Checkliste zur Überprüfung der Sicherheit bei Nutzung von AWS

Juni 2013

(Die aktuelle Version dieses Dokuments finden Sie unter http://aws.amazon.com/compliance.)

Inhaltsverzeichnis

Inhaltsverzeichnis 2

Überblick 3

Einführung 3

Verwenden der Checklisten 4

Überwachen der Nutzung von AWS – Konzepte 5

Checkliste zur Überprüfung der Sicherheit 6

Verfahren vor der Prüfung 7

1. Governance 8

2. Konfiguration und Verwaltung von Komponenten 9

3. Logische Zugriffskontrolle 10

4. Datenverschlüsselung 12

5. Netzwerkkonfiguration und -verwaltung 13

6. Sicherheitsprotokollierung und -überwachung 14

7. Reaktion auf Sicherheitsvorfälle 16

8. Notfallwiederherstellung 16

AWS Trusted Advisor 18

Anhang A: Referenzen und weitere nützliche Informationen 19

Anhang B: Glossar der verwendeten Begriffe 20

Versionshistorie 21

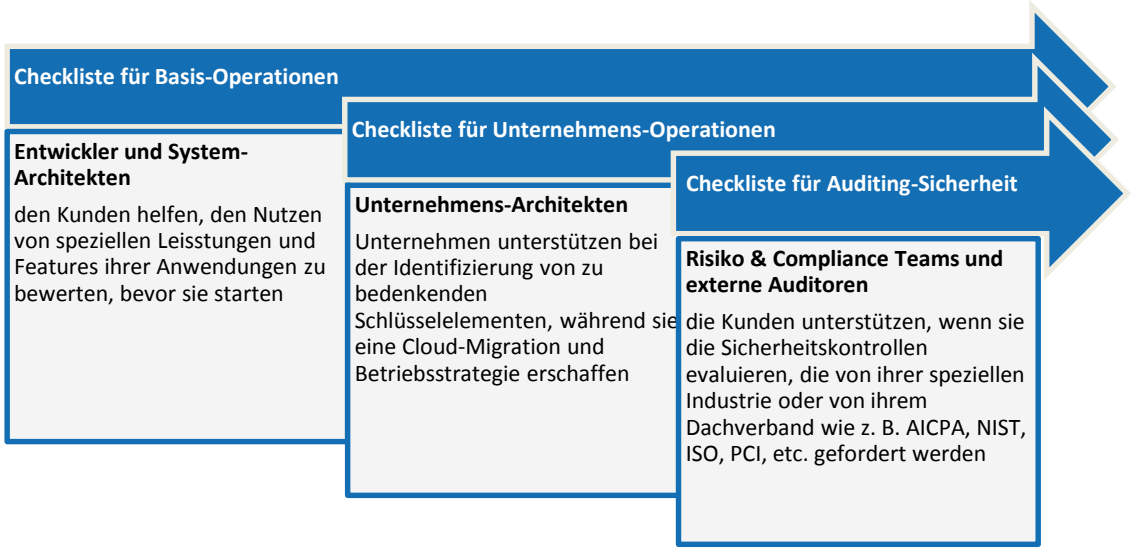
Überblick

Das Bereitstellen einer Anwendung in Amazon Web Services (AWS) erfolgt schnell, einfach und kostengünstig. Beim Bereitstellen einer Cloud-Anwendung in der Produktionist es hilfreich, über eine Checkliste zur Unterstützung der Analyse Ihrer Nutzung von AWS zum Zweck einer internen oder externen Prüfung zu verfügen. Dieses Whitepaper richtet sich an interne Compliance-Teams von AWS-Kunden und ihre externen Prüfer sowie an diejenigen Personen, die die Nutzung von AWS für eine interne Überprüfung oder externe Prüfung bewerten oder analysieren. Es bietet eine Checkliste zum Entwerfen und Ausführen einer Sicherheitsbewertung der AWS-Nutzung in einer Organisation, die möglicherweise durch Branchenregelungen oder Gesetze verlangt wird. Dieses Dokument setzt auf dem Whitepaper „Operational Checklists for AWS“ auf, das betriebs- und architekturbezogene Leitfäden zur Bewertung der Betriebsbereitschaft von Anwendungen bietet.

Einführung

Amazon Web Services ist eine flexible, kostengünstige und benutzerfreundliche Cloud Computing-Plattform. AWS stellt eine Suite von Infrastrukturdiensten bereit, die Sie zur Bereitstellung Ihrer Anwendungen nutzen können. Dieses Whitepaper richtet sich an interne Sicherheits-, Risiko- und Compliance-Teams von Kunden und ihre externen Prüfer, die die Nutzung von AWS ggf. bewerten müssen. Das Dokument ist aber auch für Unternehmen nützlich, um die geplante Nutzung von AWS mit diesen bewährten Methoden zur Überprüfung der Sicherheit zu vergleichen.

Darüber hinaus bietet AWS Betriebs-Checklisten (einschließlich der Betriebs-Checkliste „Standard“ und der Betriebs-Checkliste „Enterprise“) für Entwickler, Systemarchitekten und andere Interessenten, die Leitfäden für Betrieb und Architektur von AWS suchen, damit sie die Betriebsbereitschaft ihrer Anwendung besser bewerten können.



Verwenden der Checklisten

Checkliste zur Überprüfung der Sicherheit – Diese Checkliste soll AWS-Kunden und ihren Prüfern helfen, die Nutzung von AWS zu bewerten, was ggf. laut Branchenstandards oder Vorschriften erforderlich ist. Beispiele solcher Bewertungen sind die Notwendigkeit zum:

- Einschätzen der Fähigkeit von AWS-Services zum Erfüllen von Zielen bei der Informationssicherheit und Sicherstellen, dass künftige Bereitstellungen in der AWS-Cloud auf sichere und konforme Weise erfolgen
- Bewerten der aktuellen Nutzung von AWS im Unternehmen und Prüfen der Vorgehensweisen in Bezug auf Sicherheit
- Entwickeln von AWS-Nutzungsrichtlinien und/oder Prüfen, dass vorhandene Richtlinien befolgt werden

AWS erfüllt eine große Vielzahl von Sicherheitsstandards, die für diese Bewertungen von Relevanz sind. In diesem Dokument wird allerdings kein bestimmter Standard bzw. kein bestimmtes Rahmenwerk empfohlen. Stattdessen ist dieses Dokument allgemein gehalten, um Kunden oder Prüfern die Bewertung der Sicherheitskontrollen zu erleichtern, die vom jeweiligen Branchen- oder Dachverband gefordert werden, wie z. B. American Institute of Certified Public Accountants (AICPA), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI SSC), Information Systems Audit and Control Association (ISACA) usw.

Dieses Dokument bietet eine Checkliste für Bewertungen basierend auf den folgenden Bereichen:

- Governance
- Konfiguration und Verwaltung von Komponenten
- Logische Zugriffskontrolle
- Datenverschlüsselung
- Netzwerkkonfiguration und -verwaltung
- Sicherheitsprotokollierung und -überwachung
- Reaktion auf Sicherheitsvorfälle
- Notfallwiederherstellung

In diesem Dokument werden nur Sicherheitsbereiche und Themen behandelt, die sich für Prüfer von einer lokalen oder gehosteten Umgebung *unterscheiden*. Einige der Prüfaufgaben, die normalerweise für IT-Systeme oder -Organisationen erfolgen, z. B. Bestätigen, dass Administratoren über SSH remote auf bestimmte Ressourcen zugreifen, sind für Cloud- und lokale Umgebung identisch und werden deshalb in diesem Dokument nicht behandelt. Darüber hinaus gibt es mehrere Sicherheitskontrollen, die Kundensysteme von AWS übernehmen. Für diese Kontrollen bieten Kunden keine Dokumentation oder Tests, da sie zur AWS-Infrastruktur gehören. Zu diesen Kontrollen zählen die physischen und Umgebungsschutzmaßnahmen für die AWS-Rechenzentren, in denen sich die Server und anderen Einrichtungen befinden, sowie deren Wartung. Unternehmen, die Dokumentation und Tests dieser Kontrollen für ihre Compliance-Anstrengungen benötigen, können den entsprechenden AWS-Compliance-Bericht unter folgender Adresse anfordern: https://aws.amazon.com/compliance/contact/.

Checkliste	Beabsichtigte Verwendung	Zielgruppe
Betriebs-Checkliste „Basic“	Hilft Kunden bei der Bewertung der Nutzung bestimmter Services und Funktionen in ihrer Anwendung vor ihrer Inbetriebnahme	Entwickler und Systemarchitekten
Betriebs-Checkliste „Enterprise“	Hilft Unternehmen bei der Ermittlung wichtiger Punkte, die bei der Erstellung einer Strategie für Migration und Betrieb in der Cloud zu berücksichtigen sind	Unternehmensarchitekten
Checkliste zur Überprüfung der Sicherheit	Hilft Kunden bei der Evaluierung der Sicherheitskontrollen, die für die jeweilige Branche oder gemäß geltender Vorschriften (von Stellen wie AICPA, NIST, ISO, PCI SSC usw.) erforderlich sind	Prüfer oder Risiko- und Compliance-Experten

Überwachen der Nutzung von AWS – Konzepte

Die folgenden Konzepte sollten bei einer Sicherheitsprüfung der Systeme und Daten einer Organisation in AWS berücksichtigt werden:

I. **Verstehen des AWS-Modells der „geteilten Zuständigkeiten“** – Um sich in AWS befindende Komponenten effektiv bewerten zu können, müssen Kunden verstehen, welche Kategorien von Komponenten von ihnen und welche von AWS kontrolliert werden.

- AWS bietet eine sichere globale Infrastruktur und Services, für die AWS die Komponenten des Hostbetriebssystems und der Virtualisierungsebene betreibt, verwaltet und steuert und zudem für die Sicherheit der Standorte sorgt, an denen die Services ausgeführt werden. Diese Teile des Systems können vom Kunden mithilfe der AWS-Zertifizierungen und Berichte (z. B. Service Organization Control (SOC)-Berichte, DIN ISO 27001-Zertifizierung, PCI-Bewertungen usw.) geprüft werden. Die maßgeblichen AWS-Compliance-Zertifizierungen und -Berichte können unter https://aws.amazon.com/compliance/contact/ angefordert werden.
- Kunden sind zuständig für die Sicherheit aller Elemente, die ihre Organisation auf ihren AWS-Komponenten ablegt oder mit ihren AWS-Komponenten verbindet, z. B. das Gastbetriebssystem und die Anwendungen auf ihrer virtuellen Maschinen-Instance, die Daten und Objekte in ihren S3-Buckets oder der RDS-Datenbank usw.

Diese Aufteilung von Zuständigkeiten und Kontrolle ist erforderlich, um die Prüfanstrengungen einer Organisation effektiv zu gestalten. Siehe die nachstehende Abbildung 1.

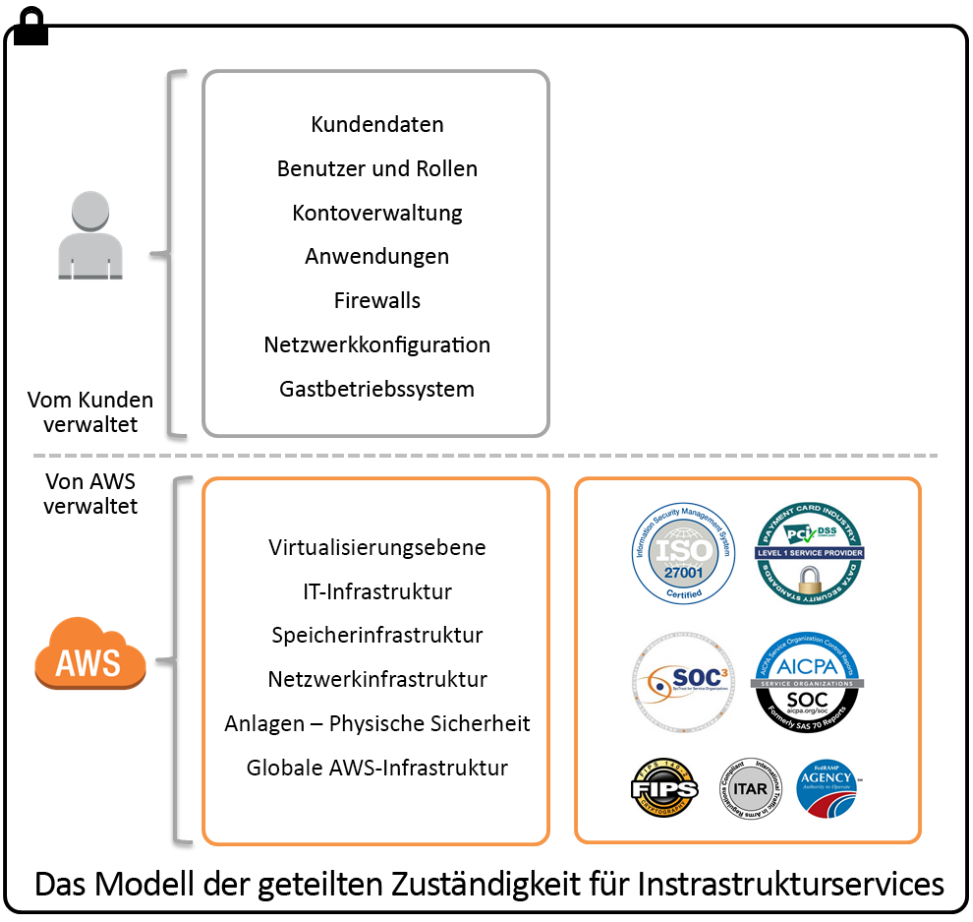


Abbildung 1: Das Modell der geteilten Zuständigkeiten

Weitere Informationen finden Sie im AWS-Sicherheitszentrum, unter AWS-Compliance und in den öffentlich verfügbaren AWS-Whitepaper unter http://aws.amazon.com/whitepapers/.

II. **Definieren der AWS-Komponenten einer Organisation** – Die AWS-Komponenten eines Kunden können Instances, Datenspeicher, Anwendungen, die Daten selbst usw. sein. Die Prüfung der Nutzung von AWS beginnt zumeist mit der Komponentenbestimmung. Komponenten in einer öffentlichen Cloud-Infrastruktur sind nicht kategorisch anders als in lokalen Umgebungen und ihr Bestand kann mitunter einfacher erfasst werden, da AWS bei Komponenten unter seiner Verwaltung für Transparenz sorgt.

III. **Ganzheitliche Sicherheitsverwaltung** – Die AWS-Infrastruktur muss ein integraler Bestandteil des Managementprogramms zur Informationssicherheit einer Organisation sein. Sicherheitskontrollziele müssen einheitlich unabhängig davon bleiben, wo sich die Systeme und Daten befinden. Kontrollen und Prüfpläne können jedoch gemäß den Leitlinien in diesem Dokument angepasst werden.

Die Liste der Aspekte ist allgemein und bietet nur begrenzte technische Details. Je nach Ihrer Kompetenz und Vertrautheit mit AWS müssen Sie ggf. Bezug auf andere AWS-Ressourcen nehmen, um die Sicherheitselemente vollständig bewerten zu können. Um beispielsweise zu verstehen, wie die Multifaktor-Authentifizierung (MFA) für API-Aufrufe (Application Programming Interface) in der Konsole erzwungen werden kann, lesen Sie auf der AWS-Website den Abschnitt zu IAM: http://aws.amazon.com/iam/. Eine technisch fundiertere Erläuterung aller dieser Sicherheitsmechanismen und servicespezifischen Aspekte finden Sie in den Ressourcen unter http://aws.amazon.com/whitepapers/.

Checkliste zur Überprüfung der Sicherheit

Über die internen Verweise auf nachfolgende Abschnitte im vorliegenden Dokument können Sie weitere Details zu den einzelnen Checklistenkategorien in der unten stehenden Tabelle anzeigen.

	Checklistenkategorie	Beschreibung
☐	Verfahren vor der Prüfung	Ist Ihre Organisation auf eine Prüfung vorbereitet?
☐	Governance	Versteht Ihre Organisation die verwendeten AWS-Services und -Ressourcen? Wird in Ihrem Risikomanagementprogramm die Nutzung von AWS berücksichtigt?
☐	Konfiguration und Verwaltung von Komponenten	Gibt es in Ihrer Organisation ein Management für Sicherheitsschwachstellen von Betriebssystemen und Anwendungen, um die Sicherheit, Stabilität und Integrität der Komponente sicherzustellen?
☐	Logische Zugriffskontrolle	Weiß Ihre Organisation, wie Benutzer und Berechtigungen in AWS eingerichtet werden? Werden in Ihrer Organisation die zu Ihren AWS-Konten gehörenden Anmeldeinformationen sicher verwaltet?
☐	Datenverschlüsselung	Weiß Ihre Organisation, wo sich die Daten Ihrer Organisation befinden und wie sie geschützt werden?
☐	Netzwerkkonfiguration und -verwaltung	Versteht Ihre Organisation die Netzwerkarchitektur von AWS-Ressourcen?
☐	Sicherheitsprotokollierung und -überwachung	Werden die sich in AWS befindenden Systeme Ihrer Organisation protokolliert und überwacht?
☐	Reaktion auf Sicherheitsvorfälle	Werden im Plan und in den Prozessen für das Vorfallmanagement in Ihrer Organisation Systeme in der AWS-Umgebung berücksichtigt?
☐	Notfallwiederherstellung	Werden in der Strategie für die Notfallwiederherstellung Ihrer Organisation Systeme in der AWS-Umgebung berücksichtigt?

Verfahren vor der Prüfung

Vor der Durchführung einer Prüfung ist es wichtig, den Prüfplan und -umfang zu bestätigen und bekannte Risiken zu bestimmen.

Verfahren vor der Prüfung – Checkliste

	Checklistenpunkt
☐	**Verstehen der Nutzung von AWS in Ihrer Organisation**. Mögliche Ansätze: • Befragen Ihrer IT- und Entwicklungsteams. • Durchführen von Netzwerküberprüfungen und eines umfassenderen Penetrationstests. • Prüfen von Kostenabrechnungen und/oder Zahlungen für Aufträge im Zusammenhang mit Amazon.com oder AWS, um zu verstehen, welche Services genutzt werden. Kredikartenbelastungen werden als „AMAZON WEB SERVICES AWS.AMAZON.CO WA“ o. ä. angezeigt. Hinweis: Einige Personen in Ihrer Organisation haben sich ggf. für ein AWS-Konto unter ihrem persönlichen Konto registriert, weshalb Sie diese Frage beim Befragen Ihre IT- und Entwicklungsteams stellen sollten.
☐	**Definieren Sie Ziele für Ihre Prüfung von AWS.** • Ihre Prüfziele sollten übergeordnet sein und allgemeine Prüfzielvorstellungen beschreiben. • Überprüfen Sie die AWS-Prüfziele in Ihrer Organisation und stimmen Sie sie auf Ihr Prüfprogramm und dessen Zeitplan ab. • Passen Sie Ihre Prüfziele an das Prüfprogramm, den Jahresplan und die Statuten der Organisation an.
☐	**Definieren Sie den Umfang der Prüfung von AWS.** Die Prüfung muss einen definierten Umfang haben. Machen Sie sich mit den wesentlichen Geschäftsprozessen Ihrer Organisation und ihrer Abstimmung mit der IT vertraut – sowohl was die lokale Umgebung als auch aktuelle oder künftige Cloud-Implementierungen angeht. • Verschaffen Sie sich eine Beschreibung der AWS-Services, die genutzt werden und/oder genutzt werden sollen. • Bestimmen Sie, nachdem Sie die Typen von AWS-Services ausgemacht haben, die genutzt werden oder genutzt werden sollen, die Services und Geschäftslösungen, die in die Prüfung einbezogen werden sollen. • Verschaffen Sie sich etwaige vorherige Prüfberichte mit Nachbesserungsplänen. • Bestimmen offene Punkte in vorherigen Prüfberichten und untersuchen Sie Aktualisierungen der Dokumente auf diese Punkte.
☐	**Identifizieren Sie Risiken.** Ermitteln Sie, ob für die maßgeblichen Komponenten eine Risikoanalyse erfolgt ist.
☐	**Überprüfen Sie Risiken.** Verschaffen Sie sich ein Exemplar etwaiger Risikoanalyseberichte und finden Sie heraus, ob diese die aktuelle Umgebung widerspiegeln und das Restrisiko in der Umgebung präzise beschreiben.
☐	**Überprüfen Sie Dokumentation zu Risiken.** Überprüfen Sie nach jedem Punkt in Ihrer Prüfung Pläne zur Risikobekämpfung samt Zeitleisten/Meilensteine im Abgleich mit Ihren Richtlinien und Verfahren für das Risikomanagement.
☐	**Beziehen Sie die Nutzung von AWS in die Risikoanalyse ein.**Führen Sie Elemente von AWS-Services in die Prozesse zur Risikobewertung Ihrer Organisation ein. Wichtige Aufgaben bei der Risikoanalyse**:** • Bestimmen Sie das geschäftliche Risiko der Nutzung von AWS sowie die geschäftlichen Verantwortlichen und wichtige Interessengruppen. • Prüfen Sie, ob die geschäftlichen Risiken im Rahmen Ihrer Nutzung von AWS-Services und der Sicherheitskriterien Ihrer Organisation für den Schutz von Vertraulichkeit, Integrität und Verfügbarkeit abgestimmt, eingestuft oder klassifiziert sind. • Gehen Sie vorherige Prüfungen von AWS-Services (auf SOC, PCI oder NIST 800-53 bezogene Prüfungen usw.) durch. • Stellen Sie fest, ob zuvor ausgemachte Risiken entsprechend bewältigt wurden. • Bewerten Sie den allgemeine Risikofaktor der Durchführung Ihrer AWS-Prüfung. • Bestimmen Sie basierend auf der Risikobewertung Änderungen an Ihrem Prüfungsumfang. • Besprechen Sie die Risiken mit der IT-Leitung und passen Sie die Risikobewertung an.

1. Governance

Definition: Zu Governance zählen die Elemente, die erforderlich sind, um der Geschäftsführung die Bestätigung zu geben, dass ihre Marchrichtung und Absicht im Sicherheitsstand der Organisation Ausdruck finden. Dies wird mithilfe eines strukturierten Ansatzes zur Implementierung eines Informationssicherheitsprogramms erreicht. Für diesen Prüfplan bedeutet dies zu wissen, welche AWS-Services Ihre Organisation erworben hat, welche Arten von Systemen und Informationen Sie mit den AWS-Services nutzen möchten und welche Richtlinien, Verfahren und Pläne für diese Services gelten.

Wesentlicher Prüfschwerpunkt: Verstehen, welche AWS-Services und -Ressourcen von Ihrer Organisation verwendet werden, und gewährleisten, dass Ihre Nutzung der öffentlichen Cloud-Umgebung im Sicherheits- oder Risikomanagementprogramm der Organisation berücksichtigt wird.

Prüfansatz: Bestimmen Sie als Teil dieser Prüfung, wer in Ihrer Organisation ein AWS-Konto- und -Ressourcen besitzt und welche Arten von AWS-Services- und Ressourcen genutzt werden. Vergewissern Sie sich, dass in den Richtlinien, Plänen und Verfahren Ihrer Organisation Cloud-Konzepte berücksichtigt werden und dass Cloud-Technologie zum Umfang des Prüfprogramms Ihrer Organisation zählt.

Governance – Checkliste

	Checklistenpunkt
☐	**Identifizieren Sie Komponenten.** Jedem AWS-Konto ist eine Kontakt-E-Mail-Adresse zugeordnet, über die Kontobesitzer bestimmt werden können. Wichtig ist der Hinweis, dass diese E-Mail-Adresse von einem öffentlichen E-Mail-Dienstanbieter stammen kann, was von der Adresse abhängt, die der Benutzer bei der Registrierung verwendet hat. • Eine formelle Besprechung mit allen AWS-Konto- und Komponentenbesitzern kann anberaumt werden, um zu ermitteln, was in AWS bereitgestellt ist, wie es verwaltet wird und wie es in die Sicherheitsrichtlinien, -verfahren und -standards Ihrer Organisation integriert ist. Hinweis: Der AWS-Kontobesitzer kann jemand in der Finanz- oder Einkaufsabteilung sein, doch die Person, die mit der Nutzung der AWS-Ressourcen in der Organisation vertraut ist, kann aus der IT-Abteilung stammen. Sie müssen ggf. beide befragen.
☐	**Bewerten Sie Richtlinien.**Bewerten und prüfen Sie die Sicherheits-, Datenschutz- und Datenklassifizierungsrichtlinien Ihrer Organisation, um zu ermitteln, welche Richtlinien für die AWS-Serviceumgebung gelten. • Stellen Sie fest, ob es eine formelle Richtlinie und/oder einen Prozess für die Buchung von AWS-Services gibt, um zu bestimmen, wie diese autorisiert wird. • Prüfen Sie, ob in den Änderungsmanagementprozessen und -richtlinien Ihrer Organisation AWS-Services berücksichtigt werden.
☐	**Bewerten Sie Risiken.** Bewerten Sie die Bedeutung der in AWS bereitgestellten Daten für das allgemeine Risikoprofil und die Risikotoleranz der Organisation. Stellen Sie sicher, dass diese AWS-Komponenten in das formelle Risikobewertungsprogramm der Organisation integriert sind. • AWS-Komponenten müssen identifiziert werden und ihnen müssen je nach ihrem Risikoprofil Schutzvorgaben zugeordnet sein.
☐	**Bearbeiten Sie den Prüfplan.** Ändern Sie den Prüfplan so, dass, falls noch nicht erfolgt, die AWS-Systeme in den Umfang einbezogen werden. Fügen Sie AWS-Komponenten bei Bedarf maßgeblichen jährlichen Sicherheitsbewertungsverfahren oder jährlichen externen Prüfinitiativen hinzu. • Vergewissern Sie sich, dass IT-Management- und -Sicherheitsrichtlinien so angepasst werden, dass die Bereitstellung von IT-Ressourcen in der AWS-Umgebung berücksichtigt wird (dies kann am Ende der Prüfung erfolgen).

2. Konfiguration und Verwaltung von Komponenten

Definition: AWS-Kunden sind zuständig für das Gewährleisten der Sicherheit aller Elemente, die sie in ihren AWS-Ressourcen installieren oder mit ihren AWS-Ressourcen verbinden. Für ein sicheres Management Ihrer AWS-Ressourcen ist es unerlässlich zu wissen, welche Ressourcen Ihre Organisation nutzt (Komponentenbestand), das Gastsystem und Anwendungen auf Ihren Ressourcen sicher zu konfigurieren (sichere Konfigurationseinstellung, Einspielen von Patches und Schutz gegen Schadsoftware) und Änderungen an Ihren Ressourcen zu kontrollieren (Änderungsmanagement).

Wesentlicher Prüfschwerpunkt: Kunden benötigen ein Management für Sicherheitsschwachstellen ihrer Betriebssysteme und Anwendungen, um die Sicherheit, Stabilität und Integrität der Komponente sicherzustellen.

Prüfansatz: Vergewissern Sie sich, dass Ihr Gastbetriebssystem und Ihre Anwendungen gemäß den Richtlinien, Verfahren und Standards Ihrer Organisation konfiguriert, mit Patches versehen und „gehärtet“ sind. Sämtliche Betriebssystem- und Anwendungsmanagementverfahren können für lokale und AWS-Systeme und -Services gleich sein.

Konfiguration und Verwaltung von Komponenten – Checkliste

	Checklistenpunkt
☐	**Erfassen Sie den Komponentenbestand.** Prüfen Sie, ob AWS-Konto- und -Ressourcenbesitzer die in ihrer Organisation verwendeten AWS-Ressource verstehen, indem Sie eine Komponentenbestandsliste erstellen und abstimmen. • Prüfen Sie anhand der Bestandsliste die auf den Komponenten installierten Services.
☐	**Bewerten Sie das Patching.** Vergewissern Sie sich, dass alle betriebenen Instances als Teil der Komponentenbestimmung im Rahmen der Prüfung unter „Governance“ hinzugefügt und klassifiziert wurden. Die Dokumentation der Gesamtanzahl aller AWS-Konten ist besonders wichtig für die effektive Bestimmung aller in der AWS-Umgebung betriebenen Komponenten. • Vergewissern Sie sich, dass die aktuellen Prozesse für das Patch-Management von Software- und Systemkomponenten (Bestimmung, Tests und Bereitstellung) die Komponenten in der AWS-Umgebung einschließen. Der Prozess muss u. a. die Bestimmung von Schwachstellen, die Überprüfung der System-Patch-Ebene und die Implementierung von Patches vorsehen.
☐	**Bewerten Sie die Konfigurationsverwaltung.** Überprüfen Sie die Konfigurationsverwaltungsverfahren Ihrer Organisation für alle AWS-Systemkomponenten und ob diese Standards geeignet sind, bekannte Sicherheitsschwachstellen in den Griff zu bekommen. • AWS bietet die Möglichkeit, neue Instances basierend auf einem allgemeinen (öffentlichen) oder organisationsspezifischen Amazon Machine Image (AMI, Computerabbild) zu starten. Prüfen Sie die verwendeten Computerabbilder und bestimmen Sie, ob ein AMI für die Nutzung genehmigt wurde, das von Ihren internen Compliance- und/oder Sicherheitsteams geprüft wurde. Das Einrichten eines genehmigten Computerabbilds hilft sicherzustellen, dass neue Abbilder mit Ihren Richtlinien und Prozessen konform sind. • Befolgen Sie bei jeder Instance die vorgegebenen Sicherheits-, Prüf- und Validierungsverfahren. Zu diesen Verfahren kann beispielsweise u. a. gehören, dass Standardeinstellungen von Herstellern vor der Bereitstellung geändert, Kennwörter modifiziert und nicht benötigte Konten gelöscht werden. • Bestimmen Sie, falls von Ihrer Organisationsrichtlinie vorgegeben, ob pro Server nur eine Hauptfunktion zugewiesen wurde. • Stellen Sie fest, ob der Remote-Verwaltungszugriff sicher erfolgt (z. B. über SSH). Dies geht einher mit einer sicheren Verschlüsselung, sofern zutreffend. • Ermitteln Sie, ob alle nicht benötigten Funktionen und Konten entfernt wurden. • Stellen Sie sicher, dass keine unnötigen Skripts, Treiber, Funktionen, Subsysteme, EBS-Volumes oder Webserver ausgeführt werden.
☐	**Bewerten Sie Zugriffsberechtigungen.** Der Zugriff auf Betriebssysteme und Anwendungen muss eingeschränkt sein. Prüfen Sie den Zugriff auf Betriebssysteme und Anwendungen, um die Angemessenheit des Zugriffs festzustellen und ob dieser in Übereinstimmung mit Organisationsrichtlinien und -verfahren verwaltet wird. • Prüfen Sie, ob die Protokollierung des Zugriffs auf die in Ihrer Organisation definierten Zugriffsstandards und die jeweilige Zugriffsberechtigungsstufe abgestimmt ist. Generell kann die Protokollierung von Gastbetriebssystemen und Anwendungen wie bei lokalen Systemen erfolgen.

3. Logische Zugriffskontrolle

Definition: Logische Zugriffskontrollen bestimmen nicht nur, wer oder was Zugriff auf eine bestimmte Systemressource hat, sondern auch die Art der Aktion, die auf die Ressource angewendet werden darf (Lesen, Schreiben usw.). Im Rahmen der Kontrolle des Zugriffs auf AWS-Ressourcen müssen Benutzer und Prozesse Anmeldeinformationen vorlegen, um nachzuweisen, dass sie für die Ausführung bestimmter Funktionen autorisiert sind oder Zugriff auf bestimmte Ressourcen haben. Die von AWS geforderten Anmeldeinformationen variieren abhängig vom Typ des Service und der Zugriffsmethode und umfassen Kennwörter, kryptografische Schlüssel und Zertifikate. Zugriff auf AWS-Ressourcen kann über das AWS-Konto, einzelne AWS Identify and Access Management (IAM)-Benutzerkonten, die unter dem AWS-Konto erstellt wurden, oder einen Identitätsverbund mit Ihrem Unternehmensverzeichnis (Einmalige Anmeldung) ermöglicht werden. Mit AWS Identity and Access Management (IAM) können Benutzer einer Organisation den Zugriff auf AWS-Services und -Ressourcen sicher kontrollieren. Mithilfe von IAM kann eine Organisation AWS-Benutzer und -Gruppen anlegen und verwalten und mittels Berechtigungen ihren Zugriff auf AWS-Ressourcen zulassen oder verweigern.

Wesentlicher Prüfschwerpunkt: In diesem Teil der Prüfung liegt der Schwerpunkt auf dem Bestimmen, wie Benutzer und Berechtigungen in AWS für die Services eingerichtet werden, die in Ihrer Organisation genutzt werden. Wichtig ist es auch sicherzustellen, dass die Anmeldeinformationen, die allen Ihren AWS-Konten zugewiesen sind, von Ihrer Organisation sicher verwaltet werden.

Prüfansatz: Vergewissern Sie sich, dass Berechtigungen für AWS-Komponenten in Übereinstimmung mit Richtlinien, Verfahren und Prozessen Ihrer Organisation verwaltet werden. Hinweis: Mithilfe von AWS Trusted Advisor können Konfigurationen von IAM-Benutzern, -Gruppen und -Rollen überprüft werden. Im Abschnitt zu AWS Trusted Advisor in diesem Whitepaper finden Sie weitere Informationen.

Interne Zugriffskontrolle – Checkliste

	Checklistenpunkt
☐	**Bewerten Sie die AWS-Kontoverwaltung.** Dokumentieren Sie den Besitz und die Verwaltung des AWS-Kontos (das als Root-Konto bezeichnet wird) für alle Informationssysteme oder Abteilungen, die Sie prüfen. • Prüfen Sie, ob die Zuweisung von Zuständigkeiten wie gewünscht ist. • Prüfen Sie, ob es zweckmäßig ist, für Personen mit Voll- bzw. umfassendem Zugriff auf AWS-Services zwei AWS-Benutzerkonten einzurichten. • Erwägen Sie die Nutzung des einen AWS-Kontos für Administratoraufgaben und des anderen für Benutzerzugriffsaktivitäten. Dies trägt dazu bei, dass sensible Konten weniger Bedrohungen ausgesetzt sind, nicht versehentlich gelöscht werden oder ihre Informationen weniger gefährdet sind.
☐	**Bewerten Sie die Multifaktor-Authentifizierung (MFA).** Bestimmen Sie, ob die Multifaktor-Authentifizierung von AWS-Konten von Ihren Richtlinien verlangt wird. Weitere Informationen… • Falls verlangt, prüfen Sie in der AWS Management Console, ob die MFA für das AWS-Konto und einzelne IAM-Benutzerkonten erzwungen wird. Weitere Informationen…
☐	**Überprüfen Sie Identify and Access Management (IAM)-Benutzerkonten.** Melden Sie sich in Zusammenarbeit mit den AWS-Kontobesitzern bei der AWS Management Console an, um festzustellen, welche IAM-Benutzerkonten vorhanden sind. • Dokumentieren Sie die Berechtigungen und überprüfen Sie sie auf Angemessenheit. Bewerten Sie die Nutzung temporärer Anmeldeinformationen im Abgleich mit den Richtlinien Ihrer Organisation. Dies kann durch Nachfrage oder eine Überprüfung der IAM-Benutzerkonten erfolgen, die unter dem AWS-Konto aktiv sind. Weitere Informationen…
☐	**Überprüfen Sie Gruppenberechtigungen.** Melden Sie sich bei der AWS Management Console an, um die Nutzung von AWS-Gruppen in AWS IAM zu prüfen. Dies sind Zusammenstellungen von AWS-Benutzern unter demselben AWS-Konto, die zum Vereinfachen von Benutzerverwaltungsaufgaben dienen. • Prüfen Sie den Zugriff auf AWS-Ressourcen jeder AWS-Gruppe und führen Sie einen Vergleich mit der

	Checklistenpunkt
	Zuweisung von AWS IAM-Richtlinien durch. • Alle Berechtigungen und Richtlinien, die einer AWS-Gruppe zugewiesen sind, gelten kumulativ für die AWS IAM-Benutzerkonten, die Mitglied der Gruppe sind. Weitere Informationen…
☐	**Überprüfen Sie die Systembenutzerkonten der Organisation.** Bestimmen Sie, ob das Authentifizierungssystem Ihrer Organisation mit AWS integriert ist, um Zugriff auf AWS-Ressourcen zu gewähren. Dies kann geprüft werden, indem einem Prüfer ein Benutzerkonto mit AWS-Berechtigungen zugewiesen wird, um die Anmelde- und Datenzugriffsberechtigungen zu testen. Richten Sie Ihre Tests so ein, dass alle als dazugehörig geltende AWS-Komponenten eingeschlossen werden. • Bestimmen Sie AWS-Systeme, die nicht den Berechtigungen des Authentifizierungssystems der Organisation unterliegen. Prüfen Sie, ob diese, soweit erforderlich, in das reguläre Berechtigungsverwaltungssystem integriert werden können.
☐	**Bewerten Sie Anmeldeinformationen für Anwendungs- und Systemprozesse.** Bestimmen Sie, welche Anwendungs- oder Systemprozesse über APIs und AWS Software Development Kits (SDKs) auf AWS-Services zugreifen. Falls Anwendungs- oder Systemprozesse Zugriff auf AWS-Ressourcen benötigen, vergewissern Sie sich, dass der Zugriff sicher und gemäß Richtlinien bereitgestellt wird, und dokumentieren Sie Ihr Verständnis. Es gibt drei Typen von Anmeldeinformationen: • Das Signieren symmetrischer Verschlüsselungsschlüssel (für den Zugriff über REST/Query-APIs und Tools anderer Anbieter) • X.509-Zertifikate und dazugehörige private Schlüssel (für den Zugriff über SOAP-APIs und Befehlszeilen) • Multifaktor-Authentifizierung (optional)
☐	**Bewerten Sie IAM-Rollen.** IAM-Rollen ermöglichen AWS-Kontoadministratoren, den Zugriff an Benutzer oder Services zu delegieren, die normalweise keinen Zugriff auf die AWS-Ressourcen Ihrer Organisation haben. IAM-Benutzer oder AWS-Services können eine Rolle annehmen, um temporäre Anmeldeinformationen zu erhalten, mit deren Hilfe Aufrufe von AWS-APIs erfolgen können. Falls IAM-Rollen unter dem AWS-Konto Ihrer Organisation verwendet werden, überprüfen Sie die Rollen, um sicherzustellen, dass eine neue AWS-Rolle für jeden neuen Zugriffstyp erstellt wird und spezifische Berechtigungen für Betriebssystemdienste und Anwendungen erteilt werden, die Zugriff auf AWS-Ressourcen benötigen. Weitere Informationen… • Prüfen Sie die einzelnen IAM-Rollen und bestimmen Sie, wie AWS-Ressourcen mithilfe von Identity and Access Management-Richtlinien im Rahmen der rollenbasierten Zugriffskontrolle ein Zugriff bereitgestellt wird. • Untersuchen Sie die Eignung der Organisationsrichtlinie im Zusammenhang mit diesem Zugriffstyp und dokumentieren Sie etwaige Abweichungen. • Prüfen Sie, ob die MFA für den API-Zugriff genutzt wird. Hinweis: Da die AWS Management Console AWS-Service-APIs aufruft, können Sie die MFA für APIs ungeachtet des Zugriffspfads erzwingen.
☐	**Führen Sie Zugriffskontrolltests durch.** Führen Sie Tests basierend auf den verwendeten Zugriffstypen den Anforderungen entsprechend durch. Getestet werden können**:** • Der Zeitplan für den Wechsel von Zugriffsschlüsseln (mit hoher Frequenz) • Die Integration von X.509-Zertifikaten und PKI oder die Verwendung von AWS-Zertifikaten • Die Sicherheit der Zertifikat- und Schlüsselverwaltung (zur Gewährleistung, dass private Schlüssel sicher gespeichert und nicht in AWS hochgeladen werden) • Implementierungen alternative Authentifizierungsmethoden wie die Lightweight Directory Access Protocol (LDAP)- oder Active Directory (AD)-Authentifizierung sowie die Deaktivierung der AWS EC2-Schlüsselpaarauthentifizierung können auch in Erwägung gezogen werden.
☐	**Dokumentieren Sie die Berechtigungsverwaltung von AWS-Ressourcen.** Vergewissern Sie sich, dass das Informationssicherheit-Managementsystem der Organisation die Verwaltung und Kontrolle von Berechtigungen für AWS-Ressourcen einschließt. AWS-Benutzerkonten, die außerhalb des Informationssicherheit-Managementsystems der Organisation verwaltet werden, müssen ermittelt werden. Weitere Informationen…

4. Datenverschlüsselung

Definition: In AWS gespeicherte Daten sind standardmäßig sicher. Nur AWS-Kontobesitzer haben Zugriff auf die AWS-Ressourcen, die sie erstellen. Doch es gibt Kunden mit sensiblen Daten, die einen zusätzlichen Schutz durch Verschlüsselung der Daten wünschen, wenn diese in AWS gespeichert werden. Nur der Service Amazon S3 bietet derzeit eine automatisierte Verschlüsselungsfunktion auf Serverseite zusätzlich dazu, dem Kunden zu erlauben, eine Verschlüsselung auf Client-Seite vorzunehmen, ehe die Daten gespeichert werden. Bei anderen AWS-Datenspeicheroptionen muss der Kunde die Verschlüsselung der Daten vornehmen.

Wesentlicher Prüfschwerpunkt: In AWS gespeicherte Daten sollten zum Schutz genau so verschlüsselt werden wie lokale Daten. Darüber hinaus wird das Internet in vielen Sicherheitsrichtlinien als unsicheres Kommunikationsmedium eingestuft, was die Verschlüsselung von Daten während der Übertragung erforderlich macht. Ein unsachgemäßer Schutz der Daten einer Organisation kann zu Sicherheitsrisiken führen.

Prüfansatz: Ermitteln Sie, wo sich die Daten befinden, und prüfen Sie die Methoden zum Schutz von Daten bei der Speicherung und während der Übertragung. Hinweis: Mithilfe von AWS Trusted Advisor können Berechtigungen und der Zugriff auf Datenkomponenten geprüft werden. Im Abschnitt zu AWS Trusted Advisor in diesem Whitepaper finden Sie weitere Informationen.

Datenverschlüsselung – Checkliste

	Checklistenpunkt
☐	**Bestimmen Sie Datenkomponenten und -anforderungen.** Vergewissern Sie sich, dass alle Unternehmensdaten als Teil der Komponentenbestimmung im Rahmen der Prüfung unter „Governance“ hinzugefügt und klassifiziert wurden. Die Dokumentation der Gesamtanzahl aller AWS-Konten ist besonders wichtig für die effektive Bestimmung aller Datenkomponenten in der AWS-Umgebung. • Bestimmen Sie die Datenspeicheranforderungen aller maßgeblichen Datenelemente.
☐	**Überprüfen Sie die Verschlüsselung gespeicherter Daten.** Bewerten Sie die kryptografischen Algorithmen und Mechanismen, die von Ihrer Organisation zur Verschlüsselung von in AWS gespeicherten Daten verwendet werden. • Für Amazon S3 zählt dazu das Bestimmen, ob die Verschlüsselung auf Client- oder Serverseite erfolgt. Weitere Informationen… • Für alle anderen AWS-Datenspeicherservices müssen die verwendeten Verschlüsselungsmethoden auf Client-Seite bestimmt werden.
☐	**Überprüfen Sie die Verschlüsselung von Daten während der Übertragung.** • Wenn die Verschlüsselung von Daten während der Übertragung erforderlich ist, bestimmen Sie, ob Verbindungen mit allen in Frage kommenden AWS-Services per HTTPS über sichere Endpunkte hergestellt werden. Ermitteln Sie außerdem die Nutzung von Windows X.509-Zertifikaten, SSH, SSL/TLS-Wrapper für geschützte Datenbankprotokolle und/oder VPN-Lösungen. • Machen Sie sich mit der Dokumentation des Schutzes von Daten während der Übertragung bei der Verwaltung von AWS-Services vertraut. Hinweis: Kunden verwalten ihre AWS-Services wie Amazon EC2 und Amazon S3 entweder über die AWS Management Console oder AWS-APIs. Da die Sicherheit dieser Kommunikationsmethoden gut dokumentiert ist, erleichtert diese Dokumentationsaktivität die Aufgabe der Risikoanalyse und die erforderliche sorgfältige Prüfung zum Verstehen der aktiven Schutzmaßnahmen für Daten während der Übertragung (z. B. wenn S3-Datenobjekte über die AWS-Konsole hochgeladen werden).

5. Netzwerkkonfiguration und -verwaltung

Definition: Die Netzwerkverwaltung in AWS entspricht praktisch der lokalen Netzwerkverwaltung mit der Ausnahme, dass Netzwerkkomponenten wie Firewalls und Router virtuell sind. Kunden müssen dafür sorgen, dass ihre Netzwerkarchitektur die Sicherheitsanforderungen ihrer Organisation erfüllt. Dazu zählt die Nutzung von DMZs (Demilitarized Zones, dt. Umkreisnetzwerk oder überwachtes Subnetz) zum Trennen von öffentlichen und privaten (d. h. nicht vertrauenswürdigen und vertrauenswürdigen) Ressourcen, die Trennung von Ressourcen mithilfe von Subnetzen und Routingtabellen, die sichere Konfiguration von DNS, ob zusätzlicher Übertragungsschutz in Form eines VPN benötigt wird und ob der ein- und ausgehende Datenverkehr begrenzt werden soll. Kunden, die ihr Netzwerk überwachen müssen, können dies mithilfe hostbasierter Systeme für die Erkennung von Eindringversuchen und Überwachung tun.

Wesentlicher Prüfschwerpunkt: Fehlende oder falsch konfigurierte Sicherheitskontrollen im Zusammenhang mit externer Zugriffs-/Netzwerksicherheit, die zu einem Sicherheitsrisiko werden können.

Prüfansatz: Machen Sie sich mit der Netzwerkarchitektur Ihrer AWS-Ressourcen und damit vertraut, wie die Ressourcen konfiguriert sind, um einen externen Zugriff aus dem öffentlichen Internet und den privaten Netzwerken Ihrer Organisation zuzulassen. Hinweis: Mithilfe von AWS Trusted Advisor können AWS-Konfigurationseinstellungen überprüft werden. Im Abschnitt zu AWS Trusted Advisor in diesem Whitepaper finden Sie weitere Informationen.

Netzwerkkonfiguration und -verwaltung – Checkliste

	Checklistenpunkt
☐	**Überprüfen Sie den Datenverkehr zu EC2-Instances.** AWS EC2-Sicherheitsgruppen fungieren als hostbasierte Firewall für Instances. Vergewissern Sie sich, dass EC2-Sicherheitsgruppen von Ihrer Organisation ordnungsgemäß konfiguriert wurden, sodass eingehender Datenverkehr zu Instances nach Port, Protokoll oder IP-Quelladresse (einzelne IP-Adresse oder Classless Inter-Domain Routing (CIDR)-Block) eingeschränkt werden kann.
☐	**Überprüfen Sie den Datenverkehr zu VPC-Netzwerken.**Ermitteln Sie die Netzwerksegmentierung in Ihrer AWS-Umgebung. • Sicherheitszonen. Bestimmen Sie, ob Ihre AWS-Ressourcen innerhalb der AWS VPC mithilfe privater und öffentlicher Subnetze (DMZs) in vertrauenswürdige und nicht vertrauenswürdige Sicherheitszonen unterteilt werden müssen. Dazu muss ggf. die Kontrolle und Überwachung der folgenden Aspekte geprüft werden: - Kommunikation zwischen Zonen - Einsatz zonenbezogener Zugriffskontrollrechte - Verwaltung von Zonen mithilfe fest zugeordneter Verwaltungsschienen/-rollen - Anwendung zonenbezogener Vertraulichkeits- und Integritätsregeln • Netzwerksegmentierung. Wenn mithilfe einer AWS VPC private Subnetze erstellt werden, bestimmen Sie diese und ihre Verwendung. Prüfen Sie beispielsweise, ob sie Organisationseinheiten oder spezifische Verarbeitungslasten isolieren. • Ermitteln Sie, ob Kontrolllisten für den Netzwerkzugriff (NACLs) erforderlich sind, um den Zugriff auf Services zwischen Subnetzen einzuschränken. Überprüfen Sie die NACLs für die VPC und vergleichen Sie sie mit der NACL-Richtlinie Ihrer Organisation. • Überprüfen Sie die Nutzung von Schutzebenen im Datenverkehrsfluss, um zu erzwingen, dass der gesamte Datenverkehr Sicherheitszonen durchquert. • Prüfen Sie, ob alle Netzwerkkontrollen einheitlich implementiert sind. Einer der Vorteile der elastischen Cloud-Infrastruktur und automatisierten Bereitstellung ist die Möglichkeit, dieselben Sicherheitseinstellungen in allen AWS-Regionen anzuwenden. Durch wiederholbare und einheitliche Bereitstellungen kann sich der gesamte Sicherheitsstand verbessern.

☐	**Prüfen Sie zusätzliche Netzwerkkontrollen.** Organisationen können auf Wunsch auch unter Befolgung eines linearen Ansatzes eine Sicherheitskontroll-Appliance auf Netzwerkebene bereitstellen, von der Datenverkehr abgefangen und analysiert wird, ehe seine Weiterleitung an das endgültige Ziel erfolgt. • Vergewissern Sie sich, dass externe Überprüfungen auf Schwachstellen regelmäßig bzw. gemäß Ihrer Richtlinie oder nach einer größeren Systemänderung stattfinden. • Vergewissern Sie sich, dass Ihre Organisation Penetrationstests regelmäßig durchführt. • Verschaffen Sie sich ein Exemplar der letzten Analyse auf Schwachstellen und überprüfen Sie Abhilfemaßnahmen, die Nachverfolgung von Problemen und den Zeitrahmen zum Beseitigen von Schwachstellen. • Prüfen Sie, ob die Prozesse für die Beseitigung von Schwachstellen und Penetrationstests den Richtlinien und Verfahren Ihrer Organisation entsprechen. • Vergewissern Sie sich, dass für die in AWS durchgeführten Penetrationstests die Richtlinien zur angemessenen Nutzung von AWS (AWS Acceptable Use Policy) und die ordnungsgemäßen Zeitplanungsverfahren befolgen. Unter https://aws.amazon.com/security/penetration-testing/ finden Sie weitere Informationen zum AWS-Penetrationstestprozess.

6. Sicherheitsprotokollierung und -überwachung

Definition: In Prüfprotokollen wird eine Vielzahl von Ereignissen aufgezeichnet, die in den Informationssystemen und Netzwerk einer Organisation eintreten. Prüfprotokolle dienen zum Bestimmen von Aktivitäten, die sich ggf. auf die Sicherheit dieser Systeme auswirken (ob in Echtzeit oder im Anschluss an das Ereignis), weshalb eine ordnungsgemäß Konfiguration und der Schutz der Protokolle wichtig ist.

Wesentlicher Prüfschwerpunkt: AWS-Systeme müssen ebenso wie lokale Systeme protokolliert und überwacht werden. Wenn AWS-Systeme nicht in den allgemeinen Sicherheitsplan des Unternehmens einbezogen sind, können bei der Überwachung kritische Systeme unberücksichtigt bleiben.

Prüfansatz: Vergewissern Sie sich, dass die Prüfprotokollierung für das Gastbetriebssystem und die wichtigen Anwendungen erfolgt, die auf Ihren EC2-Instances installiert sind, und dass die Implementierung den Richtlinien und Verfahren Ihrer Organisation entspricht, insbesondere in Bezug auf die Speicherung, den Schutz und die Analyse der Protokolle.

Sicherheitsprotokolle und -überwachung – Checkliste:

	Checklistenpunkt
☐	**Überprüfen Sie die Protokollieranforderungen.** Machen Sie sich damit vertraut, was gemäß den Richtlinien, Verfahren und Compliance-Anforderungen Ihrer Organisation in Ihrer Umgebung protokolliert werden muss. • Berücksichtigen Sie die Protokollierung aller Benutzeraktivitäten, Ausnahmen und Sicherheitsereignisse, was möglicherweise Folgendes einschließen kann: - Aktionen durch Personen mit Root- oder Administratorberechtigungen - Zugriff auf alle Audit-Trails - Ungültige logische Zugriffsversuche - Verwendung von Identifikations- und Authentifizierungsmethoden - Initialisierungen von Prüfprotokollprozessen - Erstellen und Löschen von Objekten auf Systemebene • Überprüfen Sie den Bestand Ihrer AWS-Komponenten, um zu bestimmen, welche Richtlinien und Verfahren für die AWS-Komponenten aus Sicht der Protokollierung gelten. Konzentrieren Sie Ihren Prüfaufwand darauf, den Grad der Protokollierung innerhalb von AWS-Systemen zu verstehen. Bei kritischen Anwendungen können Transaktionen vom Typ „Ändern“, „Hinzufügen“ und „Löschen“ einen Protokolleintrag erforderlich machen. Die folgenden Informationen können in einem Protokolleintrag aufgezeichnet werden: - Benutzeridentifizierung - Typen von Ereignissen - Datum- und Uhrzeitstempel - Angaben von Erfolg oder Misserfolg - Ursprung von Ereignissen - Identität oder Name der betroffenen Daten, Systemkomponenten oder Ressourcen

	Checklistenpunkt
	• Vergewissern Sie sich basierend auf Ihren Organisationsrichtlinien, dass Sie die Protokollierung für alle Ihre AWS-Systemkomponenten und -Umgebungen aktiviert haben. • Prüfen Sie, ob das Ausmaß der Protokollierung den Anforderungen Ihrer Organisation entspricht.
☐	**Überprüfen Sie die Protokollierung des Benutzerzugriffs.** Überprüfen Sie für alle betroffenen Systeme und Benutzer, ob die Zugriffsprotokollierung aktiv ist und dass Ihre Protokolle alle relevanten Benutzeraktivitäten, Ausnahmen und Sicherheitsereignisse enthalten. Beachten Sie, dass viele AWS-Services integrierte Zugriffskontroll- und Audit-Trail-Funktionen bieten. • Prüfen Sie, ob Protokolle für einen Zeitraum aufbewahrt werden, der den Richtlinien Ihrer Organisation entspricht, um künftige Untersuchungen unterstützen zu können.
☐	**Überprüfen Sie die Protokollierung des Änderungsmanagements.** Machen Sie sich mit dem Umfang Ihrer Änderungsprotokollierung vertraut und prüfen Sie, ob sie basierend auf den Richtlinien und Verfahren Ihres Unternehmens angemessen ist. Änderungsmanagementprotokolle sollten nicht nur auf Änderungs-, Hinzufüge- und Löschanforderungen an die Infrastruktur beschränkt werden. Sie sollten auch Änderungen am Codespeicher, am Master-Image/Anwendungsbestand, an Prozessen/Richtlinien und Dokumentationen enthalten. • Überprüfen Sie aktuellen Verfahren zum Schutz Ihres AWS-Protokollspeichers. Prüfen, ob dieser Schutz die internen Richtlinienvorgaben Ihrer Organisation erfüllt. • Prüfen Sie die verschiedenen Rollenzuweisungen zum Modifizieren und Löschen von Änderungen. • Prüfen Sie, ob Warnungen aktiviert sind, um zu erkennen, wenn Benutzer versuchen, Protokolldaten zu ändern. Software zur Überwachung der Dateiintegrität und Erkennung von Änderungen an Protokollen kann hierbei hilfreich sein. • Machen Sie sich mit den vorhandenen Verfahren zur Überprüfung von Protokollen für alle Systemkomponenten vertraut und stellen Sie fest, ob die Überprüfungen regelmäßig erfolgen. In Protokollüberprüfungen müssen die Server einbezogen werden, die Sicherheitsaufgaben erfüllen, wie beispielsweise Systeme zur Erkennung von Eindringversuchen (IDS) und Server für Authentifizierung, Autorisierung und Abrechnung (z. B. RADIUS).
☐	**Überprüfen Sie den Protokollschutz.** Protokollierungsfunktionen und Protokollinformationen müssen gegen Manipulationen und unbefugten Zugriff geschützt werden. Administrator- und Bedienerprotokolle sind ein sensibles Ziel für unbefugte Löschvorgänge. Führen Sie zum Schutz der Protokollinformationen des AWS-Systems die folgenden Schritte aus: • Prüfen Sie, ob Audit-Trails für Systemkomponenten aktiv sind. • Überprüfen Sie, ob nur Einzelpersonen Zugriff auf Audit-Trail-Dateien haben, die aus geschäftlichen Gründen darauf zugreifen müssen. • Prüfen Sie, ob aktuelle Audit-Trail-Dateien mithilfe von Zugriffskontrollmethoden, physischer Trennung und/oder Netzwerktrennung gegen unbefugte Änderungen geschützt sind. • Überprüfen Sie, ob Dateien des aktuellen Audit-Trails auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen, gesichert werden. • Vergewissern Sie sich, dass Protokolle für mit dem öffentlichen Internet verbundene Technologien (z. B. WLANs, Firewalls, DNS und E-Mail) ausgelagert oder auf einen sicheren zentralen internen Protokollserver oder entsprechende Medien kopiert werden. • Überprüfen Sie die Verwendung der Software zur Dateiintegritätsüberwachung und Änderungserfassung für Protokolle, indem Sie die Systemeinstellungen und die überwachten Dateien sowie die Ergebnisse der Überwachung untersuchen. • Untersuchen Sie Sicherheitsrichtlinien und -verfahren daraufhin, ob sie Verfahren zur mindestens täglichen Prüfung von Sicherheitsprotokollen enthalten und dass Ausnahmen zwingend überprüft werden müssen. • Stellen Sie sicher, dass Protokollüberprüfungen für alle Systemkomponenten regelmäßig erfolgen. • Untersuchen Sie Sicherheitsrichtlinien und -verfahren und vergewissern Sie sich, dass diese Richtlinien für die Aufbewahrung von Prüfprotokollen aufweisen und die Aufbewahrung von Prüfprotokollen für die erforderliche Dauer vorsehen.
☐	**Überprüfen Sie Überwachungsmethoden und/oder -verfahren.** Prüfen Sie, ob die Methoden und/oder Verfahren im System für das Management von Informationen zu Sicherheit und Ereignissen Ihrer Organisation Ihre AWS-Umgebungen berücksichtigen. • Prüfen Sie außerdem, ob aus Ihren AWS-Umgebungen stammende Benachrichtigungen zeitgerecht bestimmt und bearbeitet werden und ob die Reaktion den Richtlinien und Verfahren der Organisation entspricht.

7. Reaktion auf Sicherheitsvorfälle

Definition: Im Rahmen eines Modells der geteilten Zuständigkeiten können sicherheitsbezogene Ereignisse sowohl von AWS als auch von AWS-Kunden überwacht werden. AWS erkennt und reagiert auf Ergebnisse, die sich auf den Hypervisor und die zugrunde liegende Infrastruktur auswirken. Kunden kümmern sich um Ereignisse im Gastbetriebssystem und in den Anwendungen. Die Organisation muss mit ihren Zuständigkeiten für die Reaktion auf Vorfälle vertraut sein und vorhandene Tools und Prozesse für die Sicherheitsüberwachung, Warnun und Prüfung auf ihre AWS-Ressourcen anwenden.

Wesentlicher Prüfschwerpunkt: Sicherheitsbezogene Ereignisse müssen unabhängig davon, wo sich die Komponenten befinden, überwacht werden. Der Prüfer kann die Einheitlichkeit der Bereitstellung von Kontrollen für das Vorfallmanagement in allen Umgebungen bewerten und mithilfe von Tests auf eine vollständige Abdeckung prüfen.

Prüfansatz: Bewerten Sie das Vorhandensein und die betriebliche Effektivität der Kontrollen für das Vorfallmanagement für Systeme in der AWS-Umgebung.

Reaktion auf Sicherheitsvorfälle – Checkliste:

	Checklistenpunkt
☐	**Bewerten Sie den aktuellen Vorfallmanagementprozess.** Bewerten Sie den aktuellen Status des Prozesses zum Umgang mit auf die Informationssicherheit bezogenen Ereignissen in Ihrer Organisation. • Prüfen Sie, ob die Nutzung von AWS-Services in den Vorfallmanagementprozess einbezogen wurde.
☐	**Überprüfen Sie den Vorfallmanagementplan.** Überprüfen Sie den Vorfallmanagementplan zusammen mit den maßgeblichen internen Rollen und Zuständigkeiten für Ihre Organisation.
☐	**Bewerten Sie das Kommunizieren des Vorfallmanagementplans.** Prüfen Sie die Verteilung von Vorfallmanagementplänen in Ihrer Organisation.

8. Notfallwiederherstellung

Definition: AWS bietet eine hoch verfügbar Infrastruktur, in der Kunden ausfallsichere Anwendungen entwickeln und schnell auf kritische Vorfälle und Notfallszenarien reagieren können. Kunden müssen jedoch sicherstellen, dass sie Systeme, die Hochverfügbarkeit und schnelle Wiederherstellungszeiten benötigen, so konfigurieren, dass die von AWS gebotenen mehreren Regionen und Availability Zones genutzt werden.

Wesentlicher Prüfschwerpunkt: Eine nicht erkannte einzelne Fehlerstelle und/oder nicht ausreichende Planung von Notfallwiederherstellungsszenarien kann sich sehr negativ auf Ihre Organisation auswirken. Wenngleich Service Level Agreements (SLAs) auf Ebene der einzelnen Instances/Services von AWS geboten werden, dürfen diese nicht mit den Zielen des Kunden für Geschäftskontinuität und Notfallwiederherstellung, z. B. Wiederherstellungsdauer (Recovery Time Objective, RTO) und Wiederherstellungszeitpunkt (Recovery Point Objective RPO), verwechselt werden. Die Parameter Geschäftskontinuität/Notfallwiederherstellung werden der Lösungskonzeption zugeordnet. Um Ausfallsicherheit besser zu gewährleisten, zeichnen sich Konzeptionen häufig durch die Nutzung mehrerer Komponenten in verschiedenen Availability Zones von AWS und Datenreplikation aus.

Prüfansatz: Machen Sie sich mit der Strategie für die Notfallwiederherstellung für Ihre Umgebung vertraut und bestimmen Sie die fehlertoleranten Architekturkomponenten, die für die kritischen Komponenten Ihrer Organisation genutzt werden. Hinweis: Mithilfe von AWS Trusted Advisor können verschiedene Aspekte Ihrer Funktionen für Ausfallsicherheit überprüft werden. Im Abschnitt zu AWS Trusted Advisor in diesem Whitepaper finden Sie weitere Informationen.

Notfallwiederherstellung – Checkliste:

	Checklistenpunkt
☐	**Machen Sie sich mit dem Istzustand vertraut.** Überprüfen Sie die Pläne zur Notfallwiederherstellung Ihrer Organisation, die für Ihre AWS-Ressourcen spezifisch sind. • Bestimmen Sie die aktuellen AWS-Regionen und dazugehörigen Availability Zones (AZs), die von den Komponenten Ihrer Organisation genutzt werden. • Ermitteln Sie, ob eine Multi-AZ-Bereitstellungsstrategie für die Komponenten Ihrer Organisation befolgt wird. Eine AZ ist ein eigenständiger Standort, der so entwickelt wurde, dass er von Ausfällen in anderen AZs isoliert ist. AWS empfiehlt Kunden, Instances in mehreren AZs zu starten, um bei einem Ausfall einer gesamten AZ einen Serviceausfall zu vermeiden. • Bestimmen Sie alle Regionen, in denen sich Ihre Komponenten derzeit befinden. Ermitteln Sie, ob Richtlinien für Ihre Organisation vorgeben, dass bestimmte Regionen aufgrund rechtlicher oder gesetzlicher Vorgaben nicht genutzt werden dürfen. • Bestimmen Sie nach einer Prüfung der Dokumentation der AWS-Architektur Ihrer Organisation, der Pläne für die Notfallwiederherstellung und Besprechungen mit dem dafür zuständigen Personal den angestrebten Ansatz zur Wiederherstellung nach Auftreten eines Notfalls.
☐	**Überprüfen Sie den Vorfallmanagementplan.** Überprüfen Sie den Vorfallmanagementplan zusammen mit den maßgeblichen internen Rollen und Zuständigkeiten für Ihre Organisation.
☐	**Bewerten Sie das Kommunizieren des Vorfallmanagementplans.** Prüfen Sie die Verteilung von Vorfallmanagementplänen in Ihrer Organisation.
☐	**Prüfen Sie die Nutzung von AWS-Funktionen.** Ermitteln Sie, ob der Plan für die Notfallwiederherstellung Ihrer Organisation eine oder mehrere der folgenden Lösungen vorsieht: • Nutzen von AWS für Speicherung/Sicherung und Wiederherstellung – Die AWS-Services EBS und S3 können für Speicherungs-/Sicherungszwecke genutzt werden. Bei einem Notfall können Ihre Daten aus der entsprechenden Quelle wiederhergestellt werden. • Lösung nach dem Prinzip der Zündflamme – Die wichtigen Systeme Ihrer Organisation sind für die Ausführung in AWS konfiguriert und zum Zeitpunkt eines Notfalls können Sie den Rest Ihrer Umgebung wie gewünscht skalieren. • Einsatzbereite Standby-Lösung – Alle Ihre kritischen Systeme und relevanten unterstützenden Systeme werden in der kleinstmöglichen Konfiguration in AWS ausgeführt. • Lösung für mehrere Standorte – Ihre kritischen Systeme sind für die Ausführung als Aktiv/Aktiv-Konfiguration sowohl in AWS als auch in Ihrer eigenen Infrastruktur bereitgestellt. • Automatisierte Bereitstellung – Alle Ihre kritischen Infrastruktur- und unterstützenden Systeme werden in einer AWS-Lösung mit mehreren AZs ausgeführt. • Berücksichtigen Sie je nach Anwendungsfall für Notfallwiederherstellungszwecke Folgendes: - Überprüfen Sie für Datensicherungsprozesse die mithilfe von AWS-Services gesicherten Daten und vergewissern Sie sich, dass Richtlinien für die Datenaufbewahrung Ihrer Organisation bei der Nutzung der einzelnen Services befolgt werden. - Überprüfen Sie den Test der letzten Wiederherstellung, bei dem geprüft wurde, ob Ihre Daten erfolgreich wiederhergestellt wurden. • Weitere Prüfbereiche: - Überprüfen Sie Ihre Bibliothek der Amazon Machine Images (AMIs) auf Vollständigkeit. Vergewissern Sie sich, dass das AMI mit allen relevanten Software-Updates, Konfigurationsänderungen und Patches vollständig und aktuell ist. - Finden Sie heraus, ob die automatisierte Bereitstellung von AWS-Ressourcen genutzt wird. Falls nicht, bestimmen Sie den aktuellen Prozess für die regelmäßige Aktualisierung und Pflege dieser AMIs und vergewissern Sie sich, dass dieser in Einklang mit den Richtlinien Ihrer Organisation für die Patch- und Konfigurationsverwaltung ist. - Machen Sie sich mit der Replikation Ihrer Instances, Datenspeicher und Datenbanken vertraut. - Prüfen Sie die in Ihrer Organisation erforderlichen Änderungen an DNS (Domain Name System) zum Zeitpunkt eines Notfalls und ob dieser Prozess im Plan für die Notfallwiederherstellung dokumentiert ist. - Gehen Sie die Analyse einzelner Fehlerstellen mit Ihren Teams aus der IT und den Geschäftsbereichen durch. - Stellen Sie sicher, dass diese Teams als Teil des Plans für die Notfallwiederherstellung einen spezifischen

	Checklistenpunkt
	Prozess zum Ermitteln der kritischen Komponenten der Organisation in AWS entwickelt haben.
☐	**Überprüfen Sie Tests von Notfallwiederherstellungen.** Machen Sie sich mit den Intervallen und Arten von Tests der Notfallwiederherstellung in Ihrer gesamten AWS-Infrastruktur vertraut. • Stellen Sie fest, ob detaillierte Überprüfungen von Komponentenausfallanalysen erfolgt sind, und überprüfen Sie die Ergebnisse, um zu bestimmen, ob der Single- oder Multi-AZ-Bereitstellungsansatz in Ihrer Organisation befolgt wird.

AWS Trusted Advisor

Es gibt zahlreiche Tools anderer Anbieter, die Ihnen bei Ihrer Analyse helfen können. Da AWS-Kunden die volle Kontrolle über ihre Betriebssysteme, Netzwerkeinstellungen und die Weiterleitung von Datenverkehr haben, können viele intern genutzte Tools zum Analysieren und Prüfen der Komponenten in AWS genutzt werden.

Ein nützliche von AWS bereitgestelltes Tool ist AWS Trusted Advisor. AWS Trusted Advisor basiert auf den Erfahrungen und Vorgehensweisen, gemäß denen AWS seinen Hunderttausenden von Kunden zuverlässig seine Services anbietet. AWS Trusted Advisor unterzieht Ihre AWS-Umgebung mehreren grundlegenden Prüfungen und gibt Empfehlungen, sobald sich Möglichkeiten ergeben, Kosten zu senken, die Systemleistung zu verbessern oder Sicherheitslücken zu schließen. Trusted Advisor überprüft derzeit das Befolgen der folgenden Sicherheitsempfehlungen:

- Begrenzen des externen Zugriffs auf gängige Ports für die Verwaltung auf eine kleine Gruppe von Adressen
- Überprüfen des externen Zugriffs auf gängige Datenbank-Ports
- Prüfen, ob IAM konfiguriert ist, um einen begrenzten internen Zugriff auf AWS-Ressourcen sicherzustellen
- Prüfen, ob die MFA aktiviert ist, um für das AWS-Root-Konto eine Zwei-Faktor-Authentifizierung zu ermöglichen

Dieses Tool kann für einige Punkte der Checkliste für die Prüfung genutzt werden, um die Prüf- und Analyseprozesse Ihrer Organisation zu unterstützen und zu optimieren.

Anhang A: Referenzen und weitere nützliche Informationen

1. Amazon Web Services: Übersicht über Sicherheitsverfahren – http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
2. Amazon Web Services: Amazon Web Services – Risiko und Compliance – http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf
3. Verwendung von Amazon Web Services zur Notfallwiederherstellung – http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
4. Identity federation sample application for an Active Directory use case – http://aws.amazon.com/code/1288653099190193
5. Single Sign-on with Windows ADFS to Amazon EC2 .NET Applications – http://aws.amazon.com/articles/3698?_encoding=UTF8&queryArg=searchQuery&x=20&y=25&fromSearch=1&searchPath=all&searchQuery=identity%20federation
6. Authenticating Users of AWS Mobile Applications with a Token Vending Machine – http://aws.amazon.com/articles/4611615499399490?_encoding=UTF8&queryArg=searchQuery&fromSearch=1&searchQuery=Token%20Vending%20machine
7. Client-Side Data Encryption with the AWS SDK for Java and Amazon S3 – http://aws.amazon.com/articles/2850096021478074
8. Amazon's Corporate IT Deploys SharePoint 2010 to the Amazon Web Services Cloud – http://media.amazonwebservices.com/AWS_Amazon_SharePoint_Deployment.pdf
9. Amazon Web Services Acceptable Use Policy – http://aws.amazon.com/aup/

Anhang B: Glossar der verwendeten Begriffe

Authentifizierung: Authentifizierung ist der Vorgang zur Bestimmung, ob jemand oder etwas auch wirklich der oder das ist, was er oder es zu sein vorgibt.

Availability Zone: Amazon EC2-Standorte bestehen aus Regionen und Availability Zones. Availability Zones sind eigenständige Standorte, die so entwickelt wurden, dass sie von Fehlern in anderen Availability Zones isoliert sind. Sie bieten eine kostengünstige Netzwerkverbindung mit geringer Verzögerungszeit zu anderen Availability Zones in derselben Region.

Amazon Elastic Block Store (EBS) bietet Volumes für die Speicherung auf Blockebene zur Verwendung mit Amazon EC2-Instances. Amazon EBS-Volumes ermöglichen die Speicherung außerhalb der Instance, die unabhängig vom Status einer Instance besteht.

FISMA: Der Federal Information Security Management Act von 2002. In Übereinstimmung mit FISMA ist das National Institute of Standards and Technology (NIST) zuständig für die Entwicklung von Normen, Richtlinien und dazugehörigen Methoden und Verfahren, um für alle behördlichen Vorgänge und Komponenten (mit Ausnahmen von Systemen für die nationale Sicherheit) eine angemessene Informationssicherheit zu ermöglichen.

Hypervisor: Ein Hypervisor, auch Virtual Machine Monitor (VMM) genannt, ist eine Virtualisierungssoftware für Software-/Hardware-Plattformen, dank der mehrere Betriebssysteme gleichzeitig auf einem Host-Computer ausgeführt werden können.

IAM: Identity and Access Management (AWS IAM) ermöglicht einem Kunden, mehrere Benutzerkonten zu erstellen und deren Berechtigungen innerhalb seines AWS-Kontos zu verwalten.

ISAE 3402: International Standards for Assurance Engagements No. 3402 (ISAE 3402) ist der internationale Standard für Prüfberichte. Dieser wurde auf Grundlage von Empfehlungen des IAASB (International Auditing and Assurance Standards Board), einer für die Ausarbeitung von Standards zuständigen Abteilung des IFAC (International Federation of Accountants), entwickelt. ISAE 3402 ist mittlerweile der weltweit anerkannte Standard für Prüfberichte für Dienstleistungsunternehmen.

DIN ISO/IEC 27001: DIN ISO/IEC 27001 ist eine Norm für Informationssicherheits-Managementsysteme, die von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) veröffentlicht wurde. DIN ISO/IEC 27001 spezifiziert formell Anforderungen an ein Managementsystem mit dem Ziel, die Informationssicherheit unter die explizite Kontrolle des Managements zu bringen. Da es sich um eine formelle Spezifikation handelt, müssen bestimmte Anforderungen erfüllt sein. Organisationen, die vorgeben, DIN ISO/IEC 27001 zu befolgen, können geprüft und als mit der Norm konform zertifiziert werden.

Objekt: Die Grundeinheiten, die in Amazon S3 gespeichert sind. Objekte bestehen aus Objekt- und Metadaten. Die Datenteile sind für Amazon S3 unverständlich. Metadaten bestehen aus mehreren Name/Wert-Paaren, die das Objekt beschreiben. Dazu gehören Standardmetadaten wie das Datum der letzten Aktualisierung und Standard-HTTP-Metadaten wie „Content-Type“. Der Entwickler kann zudem die Kundenmetadaten zum Zeitpunkt der Speicherung des Objekts festlegen.

PCI (Payment Card Industry): Bezieht sich auf das Payment Card Industry Security Standards Council, ein unabhängig Gremium, das von American Express, Discover Financial Services, JCB, MasterCard Worldwide und Visa International mit dem Ziel ins Leben gerufen wurde, den Datensicherheitsstandard für die Kreditkartenbranche (PCI DSS) zu betreuen und weiterzuentwickeln.

Service: Software oder Datenverarbeitungsfunktionalität, die über ein Netzwerk (z. B. EC2, S3, VPC) zur Verfügung gestellt wird.

Service Level Agreement (SLA): Ein Service Level Agreement ist Teil eines Servicevertrags, in dem der Grad des Service formal definiert wird. Die SLA dient zur Bezugnahme auf die vertraglich vereinbarte Lieferzeit (des Service) oder Leistung.

SOC 1: Der Service Organization Controls 1 (SOC 1) Type II-Bericht, zuvor Statement on Auditing Standards (SAS) No. 70, Service Organizations-Bericht oder SSAE 16-Bericht genannt) ist eine umfassend anerkannte Bilanzprüfungsvorschrift des American Institute of Certified Public Accountants (AICPA). Der internationale Standard wird als International Standards for Assurance Engagements No. 3402 (ISAE 3402) bezeichnet.

SSAE 16: Das Statement on Standards for Attestation Engagements No. 16 (SSAE 16) ist ein von den Auditing Standards Board (ASB) des American Institute of Certified Public Accountants (AICPA) veröffentlichter Bescheinigungsstandard. Der Standard gilt für die Beauftragung von Serviceprüfern mit der Erstellung eines Berichts zu Kontrollen in Organisationen, die Unternehmen Services bereitstellen, bei denen die Kontrollen eines Serviceanbieters voraussichtlich für die interne Kontrolle der Finanzberichterstattung eines Unternehmens relevant sind. SSAE 16 ersetzt das Statement on Auditing Standards No. 70 (SAS 70) für Berichtszeiträume von Serviceprüfern, die am bzw. nach dem 15.06.2011 enden.

Virtuelle Instance: Sobald ein AMI erstellt wurde, wird das sich daraus ergebende ausgeführte System als Instance bezeichnet. Alle Instances, die auf demselben AMI basieren, sind anfangs identisch. Sämtliche Informationen, die auf ihnen gespeichert sind, gehen verloren, wenn die Instance beendet wird oder ausfällt.

Versionshistorie

Juni 2013 – Erste Version