Anmeldeinformationstypen für programmgesteuerten Zugriff 18
Tabelle 6: Häufige Anwendungsfälle, die Zugriffsübertragungen erfordern 19
Tabelle 7: Bedrohungen für Daten im Ruhezustand 25
Tabelle 8: Amazon S3-Funktionen zum Schützen von Daten im Ruhezustand 26
Tabelle 9: Amazon EBS-Funktionen zum Schützen von Daten im Ruhezustand 27
Tabelle 10: Schutzfunktionen auf Amazon RDS-Plattformebene für Daten im Ruhezustand 28
Tabelle 11: Schützen von Daten im Ruhezustand auf Amazon EMR 30
Tabelle 12: Bedrohungen für Daten im Transit 32
Tabelle 13: Schützen von Daten im Transit beim Zugriff auf die öffentliche Cloud 33
Tabelle 14: Schützen von Daten im Transit beim Zugriff auf Amazon EMR 36
Tabelle 15: Bereinigungsaufgaben vor dem Veröffentlichen eines AMI 37
Tabelle 16: Schützen von Linux-/UNIX-AMIs 38
Tabelle 17: Schützen von Windows-AMIs 38
Tabelle 18: Ansätze für den Schutz vor Malware 41
Tabelle 19: Bewährte Methoden für das Einschränken von Missbrauch 44
Tabelle 20: Zugreifen auf Ressourcen in Amazon VPC 47
Tabelle 21: Kontrollen für Peripheriesysteme 51
Tabelle 22: Verwaltung und Verbesserung von Metriken 56
Tabelle 23: Techniken zur Risikovermeidung und zum Schutz vor DoS/DDoS-Angriffen 58
Tabelle 24: Erwägungen zu Protokolldateien 60

Zusammenfassung

Dieses Whitepaper richtet sich an Kunden, deren Aufgabe die Gestaltung der Sicherheitsinfrastruktur und die Konfiguration von Anwendungen ist, welche auf Amazon Web Services (AWS) betrieben werden sollen. Beschrieben werden Best Practices für die Sicherheit, die Sie nutzen können, um ein Informationssicherheits-Managementsystem (ISMS) zu entwerfen und eine Sammlung von Sicherheitsrichtlinien und Prozessen für Ihr Unternehmen zu erstellen, mit denen Sie Ihre Daten und Komponenten in der AWS-Cloud sichern können. Das Whitepaper bietet auch einen Überblick über verschiedene Sicherheitsthemen wie Identifizierung, Kategorisierung und Schutz Ihrer Komponenten auf AWS sowie die Verwaltung des Zugriffs auf AWS-Ressourcen mithilfe von Konten, Benutzern und Gruppen. Zudem werden Verfahren vorgestellt, mit denen Sie Ihre Daten, Betriebssysteme, Anwendungen und die allgemeine Infrastruktur in der Cloud sichern können.

Das Papier richtet sich an IT-Entscheider und Sicherheitspersonal. Es wird vorausgesetzt, dass Sie mit den grundlegenden Sicherheitskonzepten im Bereich Vernetzung, Betriebssysteme, Datenverschlüsselung und Betriebssteuerung vertraut sind.

Überblick

Informationssicherheit ist von größter Bedeutung für Amazon Web Services (AWS)-Kunden. Sicherheit ist eine grundlegende Voraussetzung für den Schutz erfolgskritischer Informationen vor zufälligem oder vorsätzlichem Diebstahl, Datenlecks, Integritätsverlust und Löschung.Auf der Grundlage des *AWS-Modells der geteilten Verantwortung* stellt AWS eine globale Sicherheitsinfrastruktur bereit, welche grundlegende Compute-, Speicher-, Netzwerk und Datenbank-Services sowie auch Services auf höherer Ebene enthält. AWS bietet eine Reihe von Sicherheits-Services und -funktionen, die AWS-Kunden nutzen können, um ihre Komponenten zu schützen. AWS-Kunden sind sowohl für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit ihrer Daten in der Cloud als auch für die Erfüllung spezieller Geschäftsanforderungen für den Datenschutz verantwortlich. Weitere Informationen über die AWS-Sicherheitsfunktionen finden Sie unter Overview of Security Processes Whitepaper.

Dieses Whitepaper beschreibt Best Practices, um ein Informationssicherheits-Managementsystem (ISMS) zu entwerfen und zu erstellen, also eine Sammlung von Richtlinien für Informationssicherheit und von Prozessen für die Komponenten Ihres Unternehmens auf AWS. Weitere Informationen über ISMSs finden Sie im Abschnitt über ISO 27001 unter http://www.27000.org/iso-27001.htm. Um AWS zu verwenden ist es nicht erforderlich ein ISMS zu erstellen. Trotzdem denken wir, dass ein strukturierter Ansatz zur Verwaltung von Informationssicherheit, der auf den Grundbausteinen eines weit verbreiteten globalen Sicherheitskonzepts beruht, Ihnen bei der Verbesserung der allgemeinen Sicherheitslage Ihres Unternehmens helfen kann.

Folgende Themen werden behandelt:

- Aufteilen der Verantwortlichkeit zwischen AWS und Ihnen, dem Benutzer
- Definieren und Kategorisieren Ihrer Komponenten
- Verwalten des Benutzerzugriffs auf Ihre Daten mithilfe privilegierter Konten und Gruppen
- Sichern Ihrer Daten, Betriebssysteme und Netzwerke durch Anwendung von Best Practices
- Erreichen Ihrer Sicherheitsziele durch Überwachen und Alarmieren

In diesem Whitepaper werden Best Practices für die genannten Themen im Überblick erörtert. (Es handelt sich nicht um praktische Konfigurationsanleitungen. Hilfestellung für die Konfiguration finden Sie in der AWS-Dokumentation unter http://aws.amazon.com/de/documentation/.

Das AWS-Modell geteilter Verantwortung

Amazon Web Services bietet eine sichere globale Infrastruktur und Services in der Cloud. Sie können Ihre Systeme auf der Grundlage von AWS erstellen und ein ISMS entwerfen, das die Vorteile der AWS-Funktionen nutzt.

Um ein ISMS in AWS zu entwerfen, müssen Sie mit dem AWS-Modell geteilter Verantwortung vertraut sein. In diesem Modell arbeiten AWS und Kunden gemeinsam an der Realisierung von Sicherheitszielen.

AWS bietet eine sichere Infrastruktur und Services, während Sie, der Kunde, für sichere Betriebssysteme, Plattformen und Daten verantwortlich sind. Um eine sichere globale Infrastruktur zu gewährleisten, konfiguriert AWS Infrastrukturkomponenten und stellt Services und Funktionen bereit, die Sie verwenden können, um die Sicherheit zu verbessern. Eine solche Komponente ist beispielsweise der Identity und Access Management (IAM)-Service, der Ihnen ermöglicht, Benutzer und Benutzerberechtigungen in einer Untergruppe der AWS-Services zu verwalten. Um sichere Services zu gewährleisten, bietet AWS Modelle geteilter Verantwortung für jede unserer Service-Arten an:

- Infrastruktur-Services
- Container-Services
- Abstrakte Services

Im Modell geteilter Verantwortung für Infrastruktur-Services wie beispielsweise Amazon Elastic Compute Cloud (Amazon EC2) ist festgelegt, dass AWS die Sicherheit der folgenden Komponenten verwaltet:

- Einrichtungen
- Physische Sicherheit von Hardware
- Netzwerkinfrastruktur
- Virtualisierungsinfrastruktur

Betrachten Sie AWS für die Zwecke Ihrer ISMS-Komponentendefinition als verantwortlich für diese Komponenten. Nutzen Sie diese AWS-Kontrollen in Ihrem ISMS.

In diesem Amazon EC2-Beispiel sind Sie als Kunde für die Sicherheit der folgenden Komponenten verantwortlich:

- Amazon Machine Images (AMIs)
- Betriebssysteme
- Anwendungen
- Daten im Transit
- Ruhende Daten
- Datenspeicher
- Anmeldeinformationen
- Richtlinien und Konfiguration

In bestimmten Services gibt es weitere Unterteilungen bezüglich der Verantwortlichkeiten zwischen Ihnen und AWS.

Weitere Informationen finden Sie unter http://aws.amazon.com/compliance/#third-party.

Die sichere globale AWS-Infrastruktur

Die sichere globale Infrastruktur und die Services von AWS werden von AWS verwaltet. Damit ist eine vertrauenswürdige Basis für Unternehmenssysteme und individuelle Anwendungen gegeben. AWS etabliert hohe Standards für Informationssicherheit innerhalb der Cloud und verfügt über ein umfassendes und ganzheitliches Bündel von Kontrollvorgaben, unter anderem für die physische Sicherheit, den Erwerb und die Entwicklung von Software, die Verwaltung der Mitarbeiterlaufbahn und die Sicherheitsorganisation. Die sichere globale Infrastruktur und die Services

von AWS unterliegen einer regelmäßigen externen Compliance-Überprüfung. Weitere Informationen finden Sie im Whitepaper Amazon Web Services Risk and Compliance. (Siehe Referenzen und *Weiterführende Literatur*)

Verwenden des IAM-Services

Der IAM-Service ist eine Komponente der sicheren globalen Infrastruktur von AWS, die wir in diesem Papier vorstellen. Mit IAM können Sie Benutzer und Anmeldeinformationen und Berechtigungsrichtlinien (wie Kennwörter oder Zugriffsschlüssel) zentral verwalten, die festlegen, auf welche AWS-Services und Ressourcen Benutzer zugreifen dürfen.

Wenn Sie sich erstmals bei AWS anmelden, erstellen Sie ein AWS-Konto und geben dafür einen Benutzernamen (Ihre E-Mail-Adresse) und ein Passwort an. Durch die Eingabe von Benutzername und Passwort öffnen Sie die AWS Management Console, in der Sie über eine Browser-basierte Schnittstelle Ihre AWS-Ressourcen verwalten. Sie haben auch die Möglichkeit, Zugriffsschlüssel zu erstellen (die aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel bestehen) und AWS damit über die Befehlszeile (Command Line Interface, CLI), die AWS-SDKs oder API-Aufrufe programmgesteuert zu instrumentieren.

Mit IAM können Sie einzelne Benutzer, jeweils mit eigenem Benutzernamen, Passwort und Zugriffsschlüssel, innerhalb Ihres AWS-Konto anlegen. Diese Benutzer haben dann über eine URL, die speziell für Ihr Konto gilt, Zugriff auf die Konsole, respektive die AWS Ressourcen. Ein Benutzer kann auch eigene Zugriffsschlüssel von Ihnen erhalten und damit über programmgesteuerte Aufrufe auf AWS-Ressourcen zugreifen. Alle Kosten für die Aktivitäten Ihrer IAM-Benutzer werden über Ihr AWS-Konto abgerechnet. Wir empfehlen, dass Sie auch für sich selbst einen IAM-Benutzer anlegen und die Anmeldeinformationen für Ihr AWS-Konto nicht für den täglichen Zugriff auf AWS verwenden. Weitere Informationen finden Sie unter IAM Best Practices.

Regionen, Availability Zones und Endpunkte

Sie sollten auch mit Regionen, Availability Zones und Endpunkten vertraut sein, welche Komponenten der sicheren globalen AWS-Infrastruktur sind.

Durch die Auswahl einer AWS-Region haben Sie Einfluss auf die Netzwerklatenz und sind in der Lage regulatorische Vorgaben zu erfüllen. Wenn Sie Daten in einer bestimmten Region speichern, werden sie nicht außerhalb dieser Region repliziert. Wenn Ihre Geschäftsanforderungen dies verlangen, liegt in Ihrer Verantwortung, Daten zwischen den Regionen zu replizieren. AWS stellt Informationen über das Land (und gegebenenfalls das Bundesland bzw. den Landkreis) bereit, zu dem eine Region gehört. Sie sind für die Auswahl der Region verantwortlich, in der Sie – unter Berücksichtigung Ihrer Anforderungen bezüglich Compliance und Netzwerklatenz – Daten speichern möchte. Die Regionen sind in Hinblick auf Verfügbarkeit konzipiert und bestehen aus mindestens zwei (oft mehr) Availability Zones. Availability Zones sind fehlertolerant ausgelegt. Sie sind mit mehreren Internet Service Providern (ISPs) verbunden und werden von unabhängigen Stromnetzen versorgt. Sie sind über Hochgeschwindigkeitsverbindungen miteinander vernetzt, sodass für Anwendungen die Kommunikation zwischen Availability Zones innerhalb der gleichen Region über Local Area Network (LAN)-Konnektivität sichergestellt ist. Dem Kunden obliegt die sorgfältige Auswahl der Availability Zones, zu denen seine Systeme gehören sollen. Systeme können sich über mehrere Availability Zones erstrecken. Wir empfehlen, alle Systeme so zu entwerfen, dass sie einen temporären oder längeren Ausfall einer Availability Zone im Fall einer Katastrophe überstehen.

AWS ermöglicht Web-basierten Zugriff auf Services über die AWS Management Console, die für jeden Service eine eigene Konsole enthält. AWS bietet programmgesteuerten Zugriff auf Services über Application Programming Interfaces (APIs) und Befehlszeilenschnittstellen (Command Line Interfaces, CLIs). Service-Endpunkte, die von AWS verwaltet werden, ermöglichen Verwaltungszugriff („Backplane“-Access).

Geteilte Verantwortung für die Sicherheit von AWS-Services

AWS bietet eine Vielzahl verschiedener Infrastruktur- und Plattform-Services. Zur Erläuterung der geteilten Verantwortung für diese AWS-Services und ihrer Sicherheit haben wir sie in drei Hauptkategorien gegliedert: Infrastruktur-, Container- und abstrakte Dienste. Jede Kategorie verfügt über ein leicht abgewandeltes Modell für die Sicherheitsverantwortung, welche auf der Art und Weise basiert, in der Sie die Funktionalität verwenden und darauf zugreifen.

- **Infrastruktur-Services:** Diese Kategorie umfasst Compute-Services wie Amazon EC2 und zugehörige Services wie Amazon Elastic Block Store (Amazon EBS), Auto Scaling und Amazon Virtual Private Cloud (Amazon VPC). Mit diesen Services können Sie unter Verwendung von Technologien, die lokalen Lösungen ähnlich und mit diesen weitgehend kompatibel sind, eine Cloud-Infrastruktur entwerfen und realisieren. Sie kontrollieren das Betriebssystem und können jedes IAM-System einsetzen, das Zugriff auf die Benutzerschicht des Virtualisierungsstapels ermöglicht.
- **Container Services:** Services aus dieser Kategorie werden in der Regel auf separaten Amazon EC2-Instanzen oder anderen Infrastruktur-Instanzen ausgeführt, allerdings können Sie das Betriebssystem oder die Plattformebene nicht verwalten. AWS bietet einen verwalteten Service für diese Anwendungs-„Container“. Sie sind für die Einrichtung und Verwaltung von Kontrollelementen für das Netzwerk (wie beispielsweise Firewall-Regeln) verantwortlich, ebenso für die Identitätsverwaltung auf Plattformebene und die Zugriffsverwaltung unabhängig von IAM. Beispiele für Container-Services sind Amazon Relational Database Service (Amazon RDS), Amazon Elastic Map Reduce (Amazon EMR) und AWS Elastic Beanstalk.
- **Abstrakte Services**: Diese Kategorie umfasst High-Level-Speicherung, Datenbanken und Messaging-Services wie Amazon Simple Storage Service (Amazon S3), Amazon Glacier, Amazon DynamoDB, Amazon Simple Queuing Service (Amazon SQS) und Amazon Simple Email Service (Amazon SES). Diese Services abstrahieren die Plattform- oder Management-Ebene, auf der Sie Cloud-Anwendungen erstellen und betreiben. Sie greifen auf die Endpunkte dieser abstrakten Services über AWS-APIs zu. AWS verwaltet die zugrunde liegenden Service-Komponenten oder das Betriebssystem, unter dem sie ausgeführt werden. Sie verwenden ebenfalls die zugrunde liegende Infrastruktur. Abstrakte Services stellen eine Multi-Tenant-Plattform bereit, die Ihre Daten in sicherer Weise isoliert und eine leistungsfähige IAM-Integration ermöglicht.

Lassen Sie uns das Modell geteilter Verantwortung für jeden Service-Typ etwas näher betrachten.

Das Modell geteilter Verantwortung für Infrastruktur-Services

Infrastruktur-Services wie Amazon EC2, Amazon EBS und Amazon VPC werden auf oberster Ebene der globalen AWS-Infrastruktur ausgeführt. Sie unterscheiden sich in Bezug auf Verfügbarkeit und Haltbarkeit, arbeiten aber immer in der Region, in der sie gestartet wurden. Sie können Systeme einrichten, deren Verfügbarkeit über die einzelner AWS-Services hinausgeht, indem Sie robuste Komponenten in mehreren Availability Zones einsetzen.

Abbildung 1 zeigt die Bausteine, aus denen das Modell geteilter Verantwortung für Infrastruktur-Services aufgebaut ist.

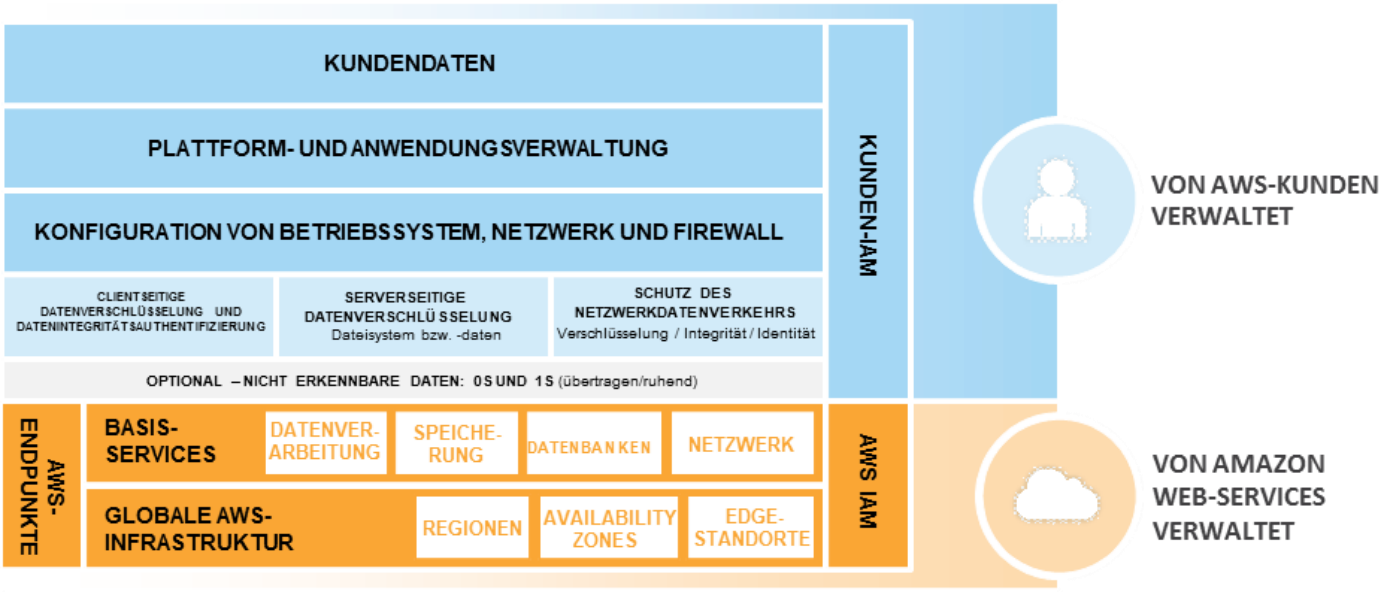

Abbildung 1: Das Modell geteilter Verantwortung für Infrastruktur-Services

Basierend auf der sicheren globalen AWS-Infrastruktur installieren und konfigurieren Sie Ihre Betriebssysteme und Plattformen in der AWS-Cloud auf die gleiche Weise wie vor Ort in Ihren eigenen Rechenzentren. Dann installieren Sie Ihre Anwendungen auf Ihrer Plattform. Letztlich sind Ihre Daten in Ihren eigenen Anwendungen enthalten und werden durch diese verwaltet. Sofern keine strengeren Geschäfts- oder Compliance-Anforderungen vorliegen, müssen Sie die von der sicheren globalen AWS-Infrastruktur bereitgestellten Sicherheitsschichten nicht durch zusätzliche ergänzen.

Für bestimmte Compliance-Anforderungen benötigen Sie möglicherweise eine zusätzliche Schutzschicht zwischen den AWS-Services einerseits und Ihren Betriebssystemen und Plattformen mit Ihren Anwendungen und Daten andererseits. Sie haben deshalb die Möglichkeit, zusätzliche Kontrollen einzuführen, etwa für ruhende Daten und für Daten im Transit. Oder fügen Sie zwischen den AWS-Services und Ihrer Plattform eine Trennschicht ein. Die Trennschicht kann Datenverschlüsselung, Datenintegritäts-Authentifizierung, Software- und Datensignierung, sichere Zeitstempel und mehr umfassen.

AWS stellt Technologien bereit, welche Sie implementieren können, um ruhende Daten oder Daten im Transit zu schützen. Weitere Informationen dazu finden Sie in den Abschnitten „Verwalten des Zugriffs auf Amazon EC2-Instanzen auf Betriebssystemebene“ und „Sichern Ihrer Daten“ in diesem Whitepaper. Es steht Ihnen frei, eigene Datenschutz-Werkzeuge einzusetzen oder die Angebote von AWS-Partnern zu nutzen.

Im vorherigen Abschnitt wurde beschrieben, auf welche Weise Sie den Zugriff auf Ressourcen verwalten, die eine Authentifizierung für AWS-Services erfordern. Für den Zugriff auf das Betriebssystem Ihrer EC2-Instanzen benötigen Sie jedoch andere Anmeldeinformationen. Im Modell geteilter Verantwortung sind Sie verantwortlich für die Anmeldeinformationen für das Betriebssystem. Beim erstmaligen Zugriff auf das Betriebssystem werden Sie von AWS unterstützt.

Wenn Sie eine neue Amazon EC2-Instanz aus einem Standard-AMI starten, können Sie auf diese Instanz mithilfe sicherer Netzwerkprotokolle zugreifen, beispielsweise mit Secure Shell (SSH) oder Windows Remote Desktop Protocol (RDP). Sie müssen sich auf der Betriebssystemebene erfolgreich authentifizieren, bevor Sie die Amazon EC2-Instanz nutzen und konfigurieren können. Nachdem Sie sich authentifiziert haben und der Remotezugriff auf die Amazon EC2-Instanz möglich ist, richten Sie einen beliebigen Authentifizierungsmechanismus für das Betriebssystem ein, beispielsweise X.509-Zertifikat-Authentifizierung, Microsoft Active Directory oder lokale Betriebssystemkonten.

Für die Authentifizierung bei der EC2-Instanz bietet AWS asymmetrische Schlüsselpaare, Amazon EC2-Schlüsselpaare genannt. Dabei handelt es sich um RSA-Schlüsselpaare nach Industriestandard. Jeder Benutzer kann mehrere Amazon EC2-Schlüsselpaare besitzen und neue Instanzen mit unterschiedlichen Schlüsselpaaren starten. EC2-Schlüsselpaare haben keinen Bezug zu den zuvor vorgestellten Anmeldeinformationen für das AWS-Konto oder für IAM-Benutzer. Diese Anmeldeinformationen steuern den Zugang zu anderen AWS-Services, während EC2-Schlüsselpaare nur für den Zugriff auf Ihre spezielle Instanz gelten.

Sie können auch Ihre eigenen Amazon EC2-Schlüsselpaare mit Industriestandard-Tools wie OpenSSL generieren. Sie generieren das Schlüsselpaar in einer sicheren und vertrauenswürdigen Umgebung. Nur der öffentliche Schlüssel des Schlüsselpaares wird in AWS importiert – den privaten Schlüssel müssen Sie selbst sicher speichern. Wir empfehlen für die Generierung von Schlüsseln die Verwendung eines hochwertigen Zufallszahlengenerators.

Sie haben auch die Möglichkeit, Amazon EC2-Schlüsselpaare von AWS generieren zu lassen. In diesem Fall werden Ihnen sowohl der private als auch der öffentliche Schlüssel des RSA-Schlüsselpaar angezeigt, wenn Sie die Instanz erstmals erstellen. Sie müssen den privaten Schlüssel des Amazon EC2-Schlüsselpaars herunterladen und sicher speichern. AWS speichert den privaten Schlüssel nicht – geht er verloren, müssen Sie ein neues Schlüsselpaar generieren.

Für Amazon EC2 Linux-Instanzen, die den **cloud-init**-Service verwenden, gilt Folgendes: Beim Start einer neuen Instanz von einem Standard-AWS-AMI wird der öffentliche Schlüssel des Amazon EC2-Schlüsselpaars an die ursprüngliche **~/.ssh/authorized_keys**-Datei des Betriebssystembenutzers angefügt. Dieser Benutzer kann dann einen SSH-Client verwenden, um sich mit der Amazon EC2-Linux-Instanz zu verbinden. Dazu muss er den Client so konfigurieren, dass für dessen Identität der korrekte Benutzername für die Amazon EC2-Instanz verwendet wird (beispielsweise ec2-user), zudem muss lokal die Datei mit dem privaten Schlüssel für die Benutzerauthentifizierung bereitgestellt werden.

Für Amazon EC2 Windows-Instanzen, die den **ec2config**-Service verwenden, gilt Folgendes: Wenn eine neue Instanz von einem Standard-AWS-AMI gestartet wird, legt der **ec2config**-Service ein neues zufälliges Administratorpasswort für die Instanz fest und verschlüsselt dieses mit dem öffentlichen Schlüssel des entsprechenden Amazon EC2-Schlüsselpaars. Der Benutzer kann das Passwort für die Windows-Instanz mit der AWS Management Console oder mit Befehlszeilen-Tools abrufen und durch die Bereitstellung des entsprechenden privaten Amazon EC2-Schlüssels entschlüsseln. Dieses Passwort kann zusammen mit dem Standard-Administratorkonto für die Amazon EC2-Instanz verwendet werden, um den Administratorzugriff zu authentifizieren.

AWS bietet eine Reihe flexibler und praktischer Werkzeuge für die Verwaltung von Amazon EC2-Schlüsseln und stellt Authentifizierung nach Industriestandard für neu gestartete Amazon EC2-Instanzen bereit. Wenn Sie höhere Sicherheitsanforderungen haben, können Sie alternative Authentifizierungsmechanismen wie LDAP- oder Active Directory-Authentifizierung implementieren und die Authentifizierung mit Amazon EC2-Schlüsselpaaren deaktivieren.

Das Modell geteilter Verantwortung für Container-Services

Das AWS-Modell geteilter Verantwortung gilt auch für Container-Services wie Amazon RDS und Amazon EMR. Für diese Services verwaltet AWS die zugrunde liegende Infrastruktur und grundlegende Services, das Betriebssystem und die Anwendungsplattform. Zum Beispiel ist Amazon RDS für Oracle ein verwalteter Datenbank-Service, bei dem AWS alle Ebenen des Containers verwaltet, einschließlich der Oracle-Datenbankplattform. Für Services wie Amazon RDS bietet die AWS-Plattform Tools zur Sicherung und Wiederherstellung von Daten. Es liegt in Ihrer Verantwortung, diese Tools entsprechend Ihren Richtlinien für unterbrechungsfreie Geschäftsabläufe und Notfallwiederherstellung zu konfigurieren.

Bei AWS Container-Services sind Sie für die Daten und für die Firewall-Regeln für den Zugang zum Container-Service verantwortlich. Amazon RDS stellt beispielsweise RDS-Sicherheitsgruppen bereit, und mit Amazon EMR können Sie Firewall-Regeln für Amazon EMR-Instanzen mithilfe von Amazon EC2-Sicherheitsgruppen verwalten.

Abbildung 2 zeigt das Modell geteilter Verantwortung für Container-Services

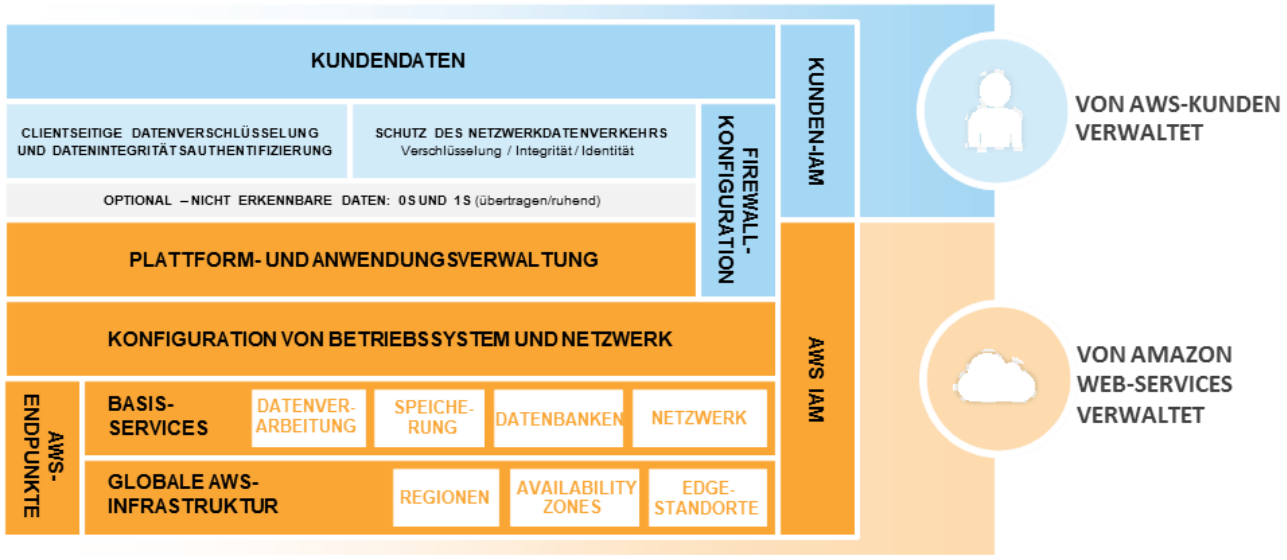

Abbildung 2: Das Modell geteilter Verantwortung für Container-Services

Das Modell geteilter Verantwortung für abstrakte Services

Für abstrakte Services wie Amazon S3 und Amazon DynamoDB betreibt AWS die Infrastrukturebene, das Betriebssystem und die Plattformen. Sie greifen auf die Endpunkte zu, um Daten zu speichern und abzurufen. IAM ist optimal in Amazon S3 und DynamoDB integriert. Sie sind für die Verwaltung Ihrer Daten (einschließlich der Klassifizierung Ihrer Komponenten) verantwortlich, ebenso für die Verwendung von IAM-Tools zum Zuordnen ACL-typischer Berechtigungen für einzelne Ressourcen auf Plattformebene. Zudem sind Sie für die Berechtigungen basierend auf Benutzeridentität oder Benutzerverantwortung auf der IAM-Benutzer/Gruppenebene zuständig. Einige Services (wie Amazon S3) bieten auch plattformgestützte Verschlüsselung für ruhende Daten. Daten im Transit (vom oder zum Service) werden durch plattformgestützte HTTPS-Nutzdatenkapselung geschützt.

Abbildung 3 zeigt das Modell geteilter Verantwortung für abstrakte Services:

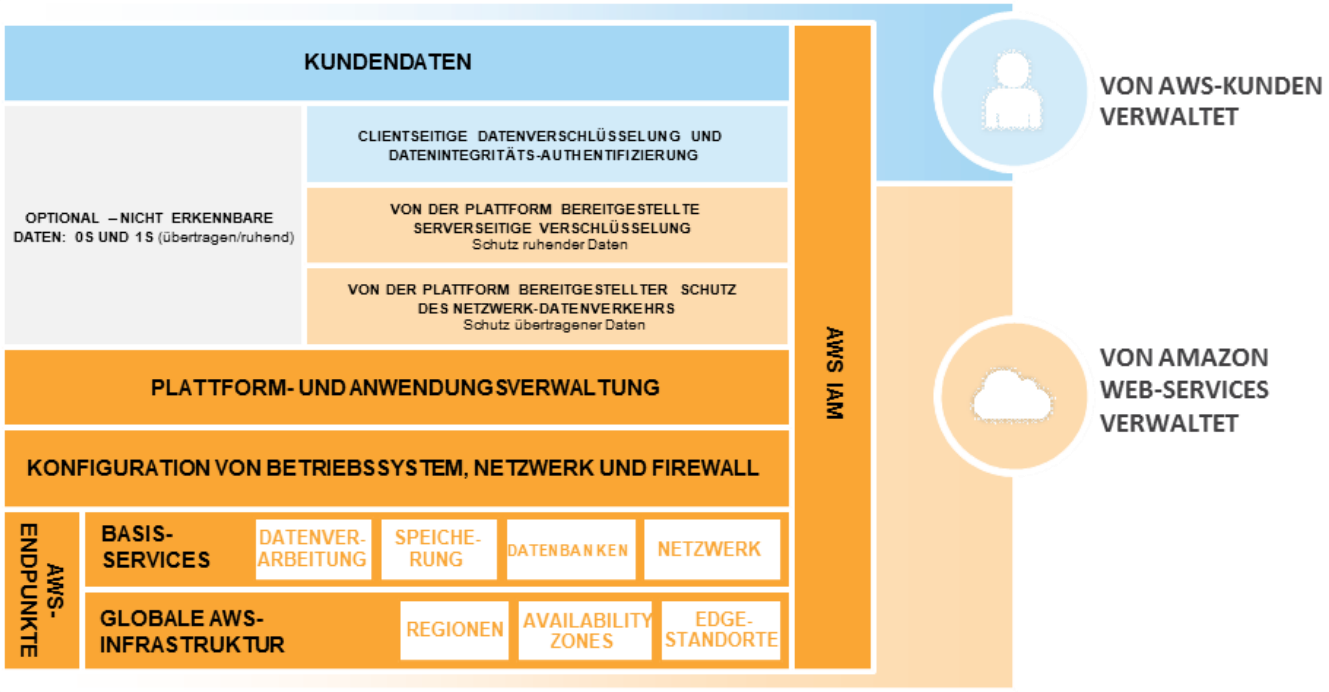

Abbildung 3: Das Modell geteilter Verantwortung für abstrakte Services

Verwenden des Trusted Advisor-Tools

Einige AWS Premium Support-Kategorien beinhalten den Zugriff auf das Trusted Advisor-Tool, das ein umfassendes Abbild der Konfiguration Ihrer Services bereitstellt und bei der Identifizierung gängiger fehlerhafter Sicherheitskonfigurationen hilft, Vorschläge zur Verbesserung der Systemleistung macht und nicht ausgelastete Ressourcen erkennt. In diesem Whitepaper werden die Sicherheitsaspekte bezüglich Trusted Advisor behandelt, die für Amazon EC2 gelten.

Trusted Advisor überprüft die Einhaltung der folgenden Sicherheitsempfehlungen:

- Begrenzen Sie den Zugang zu allgemeinen Verwaltungsports auf eine kleine Teilmenge von Adressen. Das betrifft die Ports 22 (SSH), 23 (Telnet), 3389 (RDP) und 5500 (VNC).
- Beschränken Sie den Zugang zu allgemeinen Datenbankports. Das betrifft die Ports 1433 (MSSQL Server), 1434 (MSSQL Monitor), 3306 (MySQL), Oracle (1521) und 5432 (PostgreSQL).
- Konfigurieren Sie IAM derart, dass eine sichere Kontrolle der Zugriffe auf AWS-Ressourcen sichergestellt ist.
- Aktivieren Sie das Multi-Factor Authentication (MFA)-Token und damit die Zwei-Faktor-Authentifizierung für das AWS-Stammkonto.

Definieren und Kategorisieren von AWS-Komponenten

Bevor Sie Ihr ISMS entwerfen, sollten Sie alle Informationskomponenten identifizieren, die Sie schützen müssen. Entwickeln Sie dann eine technisch und finanziell tragfähige Lösung für den Schutz dieser Komponenten. Sollte es sich als schwierig erweisen, jede Komponente in finanzieller Hinsicht zu quantifizieren, können Sie qualitative Kennwerte (wie vernachlässigbar/niedrig/mittel/hoch/sehr hoch) verwenden.

Es gibt zwei Arten von Komponenten:

- Essenzielle Elemente, beispielsweise Geschäftsinformationen, Prozesse und Aktivitäten
- Komponenten zur Unterstützung der essenziellen Elemente, beispielsweise Hardware, Software, Personal, Standorte und Partnerunternehmen

Tabelle 1 zeigt Beispiele für Komponenten.

Bezeichnung der Komponente	Verantwortlich für die Komponente	Kategorie der Komponente	Abhängigkeiten	Kosten
Kundenorientierte Website-Anwendungen	E-Commerce-Team	Essenziell	EC2, Elastic Load Balancing, RDS, Entwicklung, Operationen, Qualitätssicherung	Bereitstellung, Austausch, Wartung, Kosten/Konsequenzen bei Verlust.
Kreditkartendaten von Kunden	E-Commerce-Team	Essenziell	PCI-Karteninhaberumgebung, Verschlüsselung, AWS-PCI-Dienstanbieterzertifizierung	
Personaldaten	COO	Essenziell	Amazon RDS, Verschlüsselungsanbieter, DevOps-IT, Fremdsoftwareanbieter	
Datenarchiv	COO	Essenziell	S3, Glacier, DevOps-IT	
HRM-System	Personalabteilung	Essenziell	EC2, S3, RDS, DevOps-IT, Fremdsoftwareanbieter	
AWS Direct Connect-Infrastruktur	CIO	Netzwerk	Netzwerkbetreiber, Telekommunikationsanbieter, AWS Direct Connect	
Business Intelligence (BI)-Infrastruktur	BI-Team	Software	EMR, Redshift, Dynamo DB, S3, DevOps	
BI-Services	COO	Essenziell	BI-Infrastruktur, BI-Analyseteams	
LDAP-Verzeichnis	IT-Sicherheitsteam	Sicherheit	EC2, IAM, eigene Software, DevOps	
Windows AMI	Server-Team	Software	EC2, Patch-Management-Software, DevOps	
Anmeldeinformationen von Kunden	Compliance-Team	Sicherheit	Tägliche Updates, Archivierungsinfrastruktur	

Tabelle 1: Beispiele für Komponenten

Entwerfen Sie Ihr eigenes ISMS zum Schutz Ihrer Komponenten auf AWS

Nachdem Sie Komponenten, Kategorien und Kosten ermittelt haben, etablieren Sie einen Standard für Implementierung, Betrieb, Monitoring, Überprüfung, Wartung und Verbesserung Ihres Informationssicherheits-Managementsystems (ISMS) auf AWS. Sicherheitsanforderungen sind in jedem Unternehmen unterschiedlich und von folgenden Faktoren abhängig:

- Geschäftliche Anforderungen und Ziele
- Verwendete Prozesse
- Größe und Struktur des Unternehmens

Alle diese Faktoren können sich im Laufe der Zeit ändern. Es ist daher empfehlenswert, einen zyklischen Prozess für die Verwaltung diese Informationen einzurichten.

Tabelle 2 enthält einen Vorschlag für den stufenweisen Entwurf und Aufbau eines ISMS in AWS. Für den ISMS-Entwurf und die Implementierung können auch Standard-Frameworks wie ISO 27001 hilfreich sein.

Phase	Aufgabe	Beschreibung
1	**Umfang und Grenzen definieren**	Definieren Sie, welche Regionen, Availability Zones, Instanzen und AWS-Ressourcen integriert werden sollen. Wenn Sie eine Komponente ausschließen (zum Beispiel verwaltet AWS die Betriebsanlagen, so dass Sie diese Funktion im eigenen ISMS nicht benötigen), geben Sie explizit an, welche Komponente ausgeschlossen wurde und warum.
2	**ISMS-Richtlinie definieren**	Berücksichtigen Sie Folgendes: • Zielrichtung und Handlungsgrundsätze in Bezug auf Informationssicherheit • Gesetzliche, vertragliche und regulatorische Anforderungen • Risikomanagementziele für das Unternehmen • Methode zur Risikobewertung • Stellungnahme des Managements zum Plan
3	**Methode zur Risikobewertung auswählen**	Wählen Sie eine Methode zur Risikobewertung, basierend auf den Informationen, die Sie von den entsprechenden Gruppen im Unternehmen zu den folgenden Themen erhalten haben: • Geschäftliche Anforderungen • Anforderungen bezüglich der Informationssicherheit • Fähigkeiten in Bezug auf Informationstechnologie und deren Anwendung • Rechtliche Anforderungen • Regulatorische Verantwortlichkeit Weil eine öffentliche Cloud-Infrastruktur anders funktioniert als Legacy-Umgebungen, ist es wichtig, Kriterien für die Übernahme von Risiken und die Ermittlung des akzeptablen Risikoniveaus (Risikotoleranzen) festzulegen.

Phase	Aufgabe	Beschreibung
		Wir empfehlen, mit einer Risikobewertung und deren Automatisierung so früh wie möglich zu beginnen. Durch Verwendung des automatischen AWS-Risikomanagements kann der Umfang der für das Risikomanagement erforderlichen Ressourcen verringert werden. Es gibt mehrere Methoden und Anleitungen zur Risikobewertung, beispielsweise Oktave (Operationally Critical Threat, Asset, and Vulnerability Evaluation), ISO 31000:2009 Risk Management, ENISA (European Network and Information Security Agency), IRAM (Information Risk Analysis Methodology) und eine National Institute of Standards & Technology (NIST)-Sonderveröffentlichung (800-30 Revision 1: Guide for Conducting Risk Assessments).
4	**Risiken ermitteln**	Wir empfehlen, dass Sie zunächst alle bedrohten Komponenten in einem Risikoregister aufführen. Anschließend erstellen Sie auf Grundlage der Ergebnisse einer Schwachstellen- und Auswirkungsanalyse eine neue Risikomatrix für jede AWS-Umgebung. Hier ein Beispiel für die Struktur eines Risikoregisters: • Komponenten • Bedrohungen für diese Komponenten • Sicherheitslücken, die durch diese Bedrohungen ausgenutzt werden könnten • Konsequenzen, wenn diese Sicherheitslücken ausgenutzt werden
5	**Risiken analysieren und bewerten**	Analysieren und bewerten Sie Risiken anhand folgender Kriterien: Auswirkung auf das Geschäft, Wahrscheinlichkeit und Risikostufe
6	**Risiken behandeln**	Wählen Sie Optionen für die Behandlung von Risiken. Mögliche Optionen: Anwenden von Sicherheitskontrollen, Akzeptieren von Risiken, Vermeiden von Risiken, Transferieren von Risiken
7	**Sicherheitskontrollrahmen auswählen**	Verwenden Sie für die Auswahl Ihrer Sicherheitskontrollen ein Framework wie ISO 27002, NIST SP 800-53, COBIT (Control Objectives for Information and related Technology) oder CSA-CCM (Cloud Security Alliance-Cloud Control Matrix). Diese Frameworks umfassen eine Reihe von bewährten Methoden und können Ihnen dabei helfen, entsprechende Kontrollelemente auszuwählen.
8	**Einwilligung des Managements einholen**	Auch nachdem Sie alle Kontrollelemente implementiert haben, verbleibt ein Restrisiko. Wir empfehlen, dass Sie sich vom Management die Möglichkeit von Restrisiken bestätigen lassen und die Genehmigung für die Implementierung und den Betrieb des ISMS einholen.

Phase	Aufgabe	Beschreibung
9	**Erklärung zur Anwendbarkeit abgeben**	Erstellen Sie eine Erklärung zur Anwendbarkeit, die folgende Informationen enthält: • Welche Kontrollelemente wurden ausgewählt und warum • Welche Kontrollelemente sind implementiert • Welche Kontrollelemente sollen implementiert werden • Welche Kontrollelemente wurden ausgeschlossen und warum

Tabelle 2: Phasen bei der ISMS-Erstellung

Verwalten von AWS-Konten, IAM-Benutzern, Gruppen und Rollen

Benutzer dürfen nur auf die Ressourcen zugreifen können, die sie benötigen, aber keine weitergehenden Berechtigungen besitzen. Dies sicherzustellen ist eine wichtige Aufgabe jedes ISMS. Diese Vorgabe können Sie mit IAM realisieren. Dazu *erstellen Sie IAM-Benutzer* unter Ihrem AWS-Konto. Diesen können Sie dann direkt Berechtigungen zuweisen. Oder ordnen Sie diese Benutzer einer Gruppe zu, der Sie Berechtigungen zuweisen. Hier weitere Details zu AWS-Konten und IAM-Benutzern:

- **AWS-Konto.** Dies ist das Konto, das Sie erstellen, wenn Sie sich erstmals bei AWS anmelden. Ihr AWS-Konto stellt eine Geschäftsbeziehung zwischen Ihnen und AWS dar. Sie nutzen Ihr AWS-Konto, um Ihre AWS-Ressourcen und -Services zu verwalten. AWS-Konten besitzen Root-Rechte für alle AWS-Ressourcen und -Services, sie sind also sehr mächtig. Verwenden Sie Root-Anmeldeinformationen nicht für die täglichen Interaktionen mit AWS. Es ist möglich, dass Ihr Unternehmen mehrere AWS-Konten besitzt, beispielsweise eines für jede größere Abteilung, und dann unter diesen AWS-Konten IAM-Benutzer für die entsprechenden Personen und Ressourcen einrichtet.
- **IAM-Benutzer.** Mit IAM können Sie mehrere Benutzer mit jeweils individuellen Sicherheits-Anmeldeinformationen einrichten, die alle unter einem AWS-Konto verwaltet werden. IAM-Benutzer kann eine Person, ein Service oder eine Anwendung sein, die über die Management Console, CLI oder direkt über APIs auf Ihre AWS-Ressourcen zugreifen muss. Es ist eine bewährte Methode, für jede Person oder Software, die Zugriff auf Services und Ressourcen Ihres AWS-Kontos benötigt, einen eigenen IAM-Benutzer einzurichten. *Erstellen Sie fein abgestimmte Berechtigungen für die Ressourcen unter Ihrem AWS-Konto, richten Sie Gruppen ein, erteilen sie diesen die jeweiligen Berechtigungen und ordnen Sie dann die Benutzer einer Gruppe zu.* Diese bewährte Methode hilft sicherzustellen, dass Benutzer nur genau die Berechtigungen besitzen, die sie für ihre Aufgaben benötigen.

Strategien für die Verwendung mehrerer AWS-Konten

Gestalten Sie Ihre Strategie für AWS-Konten im Hinblick auf maximale Sicherheit und entsprechend Ihren geschäftlichen und organisatorischen Anforderungen.

In Tabelle 3 sind mögliche Strategien aufgeführt.

Geschäftliche Anforderung	Vorgeschlagener Entwurf	Kommentar
Zentrale Sicherheitsverwaltung	Einzelnes AWS-Konto	Damit zentralisieren Sie die Verwaltung der Informationssicherheit und minimieren den Overhead.
Trennung von Produktions-, Entwicklungs- und Testumgebungen	Drei AWS-Konten	Erstellen Sie für Produktion, Entwicklung und Tests jeweils ein eigenes AWS-Konto.
Mehrere unabhängige Abteilungen	Mehrere AWS-Konten	Erstellen Sie für jede autonome Abteilung des Unternehmens ein eigenes AWS-Konto. Sie können dann unter jedem Benutzerkonto Berechtigungen und Richtlinien zuordnen.
Zentrale Sicherheitsverwaltung mit mehreren autonomen Projekten	Mehrere AWS-Konten	Erstellen Sie ein einzelnes AWS-Konto für gemeinsame Projektressourcen (wie DNS-Dienste, Active Directory, CMS usw.). Dann erstellen Sie separate AWS-Konten pro Projekt. Sie können nun Berechtigungen und Richtlinien unter jedem Projektkonto zuweisen und den Zugriff auf Ressourcen kontoübergreifend gewähren.

Tabelle 3: Strategien für AWS-Konten

Sie haben die Möglichkeit, eine konsolidierte Abrechnung über mehrere Konten zu konfigurieren, sodass Sie nicht für jedes Konto eigene Rechnungen verwalten müssen und zudem Skaleneffekte nutzen können. Wenn Sie Rechnungskonsolidierung verwenden, werden die Ressourcen und die Anmeldeinformationen nicht zwischen Konten geteilt.

Verwalten von IAM-Benutzern

IAM-Benutzer mit der entsprechenden Berechtigungsstufe dürfen neue IAM-Benutzer erstellen oder bestehende verwalten und löschen. Diese hoch privilegierten IAM-Benutzer können für jede Person, jeden Service und jede Anwendung innerhalb des Unternehmens einen bestimmten IAM-Benutzer anlegen, der die AWS-Konfiguration verwalten und direkt auf AWS-Ressourcen zugreifen kann. Wir raten dringend von der Verwendung gemeinsamer Benutzeridentitäten (mehreren Personen sind die gleichen Anmeldeinformationen zugeordnet) ab.

Verwalten von IAM-Gruppen

IAM-Gruppen sind Sammlungen von IAM-Benutzern in einem AWS-Konto. Erstellen Sie IAM-Gruppen auf funktioneller, organisatorischer oder regionaler Basis (beispielsweise pro Projekt) oder entsprechend der Voraussetzung, nach der IAM-Benutzer auf gleichartige AWS-Ressourcen zugreifen müssen, um ihre Arbeit erledigen zu können. Gewähren Sie jeder IAM-Gruppe Berechtigungen für den Zugriff auf AWS-Ressourcen, indem Sie ihr eine oder mehrere IAM-Richtlinien zuweisen. Alle einer IAM-Gruppe zugeordneten Richtlinien werden von den IAM-Benutzern, die Mitglieder der Gruppe sind, geerbt.

Beispiel: Der IAM-Benutzer John ist für Backups innerhalb des Unternehmens verantwortlich und muss auf Objekte im Amazon S3-Bucket `Archives` zugreifen. Sie könnten John die Berechtigung für den Zugriff auf `Archives` direkt erteilen. Später sollen jedoch auch Sally und Betty in das Team von John aufgenommen werden. Dann müssten Sie auch ihnen individuell die Berechtigung für den Zugriff auf `Archives` erteilen. Einfacher und besser zu verwalten ist es jedoch, wenn Sie die Berechtigung einer Gruppe zuweisen und dann John, Sally und Betty in diese Gruppe aufnehmen. Wenn weitere Benutzer den gleichen Zugriff benötigen, ordnen Sie diese einfach der Gruppe zu. Sollte ein Benutzer den Zugriff auf eine Ressource nicht mehr benötigen, entfernen Sie ihn aus der Gruppe, die den Zugriff auf diese Ressource ermöglicht.

IAM-Gruppen sind ein leistungsfähiges Werkzeug für die Verwaltung des Zugriffs auf AWS-Ressourcen. Selbst wenn nur ein Benutzer Zugriff auf eine bestimmte Ressource benötigt, ist es eine bewährte Methode, für diesen Zugriff eine eigene AWS-Gruppe einzurichten. Sie sollten Berechtigungen und Richtlinien nur an Gruppen zuweisen und den Zugriff auf Ressourcen nur über eine Gruppenmitgliedschaft ermöglichen.

Verwalten von Anmeldeinformationen

Jedes AWS-Konto und jeder IAM Benutzer ist einzigartig und verfügt über dauerhafte Anmeldeinformationen. Für diese Identitäten gibt es zwei Haupttypen von Anmeldeinformationen. Der erste Typ dient zur Anmeldung bei der AWS Management Console und bei AWS-Portalseiten, der zweite Typ ermöglicht programmgesteuerten Zugriff auf die AWS-APIs.

Die beiden Anmeldeinformationstypen werden in Tabelle 4 erläutert.

Anmeldeinformation Typ 1	Details
Benutzername/Passwort	Benutzernamen für AWS-Konten sind immer E-Mail-Adressen. IAM-Benutzernamen ermöglichen mehr Flexibilität. Für ein AWS-Kontopasswort sind beliebige Informationen verwendbar. Für IAM-Benutzerpasswörter kann festgelegt werden, dass sie einer Richtlinie entsprechen müssen (die beispielsweise die Passwortlänge oder die erlaubten Zeichen vorgibt).
Multi-Factor Authentication (MFA)	Multi-Factor Authentication (MFA) bietet eine zusätzliche Sicherheitsschicht für Anmeldeinformationen. Ist MFA aktiviert, wird ein Benutzer bei der Anmeldung auf einer AWS-Website sowohl nach Benutzernamen und Passwort gefragt (der erste Faktor – etwas, was der Benutzer weiß) als auch nach einem Authentifizierungscode aus seinem MFA-Gerät (der zweite Faktor – etwas, was der Benutzer besitzt). Sie können MFA auch verwenden, wenn Benutzer S3-Objekte löschen möchten. Wir empfehlen ihnen, MFA für Ihr AWS-Konto und Ihre IAM-Benutzer zu aktivieren, um unbefugten Zugriff auf Ihre AWS-Umgebung zu verhindern. Derzeit unterstützt AWS die MFA-Hardware der Firma Gemalto sowie virtuelle MFA-Geräte in Form von Smartphone-Anwendungen.

Tabelle 4: Anmeldeinformationstypen

In Tabelle 5 werden Anmeldeinformationstypen für den programmgesteuerten Zugriff auf APIs erläutert.

Anmeldeinformation Typ 2	Details
Zugriffsschlüssel	Zugriffschlüssel werden verwendet, um API-Aufrufe von AWS-Services digital zu signieren. Jeder Zugriffschlüssel besteht aus einer Zugriffsschlüssel-ID und einem geheimen Schlüssel. Der geheime Schlüssel muss vom Besitzer (AWS-Kontoinhaber oder IAM-Benutzer) gesichert werden. Benutzer können zu jeder Zeit zwei Sätze aktiver Zugriffsschlüssel besitzen. Als bewährte Methode sollten die Benutzer ihre Zugriffsschlüssel regelmäßig wechseln.
MFA für API-Aufrufe	Bei einem durch Multi-Factor Authentication (MFA) geschützten API-Zugriff müssen IAM-Benutzer einen gültigen MFA-Code eingeben, bevor sie bestimmte Funktionen, bei denen es sich um APIs handelt, verwenden können. Durch Richtlinien, die Sie in IAM erstellen, wird festgelegt, welche APIs durch MFA geschützt sind. Da AWS-Service-APIs über die AWS Management Console aufgerufen werden, können Sie MFA in jedem Fall für APIs erzwingen, gleichgültig, ob sie über die Konsole oder über APIs aufgerufen werden.

Tabelle 5: Anmeldeinformationstypen für programmgesteuerten Zugriff

Delegieren der Zugriffsberechtigung mithilfe von IAM-Rollen und temporären Sicherheits-Anmeldeinformationen

Es gibt Szenarien, in denen Sie eine Zugriffsberechtigung an Benutzer oder Services delegieren müssen, die normalerweise keinen Zugriff auf Ihre AWS-Ressourcen haben. Die nachstehende Tabelle 6 enthält häufige Anwendungsfälle, in denen solche Zugriffsübertragungen erforderlich sind.

Anwendungsfall	Beschreibung
Anwendungen, die auf Amazon EC2-Instanzen ausgeführt werden und auf AWS-Ressourcen zugreifen müssen	Anwendungen, die auf einer Amazon EC2-Instanz ausgeführt werden und auf AWS-Ressourcen wie Amazon S3-Buckets oder eine Amazon DynamoDB-Tabelle zugreifen müssen, benötigen Sicherheits-Anmeldeinformationen, um programmgesteuert Anforderungen an AWS richten zu können. Entwickler können ihre Anmeldeinformationen einer Instanz und Anwendung zuweisen und diese Anmeldeinformationen dann für den Zugriff auf Ressourcen nutzen, aber eine solche Verteilung von dauerhaften Anmeldeinformationen auf Instanzen ist schwer zu verwalten und stellt ein potenzielles Sicherheitsrisiko dar.
Kontoübergreifender Zugriff	Um den Zugang zu Ressourcen zu verwalten, haben Sie möglicherweise mehrere AWS-Konten eingerichtet, etwa um eine Entwicklungsumgebung von einer Produktionsumgebung zu isolieren. Es kann aber erforderlich sein, dass Benutzer eines Kontos Zugriff auf die Ressourcen eines anderen Kontos benötigen, beispielsweise um ein Update aus der Entwicklungsumgebung in die Produktionsumgebung zu übertragen. Solche Benutzer benötigen eigene Identitäten für jedes Konto. Die Verwaltung von Anmeldeinformationen für mehrere Konten erschwert jedoch die Identitätsverwaltung.

Identitätsverbund (Identity Federation)	Wahrscheinlich gibt es Benutzer, die bereits Identitäten außerhalb des AWS besitzen, etwa in einem Firmenverzeichnis. Möglicherweise müssen solche Benutzer auch mit AWS-Ressourcen arbeiten (oder mit Anwendungen, die auf diese Ressourcen zugreifen). Wenn das der Fall ist, benötigen diese Benutzer ebenfalls AWS-Anmeldeinformationen.

Tabelle 6: Häufige Anwendungsfälle, die Zugriffsübertragungen erfordern

Für solche Fälle sind IAM-Rollen und temporäre Sicherheits-Anmeldeinformationen vorgesehen. Eine IAM-Rolle ermöglicht, eine Anzahl von Berechtigungen für die Ressourcen zu definieren, die ein Benutzer oder ein Service benötigt, wobei diese Berechtigungen nicht mit einem bestimmten IAM- Benutzer oder einer IAM-Gruppe verknüpft sind. Stattdessen können IAM-Benutzer, mobile oder EC2-basierte Anwendungen oder AWS-Services (wie Amazon EC2) programmgesteuert eine Rolle übernehmen. Die Rolle kann temporäre Sicherheits-Anmeldeinformationen enthalten, die vom Benutzer oder der Anwendung genutzt werden können, um programmgesteuerte Anfragen an AWS zu richten. Diese temporären Sicherheits-Anmeldeinformationen besitzen eine konfigurierbare Laufzeit und werden automatisch gewechselt. Wenn Sie IAM-Rollen und temporäre Sicherheits-Anmeldeinformationen verwenden, müssen Sie keine dauerhaften Anmeldeinformationen und IAM-Benutzer für jede Entität verwalten, die Zugriff auf eine Ressource benötigt.

IAM-Rollen für Amazon EC2

IAM-Rollen für Amazon EC2 sind spezifische Implementierungen von IAM-Rollen für den ersten Anwendungsfall in Tabelle 6. In der folgenden Abbildung führt ein Entwickler auf einer Amazon EC2-Instanz eine Anwendung aus, die Zugriff auf ein Amazon S3-Bucket mit dem Namen `photos` benötigt. Ein Administrator erstellt die `Get-pics`-Rolle. Die Rolle enthält Richtlinien, die Leseberechtigungen für den Bucket gewähren und es dem Entwickler gestatten, die Rolle auf einer Amazon EC2-Instanz zu starten. Wenn die Anwendung auf der Instanz ausgeführt wird, kann sie mithilfe der temporären Anmeldeinformationen der Rolle auf den `photos`-Bucket zugreifen. Der Administrator muss dem Entwickler keine Berechtigung für den Zugriff auf den `photos`-Bucket gewähren, und der Entwickler muss die Anmeldeinformationen nie teilen.

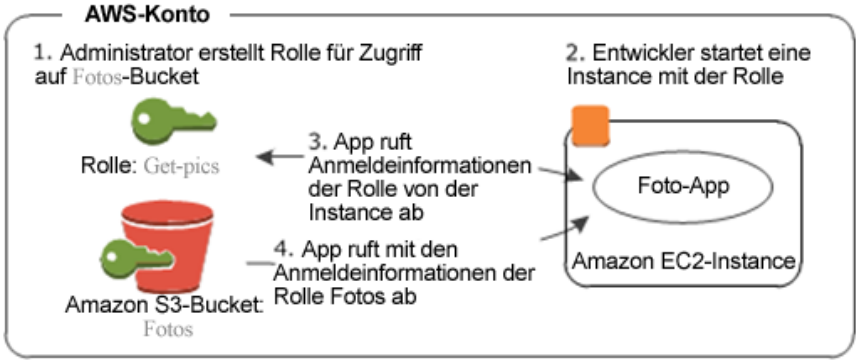

Abbildung 4: Funktionsweise von EC2-Rollen

1. Ein Administrator erstellt mit IAM die `Get-pics`-Rolle. Für die Rolle definiert der Administrator eine Richtlinie, welche festlegt, dass nur Amazon EC2-Instanzen die Rolle übernehmen können, und dass für den `photos`-Bucket nur Leserechte gelten.

2. Ein Entwickler startet eine Amazon EC2-Instanz und verknüpft die `Get-pics`-Rolle mit dieser Instanz.

3. Wenn die Anwendung ausgeführt wird, übernimmt sie die Anmeldeinformationen aus den Metadaten der Amazon EC2-Instanz.

4. Mithilfe der Anmeldeinformationen der Rolle greift die Anwendung auf den schreibgeschützten `photo`-Bucket zu.

Kontoübergreifender Zugriff

Sie können IAM-Rollen für den zweiten Anwendungsfall in Tabelle 6 verwenden, indem Sie IAM-Benutzern eines anderen AWS-Kontos den Zugriff auf Ressourcen in Ihrem AWS-Konto ermöglichen. Dieser Vorgang wird als kontoübergreifender Zugriff bezeichnet. Kontoübergreifender Zugriff ermöglicht Ihnen, den Zugriff auf Ihre Ressourcen mit Benutzern in anderen AWS-Konten zu teilen.

Um kontoübergreifenden Zugriff im vertrauenden Konto (Konto A) einzurichten, erstellen Sie eine IAM-Richtlinie, die dem vertrauten Konto (Konto B) den Zugriff auf bestimmte Ressourcen gewährt. Konto B kann diesen Zugriff dann an seine IAM-Benutzer delegieren. Konto B kann an seine IAM-Benutzer nur die Berechtigungen delegieren, die es von Konto A erhalten hat, aber keine weitergehenden.

Identitätsverbund

Sie können IAM-Rollen für den dritten Anwendungsfall in Tabelle 6 verwenden, indem Sie einen Identitäts-Broker erstellen, der zwischen den Unternehmensnutzern und Ihren AWS-Ressourcen agiert und den Authentifizierungs- und Autorisierungprozess verwaltet, ohne dass alle Ihre Benutzer nochmals als IAM-Benutzer in AWS angelegt werden müssen.

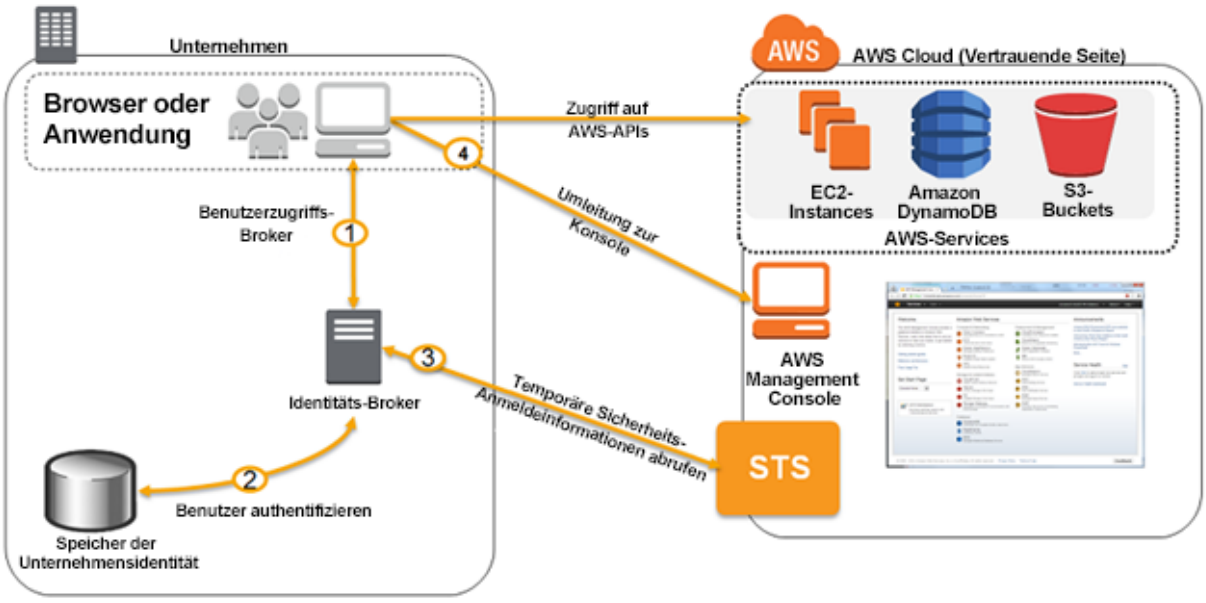

Abbildung 5: AWS-Identitätsverbund mit temporären Sicherheits-Anmeldeinformationen

1. Der Unternehmensnutzer greift auf die Identitäts-Broker-Anwendung zu.

2. Die Identitäts-Broker-Anwendung authentifiziert die Benutzer mithilfe der Identitäts-Datenbank des Unternehmens.

3. Die Identität Broker-Anwendung hat die Berechtigung, auf den AWS Security Token Service (STS) zugreifen, um temporäre Sicherheits-Anmeldeinformationen abzurufen.

4. Unternehmensnutzer können eine temporäre URL abrufen, die ihnen den Zugang zu den AWS-APIs oder der Management Console ermöglicht.

Eine Identitäts-Broker-Beispielanwendung für die Verwendung mit Microsoft Active Directory wird von AWS zur Verfügung gestellt.

Verwalten des Zugriffs auf Amazon EC2-Instanzen auf Betriebssystemebene

Im vorherigen Abschnitt wurde beschrieben, auf welche Weise Sie den Zugriff auf Ressourcen verwalten, die eine Authentifizierung für AWS-Services erfordern. Für den Zugriff auf das Betriebssystem Ihrer EC2-Instanzen benötigen Sie jedoch andere Anmeldeinformationen. Im Modell geteilter Verantwortung sind Sie verantwortlich für die Anmeldeinformationen für das Betriebssystem. AWS unterstützt Sie beim erstmaligen Zugriff auf das Betriebssystem.

Wenn Sie eine neue Amazon EC2-Instanz aus einem Standard-AMI starten, können Sie auf diese Instanz mithilfe sicherer Netzwerkprotokolle zugreifen, beispielsweise mit Secure Shell (SSH) oder Windows Remote Desktop Protocol (RDP). Sie müssen sich auf der Betriebssystemebene erfolgreich authentifizieren, bevor Sie die Amazon EC2-Instanz nutzen und konfigurieren können. Nachdem Sie sich authentifiziert haben und der Remotezugriff auf die Amazon EC2-Instanz möglich ist, richten Sie einen beliebigen Authentifizierungsmechanismus für das Betriebssystem ein, beispielsweise X.509-Zertifikat-Authentifizierung, Microsoft Active Directory oder lokale Betriebssystemkonten.

Für die Authentifizierung bei der EC2-Instanz bietet AWS asymmetrische Schlüsselpaare an, Amazon EC2-Schlüsselpaare genannt. Dabei handelt es sich um RSA-Schlüsselpaare nach Industriestandard. Jeder Benutzer kann mehrere Amazon EC2-Schlüsselpaare besitzen und neue Instanzen mit unterschiedlichen Schlüsselpaaren starten. EC2-Schlüsselpaare haben keinen Bezug zu den zuvor vorgestellten Anmeldeinformationen für das AWS-Konto oder für IAM-Benutzer. Diese Anmeldeinformationen steuern den Zugang zu anderen AWS-Services, während EC2-Schlüsselpaare nur für den Zugriff auf Ihre spezielle Instanz gelten.

Sie können auch Ihre eigenen Amazon EC2-Schlüsselpaare mit Industriestandard-Tools wie OpenSSL generieren. Sie generieren das Schlüsselpaar in einer sicheren und vertrauenswürdigen Umgebung. Nur der öffentliche Schlüssel des Schlüsselpaares wird in AWS importiert – den privaten Schlüssel müssen Sie selbst sicher speichern. Wir empfehlen für die Generierung von Schlüsseln die Verwendung eines hochwertigen Zufallszahlengenerators.

Sie haben auch die Möglichkeit, Amazon EC2-Schlüsselpaare von AWS generieren zu lassen. In diesem Fall werden Ihnen sowohl der private als auch der öffentliche Schlüssel des RSA-Schlüsselpaar angezeigt, wenn Sie die Instanz erstmals erstellen. Sie müssen den privaten Schlüssel des Amazon EC2-Schlüsselpaars herunterladen und sicher speichern. AWS speichert den privaten Schlüssel nicht – geht er verloren, müssen Sie ein neues Schlüsselpaar generieren.

Für Amazon EC2 Linux-Instanzen, die den **cloud-init**-Service verwenden, gilt Folgendes: Beim Start einer neuen Instanz von einem Standard-AWS-AMI wird der öffentliche Schlüssel des Amazon EC2-Schlüsselpaars an die ursprüngliche **~/.ssh/authorized_keys**-Datei des Betriebssystembenutzers angefügt. Dieser Benutzer kann dann einen SSH-Client verwenden, um sich mit der Amazon EC2-Linux-Instanz zu verbinden. Dazu muss er den Client so konfigurieren, dass für dessen Identität der korrekte Benutzername für die Amazon EC2-Instanz verwendet wird (beispielsweise ec2-user), und zudem muss die Datei mit dem privaten Schlüssel für die Benutzerauthentifizierung bereitgestellt werden.

Für Amazon EC2 Windows-Instanzen, die den **ec2config**-Service verwenden, gilt Folgendes: Wenn eine neue Instanz von einem Standard-AWS-AMI gestartet wird, legt der **ec2config**-Service ein neues zufälliges Administratorpasswort für die Instanz fest und verschlüsselt dieses mit dem öffentlichen Schlüssel des entsprechenden Amazon EC2-Schlüsselpaars. Der Benutzer kann das Passwort für die Windows-Instanz mit der AWS Management Console oder mit Befehlszeilen-Tools abrufen und durch die Bereitstellung des entsprechenden privaten Amazon EC2-Schlüssels entschlüsseln. Dieses Passwort kann zusammen mit dem Standard-Administratorkonto für die Amazon EC2-Instanz verwendet werden, um die Windows-Instanz zu authentifizieren.

AWS bietet eine Reihe flexibler und praktischer Werkzeuge für die Verwaltung von Amazon EC2-Schlüsseln und stellt Authentifizierung nach Industriestandard für neu gestartete Amazon EC2-Instanzen bereit. Wenn Sie höhere Sicherheitsanforderungen haben, können Sie alternative Authentifizierungsmechanismen wie LDAP- oder Active Directory-Authentifizierung implementieren und die Authentifizierung mit Amazon EC2-Schlüsselpaaren deaktivieren.

Sichern Ihrer Daten

In diesem Abschnitt wird der Schutz von ruhenden Daten und Daten in Transit auf der AWS-Plattform behandelt. Wir gehen davon aus, dass Sie Ihre Komponenten bereits identifiziert und klassifiziert haben und für diese Komponenten Schutzziele auf der Grundlage ihrer Risikoprofile festgelegt wurden.

Zugriff auf Ressourcen Autorisieren

Nachdem ein Benutzer oder eine IAM-Rolle authentifiziert wurde, können diese Identitäten auf die Ressourcen zugreifen, zu denen sie berechtigt sind. Sie stellen diese Berechtigungen mithilfe von Ressourcen- oder Ausführungsrichtlinien bereit, je nachdem, ob der Benutzer über die Ressourcen verfügen soll oder bestimmte Benutzerkontrollen ändern darf.

- **Ressourcenrichtlinien** beziehen sich auf den Fall, dass der Benutzer Ressourcen erstellt und dann anderen Benutzern die Erlaubnis erteilen möchte, auf diese Ressourcen zuzugreifen. In dieser Situation wird die Richtlinie direkt der Ressource zugeordnet und beschreibt, wer und auf welche Weise darüber verfügen kann. Der Benutzer kontrolliert die Ressource. Sie können einem IAM-Benutzer expliziten Zugriff auf eine Ressource gewähren. Das AWS-Root-Konto hat immer die Kontrolle über Ressourcenrichtlinien und ist verantwortlich für alle in diesem Konto erstellten Ressourcen. Alternativ können Sie Benutzern explizit gestatten, die Berechtigungen für eine Ressource zu verwalten.
- **Ausführungsrichtlinien** (in der IAM-Dokumentation als „Benutzer-basierte Berechtigungen“ bezeichnet) werden oft verwendet, um unternehmensweite Zugriffsrichtlinien durchzusetzen. Ausführungsrichtlinien werden einem IAM-Benutzer entweder direkt oder indirekt über eine IAM-Gruppe zugeordnet. Sie lassen sich auch einer Rolle zuweisen, die zur Laufzeit angenommen wird. Ausführungsrichtlinien definieren, welche Aktionen der Benutzer ausführen darf und welche nicht. Zudem können Ausführungsrichtlinien ressourcenbasierte Berechtigungen außer Kraft setzen, indem sie diese explizit aufheben.
- Mit IAM-Richtlinien kann der Zugriff auf Grundlage bestimmter Bedingungen eingeschränkt werden, beispielsweise anhand eines bestimmten IP-Quelladressbereichs oder bestimmter Tage und Tageszeiten.
- Ressourcenrichtlinien und Ausführungsrichtlinien sind kumulativer Natur: Die effektiven Berechtigungen eines einzelnen Benutzers sind die Summe der Berechtigungen aus Ressourcen- und Ausführungsrichtlinien, die entweder direkt oder über eine Gruppenmitgliedschaft erteilt wurden.

Speichern und Verwalten von Schlüsseln in der Cloud

Sicherheitsmaßnahmen, die auf Verschlüsselung beruhen, benötigen Schlüssel. In der Cloud ist es wie in lokalen Systemen von äußerster Wichtigkeit, Schlüssel zu sichern.

Sie können entweder eigene Prozesse verwenden, um Schlüssel in der Cloud zu verwalten, oder die serverseitige Verschlüsselung samt der Schlüsselverwaltung und den Speicherfunktionen von AWS nutzen.

Wenn Sie sich entscheiden, Ihre eigenen Schlüsselverwaltungsprozesse verwenden, haben Sie verschiedene Möglichkeiten zum Speichern und Schützen von Schlüsseldaten. Wir empfehlen dringend, Schlüssel in manipulationssicheren Speichern wie einem Hardware-Sicherheitsmodul (HSM) zu speichern. Amazon Web Services bietet mit AWS CloudHSM einen sicheren HSM-Service in der Cloud. Alternativ können Sie HSMs einsetzen, die Schlüssel lokal speichern und darauf über sichere Verbindungen zugreifen. Verwenden Sie beispielsweise Amazon VPC in einem mit IPSec gesicherten VPN (virtuelles privates Netzwerk) oder AWS Direct Connect zusammen mit IPSec.

Lokale HSMs oder CloudHSM sind für eine Vielzahl von Anwendungsfällen und Anwendungen geeignet, beispielsweise für Datenbankverschlüsselung, Digital Rights Management (DRM), Public Key Infrastructure (PKI), Authentifizierung und Autorisierung, Dokumentsignierung und Transaktionsverarbeitung. CloudHSM verwendet derzeit Luna SA HSM von SafeNet. Luna SA entspricht dem Federal Information Processing Standard (FIPS) 140-2 und den Common Criteria EAL4+-Standards. Zudem wird eine Vielzahl von Verschlüsselungsalgorithmen nach Industriestandard unterstützt.

Wenn Sie sich für CloudHSM anmelden, erhalten Sie einen dedizierten Single-Tenant-Zugang zu CloudHSM-Appliances. Jede Appliance wird als Ressource in Ihrer Amazon VPC dargestellt. Sie, nicht AWS, initialisieren und verwalten die kryptografische Domain in CloudHSM. Die kryptografische Domain ist eine logische und physische Sicherheitsgrenze, die den Zugriff auf Ihre Schlüssel beschränkt. Nur Sie kontrollieren Ihre Schlüssel und die von CloudHSM durchgeführten Operationen. AWS-Administratoren verwalten, pflegen und überwachen die Funktionsfähigkeit der CloudHSM-Appliance, haben aber keinen Zugriff auf die kryptografische Domain. Nachdem Sie die kryptografische Domain initialisiert haben, können Sie Clients auf Ihren EC2-Instanzen konfigurieren, die es Anwendungen gestatten, die von CloudHSM bereitgestellten APIs zu verwenden.

Für Ihre Anwendungen stehen die von CloudHSM unterstützen Standard-APIS PKCS#11, MS CAPI und Java JCA/JCE (Java Cryptography Architecture/Java Cryptography Extensions) zur Verfügung. Der CloudHSM-Client stellt die APIs Ihren Anwendungen bereit und implementiert jeden API-Aufruf durch einen Aufruf der CloudHSM-Appliance über eine von beiden Seiten authentifizierte SSL-Verbindung.

Sie können CloudHSMs in mehreren Availability Zones implementieren und mit Replikation zwischen den Zonen für eine hohe Verfügbarkeit und Speicherelastizität sorgen.

Schützen von ruhenden Daten

Möglicherweise sind aus regulatorischen oder geschäftlichen Gründen für Ihre ruhenden Daten, die in Amazon S3, Amazon EBS, Amazon RDS oder anderen AWS-Services gespeichert sind, zusätzliche Schutzmaßnahmen erforderlich.

In Tabelle 7 sind mögliche Bedrohungen aufgeführt, die Sie bei der Implementierung von Schutzmaßnahmen für Daten berücksichtigen sollten, die sich in AWS im Ruhezustand befinden.

Bedrohung	Empfohlene Schutzmaßnahme	Strategie
Versehentliche Offenlegung von Informationen	Bezeichnen Sie die Daten als vertraulich und begrenzen Sie die Anzahl der Benutzer, die darauf zugreifen dürfen. Verwenden Sie AWS-Berechtigungen für den Zugriff auf Ressourcen für Services wie Amazon S3. Verschlüsseln Sie vertrauliche Daten auf Amazon EBS oder Amazon RDS.	Berechtigungen Verschlüsselung auf Datei-, Partitions-, Volume- oder Anwendungsebene
Kompromittierung der Datenintegrität	Verringern Sie das Risiko, dass die Integrität der Daten durch mutwillige oder zufällige Änderungen beeinträchtigt wird, indem Sie Ressourcenberechtigungen verwenden, um die Anzahl der Benutzer zu begrenzen, die Daten ändern dürfen. Aber auch Ressourcenberechtigungen können nicht verhindern, dass ein privilegierter Benutzer Daten versehentlich löscht oder ein Trojaner mit den Anmeldeinformationen des privilegierten Benutzers Daten verändert. Beide Szenarien veranschaulichen die Bedeutung des Prinzips der geringsten Rechte. Verwenden Sie Datenintegritätsprüfungen wie Message Authentication Codes (SHA-1/SHA-2) oder Hash Message Authentication Codes (HMACs), digitale Signaturen, Verschlüsselung oder Authentifizierung (AES-GCM), um veränderte Daten zu finden. Wenn Sie kompromittierte Daten erkennen, stellen Sie diese entweder aus dem Backup wieder her oder aus einer früheren Objektversion, sofern Sie Amazon S3 verwenden.	Berechtigungen Datenintegritätsprüfungen (MAC/HMAC/digitale Signaturen/authentifizierte Verschlüsselung) Backup Versioning (Amazon S3)
Versehentliches Löschen	Die Verwendung geeigneter Berechtigungen und die Berücksichtigung des Prinzips der geringsten Rechte ist der beste Schutz gegen unbeabsichtigtes oder böswilliges Löschen. Für Services wie Amazon S3 ist MFA Delete verfügbar. Damit erzwingen Sie Multi-Factor Authentication vor dem Löschen eines Objekts und stellen sicher, dass nur privilegierte Benutzer auf Amazon S3-Objekte zugreifen können. Wenn Sie kompromittierte Daten erkennen, stellen Sie diese entweder aus dem Backup wieder her oder aus einer früheren Objektversion, sofern Sie Amazon S3 verwenden.	Berechtigungen Backup Versioning (Amazon S3) MFA Delete (Amazon S3)
Eingeschränkte System-, Infrastruktur-,	Im Falle eines Systemausfalls oder einer Naturkatastrophe stellen Sie Ihre Daten aus dem Backup oder aus Repliken wieder her. Einige Services wie Amazon S3 und Amazon	Backup

Bedrohung	Empfohlene Schutzmaßnahme	Strategie
Hardware- oder Software-Verfügbarkeit	DynamoDB bieten eine automatische Datenreplikation zwischen mehreren Availability Zones innerhalb einer Region. Für andere Services müssen Sie selbst die Replikation oder Backups konfigurieren.	Replikation

Tabelle 7: Bedrohungen für ruhende Daten

Analysieren Sie die Bedrohungsszenarien, die auf Sie zutreffen, und wenden Sie die relevanten Schutztechniken wie in Abschnitt *Tabelle 1: Beispiele für Komponenten*

Entwerfen Sie Ihr *eigenes* ISMS zum Schutz Ihrer Komponenten beschrieben an.

In den folgenden Abschnitten wird erläutert, wie Sie verschiedene AWS-Services konfigurieren, um ruhende Daten zu schützen.

Schützen von ruhenden Daten auf Amazon S3

Amazon S3 bietet eine Reihe von Sicherheitsfunktionen für den Schutz von ruhenden Daten, die Sie entsprechend Ihrem Bedrohungsprofil verwenden können. Diese Funktionen sind in Tabelle 8 aufgeführt.

Amazon S3-Funktion	Beschreibung
Berechtigungen	Verwenden Sie neben IAM-Richtlinien auch Berechtigungen auf Bucket- oder Objektebene, um Ressourcen vor unbefugtem Zugriff zu schützen und die Offenlegung von Informationen, die Beeinträchtigung der Datenintegrität oder das Löschen von Daten zu verhindern.
Versioning	Amazon S3 unterstützt das Versioning von Objekten. Versioning ist standardmäßig deaktiviert. Aktivieren Sie Versioning, um eine neue Version für jedes geänderte oder gelöschte Objekt erstellen zu lassen, damit Sie bei Bedarf kompromittierte Objekte wiederherstellen können.
Replikation	Amazon S3 repliziert jedes Objekt in allen Availability Zones innerhalb der jeweiligen Region. Replikation garantiert die Verfügbarkeit von Daten und Services im Fall eines Systemausfalls, bietet aber keinen Schutz gegen versehentliches Löschen oder Beeinträchtigungen der Datenintegrität, da Änderungen in allen Availability Zones repliziert werden, in denen Daten gespeichert sind. Für Amazon S3 stehen mehrere Redundanzoptionen für unterschiedliche Haltbarkeitsanforderungen zu unterschiedlichen Preisen zur Verfügung.
Backup	Amazon S3 unterstützt Datenreplikation und Versioning anstelle des automatischen Backups. Sie können jedoch auf Anwendungsebene Programme verwenden, um Daten aus Amazon S3 in anderen AWS-Regionen oder auf lokalen Backup-Systemen zu speichern.
Verschlüsselung auf dem Server	Amazon S3 unterstützt die serverseitige Verschlüsselung von Benutzerdaten. Serverseitige Verschlüsselung ist für den Endbenutzer transparent. AWS erzeugt einen eindeutigen Schlüssel für jedes Objekt und verschlüsselt es anschließend mit AES-256. Der Schlüssel wird dann mithilfe eines Master-Schlüssels mit AES-256 verschlüsselt und an einem sicheren Ort gespeichert. Der Master-Schlüssel wird regelmäßig gewechselt.

Amazon S3-Funktion	Beschreibung
Verschlüsselung auf dem Client	Bei clientseitiger Verschlüsselung erstellen und verwalten Sie Ihre eigenen Schlüssel. Von Ihnen erstellte Schlüssel werden nicht im Klartext nach AWS exportiert. Ihre Anwendungen verschlüsseln Daten, bevor sie diese zu Amazon S3 senden, und entschlüsseln Daten, nachdem sie diese von Amazon S3 abgerufen haben. Daten werden in verschlüsselter Form gespeichert, Schlüssel und Algorithmen sind nur Ihnen bekannt. Sie können jeden Verschlüsselungsalgorithmus und symmetrische oder asymmetrische Schlüssel verwenden, um Daten zu verschlüsseln. Dagegen bietet das von AWS bereitgestellt Java SDK clientseitige Amazon S3-Verschlüsselungsfunktionen. Weitere Informationen finden Sie unter *Referenzen und weiterführende Literatur*.

Tabelle 8: Amazon S3-Funktionen zum Schützen von ruhenden Daten

Schützen von ruhenden Daten auf Amazon EBS

Amazon EBS ist ein abstrakter AWS-Blockspeicher-Service. Sie erhalten jedes Amazon EBS-Volume in einem unformatierten Rohzustand, so als ob es sich um eine neue Festplatte handeln würde. Sie können das Amazon EBS-Volume partitionieren, Software-RAID-Arrays erstellen, die Partitionen mit einem beliebigen Dateisystem formatieren und Daten auf dem Amazon EBS-Volume schützen. Alle diese Entscheidungen und Vorgänge auf dem Amazon EBS-Volume sind für AWS nicht erkennbar.

Es besteht die Möglichkeit, Amazon EBS-Volumes an Amazon EC2-Instanzen anzufügen.

Tabelle 9 enthält die Funktionen für den Schutz von ruhenden Daten auf Amazon EBS, wobei das Betriebssystem auf einer Amazon EC2-Instanz ausgeführt wird.

Amazon EBS-Funktion	Beschreibung
Replikation	Jedes Amazon EBS-Volume wird als Datei gespeichert. Sicherheitshalber erstellt AWS zwei Kopien des EBS-Volumes. Beide Kopien befinden sich in der gleichen Availability Zone, sollten aber nicht zur Überbrückung längerer Ausfälle oder zur Notfallwiederherstellung zweckentfremdet werden, auch wenn die Amazon EBS-Replikation dafür sorgt, dass Hardware-Ausfälle ohne Folgen bleiben. Wir empfehlen, Daten auf Anwendungsebene zu replizieren und/oder Backups zu erstellen.
Backup	Amazon EBS ermöglicht Snapshots, in denen die auf einem Amazon EBS-Volume zu einem bestimmten Zeitpunkt gespeicherten Daten erfasst werden. Ist das Volume beschädigt (zum Beispiel durch Systemausfall) oder wurden Daten von ihm gelöscht, können Sie es anhand eines Snapshots wiederherstellen. Amazon EBS-Snapshots sind AWS-Objekte, für die IAM-Benutzer, Gruppen und Rollen Berechtigungen erhalten können, so dass nur autorisierte Benutzer auf Amazon EBS-Backups zugreifen können.
Verschlüsselung: Microsoft Windows EFS	Wenn Sie Microsoft Windows Server auf AWS verwenden und eine zusätzliche Vertraulichkeitsebene für Ihre Daten benötigen, können Sie Encrypted File System (EFS) implementieren, um sensible Daten auf System- oder Datenpartitionen zu schützen. EFS ist eine Erweiterung für das NTFS-Dateisystem. EFS bietet transparente Datei- und Ordnerverschlüsselung, ist in Windows integriert und unterstützt PKI und

	Schlüsselverwaltungsfunktionen in Active Directory. Mit EFS verwalten Sie ihre eigenen Schlüssel.
Verschlüsselung: Microsoft Windows BitLocker	Windows BitLocker ist eine Verschlüsselungslösung für Volumes (oder Partitionen auf Einzellaufwerken) in Windows Server 2008 und neueren Windows-Betriebssystemen. BitLocker verwendet AES 128- und 256-Bit-Verschlüsselung. BitLocker erfordert standardmäßig ein Trusted Platform Module (TPM) zum Speichern von Schlüsseln. Dies wird auf Amazon EC2 nicht unterstützt. Wenn Sie BitLocker jedoch so konfigurieren, dass Passwörter unterstützt werden, ist es möglich, EBS-Volumes mit BitLocker zu schützen. Weitere Informationen finden Sie im folgenden Whitepaper: Amazon's Corporate IT Deploys SharePoint 2010 to the Amazon Web Services Cloud.
Verschlüsselung: Linux dm-crypt	Auf Linux-Instanzen ab der Kernel-Version 2.6 können Sie dm-crypt verwenden, um transparente Datenverschlüsselung auf Amazon EBS-Volumes und Auslagerungsspeicher zu konfigurieren. Es sind verschiedene Verschlüsselungstechniken einschließlich Linux Unified-Key Setup (LUKS) für die Schlüsselverwaltung verwendbar.
Verschlüsselung: TrueCrypt	TrueCrypt ist ein Drittanbieter-Tool zur transparenten Verschlüsselung von ruhenden Daten auf Amazon EBS-Volumes. TrueCrypt unterstützt sowohl Microsoft Windows- als auch Linux-Betriebssysteme.
Verschlüsselung und Integritätsauthentifizierung: SafeNet ProtectV	SafeNet ProtectV ist eine Drittanbieter-Lösung, die Amazon EBS-Volumes vollständig verschlüsseln und AMIs vor dem Boot-Vorgang authentifizieren kann. SafeNet ProtectV sorgt für die Vertraulichkeit der Daten und die Authentifizierung der Datenintegrität und des Betriebssystem.

Tabelle 9: Amazon EBS-Funktionen zum Schützen von ruhenden Daten

Schützen von ruhenden Daten auf Amazon RDS

Amazon RDS nutzt die gleiche sichere Infrastruktur wie Amazon EC2. Der Amazon RDS-Service ist ohne zusätzlichen Schutz verwendbar, aber wenn Sie Datenverschlüsselung benötigen oder wenn für Compliance- oder andere Zwecke eine Authentifizierung der Integrität von ruhenden Daten erforderlich ist, steht es Ihnen frei, auf der Anwendungs- oder der Plattformschicht kryptografische SQL-Funktionen anzuwenden.

Für Schutz auf der Anwendungsebene fügen Sie beispielsweise mit einer integrierten Verschlüsselungsfunktion hinzu, die alle sensiblen Datenbankfelder vor dem Speichern mit einem Anwendungsschlüssel verschlüsselt. Die Anwendung kann Schlüssel mithilfe von symmetrischer Verschlüsselung und PKI-Infrastruktur verwalten. Möglich sind auch andere asymmetrische Schlüsseltechniken, die einen Master-Schlüssel verwenden.

Sie schützen die Plattform mit kryptografischen MySQL-Funktionen in Form einer Anweisung wie beispielsweise der folgenden:

```
INSERT INTO Customers (CustomerFirstName,CustomerLastName) VALUES
(AES_ENCRYPT('John',@key), AES_ENCRYPT('Smith',@key);
```

Plattformbasierte Schlüssel werden wie anwendungsbasierte Schlüssel auf der Anwendungsebene verwaltet.

In Tabelle 10 sind Schutzfunktionen auf Amazon RDS-Plattformebene zusammengefasst.

Amazon RDS-Plattform	Kommentar
MySQL	Die kryptografischen Funktionen von MySQL ermöglichen Verschlüsselung, Hashing und Kompression. Weitere Informationen finden Sie unter *https://dev.mysql.com/doc/refman/5.5/en/encryption-functions.html.*
Oracle	Oracle Transparent Data Encryption wird auf Amazon RDS für Oracle Enterprise Edition gemäß dem Bring Your Own License (BYOL)-Modell unterstützt.
Microsoft SQL	Die Microsoft Transact-SQL-Datenschutzfunktionen unterstützen Verschlüsselung, Signierung und Hashing. Weitere Informationen finden Sie unter *http://msdn.microsoft.com/en-us/library/ms173744.*

Tabelle 10: Schutzfunktionen auf Amazon RDS-Plattformebene für ruhenden Daten

Beachten Sie, dass SQL-Bereichsabfragen für den verschlüsselten Teil der Daten nicht mehr anwendbar sind. Zum Beispiel würde die folgende Abfrage nicht die erwarteten Ergebnisse für Namen wie „John“, „Jonathan“ und „Joan“ liefern, wenn der Inhalt der Spalte `CustomerFirstName` auf der Anwendung- oder Plattformebene verschlüsselt ist:

```
SELECT CustomerFirstName, CustomerLastName FROM Customers WHERE
CustomerName LIKE 'Jo%';”
```

Direkte Vergleiche wie die folgenden würden funktionieren und das erwartete Ergebnis für alle Felder liefern, in denen `CustomerFirstName` genau "John" entspricht.

```
SELECT CustomerFirstName, CustomerLastName FROM Customers WHERE
CustomerFirstName = AES_ENCRYPT('John', @key);
```

Bereichsabfragen funktionieren auch mit Feldern, die nicht verschlüsselt sind. Beispielsweise könnte ein Datumsfeld in einer Tabelle unverschlüsselt bleiben und folglich in Bereichsabfragen verwendet werden.

Zum Verschleiern von eindeutigen Personendaten wie Sozialversicherungsnummern oder ähnlichen persönlichen Kennungen sind Einwegfunktionen gut geeignet. Sie können zwar Personenkennungen verschlüsseln und sie vor Verwendung auf der Anwendungs- oder Plattformebene entschlüsseln, aber es ist bequemer, Einwegfunktionen wie HMAC-SHA1 zu verwenden, um eine persönliche Kennung in einen Hash-Wert fester Länge zu konvertieren. Die persönliche Kennung bleibt dabei eindeutig, weil Kollisionen in kommerziellen HMACs sehr selten sind. Aus dem HMAC kann die ursprüngliche Kennung nicht berechnet werden. Eine Person damit zu identifizieren wäre nur möglich, wenn die Originalkennung bekannt ist und mit derselben HMAC-Funktion verarbeitet wird.

In allen Regionen unterstützt Amazon RDS die beiden Komponenten Transparent Data Encryption und Native Network der Advanced Security-Option aus der Oracle Database 11g Enterprise Edition. Die Oracle Database 11g Enterprise Edition ist auf Amazon RDS für Oracle im Rahmen des Bring Your Own License (BYOL)-Modells verfügbar. Es fallen dafür keine zusätzlichen Gebühren an.

Oracle Transparent Data Encryption verschlüsselt Daten vor dem Speichern und entschlüsselt sie beim Abruf aus dem Speicher. Mit Oracle Transparent Data Encryption können Sie Tabellenbereiche oder bestimmte Tabellenspalten mit Verschlüsselungsalgorithmen nach Industriestandard wie Advanced Encryption Standard (AES) und Data Encryption Standard (Triple DES) verschlüsseln.

Schützen von ruhenden Daten auf Amazon Glacier

Alle auf Amazon Glacier gespeicherten Daten sind durch serverseitige Verschlüsselung geschützt. AWS erzeugt eindeutige Schlüssel für jedes Amazon Glacier-Archiv und verschlüsselt es anschließend mit AES-256. Der Schlüssel wird dann mithilfe eines Master-Schlüssels mit AES-256 verschlüsselt und an einem sicheren Ort gespeichert. Der Master-Schlüssel wird regelmäßig gewechselt. Wenn Sie mehr Schutz für ruhende Daten benötigen, können Sie Daten vor dem Hochladen nach Amazon Glacier verschlüsseln.

Schützen von ruhenden Daten auf Amazon DynamoDB

Amazon DynamoDB ist ein Shared-Service von AWS. Sie können DynamoDB ohne zusätzlichen Schutz verwenden oder eine Datenverschlüsselungsebene über dem standardmäßigen DynamoDB-Service implementieren. Überlegungen zum Schutz von Daten auf der Anwendungsebene sowie zu den Auswirkungen auf SQL-Bereichsabfragen finden Sie im vorherigen Abschnitt.

DynamoDB unterstützt die Datentypen Zahlen, Zeichenfolgen und unformatierte Binärdaten. Eine bewährte Methode zur Speicherung verschlüsselter Felder in DynamoDB ist die Verwendung unformatierter binärer Felder oder mit Base64 codierter Zeichenfolgenfelder.

Schützen von ruhenden Daten auf Amazon EMR

Amazon EMR ist ein verwalteter Service in der Cloud. AWS stellt die für Amazon EMR erforderlichen AMIs bereit – andere AMIs oder Ihre eigenen EBS-Volumes werden nicht unterstützt. Standardmäßig verschlüsseln Amazon EMR-Instanzen keine ruhenden Daten.

Amazon EMR-Cluster verwenden oft Amazon S3 oder DynamoDB als persistenten Datenspeicher. Wenn ein Amazon EMR-Cluster startet, kann er die erforderlichen Betriebsdaten aus dem persistenten Speicher in HDFS kopieren oder die Daten direkt von Amazon S3 oder DynamoDB beziehen.

Für einen erhöhten Schutz von ruhenden Daten oder deren Integrität stehen mehrere Techniken zur Verfügung, die in Tabelle 11 zusammengefasst sind.

Anforderung	Beschreibung
Serverseitige Verschlüsselung mit Amazon S3 – keine HDFS-Kopie	Daten sind dauerhaft nur auf Amazon S3 gespeichert und werden nicht in HDFS kopiert. Hadoop ruft Daten von Amazon S3 ab und verarbeitet sie lokal, ohne persistente lokale Kopien anzulegen. Weitere Informationen über serverseitige Verschlüsselung mit Amazon S3 finden Sie im Abschnitt *Schützen von ruhenden Daten auf Amazon S3*.
Clientseitige Verschlüsselung mit Amazon S3	Daten sind dauerhaft nur auf Amazon S3 gespeichert und werden nicht in HDFS kopiert. Hadoop ruft Daten von Amazon S3 ab und verarbeitet sie lokal, ohne persistente lokale Kopien anzulegen. Für clientseitige Entschlüsselung können Sie einen eigenen Serializer/Deserializer (SerDe) mit Produkten wie Hive verwenden oder InputFormat für Java Map Reduce-Aufträge. Verschlüsseln Sie jede einzelnen Zeile oder jeden Datensatz, damit Sie die Datei aufteilen können. Weitere Informationen über clientseitige Verschlüsselung mit Amazon S3 finden Sie im Abschnitt *Schützen von ruhenden Daten auf Amazon S3*.
Verschlüsselung auf Anwendungsebene – gesamte Datei verschlüsselt	Sie können Daten, die in Amazon S3 oder DynamoDB gespeichert werden sollen, auf der Anwendungseben aus Sicherheitsgründen oder zum Schutz der Integrität verschlüsseln (zum Beispiel mit HMAC-SHA1). Zum Entschlüsseln der Daten verwenden Sie in Hive einen eigenen SerDe. Oder Sie rufen die Daten von Amazon S3 mithilfe eines Skripts oder einer Bootstrap-Aktion ab, entschlüsseln sie und laden sie vor der Verarbeitung in HDFS. Weil die gesamte Datei verschlüsselt ist, müssen Sie diese Aktion möglicherweise auf einem einzigen Knoten durchzuführen, wie beispielsweise dem Master-Knoten. Sie können Tools wie S3Distcp mit speziellen Codecs verwenden.
Verschlüsselung auf Anwendungsebene – einzelne Felder verschlüsselt/Struktur erhalten	Hadoop unterstützt jeden Standard-SerDe (beispielsweise JSON). Die Datenentschlüsselung kann während der Map-Stufe des Hadoop-Auftrags erfolgen. Sie können die standardmäßige Eingabe-/Ausgabeumleitung über eigene Entschlüsselungs-Tools für Streaming-Aufträge verwenden.
Hybrid	Es ist möglich, eine Kombination aus serverseitiger Verschlüsselung mit Amazon S3, clientseitiger Verschlüsselung und Verschlüsselung auf Anwendungsebene anzuwenden.

Tabelle 11: Schützen von ruhenden Daten auf Amazon EMR

Die Software-Partner von Amazon (beispielsweise Gazzang) bieten für Amazon EMR spezielle Lösungen zum Schutz von ruhenden Daten und im Transit an.

Sicheres Löschen von Daten und Stilllegen von Speichermedien

Daten werden in der Cloud auf andere Weise gelöscht als in den üblichen lokalen Umgebungen.

Wenn Sie AWS anweisen, Daten in der Cloud zu löschen, legt AWS nicht die zugrunde liegenden physischen Speichermedien still, sondern markiert die entsprechenden Speicherblöcke als nicht zugewiesen. Für eine erneute Zuweisung an andere Instanzen verwendet AWS sichere Mechanismen. Wenn Sie Blockspeicherung verwenden, protokolliert der Hypervisor oder Virtual Machine Manager (VMM), welche Blöcke Ihre Instanz beschrieben hat. Wenn eine Instanz in einem Speicherblock schreibt, wird dieser zuvor mit Nullen überschrieben. Liest eine Instanz aus einem unmittelbar zuvor beschrieben Block, werden ihr die zuvor gespeicherten Daten zurückgegeben. Versucht eine Instanz, aus einem Block zu lesen, den sie nicht unmittelbar zuvor beschrieben hat, überschreibt der Hypervisor die vorherigen Daten auf der Festplatten mit Nullen und gibt eine Null an die Instanz zurück.

Wenn AWS einen Hardwarefehler erkennt oder feststellt, dass ein Medium das Ende seiner Lebensdauer erreicht hat, zerstört AWS die Daten unter Anwendung der Techniken, die in den folgenden Dokumenten genannt sind: Department of Defense (DoD) 5220.22-M („National Industrial Security Program Operating Manual“) und NIST SP 800-88 („Guidelines for Media Sanitization“).

Weitere Informationen über das Löschen von Daten in der Cloud finden Sie im Whitepaper *AWS Security Processes*. (Siehe *Referenzen und weiterführende Literatur*).

Sollten Sie aus regulatorischen oder geschäftlichen Gründen eine weitergehende Kontrolle über sicher gelöschte Daten benötigen, implementieren Sie Datenverschlüsselung für ruhenden Daten und verwenden selbstverwaltete Schlüssel, welche nicht in der Cloud gespeichert werden. Bei Bedarf löschen Sie dann die Schlüssel und stellen damit sicher, dass die Daten nie wiederhergestellt werden können.

Schützen von Daten im Transit

Da Cloud-Anwendungen oft über öffentliche Verbindungen (wie das Internet) kommunizieren, ist es wichtig, Daten im Transit zu schützen, wenn Sie Anwendungen in der Cloud ausführen. Dies beinhaltet den Schutz des Netzwerkverkehrs zwischen Clients und Servern und zwischen Servern untereinander.

In Tabelle 12 sind übliche Bedrohungen für Daten während der Kommunikation über öffentliche Verbindungen wie dem Internet aufgeführt.

Bedrohung	Kommentar	Empfohlene Schutzmaßnahme
Versehentliche Offenlegung von Informationen	Der Zugriff auf vertrauliche Daten sollte begrenzt werden. Wenn Daten in einem öffentlichen Netz übertragen werden, sollten sie zum Schutz gegen Offenlegung verschlüsselt sein.	Verschlüsseln Sie Daten im Transit mit IPSec ESP und/oder SSL/TLS.
Kompromittierung der Datenintegrität	Stellen Sie sowohl für allgemeine als auch für vertrauliche Daten sicher, dass die Integrität der Daten nicht durch mutwillige oder zufällige Änderungen beeinträchtigt werden kann.	Gewährleisten Sie die Datenintegrität mithilfe von IPSec ESP und/oder SSL/TLS.
Kompromittierung der Peer-Identität /	Verschlüsselung und Datenintegritäts-Authentifizierung sind wichtig für den Schutz	Verwenden Sie IPSec mit IKE und Pre-Shared Keys oder X.509-Zertifikate, um die

Identitäts-Spoofing/Man-in-the-Middle	des Kommunikationskanals. Ebenso wichtig ist es, die Identität der Gegenseite zu authentifizieren. Ein verschlüsselter Kanal ist wertlos, wenn die Gegenseite ein Angreifer ist oder wenn ein Betrüger die Verbindung zum gewünschten Empfänger weiterleitet.	Gegenseite zu authentifizieren. Alternativen sind Alternative Name (AN/SAN) sowie SSL/TLS mit einer Server-Zertifikat-Authentifizierung anhand des Common Name (CN) des Servers.

Tabelle 12: Bedrohungen für Daten im Transit

AWS-Services bieten Unterstützung für IPSec und SSL/TLS zum Schutz von Daten im Transit. IPSec ist ein Protokoll, das den IP-Protokollstapel erweitert (oft in der Netzwerkinfrastruktur) und sicherstellt, dass Anwendungen auf den oberen Ebenen ohne Modifikation sicher kommunizieren können. Dagegen arbeitet SSL/TLS auf der Sitzungsebene und benötigt oft Unterstützung auf der Anwendungsebene, was SL/TLS-Wrapper von Drittanbietern übernehmen können.

Die folgenden Abschnitte enthalten Details über den Schutz von Daten im Transit.

Verwalten des Anwendungs- und administrativen Zugriffs auf Services der öffentlichen AWS-Cloud

Beim Zugriff auf Anwendungen in der öffentlichen AWS-Cloud durchlaufen Ihre Daten das Internet. In den meisten Fällen werden Ihre Sicherheitsrichtlinien das Internet als ein unsicheres Kommunikationsmedium betrachten und den Schutz von Anwendungsdaten im Transit fordern.

In Tabelle 13 sind gängige Ansätze für den Schutz von Daten im Transit beim Zugriff auf Services in einer öffentlichen Cloud aufgeführt.

Protokoll/Szenario	Beschreibung	Empfohlene Schutzmaßnahme
HTTP/HTTPS-Datenverkehr (Web-Anwendungen)	Standardmäßig ist HTTP/HTTPS-Datenverkehr ungeschützt. SSL/TLS-Schutz für HTTP-Datenverkehr, auch als HTTPS bekannt, ist Industriestandard und wird von den meisten Web-Servern und Browsern unterstützt. Zum HTTP-Datenverkehr gehört nicht nur der Client-Zugriff auf Web-Seiten, sondern auch Web-Services (REST- oder SOAP-basierter Zugriff).	Verwenden Sie HTTPS (HTTP über SSL/TLS) mit Server-Zertifikatauthentifizierung.

Protokoll/Szenario	Beschreibung	Empfohlene Schutzmaßnahme
HTTPS-Offload (Web-Anwendungen)	HTTPS wird zwar oft empfohlen, vor allem für sensible Daten, jedoch erfordert die SSL/TLS-Verarbeitung zusätzliche CPU- und Speicherressourcen auf dem Web-Server und dem Client. Dies kann eine erhebliche Belastung auf Web-Servern darstellen, die Tausende von SSL/TLS-Sitzungen bearbeiten. Ein Client ist weniger betroffen, da er nur eine begrenzte Anzahl von SSL/TLS-Verbindungen verarbeitet.	Verlagern Sie die HTTPS-Verarbeitung auf Elastic Load Balancing, wodurch die Belastung von Web-Servern vermindert wird, während die Daten im Transit weiterhin geschützt sind. Schützen Sie außerdem die Backend-Verbindung zu Instanzen mit einem Anwendungsprotokoll wie HTTP über SSL.
Remote Desktop Protocol (RDP)-Datenverkehr	Benutzer, die auf Windows Terminal Services in der öffentlichen Cloud zugreifen, nutzen in der Regel das Microsoft Remote Desktop Protocol (RDP). Standardmäßig bauen RDP-Verbindungen eine zugrunde liegende SSL/TLS-Verbindung auf.	Für einen optimalen Schutz sollte der Windows-Server, auf den zugegriffen wird, über ein vertrauenswürdiges X.509-Zertifikat verfügen, damit Identitäts-Spoofing und Man-in-the-Middle-Angriffe ausgeschlossen sind. Standardmäßig verwenden Windows RDP-Server selbstsignierte Zertifikate, die nicht vertrauenswürdig sind und vermieden werden sollten.
Secure Shell (SSH)-Datenverkehr	SSH ist die bevorzugte Lösung für administrative Verbindungen zu Linux-Servern. SSH ist ein Protokoll, das wie SSL einen sicheren Kommunikationskanal zwischen dem Client und dem Server einrichtet. Darüber hinaus unterstützt SSH auch Tunneling, das Sie zum Ausführen von Anwendungen wie X-Windows basierend auf SSH verwenden sollten, und schützt die Daten der Anwendungssitzung im Transit.	Verwenden Sie SSH Version 2 mit nicht-privilegierten Benutzerkonten.
Datenbank-Server-Datenverkehr	Wenn Clients oder Server auf Datenbanken in der Cloud zugreifen müssen, werden sie dafür wahrscheinlich das Internet verwenden.	Die meisten modernen Datenbanken unterstützen SSL/TLS-Wrapper für native Datenbankprotokolle. Für Datenbank-Server auf Amazon EC2 empfehlen wir diesen Ansatz zum Schutz von Daten im Transit. Amazon RDS unterstützt SSL/TLS in einigen Fällen. Weitere Informationen finden Sie im Abschnitt *Schützen von Daten im Transit beim Zugriff* auf Amazon RDS.

Tabelle 13: Schützen von Daten im Transit beim Zugriff auf die öffentliche Cloud

Schützen von Daten im Transit beim Verwalten von AWS-Services

Sie verwalten Ihre AWS-Services wie Amazon EC2 und Amazon S3 über die AWS Management Console oder AWS-APIs. Datenverkehr durch Service-Verwaltung entsteht beispielsweise beim Start einer neuen Amazon EC2-Instanz, beim Speichern eines Objekts in einem Amazon S3-Bucket oder durch Änderung einer Sicherheitsgruppe auf Amazon VPC.

Die AWS Management Console verwendet SSL/TLS zwischen den Service-Endpunkten Client-Browser und Konsole, um den Datenverkehr zur Verwaltung von AWS-Services zu schützen. Der Datenverkehr ist verschlüsselt, die Datenintegrität wird authentifiziert, und der Client-Browser authentifiziert die Identität des Service-Endpunkts Konsole mithilfe eines X.509-Zertifikats. Nachdem eine SSL/TLS-Sitzung zwischen den Service-Endpunkten Client-Browser und Konsole eingerichtet ist, ist der gesamte HTTP-Datenverkehr während der SSL/TLS-Sitzung verschlüsselt.

Sie können auch AWS-APIs verwenden, um AWS-Services direkt aus Anwendungen heraus zu verwalten. Oder Sie nehmen die Verwaltung mit Tools von Drittanbietern, über SDKs oder mit AWS-Befehlszeilen-Tools vor. AWS-APIs sind Web-Services (SOAP oder REST), die über HTTPS ausgeführt werden. SSL/TLS-Sitzungen werden zwischen dem Client und dem jeweiligen AWS-Service-Endpunkt eingerichtet, je nach verwendeten APIs, und der gesamte anschließende Datenverkehr, einschließlich SOAP/REST-Envelope und Nutzdaten des Benutzers, ist während der SSL/TLS-Sitzung geschützt.

Schützen von Daten im Transit beim Zugriff auf Amazon S3

Auf Amazon S3 wird mit SOAP über HTTPS zugegriffen. Auch der Datenverkehr zur Verwaltung von AWS-Services verwendet dieses Protokoll. Verkehrsdaten sind alle Amazon S3-Verwaltungsanforderungen sowie die Nutzdaten des Benutzers, beispielsweise die Inhalte von Objekten, die in Amazon S3 gespeichert oder abgerufen werden, samt den zugehörigen Metadaten.

Zur Verwaltung von Amazon S3 über die AWS Management Console wird eine sichere SSL/TLS-Verbindung zwischen den Endpunkten Client-Browser und Konsole eingerichtet. Anschließend ist jeglicher Datenverkehr über diese Verbindung geschützt.

Bei Verwendung von Amazon S3-APIs (direkt oder indirekt) wird eine SSL/TLS-Verbindung zwischen den Endpunkten Client und Amazon S3 eingerichtet. Anschließend ist jeglicher Datenverkehr (HTTP, SOAP und Benutzernutzlast) innerhalb der gesicherten Sitzung gekapselt.

Schützen von Daten im Transit beim Zugriff auf Amazon RDS

Wenn Sie von Amazon EC2-Instanzen derselben Region eine Verbindung zu Amazon RDS herstellen, können Sie sich auf die Sicherheit des AWS-Netzwerks verlassen, zudem können Sie auch eine verschlüsselte Verbindung zu dem Datenbankmanagementsystem der RDS Instanz herstellen. Sofern Sie die Verbindung aber über das Internet herstellen, sollten Sie in Erwägung ziehen, mit SSL/TLS für zusätzlichen Schutz zu sorgen.

SSL/TLS bietet Peer-Authentifizierung über X.509-Server-Zertifikate, Authentifizierung der Datenintegrität und Datenverschlüsselung für die Client-Server-Verbindung.

SSL/TLS wird derzeit für Verbindungen zu Amazon RDS MySQL und Microsoft SQL-Instanzen unterstützt. Für beide Produkte stellt Amazon Web Services ein einzelnes selbstsigniertes Zertifikat für den MySQL- oder Microsoft SQL-Listener aus. Laden Sie das selbstsignierte Zertifikat herunter und bezeichnen sie es als vertrauenswürdig. Das sorgt für eine Peer-Identitätsauthentifizierung und verhindert Man-in-the-Middle-Angriffe oder Spoofing auf der Server-Seite. SSL/TLS bietet native Verschlüsselung und Authentifizierung der Datenintegrität für den Kommunikationskanal zwischen dem Client und dem Server. Da dasselbe selbstsignierte Zertifikat auf allen Amazon RDS MySQL-Instanzen auf AWS verwendet wird und ein weiteres einzelnes selbstsigniertes Zertifikat in allen Amazon RDS Microsoft SQL-Instanzen auf AWS, ermöglicht Peer-Identitätsauthentifizierung keine individuelle Instanz-Authentifizierung. Wenn Sie die

Authentifizierung einzelner Server über SSL/TLS benötigen, müssen Sie möglicherweise Amazon EC2 und selbstverwaltete relationale Datenbanken benutzen.

Amazon RDS for Oracle Native Network Encryption verschlüsselt Daten, während sie in der Datenbank gespeichert oder daraus abgerufen werden. Mit Oracle Native Network Encryption können Sie den über Oracle Net Services abgewickelten Datenverkehr mit Verschlüsselungsalgorithmen nach Industriestandard wie AES und Triple DES verschlüsseln.

Schützen von Daten im Transit beim Zugriff auf Amazon DynamoDB

Wenn Sie von anderen AWS-Services derselben Region eine Verbindung zu DynamoDB herstellen, können Sie sich auf die Sicherheit des AWS-Netzwerks verlassen. Sofern Sie die Verbindung aber über das Internet herstellen, sollten Sie HTTP über SSL/TLS (HTTPS) zur Verbindung mit DynamoDB-Service-Endpunkten verwenden. Vermeiden Sie HTTP für den Zugriff auf DynamoDB und für alle Verbindungen über das Internet.

Schützen von Daten im Transit beim Zugriff auf Amazon EMR

Amazon EMR enthält eine Reihe von Anwendungskommunikationspfaden, von denen jeder separate Schutzmechanismen für die Daten im Transit benötigt. In Tabelle 14 sind die Kommunikationspfade sowie die von uns empfohlenen Schutzmaßnahmen aufgeführt.

Art des Amazon EMR-Datenverkehrs	Beschreibung	Empfohlene Schutzmaßnahme
Zwischen Hadoop-Knoten	Die Hadoop-Master-, Worker- und Core-Knoten kommunizieren alle untereinander über einfache TCP-Verbindungen. Da sich aber alle Hadoop-Knoten auf Amazon EMR in der gleichen Availability Zone befinden, sind sie durch die Sicherheitsstandards der physikalischen und der Infrastrukturebene geschützt.	Normalerweise ist kein zusätzlicher Schutz erforderlich – alle Knoten befinden sich in derselben Availability Zone
Zwischen Hadoop-Cluster und Amazon S3	Amazon EMR verwendet HTTPS, um Daten zwischen DynamoDB und Amazon EC2 auszutauschen. Weitere Informationen finden Sie im Abschnitt *Schützen von Daten im Transit beim Zugriff* auf Amazon S3.	HTTPS wird standardmäßig verwendet.
Zwischen Hadoop-Cluster und Amazon DynamoDB	Amazon EMR verwendet HTTPS, um Daten zwischen Amazon S3 und Amazon EC2 auszutauschen. Weitere Informationen finden Sie im Abschnitt *Schützen von Daten im Transit beim Zugriff* auf Amazon DynamoDB.	HTTPS wird standardmäßig verwendet.

Zugriff auf Hadoop-Cluster durch Benutzer oder Anwendung	Clients oder lokale Anwendungen können auf Amazon EMR-Cluster über das Internet zugreifen, mithilfe von Skripts (SSH-basierter Zugriff), REST oder Protokollen wie Thrift oder Avro.	Verwenden Sie SSH für interaktiven Zugriff auf Anwendungen oder zum Tunneln anderer Protokolle. Für Thrift, REST oder Avro setzen Sie SSL/TLS ein.
Administrativer Zugriff auf Hadoop-Cluster	Administratoren für Amazon EMR-Cluster verwenden üblicherweise SSH zur Verwaltung der Cluster.	Verwenden Sie SSH für den Amazon EMR-Master-Knoten.

Tabelle 14: Schützen von Daten im Transit beim Zugriff auf Amazon EMR

Schützen Ihrer Betriebssysteme und Anwendungen

Gemäß dem AWS-Modell geteilter Verantwortung sind Sie für die Sicherheit Ihrer Betriebssysteme und Anwendungen zuständig. Amazon EC2 stellt eine echte virtuelle Computerumgebung bereit, in der Sie Web-Service-Schnittstellen verwenden können, um Instanzen mit einer Vielzahl an Betriebssystemen mit benutzerdefinierten, vorab geladenen Anwendungen zu starten. Sie können Betriebssystem- und Anwendungs-Builds standardisieren und die Sicherheit Ihrer Betriebssysteme und Anwendungen in einem einzigen sicheren Build-Repository zentral verwalten. Sie können ein vorkonfiguriertes AMI erstellen und testen, um Ihre Sicherheitsanforderungen zu erfüllen.

In diesem Abschnitt soll keine umfassende Liste von Härtungsstandards für AMIs bereitgestellt werden. Zu den Quellen der branchenweit anerkannten Standards zur Systemhärtung gehören unter anderem:

- Center for Internet Security (CIS)
- Internationale Organisation für Normung (International Organization for Standardization, ISO)
- SysAdmin Audit Network Security (SANS) Institute
- National Institute of Standards Technology (NIST)

Wir empfehlen, Konfigurationsstandards für alle Systemkomponenten zu entwickeln. Stellen Sie sicher, dass diese Standards alle bekannten Sicherheitsrisiken abdecken und an branchenweit anerkannten Standards zur Systemhärtung ausgerichtet sind.Wenn sich herausstellt, dass ein veröffentlichtes AMI gegen Best Practices verstößt oder ein signifikantes Risiko für Kunden darstellt, die das AMI ausführen, behält sich AWS das Recht vor, Maßnahmen zu ergreifen, um das AMI aus dem öffentlichen Katalog zu entfernen und den Herausgeber und diejenigen, die das AMI ausführen, über die Erkenntnisse zu informieren.

Erstellen benutzerdefinierter AMIs

Sie können eigene AMIs erstellen, welche die speziellen Anforderungen Ihrer Organisation erfüllen, und sie für den internen (privaten) oder externen (öffentlichen) Gebrauch veröffentlichen. Als Herausgeber eines AMI sind Sie für die ursprünglichen Sicherheitseinstellungen der Machine Images verantwortlich, die Sie in der Produktion verwenden. Die Sicherheitskontrollen, welche Sie auf das AMI anwenden, werden zu einem bestimmten Zeitpunkt wirksam. Sie sind nämlich nicht dynamisch. Sie können private AMIs so konfigurieren, dass sie Ihre Unternehmensanforderungen erfüllen solange sie nicht gegen die AWS Acceptable Use Policy verstoßen. Weitere Informationen finden Sie unter Amazon Web Services Acceptable Use Policy –http://*aws.amazon.com/aup*/.

Benutzer, die über AMIs starten, sind jedoch nicht notwendigerweise Sicherheitsexperten. Daher wird empfohlen, gewisse Mindestsicherheitsstandards einzuhalten.

Stellen Sie vor Veröffentlichung eines AMI sicher, dass die veröffentlichte Software auf dem aktuellen Stand ist und die jeweiligen Sicherheits-Patches beinhaltet. Führen Sie außerdem die in Tabelle 15 aufgeführten Bereinigungs- und Härtungsmaßnahmen durch.

Bereich	Empfohlene Aufgabe
Deaktivieren unsicherer Anwendungen	Deaktivieren Sie Services und Protokolle, die Benutzer als Klartext über das Netzwerk oder auf eine andere unsichere Art und Weise authentifizieren.
Minimieren des Risikos	Deaktivieren Sie das Starten nicht erforderlicher Netzwerk-Services. Nur Verwaltungs-Services (SSH/RDP) und die für wichtige Anwendungen erforderlichen Services sollten gestartet werden.
Schützen von Anmeldeinformationen	Löschen Sie alle AWS-Anmeldeinformationen auf sichere Art und Weise aus Datenträger- und Konfigurationsdateien.
Schützen von Anmeldeinformationen	Löschen Sie alle Anmeldeinformationen Dritter auf sichere Art und Weise aus Datenträger- und Konfigurationsdateien.
Schützen von Anmeldeinformationen	Löschen Sie alle zusätzlichen Zertifikate oder Schlüsselmaterial auf sichere Art und Weise aus dem System.
Schützen von Anmeldeinformationen	Stellen Sie sicher, dass die installierte Software keine standardmäßigen internen Konten und Passwörter verwendet.
Handeln gemäß geltenden Richtlinien	Stellen Sie sicher, dass das System nicht gegen die Amazon Web Services Acceptable Use Policy verstößt. Zu Beispielen solcher Verstöße gehören etwa offene SMTP-Relays oder -Proxy-Server. Weitere Informationen finden Sie unter Amazon Web Services Acceptable Use Policy –http://*aws.amazon.com/aup/*.

Tabelle 15: Bereinigungsaufgaben vor dem Veröffentlichen eines AMI

In den Tabellen 16 und 17 sind zusätzliche betriebssystemspezifische Bereinigungsaufgaben aufgeführt.

In Tabelle 16 sind die Schritte für das Schützen von Linux-AMIs aufgeführt.

Bereich	Härtungsmaßnahmen
Schützen von Services	Konfigurieren Sie SSHD so, dass nur die Authentifizierung durch öffentliche Schlüssel zulässig ist. Legen Sie in **sshd_config** die Option **PubkeyAuthentication** auf **yes** und **PasswordAuthentication** auf **no** fest.
Schützen von Services	Generieren Sie bei der Erstellung der Instanz einen eindeutigen SSH-Hostschlüssel. Wenn das AMI **cloud-init** verwendet, führt es dies automatisch durch.
Schützen von Anmeldeinformationen	Entfernen und deaktivieren Sie Passwörter für alle Benutzerkonten, sodass sie nicht zum Anmelden verwendet werden können. Verwenden Sie kein Standardpasswort. Führen Sie **passwd -l <BENUTZERNAME>** für jedes Konto aus.
Schützen von Anmeldeinformationen	Löschen Sie auf sichere Art und Weise alle öffentlichen und privaten SSH-Schlüsselpaare für Benutzer.
Schützen von Daten	Löschen Sie auf sichere Art und Weise alle Shell-Verlaufs- und Systemprotokolldateien, die vertrauliche Daten enthalten.

Tabelle 16: Schützen von Linux-/UNIX-AMIs

In Tabelle 17 sind die Schritte zum Schützen von Windows-AMIs aufgeführt:

Bereich	Härtungsmaßnahmen
Schützen von Anmeldeinformationen	Stellen Sie sicher, dass bei Instanz-Erstellung alle aktivierten Benutzerkonten ein neues, zufallsgeneriertes Passwort aufweisen. Sie können den EC2Config-Service so konfigurieren, dass er dies beim Start für das Administratorkonto ausführt. Dies muss jedoch vor dem Bündeln des Images explizit konfiguriert werden.
Schützen von Anmeldeinformationen	Stellen Sie sicher, dass das Gästekonto deaktiviert ist.
Schützen von Daten	Löschen Sie die Windows-Ereignisprotokolle.
Schützen von Anmeldeinformationen	Stellen Sie sicher, dass das AMI nicht Teil einer Windows-Domain ist.
Minimieren des Risikos	Aktivieren Sie keine Dateifreigaben, Druckerspooler, RPC und andere Windows-Services, die nicht erforderlich, aber standardmäßig aktiviert sind.

Tabelle 17: Schützen von Windows-AMIs

Bootstrapping

Nachdem das gehärtete AMI instanziiert ist, können Sie Sicherheitskontrollen mithilfe von Bootstrapping-Anwendungen nach wie vor ändern und aktualisieren. Bekannte Bootstrapping-Anwendungen sind etwa Puppet, Chef, Capistrano, Cloud-Init und Cfn-Init. Außerdem können Sie benutzerdefinierte Bash- oder Microsoft Windows PowerShell-Skripts für Bootstrapping ausführen, ohne Drittanbieter-Tools zu verwenden.

Hier finden Sie einige Bootstrap-Aktionen, die zu beachten sind:

- Updates für Sicherheitssoftware installieren die aktuellsten Patches, Service Packs und wichtige Updates über die Patch-Ebene des AMI hinaus.
- Erstmalige Anwendungs-Patches installieren Updates auf Anwendungsebene, über das aktuelle Build auf Anwendungsebene, wie im AMI erfasst, hinaus.
- Durch kontextbezogene Daten und Konfigurationen können Instanzen Konfigurationen anwenden, die für die Umgebung, in denen sie gestartet werden, spezifisch sind, wie beispielsweise „Produktion“, „Test“ oder „DMZ/intern“.
- Registrieren Sie Instanzen mit Remote-Systemen für Sicherheits-Monitoring und -verwaltung.

Verwalten von Patches

Sie sind für die Verwaltung der Patches für Ihre AMIs und laufender Instanzen verantwortlich. Wir empfehlen, die Verwaltung der Patches genau festzulegen und ein schriftlich abgefasstes Verfahren zu befolgen.

Sie können Patch-Verwaltungssysteme von Drittanbietern für Betriebssysteme und wichtige Anwendungen verwenden. Es empfiehlt sich jedoch, eine Aufstellung des gesamten Bestands an Software- und Systemkomponenten zu pflegen und die Liste der auf jedem System installierten Sicherheits-Patches mit der aktuellsten Liste der Sicherheits-Patches der Anbieter abzugleichen. So können Sie überprüfen, ob die aktuellen Patches der Anbieter installiert sind.

Führen Sie Prozesse ein, um neue Sicherheitsrisiken zu ermitteln und solchen Sicherheitslücken Risikobewertungen zuzuweisen. Stufen Sie zumindest die gravierendsten, höchsten Sicherheitsrisiken als „Hoch“ ein.

Kontrollieren der Sicherheit für öffentliche AMIs

Achten Sie darauf, dass Sie wichtige Anmeldeinformationen nicht in AMIs belassen, wenn Sie sie öffentlich freigeben. Weitere Informationen finden Sie in diesem Tutorial über das sichere Freigeben und Nutzen öffentlicher AMIs: *http://aws.amazon.com/articles/0155828273219400.*

Schützen Ihres Systems vor Malware

Schützen Sie Ihre Systeme in der Cloud ebenso, wie Sie eine konventionelle Infrastruktur vor Bedrohungen wie Viren, Würmer, Trojaner, Rootkits, Botnets und Spam schützen würden.

Es ist wichtig, dass Ihnen bewusst ist, wie sich eine Malware-Infektion auf eine einzelne Instanz oder auf das gesamte Cloud-System auswirkt: Wenn ein Benutzer – wissentlich oder unwissentlich – ein Programm auf einem Linux- oder Windows-System ausführt, übernimmt die ausführbare Datei die Berechtigungen dieses Benutzers (oder gibt sich in manchen Fällen als ein anderer Benutzer aus). Ob Code eine Aktion ausführen kann, hängt davon ab, ob der Benutzer, der den Code startet, über die entsprechenden Berechtigungen verfügt. Benutzer müssen sicherstellen, dass sie nur vertrauenswürdigen Code ausführen.

Wenn Sie nicht vertrauenswürdigen Code auf Ihrem System ausführen, ist es nicht länger Ihr System – es gehört jemand anderem. Wenn ein Superuser oder ein Benutzer mit Administratorberechtigungen ein nicht vertrauenswürdiges Programm ausführt, ist auch das System, auf dem das Programm ausgeführt wurde, nicht mehr vertrauenswürdig. Schadcode kann Teile des Betriebssystems ändern, ein Rootkit installieren oder eine Art Hintertür für den Zugriff auf das System einrichten. Es ist möglich, dass er Daten löscht, die Datenintegrität gefährdet, die Verfügbarkeit von Services einschränkt oder Daten auf verdeckte oder offenkundige Art und Weise für Dritte offenlegt.

Betrachten Sie die Instanz, auf der der Code ausgeführt wurde, als infiziert. Wenn die infizierte Instanz Teil einer Single-Sign-on-Umgebung ist oder wenn ein implizites Vertrauensmodell für den Zugriff zwischen Instanzen vorhanden ist, kann sich die Infektion schnell von der einzelnen Instanz auf das gesamte System und darüber hinaus ausbreiten. Eine Infektion dieses Ausmaßes kann schnell zu Datenverlusten sowie Daten und Services, deren Sicherheit nicht mehr gewährleistet ist, führen. Und sie kann den Ruf des Unternehmens schädigen. Außerdem kann ein solcher Vorfall direkte finanzielle Konsequenzen nach sich ziehen, wenn beispielsweise Services für Dritte beschädigt oder übermäßig viele Cloud-Ressourcen verbraucht werden. Sie sind für den Schutz vor Malware zuständig.

In Tabelle 18 finden Sie einige allgemeine Ansätze für den Schutz vor Malware.

Bedrohung	Allgemeine Ansätze
Nicht vertrauenswürdige AMIs	Starten Sie Instanzen nur über vertrauenswürdige AMIs. Zu vertrauenswürdigen AMIs gehören die von AWS bereitgestellten standardmäßigen Windows- und Linux-AMIs sowie AMIs von vertrauenswürdigen Drittanbietern. Wenn Sie Ihre eigenen benutzerdefinierten AMIs von den standardmäßigen und vertrauenswürdigen AMIs ableiten, müssen die zusätzliche Software und die zusätzlichen Einstellungen, die Sie darauf anwenden, ebenfalls vertrauenswürdig sein. Das Starten eines nicht vertrauenswürdigen Drittanbieter-AMI kann die gesamte Cloud-Umgebung gefährden und infizieren.
Nicht vertrauenswürdige Software	Sie sollten nur vertrauenswürdige Software von einem vertrauenswürdigen Softwareanbieter installieren und ausführen. Ein vertrauenswürdiger Softwareanbieter ist ein Anbieter, der in der Branche renommiert und anerkannt ist und Software auf sichere und verantwortungsvolle Art und Weise entwickelt. Dabei lässt er nicht zu, dass Schadcode seine Softwarepakete infiziert. Open-Source-Software kann auch vertrauenswürdige Software sein und Sie sollten in der Lage sein, eigene ausführbare Dateien zu kompilieren. Wir empfehlen dringend, Code sorgfältig zu überprüfen, um sicherzustellen, dass der Quell-Code nicht schädlich ist. Vertrauenswürdige Softwareanbieter signieren ihre Software oft mithilfe von Code-Signing-Zertifikaten oder stellen MD5- oder SHA-1-Signaturen ihrer Produkte bereit, sodass Sie die Integrität der Software, die Sie herunterladen, überprüfen können.
Nicht vertrauenswürdige Softwaredepots	Sie laden vertrauenswürdige Software von vertrauenswürdigen Quellen herunter. Es ist möglich, dass zufällige Softwarequellen im Internet oder an anderen Stellen im Netzwerk Malware innerhalb eines ansonsten legitimen und seriösen Softwarepakets verteilen. Solche nicht vertrauenswürdigen Personen stellen möglicherweise MD5- oder SHA-1-Signaturen des manipulierten Pakets, das Malware enthält, bereit. Solchen Signaturen sollten also nicht vertraut werden. Wir raten Ihnen, eigene interne Softwaredepots vertrauenswürdiger Software für Ihre Benutzer zur Installation und Verwendung zusammenzustellen. Raten Sie Benutzern dringend davon ab, Software von zufälligen Quellen im Internet herunterzuladen und zu installieren.

Prinzip der geringsten Rechte	Weisen Sie Benutzern nur die Berechtigungen zu, die sie benötigen, um ihre Aufgaben auszuführen. Selbst wenn ein Benutzer versehentlich eine infizierte ausführbare Datei startet, sind auf diese Weise die Auswirkungen auf die Instanz und das weitere Cloud-System auf ein Minimum beschränkt.
Patchen	Wenden Sie Patches auf extern zugängliche oder interne Systeme an, um das aktuelle Sicherheitsniveau sicherzustellen. Würmer verbreiten sich oft über nicht gepatchte Systeme im Netzwerk.
Botnets	Wenn sich eine Infektion – ob durch einen konventionellen Virus, einen Trojaner oder einen Wurm – über die einzelne Instanz hinaus verbreitet und einen größeren Bestand von Instanzen infiziert, kann sie Schadcode enthalten, der ein Botnet erstellt. Ein Botnet ist ein Netzwerk infizierter Hosts, die von einem Angreifer remote gesteuert werden können. Folgen Sie allen vorangehenden Empfehlungen, um eine Botnet-Infektion zu vermeiden.
Spam	Infizierte Systeme können von Angreifern genutzt werden, um große Mengen unerwünschter E-Mails (Spam) zu versenden. AWS bietet spezielle Kontrollmechanismen, um die Anzahl der E-Mails zu begrenzen, die von einer Amazon EC2-Instanz gesendet werden kann. Dennoch sind Sie dafür verantwortlich, eine Infektion von vornherein zu verhindern. Vermeiden Sie offene SMTP-Relays, die zur Verbreitung von Spam verwendet werden können und außerdem möglicherweise einen Verstoß gegen die AWS Acceptable Use Policy darstellen können. Weitere Informationen finden Sie unter Amazon Web Services Acceptable Use Policy – http://*aws.amazon.com/aup/*.
Antivirus-/Antispam-Software	Stellen Sie sicher, dass Sie eine renommierte und aktuelle Antivirus- und Antispam-Lösung für Ihr System verwenden.
Hostbasierte IDS-Software	Viele AWS-Kunden installieren hostbasierte IDS-Software, wie etwa die Open-Source-Lösung OSSEC, die Software zur Überprüfung der Dateiintegrität und zur Erkennung von Rootkits enthält. Verwenden Sie diese Lösungen zum Analysieren wichtiger Systemdateien und -ordner und zum Errechnen von Prüfsummen, die deren vertrauenswürdigen Zustand wiedergeben. Überprüfen Sie dann regelmäßig, ob diese Dateien verändert wurden, und informieren Sie den Systemadministrator, wenn dies der Fall ist.

Tabelle 18: Ansätze für den Schutz vor Malware

Wenn eine Instanz infiziert ist, ist Antivirus-Software möglicherweise in der Lage, die Infektion zu erkennen und den Virus zu entfernen. Wir empfehlen den sichersten und allgemein empfohlenen Ansatz, der darin besteht, alle Systemdaten zu speichern, dann alle Systeme, Plattformen und ausführbaren Anwendungsdateien von einer vertrauenswürdigen Quelle erneut zu installieren und dann nur die Daten aus den Backups wiederherzustellen.

Minimierung von Gefährdung und Missbrauch

AWS stellt Kunden eine globale Infrastruktur für die Erstellung von Lösungen bereit, von denen viele vom Internet aus zugänglich sind. Unsere Kundenlösungen müssen so betrieben werden, dass dem Rest der Internetgemeinschaft kein Schaden zugefügt wird. Das bedeutet, Missbrauch muss vermieden werden.

Missbrauchsaktivitäten sind extern beobachtete Verhaltensweisen von Instanzen oder anderen Ressourcen von AWS-Kunden, die böswillig, anstößig oder illegal sind oder andere Websites im Internet schädigen könnten.

AWS arbeitet gemeinsam mit Ihnen daran, verdächtige und böswillige Aktivitäten auf Seiten Ihrer AWS-Ressourcen zu erkennen und zu behandeln. Unerwartetes oder verdächtiges Verhalten Ihrer Ressourcen kann ein Hinweis darauf sein, dass die Sicherheit Ihrer AWS-Ressourcen nicht mehr gewährleistet ist, was potentielle Risiken für Ihr Unternehmen bergen kann.

AWS verwendet die folgenden Mechanismen zur Erkennung von Missbrauch durch Kundenressourcen:

- AWS-interne Ereignisüberwachung
- Externe Sicherheitslösungen für das AWS-Netzwerk
- Beschwerden über Internet-Missbrauchs gegen AWS-Ressourcen

Das AWS-Team, das für das Bearbeiten von Missbrauchsvorwürfen zuständig ist, überwacht intensiv Missbrauch oder betrügerische Aktionen auf AWS und beendet solche Aktivitäten. Der Großteil der Beschwerden über Missbrauch bezieht sich jedoch auf Kunden, die auf legitime Weise mit AWS arbeiten. Zu häufigen Ursachen unabsichtlichen Missbrauchs zählen unter anderem:

- **Beschädigte Ressourcen.** Beispiel: Eine nicht gepatchte Amazon EC2-Instanz kann infiziert werden und als Botnet-Agent agieren.
- **Unabsichtlicher Missbrauch.** Beispiel: Ein übermäßig aggressiver Web-Crawler kann von einigen Websites im Internet als DOS-Angreifer klassifiziert werden.
- **Sekundärer Missbrauch.** Beispiel: Ein Endbenutzer eines von einem AWS-Kunden bereitgestellten Services postet Malware-Dateien in einem öffentlichen Amazon S3-Bucket.
- **Falsche Beschwerden.** Internetbenutzer halten legitime Aktivitäten fälschlicherweise für Missbrauch.

AWS ist bestrebt, gemeinsam mit AWS-Kunden an der Vermeidung, Erkennung und Eindämmung von Missbrauch zu arbeiten und ein erneutes Auftreten solcher Fälle in der Zukunft zu vermeiden. Wenn Sie von AWS eine Warnung über Missbrauch erhalten, müssen Ihre Sicherheitsexperten und Mitarbeiter im operativen Bereich die Angelegenheit sofort überprüfen. Durch Verzögerungen kann sich der Schaden auf andere Websites im Internet ausbreiten. Dies kann Ihren Ruf schädigen und rechtliche Konsequenzen nach sich ziehen. Darüber hinaus können die betroffenen Ressourcen von böswilligen Benutzern beschädigt werden. Diese Gefährdung zu ignorieren, könnte Ihrem Unternehmen noch größeren Schaden zufügen.

Böswillige, illegale oder schädliche Aktivitäten, die Ihre AWS-Ressourcen nutzen, verstoßen gegen die AWS Acceptable Use Policy und können zu einer Kontosperrung führen. Weitere Informationen finden Sie unter Amazon Web Services Acceptable Use Policy –http://*aws.amazon.com/aup/*. Sie sind dafür verantwortlich, einwandfreie Services zu unterhalten, wie dies die Internetgemeinschaft erwarten kann. Wenn ein AWS-Kunde es versäumt, gegen gemeldete Missbrauchsaktivitäten vorzugehen, sperrt AWS das AWS-Konto, um die Integrität der AWS-Plattform und der Internetgemeinschaft zu schützen.

In Tabelle 19 sind Best Practices aufgeführt, die Ihnen dabei helfen, auf Missbrauchsvorfälle angemessen zu reagieren:

Best Practice	Beschreibung
Ignorieren Sie nie AWS-Informationen über Missbrauch.	Im Fall eines Missbrauchs sendet AWS umgehend eine E-Mail-Benachrichtigung an die registrierten E-Mail-Adressen der Kunden. Sie können einfach auf die E-Mail mit der Missbrauchswarnung antworten, um Informationen mit dem AWS-Missbrauchsteam auszutauschen. Die gesamte Kommunikation wird für die spätere Verwendung im AWS-System für Missbrauchsnachverfolgung gespeichert. Das Team von AWS zur Bearbeitung von Missbrauchsvorwürfen ist bemüht, Kunden dabei zu unterstützen, die Art der Beschwerden zu verstehen. AWS hilft Kunden, Missbrauchsaktivitäten einzudämmen und zu verhindern. Eine Kontosperrung ist die letzte Maßnahme, die das AWS-Missbrauchsteam ergreift, um Missbrauch zu beenden. Wir arbeiten gemeinsam mit unseren Kunden daran, Probleme zu entschärfen und die Notwendigkeit, Maßnahmen zu ergreifen, zu vermeiden. Sie müssen jedoch auf Missbrauchswarnungen reagieren, Maßnahmen zum Beenden der böswilligen Aktionen ergreifen und ein erneutes Auftreten in der Zukunft verhindern. Ausbleibende Reaktionen auf Seiten der Kunden ist der Hauptgrund für das Blockieren von Instanzen und Konten.
Befolgen Sie die Best Practices für die Sicherheit.	Der beste Schutz vor Ressourcenschädigungen besteht darin, die Best Practices für die Sicherheit zu befolgen, die in diesem Dokument aufgeführt sind. AWS stellt bestimmte Sicherheits-Werkzeuge bereit, um Ihnen dabei zu helfen, effektive Schutzmechanismen für Ihre Cloud-Umgebung einzurichten. Sie müssen jedoch die Best Practices anwenden, wie Sie dies für Server innerhalb Ihres eigenen Rechenzentrums tun würden. Führen Sie konsequent einfache Schutzmechanismen ein, wie etwa das Anwenden der aktuellen Software-Patches, die Beschränkung des Netzwerkverkehrs über eine Firewall und/oder Amazon EC2-Sicherheitsgruppen und die Erteilung von möglichst niedrigen Berechtigungen für Benutzer.

Eindämmung von Gefährdungen.	Wenn Ihre Computerumgebung kompromittiert oder infiziert wurde, empfehlen wir, die folgenden Schritte durchzuführen, um einen sicheren Status wiederherzustellen: • Betrachten Sie alle bekannten Amazon EC2-Instanzen oder AWS-Ressourcen, deren Sicherheit nicht gewährleistet ist, als unsicher. Wenn Ihre Amazon EC2-Instanz Datenverkehr generiert, der nicht durch Ihre Anwendungsnutzung erklärt werden kann, wurde Ihre Instanz wahrscheinlich mit Schadsoftware kompromittiert oder infiziert. Fahren Sie diese Instanz herunter und erstellen Sie diese komplett neu, um zu einem sicheren Zustand zurückzukehren. Während ein absoluter Neustart in der physischen Welt eine Herausforderung darstellen kann, ist er in der Cloud-Umgebung der erste Ansatz zur Schadensbegrenzung. • Sie müssen möglicherweise forensische Analysen für eine kompromittierte Instanz durchführen, um die Grundursache zu ermitteln. Nur gut ausgebildete Sicherheitsexperten sollten eine solche Untersuchung durchführen und Sie sollten die infizierte Instanz isolieren, um weiteren Schaden und eine Infektion während der Untersuchung zu verhindern. Um eine Amazon EC2-Instanz für die Überprüfung zu isolieren, können Sie beispielsweise eine sehr restriktive Sicherheitsgruppe einrichten. Schließen Sie alle Ports, sodass nur eingehender SSH- oder RDP-Verkehr von einer einzigen IP-Adresse akzeptiert wird, von der aus der forensische Prüfer die Instanz sicher untersuchen kann. Sie können auch einen Amazon EBS-Offline-Snapshot der infizierten Instanz aufnehmen und den Offline-Snapshot dann an den forensischen Prüfer zur umfassenden Analyse weitergeben. AWS hat keinen Zugriff auf die privaten Informationen innerhalb Ihrer Instanzen oder anderer Ressourcen, daher können wir Gastbetriebssysteme oder Beschädigungen auf Anwendungsebene, wie etwa die Übernahme eines Anwendungskontos, nicht ermitteln. AWS kann Informationen (wie etwa Zugriffsprotokolle, IP-Verbindungsprotokolle oder andere Attribute) nicht rückwirkend bereitstellen, wenn Sie diese Daten nicht mithilfe eigener Tools aufzeichnen. Die meisten Maßnahmen zur Untersuchung von Störungen und zur Schadensbegrenzung gehören in Ihren Verantwortungsbereich. • Der letzte Schritt, den Sie durchführen müssen, um kompromittierte Amazon EC2-Instanzen wiederherzustellen, besteht darin, wichtige Unternehmensdaten zu sichern, die infizierten Instanzen komplett zu beenden und sie dann als frische Instanzen neu zu starten. Um zukünftige Beeinträchtigungen zu vermeiden, empfehlen wir, die Sicherheitskontrollumgebung der neu gestarteten Instanzen zu überprüfen. Einfache Schritte, wie das Anwenden der aktuellsten Software-Patches und einschränkende Firewalls, sind effiziente und wirksame Maßnahmen.
Richten Sie eine E-Mail-Adresse für Sicherheitsinformationen ein.	Das AWS-Missbrauchsteam versendet E-Mails, um Missbrauchswarnungen zu kommunizieren. Diese E-Mails werden an die von Ihnen registrierte E-Mail-Adresse versendet. Wenn Sie jedoch in einem großen Unternehmen arbeiten, ist es ratsam, eine dedizierte Antwort-E-Mail-Adresse für diese Zwecke einzurichten. Sie können auf der Seite **Personal Information** unter **Configure Additional Contacts** zusätzliche E-Mail-Adressen einrichten.

Tabelle 19: Best Practices für das Einschränken von Missbrauch

Anwenden zusätzlicher Verfahren für die Anwendungssicherheit

Hier finden Sie einige zusätzliche Best Practices für mehr Sicherheit für Ihre Betriebssysteme und Anwendungen:

- Ändern Sie immer die vom Anbieter bereitgestellten Standardwerte, bevor Sie neue AMIs erstellen oder bevor Sie neue Anwendungen bereitstellen. Hierzu gehören unter anderem Passwörter, Community-Strings für SNMP (Simple Network Management Protocol) und Sicherheitskonfigurationen.

- Entfernen oder deaktivieren Sie nicht benötigte Benutzerkonten.

- Implementieren Sie eine einzige Hauptfunktion pro Amazon EC2-Instanz, um zu verhindern, dass Funktionen, die unterschiedliche Sicherheitsstufen erfordern, auf demselben Server vorhanden sind. Richten Sie beispielsweise Webserver, Datenbankserver und DNS auf verschiedenen Servern ein.

- Aktivieren Sie nur erforderliche und sichere Services, Protokolle, Daemons etc., die für das Funktionieren des Systems benötigt werden. Deaktivieren Sie alle nicht erforderlichen Services, da sie das Sicherheitsrisiko für die Instanz und das gesamte System erhöhen.

- Deaktivieren oder entfernen Sie alle unnötigen Funktionen, wie etwa Scripts, Treiber, Funktionen, Subsysteme, EBS-Volumes und unnötige Webserver.

Denken Sie bei der Konfiguration aller Services an die Best Practices für die Sicherheit. Aktivieren Sie Sicherheitsfunktionen für alle erforderlichen Services, Protokolle oder Daemons. Ziehen Sie Services wie SSH, die integrierte Sicherheitsmechanismen für Benutzer-/Peer-Authentifizierung, Verschlüsselung und Datenintegritätsauthentifizierung aufweisen, gegenüber weniger sicheren Services wie Telnet vor. Verwenden Sie SSH für Dateiübertragungen anstelle von unsicheren Protokollen wie FTP. In den Bereichen, in denen Sie nicht vermeiden können, weniger sichere Protokolle und Services zu verwenden, sollten Sie zusätzliche Sicherheitsschichten einführen, wie IPSec oder andere VPN-Technologien, um die Kommunikationskanäle auf Netzwerkebene zu schützen, oder GSS-API, Kerberos, SSL oder TLS, um Netzwerkverkehr auf Anwendungsebene zu schützen.

Konsequente Sicherheitsstandards sind wichtig für alle Organisationen. Gleichzeitig sind sie eine bewährte Methode zur Umsetzung von Sicherheitsrichtlinien. Konfigurieren Sie, wann immer möglich, Ihre Systemsicherheitsparameter so, dass sie mit Ihren Sicherheitsrichtlinien und -vorgaben konform sind, um Missbrauch zu vermeiden.

Für den Verwaltungszugriff auf Systeme und Anwendungen verschlüsseln Sie den gesamten Nichtkonsolen-Verwaltungszugriff mithilfe effektiver Kryptographiemechanismen. Verwenden Sie Technologien wie SSH, IPSec-VPNs (User-to-Site oder Site-to-Site) oder SSL/TLS für weitere, sichere Remote-Systemverwaltung.

Schützen Ihrer Infrastruktur

In diesem Abschnitt finden Sie Empfehlungen für das Schützen von Infrastruktur-Services auf der AWS-Plattform.

Verwenden von Amazon Virtual Private Cloud (VPC)

Mit Amazon Virtual Private Cloud (VPC) können Sie private Clouds innerhalb einer öffentlichen AWS-Cloud erstellen.

Jede Amazon VPC eines Kunden verwendet den vom Kunden zugewiesenen IP-Adressraum. Sie können private IP-Adressen (wie von RFC 1918 empfohlen) für Ihre Amazon VPCs verwenden und private Clouds und zugeordnete Netzwerke in der Cloud erstellen, die nicht direkt im Internet verfügbar sind.

Amazon VPC bietet nicht nur Isolierung von anderen Kunden in der privaten Cloud, sondern bietet außerdem Layer 3-Isolierung (IP-Routing durch die Vermittlungsschicht) vom Internet. In Tabelle 20 finden Sie Optionen für den Schutz Ihrer Anwendungen in Amazon VPC:

Bedrohung	Beschreibung	Empfohlene Schutzmaßnahme
Nur Internet	Die Amazon VPC ist nicht mit einer Ihrer Infrastrukturen vor Ort oder an einem anderen Ort verbunden. Sie verfügen über eine zusätzliche Infrastruktur vor Ort oder an einem anderen Ort oder auch nicht. Wenn Sie Verbindungen von Internetbenutzern akzeptieren müssen, können Sie eingehenden Zugriff bereitstellen, indem Sie Elastic IP-Adressen (EIPS) nur den Amazon VPC-Instanzen zuordnen, die sie benötigen. Sie können eingehende Verbindungen weiter einschränken, indem Sie Sicherheitsgruppen oder NACLs nur für bestimmte Ports und Quell-IP-Adressbereichen verwenden. Wenn Sie Load Balancing für eingehenden Datenverkehr aus dem Internet durchführen können, benötigen Sie keine EIPs. Sie können Instanzen hinter Elastic Load Balancing positionieren. Für ausgehenden Zugriff (zum Internet), etwa um Softwareupdates abzurufen oder um auf Daten öffentlicher AWS-Services wie Amazon S3 zuzugreifen, können Sie eine NAT-Instanz verwenden, um Masquerading für ausgehende Verbindungen bereitzustellen. EIPs sind nicht erforderlich.	Verschlüsseln Sie Anwendungs- und Verwaltungsdatenverkehr mithilfe von SSL/TLS oder erstellen Sie benutzerdefinierte VPN-Lösungen. Planen Sie die Routing- und Serverplatzierung in öffentlichen und privaten Subnetzen sorgfältig. Verwenden Sie Sicherheitsgruppen und NACLs.
IPSec über das Internet	AWS stellt eine stabile Infrastruktur für IPSec-Terminierung für VPC nach Branchenstandards bereit. Kunden können IPSec-Tunnel von ihren Standorten oder anderen VPN-Infrastrukturen zu Amazon VPC einrichten.	Stellen Sie eine private IPSec-Verbindung mithilfe von IKEv1 und IPSec unter Verwendung standardmäßiger AWS VPN-Funktionen (Amazon VPC VPN-

	IPSec-Tunnel werden zwischen AWS und Ihren Infrastrukturendpunkten eingerichtet. Anwendungen, die in der Cloud oder vor Ort ausgeführt werden, machen keine Änderungen erforderlich und können sofort vom IPSec-Datenschutz bei der Übertragung profitieren.	Gateways, Kunden-Gateways und VPN-Verbindungen) her. Richten Sie alternativ eine kundenspezifische VPN-Softwareinfrastruktur in der Cloud und vor Ort ein.
AWS Direct Connect ohne IPSec	Mit AWS Direct Connect können Sie eine Verbindung mit Ihrer Amazon VPC mithilfe von privatem Peering mit AWS über bestimmte Links herstellen, ohne das Internet zu verwenden. Sie haben vorbehaltlich Ihrer Datenschutzanforderungen die Möglichkeit, IPSec in diesem Fall nicht zu verwenden.	Abhängig von Ihren Datenschutzanforderungen kann es sein, dass Sie keinen zusätzlichen Schutz durch privates Peering benötigen.
AWS Direct Connect mit IPSec	Sie können IPSec über AWS Direct Connect-Links für zusätzlichen, umfassenden Schutz verwenden.	Siehe "IPSec über das Internet" weiter oben.
Hybrid	Sie können eine Kombination dieser Ansätze in Betracht ziehen. Wenden Sie für jeden Konnektivitätsansatz, den Sie verwenden, entsprechende Schutzmechanismen an.	

Tabelle 20: Zugriff auf Ressourcen in Amazon VPC

Sie können Amazon VPC-IPSec oder VPC-AWS Direct Connect verwenden, um Infrastrukturen vor Ort oder andere gehostete Infrastrukturen nahtlos und sicher in Ihre Amazon VPC-Ressourcen zu integrieren. Bei beiden Ansätzen schützen IPSec-Verbindungen Daten bei der Übertragung, während BGP auf IPSec- oder AWS Direct Connect-Links Ihre Amazon VPC-Routing-Domains und Ihre Routing-Domains vor Ort für die transparente Integration für alle Anwendungen integrieren, sogar Anwendungen, die keine systemeigenen Netzwerksicherheitsmechanismen unterstützen.

Obwohl VPC-IPSec transparenten Schutz nach Industriestandards für Ihre Anwendungen bereitstellt, möchten Sie vielleicht zusätzliche Ebenen von Schutzmechanismen verwenden, wie etwa SSL/TLS über VPC-IPSec-Links.

Weitere Informationen finden Sie im Whitepaper Amazon VPC Connectivity Options.

Verwenden von Sicherheitszonen und Netzwerksegmentierung

Unterschiedliche Sicherheitsanforderungen machen unterschiedliche Sicherheitskontrollen erforderlich. Im Bereich Sicherheit ist es eine bewährte Methode, Infrastrukturen in Zonen zu unterteilen, in denen ähnliche Sicherheitskontrollen erforderlich sind.

Der Großteil der AWS zugrunde liegenden Infrastruktur wird von AWS-Betriebs- und -Sicherheitsteams verwaltet. Dennoch können Sie Ihre eigenen Overlay-Infrastrukturkomponenten erstellen. Amazon VPCs, Subnetze, Routing-Tabellen, segmentierte/in Zonen unterteilte Anwendungen und benutzerdefinierte Service-Instanzen wie Benutzer-Repositorien, DNS und Zeitserver ergänzen die AWS-verwaltete Cloud-Infrastruktur.

Teams von Netzwerktechnikern interpretieren Segmentierung normalerweise als eine weitere Infrastrukturdesignkomponente und wenden netzwerkspezifische Zugriffskontroll- und Firewall-Regeln für die Zugriffsverwaltung an. Sicherheits-Zoning und Netzwerksegmentierung sind zwei unterschiedliche Konzepte. Dennoch gilt Folgendes: Ein Netzwerksegment isoliert einfach ein Netzwerk von einem anderen. Mithilfe von Sicherheits-Zoning dagegen wird eine Gruppe von Systemkomponenten mit ähnlichen Sicherheitsstufen mit gemeinsamen Kontrollen erstellt.

In AWS können Sie Netzwerksegmente mithilfe der folgenden Zugriffskontrollmechanismen erstellen:

- Verwenden von **Amazon VPC** zum Definieren eines isolierten Netzwerks für jede Arbeitslast oder Organisationseinheit.
- Verwenden von **Sicherheitsgruppen** zum Verwalten des Zugriffs auf Instanzen, die ähnliche Funktionen und Sicherheitsanforderungen aufweisen. Sicherheitsgruppen sind zustandsbehaftete Firewalls, die Firewall-Regeln in beide Richtungen für alle zulässigen und eingerichteten TCP-Sitzungen oder UDP-Kommunikationskanäle ermöglichen.
- Verwenden von **Netzwerkzugriffskontrolllisten** (Network Access Control Lists, NACLs), welche die zustandslose Verwaltung von IP-Verbindungen ermöglichen. NACLs sind unabhängig von TCP- und UDP-Sitzungen, aber sie ermöglichen die differenzierte Kontrolle über IP-Protokolle (beispielsweise GRE, IPSec ESP, ICMP) sowie die Kontrolle über eine Quell/Ziel-IP-Adresse und einen Quell/Ziel-IP-Port für TCP und UDP. NACLs funktionieren in Verbindung mit Sicherheitsgruppen und können Datenverkehr zulassen oder ablehnen, sogar bevor er die Sicherheitsgruppe erreicht.
- Verwendung **hostbasierter Firewalls** zur Kontrolle des Zugriffs auf jede Instanz.
- Erstellen einer **Ebene zum Schutz vor Bedrohungen** im Datenfluss und Erzwingen, dass der gesamte Datenverkehr die Zone durchläuft.
- Anwenden von **Zugriffkontrollen auf anderen Ebenen** (etwa Anwendungen und Services).

In herkömmlichen Umgebungen ist es erforderlich, dass separate Netzwerksegmente unterschiedliche Übertragungsentitäten darstellen, um Datenverkehr über ein zentrales Sicherheitssystem wie etwa eine Firewall weiterzuleiten. Das Konzept von Sicherheitsgruppen in der AWS-Cloud macht diese Anforderung überflüssig. Sicherheitsgruppen sind logische Gruppierungen von Instanzen und sie ermöglichen auch die Erzwingung von Regeln für eingehenden und ausgehenden Datenverkehr für diese Instanzen, unabhängig vom Subnetz, in dem sich diese Instanzen befinden.

Das Erstellen einer Sicherheitszone erfordert zusätzliche Kontrollen pro Netzwerksegment. Häufig zählen hierzu unter anderem:

- **Gemeinsame Zugriffskontrolle** – ein zentrales Identity and Access Management (IAM)-System. Beachten Sie, dass obwohl ein Verbund möglich ist, dies oft von IAM getrennt ist.
- **Gemeinsame Auditprotokollierung** – gemeinsame Protokollierung ist für die Ereignisanalyse und -zuordnung sowie das Nachverfolgen von Sicherheitsereignissen erforderlich.
- **Gemeinsame Datenklassifizierung**– im Abschnitt Tabelle 1: Beispiele für Komponenten
- Entwerfen Sie *Ihr eigenes ISMS zum Schutz* Ihrer Komponenten finden Sie weitere Informationen.
- **Gemeinsame Verwaltungsinfrastruktur** – verschiedene Komponenten, wie Antivirus-/Antispam-Systeme, Patch-Systeme und Leistungsüberwachungssysteme.
- Gemeinsame Sicherheitsanforderungen (Vertraulichkeit/Integrität) – oft in Verbindung mit Datenklassifizierung.

Um Ihre Anforderungen im Bereich Netzwerksegmentierung und Sicherheits-Zoning einschätzen zu können, beantworten Sie die folgenden Fragen:

- Kontrolliere ich die Kommunikation zwischen verschiedenen Zonen? Kann ich Netzwerksegmentierungs-Tools verwenden, um die Kommunikation zwischen den Sicherheitszonen A und B zu verwalten? Normalerweise sollten Zugriffskontrollelemente wie Sicherheitsgruppen, ACLs und Netzwerk-Firewall die Trennungen zwischen Sicherheitszonen erstellen. Amazon VPCs erstellen standardmäßig Trennungen zur Isolation der Zonen.
- Kann ich die Kommunikation zwischen Zonen mithilfe eines IDS-/IPS-/DLP-/SIEM-/NBAD-Systems überwachen, abhängig von den Unternehmensanforderungen? Das Blockieren des Zugriffs und das Verwalten des Zugriffs sind unterschiedliche Konzepte. Die durchlässige Kommunikation zwischen Sicherheitszonen macht leistungsstarke Tools für das Sicherheits-Monitoring zwischen den Zonen erforderlich. Die horizontale Skalierbarkeit von AWS-Instanzen ermöglicht es, für jede Instanz auf Betriebssystemebene Zonen zu erstellen und hostbasierte Vorrichtungen für das Sicherheits-Monitoring zu nutzen.
- Kann ich Zugriffskontrollrechte pro Zone anwenden? Einer der Vorteile der Verwendung von Zoning ist die Kontrolle von ausgehendem Zugriff. Es ist technisch möglich, den Zugriff durch Ressourcen wie Amazon S3- und Amazon SMS-Ressourcenrichtlinien zu kontrollieren.
- Kann ich jede Zone mithilfe dedizierter Verwaltungskanäle oder -rollen verwalten? Rollenbasierte Zugriffskontrolle für privilegierten Zugriff ist eine häufige Anforderung. Sie können mithilfe von IAM Gruppen und Rollen in AWS einrichten, um unterschiedliche Berechtigungsebenen zu erstellen. Sie können denselben Ansatz mit Anwendungs- und Systembenutzern nachahmen. Eine der wichtigen neuen Funktionen Amazon VPC-basierter Netzwerke ist die Unterstützung für mehrere elastische Netzwerkschnittstellen. Sicherheitstechniker können ein Overlay-Netzwerk für die Verwaltung mithilfe von Instanzen mit zwei Heimatnetzen erstellen.
- Kann ich Vertraulichkeits- und Integritätsregeln pro Zone anwenden? Verschlüsselung pro Zone, Datenklassifizierung und DRM verbessern insgesamt die Sicherheitslage. Wenn die Sicherheitseinstellungen in den einzelnen Sicherheitszonen unterschiedlich sind, dann müssen die Datensicherheitsanforderungen auch unterschiedlich sein. Zudem ist es immer ratsam, verschiedene Verschlüsselungsoptionen mit rotierenden Schlüsseln für die einzelnen Sicherheitszonen zu verwenden.

AWS bietet flexible Optionen für das Einrichten von Sicherheitszonen. Sicherheitstechniker und -architekten können die folgenden AWS-Funktionen nutzen, um isolierte Sicherheitszonen/-segmente in AWS durch Amazon VPC-Zugriffskontrolle zu erstellen:

- Zugriffskontrolle pro Subnetz
- Zugriffskontrolle pro Sicherheitsgruppen
- Zugriffskontrolle pro Instanz(hostbasiert)
- Routing-Block pro Amazon VPC
- Richtlinien pro Ressource (S3/SNS/SMS)
- Zonenweise IAM-Richtlinien
- Zonenweise Protokollverwaltung
- Zonenweise IAM-Benutzer, Administrator
- Zonenweiser Protokoll-Feed
- Zonenweise Verwaltungskanäle (Rollen, Schnittstellen, Managementkonsolen)
- Zonenweise AMIs
- Zonenweise Datenspeicherungsressourcen (Amazon S3-Buckets oder Glacier-Archive)
- Zonenweise Benutzerverzeichnisse
- Zonenweise Anwendungen/Anwendungskontrolle

Mit elastischer Cloud-Infrastruktur und automatisierter Bereitstellung können Sie dieselben Sicherheitskontrollen auf alle AWS-Regionen anwenden. Wiederholbare und einheitliche Bereitstellungen verbessern die gesamte Sicherheitslage.

Verstärken der Netzwerksicherheit

In Übereinstimmung mit dem Modell geteilter Verantwortung konfiguriert AWS Infrastrukturkomponenten wie Netzwerke für Rechenzentren, Router, Switches und Firewalls auf sichere Art und Weise. Sie sind für die Kontrolle des Zugriffs auf Ihre Systeme in der Cloud und für das Konfigurieren der Netzwerksicherheit innerhalb Ihrer Amazon VPC sowie für sicheren eingehenden und ausgehenden Netzwerkverkehr verantwortlich.

Das Anwenden von Authentifizierung und Autorisierung für Ressourcenzugriffe ist von besonderer Wichtigkeit. Jedoch wird dadurch nicht verhindert, dass Angreifer Zugriff auf Netzwerkebene erhalten und versuchen, sich als autorisierte Benutzer auszugeben. Das Kontrollieren des Zugriffs auf Anwendungen und Services basierend auf den Netzwerkstandorten der Benutzer bietet eine zusätzliche Sicherheitsschicht. So kann beispielsweise eine webbasierte Anwendung mit sicherer Benutzerauthentifizierung ebenfalls von einer auf IP-Adressen basierenden Firewall, die Quelldatenverkehr auf einen bestimmten Bereich an IP-Adressen einschränkt, und von einem Intrusion-Prevention-System zur Eindämmung des Sicherheitsrisikos und Minimierung der potentiellen Angriffsfläche für die Anwendung profitieren.

Zu den Best Practices für die Netzwerksicherheit in der AWS-Cloud gehören unter anderem die Folgenden:

- Verwenden Sie immer Sicherheitsgruppen: Sie bieten zustandsbehaftete Firewalls für Amazon EC2-Instanzen auf Hypervisor-Ebene. Sie können mehrere Sicherheitsgruppen auf eine einzige Instanz und auf eine einzige ENI anwenden.
- Erweitern Sie Sicherheitsgruppen mit Netzwerk-ACLs: Sie sind zustandslos, bieten jedoch schnelle und effiziente Kontrollmöglichkeiten. Netzwerk-ACLs gelten nicht für bestimmte Instanzen, daher können sie eine weitere Ebene der Kontrolle, zusätzlich zu Sicherheitsgruppen, darstellen. Sie können das Vier-Augen-Prinzip auf die Verwaltung von ACLs und Sicherheitsgruppen anwenden.
- Verwenden Sie IPSec oder/und AWS Direct Connect für vertrauenswürdige Verbindungen zu anderen Websites. Verwenden Sie Virtual Gateway (VGW), wo Amazon VPC-basierte Ressourcen Remote-Netzwerkkonnektivität erforderlich machen.
- Schützen Sie Daten bei der Übertragung, um die Vertraulichkeit und Integrität von Daten sowie die Identitäten der kommunizierenden Parteien sicherzustellen.
- Legen Sie für groß angelegte Bereitstellungen die Netzwerksicherheit in Schichtenfest. Wenden Sie Netzwerksicherheit auf externe, DMZ- und interne Schichten an, anstatt eine einzelne Schutzschicht für die Netzwerksicherheit zu erstellen.

Viele der AWS-Service-Endpunkte, mit denen Sie interagieren, bieten keine systemeigene Firewall-Funktionalität oder Zugriffskontrolllisten. AWS überwacht und schützt diese Endpunkte mit hochmodernen Kontrollsystemen auf Netzwerk- und Anwendungsebene. Sie können IAM-Richtlinien verwenden, um den Zugriff auf Ihre Ressourcen basierend auf der Quell-IP-Adresse der Anforderung einzuschränken.

Die Sicherung von Peripheriesystemen: Benutzer-Repositorien, DNS, NTP

Overlay-Sicherheitskontrollen sind nur dann wirksam, wenn sie zusätzlich zu einer sicheren Infrastruktur eingerichtet werden. Ein gutes Beispiel für diese Art der Kontrolle ist der DNS-Abfrage-Verkehr. Bei unzureichender Sicherung von DNS-Systemen kann der Datenverkehr von DNS-Kunden abgefangen werden, wodurch DNS-Namen in Abfragen oder Antworten manipuliert ("spoofed") werden können. Das "Spoofing" ist ein einfacher, aber wirksamer Angriff auf eine Infrastruktur, in der keine grundlegende Kontrolle existiert. SSL/TLS kann zusätzlichen Schutz bieten.

Manche AWS-Kunden nutzen Amazon Route 53, einen sicheren DNS-Dienst. Sollten Sie ein internes DNS benötigen, können Sie eine maßgeschneiderte DNS-Lösung auf Amazon EC2-Instanzen implementieren. Das DNS ist ein wesentlicher Bestandteil unserer Lösungsinfrastruktur und hat als solcher maßgeblichen Anteil an unserem

Sicherheitsverwaltungsplan. So wie in anderen wichtigen benutzerdefinierten Infrastrukturkomponenten auch, sollten in allen DNS-Systemen die folgenden Kontrollen Anwendung finden:

Gemeinsame Kontrolle	Beschreibung
Separater Zugang zu Verwaltungsebenen	Implementierung von Rollentrennung und Zugriffskontrollen zur Beschränkung des Zugangs zu diesen Diensten, häufig getrennt von der für den Anwendungszugang erforderlichen Zugriffskontrolle, sowie des Zugangs zu anderen Teilen der Infrastruktur.
Monitoring, Alarmierung, Prüfpfad	Protokollierung und Monitoringautorisierter und nicht autorisierter Aktivitäten
Kontrolle des Zugriffs auf die Netzwerkebene	Beschränkung des Netzwerkzugriffs ausschließlich auf Systeme, die diesen benötigen Sofern möglich, Durchsetzung einer Protokollierungspflicht für alle Zugriffsversuche auf Netzwerkebene (nämlich Durchsetzung benutzerdefinierter RFC-Standards für NTP und DNS)
Auf dem neuesten Stand befindliche stabile Software mit Sicherheitspatches	Sicherstellung, dass Software gepatcht und immun gegen bekannte Sicherheitslücken oder sonstige Risiken ist
Fortlaufende Sicherheitstests (Bewertungen)	Sicherstellung regelmäßiger Überprüfungen der Infrastruktur
Alle sonstigen Sicherheitskontrollprozesse vorhanden	Sicherstellung, dass die Peripheriesysteme neben Service-spezifischen maßgeschneiderten Sicherheitskontrollen im Einklang mit den Best Practices für Informationssicherheits-Managementsysteme (ISMS) funktionieren

Tabelle 21: Kontrollen für Peripheriesysteme

Nicht nur das DNS, sondern auch andere Infrastruktur-Services könnten spezifische Kontrollen erfordern.

Für das Risikomanagement ist eine zentrale Zugriffskontrolle von entscheidender Bedeutung. Der IAM-Service bietet rollenbasierte Identitäts- und Zugriffsverwaltung für AWS, allerdings hält AWS keine Endbenutzer-Repositorien wie Active Directory, LDAP oder RADIUS für Ihre Betriebssysteme und Anwendungen bereit. Sie erstellen vielmehr Benutzeridentifikations- und -authentifizierungssysteme, daneben AAA-Server (Authentifizierung, Autorisierung und Kontoverwaltung), manchmal auch proprietäre Datenbanktabellen. Alle Identitäts- und Zugriffsverwaltungsserver für Benutzerplattformen und Anwendungen sind sicherheitskritische Systeme und erfordern besondere Aufmerksamkeit.

Zu den kritischen benutzerspezifischen Diensten zählen auch Zeitserver. Sie sind für viele sicherheitsrelevante Transaktionen unerlässlich, darunter die Erstellung von Zeitstempeln für Protokolle und die Validierung von Zertifikaten. Es ist sehr wichtig, einen zentralen Zeitserver zu nutzen und alle Systeme mit demselben Zeitserver zu synchronisieren. Der Datensicherheitsstandard (DSS) der Zahlungskartenindustrie (PCI) schlägt folgenden guten Ansatz für die Zeitsynchronisierung vor:

- Überprüfen, ob die Zeitsynchronisierungstechnologie implementiert und auf dem neuesten Stand ist
- Überprüfung des Verfahrens zur Erfassung, Verteilung und Speicherung der korrekten Zeit innerhalb der Organisation sowie Überprüfung der Einstellungen zeitrelevanter Systemparameter für ausgesuchte Systemkomponenten
- Überprüfung, dass ausschließlich die dafür vorgesehenen Zeitserver Zeitsignale von externen Quellen empfangen, und dass besagte Zeitsignale auf der Internationalen Atomzeit bzw. koordinierten Weltzeit (UTC) basieren
- Überprüfung, dass zwischen den zugewiesenen Zeitservern ein ständiger Abgleich erfolgt, um die korrekte Zeit zu gewährleisten, und dass andere interne Server die Zeit ausschließlich von den zentralen Zeitservern erhalten
- Überprüfung der Systemkonfigurationen und Einstellungen der Zeitsynchronisation, um sicherzustellen, dass der Zugriff auf Zeitdaten auf Mitarbeiter beschränkt bleibt, die aus dienstlichen Gründen auf die Zeitdaten zugreifen müssen
- Überprüfung der Systemkonfigurationen sowie Einstellungen und Abläufe der Zeitsynchronisation, um sicherzustellen, dass Änderungen an den Zeiteinstellungen kritischer Systeme protokolliert, überwacht und überprüft werden
- Überprüfung, dass die Zeitserver Zeit-Updates von speziellen, branchenweit anerkannten externen Quellen erhalten. (Dies hilft mit zu verhindern, dass die Uhr von einer Einzelperson in böser Absicht verstellt wird.) (Sie haben die Möglichkeit, sich diese Updates mit einem symmetrischen Schlüssel verschlüsselt zukommen zu lassen. Ferner können Sie Zugriffskontrolllisten erstellen, die die IP-Adressen der zu aktualisierenden Client-Computer enthalten. Hierdurch lässt sich die nicht autorisierte Nutzung interner Zeitserver besser verhindern.)

Die Überprüfung der Sicherheit benutzerdefinierter Infrastrukturen ist ein zentraler Bestandteil des Sicherheitsmanagements in der Cloud.

Erstellung von Schutzschichten

Viele Organisationen greifen als bewährte Methode zum Schutz ihrer Netzwerkinfrastruktur auf einen mehrschichtigen Sicherheitsansatz zurück. In der Cloud lassen sich Amazon VPC, implizite Firewall-Regeln auf Hypervisor-Ebene neben Netzwerkzugriffskontrolllisten, Sicherheitsgruppen, hostbasierte Firewalls und IDS/IPS-Systeme als schichtbezogene Lösung für die Netzwerksicherheit kombinieren.

Während Sicherheitsgruppen, NACLs und hostbasierte Firewalls für viele Kunden ausreichend sind, sollten Sie, wenn Sie umfassenden Schutz wünschen, eine Sicherheitskontrollanwendung auf Netzwerkebene einsetzen. Dies sollte "inline" erfolgen, dort wo der Verkehr abgefangen und analysiert wird, bevor er zu seinem Bestimmungsort, beispielsweise einem Anwendungsserver, weitergeleitet wird.

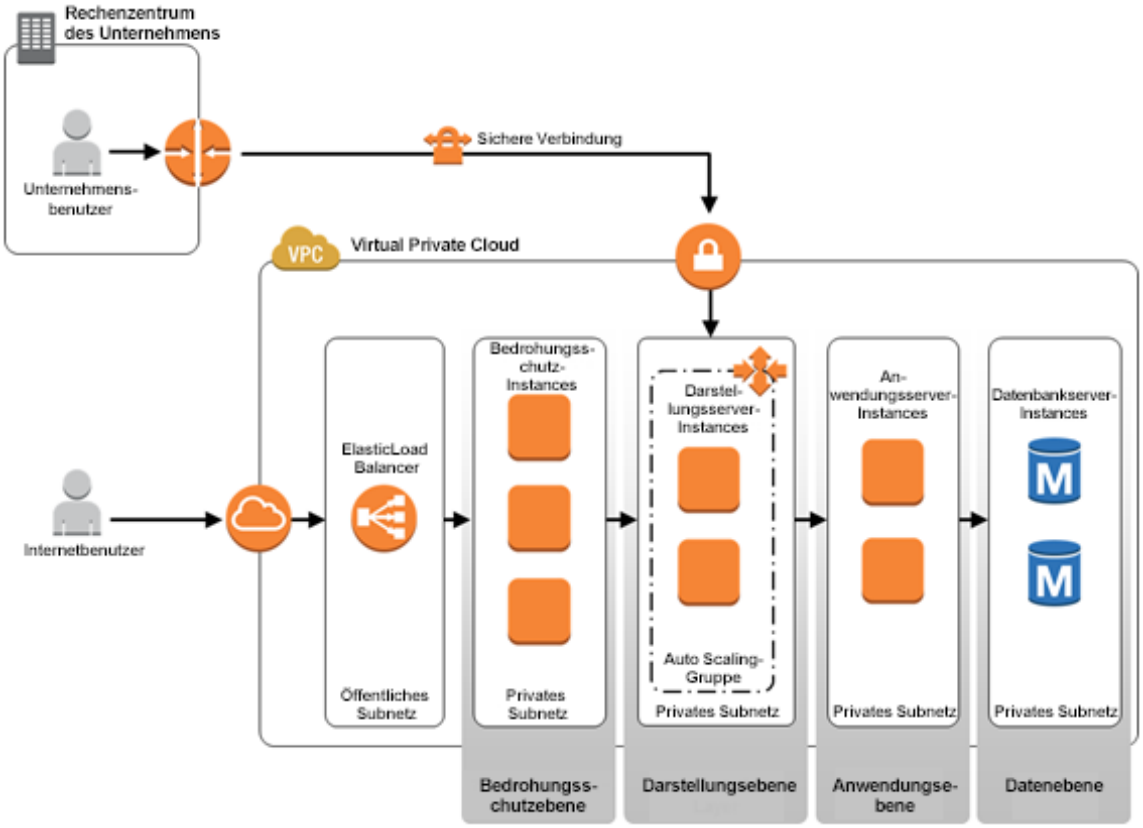

Abbildung 6: Schichtbezogener Netzwerkschutz in der Cloud

Zu den Technologien der Inline Threat Protection zählen u. a. folgende:

- Auf Amazon EC2-Instanzen installierte Firewall-Einrichtungen Dritter (auch als „Soft Blades“ bekannt)
- UTM-Gateways (Unified Threat Management)
- Intrusion-Prevention-Systeme
- Gateways zum Management von Datenverlusten
- Gateways zur Erkennung von Unregelmäßigkeiten
- Erweiterte Gateways zur Erkennung von Dauergefährdungen

Folgende Hauptfunktionen der Amazon VPC-Infrastruktur unterstützen die Bereitstellung von schichtbezogenen Technologien zum Schutz vor Bedrohungen:

- **Unterstützung mehrerer Ebenen von Load Balancern:** Wenn Sie Sicherheits-Gateways für den Schutz von Clustern aus Webservern, Anwendungsservern oder sonstigen kritischen Servern nutzen, ist die Skalierbarkeit von entscheidender Bedeutung. AWS-Referenzarchitekturen betonen die Bereitstellung externer und interner Load Balancer für das Risikomanagement, die interne Serverlastverteilung sowie Hochverfügbarkeit. Sie können Elastic Load Balancing oder Ihre eigenen Lastverteilungsvorrichtungen für Ihre mehrstufigen Systeme wirksam einsetzen. Für zustandsbehaftete Gateway-Installationen müssen Sie die Sitzungsaufrechterhaltung auf Load-Balancer-Ebene verwalten.
- **Unterstützung mehrerer IP-Adressen:** Wenn durch Sicherheits-Gateways eine Darstellungsschicht geschützt wird, die mehrere Instanzen umfasst (z. B. Webserver, E-Mail-Server, Anwendungsserver), dann müssen diese mehreren Instanzen ein gemeinsames Sicherheits-Gateway in einer n:1-Beziehung nutzen. AWS unterstützt mehrere IP-Adressen für eine einzige Netzwerkschnittstelle.
- **Unterstützung von Schnittstellen für mehrere elastische Netzwerke (Elastic Network Interfaces, ENI):** Die Sicherheits-Gateways müssen zwei Heimatnetze sowie in vielen Fällen – je nach Komplexität des Netzwerks – mehrere Schnittstellen aufweisen. Mithilfe des ENI-Konzepts unterstützt AWS mehrere Netzwerkschnittstellen auf mehreren unterschiedlichen Instanztypen, was den Einsatz von Sicherheitsfunktionen für mehrere Zonen ermöglicht.

Aufgrund von Latenz, Komplexität und weiteren architekturbedingten Einschränkungen ist mitunter die Nutzung einer internen Risikomanagementebene ausgeschlossen. In solchen Fällen können Sie auf eine der folgenden Alternativen ausweichen.

- Eine **verteilte Lösung für den Schutz vor Bedrohungen**: Bei diesem Ansatz werden Sicherheitsvorrichtungen individuell auf Instanzen in der Cloud installiert. Ein zentraler Sicherheitsserver kommuniziert mit allen hostbasierten Threat Management-Vorrichtungen zwecks Protokollerfassung, -analyse, -zuordnung sowie aktivem Umgang mit Bedrohungen.
- Eine **Overlay-Lösung für die Netzwerksicherheit**: Einrichtung eines übergelagernden Netzwerks über Ihr Amazon VPC unter Nutzung von Technologien wie GRE-Tunnels, vtun-Schnittstellen oder durch die Weiterleitung von Datenverkehr eines anderen ENI zu einer zentralen Netzwerkverkehrsanalyse sowie einem Intrusion-Detection-System, das einen aktiven oder passiven Schutz vor Bedrohungen bietet.

Überprüfung der Sicherheit

Jedes Informationssicherheits-Managementsystem muss regelmäßige Überprüfungen der Wirksamkeit von Sicherheitskontrollen und -vorschriften gewährleisten. Um die Wirksamkeit von Kontrollen auf neue Bedrohungen und Schwachstellen sicherzustellen, müssen die Kunden dafür sorgen, dass die Infrastruktur vor Angriffen geschützt wird.

Für die Überprüfung vorhandener Kontrollen sind Tests erforderlich. AWS-Kunden sollten mehrere Testansätze durchführen:

- **Externe Sicherheitsrisikobewertung:** Die Bewertung der Systemschwachstellen wird von Dritten durchgeführt, die über keine oder nur wenig Kenntnisse der Infrastruktur und ihrer Bestandteile verfügen;
- **Externe Penetrationstests:** Ein Dritter, dem das System vollständig oder weitgehend unbekannt ist, versucht aktiv in kontrollierter Weise in das System einzudringen.
- **Interne Gray/White-Box-Prüfung von Anwendungen und Plattformen**: Ein Prüfer, der vollständig oder weitgehend mit dem System vertraut ist, bewertet die Wirksamkeit der vorhandenen Kontrollen bzw. untersucht Anwendungen und Plattformen auf bekannte Schwachstellen.

In der AWS Acceptable Use Policy werden zulässiges und unzulässiges Verhalten in der AWS-Cloud beschrieben sowie Sicherheitsverletzungen und Netzwerkmissbrauch definiert. AWS unterstützt sowohl ein- als auch ausgehende

Penetrationstests in der Cloud, wobei Sie für die Durchführung von Penetrationstests Genehmigungen einholen müssen. Weitere Informationen finden Sie unter Amazon Web Services Acceptable Use Policy –http://*aws.amazon.com/aup/*.

Zur Beantragung von Penetrationstests für Ihre Ressourcen füllen Sie das Formular „Beantragung eines AWS-Schwachstellen-Penetrationstests“ aus und reichen es ein. Dafür müssen Sie in der AWS Management Console mit den Benutzerdaten eingeloggt sein, die mit den zu testenden Instanzen verknüpft sind, da im Formular sonst die falschen Daten vorausgefüllt werden. Soll der Penetrationstest von Dritten ausgeführt werden, müssen Sie das Formular selbst ausfüllen und bei Vorliegen der Genehmigung seitens AWS die Dritten informieren.

Das Formular enthält Informationen über die zu testenden Instanzen und das voraussichtliche Start- und Enddatum der Tests. Hierfür müssen Sie die für Penetrationstests und die Nutzung der entsprechenden Testwerkzeuge geltenden Bedingungen durchlesen und ihnen zustimmen. Die AWS-Richtlinien gestatten keine Tests von Instanzen vom Typ m1.small oder t1.micro. Nachdem Sie das Formular eingereicht haben, erhalten Sie innerhalb eines Werktags die Antwort mit der Eingangsbestätigung Ihres Antrags.

Sollten Sie für zusätzliche Tests mehr Zeit benötigen, können Sie auf die Autorisierungs-E-Mail antworten und darin um eine Verlängerung des Testzeitraums bitten. Jeder Antrag muss separat genehmigt werden.

Verwaltung von Metriken und Verbesserung

Die Messung der Kontrollwirksamkeit ist ein integraler Bestandteil jedes ISMS. Anhand von Metriken lässt sich darstellen, wie gut die Umgebung durch die Kontrollen geschützt wird. Das Risikomanagement ist häufig von qualitativen und quantitativen Metriken abhängig. Tabelle 22 enthält Best Practices zu Messung und Verbesserung:

Best Practices	Verbesserung
Monitoringund Überprüfung von Verfahren und sonstige Kontrollen	• Sofortige Fehlererkennung in den Verarbeitungsergebnissen • Sofortige Erkennung von versuchten und erfolgreichen Sicherheitsverletzungen • Versetzen Sie die Führungsebene in die Lage zu beurteilen, ob die an Personen delegierten bzw. IT-technisch umgesetzten Sicherheitsmaßnahmen erwartungsgemäß funktionieren. • Hilfe bei der Erkennung von Sicherheitsvorkommnissen und somit der Vermeidung von Sicherheitsvorfällen durch den Einsatz von Indikatoren • Feststellung, ob die unternommenen Maßnahmen zur Schließung einer Sicherheitslücke wirksam waren
Regelmäßige Überprüfung der Wirksamkeit des Informationssicherheits-Managementsystems	• Berücksichtigung der Ergebnisse von Sicherheitsprüfungen, Vorfällen und Wirksamkeitsmessungen sowie von Vorschlägen und Rückmeldungen aller Beteiligten • Sicherstellung, dass das ISMS die Richtlinien und Zielsetzungen erfüllt • Überprüfung von Sicherheitskontrollen
Messung der Kontrollwirksamkeit	• Überprüfung der Einhaltung von Sicherheitsanforderungen
Risikobewertungsprüfungen in regelmäßigen Abständen	Prüfung von Restrisiken und der erkannten annehmbaren Risiken unter Berücksichtigung folgender Faktoren: • Änderungen der Organisation, Technologie, Geschäftsziele und -vorgänge sowie erkannte Bedrohungen • Wirksamkeit der implementierten Kontrollen

	• Externe Ereignisse, darunter Änderungen der rechtlichen oder regulatorischen Umgebung, geänderte vertragliche Verpflichtungen oder Änderungen des sozialen Klimas
Interne ISMS-Prüfungen	Prüfungen auf erster Ebene (interne Prüfungen) werden von der Organisation selbst oder in ihrem Namen zu internen Zwecken durchgeführt.
Regelmäßige Prüfungen seitens der Unternehmensleitung	• Angemessenheit des Anwendungsbereichs des ISMS sicherstellen • Suche nach Verbesserungen im ISMS-Verfahren
Aktualisierung der Sicherheitskonzepte	• Berücksichtigung der Ergebnisse von Monitoring- und Prüfmaßnahmen • Erfassung von Maßnahmen und Ereignissen, die sich auf die Wirksamkeit oder Leistung des ISMS auswirken könnten

Tabelle 22: Verwaltung und Verbesserung von Metriken

Minimierung der Risiken von und Schutz vor DoS/DDoS-Attacken

Organisationen, die Internetanwendungen betreiben, ist das Risiko bekannt, Opfer von Denial-of-Service- (DoS) oder Distributed-Denial-of-Service- (DDoS) Attacken von Wettbewerbern, Aktivisten oder Einzelpersonen zu werden. Das Risikoprofil ist von der Art der Geschäftstätigkeit, aktuellen Ereignissen, der politischen Lage, aber auch dem Gefährdungsgrad der Technologie abhängig. Die Vermeidungs- und Schutztechniken ähneln jenen, die unternehmensintern genutzt werden.

Wenn Sie an einem Schutz vor und der Vermeidung von DoS/DDoS-Attacken interessiert sind, möchten wir Ihnen die Registrierung beim AWS Premium Support nahe legen, damit Sie die AWS-Supportdienste proaktiv und reaktiv in den Prozess der Vermeidung solcher Angriffe oder laufende Vorfälle innerhalb Ihrer Umgebung auf AWS einbeziehen können.

Manche Services, darunter Amazon S3, nutzen eine gemeinsame Infrastruktur, in der mehrere AWS-Konten Zugriff auf dieselben Komponenten der Amazon S3-Infrastruktur haben und darin Daten speichern können. In diesem Fall könnte sich eine DoS/DDoS-Attacke auf abstrakte Services sehr wahrscheinlich auf verschiedene Kunden auswirken. AWS bietet Kontrollen an, die sowohl der Risikominimierung als auch dem Schutz vor DoS/DDoS-Attacken auf abstrakte Services von AWS dienen, um die Auswirkungen auf Sie im Falle eines solchen Angriffs zu minimieren. Sie müssen keine zusätzlichen Schutzmaßnahmen gegen DoS/DDoS für diese Services ergreifen, jedoch empfehlen wir Ihnen, die in diesem Whitepaper genannten Best Practices anzuwenden.

Andere Services, darunter Amazon EC2, nutzen eine gemeinsame physische Infrastruktur. Die Verwaltung des Betriebssystems, der Plattform und der Kundendaten obliegt jedoch Ihnen. Bei diesen Services müssen wir gemeinsam an der Risikominderung und am effektiven Schutz vor DDoS-Atacken arbeiten.

Bei der Risikominimierung und Erkennung von DoS/DDoS-Attacken auf die AWS-Plattform bedient sich AWS proprietärer Techniken. Um jedoch den laufenden Benutzerverkehr nicht zu beeinträchtigen, stellt AWS entsprechend dem Modell geteilter Verantwortung keine Risikominimierung für einzelne Amazon EC2-Instanzen bereit und blockiert darin auch keinen Netzwerkverkehr: Nur Sie können feststellen, ob verstärkter (harmloser) Verkehr erwartet wird oder ob es sich um eine DoS/DDoS-Attacke handelt.

Für die Abwehr von DoS/DDoS-Attacken stehen in der Cloud eine ganze Reihe von Techniken zur Verfügung, dennoch empfehlen wir, dass Sie eine Sicherheits- und Performance-Baseline definieren, welche die Systemparameter unter normalen Bedingungen erfasst, in denen auch tages-, wochen-, jahresabhängige oder sonstige Muster berücksichtigt werden, die für Ihr Geschäft typisch sind. Einige DoS/DDoS-Schutztechniken, darunter Statistik- und Verhaltensmodelle, können Anomalien anhand eines Vergleichs mit normalen Betriebsmustern erkennen. So kann zum Beispiel ein Kunde, der auf seiner Webseite mit etwa 2 000 gleichzeitigen Besuchen zu einer bestimmten Tageszeit rechnet, mithilfe von Amazon CloudWatch oder Amazon SNS einen Alarm auslösen, wenn die aktuelle Anzahl gleichzeitiger Sitzungen diese Menge um das Doppelte (4 000) überschreitet.

Berücksichtigen Sie bei der Einrichtung Ihrer Sicherheitsvorkehrungen in der Cloud die gleichen Komponenten, die für Ihre internen Installationen gelten.

Tabelle 23 enthält gängige Ansätze für die Risikovermeidung und den Schutz vor DoS/DDoS-Angriffen in der Cloud.

Technik	Beschreibung	Schutz vor DoS/DDoS-Attacken
Firewalls: Sicherheitsgruppen, Listen für die Netzwerkzugriffskontrolle und hostbasierte Firewalls	Herkömmliche Firewall-Techniken verringern die Angriffsfläche für potenzielle Angreifer und unterbinden den Verkehr von und zur Quelle des Angriffs.	• Verwaltung der Liste erlaubter Zielserver und Services (IP-Adressen & TCP/UDP-Ports) • Verwaltung der Liste erlaubter Quellen von Besucherverkehr • Verwaltung der Liste erlaubter Protokolle • Explizite Sperrung (vorübergehend oder dauerhaft) des Zugriffs von bestimmten IP-Adressen aus
Web Application Firewalls (WAF)	Web Application Firewalls bieten Deep Packet Inspection für den Web-Datenverkehr.	• Plattform- und anwendungsspezifische Angriffe • Angriffe auf die Protokollplausibilität • Unautorisierter Benutzerzugriff
Hostbasierte oder interne IDS/IPS-Systeme	IDS/IPS-Systeme können bei der Erkennung von Netzwerkangriffen und Trojanern auf statistik-/verhaltensbasierte bzw. signaturbasierte Algorithmen zurückgreifen.	• Angriffe jeglicher Art

Traffic Shaping/Durchsatzbeschränkung	Häufig werden durch DoS/DDoS-Attacken die Netzwerk- und Systemressourcen erschöpft. Die Durchsatzbeschränkung eignet sich gut für den Schutz knapper Ressourcen vor übermäßigem Datenverkehr.	• ICMP-Flooding • Anwendungsanforderungs-Flooding
Beschränkung halbgeöffneter Sitzungen	TCP-SYN-Flooding-Attacken können sowohl in einfacher als auch verteilter Form erfolgen. In beiden Fällen können Sie, wenn Sie über eine Baseline des Systems verfügen, in halbgeöffneten (embryonischen) TCP-Sitzungen auffällige Abweichungen vom Normalzustand erkennen und alle weiteren TCP-SYN-Pakete aus den fraglichen Quellen ignorieren.	• TCP-SYN-Flooding

Tabelle 23: Techniken zur Risikovermeidung und zum Schutz vor DoS/DDoS-Angriffen

Neben herkömmlichen Ansätzen zur Risikominderung und zum Schutz vor DoS/DDoS-Attacken hält die AWS-Cloud je nach Elastizität verschiedene Funktionen bereit. DoS/DDoS-Attacken zielen auf die Erschöpfung beschränkter Rechen-, Speicher-, Festplatten- oder Netzwerkressourcen ab, was sich häufig nachteilig auf die lokale Infrastruktur auswirkt. Definitionsgemäß ist die AWD-Cloud jedoch elastisch, nämlich in dem Sinne, dass bei Bedarf und auf Anforderung zusätzliche Ressourcen verfügbar sind. Beispielsweise können Ihre Webserver während einer DDoS-Attacke durch ein Botnet Hunderttausenden von Anfragen pro Sekunde ausgesetzt sein, die von legitimen Benutzeranfragen nicht unterscheidbar sind. Wenn Sie herkömmliche Eindämmungsmaßnahmen einsetzen, würden Sie zunächst den Datenverkehr aus bestimmten Quellen blockieren, oftmals ganze Regionen, da Sie davon ausgehen, dass von dort nur Angriffe und keine normalen Kundenanfragen kommen. Diese Annahmen und Maßnahmen führen jedoch zum Ausfall des Services für Ihre eigentlichen Kunden.

In der Cloud haben Sie die Möglichkeit, eine solche Attacke abzuwehren. Durch den Einsatz von AWS-Technologien wie Elastic Load Balancing und Auto Scaling können Sie die Webserver dahingehend konfigurieren, dass sie im Falle einer Attacke (auf Grundlage von Last) ihre Aufnahmefähigkeit vergrößern und nach Beendigung der Attacke wieder schrumpfen. Selbst bei größeren Attacken hätten die Webserver genügend Kapazität, um ihre Funktion durch Nutzung der Cloud-Elastizität aufrechtzuerhalten und eine optimale Benutzererfahrung zu bieten. Durch das Auffangen der Attacke könnten Ihnen zusätzliche Servicekosten für AWS entstehen; gleichzeitig ist jedoch die Aufrechterhaltung einer solchen Attacke für den Angreifer dermaßen kostspielig, dass aufgefangene Attacken kaum über längere Zeiträume fortgesetzt werden.

Zur Abwehr von DoS/DDoS-Flooding-Angriffen könnten Sie auch Amazon CloudFront verwenden. Ein potenzieller Angreifer, der hinter CloudFront liegende Inhalte zu attackieren versucht, wird die meisten, wenn nicht alle Anfragen an Standorte am Rande von CloudFront richten, wo die AWS-Infrastruktur die zusätzlichen Anfragen mit äußerst geringen Auswirkungen auf die Backend-Server des Kunden abfangen kann. Auch hier würden für die Abwehr der Attacke durch AWS zusätzliche Servicegebühren anfallen. Diese sollten Sie jedoch gegen die Kosten abwägen, die dem Angreifer durch die Fortführung der Attacke entstünden.

Für eine wirksame Minimierung, Erkennung und allgemeine Verwaltung Ihres Risikos, DoS/DDoS-Attacken ausgesetzt zu werden, sollten Sie ein mehrschichtiges Schutzmodell errichten, das an anderer Stelle in diesem Dokument beschrieben wird.

Management von Sicherheits-Monitoring, Alarmierung, Prüfpfaden und Vorfallreaktion

Gemäß dem Modell geteilter Verantwortung sind Sie für das Monitoring und Verwaltung Ihrer Umgebung auf Betriebssystemebene und höheren Ebenen zuständig. Wahrscheinlich tun Sie dies bereits auf lokaler Ebene oder in anderen Umgebungen, so dass Sie Ihre vorhandenen Prozesse, Werkzeuge und Methoden für die Verwendung in der Cloud anpassen können.

Eine ausführliche Anleitung zum Sicherheits-Monitoring können Sie dem Whitepaper *ENISA Procure Secure* entnehmen, in dem die Konzepte eines fortlaufenden Sicherheits-Monitoring in der Cloud beschrieben werden (siehe *Referenzen und weiterführende Literatur*).

Beim Sicherheits-Monitoring sind zunächst die folgenden Fragen zu beantworten:

- Welche Parameter sollten wir messen?
- Wie sollten wir sie messen?
- Welche Schwellenwerte gelten für diese Parameter?
- Wie funktionieren Eskalationsprozesse?
- Wo werden die Daten gespeichert?

Die vielleicht wichtigste Frage dürfte lauten: "Was muss ich protokollieren?"

Wir empfehlen für Protokollierungs- und Analysezwecke die Konfigurierung folgender Bereiche:

- Jegliche Aktivitäten von Personen mit Root- oder Administratorberechtigungen
- Zugriff auf alle Prüfpfade
- Ungültige logische Zugriffsversuche
- Verwendung von Identifikations- und Authentifizierungsmechanismen
- Initialisierung von Auditprotokollen
- Erstellung und Löschung von Objekten auf Systemebene

Behalten Sie bei der Erstellung Ihrer Protokolldatei die Erwägungen aus Tabelle 24 im Auge:

Bereich	Erwägung
Protokollerfassung	Beachten Sie, wie Protokolldateien erfasst werden. Häufig werden Informationen für die Protokolldatei von Vorrichtungen des Betriebssystems, einer Anwendung oder Dritten/Middleware gesammelt.
Protokolltransport	Wenn Protokolldateien zentral erfasst werden, sorgen Sie für eine sichere, verlässliche und zeitnahe Übermittlung an den zentralen Standort.
Protokollspeicher	Nutzen Sie für verschiedene Instanzen zentrale Protokolldateien, um deren Aufbewahrung, aber auch Analysen und Zuordnungen zu ermöglichen.

Protokollsystematik	Sorgen Sie dafür, dass unterschiedliche Kategorien von Protokolldateien in einem analysetauglichen Format vorliegen.
Protokollanalyse/-zuordnung	Protokolldateien bieten Sicherheitsinformationen, wenn Sie diese analysieren und Ereignisse in Beziehung zueinander setzen. Die Analyse kann in Echtzeit oder in festgelegten Abständen erfolgen.
Protokollschutz/-sicherheit	Protokolldateien sind vertraulich. Schützen Sie diese durch Netzwerkkontrolle, Identitäts- und Zugriffsverwaltung, Verschlüsselung, Authentifizierung der Datenintegrität sowie manipulationssichere Zeitstempel.

Tabelle 24: Erwägungen zu Protokolldateien

Möglicherweise verfügen Sie über Security Logs aus unterschiedlichen Quellen. Protokolldateien werden von den verschiedensten Netzwerkkomponenten erstellt, darunter Firewalls, IDP, DLP, AV-Systeme, das Betriebssystem, Plattformen oder Anwendungen. Viele sind sicherheitsrelevant, und diese sollten in die Protokolldateistrategie einbezogen werden. Andere, die mit dem Thema Sicherheit nichts zu tun haben, bleiben besser davon ausgenommen. Protokolle sollten alle Benutzeraktivitäten, Ausnahmen und Sicherheitsvorfälle enthalten, und Sie sollten sie für einen bestimmten Zeitraum für Untersuchungszwecke aufbewahren.

Um herauszufinden, welche Protokolle berücksichtigt werden müssen, beantworten Sie die folgenden Fragen:

- Wer sind die Benutzer der Cloud-Systeme? Wie melden sie sich an, wie authentifizieren sie sich, wie werden sie für den Zugriff auf Ressourcen autorisiert?
- Welche Anwendungen greifen auf Cloud-Systeme zu? Wie gelangen sie an die Anmeldedaten, wie authentifizieren sie sich und wie werden sie für solche Zugriffe autorisiert?
- Welche Benutzer verfügen über privilegierten Zugriff (auf Verwaltungsebene) zu AWS-Infrastruktur, Betriebssystemen und Anwendungen? Wie authentifizieren sie sich und wie werden sie für solche Zugriffe autorisiert?

Viele Services stellen integrierte Prüfpfade für die Zugriffskontrolle bereit (zum Beispiel verfügen Amazon S3 und Amazon EMR über solche Protokolle), doch in manchen Fällen könnten Ihre betrieblichen Protokollierungsanforderungen über die des ursprünglichen Service-Protokolls hinausgehen. Erwägen Sie in solchen Fällen ein Privilegien-Eskalations-Gateway für die Verwaltung von Zugriffsprotokollen und Autorisierung.

Bei der Nutzung eines Privilegien-Eskalations-Gateways leiten Sie alle Zugriffe auf das System zentral über ein einziges (geclustertes) Gateway. Statt direkt auf die AWS-Infrastruktur, Ihre Betriebssysteme oder Anwendungen zuzugreifen, erfolgen alle Anfragen von Proxy-Systemen aus, die als vertrauenswürdige Vermittler für die Infrastruktur agieren. Solche Systeme müssen meist die folgenden Anforderungen erfüllen:

- **Automatische Passwortverwaltung** für privilegierten Zugriff: Privileged Access Control-Systeme können Passwörter und Anmeldeinformationen gemäß vorhandenen Richtlinien regelmäßig automatisch wechseln. Hierfür werden integrierte Konnektoren für Microsoft Active Directory, UNIX, LDAP, MYSQL usw. genutzt.
- **Benutzer-Authentifizierung** am Frontend und delegierter Zugriff auf AWS-Service am Backend: In der Regel eine Webseite, die eine Einmal-Anmeldung für alle Benutzer bietet. Den Benutzern werden je nach Autorisierungsprofil Zugriffsberechtigungen zugewiesen. Nach einem häufig verwendeten Ansatz erfolgt eine tokenbasierte Authentifizierung für die Webseite und der Erwerb eines „Clickthrough“-Zugangs zu anderen, gemäß Benutzerprofil zulässigen Systemen.
- Speicherung aller kritischen Aktivitäten in einem **manipulationssicheren Prüfpfad**.

- **Unterschiedliche Anmeldeinformationen für gemeinsam genutzte Konten**: Manchmal müssen mehrere Benutzer das gleiche Passwort benutzen. Mit einem Privilegien-Eskalations-Gateway wird ein Fernzugriff ohne Offenlegung des gemeinsam genutzten Kontos ermöglicht.
- Beschränkung von Leapfrogging oder Remote Desktop-Hopping durch die Zugriffsgewährung nur für Zielsysteme
- **Verwaltung von Befehlen**, die während den Sitzungen verwendet werden dürfen. Für interaktive Sitzungen wie SSH bzw. Anwendungsverwaltung oder AWS CLI lassen sich mit solchen Lösungen Richtlinien durch die Beschränkung der verfügbaren Auswahl an Befehlen und Aktivitäten durchsetzen.
- Bereitstellung eines **Prüfpfades für Terminals und GUI-basierte Sitzungen** zur Erfüllung von Compliance- und Sicherheitsanforderungen
- **Lückenlose Protokollierung** und Warnmeldungen gemäß vorgegebener Schwellenwerte für die Richtlinien.

Verwenden von Änderungsverwaltungsprotokollen

Durch die Verwaltung von Security Logs können Sie auch Änderungen nachverfolgen. Dies könnte zum Beispiel geplante Änderungen sein, welche Teil des Änderungskontrollprozesses des Unternehmens sind (manchmal als „MACD“ bezeichnet – Move/Add/Change/Delete), ferner spontane Änderungen oder unerwartete Änderungen, beispielsweise Incidents. Es können sowohl der infrastrukturelle Teil des Systems als auch andere Kategorien von Änderungen betroffen sein, darunter Änderungen an Code-Repositorien, Bestandsänderungen an „Gold-Images“/Anwendungen, Prozess- und Richtlinienänderungen oder auch Änderungen an der Dokumentation. Als bewährte Methode empfehlen wir für alle vorstehend genannten Änderungskategorien den Einsatz von manipulationssicheren Protokoll-Repositorien. Verbinden Sie Änderungsverwaltungs- und Protokollverwaltungssysteme miteinander.

Beauftragen Sie damit einen bestimmen Benutzer, der über Berechtigungen zum Löschen oder Ändern von Änderungsprotokollen verfügt. Für die meisten Systeme, Geräte und Anwendungen sollten die Änderungsprotokolle vor Manipulationen geschützt sein; normale Benutzer sollten nicht berechtigt sein, die Protokolle zu verwalten. Außerdem sollten sie keine Beweise aus Änderungsprotokollen löschen können. Manchmal nutzen AWS-Kunden Software für die Dateiintegritätsüberwachung und die Erkennung von Änderungen in Protokollen, um sicherzustellen, dass vorhandene Protokolldaten nicht ohne Erzeugung von Warnmeldungen geändert werden können, wohingegen durch das Hinzufügen neuer Einträge keine Warnmeldungen erzeugt werden.

Alle Protokolle für Systemkomponenten müssen mindestens einmal täglich überprüft werden. Dazu zählt die Überprüfung der Protokolle von Servern, die Sicherheitsfunktionen ausführen, darunter Angriffserkennungs-Server (intrusion-detection systems, IDS) und AAA-Protokoll-Server (Authentifizierung, Autorisierung und Kontoverwaltung, z. B. RADIUS). Hierfür können Sie Protokollauswertungs-, -analyse- und -warnungswerkzeuge nutzen.

Verwaltung von Protokollen für kritische Transaktionen

Bei kritischen Anwendungen muss für alle Aktivitäten bzw. Transaktionen vom Typ Hinzufügen, Ändern oder Löschen ein Protokolleintrag erstellt werden. Jeder Protokolleintrag sollte die folgenden Informationen enthalten:

- Angaben zur Benutzeridentifikation
- Art des Ereignisses
- Datum und Zeitstempel
- Erfolgs- oder Fehleranzeige
- Ursprung des Ereignisses
- Identität oder Name betroffener Daten, Systemkomponenten oder Ressourcen

Schutz von Protokolldaten

Die Protokollfunktion und -daten sind vor Manipulation und nicht autorisiertem Zugriff zu schützen. Administrator- und Betreiberprotokolle sind häufig das Ziel, um Spuren zu verwischen.

Gängige Kontrollen zum Schutz von Protokolldaten beinhalten Folgendes:

- Überprüfung, ob Prüfpfade vorhanden und für Systemkomponenten aktiviert sind
- Sicherstellung, dass Prüfpfaddateien nur Personen mit entsprechendem dienstlichen Auftrag zugänglich sind
- Bestätigung, dass die vorhandenen Prüfpfaddateien über Zugriffskontrollmechanismen, physische Abtrennung und/oder Netzwerkabtrennung vor nicht autorisierten Änderungen geschützt sind
- Sicherstellung, dass die vorhandenen Prüfpfaddateien sofort auf einem zentralen Protokollserver oder Medium gesichert werden, das schwierig zu verändern ist
- Überprüfung, ob Protokolle für nach außen gerichtete Technologien (zum Beispiel WLAN, Firewalls, DNS, E-Mail) auf einen sicheren zentralen internen Protokollserver oder ein entsprechendes Medium ausgelagert bzw. kopiert werden
- Einsatz von Dateiintegrität-Überwachungs- oder -Änderungsermittlungssoftware für Protokolle durch die Prüfung von Systemeinstellungen und überwachten Dateien sowie der Ergebnisse von Monitoring-Aktivitäten überwacht werden
- Beschaffung und Prüfung von Sicherheitsrichtlinien und -verfahren, um festzustellen, ob diese mindestens täglich durchgeführte Verfahren zur Überprüfung von Security Logs enthalten bzw. ob die Weiterverfolgung von Ausnahmen erforderlich ist
- Überprüfung, ob die regelmäßigen Protokollprüfungen für alle Systemkomponenten durchgeführt werden
- Sicherstellung, dass die Sicherheitsrichtlinien und -verfahren Aufbewahrungsbestimmungen für Prüfprotokolle beinhalten und die Aufbewahrung eines Prüfprotokolls für einen bestimmten, von den geschäftlichen und Compliance-Anforderungen abhängigen Zeitraum erfordern

Protokollierungsfehler

Zusätzlich zum Monitoring von MACD-Ereignissen sollten Software- oder Komponentenfehler überwacht werden. Fehler können das Ergebnis eines Hardware- oder Softwareversagens sein. Auch wenn sich dieses auf die Verfügbarkeit von Service und Daten auswirken mag, muss kein Zusammenhang mit einem Sicherheitsvorfall bestehen. Ein Service-Fehler kann aber auch das Ergebnis vorsätzlicher böswilliger Aktivitäten sein, z. B. einer Denial-of-Service-Attacke. In jedem Fall sollten bei Fehlern Warnmeldungen ausgelöst werden, woraufhin Sie Ereignisanalyse- und -zuordnungstechniken einsetzen sollten, um die Ursache des Fehlers zu ermitteln sowie um festzulegen, ob eine Sicherheitsreaktion auszulösen ist.

Zusammenfassung

Die AWS Cloud-Plattform hält zahlreiche wichtige Vorzüge für moderne Unternehmen bereit, darunter Flexibilität, Elastizität, bedarfsbezogene Abrechnung und kurze Produkteinführungszeit. Es bietet eine Reihe von Sicherheits-Services und -funktionen, welche Sie für das Management der Sicherheit Ihrer Komponenten und Daten im AWS nutzen können. Während mit AWS eine hervorragende Service Management-Ebene rund um Infrastruktur- oder Plattform-Services bereitsteht, sind die Unternehmen nach wie vor sowohl für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit ihrer Daten in der Cloud als auch für die Erfüllung konkreter geschäftlicher Anforderungen an den Datenschutz verantwortlich. In der Cloud behalten herkömmliche Sicherheits- und Compliance-Konzepte weiterhin ihre Gültigkeit. Mit dem Einsatz der in diesem Whitepaper beschriebenen Best Practices sind Sie eingeladen, ein Maßnahmen- und Vorgehenspaket für die Sicherheit in Ihrer Organisation zu erstellen, um Anwendungen und Daten schnell und sicher bereitstellen zu können.

Referenzen und weiterführende Literatur

- Amazon Web Services: Übersicht über die Sicherheitsprozesse – http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
- Amazon Web Services Whitepaper zu Risiko und Compliance – http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf
- Verwenden von Amazon Web Services für die Notfallwiederherstellung – http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
- Optionen für die Amazon VPC-Netzwerkkonnektivität – http://media.amazonwebservices.com/AWS_Amazon_VPC_Connectivity_Options.pdf
- Anwendung eines Identitätsverbunds am Beispiel von Active Directory – http://aws.amazon.com/code/1288653099190193
- Einfache Anmeldung mit Windows ADFS in Amazon EC2 .NET-Anwendungen – http://aws.amazon.com/articles/3698?_encoding=UTF8&queryArg=searchQuery&x=20&y=25&fromSearch=1&searchPath=all&searchQuery=identity%20federation
- Authentifizierung der Benutzer von AWS-Mobilanwendungen mit einem Token-Generator – http://aws.amazon.com/articles/4611615499399490?_encoding=UTF8&queryArg=searchQuery&fromSearch=1&searchQuery=Token%20Vending%20machine
- Kundenseitige Datenverschlüsselung mit AWS SDK für Java und Amazon S3 – http://aws.amazon.com/articles/2850096021478074
- Amazons Unternehmens-IT nutzt SharePoint 2010 für die Amazon Web Services-Cloud – http://media.amazonwebservices.com/AWS_Amazon_SharePoint_Deployment.pdf
- Amazon Web Services Acceptable Use Policy –http://aws.amazon.com/aup/
- Procure Secure: A guide to monitoring of security service levels in cloud contracts– http://www.enisa.europa.eu/activities/application-security/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts
- Der PCI-Datensicherheitsstandard – https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0
- ISO/IEC 27001:2005 – http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103
- Auditing Security Checklist for Use of AWShttp://media.amazonwebservices.com/AWS_Auditing_Security_Checklist.pdf