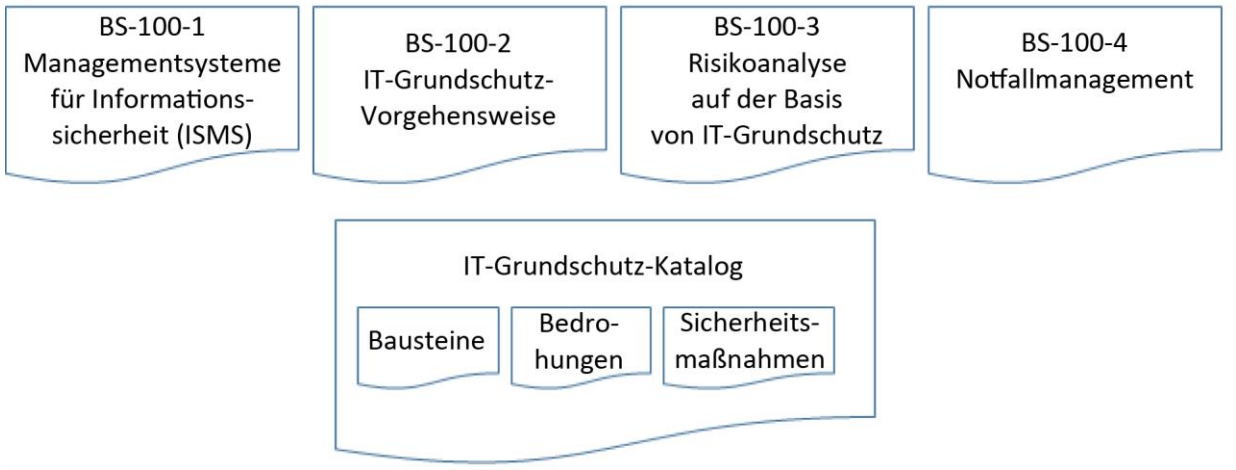
Zusammenfassung

Bei Amazon Web Services (AWS) handelt es sich um eine hoch sichere Cloud-Plattform, die regelmäßigen Audits unterzogen wird und mit deren Hilfe Kunden die unterschiedlichsten Anforderungen hinsichtlich behördlicher Vorschriften und Best Practices zur Gewährleistung der Datensicherheit erfüllen können. Dazu gehören unter anderem die IT-Grundschutz-Standards des deutschen Bundesamts für Sicherheit in der Informationstechnik. Mit der sicheren Infrastruktur von AWS können Kunden ein Informationssicherheits-Managementsystem (ISMS) erstellen, das mit den IT-Grundschutz-Empfehlungen für bewährte Methoden zur Datensicherheit im Einklang steht, und gleichzeitig die AWS-Services nutzen.

IT-Grundschutz – Übersicht

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Programm entwickelt, das Unternehmen die notwendige Methodik an die Hand gibt, um effektive Informationssicherheitsprozesse zu schaffen. Die IT-Grundschutz-Methodik stützt sich auf vier Standards, die technische Hinweise zum Aufbau eines Informationssicherheits-Managementsystems, die empfohlene Vorgehensweise zur Implementierung und Bewertung des IT-Grundschutzes, Informationen zur Durchführung einer Risikoanalyse anhand der IT-Grundschutzanforderungen und schließlich Informationen zur Entwicklung eines Plans zum Notfallmanagement umfassen. Bei dem fünften Dokument handelt es sich um den IT-Grundschutz-Katalog. Dieses Dokument enthält technische Empfehlungen zum Schutz vor den wichtigsten Gefährdungen der Datensicherheit.[1]



Die Standards "BSI 100-1 Managementsysteme für Informationssicherheit (ISMS)" und "BSI 100-2 IT-Grundschutz-Vorgehensweise" wurden auf Basis der Standards ISO 27001 und ISO 27002 erstellt. [2] In diesen Dokumenten finden Benutzer über den Katalog hinaus praktische Beispiele und Hinweise zur Implementierung.
Der IT-Grundschutz-Katalog hingegen enthält Erläuterungen der bekannten Gefährdungen und empfohlene Schutzmaßnahmen und Implementierungen, die dagegen zu ergreifen sind.

---

[1] Weitere Informationen sowie die aktuellen BSI-Standards und den IT-Grundschutz-Katalog finden Sie auf der BSI-Website "IT-Grundschutz-Standards": https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

[2] Siehe BSI-Standard 100-1 Managementsysteme für Informationssicherheit (ISMS), Seite 10, vorletzter Absatz. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001_pdf.pdf?__blob=publicationFile

Geteilte Verantwortung für die Sicherheit in einer Cloud-Umgebung und Ausrichtung am IT-Grundschutz-Ebenenmodell

Wie bei jedem Drittanbieter führt die Verwendung von AWS zu einem Modell geteilter Verantwortung hinsichtlich des Einsatzes und der Verwaltung von Sicherheitsmaßnahmen. Dieses Modell kann Ihnen einen Teil der Arbeit abnehmen, denn Sie und AWS teilen sich Ausführung, Verwaltung und Steuerung der Komponenten der Informationssicherheitsmaßnahmen. Bei Sicherheitsmaßnahmen kann es sich um geteilte, vererbte oder duale Maßnahmen handeln.

Bei der Erfüllung der Informationssicherheitsanforderungen im Cloud Computing muss zwischen der Compliance der Cloud-Lösung selbst und Ihrer eigenen Nutzung der Cloud-Lösung unterschieden werden. "Sicherheit ***DER*** Cloud" bezieht sich auf die Compliance-Pläne und -Maßnahmen, die der Cloud Service Provider (AWS) innerhalb der AWS-Infrastruktur implementiert. "Sicherheit ***IN*** Cloud" bezieht sich auf die Implementierung von Sicherheitsmaßnahmen im Zusammenhang mit den Abläufen, die in dieser AWS-Infrastruktur ausgeführt werden.

Sicherheit *DER* Cloud

Sicherheit ***DER*** Cloud bezieht sich darauf, wie AWS die Sicherheit der zugrunde liegenden Cloud-Infrastruktur handhabt. Alle Komponenten, von Host-Betriebssystem und Virtualisierungsebene bis hin zur physischen Sicherheit der Anlagen, in denen die AWS-Services ausgeführt werden, werden von AWS betrieben, verwaltet und gesteuert.

Wie kann ein Unternehmen die in der AWS-Kontrollumgebung eingesetzten Sicherheitsmaßnahmen nachprüfen?

Von externen AWS-Prüfern werden AWS-Zertifizierungen und -Berichte erstellt, die die konzeptionelle und operative Wirksamkeit der AWS-Umgebung bezeugen. Dazu gehören:

SOC 1/ ISAE 3402: AWS veröffentlicht den Bericht "Service Organization Controls 1 (SOC 1), Type II". Diese Prüfung ersetzt den Prüfbericht "Statement on Auditing Standards Nr. 70 (SAS 70) Type II". Im SOC 1-Prüfbericht wird bestätigt, dass die AWS-Kontrollziele ihren Zweck erfüllen und die Maßnahmen zum Schutz von Kundendaten wirksam sind.

SOC 2 – Sicherheit: Zusätzlich zum SOC 1-Bericht veröffentlicht AWS den Bericht "Service Organization Controls 2 (SOC 2), Type II". Wie bei SOC 1 werden auch beim SOC 2-Bericht die Maßnahmen bewertet, allerdings erstreckt sich dieser Bericht darüber hinaus auf die in den American Institute of Certified Public Accountants (AICPA) Trust Services Principles dargelegten Kriterien. Bei AWS SOC 2 wird die konzeptionelle und operative Wirksamkeit der Maßnahmen bewertet, die das Sicherheitsprinzip gemäß den AICPA Trust Services Principles erfüllen. Dieser Bericht bietet zusätzliche Transparenz hinsichtlich der AWS-Sicherheit basierend auf einer definierten Industrienorm und unterstreicht ferner das Bekenntnis von AWS, Kundendaten zu schützen.

SOC 3 – Sicherheit: AWS veröffentlicht den Bericht "Service Organization Controls 3 (SOC 3)". Der SOC 3-Bericht ist eine öffentlich zugängliche Zusammenfassung des SOC 2-Berichts und beinhaltet das Sicherheitssiegel AICPA SysTrust Security Seal.

Der Bericht umfasst das Gutachten des externen Auditors hinsichtlich der Umsetzung der Maßnahmen (basierend auf den im SOC 2-Bericht enthaltenen AICPA's Security Trust Principles), eine Erklärung des AWS-Managements bezüglich der Wirksamkeit der Maßnahmen und einen Überblick über die AWS-Infrastruktur und -Services.

DIN ISO/IEC 27001: AWS ist gemäß DIN ISO/IEC 27001 (International Organization for Standardization) zertifiziert. DIN ISO/IEC 27001 ist ein weit verbreiteter globaler Sicherheitsstandard, der Sicherheitsanforderungen für Informationsmanagementsysteme beschreibt. Der Standard bietet eine systematische, auf regelmäßigen Risikobewertungen basierende Vorgehensweise für den Umgang mit Unternehmens- und Kundendaten. Um die Zertifizierung zu erhalten, muss ein Unternehmen nachweisen, dass es über einen systematischen und kontinuierlichen Ansatz für den Umgang mit Informationssicherheitsrisiken verfügt, die die Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmens- und Kundendaten bedrohen.

PCI – Sicherheit: AWS erfüllt die Anforderungen von "Level 1" des PCI (Payment Card Industry) DSS (Data Security Standard), dem Datensicherheitsstandard der Zahlungs- und Kreditkartenbranche. Kunden können ihre Anwendungen auf unserer PCI-konformen Technologieinfrastruktur für die Speicherung, Verarbeitung und Übermittlung von Kreditkartendaten in der Cloud ausführen. Im Februar 2013 hat das PCI Security Standards Council die PCI DSS Cloud Computing Guidelines herausgegeben. Diese Leitlinien bieten Kunden, die eine Umgebung für Kreditkartendaten betreiben, Anleitungen zum Einrichten von PCI DSS-Kontrollen in der Cloud. AWS hat die PCI DSS Cloud Computing-Leitlinien in das AWS PCI-Compliance-Paket für Kunden integriert.

Compliance-Berichte und Zertifizierungen von AWS anfordern

Sie können die jeweiligen AWS-Compliance-Zertifizierungen und -Berichte unter https://aws.amazon.com/compliance/contact anfordern.

Weitere Informationen und Material zur AWS-Compliance-Umgebung

AWS verfügt über Whitepaper zur Compliance, die Informationen für AWS-Kunden enthalten, die AWS in ihre vorhandenen Kontrollrahmen integrieren und Sicherheitsbewertungen zum Einsatz von AWS durch ein Unternehmen erstellen und durchführen möchten.

Weitere Informationen zu AWS-Compliance-Zertifizierungen und -Berichten sowie zur Orientierung an bewährten Verfahren und Standards wie MPAA finden Sie auf der Compliance-Website von AWS.

Sicherheit IN Cloud

Während AWS für die Sicherheit der Cloud selbst sorgt, liegt die Verantwortung für die Sicherheit der Daten in der Cloud beim Kunden. Kunden sorgen daher selbst für ausreichende Sicherheitsmaßnahmen zum Schutz ihrer eigenen Inhalte, ihrer Plattform, Anwendungen, Systeme und Netzwerke, wie dies auch in einem Rechenzentrum vor Ort der Fall wäre.

Kunden behalten bei Nutzung der AWS-Services die Kontrolle über ihre eigenen Inhalte. Nicht AWS, sondern die Kunden bestimmen, welche Inhalte auf AWS gespeichert werden sollen, wie die Umgebungen konfiguriert und deren Inhalte gesichert werden sollen und welche Sicherheitsfunktionen und -tools sie einsetzen möchten und wie sie sie einsetzen. Aus diesem Grund sind die Kunden auch für die Sicherheit aller Daten verantwortlich, die ihr Unternehmen auf AWS ablegt, und für alle Komponenten, die sie mit ihrer AWS-Infrastruktur verbinden. Dazu gehören beispielsweise Gastbetriebssysteme, Anwendungen auf den Datenverarbeitungs-Instanzen der Kunden und Inhalte, die auf AWS-Speicher-, Plattform- und Datenbank-Services abgelegt und verarbeitet werden.

AWS bietet eine große Auswahl an Sicherheitsfunktionen, die Kunden zur Einrichtung, Implementierung und zum Betrieb ihrer eigenen sicheren AWS-Umgebung einsetzen können. Alternativ können Kunden ihre eigenen Sicherheitstools und -kontrollen verwenden. Die AWS-Services lassen sich nach Wunsch konfigurieren, damit Kunden diese Sicherheitsfunktionen nutzen und ihre Inhalte schützen können. Dazu gehören leistungsstarke Tools zur Identitäts- und Zugriffsverwaltung, Sicherheitsfunktionen, Verschlüsselung und Netzwerksicherheit. Folgende Maßnahmen können Kunden beispielsweise dabei helfen, ihre Inhalte schützen:

- Richtlinien für sichere Passwörter, individuelle Gewährung angemessener Zugriffsrechte und zuverlässiger Schutz von Zugriffsschlüsseln
- Angemessene Firewalls und Netzwerksegmentierung, Verschlüsselung von Inhalten und durchdachte Systemarchitektur, um Datenverlust und nicht autorisierten Zugriff zu verhindern

All diese Faktoren werden vom Kunden kontrolliert, nicht von AWS. AWS hat keine Informationen über die Inhalte, die vom Kunden auf AWS abgelegt werden, und ändert auch keine Konfigurationseinstellungen des Kunden. Diese werden vom Kunden festgelegt und gesteuert. Einzig und allein der Kunde kann entscheiden, welches Sicherheitsniveau für die Daten angemessen ist, die er mit AWS speichert und verarbeitet.

AWS veröffentlicht verschiedene Whitepaper zu Datensicherheit, Organisation, Risiko und Compliance sowie diverse Checklisten und bewährte Methoden, mit deren Hilfe Kunden die AWS-Sicherheitsmaßnahmen in ihre vorhandenen Kontrollrahmen integrieren und Sicherheitsbewertungen zum Einsatz von AWS in ihren Unternehmen erstellen und durchführen können. Natürlich können Kunden auch ihre eigenen Sicherheitsbewertungen erstellen und durchführen und die Erlaubnis zur Durchführung eigener Scans in ihrer Cloud-Infrastruktur beantragen, solange sich diese Scans auf die Datenverarbeitungs-Instanzen des Kunden beschränken und nicht gegen die AWS Acceptable Use Policy verstoßen.

Die Ausrichtung von AWS an den BSI-Standards für Informationssicherheit und den Bausteinen des IT-Grundschutz-Katalogs

AWS ist gemäß DIN ISO/IEC 27001 (International Organization for Standardization) zertifiziert. DIN ISO/IEC 27001 ist ein Sicherheitsstandard, der bewährte Verfahren zum Sicherheitsmanagement und umfassende Sicherheitsmaßnahmen gemäß den in ISO 27002 aufgestellten Leitlinien festlegt. Damit AWS die ISO 27001-Zertifizierung erhält, wird Folgendes erwartet:

- Systematische Bewertung der Informationssicherheitsrisiken unter Berücksichtigung der Auswirkungen von Gefährdungen und Schwachstellen im Unternehmen
- Konzeption und Implementierung umfassender Informationssicherheitsmaßnahmen und anderer Risikomanagementtypen, um Sicherheitsrisiken in Unternehmen und Architektur zu begegnen
- Einsatz eines übergreifenden Managementprozesses, durch den sichergestellt wird, dass die Informationssicherheitsmaßnahmen langfristig den Anforderungen der Informationssicherheit entsprechen

Wichtigster Punkt der kontinuierlichen Zertifizierung gemäß diesem Standard ist die effektive Pflege eines zuverlässigen Sicherheitsplans. Das durch diesen Standard geforderte Informationssicherheits-Managementsystem (ISMS) gibt vor, wie Sicherheit ganzheitlich und kontinuierlich gewährleistet wird. Die ISO 27001-Zertifizierung konzentriert sich vor allem auf das AWS-ISMS und bewertet, inwieweit die internen AWS-Prozesse dem ISO-Standard entsprechen. Die Zertifizierung wird erst vergeben, nachdem ein unabhängiger, externer Auditor eine Bewertung der AWS-Prozesse und -Maßnahmen durchgeführt und bestätigt hat, dass diese den umfassenden ISO 27001-Zertifizierungsstandard erfüllen. Wenn Sie an einer ISO 27001-Zertifizierung interessiert sind und einen Teil Ihrer oder Ihre gesamte IT in der AWS-Cloud verwalten, bedeutet dies zwar nicht, dass Sie automatisch zertifiziert sind, aber es kann die Zertifizierung möglicherweise erleichtern.

Zusätzlich zu unserer ISO 27001-Zertifizierung veranschaulicht die folgende Übersicht die Ausrichtung von AWS am IT-Grundschutz-Katalog. Außerdem sehen Sie, welche technischen Maßnahmen gemäß Definition im IT-Grundschutz-Katalog Ihnen als dem Kunden obliegen.

Baustein-Referenznr.	Bezeichnung des Bausteins	Verantwortung von AWS (A) bzw. des Kunden (K)	Zusätzliche Informationen
B1	**Übergreifende Aspekte**		
B 1.0	Sicherheitsmanagement	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 1.0
B 1.1	Organisation	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 1.1
B 1.2	Personal	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 1.2
B 1.3	Notfallmanagement	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 1.3
B 1.4	Datensicherungskonzept	K	Kunden behalten die Verantwortung und Kontrolle über ihre Daten und dazugehörige Sicherheitsrichtlinien
B 1.5	Datenschutz	K	Kunden behalten die Verantwortung und Kontrolle über ihre Daten und dazugehörige Sicherheitsrichtlinien
B 1.6	Schutz vor Schadprogrammen	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 1.6
B 1.7	Kryptokonzept	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 1.7
B 1.8	Behandlung von Sicherheitsvorfällen	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 1.8
B 1.9	Hard- und Software-Management	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 1.9

Baustein-Referenznr.	Bausteintitel	Verantwortung von AWS (A) bzw. des Kunden (K)	Zusätzliche Informationen
B 1.10	Standardsoftware	K	Kunden behalten die Verantwortung und Kontrolle über mit COTS zusammenhängende Maßnahmen. Innerhalb des AWS-Systems wird COTS von AWS nicht eingesetzt.
B 1.11	Outsourcing	K	Kunden bleiben verantwortlich für die mit Outsourcing zusammenhängenden Maßnahmen. AWS nutzt keine Dienste von Cloud-Drittanbietern zur Bereitstellung von AWS-Services.
B 1.12	Archivierung	K	Kunden sind weiterhin für die Kontrolle und angemessene Archivierung ihrer Daten verantwortlich.
B 1.13	Sensibilisierung und Schulung zur Informationssicherheit	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 1.13
B 1.14	Patch- und Änderungsmanagement	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 1.14
B 1.15	Löschen und Vernichten von Daten	K	Kunden sind für das Löschen ihrer Daten verantwortlich. Weitere Informationen zur Vernichtung physischer Mediengeräte durch AWS siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen.
B 1.16	Anforderungsmanagement	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 1.16
B 2	**Infrastruktur**		
B 2.1	Allgemeines Gebäude	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 2.1
B 2.2	Elektrotechnische Verkabelung	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 2.2
B 2.3	Büroraum/Lokaler Arbeitsplatz	n. z.	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 2.1
B 2.4	Serverraum	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 2.1
B 2.5	Datenträgerarchiv	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 2.1
B 2.6	Raum für technische Infrastruktur	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 2.1
B 2.7	Schutzschränke	n. z.	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 2.1

Baustein-Referenznr.	Bausteintitel	Verantwortung von AWS (A) bzw. des Kunden (K)	Zusätzliche Informationen
B 2.8	Häuslicher Arbeitsplatz	n. z.	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 2.1
B 2.9	Rechenzentrum	n. z.	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 2.1
B 2.10	Mobiler Arbeitsplatz	n. z.	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 2.1
B 2.11	Besprechungs-, Veranstaltungs- und Schulungsräume	n. z.	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 2.1
B 2.12	IT-Verkabelung	n. z.	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 2.1
B 3	**IT-Systeme**		
B 3.101	Allgemeiner Server	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 3.101
B 3.102	Server unter Unix	K	Kunden sind weiterhin für ihr Betriebssystem in der AWS-Umgebung verantwortlich.
B 3.103	Server unter Windows NT – entfallen	n. z.	n. z.
B 3.104	Server unter Novell Netware 3.x – entfallen	n. z.	n. z.
B 3.105	Server unter Novell Netware Version 4.x – entfallen	n. z.	n. z.
B 3.106	Server unter Windows 2000 – entfallen	n. z.	n. z.
B 3.107	S/390- und zSeries-Mainframe	n. z.	n. z.
B 3.108	Windows Server 2003	K	Kunden sind weiterhin für ihr Betriebssystem in der AWS-Umgebung verantwortlich.
B 3.109	Windows Server 2008	K	Kunden sind weiterhin für ihr Betriebssystem in der AWS-Umgebung verantwortlich.
B 3.201	Allgemeiner Client	K	Kunden sind weiterhin für ihr Betriebssystem in der AWS-Umgebung verantwortlich.
B 3.202	Allgemeines nicht vernetztes IT-System	K	Kunden sind weiterhin für ihr Betriebssystem in der AWS-Umgebung verantwortlich.
B 3.203	Laptop	K	Kunden sind weiterhin für ihr Betriebssystem in der AWS-Umgebung verantwortlich.
B 3.204	Client unter Unix	K	Kunden sind weiterhin für ihr Betriebssystem in der AWS-Umgebung verantwortlich.

Baustein-Referenznr.	Bausteintitel	Verantwortung von AWS (A) bzw. des Kunden (K)	Zusätzliche Informationen
B 3.205	Client unter Windows NT – entfallen	n. z.	n. z.
B 3.206	Client unter Windows 95 – entfallen	n. z.	n. z.
B 3.207	Client unter Windows 2000 – entfallen	n. z.	n. z.
B 3.208	Internet-PC	K	Kunden sind weiterhin für ihr Betriebssystem in der AWS-Umgebung verantwortlich.
B 3.209	Client unter Windows XP	K	Kunden sind weiterhin für ihr Betriebssystem in der AWS-Umgebung verantwortlich.
B 3.210	Client unter Windows Vista	K	Kunden sind weiterhin für ihr Betriebssystem in der AWS-Umgebung verantwortlich.
B 3.211	Client unter Mac OS X	K	Kunden sind weiterhin für ihr Betriebssystem in der AWS-Umgebung verantwortlich.
B 3.212	Client unter Windows 7	K	Kunden sind weiterhin für ihr Betriebssystem in der AWS-Umgebung verantwortlich.
B 3.301	Sicherheitsgateway (Firewall)	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 3.301
B 3.302	Router und Switches	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 3.302
B 3.303	Speichersysteme und Speichernetze	K	Kunden sind weiterhin für ihre Speichersysteme und Speichernetze in der AWS-Umgebung verantwortlich.
B 3.304	Virtualisierung	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 3.304
B 3.305	Terminalserver	K	Kunden sind weiterhin für ihre Terminalserver verantwortlich.
B 3.401	TK-Anlage	K	Kunden sind weiterhin für ihre TK-Anlagen verantwortlich.
B 3.402	Faxgerät	K	Kunden sind weiterhin für ihre Faxgeräte verantwortlich.
B 3.403	Anrufbeantworter – entfallen	n. z.	n. z.
B 3.404	Mobiltelefon	K	Kunden sind weiterhin für ihre Mobiltelefone verantwortlich.
B 3.405	PDA	K	Kunden sind weiterhin für ihre PDAs verantwortlich.
B 3.406	Drucker, Kopierer und Multifunktionsgeräte	K	Kunden sind weiterhin für ihre Drucker, Kopierer und Multifunktionsgeräte verantwortlich.
B4	**Netze**		
B 4.1	Heterogene Netze	n. z.	Trifft nicht auf die AWS-Umgebung zu
B 4.2	Netz- und Systemmanagement	A, K	Siehe Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen, Abschnitt B 4.2

Baustein-Referenznr.	Bausteintitel	Verantwortung von AWS (A) bzw. des Kunden (K)	Zusätzliche Informationen
B 4.3	Modem	K	Kunden sind weiterhin für ihre Modems verantwortlich.
B 4.4	VPN	K	Kunden sind weiterhin für ihre VPNs und Einsatz von VPC verantwortlich.
B 4.5	LAN-Anbindung eines IT-Systems über ISDN	K	Kunden sind weiterhin für ihre LAN-Anbindung eines IT-Systems über ISDN verantwortlich.
B 4.6	WLAN	K	Kunden sind weiterhin für ihre WLANs verantwortlich.
B 4.7	VoIP	K	Kunden sind weiterhin für ihre VoIPs verantwortlich.
B 4.8	Bluetooth	K	Kunden sind weiterhin für ihre Bluetoothgeräte verantwortlich.
B5	**Anwendungen**		
B 5.1	Peer-to-Peer-Dienste - entfallen	n. z.	n. z.
B 5.2	Datenträgeraustausch	K	Kunden sind weiterhin für ihren Datenträgeraustausch verantwortlich.
B 5.3	Groupware	K	Kunden sind weiterhin für ihre Groupware verantwortlich.
B 5.4	Webserver	K	Kunden sind weiterhin für ihre Webserver verantwortlich.
B 5.5	Lotus Notes/Domino	K	Kunden sind weiterhin für ihr Lotus Notes/Domino verantwortlich.
B 5.6	Faxserver	K	Kunden sind weiterhin für ihre Faxserver verantwortlich.
B 5.7	Datenbanken	K	Kunden sind weiterhin für ihre Datenbanken verantwortlich.
B 5.8	Telearbeit	K	Kunden sind weiterhin für ihre Telearbeitsverfahren verantwortlich.
B 5.9	Novell eDirectory	K	Kunden sind weiterhin für ihr Novell eDirectory verantwortlich.
B 5.10	Internet Information Server – entfallen	n. z.	n. z.
B 5.11	Apache Webserver – entfallen	K	Kunden sind weiterhin für ihre Apache Webserver verantwortlich.
B 5.12	Microsoft Exchange/Outlook	K	Kunden sind weiterhin für ihr Microsoft Exchange/Outlook verantwortlich.
B 5.13	SAP-System	K	Kunden sind weiterhin für ihre SAP-Systeme verantwortlich.
B 5.14	Mobile Datenträger	K	Kunden sind weiterhin für ihre mobilen Datenträger verantwortlich.
B 5.15	Allgemeiner Verzeichnisdienst	K	Kunden sind weiterhin für ihre allgemeinen Verzeichnisdienste verantwortlich.
B 5.16	Active Directory	K	Kunden sind weiterhin für ihr Active Directory verantwortlich.

Baustein-Referenznr.	Bausteintitel	Verantwortung von AWS (A) bzw. des Kunden (K)	Zusätzliche Informationen
B 5.17	Samba	K	Kunden sind weiterhin für ihre Sambas verantwortlich.
B 5.18	DNS-Server	K	Kunden sind weiterhin für ihre DNS-Server verantwortlich.
B 5.19	Internet-Nutzung	K	Kunden sind weiterhin für ihre Internet-Nutzung verantwortlich.
B 5.20	OpenLDAP	K	Kunden sind weiterhin für ihre OpenLDAPs verantwortlich.
B 5.21	Webanwendungen	K	Kunden sind weiterhin für ihre Webanwendungen verantwortlich.
B 5.22	Protokollierung	A, K	Kunden sind weiterhin für ihre Protokollierung verantwortlich.

Ausrichtung von AWS an IT-Grundschutz-Bausteinen, Gefährdungen und Maßnahmen

M 1.0 Sicherheitsmanagement

AWS hat einen Rahmen für die Informationssicherheit und Richtlinien festgelegt, die auf dem COBIT-Framework (Control Objectives for Information and related Technology) beruhen, und hat das zertifizierbare Framework ISO 27001 mithilfe der ISO 27002-Kontrollen, der American Institute of Certified Public Accountants (AICPA) Trust Services Principles, dem PCI DSS v2.0 und der Veröffentlichung 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems) des National Institute of Standards and Technology (NIST) integriert. Die Kontrollumgebung beginnt bei Amazon auf höchster Unternehmensebene. Die Geschäftsführung sowie die Führungskräfte des oberen Managements spielen bei der Festlegung der Grundwerte des Unternehmens eine entscheidende Rolle.

AWS verfügt über eine etablierte Informationssicherheits-Organisation, die durch das AWS-Sicherheitsteam gemanagt und durch den AWS Chief Information Security Officer (CISO, Beauftragter für die zentrale IT-Sicherheit) geleitet wird. AWS führt für alle Benutzer des Informationssystems, die AWS unterstützen, Schulungen zur Sensibilisierung durch. Diese jährliche Schulung zur Sicherheitssensibilisierung umfasst die folgenden Themen: Zielsetzung der Schulung über Sicherheit und Sensibilisierung, Ablageorte aller AWS-Richtlinien, AWS-Vorfallreaktionsprozesse (einschließlich Anweisungen darüber, wie interne und externe Sicherheitsvorfälle zu berichten sind).

AWS hat Richtlinien zur Zertifizierung, Autorisierung und Sicherheitsbewertung erarbeitet, die die Zielsetzung, den Umfang, die Rollen, die Verantwortlichkeiten und das Engagement der Unternehmensleitung in Bezug darauf festlegt, wie AWS die Ausrichtung an durch Dritte geprüften Zertifizierungen/Akkreditierungen verwaltet, überwacht und kommuniziert. Das AWS Security Assurance-Team ist damit beauftragt, die Compliance-Frameworks einzuführen, zu verwalten, zu überwachen und zu bewerten. Dazu gehört auch die Verwaltung der Prüfgegenstände wie Dokumentationen zur Systemsicherheit, Prüfgegenstände, Prüfungsergebnisse und Abhilfemaßnahmen. AWS arbeitet mit externen Zertifizierungsstellen und unabhängigen Auditoren zusammen, um unsere Compliance mit allen Compliance-Frameworks im gesamten System zu überprüfen und zu validieren.

Die Verantwortung der AWS-Kunden

Die Kunden sind für die Einrichtung eines Programms für das Sicherheitsmanagement verantwortlich, das ihrer Umgebung angepasst ist und mit M 1.0 im Einklang steht.

M 1.1 Organisation

AWS hat einen Rahmen für die Informationssicherheit und Richtlinien festgelegt, die auf dem COBIT-Framework (Control Objectives for Information and related Technology) beruhen, und hat das zertifizierbare Framework ISO 27001 mithilfe der ISO 27002-Kontrollen, der American Institute of Certified Public Accountants (AICPA) Trust Services Principles, dem PCI DSS v2.0 und der Veröffentlichung 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems) des National Institute of Standards and Technology (NIST) integriert. AWS befolgt Sicherheitsrichtlinien, bietet Sicherheitsschulungen für Mitarbeiter an und führt Sicherheitsprüfungen für Anwendungen durch. Diese Prüfungen beurteilen die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie die Einhaltung der Richtlinien zur Informationssicherheit. Die Kontrollumgebung beginnt bei Amazon auf höchster Unternehmensebene. Die Geschäftsführung sowie die Führungskräfte des oberen Managements spielen bei der Festlegung der Grundwerte des Unternehmens eine entscheidende Rolle. Die AWS-Organisationsstruktur bietet einen Rahmen für die Planung, Ausführung und Kontrolle der Geschäftstätigkeiten. Die Organisationsstruktur weist Rollen und Verantwortlichkeiten zu, um eine angemessene Personalausstattung, Betriebseffizienz und Aufgabenverteilung zu gewährleisten. Das Management hat auch leitendes Personal mit Kompetenzen ausgestattet und geeignete Berichtslinien eingerichtet. Die Überprüfung der Ausbildung, der vorherigen Beschäftigung und, in einzelnen Fällen und soweit rechtlich zulässig, der Hintergrundinformationen zählen zu den Bestandteilen des Einstellungsprozesses des Unternehmens, wobei diese Überprüfungen im angemessenen Verhältnis zur Position und zum Level der Zugriffsberechtigung des Mitarbeiters auf AWS-Einrichtungen durchgeführt werden müssen. Das Unternehmen befolgt einen strukturierten Onboarding-Prozess, um neue Mitarbeiter mit den Tools, Prozessen, Systemen, Richtlinien und Verfahren von Amazon vertraut zu machen.

AWS hat die folgende Maßnahmenliste zusammengestellt, um Bedrohungen in der Lieferkette vorzubeugen, welche wiederum die Ressourcen beeinträchtigen könnten.

Agile Beschaffung – Das obere Management von AWS hält eine wöchentliche Besprechung ab, in der festgelegt wird, welche Maßnahmen notwendig sind, um die Geschäftsanforderungen zu erfüllen. Die Einzelposten, die für die Abdeckung der Kapazitätsanforderungen ermittelt wurden, werden in RFQs (Requests for Quotation, Aufforderungen zur Angebotsabgabe) bekanntgegeben und anschließend erworben. Diese häufige Überprüfung der Anforderungen und der daraus erfolgende Angebots- und Akquisitionszyklus führen zu einem wesentlich agileren Akquisitionsprozess, als wenn die Ausgaben für die Einzelposten in einem Jahreszyklus eingeplant werden. Durch diesen Prozess ist es AWS möglich, schnell auf Geschäftsanforderungen zu reagieren.

Einzelverträge – Die wöchentlichen Gespräche und häufigen RFQs erlauben eine größere Anzahl kleinerer Verträge, die bei Bedarf erneuert werden. Falls ein Anbieter aus welchem Grund auch immer nicht in der Lage ist, die Lieferung auszuführen, sind die Auswirkungen gering und für die Beschaffung kann leicht eine neue Quelle gefunden werden.

Verwendung anerkannter, etablierter, diversifizierter Lieferanten – Dem Eingehen vertraglicher Vereinbarungen, um Hardware, Software, Firmware oder Services zu erwerben, muss eine Unternehmensprüfung (Due Diligence) der Lieferanten vorausgehen.

Mehrere Anbieter – Eine Liste zugelassener Anbieter wird vom AWS-Team geführt, jeweils mit mehreren Anbietern zur Auswahl für jeden Komponententyp. Sollte ein Lieferant außerstande sein, die Lieferung auszuführen, kann ein anderer Anbieter für die nächsten Beschaffungsvorgänge verwendet werden.

Obwohl ein Großteil des AWS-Systems unternehmensintern entwickelt wurde, um den besonderen AWS-Anforderungen gerecht zu werden, verwendet AWS soweit wie möglich auch standardmäßige, kommerziell erhältliche Informationssystemkonfigurationen und reduziert so die Möglichkeit, Systeme und Produkte zu erwerben, die während der Lieferkettenvorgänge beschädigt wurden.

Beim Erwerb der AWS-Ressourcen werden diese mit einer Komponentenkennzeichnung versehen. AWS-Komponentenkennzeichnungen sind kundenunabhängig und dienen der Inventarisierung der Hardware innerhalb des AWS-Tools zur Komponentenverwaltung. In den AWS-Rechenzentren wird die Hardware normalerweise nicht physisch speziellen Kunden oder den auf der Hardware gespeicherten Daten zugeordnet. Alle Kundendaten werden unabhängig von ihrer Quelle als kritisch angesehen und aus diesem Grund werden alle Medien vertraulich behandelt. Die Prozesse und Vorgänge der AWS-Komponentenverwaltung werden von unabhängigen, externen Auditoren während der Prüfungen bezüglich der Compliance mit PCI DSS, ISO 27001 und FedRAMP überprüft.

AWS verwendet für den Zugang zu Rechenzentren nicht nur Multi-Factor Authentication-Mechanismen sondern auch zusätzliche Sicherheitsmechanismen, die so ausgelegt sind, dass nur autorisierte Personen Zugang zu einem AWS-Rechenzentrum erhalten. Die autorisierten Personen müssen ihren Zugangsausweis an einem Kartenleser verwenden und ihre individuelle PIN eingeben, um Zugang zur Einrichtung und den Räumen zu erhalten, für die sie autorisiert wurden.

Der physische Zugang zu den Rechenzentren wird durch das elektronische AWS-Zugangskontrollsystem überwacht. Für den Zugang in das Gebäude und die Räume setzt sich das System aus Kartenlesern und PIN-Pads zusammen, für das Verlassen besteht es nur aus Kartenlesern. Durch die Verwendung von Kartenlesern beim Verlassen von Gebäuden und Räumen treten Doppelzutrittssperren in Kraft, die sicherstellen, dass autorisierte Personen nicht von unautorisierten Personen verfolgt werden, die sich so ohne Ausweis Zutritt verschaffen. Zusätzlich zum Zugangskontrollsystem sind alle Eingänge der AWS-Rechenzentren, einschließlich des Haupteingangs, der Laderampe und aller Dachausstiege/-luken, mit Einbruchmeldevorrichtungen versehen, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird. Neben den elektronischen Mechanismen verwenden die AWS-Rechenzentren rund um die Uhr auch ausgebildete Sicherheitskräfte, die sowohl innerhalb der Gebäude als auch in deren Umgebung stationiert sind. Innerhalb des Systems wird der Zugang zu den Rechenzentren nur nach Notwendigkeit erteilt; alle physischen Zugangsanfragen werden vom zuständigen AAM (Area Access Manager, Zugangsmanager) überprüft und genehmigt. AWS-Rechenzentren sind in unauffälligen Anlagen untergebracht und sind nicht für die Öffentlichkeit zugänglich. Der physische Zugang wird sowohl in der Umgebung als auch an den Zutrittspunkten zum Gebäude streng kontrolliert. AWS gewährt nur solchen Anbietern, Auftragnehmern und Besuchern Zugang und Informationen zu den Rechenzentren, für die eine legitime geschäftliche Notwendigkeit besteht, wie Notfallreparaturen. Alle Besucher der Rechenzentren müssen vorab durch den zuständigen Zugangsmanager (AAM) autorisiert worden sein und im AWS-Ticketmanagementsystem dokumentiert werden. Bei der Ankunft am Rechenzentrum müssen sie sich ausweisen und anmelden, bevor ihnen ein Besucherausweis ausgestellt wird. Während sie sich im Rechenzentrum befinden, werden sie beständig von autorisiertem Personal begleitet. Die physischen Sicherheitsmechanismen von AWS werden von unabhängigen, externen Auditoren während der Prüfungen bezüglich der Compliance mit SOC, PCI DSS, ISO 27001 und FedRAMP überprüft.

AWS hat formale Richtlinien und Verfahren gemäß ISO 27001 erstellt, um Mindeststandards für den logischen Zugriff auf die AWS-Ressourcen festzulegen. Der Bericht AWS-SOC 1-Typ II und SOC 2-Typ II beschreibt die vorhandenen Kontrollen, um die Zugriffsberechtigungen von AWS-Ressourcen zu verwalten. Das AWS-Produktionsnetzwerk ist vom Amazon-Unternehmensnetzwerk getrennt und erfordert separate Anmeldeinformationen für den logischen Zugriff. Das Amazon-Unternehmensnetzwerk verwendet Benutzer-IDs, Passwörter und Kerberos, während das AWS-Produktionsnetzwerk eine Authentifizierung mit einem öffentlichen SSH-Schlüssel durch einen Bastion-Host erfordert. AWS-Entwickler und Administratoren des Amazon-Unternehmensnetzwerks, die Zugriff auf die AWS-Cloud-Komponenten benötigen, müssen ausdrücklich eine Anforderung auf Zugriff über das AWS-Zugriffsverwaltungssystem stellen. Alle Anforderungen werden vom entsprechenden Verantwortlichen oder Manager überprüft und genehmigt. Konten werden alle 90 Tage überprüft; es ist eine ausdrückliche erneute Überprüfung erforderlich oder der Zugriff auf die Ressource wird automatisch widerrufen. Der Zugriff wird ebenfalls automatisch widerrufen, wenn ein Mitarbeiterdatensatz im Personalverwaltungssystem von Amazon geschlossen wird. Windows- und UNIX-Konten werden deaktiviert und das Zugriffsverwaltungssystem von Amazon entfernt den Benutzer aus allen Systemen. Anforderungen für Zugriffsänderungen werden im Auditprotokoll des Zugriffsverwaltungssystem von Amazon erfasst. Wenn sich die Funktion eines Mitarbeiters ändert, muss der kontinuierliche Zugriff ausdrücklich in der Ressource genehmigt werden, da dieser sonst automatisch widerrufen wird.

Wenn die Lebensdauer eines Speichergeräts zu Ende geht, führt AWS einen Prozess zur Außerbetriebnahme durch, der entwickelt wurde, damit Kundendaten nicht an unautorisierte Personen offengelegt werden. AWS wendet die in DoD 5220.22-M ("Betriebshandbuch zum nationalen Branchensicherheitsprogramm") oder NIST 800-88 ("Richtlinien zur Medienbereinigung") beschriebenen Techniken an, um Daten im Rahmen des Prozesses zur Außerbetriebnahme zu zerstören. Wenn ein Hardware-Gerät nicht mithilfe dieser Prozesse außer Betrieb genommen werden kann, dann wird das Gerät entmagnetisiert und physisch den branchenüblichen Vorgehensweisen entsprechend zerstört. Weitere Informationen finden Sie im AWS-Whitepaper "Übersicht über die Sicherheitsprozesse" unter http://aws.amazon.com/security.

Die Verantwortung der AWS-Kunden

Die Kunden sind für die Einrichtung einer Sicherheitsorganisation verantwortlich, die ihrer Umgebung angepasst ist und mit M 1.1 im Einklang steht.

M 1.2 Personal

Die AWS-Organisationsstruktur bietet einen Rahmen für die Planung, Ausführung und Kontrolle der Geschäftstätigkeiten. Die Organisationsstruktur weist Rollen und Verantwortlichkeiten zu, um eine angemessene Personalausstattung, Betriebseffizienz und Aufgabenverteilung zu gewährleisten. Das Management hat auch leitendes Personal mit Kompetenzen ausgestattet und geeignete Berichtslinien eingerichtet.
Die Überprüfung der Ausbildung, der vorherigen Beschäftigung und, in einzelnen Fällen und soweit rechtlich zulässig, der Hintergrundinformationen zählen zu den Bestandteilen des Einstellungsprozesses des Unternehmens, wobei diese Überprüfungen im angemessenen Verhältnis zur Position und Level der Zugriffsberechtigung des Mitarbeiters auf AWS-Einrichtungen durchgeführt werden müssen. Das Unternehmen befolgt einen strukturierten Onboarding-Prozess, um neue Mitarbeiter mit den Tools, Prozessen, Systemen, Richtlinien und Verfahren von Amazon vertraut zu machen.

AWS hat verschiedene Methoden zur internen Kommunikation auf weltweiter Ebene implementiert, um Mitarbeiter dabei zu unterstützen, ihre jeweiligen Rollen und Verantwortlichkeiten zu verstehen und wichtige Vorfälle zeitgerecht zu kommunizieren. Diese Methoden umfassen Orientierungs- und Schulungsprogramme für neu eingestellte Mitarbeiter sowie E-Mail-Benachrichtigungen und das Posten von Informationen über das Amazon-Intranet.

Die Rechtsberater von Amazon verwalten und überarbeiten regelmäßig die Geheimhaltungsvereinbarung von Amazon, um die Geschäftsbedürfnisse von AWS widerzuspiegeln. Die Geheimhaltungsvereinbarung von AWS wird von unabhängigen, externen Auditoren während der Prüfungen bezüglich der Compliance mit ISO 27001 und FedRAMP überprüft.

AWS führt für alle Benutzer des Informationssystems, die AWS unterstützen, Schulungen zur Sensibilisierung durch. Diese jährliche Schulung zur Sicherheitssensibilisierung umfasst die folgenden Themen:

- die Zielsetzung der Schulung über Sicherheit und Sensibilisierung,
- die Ablageorte aller AWS-Richtlinien,
- die AWS-Vorfallreaktionsprozesse (einschließlich Anweisungen darüber, wie interne und externe Sicherheitsvorfälle zu berichten sind).

Das Onboarding von Auftragnehmern und Anbietern wird für Mitarbeiter und Auftragnehmer gleich gehandhabt, wobei die Verantwortung hierfür zwischen den Bereichen Personalverwaltung und Betriebsprozesse sowie den Service-Inhabern aufgeteilt wird. Die AWS-Richtlinien, Prozesse und relevanten Schulungsprogramme werden von unabhängigen, externen Auditoren während der Prüfungen bezüglich der Compliance mit SOC, PCI DSS, ISO 27001 und FedRAMP überprüft. Weitere Informationen finden Sie im AWS-Whitepaper "Übersicht über die Sicherheitsprozesse" unter http://aws.amazon.com/security.

Das AWS-Personalverwaltungsteam definiert die internen Verwaltungsaufgaben, die im Falle einer Kündigung bzw. einer Rollenveränderung der Mitarbeiter und Anbieter befolgt werden müssen. Die Verantwortung für die Genehmigung/Entziehung der Zugangsrechte der Mitarbeiter und Auftragnehmer wird zwischen den Bereichen Personalverwaltung und Betriebsprozesse sowie den Service-Inhabern aufgeteilt. Weitere Informationen finden Sie im AWS-Whitepaper "Übersicht über die Sicherheitsprozesse" unter http://aws.amazon.com/security.

Die Verantwortung der AWS-Kunden

Die Kunden sind für die Einrichtung eines Personalverwaltungsprogramms gemäß M 1.2 für ihre Umgebung verantwortlich.

B 1.3 Notfallmanagement

Die AWS-Richtlinien und -Pläne zum Notfallmanagement wurden im Einklang mit ISO 27001 entwickelt und getestet und sind Teil des umfassenderen Ansatzes von AWS hinsichtlich der Entwicklung von Informationssicherheitsrichtlinien.

Das Programm AWS Resilience umfasst die Verfahren und Vorgehensweisen, die die AWS-Komponenten zur Identifizierung und Behebung eines erheblichen Vorfalls einsetzen. Dieses Programm nimmt den traditionellen Ansatz des Contingency Managements mit Elementen herkömmlicher Betriebskontinuitäts- und Notfallwiederherstellungspläne zur Grundlage. Ergänzt werden diese jedoch um wichtige Elemente proaktiver Strategien zur Gefahreneindämmung, z. B. durch Schaffung physisch separater Availability Zones (AZ) und fortlaufende Infrastrukturkapazitätsplanung. Die Notfallpläne und Vorfallleitfäden von AWS werden ständig um neu erkannte Betriebsrisiken und aus vergangenen Störungen Gelerntes ergänzt. Die Handhabung von Störungen durch AWS wird regelmäßig getestet. Aus diesen Tests gewonnene Erkenntnisse werden umgesetzt und die Dokumentation wird entsprechend aktualisiert.

AWS-Rechenzentren werden gruppenweise in verschiedenen Regionen der Welt errichtet. Alle Rechenzentren sind online und bedienen Kunden; kein Rechenzentrum ist abgeschaltet. Bei einem Ausfall verschieben automatische Prozesse den Kundendatenverkehr weg von den betroffenen Bereichen. Die Kernanwendungen werden in einer N+1-Konfiguration bereitgestellt, sodass im Falle eines Rechenzentrumsausfalls ausreichend Kapazität vorhanden ist, um den Datenverkehr lastverteilt an die verbleibenden Standorte zu verteilen. AWS bietet Kunden die Flexibilität, Instanzen zu platzieren und Daten innerhalb mehrerer geografischer Regionen sowie über mehrere Availability Zones innerhalb der einzelnen Regionen zu speichern. Jede Availability Zone wurde als unabhängige Ausfallszone entwickelt. Dies bedeutet, dass Availability Zones innerhalb einer typischen Stadtregion physisch verteilt sind und sich in Gebieten mit niedrigerem Überschwemmungsrisiko befinden (je nach Region gibt es unterschiedliche Überschwemmungszonenkategorisierungen). Zusätzlich zu einer eigenständigen unterbrechungsfreien Stromversorgung und Notstromgeneratoren vor Ort werden alle Availability Zones über unterschiedliche Stromnetze von unabhängigen Stromversorgern gespeist, um Einzelfehlerstellen zu minimieren. Sämtliche Availability Zones sind redundant mit mehreren Tier-1-Transit-Providern verbunden. Kunden sollten die Architektur ihrer AWS-Nutzung so erstellen, dass sie mehrere Regionen und Availability Zones umfasst. Durch das Verteilen von Anwendungen über mehrere Availability Zones bleibt die Architektur bei den meisten Ausfallarten, einschließlich Naturkatastrophen oder Systemausfällen, stabil.

Weitere Details finden Sie im AWS-SOC 1-Typ II-Bericht. Außerdem enthält ISO 27001, Anhang A.11.2, zusätzliche Informationen. AWS wurde durch einen unabhängigen Auditor auf Erfüllung der ISO 27001-Zertifizierungsanforderungen geprüft.

Die Verantwortung der AWS-Kunden

Kunden sind für die Einrichtung eines Geschäftskontinuitätsplans für ihre Umgebung im Einklang mit B 1.3 verantwortlich.

AWS bietet Kunden eine raschere Notfallwiederherstellung ihrer kritischen IT-Systeme, ohne dass ein kostspieliger zweiter physischer Standort erforderlich ist. Die AWS Cloud unterstützt zahlreiche bekannte Notfallwiederherstellungsarchitekturen, von "Pilot-Light"-Umgebungen, die sich ohne Zeitverlust skalieren lassen, bis zu Hot-Standby-Umgebungen, die ein rasches Failover erlauben. Weitere Informationen zur Notfallwiederherstellung bei AWS finden Sie unter http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf.

Mit AWS können Kunden einen zuverlässigen Kontinuitätsplan implementieren, der häufige Server-Instanz-Backups, Datenredundanz-Replikation und Bereitstellungsarchitekturen für mehrere Regionen bzw. Availability Zones umfasst. AWS bietet Kunden die Flexibilität, Instanzen zu platzieren und Daten innerhalb mehrerer geografischer Regionen sowie über mehrere Availability Zones innerhalb der einzelnen Regionen zu speichern. Jede Availability Zone wurde als unabhängige Ausfallszone entwickelt. Bei einem Ausfall wird der Datenverkehr des Kunden durch automatische Prozesse von dem betroffenen Bereich ferngehalten.

B 1.6 Schutz vor Schadprogrammen

Das Programm, die Verfahren und die Vorgehensweisen von AWS zur Handhabung von Virenschutz bzw. Schadprogrammen entsprechen den ISO 27001-Standards. Weitere Informationen finden Sie im SOC 1-Typ II-Bericht für AWS. Das gesamte Konfigurationsmanagement und alle Nachbesserungsprozesse von AWS werden regelmäßig von unabhängigen Auditoren auf Erfüllung der Anforderungen von SOC, PCI DSS, ISO 27001 und FedRAMP geprüft.

Ein Konfigurationsmanagementtool wird zur Verwaltung von bereitstellbarer Software in Paketen, Paketgruppen und Umgebungen verwendet. Bei einem Paket handelt es sich um eine Sammlung zusammenhängender Dateien, z. B. eng miteinander verknüpfte Software oder verknüpfter Content. Mehrere Pakete, die oft gemeinsam bereitgestellt werden, werden als Paketgruppe bezeichnet. Eine Umgebung schließlich ist eine Kombination von Paketen und Paketgruppen, die in einer Gruppe von Hostklassen (Hosts oder Servern mit derselben Funktion) bereitgestellt werden. Eine Umgebung stellt die Gesamtheit aller Pakete dar, die zur Ausführung einer bestimmten Funktion durch den Server erforderlich sind. Amazon-Geräte, z. B. Laptops, sind mit Virenschutzsoftware konfiguriert, die E-Mail-Filterung und Schadware-Erkennung umfasst.

Bei jeder Änderung, die in den Systemen und Geräten innerhalb des AWS-Systems vorgenommen wird, wird ein Change Management-Ticket (CM, Änderungsverwaltung) erstellt. In diesem CM-Ticket werden alle Details der Änderung festgehalten. Dazu gehören eine Beschreibung der Änderung, Auswirkungsanalyse, ggf. Sicherheitsüberlegungen, Änderungszeitraum und erforderliche Genehmigungen.

AWS sorgt für die Verteilung des Basis-OS, das auf den Hosts verwendet wird. AWS nutzt eine speziell angepasste Version von RHEL mit minimaler Basisfunktionalität. Ports, Protokolle und Services, die nicht benötigt werden, sind in den Basis-Builds deaktiviert. Mithilfe der Build-Tools fügen die Serviceteams nur die zugelassenen Softwarepakete hinzu, die zur Serverfunktion gemäß den Basiskonfigurationen notwendig sind. Die Server werden regelmäßig gescannt und unnötige Ports oder Protokolle werden mithilfe des Nachbesserungsprozesses behoben. Bereitgestellte Software durchläuft wiederholte Penetrationstests, die durch ausgewählte Branchenexperten ausgeführt werden. Die aus den jährlichen Penetrationstests resultierenden Nachbesserungen werden über den Nachbesserungsprozess ebenfalls in die Basiskonfiguration aufgenommen.

Die Verantwortung der AWS-Kunden

Kunden sind für den Schutz ihrer Umgebung vor Schadprogrammen im Einklang mit B 1.3 verantwortlich.

B 1.7 Kryptokonzept

AWS gibt Ihnen die Möglichkeit, für nahezu alle Services einschließlich S3, EBS und EC2 Ihren eigenen Verschlüsselungsmechanismus zu verwenden. VPC-Sitzungen sind ebenfalls verschlüsselt. Für AWS-Verbindungen stehen FIPS-zugelassene Hashes zur Verfügung. AWS nutzt kryptografische Module zur Benutzerauthentifizierung über folgende Zugriffsmethoden: API-Endpunkte, VPC IPSEC VPN, IAM, MFA-Hardware-Token, SSH.

Intern erstellt und verwaltet AWS kryptografische Schlüssel zur Kryptografie, die innerhalb der AWS-Infrastruktur eingesetzt wird. AWS erstellt, steuert und verteilt symmetrische kryptografische Schlüssel mithilfe NIST-zugelassener Schlüsselverwaltungstechnologie und -prozesse im AWS-Informationssystem. Zur Erstellung, zum Schutz und zur Verteilung symmetrischer Schlüssel wird ein von AWS entwickelter Verschlüsselungs- und Anmeldungsmanager verwendet. Damit wird Folgendes gesichert und verteilt: AWS-Anmeldeinformationen, die für Hosts benötigt werden, öffentliche/private RSA-Schlüssel und X.509-Zertifizierungen.

Die kryptografischen Prozesse von AWS werden regelmäßig von unabhängigen Auditoren auf Erfüllung der Anforderungen von SOC, PCI DSS, ISO 27001 und FedRAMP geprüft.

Die Verantwortung der AWS-Kunden

Kunden sind für die Entwicklung, Implementierung und den Betrieb relevanter und für ihre Umgebung angemessene Kryptokonzepte im Einklang mit B 1.7 verantwortlich. AWS gibt Ihnen die Möglichkeit, für nahezu alle Services einschließlich S3, EBS und EC2 Ihren eigenen Verschlüsselungsmechanismus zu verwenden. VPC-Sitzungen sind ebenfalls verschlüsselt. Darüber hinaus können Sie mit dem AWS CloudHSM-Service Ihre Schlüssel zur Datenverschlüsselung innerhalb von HSMs schützen, die für die sichere Schlüsselverwaltung konzipiert und geprüft wurden. Sichere kryptografische Schlüssel für die Datenverschlüsselung lassen sich generieren und verwalten, auf die nur Sie zugreifen können. Dank AWS CloudHSM können Sie strenge Schlüsselverwaltungsanforderungen erfüllen, ohne dafür die Anwendungsleistung zu opfern.

Der AWS CloudHSM-Service wird mit der Amazon Virtual Private Cloud (VPC) zusammen eingesetzt. CloudHSMs werden mit einer von Ihnen angegebenen IP-Adresse in Ihrer VPC bereitgestellt und bieten Ihnen eine problemlose und private Netzwerkkonnektivität mit Ihren Amazon Elastic Compute Cloud (EC2)-Instanzen. Die Platzierung von CloudHSMs in der Nähe Ihrer EC2-Instanzen verringert die Netzwerklatenz. Das kann die Anwendungsleistung erhöhen. AWS bietet Ihnen dedizierten, exklusiven Zugriff auf CloudHSMs. AWS CloudHSMs sind in verschiedenen Regionen und Availability Zones (AZs) verfügbar. Sie können damit Ihren Amazon EC2-Anwendungen eine langfristige und sichere Schlüsselspeicherung hinzufügen.

B 1.8 Behandlung von Sicherheitsvorfällen

AWS hat eine formale, dokumentierte Richtlinie und ein Programm zur Vorfallhandhabung implementiert. Diese Richtlinie beschreibt die Zielsetzung, den Umfang, die Rollen, die Verantwortlichkeiten und das Engagement der Unternehmensleitung. AWS führt außerdem für alle Benutzer des Informationssystems, die AWS unterstützen, Schulungen zur Sicherheitssensibilisierung durch. Diese jährliche Schulung zur Sicherheitssensibilisierung umfasst die folgenden Themen:

- die Zielsetzung der Schulung über Sicherheit und Sensibilisierung,
- die Ablageorte aller AWS-Richtlinien,
- die AWS-Vorfallreaktionsprozesse (einschließlich Anweisungen darüber, wie interne und externe Sicherheitsvorfälle zu berichten sind).

Systeme innerhalb von AWS sind umfassend zur Überwachung von wichtigen Betriebs- und Datensicherheitsmetriken ausgestattet. Alarme sind so konfiguriert, dass sie automatisch das Betriebs- und Verwaltungspersonal benachrichtigen, wenn die Frühwarnschwellen von wichtigen Betriebsmetriken überschritten werden. Wird eine Frühwarnschwelle überschritten, wird der AWS-Vorfallreaktionsprozess gestartet. Das Amazon-Team zur Behebung von Vorfällen wendet branchenübliche diagnostische Verfahren an, um die Behebung unternehmenskritischer Vorfälle zu beschleunigen. Das Betriebspersonal bietet eine kontinuierliche Besetzung rund um die Uhr, sieben Tage die Woche und an 365 Tagen im Jahr, um Störfälle zu erkennen und deren Auswirkungen und Behebung zu verwalten.

AWS nutzt zum Umgang mit Sicherheitsvorfällen einen Drei-Phasen-Ansatz:
1. Aktivierungs- und Benachrichtigungsphase: Ein Vorfall beginnt laut AWS-Definition mit dem Feststellen eines Ereignisses. Die Information kann aus unterschiedlichen Quellen stammen, z. B.:
a. Metriken und Alarme – Probleme werden von AWS extrem schnell ermittelt, da eine Überwachung rund um die Uhr stattfindet und Echtzeit-Metriken sowie Service-Dashboards sofort Alarme auslösen. Die Mehrheit aller Störfälle wird auf diese Weise festgestellt. AWS nutzt Alarme bei frühzeitigen Anzeichen, um Probleme zu erkennen, die letztendlich Auswirkungen auf die Kunden haben können.
b. Durch einen AWS-Mitarbeiter erstelltes Fehlertickets.
c. Anrufe bei der allzeit verfügbaren technischen Support-Hotline.

Erfüllt das Ereignis die Kriterien für einen Vorfall, leitet der relevante Support-Techniker mithilfe des AWS Event Management Tool-Systems die erforderlichen Schritte ein und benachrichtigt die jeweiligen Experten für die Behebung des Problems (z. B. das Sicherheitsteam). Diese analysieren den Vorfall, um zu ermitteln, ob weitere Hilfe benötigt wird und was die wahrscheinliche Ursache des Vorfalls sein könnte.

2. Wiederherstellungsphase – die Verantwortlichen führen eine Break-/Fix-Behebung der Störung durch. Nachdem Fehlersuche, Break/Fix und Feststellung betroffener Komponenten durchgeführt wurden, weist der Verantwortliche die weiteren Schritte hinsichtlich Dokumentation und anderer Maßnahmen entsprechend zu und schließt den Fall ab.

3. Nachbereitungsphase – Sobald die erforderlichen Schritte zur Fehlerbehebung durchgeführt wurden, wird die Wiederherstellungsphase als abgeschlossen erklärt. Nachbesprechungen und umfassende Ursachenforschung werden dem relevanten Team aufgetragen. Die daraus gewonnenen Erkenntnisse werden von den verantwortlichen Führungskräften geprüft und Maßnahmen, die sich daraus ergeben, z. B. Design-Änderungen, werden in einem Correction of Errors-Dokument (COE, Fehlerbehebungsdokument) erfasst und bis zur Durchführung nachverfolgt.

Zusätzlich zu den oben beschriebenen internen Kommunikationsmechanismen hat AWS ebenfalls verschiedene Methoden der externen Kommunikation implementiert, um den Kundenkreis und die Community zu unterstützen. Es wurden Mechanismen eingerichtet, die das Kunden-Support-Team über Betriebsprobleme benachrichtigen, wenn durch diese die Nutzererfahrung der Kunden beeinträchtigt wird. Eine "Übersicht zum Servicestatus" (Service Health Dashboard) steht zur Verfügung, die vom Kunden-Support-Team verwaltet wird und in der Kunden auf Probleme hingewiesen werden, die größere Auswirkungen haben könnten.

Verantwortungsbereich der AWS-Kunden

Kunden sind für die Entwicklung, Implementierung und Ausführung eines Plans für das Sicherheitsmanagement ihrer Umgebung im Einklang mit B 1.8 verantwortlich.

B 1.9 Hard- und Software-Management

Entsprechend den ISO 27001-Standards werden die AWS-Hardware-Komponenten einem Verantwortlichen zugewiesen und von den AWS-Mitarbeitern mithilfe AWS-eigener Bestandsverwaltungstools nachverfolgt und überwacht.

AWS hat die folgende Maßnahmenliste zusammengestellt, um Bedrohungen in der Lieferkette vorzubeugen, welche wiederum die Ressourcen beeinträchtigen könnten.

Agile Beschaffung – Das obere Management von AWS hält eine wöchentliche Besprechung ab, in der festgelegt wird, welche Maßnahmen notwendig sind, um die Geschäftsanforderungen zu erfüllen. Die Einzelposten, die für die Abdeckung der Kapazitätsanforderungen ermittelt wurden, werden in RFQs (Requests for Quotation, Aufforderungen zur Angebotsabgabe) bekanntgegeben und anschließend erworben. Diese häufige Überprüfung der Anforderungen und der daraus erfolgende Angebots- und Akquisitionszyklus führen zu einem wesentlich agileren Akquisitionsprozess, als wenn die Ausgaben für die Einzelposten in einem Jahreszyklus eingeplant werden. Durch diesen Prozess ist es AWS möglich, schnell auf Geschäftsanforderungen zu reagieren.

Einzelverträge – Die wöchentlichen Gespräche und häufigen RFQs erlauben eine größere Anzahl kleinerer Verträge, die bei Bedarf erneuert werden. Falls ein Anbieter aus welchem Grund auch immer nicht in der Lage ist, die Lieferung auszuführen, sind die Auswirkungen gering und für die Beschaffung kann leicht eine neue Quelle gefunden werden.

Verwendung anerkannter, etablierter, diversifizierter Lieferanten – Dem Eingehen vertraglicher Vereinbarungen, um Hardware, Software, Firmware oder Services zu erwerben, muss eine Unternehmensprüfung (Due Diligence) der Lieferanten vorausgehen.

Mehrere Anbieter – Eine Liste zugelassener Anbieter wird vom AWS-Team geführt, jeweils mit mehreren Anbietern zur Auswahl für jeden Komponententyp. Sollte ein Lieferant außerstande sein, die Lieferung auszuführen, kann ein anderer Anbieter für die nächsten Beschaffungsvorgänge verwendet werden.

Obwohl ein Großteil des AWS-Systems unternehmensintern entwickelt wurde, um den besonderen AWS-Anforderungen gerecht zu werden, verwendet AWS soweit wie möglich auch standardmäßige, kommerziell erhältliche Informationssystemkonfigurationen und reduziert so die Möglichkeit, Systeme und Produkte zu erwerben, die während der Lieferkettenvorgänge beschädigt wurden.

Alle neuen Informationssystemkomponenten für AWS-Rechenzentren erfordern Autorisierung durch die und Benachrichtigung der Rechenzentrumsleitung. Dazu zählen unter anderem Server, Racks, Netzwerkgeräte, Festplatten, Systemhardware-Komponenten und Baustoffe, die an Rechenzentren geliefert und von Rechenzentren in Empfang genommen werden. Die Artikel werden an die Laderampe der einzelnen AWS-Rechenzentren geliefert und dort auf Beschädigungen an Artikel oder Verpackung geprüft sowie von einem Vollzeitmitarbeiter von AWS gegengezeichnet. Jede Lieferung wird gescannt und in das Komponentenverwaltungs- und Inventarsystem von AWS aufgenommen.

Eingegangene Artikel werden vor der endgültigen Installation im Rechenzentrum zunächst in einem Lagerraum innerhalb des Rechenzentrums gelagert, zu dem der Zugang nur über Magnetstreifenkarte und PIN-Eingabe möglich ist. Bevor Artikel das Rechenzentrum verlassen können, werden sie gescannt, dokumentiert und bereinigt.

Wenn die Lebensdauer eines Speichergeräts zu Ende geht, führt AWS einen Prozess zur Außerbetriebnahme durch, der entwickelt wurde, damit Kundendaten nicht an unautorisierte Personen offengelegt werden. AWS wendet die in DoD 5220.22-M ("Betriebshandbuch zum nationalen Branchensicherheitsprogramm") oder NIST 800-88 ("Richtlinien zur Medienbereinigung") beschriebenen Techniken an, um Daten im Rahmen des Prozesses zur Außerbetriebnahme zu zerstören. Wenn ein Hardware-Gerät nicht mithilfe dieser Prozesse außer Betrieb genommen werden kann, dann wird das Gerät entmagnetisiert und physisch den branchenüblichen Vorgehensweisen entsprechend zerstört. Weitere Informationen finden Sie im AWS-Whitepaper "Übersicht über die Sicherheitsprozesse" unter http://aws.amazon.com/security.

AWS hat für alle Systeme und Geräte innerhalb des AWS-Systems auditierbare Ereigniskategorien ermittelt. Service-Teams konfigurieren die Auditfunktionen so, dass sicherheitsrelevante Ereignisse fortlaufend gemäß den Anforderungen aufgezeichnet werden. Das Protokollspeichersystem ist dafür ausgelegt, einen hoch skalierbaren und hoch verfügbaren Service zu bieten, dessen Kapazität bei steigendem Protokollspeicherbedarf automatisch erweitert wird. Die Auditdaten enthalten eine Gruppe von Datenelementen, die die erforderlichen Analyseanforderungen unterstützen. Zusätzlich stehen sie dem AWS-Sicherheitsteam oder anderen relevanten Teams bei Bedarf zur Prüfung oder Analyse und für die Behebung sicherheitsrelevanter oder geschäftsschädigender Ereignisse zur Verfügung.

Mitarbeiter des AWS-Teams erhalten automatisierte Benachrichtigungen, wenn Fehler in überwachten Prozessen auftreten. Dazu gehören unter anderem Software- oder Hardwarefehler. Nach Erhalt einer Fehlermeldung stellen die benachrichtigten Mitarbeiter ein Fehlerticket aus und behandeln das Problem, bis es gelöst ist.

Der AWS-SOC 1-Typ II-Bericht bietet einen Überblick der zur Änderungsverwaltung in der physischen und logischen AWS-Umgebung verfügbaren Kontrollen. Bei jeder Änderung, die in den Systemen und Geräten innerhalb des AWS-Systems vorgenommen wird, wird ein Change Management-Ticket (CM, Änderungsverwaltung) erstellt. In diesem CM-Ticket werden alle Details der Änderung festgehalten. Dazu gehören eine Beschreibung der Änderung, Auswirkungsanalyse, ggf. Sicherheitsüberlegungen, Änderungszeitraum und erforderliche Genehmigungen.

AWS hat formale Richtlinien und Verfahren gemäß ISO 27001 erstellt, um Mindeststandards für den logischen Zugriff auf die AWS-Ressourcen festzulegen. Der Bericht AWS-SOC 1-Typ II und SOC 2-Typ II beschreibt die vorhandenen Kontrollen, um die Zugriffsberechtigungen von AWS-Ressourcen zu verwalten. Das AWS-Produktionsnetzwerk ist vom Amazon-Unternehmensnetzwerk getrennt und erfordert separate Anmeldeinformationen für den logischen Zugriff. Das Amazon-Unternehmensnetzwerk verwendet Benutzer-IDs, Passwörter und Kerberos, während das AWS-Produktionsnetzwerk eine Authentifizierung mit einem öffentlichen SSH-Schlüssel durch einen Bastion-Host erfordert. AWS-Entwickler und Administratoren des Amazon-Unternehmensnetzwerks, die Zugriff auf die AWS-Cloud-Komponenten benötigen, müssen ausdrücklich eine Anforderung auf Zugriff über das AWS-Zugriffsverwaltungssystem stellen. Alle Anforderungen werden vom entsprechenden Verantwortlichen oder Manager überprüft und genehmigt. Konten werden alle 90 Tage überprüft; es ist eine ausdrückliche erneute Überprüfung erforderlich oder der Zugriff auf die Ressource wird automatisch widerrufen. Der Zugriff wird ebenfalls automatisch widerrufen, wenn ein Mitarbeiterdatensatz im Personalverwaltungssystem von Amazon geschlossen wird. Windows- und UNIX-Konten werden deaktiviert und das Zugriffsverwaltungssystem von Amazon entfernt den Benutzer aus allen Systemen. Anforderungen für Zugriffsänderungen werden im Auditprotokoll des Zugriffsverwaltungssystem von Amazon erfasst. Wenn sich die Funktion eines Mitarbeiters ändert, muss der kontinuierliche Zugriff ausdrücklich in der Ressource genehmigt werden, da dieser sonst automatisch widerrufen wird.

Die Verantwortung der AWS-Kunden

Kunden sind für die Entwicklung, Implementierung und den Betrieb einer angemessenen Hardware- und Softwarestrategie für ihre Umgebung im Einklang mit B 1.9 verantwortlich.

M 1.13 Sensibilisierung und Schulung zur Informationssicherheit

Die Kontrollumgebung beginnt bei Amazon auf höchster Unternehmensebene. Die Geschäftsführung sowie die Führungskräfte des oberen Managements spielen bei der Festlegung der Grundwerte des Unternehmens eine entscheidende Rolle.

AWS führt für alle Benutzer des Informationssystems, die AWS unterstützen, Schulungen zur Sensibilisierung durch. Diese jährliche Schulung zur Sicherheitssensibilisierung umfasst die folgenden Themen: Zielsetzung der Schulung über Sicherheit und Sensibilisierung, Ablageorte aller AWS-Richtlinien, AWS-Vorfallreaktionsprozesse (einschließlich Anweisungen darüber, wie interne und externe Sicherheitsvorfälle zu berichten sind).

Die AWS-Richtlinien, Prozesse und relevanten Schulungsprogramme werden von unabhängigen, externen Auditoren während der Prüfungen bezüglich der Compliance mit SOC, PCI DSS, ISO 27001 und FedRAMP überprüft.

Die Verantwortung der AWS-Kunden

Die Kunden sind für die Entwicklung, Implementierung und den Durchführung eines geeigneten Programms für die Sensibilisierung und Schulung zur Informationssicherheit verantwortlich. Dieses Programm muss ihrer Umgebung angepasst sein und mit M 1.13 im Einklang stehen.

M 1.14 Patch- und Änderungsmanagement

AWS hat eine formale, dokumentierte Richtlinie zur Konfigurationsverwaltung implementiert. Diese Richtlinie beschreibt die Zielsetzung, den Umfang, die Rollen, die Verantwortlichkeiten und das Engagement der Unternehmensleitung im Hinblick auf die Konfigurations- und Änderungsverwaltung. Bei jeder Änderung, die an den Systemen und Geräten vorgenommen wird, wird ein Change Management-Ticket (CM, Änderungsverwaltung) erstellt. In diesem CM-Ticket werden alle Details der Änderung festgehalten. Dazu gehören eine Beschreibung der Änderung, Auswirkungsanalyse, ggf. Sicherheitsüberlegungen, Änderungszeitraum und erforderliche Genehmigungen. Der Änderungsverwaltungsprozess wird von externen Dritten während der Tests für AWS SOC, PCI DSS, ISO 27001 und FedRAMP überprüft und bewertet.

AWS ist für das Patchen von Systemen verantwortlich, die das Erbringen des Services für die Kunden unterstützen, wie zum Beispiel die Hypervisoren und Netzwerkdienste. Dies wird entsprechend den AWS-Richtlinien und gemäß den Anforderungen von ISO 27001, NIST und PCI durchgeführt. Die Kunden kontrollieren ihre eigenen Gastbetriebssysteme, -software und -anwendungen und sind aus diesem Grund dafür verantwortlich, ihre eigenen Systeme zu patchen. AWS erfordert kein Abschalten der Systeme, um regelmäßige Wartungsarbeiten und Patch-Vorgänge am System durchzuführen. Die eigenen Wartungsarbeiten und Patch-Vorgänge von AWS bringen in der Regel keine Beeinträchtigungen für die Kunden mit sich. Die Wartung der Instanzen selbst wird vom Kunden kontrolliert.

AWS implementiert das Prinzip der geringsten Rechte innerhalb der Infrastrukturkomponenten. AWS unterbindet die Verwendung aller Ports und Protokolle, die keinen speziellen geschäftlichen Zweck erfüllen. AWS verfolgt konsequent den Ansatz der minimalen Implementierung außerschließlich der Merkmale und Funktionen, die für die Verwendung des Geräts notwendig sind. Netzwerkscans werden durchgeführt und unnötige Ports oder Protokolle deaktiviert.

Es werden regelmäßig mit verschiedenen Tools interne und externe Schwachstellen-Scans auf dem Host-Betriebssystem, der Webanwendung und den Datenbanken in der AWS-Umgebung vollzogen. Die Schwachstellen-Scans und Wiederherstellungsverfahren von AWS werden regelmäßig auf die Erfüllung der Anforderungen mit PCI DSS und FedRAMP geprüft.

Das Amazon-Team für Informationssicherheit und die AWS-Sicherheitsteams abonnieren des Weiteren Newsfeeds zu den entsprechenden Anbieterfehlern von Secunia und TELUS Security Labs. Das Amazon-Team für Informationssicherheit überwacht proaktiv die Websites der Anbieter und andere relevante Quellen für neue Patches. Vor der Implementierung werden die Patches hinsichtlich ihrer Auswirkungen auf die Sicherheit und den Geschäftsbetrieb bewertet und entsprechend der Bewertung zeitgerecht angewendet.

Die Verantwortung der AWS-Kunden

Die Kunden sind für die Entwicklung, Implementierung und die Durchführung eines Programms für das Änderungsmanagement und die Patch-Vorgänge verantwortlich. Dieses Programm muss ihrer Umgebung angepasst sein und mit M 1.14 im Einklang stehen.

Die Kunden kontrollieren ihre eigenen Gastbetriebssysteme, -software und -anwendungen und sind aus diesem Grund dafür verantwortlich, ihre eigenen Schwachstellen-Scans durchzuführen und ihre eigenen Systeme zu patchen. Kunden können eine Genehmigung zur Durchführung von Scans ihrer Cloud-Infrastruktur anfordern, solange diese sich auf die Instanzen des Kunden beschränken und nicht gegen die Acceptable Use Policy von AWS verstoßen.

M 1.16 Compliance-Management

AWS hat Richtlinien zur Zertifizierung, Autorisierung und Sicherheitsbewertung erarbeitet, die die Zielsetzung, den Umfang, die Rollen, die Verantwortlichkeiten und das Engagement der Unternehmensleitung in Bezug darauf festlegt, wie AWS die Ausrichtung an durch Dritte geprüften Zertifizierungen/Akkreditierungen verwaltet, überwacht und kommuniziert. Das AWS Security Assurance-Team ist damit beauftragt, die Compliance-Frameworks einzuführen, zu verwalten, zu überwachen und zu bewerten. Dazu gehört auch die Verwaltung der Prüfgegenstände wie Dokumentationen zur Systemsicherheit, Prüfgegenstände, Prüfungsergebnisse und Abhilfemaßnahmen. AWS arbeitet mit externen Zertifizierungsstellen und unabhängigen Auditoren zusammen, um unsere Compliance mit allen Compliance-Frameworks im gesamten System zu überprüfen und zu validieren.

Kunden behalten bei Nutzung der AWS-Dienste die wirksame Kontrolle über ihre eigenen Inhalte und sind nicht davon entbunden. Kunden kontrollieren ihre eigenen Inhalte ab dem Zeitpunkt der Erstellung. Kunden können:

- festlegen, wo die Inhalte gespeichert werden, zum Beispiel die Speicherart und an welchem geografischen Standort die Speicherung erfolgen soll
- das Format der Inhalte kontrollieren, zum Beispiel Nur-Text, maskiert, anonymisiert oder verschlüsselt
- andere Zugriffskontrollen verwalten, wie Identitätsmanagement und Sicherheitsanmeldeinformationen

Auf diese Weise können die AWS-Kunden den gesamten Lebenszyklus ihrer Inhalte auf AWS kontrollieren und die Inhalte ihren speziellen Bedürfnissen entsprechend verwalten, einschließlich der Klassifizierung der Inhalte, Zugriffskontrolle, Aufbewahrung und Vernichtung.

AWS verfügt über eine etablierte Informationssicherheits-Organisation, die durch das AWS-Sicherheitsteam gemanagt und durch den AWS Chief Information Security Officer (CISO, Beauftragter für die zentrale IT-Sicherheit) geleitet wird. AWS führt für alle Benutzer des Informationssystems, die AWS unterstützen, Schulungen zur Sensibilisierung durch. Diese jährliche Schulung zur Sicherheitssensibilisierung umfasst die folgenden Themen: Zielsetzung der Schulung über Sicherheit und Sensibilisierung, Ablageorte aller AWS-Richtlinien, AWS-Vorfallreaktionsprozesse (einschließlich Anweisungen darüber, wie interne und externe Sicherheitsvorfälle zu berichten sind).

Die Verantwortung der AWS-Kunden

Die AWS-Kunden sind für die Entwicklung, Implementierung und Durchführung eines Compliance-Programms verantwortlich. Dieses Programm muss ihrer Umgebung angepasst sein und mit den M 16-Anforderungen im Einklang stehen.

Die AWS-Kunden sind weiterhin dafür verantwortlich, dass ihre AWS-Nutzung den geltenden Gesetzen und Vorschriften entspricht. AWS unterrichtet seine Kunden über die Sicherheits- und Kontrollumgebung anhand von branchenüblichen Zertifizierungen und Bestätigungen durch unabhängige Dritte, durch Whitepapers (erhältlich unter http://aws.amazon.com/compliance) sowie durch die direkte Bereitstellung von Zertifizierungen, Berichten und anderen geeigneten Dokumenten.

M 2.0 Allgemeines Gebäude

AWS-Rechenzentren sind in unauffälligen Anlagen untergebracht und sind nicht für die Öffentlichkeit zugänglich. Die AWS-Rechenzentren sind mit physischen Schutzmaßnahmen gegen Umweltrisiken ausgerüstet. Die von AWS implementierten physischen Schutzmaßnahmen gegen Umweltrisiken wurden von einem unabhängigen Auditor geprüft und es wurde zertifiziert, dass sie mit den in ISO 27002 aufgelisteten bewährten Methoden übereinstimmen. Die Rechenzentren verfügen über Branderkennungs- und Brandbekämpfungsmechanismen. Die Branderkennungs- sowie Brandbekämpfungssysteme in den Rechenzentren bestehen aus Feuerlöschgeräten und VESDA-Rauchmeldern (Very Early Smoke Detection Apparatus, Brandfrühwarnsysteme). Die Branderkennungs- und Brandbekämpfungssysteme werden im Fall eines Stromausfalls durch eine unabhängige Notstromversorgung gespeist. Sollte ein Brandbekämpfungssystem eingesetzt werden, verfügt AWS über die notwendigen Kapazitäten, um den Betrieb in ein anderes Rechenzentrum umzuleiten. Die Verfahren, die bei der Schließung eines Rechenzentrums zur Anwendung kommen, umfassen auch ausführliche Informationen darüber, wie ein Rechenzentrum zu schließen und der Verkehr zu einem anderen Rechenzentrumcluster oder einer anderen Region umzuleiten ist. AWS verwendet für das Informationssystem Branderkennungsgeräte/-systeme, die automatisch aktiviert werden und im Falle eines Feuers die Organisation und die Notfall-Einsatzkräfte benachrichtigen.

AWS-Rechenzentren werden gruppenweise in verschiedenen Regionen der Welt errichtet. Alle Rechenzentren sind online und bedienen Kunden; kein Rechenzentrum ist abgeschaltet. Bei einem Ausfall verschieben automatische Prozesse den Kundendatenverkehr weg von den betroffenen Bereichen. Die Kernanwendungen werden in einer N+1-Konfiguration bereitgestellt, sodass im Falle eines Rechenzentrumsausfalls ausreichend Kapazität vorhanden ist, um den Datenverkehr lastverteilt an die verbleibenden Standorte zu verteilen. AWS bietet Kunden die Flexibilität, Instanzen zu platzieren und Daten innerhalb mehrerer geografischer Regionen sowie über mehrere Availability Zones innerhalb der einzelnen Regionen zu speichern. Jede Availability Zone wurde als unabhängige Ausfallszone entwickelt. Dies bedeutet, dass Availability Zones innerhalb einer typischen Stadtregion physisch verteilt sind und sich in Gebieten mit niedrigerem Überschwemmungsrisiko befinden (je nach Region gibt es unterschiedliche Überschwemmungszonenkategorisierungen). Zusätzlich zu einer eigenständigen unterbrechungsfreien Stromversorgung und Notstromgeneratoren vor Ort werden alle Availability Zones über unterschiedliche Stromnetze von unabhängigen Stromversorgern gespeist, um Einzelfehlerstellen zu minimieren. Sämtliche Availability Zones sind redundant mit mehreren Tier-1-Transit-Providern verbunden. Kunden sollten die Architektur ihrer AWS-Nutzung so erstellen, dass sie mehrere Regionen und Availability Zones umfasst. Durch das Verteilen von Anwendungen über mehrere Availability Zones bleibt die Architektur bei den meisten Ausfallarten, einschließlich Naturkatastrophen oder Systemausfällen, stabil.

Der physische Zugang zu den Rechenzentren wird durch das elektronische AWS-Zugangskontrollsystem überwacht. Für den Zugang in das Gebäude und die Räume setzt sich das System aus Kartenlesern und PIN-Pads zusammen, für das Verlassen besteht es nur aus Kartenlesern. Durch die Verwendung von Kartenlesern beim Verlassen von Gebäuden und Räumen treten Doppelzutrittssperren in Kraft, die sicherstellen, dass autorisierte Personen nicht von unautorisierten Personen verfolgt werden, die sich so ohne Ausweis Zutritt verschaffen. Zusätzlich zum Zugangskontrollsystem sind alle Eingänge der AWS-Rechenzentren, einschließlich des Haupteingangs, der Laderampe und aller Dachausstiege/-luken, mit Einbruchmeldevorrichtungen versehen, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird. Neben den elektronischen Mechanismen verwenden die AWS-Rechenzentren rund um die Uhr auch ausgebildete Sicherheitskräfte, die sowohl innerhalb der Gebäude als auch in deren Umgebung stationiert sind. Innerhalb des Systems wird der Zugang zu den Rechenzentren nur nach Notwendigkeit erteilt; alle physischen Zugangsanfragen werden vom zuständigen AAM (Area Access Manager, Zugangsmanager) überprüft und genehmigt. AWS-Rechenzentren sind in unauffälligen Anlagen untergebracht und sind nicht für die Öffentlichkeit zugänglich. Der physische Zugang wird sowohl in der Umgebung als auch an den Zutrittspunkten zum Gebäude streng kontrolliert. AWS gewährt nur solchen Anbietern, Auftragnehmern und Besuchern Zugang und Informationen zu den Rechenzentren, für die eine legitime geschäftliche Notwendigkeit besteht, wie Notfallreparaturen. Alle Besucher der Rechenzentren müssen vorab durch den zuständigen Zugangsmanager (AAM) autorisiert worden sein und im AWS-Ticketmanagementsystem dokumentiert werden. Bei der Ankunft am Rechenzentrum müssen sie sich ausweisen und anmelden, bevor ihnen ein Besucherausweis ausgestellt wird. Während sie sich im Rechenzentrum befinden, werden sie beständig von autorisiertem Personal begleitet.

Weitere Informationen finden Sie in den Berichten AWS SOC 1-Typ II und SOC 2-Typ II – Sicherheit. Außerdem enthält ISO 27001, Anhang A.11.2, zusätzliche Informationen. AWS wurde durch einen unabhängigen Auditor auf Erfüllung der ISO 27001-Zertifizierungsanforderungen geprüft.

Die Verantwortung der AWS-Kunden

Die AWS-Kunden sind dafür verantwortlich, dass alle Gebäude, die Komponenten außerhalb der AWS-Umgebung beherbergen, die in M 2.0 dokumentierten Sicherheitsmaßnahmen erwägen.

M 2.1 Elektrotechnische Verkabelung

Die internen AWS-Verkabelungsverfahren regeln wie AWS die Verkabelungsanforderungen kategorisiert, implementiert und verwaltet.

AWS-Komponentenkennzeichnungen sind kundenunabhängig und dienen der Inventarisierung der Hardware innerhalb des AWS-Tools zur Komponentenverwaltung. In den AWS-Rechenzentren wird die Hardware normalerweise nicht physisch speziellen Kunden oder den auf der Hardware gespeicherten Daten zugeordnet. Alle Kundendaten werden unabhängig von ihrer Quelle als kritisch angesehen und aus diesem Grund werden alle Medien vertraulich behandelt.

Die Prozesse und Vorgänge der AWS-Komponentenverwaltung werden von unabhängigen, externen Auditoren während der Prüfungen bezüglich der Compliance mit PCI DSS, ISO 27001 und FedRAMP überprüft.

Die Verantwortung der AWS-Kunden

Die AWS-Kunden sind dafür verantwortlich sicherzustellen, dass alle Verkabelungen in Gebäuden, in denen Komponenten außerhalb der AWS-Umgebung untergebracht sind, die in M 2.1 dokumentierten Sicherheitsmaßnahmen erwägen.

M 3.20 Allgemeiner Client

AWS hat eine formale, dokumentierte Richtlinie zur Konfigurationsverwaltung implementiert. Diese Richtlinie beschreibt die Zielsetzung, den Umfang, die Rollen, die Verantwortlichkeiten und das Engagement der Unternehmensleitung.

Ein Konfigurationsverwaltungs-Tool wird zur Verwaltung von bereitstellbarer Software in Paketen, Paketgruppen und Umgebungen verwendet. Bei einem Paket handelt es sich um eine Sammlung zusammenhängender Dateien, z. B. eng miteinander verknüpfte Software oder verknüpfter Content. Mehrere Pakete, die oft gemeinsam bereitgestellt werden, werden als Paketgruppe bezeichnet. Eine Umgebung schließlich ist eine Kombination von Paketen und Paketgruppen, die in einer Gruppe von Hostklassen (Hosts oder Servern mit derselben Funktion) bereitgestellt werden. Eine Umgebung stellt die Gesamtheit aller Pakete dar, die zur Ausführung einer bestimmten Funktion durch den Server erforderlich sind.

AWS sorgt für die die Verteilung des Basis-OS, das auf den Hosts verwendet wird. Ports, Protokolle und Services, die nicht benötigt werden, sind in den Basis-Builds deaktiviert. Mithilfe der Build-Tools fügen die Serviceteams nur die zugelassenen Softwarepakete hinzu, die zur Serverfunktion gemäß den Basiskonfigurationen notwendig sind. Die Server werden regelmäßig gescannt und unnötige Ports oder Protokolle werden mithilfe des Nachbesserungsprozesses behoben. Bereitgestellte Software durchläuft wiederholte Penetrationstests, die durch ausgewählte Branchenexperten ausgeführt werden. Die aus den jährlichen Penetrationstests resultierenden Nachbesserungen werden über den Nachbesserungsprozess ebenfalls in die Basiskonfiguration aufgenommen.

AWS implementiert das Prinzip der geringsten Rechte innerhalb der Infrastrukturkomponenten. AWS unterbindet die Verwendung aller Ports und Protokolle, die keinen speziellen geschäftlichen Zweck erfüllen. AWS verfolgt konsequent den Ansatz der minimalen Implementierung ausschließlich der Merkmale und Funktionen, die für die Verwendung des Geräts notwendig sind. Es werden Netzwerk-Scans durchgeführt und unnötige Ports oder Protokolle deaktiviert.

Administratoren, die aus geschäftlichen Gründen Zugriff auf die Verwaltungsebene benötigen, müssen die Multi-Factor Authentication verwenden, um Zugriff auf speziell erstellte administrative Hosts zu erhalten. Diese administrativen Hosts sind Systeme, die speziell zum Schutz der Verwaltungsebene der Cloud entwickelt, erstellt, konfiguriert und gehärtet wurden. Jeder Zugriff wird protokolliert und geprüft. Sobald für einen Mitarbeiter keine geschäftliche Notwendigkeit mehr für den Zugriff auf die Verwaltungsebene besteht, werden die Privilegien und die Zugriffsberechtigung für diese Hosts und relevante Systeme widerrufen.

Die Verantwortung der AWS-Kunden

Die AWS-Kunden sind dafür verantwortlich, dass Server entsprechend den Vorgaben in M 3.20 gesichert sind.

M 3.301 Sicherheitsgateway (Firewall)

Überwachungsgeräte für Netzwerkgrenzen (Boundary Protection Devices) wenden Regelsätze, Zugriffskontrolllisten (ACL, Access Control Lists) und Konfigurationen an, um den Informationsfluss zwischen Netzwerk-Fabrics sicherzustellen.

Bei Amazon gibt es etliche Netzwerk-Fabrics. Diese werden jeweils durch Geräte voneinander abgegrenzt, die den Informationsfluss zwischen den Fabrics steuern. Der Informationsfluss zwischen Fabrice wird durch geprüfte Autorisierungsmechanismen gesteuert. Es handelt sich dabei um Zugriffskontrolllisten (ACL, Access Control Lists), die auf diesen Geräten implementiert sind. Diese Geräte steuern den Informationsfluss zwischen Fabrics anhand der ACLs. ACLs werden mithilfe des ACL-Manage-Tools von AWS definiert, geprüft (von geeigneten Mitarbeitern), verwaltet und bereitgestellt.

Amazon Information Security überprüft diese ACLs. Der Informationsfluss zwischen Fabrics wird durch bewährte Firewall-Regeln und geprüfte ACLs auf spezifische Informationssystem-Services beschränkt. Die Zugriffskontrolllisten und Regelsätze werden überprüft, genehmigt und in regelmäßigen Abständen (mindestens alle 24 Stunden) den Boundary Protection Devices zugewiesen, um sicherzustellen, dass Regelsätze und Zugriffskontrolllisten auf dem neusten Stand sind.

AWS Network Management wird regelmäßig von unabhängigen Auditoren auf Erfüllung der Anforderungen von SOC, PCI DSS, ISO 27001 und FedRAMP geprüft.

AWS implementiert das Prinzip der geringsten Rechte innerhalb der Infrastrukturkomponenten. AWS unterbindet die Verwendung aller Ports und Protokolle, die keinen speziellen geschäftlichen Zweck erfüllen. AWS verfolgt konsequent den Ansatz der minimalen Implementierung ausschließlich der Merkmale und Funktionen, die für die Verwendung des Geräts notwendig sind. Es werden Netzwerk-Scans durchgeführt und unnötige Ports oder Protokolle deaktiviert.

In Übereinstimmung mit ISO 27001-Standards verwenden AWS-Informationssysteme interne, über NTP (Network Time Protocol) synchronisierte Systemuhren.

Es werden regelmäßig interne und externe Schwachstellen-Scans mit verschiedenen Tools auf dem Host-Betriebssystem, der Web-Anwendung und den Datenbanken in der AWS-Umgebung durchgeführt. Die Schwachstellen-Scans und Wiederherstellungsverfahren von AWS werden regelmäßig auf die Erfüllung der Anforderungen mit PCI DSS und FedRAMP geprüft.

Das AWS-Netzwerk bietet hohen Schutz vor gängigen Netzwerksicherheitsproblemen. Zudem können Benutzer weitere Schutzmaßnahmen implementieren. Weitere Informationen finden Sie im AWS-Whitepaper "Sicherheitsprozesse im Überblick" unter http://aws.amazon.com/security.

Die Verantwortung der AWS-Kunden

Die AWS-Kunden sind dafür verantwortlich, dass Netzwerke entsprechend den Vorgaben in M 3.301 gesichert sind.

M 3.302 Router und Switches

AWS-Systeme befinden sich in einem Sicherheitsbereich innerhalb von AWS-gesteuerten Rechenzentren. Der Zugriff auf diese Systeme ist nur über SSH und Multi-Factor Authentication möglich. AWS verwendet Bastion-Hosts, um den Zugriff auf Netzwerkgeräte und andere Komponenten der Infrastruktur zu beschränken. Zusätzlich zu den Bastion-Hosts enthalten alle Netzwerkgeräte ACLs, und ein SSH-Zugriff ist nur auf Netzwerkgeräte bestimmter Bastion-Hosts möglich.

AWS isoliert Netzwerke logisch mithilfe von Boundary Devices, die ein- und ausgehende Kommunikation auf einen autorisierten Verkehrsfluss begrenzen.

AWS isoliert Informationssicherheits-Tools, Sicherheitsmechanismen und Unterstützungskomponenten von anderen internen Komponenten des Informationssystems über logisch getrennte Teilnetze, die von den Instanzen und dem Datenverkehr des Kunden getrennt sind. Alle Hosts, die Informationssicherheits-Tools, Sicherheitsmechanismen und Unterstützungskomponenten enthalten, gehören zu separaten Sicherheits-Host-Klassen, die Zugriffs- und andere Berechtigungen auf Sicherheits-Hosts von denen auf andere Arten von Produktions-Servern isolieren. Der Zugriffs und die Berechtigungen auf Sicherheit-Hosts werden vom AWS-Sicherheitsteam strikt überwacht.

AWS verfügt nur über eine begrenzte Anzahl von Zugriffspunkten auf das Informationssystem, um eine möglichst umfassende Überwachung des eingehenden und ausgehenden Netzwerkverkehrs und der Kommunikation zu ermöglichen. Diese Zugriffspunkte für Kunden werden API-Endpunkte genannt. Sie ermöglichen dem Kunden den Aufbau sicherer Kommunikationssitzungen mit ihren Speicher- oder Datenverarbeitungs-Instanzen innerhalb von AWS. In diesen Zugriffspunkten wird der eingehende und ausgehende Datenverkehr überwacht, um die Service-Verfügbarkeit sicherzustellen.

AWS hat Netzwerkgeräte implementiert, die für die Verwaltung der Schnittstellenkommunikation mit Internetdienstanbietern (Internet Service Provider, ISPs) vorgesehen sind. AWS verwendet eine redundante Verbindung zu mehr als einem Kommunikations-Service an jeder mit dem Internet verbundenen Stelle des AWS-Netzwerks. Jede dieser Verbindungen verfügt über eigene Netzwerkgeräte.

Die nachstehend aufgeführten Sicherheitskontrollen dienen zum Schutz der Vertraulichkeit und Integrität der übertragenen Informationen. Diese Sicherheitskontrollen werden all 6 Monate auf operative Wirksamkeit hin überprüft.

- Firewall-Geräte sind so konfiguriert, dass sie den Zugriff auf die Computerumgebung beschränken und die Abgrenzung der Computing-Cluster verstärken.
- Firewall-Richtlinien (Konfigurationsdateien) werden automatisch alle 24 Stunden in das Netzwerk übertragen.
- Die Aktualisierungen der Firewall-Richtlinien werden überprüft und genehmigt.
- Netzwerkgeräte werden von AWS so konfiguriert, dass ein Zugriff nur auf bestimmte Ports auf anderen Systemen innerhalb von AWS möglich ist.

AWS hat eine Konfigurationsverwaltung entwickelt und dokumentiert. AWS implementiert den AWS Configuration Management-Plan für Systeme und Geräte innerhalb der AWS- Systemgrenze. Der AWS Configuration Management-Plan beschreibt die Rollen, die Verantwortlichkeiten sowie die Prozesse und Prozeduren der Konfigurationsverwaltung. Der AWS CM-Plan definiert detailliert das Verfahren zur Verwaltung der Konfigurationselemente von Produktionssystemen. AWS identifiziert Konfigurationselemente nach einer Änderung bezüglich System, Service, DB-Schema oder Umgebung, die Einfluss auf ein anderes Team, Service oder Website haben kann, oder wenn andere Gruppen innerhalb von AWS die Änderung kennen müssen. Zu solchen Änderungen gehören Modifikationen an Konfigurationseinstellungen, Paketen, Paketgruppen oder Umgebungen auf Systemen oder Geräten innerhalb der Systemgrenze. Alle Änderungsarten werden im AWS Configuration Management-Plan berücksichtigt.

Die Verantwortung der AWS-Kunden

Die AWS-Kunden sind entsprechend M 3.302 für die Sicherung von Routern und Switches verantwortlich, die außerhalb ihrer AWS-Umgebung verwendet werden.

M 3.304 Virtualisierung

AWS verwendet Virtualisierungstechniken zur Bereitstellung von Informationssystemkomponenten anstelle anderer Arten von Komponenten oder von Komponenten mit unterschiedlichen Konfigurationen. Dazu gehören virtuelle Netzwerkgeräte und Host-basierte Firewalls, die Verkehrsflusseinschränkungen über ACLs in EC2 und VPC steuern (und in EC2-Instanzen, die eine Vielzahl von Betriebssystemen umfassen).

Wo virtuelle Compute-Instanzen mehrerer Kunden auf einem Host vorhanden sind, werden Systemressourcen für jeden Kunden entsprechend seiner ursprünglichen Einrichtung zugeordnet. Die Zuordnung von Systemressourcen erfolgt mittels Virtualisierungssoftware, wobei der Umfang der Systemressourcen, die jeden Kunden zugewiesen werden, abhängig ist von den Parametern, die der Kunde bei der ursprünglichen Einrichtung der Systemressourcen verwendet hat. Ein zentraler Region-by-Region-Server ermöglicht Aggregation und Verkehrslenkung pro Kunde. Wenn ein Kunde so viele Netzwerkgeräte belegt, dass dies Auswirkungen auf andere Kunden hat, drosselt AWS den Netzwerkverkehr dieses Kunden. Der Service überwacht und aggregiert Daten pro Minute. Die Drossel wird jede Minute zurückgesetzt, bis der Durchsatz wieder einen akzeptablen Wert erreicht.

Die Verantwortung der AWS-Kunden

Die AWS-Kunden sind für die Verwaltung von virtuellen Hosts, Speicher und Anwendungen verantwortlich. Sie müssen sicherstellen, dass geeignete Prozesse gemäß M 3.304 ausgeführt werden.

M 4.42 Netz- und Systemverwaltung

AWS-Systeme befinden sich in einem Sicherheitsbereich innerhalb von AWS-gesteuerten Rechenzentren. Der Zugriff auf diese Systeme ist nur über SSH und Multi-Factor Authentication möglich. AWS verwendet Bastion-Hosts, um den Zugriff auf Netzwerkgeräte und andere Komponenten der Infrastruktur zu beschränken. Zusätzlich zu den Bastion-Hosts enthalten alle Netzwerkgeräte ACLs, und ein SSH-Zugriff ist nur auf Netzwerkgeräte bestimmter Bastion-Hosts möglich.

AWS isoliert Netzwerke logisch mithilfe von Boundary Devices, die ein- und ausgehende Kommunikation auf einen autorisierten Verkehrsfluss begrenzen.

AWS isoliert Informationssicherheits-Tools, Sicherheitsmechanismen und Unterstützungskomponenten von anderen internen Komponenten des Informationssystems über logisch getrennte Teilnetze, die von den Instanzen und dem Datenverkehr des Kunden getrennt sind. Alle Hosts, die Informationssicherheits-Tools, Sicherheitsmechanismen und Unterstützungskomponenten enthalten, gehören zu separaten Sicherheits-Host-Klassen, die Zugriffs- und andere Berechtigungen auf Sicherheits-Hosts von denen auf andere Arten von Produktions-Servern isolieren. Der Zugriffs und die Berechtigungen auf Sicherheit-Hosts werden vom AWS-Sicherheitsteam strikt überwacht.

AWS verfügt nur über eine begrenzte Anzahl von Zugriffspunkten auf das Informationssystem, um eine möglichst umfassende Überwachung des eingehenden und ausgehenden Netzwerkverkehrs und der Kommunikation zu ermöglichen. Diese Zugriffspunkte für Kunden werden API-Endpunkte genannt. Sie ermöglichen dem Kunden den Aufbau sicherer Kommunikationssitzungen mit ihren Speicher- oder Datenverarbeitungs-Instanzen innerhalb von AWS. In diesen Zugriffspunkten wird der eingehende und ausgehende Datenverkehr überwacht, um die Service-Verfügbarkeit sicherzustellen.

AWS hat Netzwerkgeräte implementiert, die für die Verwaltung der Schnittstellenkommunikation mit Internetdienstanbietern (Internet Service Provider, ISPs) vorgesehen sind. AWS verwendet eine redundante Verbindung zu mehr als einem Kommunikations-Service an jeder mit dem Internet verbundenen Stelle des AWS-Netzwerks. Jede dieser Verbindungen verfügt über eigene Netzwerkgeräte.

M 3.301 Protokollierung

AWS hat für alle Systeme und Geräte innerhalb des AWS-Systems, für die AWS zuständig ist, auditierbare Ereigniskategorien ermittelt. Service-Teams konfigurieren die Auditfunktionen so, dass sicherheitsrelevante Ereignisse fortlaufend gemäß den Anforderungen aufgezeichnet werden. Das Protokollspeichersystem ist dafür ausgelegt, einen hoch skalierbaren und hoch verfügbaren Service zu bieten, dessen Kapazität bei steigendem Protokollspeicherbedarf automatisch erweitert wird. Die Auditdaten enthalten eine Gruppe von Datenelementen, die die erforderlichen Analyseanforderungen unterstützen. Zusätzlich stehen sie dem AWS-Sicherheitsteam oder anderen relevanten Teams bei Bedarf zur Prüfung oder Analyse und für die Behebung sicherheitsrelevanter oder geschäftsschädigender Ereignisse zur Verfügung.

Mitarbeiter des AWS-Teams erhalten automatisierte Benachrichtigungen, wenn Fehler in überwachten Prozessen auftreten. Dazu gehören unter anderem Software- oder Hardwarefehler. Nach Erhalt einer Fehlermeldung stellen die benachrichtigten Mitarbeiter ein Fehlerticket aus und behandeln das Problem, bis es gelöst ist.

Die Verantwortung der AWS-Kunden
Die Kunden kontrollieren ihre eigenen Gastbetriebssysteme, ihre Software und ihre Anwendungen und sind aus diesem Grund dafür verantwortlich, eine Überwachung der logischen Zustände dieser Systeme zu entwickeln. In Übereinstimmung mit ISO 27001-Standards verwenden AWS-Informationssysteme interne, über NTP (Network Time Protocol) synchronisierte Systemuhren.

AWS CloudTrail bietet eine einfache Lösung, um Benutzeraktivitäten aufzuzeichnen, sodass möglicherweise kein komplexes Logging-System erforderlich ist. Weitere Informationen finden Sie unter "aws.amazon.com/cloudtrail".

AWS Cloudwatch ermöglicht die Überwachung von Ressourcen in der AWS-Cloud und von Anwendungen, die Benutzer auf AWS ausführen. Weitere Informationen finden Sie unter "aws.amazon.com/cloudwatch". AWS veröffentlicht aktuelle Informationen über Service-Verfügbarkeit in der Übersicht zum Servicestatus. Weitere Informationen finden Sie unter "http://status.aws.amazon.com/".

Zusammenfassung

Kunden können die sichere globale Infrastruktur und die Dienstleistungen von AWS verwenden, um die IT-Grundschutz-Sicherheitsanforderungen des BSI zu erfüllen. Das Verständnis des Modells der zwischen Kunde und AWS geteilten Verantwortung ist Voraussetzung für die effektive Verwaltung einer sicheren Computing-Umgebung. Kunden können eine breite Palette von AWS-Sicherheitsfunktionen und Partnerprodukten nutzen, um die Einhaltung der relevanten Sicherheitsanforderungen zu ermöglichen. Die von AWS angewendeten Prozesse und Kontrollen können vom Kunden anhand von AWS-Zertifizierungen und Berichten (beispielsweise Service-Organisation Control (SOC)-Berichte, ISO 27001-Zertifizierung, PCI-Assessments usw.) validiert werden. Sie können die jeweiligen AWS-Compliance-Zertifizierungen und -Berichte unter https://aws.amazon.com/compliance/contact anfordern.

Weitere Informationen zu AWS-Compliance-Programmen finden Sie unter https://aws.amazon.com/compliance.