Logische Trennung

Eine Bewertung der Sicherheitsanforderungen für sensible Workloads des U.S. Department of Defense

Mai 2018

[AWS-Handbuchreihe für Behörden]

Hinweise

Dieses Dokument wird nur zu Informationszwecken zur Verfügung gestellt. Es stellt das aktuelle Produktangebot und die Praktiken von AWS zum Erstellungsdatum dieses Dokuments dar. Änderungen vorbehalten. Kunden sind verantwortlich für ihre eigene Interpretation der in diesem Dokument zur Verfügung gestellten Informationen und für die Nutzung der AWS-Produkte oder -Services. Diese werden alle ohne Mängelgewähr und ohne jegliche Garantie, weder ausdrücklich noch stillschweigend, bereitgestellt. Dieses Dokument gibt keine Garantien, Gewährleistungen, vertragliche Verpflichtungen, Bedingungen oder Zusicherungen von AWS, seinen Partnern, Zulieferern oder Lizenzgebern. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Teil der Vereinbarungen von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Inhalt

Zielsetzung

Dieses Whitepaper untersucht die logische Trennung im Rahmen der Sicherheitsäquivalenz für Kunden, die Amazon Web Services (AWS) Infrastructure as a Service (IaaS) Angebote nutzen. Es dient dazu, die Anforderungen aus dem Department of Defense (DOD) Cloud Computing Security Requirements Guide (SRG) darzulegen. Das Whitepaper diskutiert einen dreigliedrigen Ansatz (Virtualisierung, Verschlüsselung und Bereitstellung der Datenverarbeitung auf dedizierter Hardware), den Behörden weltweit nutzen können, um sensible, nicht als geheim eingestufte Workloads (*z. B.* „High Impact“) ohne die Notwendigkeit einer physisch dedizierten Infrastruktur sicher in die Cloud zu migrieren.

Einleitung

Die Cloud-Technologie nutzt die Vorteile transformativer Techniken in der Informationstechnologie (IT). Kunden, die die Cloud nutzen, können von einer Rechenzentrums- und Netzwerkarchitektur profitieren, die für die sicherheitskritischsten Organisationen der Welt entwickelt wurde. Neue Betriebsmodelle und Abstraktionsmöglichkeiten durch Cloud-Technologien tragen zu einer sichereren IT-Umgebung bei. Cloud Service Provider (CSPs) wie AWS nutzen die Cloud für Innovationen und bieten ihren Kunden neue und verbesserte Sicherheitsfunktionen. AWS stellt hochverfügbare Services bereit und unterstützt sowohl „Defense-in-Depth"- als auch „Defense-in-Breadth"-Funktionalitäten mit Sicherheitsmechanismen, die für das Design und den Betrieb von Cloud-Services unerlässlich sind.

AWS bietet den Kunden die Möglichkeit, ihre Inhalte mit Hilfe von Tools zu steuern, über die sie festlegen können, wo ihre Inhalte gespeichert, verwaltet und kontrolliert werden. AWS-Funktionen bieten Kunden die Möglichkeit, ihre Inhalte während der Übertragung und im gespeicherten Zustand zu sichern und den Zugriff Ihrer Benutzer auf AWS-Services und -Ressourcen zu verwalten. AWS-Kunden behalten die volle Kontrolle über den Zugriff auf ihre Inhalte. So wird verhindert, dass unbefugte Benutzer und Kunden auf andere Kundenkonten zugreifen können. AWS bietet Multi-Mandanten-Services mit der branchenweit sichersten Trennung zwischen den einzelnen Mandanten. Diese logische Trennung zwischen den von AWS bereitgestellten Kundenumgebungen bietet eine effektivere und zuverlässigere Sicherheit als die einer dedizierten physischen Infrastruktur.

Hintergrund

Im Dezember 2011 setzte der U.S. Federal Chief Information Officer eine behördenweite Richtlinie in Kraft, die den Bundesbehörden vorschreibt, das Federal Risk and Authorization Management Program (FedRAMP) zu nutzen – ein standardisiertes, bundesweites Programm für die Sicherheitsautorisierung von Cloud-Services. Der „do once, use many times"-Ansatz des FedRAMP soll erhebliche Vorteile bieten: beispielsweise eine größere Konsistenz und Zuverlässigkeit bei der Bewertung von Sicherheitskontrollen, die Senkung der Kosten für Service-Provider und behördliche Kunden und die Rationalisierung von doppelten Autorisierungsbewertungen zwischen Behörden, die denselben Service nutzen. Das wichtigste Leitungs- und Entscheidungsgremium im Rahmen des FedRAMP ist das Joint Authorization Board (JAB), das aus den Chief Information Officers (CIOs) von der General Services Administration, des Department of Homeland Security und des DoD besteht.

FedRAMP arbeitet derzeit mit drei standardisierten Sicherheits-Baselines: Low (niedrig), Moderate (mittel) und High Impact (hohe Auswirkung). Diese basieren auf den Federal Information Processing Standards Publication (FIPS) 199 -Kategorisierungen. Diese Baselines wurden gemeinsam mit Cybersicherheitsexperten aus der Privatwirtschaft und der US-Regierung (inkl. dem DoD) entwickelt. Das DoD arbeitet entsprechend der FedRAMP-Baseline „Moderate". Die FedRAMP-Baseline „High" wurde nicht umgesetzt. Stattdessen hat das DoD mit dem „DoD Cloud Computing Security Requirements Guide" (SRG) einen „FedRAMP-plus"-Ansatz mit Sicherheitskontrollen und -anforderungen entwickelt und umgesetzt.

Insbesondere schreibt das DoD im Rahmen des SRG eine physische oder logische Trennung zwischen dem DoD und den Mandanten/Aufgaben der Bundesbehörden vor. Konkret sieht der SRG vor, dass „CSPs starke virtuelle Trennungskontrollen und -überwachungen nachweisen müssen“. Sie müssen außerdem „die Fähigkeit zur Umsetzung von Such- und Beschlagnahmungsanfragen ohne die Veröffentlichung von DoD-Informationen und -Daten“ gewährleisten. Für „Impact Level 5“-Systeme (IL5)[1] schreibt das DoD eine „physische Trennung (z.B. dedizierte Infrastruktur) von Mandanten vor, die nicht dem DoD bzw. Bundesbehörden angehören“ vor. Diese DoD-Anforderungen beziehen sich auf Bedenken des DoD bezüglich der Mischung von DoD-Daten mit den Daten anderer Mandanten aufgrund von Datenlecks oder -vermischungen und dem unbefugten Zugriff auf DoD-Daten oder deren Manipulation durch einen Nicht-DoD-Mandanten.

Um eine ergebnisorientierte, bewährte Methode umzusetzen, hat der SRG den Einsatz einer logischen Trennung als praktikablen Ansatz zur Erfüllung der DoD IL5-Anforderungen bestätigt:

> *„Ein CSP kann alternative Lösungen anbieten, die eine gleichwertige Sicherheit im Rahmen der genannten Anforderungen bieten. Die Genehmigung wird fallweise im Rahmen des PA-Assessment-Prozesses [Provisional Authorization] erteilt.“*

---

1 5.2.2.2 Anforderungen zu Standort und Trennung für Impact Level 5

Informationen, die im Rahmen von Impact Level 5 verarbeitet und gespeichert werden müssen, dürfen nur über eine dedizierte Infrastruktur (vor Ort oder extern) in einem Cloud-Bereitstellungsmodell verarbeitet werden, das den physischen Speicherort der Informationen entsprechend Abschnitt 5.2.1, „Jurisdiction/Location Requirements“ einschränkt. Hiervon ausgenommen sind öffentliche Dienstleistungsangebote.

Es gilt Folgendes:

- Nur interne Clouds des DoD, Community-Clouds des DoD oder Federal Government Community-Clouds sind für Impact Level 5 geeignet.
- Jedes Bereitstellungsmodell darf mehrere Aufgaben oder Mandanten/Aufgaben aus jeder Kundenorganisation unterstützen.
- Eine virtuelle/logische Trennung zwischen dem DoD und den Mandanten/Aufgaben der Bundesbehörden ist zulässig.
- Es ist mindestens eine virtuelle/logische Trennung zwischen Systemen für die Mandanten/Aufgaben erforderlich.
- Eine räumliche Trennung (z. B. dedizierte Infrastruktur) von Mandanten die nicht dem DoD bzw. Bundesbehörden angehören, ist erforderlich.

HINWEIS: Ein CSP kann alternative Lösungen anbieten, die eine gleichwertige Sicherheit im Rahmen der genannten Anforderungen bieten. Die Genehmigung wird fallweise im Rahmen des PA-Assessment-Prozesses erteilt.

https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf

Welche Schwächen weisen die Anforderungen zur räumlichen Trennung auf?

Die Anforderungen für räumlich getrennte, dedizierte Cloud-Angebote basieren in erster Linie auf Bedenken hinsichtlich des unbefugten Zugriffs Dritter auf Anwendungen, Inhalte oder Daten, einschließlich des erzwungenen Zugriffs von Strafverfolgungsbehörden und des unbefugten Zugriffs Dritter. Bei Systemen, die über ein Netzwerk oder über das Internet zugänglich sind, bietet die räumliche Trennung dieser Systeme (z. B. die Unterbringung in einer verschlossenen Einheit oder einer separaten Rechenzentrumseinrichtung) keine zusätzliche Sicherheit oder Zugriffskontrolle. Einfach ausgedrückt werden sämtliche Zugriffskontrollen für angebundene Systeme über logische Zugriffskontrollen, das Berechtigungsmanagement, das Routing des Netzwerkverkehrs und die Verschlüsselung verwaltet. AWS deckt alle Bedenken bezüglich der räumlichen Trennung über die logischen Sicherheitsfunktionen für alle Kunden sowie die Sicherheitskontrollen zum Schutz der Kundendaten ab. Diese Funktionen und Kontrollen werden weiter unten im Rahmen des dreigliedrigen Ansatzes zur logischen Trennung näher beschrieben.

Kleinere, räumlich getrennte Umgebungen sind nicht mit allgemein verfügbaren Cloud-Umgebungen vergleichbar. Daher kann jede Anforderung für eine räumliche Trennung dafür sorgen, dass die Möglichkeiten zur Nutzung innovativer Investitionen für alle Kunden der AWS-Services (einschließlich Innovationen bei Sicherheitsmerkmalen) eingeschränkt bleiben. Weitere Nachteile sind eine höhere Kostenstruktur und eine geringere Auslastung durch eine weniger effiziente Flächennutzung sowie eingeschränkte Redundanzmöglichkeiten und -funktionen im Vergleich zu geografisch verteilten, kommerziellen Rechenzentrumsregionen.

Warum ist logische Trennung effektiver als räumliche Trennung?

Mit dem folgenden dreigliedrigen Ansatz können die Kunden eine Sicherheit erreichen, die einer räumlichen Trennung und den DoD-IL5-Anforderungen entspricht.

1. Virtual Private Cloud (VPC) – Ausführliche Darstellung der Gleichwertigkeit einer VPC zu komplett getrennten Netzwerkdomänen für jeden Mandanten.
2. Verschlüsselung von gespeicherten Daten und Daten während der Übertragung – Nutzung einer vom Benutzer bereitgestellten oder inhärenten Datenverschlüsselungsfunktionen von AWS Cloud-Services (z. B. EBS, S3 und DynamoDB) mit Verschlüsselungsschlüsseln, die von AWS Key Management Service (KMS) und/oder AWS Cloud Hardware Security Module (CloudHSM) generiert und gespeichert werden.
3. Dedicated Hosts, Dedicated Instances und Bare Metal – DoD-Verantwortliche können komplette physische AWS-Hosts bereitstellen, um sowohl virtualisierte als auch nicht virtualisierte Instances und die entsprechenden Workloads zuzuweisen.

1. Virtual Private Cloud (VPC)

Eine AWS-VPC ermöglicht die Erstellung einer logisch getrennten Netzwerkenklave innerhalb des AWS Elastic Cloud Compute-Netzwerks (Amazon EC2). Diese hostet die Datenverarbeitungs- und Storage-Ressourcen. Diese Umgebung kann über eine VPN-Verbindung (Virtual Private Network) über das Internet oder über AWS Direct Connect (ein Service für eine private Anbindung an die AWS Cloud) an die bestehende Infrastruktur eines Kunden angebunden werden. Der Einsatz einer VPC bietet den Verantwortlichen eine hohe Flexibilität und Sicherheit sowie die vollständige Kontrolle über ihre Netzwerkpräsenz in der Cloud. Es ist ein kontrollierter Übergang in die Cloud möglich. Hierbei können das bestehende Rechenzentrumsmodell und das Verwaltungsschema eines Kunden genutzt werden. Der Kunde kontrolliert die private Umgebung einschließlich der IP-Adressen, Subnetze, Netzwerk-Zugriffskontrolllisten, Sicherheitsgruppen, Betriebssystem-Firewalls, Routing-Tabellen, VPNs und/oder Internet-Gateways. Eine Amazon-VPC bietet eine robuste, logische Isolierung aller Kundenressourcen. Beispielsweise wird jede Paketübertragung im Netzwerk einzeln autorisiert. Quelle und Ziel werden vor der Übertragung validiert. Ohne ausdrückliche Genehmigung durch den übertragenden und empfangenden Kunden ist der Austausch von Informationen zwischen Mandanten unmöglich. Wenn ein Paket zu einem Ziel ohne eine passende Regel geroutet wird, wird das Paket verworfen. ARP-Pakete (Address Resolution Protocol) lösen zwar eine authentifizierte Datenbankabfrage aus, sie erreichen jedoch nie das Netzwerk, da sie für die Erkennung der virtuellen Netzwerktopologie nicht benötigt werden. So wird ARP-Spoofing unmöglich. Auch der promiskuitive Modus legt, abgesehen von Netzwerkverkehr für das Betriebssystem des Kunden, keinerlei Netzwerkverkehr offen. Diese präzisen Regeln für den ein- und ausgehenden Netzwerkverkehr des Kunden ermöglichen nicht nur eine größere Flexibilität bei der Konnektivität, sondern auch eine bessere Kontrolle des Kunden über die Segmentierung und das Routing des Netzwerkverkehrs.

Die Konnektivitätsoptionen für die VPC[2] bieten dem Kunden folgende Möglichkeiten:

- Verbindung zum Internet per NAT (Network Address Translation, private Subnetze) – Private Subnetze können für Instances verwendet werden, die keinen direkten Zugang zum oder aus dem Internet haben sollen. Instances in einem privaten Subnetz können auf das Internet zugreifen, ohne ihre private IP-Adresse preiszugeben. Ihr Datenverkehr wird über ein NAT-Gateway in einem öffentlichen Subnetz geroutet.
- Sichere Verbindung zum Rechenzentrum Ihrer Organisation – Der gesamte Datenverkehr zu und von Instances in Ihrer VPC kann über eine verschlüsselte IPsec-Hardware-VPN-Verbindung zu Ihrem Rechenzentrum geroutet werden.
- Private Anbindung an andere VPCs – Peer-VPCs nutzen Ressourcen über mehrere virtuelle Netzwerke Ihrer AWS-Konten gemeinsam.
- Binden Sie Ihre internen Services über verschiedene Konten und VPCs innerhalb Ihrer eigenen Organisation an und vereinfachen Sie so Ihre interne Netzwerkarchitektur erheblich.

2. Verschlüsselung von gespeicherten Daten und Daten während der Übertragung

Daten, die von Verantwortlichen in AWS-Storage-Services gespeichert oder über unsere Netzwerke übertragen werden, sollten unbedingt eine starke Verschlüsselung für die gespeicherten und übertragenen Daten nutzen. Um dies für unsere Kunden möglichst einfach und sicher zu gestalten, bieten wir eine Reihe von Tools und Funktionen an, mit denen Daten verschlüsselt werden können. Dazu stellen wir verschiedene Möglichkeiten für die Verwaltung von Verschlüsselungsschlüsseln bereit. Diese Verschlüsselungs- und Datenzugriffskontrollfunktionen sind bereits in grundlegende Serviceangebote wie Amazon Simple Storage Service (Amazon S3, ein hochskalierbarer Objektspeicherdienst), Amazon Elastic Block Store (Amazon EBS, Netzwerkspeicher für EC2-Instances) und Amazon Relational Database Service (Amazon RDS, verwaltete Datenbank-Engines) integriert. Die Funktionen sind sofort einsatzbereit. Es steht eine Menge von Dokumentation zur Unterstützung der Kunden bereit. So können diese überblicken, wie ihre Daten geschützt werden und welche Konfigurationsoptionen sie für die Steuerung des Zugriffs auf ihre Systeme nutzen können. Die nativen Services von AWS verfügen über neue Sicherheitsfunktionen, die in älteren Umgebungen nur durch den Einsatz von Drittanbieterlösungen erreicht werden konnten. Diese Funktionalitäten stehen heute in wachsende, Maß zur Verfügung – sodass sich die Kunden auf Service-Innovationen konzentrieren können.

AWS Key Management Service (KMS) und AWS CloudHSM bilden gemeinsam das Kernstück einer rigorosen Verschlüsselungslösung. AWS KMS ist ein vollständig verwalteter, hochverfügbarer, regionaler Service, der auf Hardware-Sicherheitsmodulen (HSMs)[2] basiert, die über eine FIPS 140-2 Level 3-Validierung (Physical Security) verfügen. Dank einer ausgefeilten Scale-Out-Software kann der Service mehrere hunderttausend API-Anfragen pro Sekunde verarbeiten. Es bietet den Kunden die Möglichkeit, wichtige Funktionen zur Schlüsselverwaltung in einer Weise auszuführen, die tief in andere AWS-Services integriert ist. AWS CloudHSM bietet ein dediziertes FIPS 140-2 Level 3 (Overall) HSM, das direkt in Ihrer Amazon Virtual Private Cloud (VPC)[3] unter Ihrer alleinigen Kontrolle steht. Der CloudHSM-Service bietet eine automatisierte Verfügbarkeit, Replikation und Datensicherung der dedizierten, individuellen HSMs der Kunden über Availability Zones hinweg. Er wird über Krypto-APIs nach Industriestandard mit den Anwendungen der Kunden integriert. Obwohl beide Services in unterschiedlichen Kontexten eingesetzt werden, sorgen sie gemeinsam dafür, dass der Verschlüsselungsalgorithmus für eine Verschleierung der Daten robust genug ist. Sie sorgen außerdem für den Schutz der Schlüssel. So ist gewährleistet, dass der Verschlüsselungstext nicht von Unbefugten gelesen werden kann. Mit anderen Worten: Die Speicherung von entsprechend verschlüsselten Daten mit ordnungsgemäß verwalteten und gesicherten Schlüsseln kann vollständig geschützte Daten gewährleisten. Dieser Ansatz ist gleichermaßen relevant, anwendbar und effektiv – und zwar unabhängig davon, ob er in einer räumlich isolierten oder einer logisch isolierten, kommerziellen Cloud-Umgebung eingesetzt wird.

Bei der Verschlüsselung ist die Vertraulichkeit der kryptographischen Schlüssel des Verantwortlichen entscheidend. Die Sicherheit hängt davon ab, wo die Daten verschlüsselt wurden und wer Zugriff auf die Schlüssel hat und diese schützt. Wenn die Daten vom Verantwortlichen verschlüsselt werden, bevor sie in die Cloud übertragen werden, gibt es für den CSP keinen Grund für einen Zugriff auf die Schlüssel. Der Verantwortliche hat die volle Kontrolle und Verantwortung. Wenn die Daten mit Hilfe von nativen Services des CSPs verschlüsselt werden, wären sowohl der CSP als auch der Dateneigentümer in die Überwachungskette (Chain of Custody) für die Schlüssel eingebunden. AWS KMS ist so konzipiert, dass

2 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3139

3 https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3108

niemand Ihre Klartext-Schlüssel aus dem Service abrufen kann. Dies gilt auch für AWS-Mitarbeiter. Der Service verwendet FIPS 140-2-HSMs, um die Vertraulichkeit und Integrität Ihrer Schlüssel zu schützen – und zwar unabhängig davon, ob Sie KMS die Schlüssel erstellen lassen oder diese in den Service importieren. Ihre Klartext-Schlüssel werden nie auf Festplatten geschrieben und nur so lange im flüchtigen Speicher der HSMs vorgehalten, wie es für die Ausführung der gewünschten kryptografischen Vorgänge erforderlich ist. KMS-Schlüssel werden niemals außerhalb der AWS-Regionen übertragen, in denen sie erstellt wurden. Updates der KMS HSM-Firmware werden durch eine Quorum-basierte Zugriffskontrolle gesteuert, die von einer unabhängigen Gruppe innerhalb von Amazon überwacht und überprüft wird. Diese Richtlinien, Prozesse und Verfahren wurden von unabhängiger Seite geprüft und durch die FedRAMP und das DoD akkreditiert. Der folgende Abschnitt fasst die Möglichkeiten von AWS KMS und AWS CloudHSM zusammen. Weitere Informationen zu AWS KMS und AWS CloudHSM finden Sie unter den Links im Text.

AWS Key Management Service (KMS)

AWS Key Management Service (KMS) bietet Kunden eine zentrale Kontrolle über die zum Schutz ihrer Daten verwendeten Verschlüsselungsschlüssel. Mit AWS KMS können Kunden Nutzungsrichtlinien für die Verschlüsselung von Kundendaten erstellen, rotieren, deaktivieren, löschen und definieren und die Verwendung von Verschlüsselungsschlüsseln überprüfen. AWS KMS ist in die AWS-Services integriert. So wird die Verschlüsselung der in diesen Services gespeicherten Daten mit durch den Kunden verwalteten Verschlüsselungsschlüsseln (oder über von einem AWS-Service im Auftrag des Kunden verwaltete Standardschlüssel) sehr einfach. Der Service ist in den fünf zentralen Services enthalten, die nach den DoD-IL5-Anforderungen für die Verschlüsselung von gespeicherten Daten und Daten während der Übertragung akkreditiert. Die Services bieten eine ausreichende logische Trennung der DoD-Daten, die in der AWS-Infrastruktur übertragen werden und sich auf Hardware befinden, auf der sich auch Nicht-DoD-Kundendaten befinden. Beispielsweise ist die Verwendung von starken kryptographischen Algorithmen zur logischen Trennung von Kundendaten bei gespeicherten Daten mit der räumlichen Trennung von gespeicherten Daten (eine IL5-Anforderung) gleichwertig.

Das Hardened Security Module (HSM) bildet die innere Sicherheitsgrenze von AWS KMS. Das HSM verfügt über eine begrenzte, interne, webbasierte API. Im Betriebszustand gibt es keine weiteren aktiven physischen Schnittstellen. Bei der Initialisierung wird ein funktionsfähiges HSM konfiguriert und mit den entsprechenden kryptographischen Schlüsseln ausgestattet. Sensible kryptographische Materialien des HSM werden nur in einem flüchtigen Speicher abgelegt und gelöscht, sobald das HSM den Betriebszustand verlässt (einschließlich beabsichtigter oder unbeabsichtigter Shutdowns oder Resets). Im Betriebszustand kann kein menschlicher Operator auf das HSM zugreifen. Über die eingeschränkte API können nur Service-Hosts Verbindungen herstellen, die Kundenanfragen bearbeiten. Die HSM-APIs stehen über eine wechselseitig authentifizierte, vertrauliche Sitzung zur Verfügung, die von menschlichen Operatoren (wenn nicht betriebsbereit) oder Service-Hosts (wenn betriebsbereit) eingerichtet wurde.

Das System ist so konzipiert, dass zur Aktualisierung der Firmware oder Softwarekonfiguration auf einem beliebigen KMS HSM mehrere Operatoren mit einer Zwei-Faktor-Authentifizierung über einen Quorum-basierten Prozess erforderlich sind. Sie ist jedoch auch dann erst möglich, wenn das HSM in einen nicht betriebsbereiten Zustand versetzt wurde und kein Schlüsselmaterial mehr enthält.

> **Hinweis:** AWS Key Management Service (KMS) verwendet heute HSMs mit FIPS 140-2-Validierung und unterstützt Endpunkte mit FIPS 140-2-Validierung. Dies bietet eine unabhängige Garantie, dass die Vertraulichkeit und Integrität Ihrer Schlüssel gewährleistet sind.

AWS CloudHSM

AWS CloudHSM bietet effektives Hardware-Schlüsselmanagement mit Cloud-Skalierung für sensible und regulierte Workloads. CloudHSM ermöglicht den Verantwortlichen die Bereitstellung und Nutzung von kryptografischen Schlüssel für die Verschlüsselung ihrer Daten innerhalb der AWS-Services und der dort befindlichen Anwendungen. Mit CloudHSM verwalten Kunden ihre eigenen Verschlüsselungsschlüssel über ein FIPS 140-2 Level 3-validiertes HSM. Über branchenübliche APIs wie PKCS#11, Java Cryptography Extensions (JCE) und Microsoft CryptoNG-Bibliotheken (CNG) haben sie die Flexibilität, eine Integration mit ihren Anwendungen durchzuführen. CloudHSM ist außerdem standardkonform, sodass Verantwortliche ihre gesamten Schlüssel in die meisten handelsüblichen HSMs exportieren können. CloudHSM ist ein verwalteter Service, der zeitaufwändige Verwaltungsaufgaben wie die Hardwarebereitstellung, die Installation von Software-Patches, die Hochverfügbarkeit und Datensicherungen automatisiert. Um Ihr CloudHSM vor anderen Amazon-Kunden zu schützen und von diesen zu isolieren, muss CloudHSM in einer VPC bereitgestellt werden.

Die Trennung der aufgaben- und rollenbasierten Zugriffskontrolle ist ein inhärentes Element des Designs von CloudHSM. AWS hat einen eingeschränkten Zugriff auf das HSM. Dieser erlaubt es uns, den Zustand und die Verfügbarkeit des HSM zu überwachen und aufrechtzuerhalten, verschlüsselte Sicherungen zu erstellen und Audit-Protokolle zu extrahieren und in Ihrem CloudWatch Logs zu veröffentlichen. AWS kann Ihre Schlüssel weder sehen noch auf diese zugreifen. AWS kann mit Ihren Schlüsseln keine kryptographischen Operationen über das HSM durchführen.

3. Dedicated Hosts, Dedicated Instances und Bare Metal

AWS bietet nicht nur hochsichere, logisch isolierte Multi-Mandanten-fähige Datenverarbeitungsservices, sondern auch drei Möglichkeiten zur Bereitstellung von Datenverarbeitungsleistung auf dedizierter Hardware: Dedicated Instances, Dedicated Hosts und Bare Metal. Diese Bereitstellungsoptionen können verwendet werden, um Amazon EC2-Instances auf physischen Servern zu starten, die nur für Sie bestimmt sind. Dedicated Instances sind virtualisierte Amazon EC2-Instances, die in einer Virtual Private Cloud (VPC) auf Hardware ausgeführt werden, die nur von einem einzelnen Kunden genutzt wird. Dedicated Instances sind auf der Host-Hardwareebene physisch von Instances isoliert, die zu anderen AWS-Konten gehören. Dedicated Instances können Hardware mit anderen Instances desselben AWS-Kontos teilen, die keine Dedicated Instances sind. Ein Dedicated Host ist ebenfalls ein physischer Server, der ausschließlich von Ihnen genutzt wird. Mit einem Dedicated Host haben Sie Einblicke in und Kontrolle über die Art der Platzierung der virtualisierten Instances auf dem Server. Bare Metal-Instances sind nicht virtualisierte Host-Hardwaregeräte. Über den Einsatz der AWS Nitro-Technologie für den Netzwerk- und Storage-Offload sowie des Nitro-Sicherheitschips zur Eliminierung der Risiken bei einer seriellen Single-Tenancy auf Bare Metal-Instances haben Kunden direkten Zugriff auf Amazon EC2-Hardware. Diese Bare Metal-Instances sind vollwertige Mitglieder des Amazon EC2-Services und haben Zugriff auf Services wie Amazon VPC und Amazon Elastic Block Store (EBS).[4]

4 Derzeit ist Amazon EC2 Bare Metal in Form des Instance-Typs i3.metal über die I3-Instance-Familie verfügbar.

Es gibt keine leistungsbezogenen, sicherheitsrelevanten oder physischen Unterschiede zwischen Dedicated Instances und Instances, die auf Dedicated Hosts bereitgestellt werden. Dedicated Hosts bieten den Verantwortlichen jedoch zusätzliche Kontrolle über die Art der Platzierung der Instances auf einem physischen Server sowie über die Nutzung des Servers. Wenn Sie Dedicated Hosts verwenden, haben Sie die Kontrolle über die Platzierung der Instance auf dem Host mithilfe der Einstellungen für Host Affinity und die automatische Instance-Platzierung. Beispielsweise, wenn Ihre Organisation AWS verwenden möchte und über eine bestehende Softwarelizenz verfügt, bei der die Software auf einer bestimmten Hardware für einen bestimmten Zeitraum ausgeführt wird. Dedicated Hosts ermöglichen einen Einblick in die Hardware des Hosts und die Umsetzung entsprechender Lizenzanforderungen.

Wie erfüllt die Multi-Mandanten-Cloud Datenanforderungen von Vollstreckungsbehörden, ohne DoD-Daten offenzulegen?

AWS erfüllt rechtmäßige Datenanforderungen von Vollstreckungsbehörden. Während Behörden bei lokalen Systemen in der Regel die Möglichkeit haben, die physische Hardware beim Dateneigentümer zu beschlagnahmen oder auf diese zuzugreifen, führt Cloud Computing ein anderes Modell ein – denn die Daten werden dort in einer Multi-Mandanten-Umgebung gehostet. Die physische Beschlagnahmung oder der Zugriff auf physische Hardware in AWS ist nicht möglich. Die Daten eines Kunden sind auf verschiedene physische Geräte verteilt. Daher müssen alle Datenanfragen einen genehmigten und autorisierten logischen Abrufprozess durchlaufen. Durch unsere FedRAMP-Akkreditierung erfüllt AWS die NIST 800-53-Kontrollen der FedRAMP-Baseline „Moderate“ (einschließlich der Sicherheitskontrollen „Information Handling and Retention“ und „System and Information Integrity“). Dies bedeutet unter anderem, dass die AWS-Services verschiedene Kundenkonten abgrenzen, eine gegenseitige Vermischung von Kundenkonten verhindern und den Kunden die volle Kontrolle über den Inhalt und den Betrieb ihrer einzelnen AWS-Konten ermöglichen. Wie alle Kunden können auch DoD-Kunden sicher sein, dass jede rechtmäßige Strafverfolgungsanfrage nur für die Daten innerhalb des Kontos des entsprechenden Kunden gilt. Wir halten uns außerdem an die „System and Information Integrity“-Kontrollen. Diese verlangen, dass konforme CSPs den Kunden Zugang zu ihren Daten gewähren und dass konforme Behörden entsprechend der geltenden Gesetze ihre eigenen Daten pflegen. Darüber hinaus verlangen die „Audit and Accountability“-Einschränkungen, dass Organisationen Audit-Aufzeichnungen aufbewahren, um nachträgliche Untersuchungen von Sicherheitsvorfällen zu ermöglichen und die gesetzlichen und organisatorischen Anforderungen an die Aufbewahrung von Informationen zu gewährleisten. Die Kunden können Cloud-Audit-Protokolle und Berichte abrufen, indem sie CloudTrail und CloudWatch Logs nutzen, die sie dann den zuständigen Behörden zur Verfügung stellen können. Diese Lösungen ermöglichen es dem DoD, direkt auf Anfragen von Inspekteuren oder Strafverfolgungsbehörden zu reagieren, so dass Regierungsbeamte direkten Zugriff auf möglicherweise benötigte Informationen haben und keine Hardware beschlagnahmen müssen.

AWS arbeitet außerdem mit strengen Richtlinien und Kontrollen in Bezug auf Bereinigung und Zerstörung. So verfolgt, dokumentiert und verifiziert AWS beispielsweise Maßnahmen zur Bereinigung und Entsorgung von Medien. Ein Kunde hat niemals physischen Zugriff auf die seinem logischen Volume oder Objekt zugeordneten Medien. Die gesamte Medienentnahme und -entsorgung erfolgt durch ausgewiesenes AWS-Personal. Inhalte auf Laufwerken werden gemäß der höchsten Stufe der Datenklassifikationsrichtlinie von AWS behandelt. Alle Medien werden am Ende des Medienlebenszyklus unlesbar gemacht und zerstört, bevor sie im Rahmen des Stilllegungsprozesses und gemäß der Sicherheitsstandards von AWS ein AWS-Rechenzentrum verlassen.

Wie schützt die mandantenfähige Cloud vor dem unberechtigten Zugriff auf DoD-Daten durch Dritte und CSP-Mitarbeiter?

Im Rahmen der Möglichkeit zur Anforderung von Kundendaten durch Strafverfolgungsbehörden bestehen Bedenken zum Potenzial für einen unbefugten Zugriff Dritter auf Kundeninhalte und die angemessenen Zugangskontrollmaßnahmen, um den unbefugten Zugriff durch CSP-Mitarbeiter zu verhindern. Wir greifen nicht auf die Inhalte unserer Kunden zu oder verwenden sie – außer dies ist gesetzlich oder für die Wartung der AWS-Dienste und ihre Bereitstellung an unsere Kunden und ihre Endbenutzer erforderlich.

Der Zugriff der Mitarbeiter auf die AWS-Systeme basiert auf der Vergabe der geringstmöglichen Privilegien, die von einer autorisierten Person vor der Zugriffsbereitstellung genehmigt und von einem AWS-Mitarbeiter überwacht wird. Obliegenheiten und Verantwortungsbereiche (z. B. Zugriffsanforderung und -genehmigung, Anforderungen im Rahmen des Änderungsmanagements und deren Genehmigung usw.) müssen auf verschiedene Individuen aufgeteilt werden, um Gelegenheiten für eine nicht autorisierte oder ungewollte Modifikation sowie für einen Missbrauch von AWS-Systemen zu minimieren. AWS-Mitarbeiter, die aus geschäftlichen Gründen Zugriff auf die Verwaltungsebene benötigen, erhalten per Multi-Factor Authentication (unabhängig von ihren normalen Amazon-Anmeldeinformationen) Zugriff nur auf zweckgebundene Verwaltungs-Hosts. Bei diesen Verwaltungs-Hosts handelt es sich um Systeme, die eigens zum Schutz der Verwaltungsebene der Cloud entworfen, erstellt, konfiguriert und gehärtet wurden. Jeder Zugriff wird protokolliert und überprüft. Wenn ein Mitarbeiter keinen Zugriff mehr auf die Verwaltungsebene benötigt, werden die entsprechenden Berechtigungen und der Zugriff auf diese Hosts und die zugehörigen Systeme widerrufen. AWS hat eine Richtlinie zur Sitzungssperrung implementiert, die systemweit durchgesetzt wird. Die Sitzungssperre bleibt aufrechterhalten, bis die etablierten Verfahren zur Identifizierung und Authentifizierung durchlaufen wurden.

Die Kunden verwalten den Zugriff auf ihre Inhalte sowie auf AWS-Services und -Ressourcen. Wir bieten eine Reihe von erweiterten Zugriffs-, Verschlüsselungs- und Protokollierungsfunktionen, die Sie hierbei effektiv unterstützen (z. B. AWS CloudTrail, CloudWatch, CloudHSM und AWS KMS wie oben beschrieben).

Wie lauten die Empfehlungen von AWS an Behörden, die eine räumliche Trennung in Betracht ziehen?

Im Rahmen des Cloud Computing SRG-Autorisierungsprozesses des DoD kann AWS aufzeigen, dass die logische Trennung ausreicht, um die Anforderungen einer dedizierten, physisch isolierten Infrastruktur für die sensibelsten, nicht als geheim eingestuften Workloads des DoD zu erfüllen. Unser Ansatz bestätigt, dass logisch getrennte Multi-Mandanten-Umgebungen mit robusten Sicherheitskontrollen ein höheres Sicherheitsniveau als dedizierte Private-Cloud-Implementierungen bieten und gleichzeitig erhebliche Vorteile in Bezug auf Verfügbarkeit und Skalierbarkeit sowie geringere Kosten bieten. Die moderne Cloud-Technologie von etablierten Anbietern bietet neuartige Lösungen, die dem Ziel der traditionellen Technologiesicherheit gerecht werden – sofern die Akkreditierungsansätze flexibel genug sind, um alternative Implementierungen zu ermöglichen.

Unsere Erfahrung hat gezeigt, dass Organisationen, die sich in erster Linie (und in einigen Fällen ausschließlich) auf die Implementierung traditioneller Kontrollen konzentrieren, ihren Zugriff auf erstklassige Sicherheitslösungen möglicherweise unbeabsichtigt einschränken. Bei der Bewertung von CSPs zur Erfüllung von Anforderungen auf der Grundlage veralteter Konzepte durch Behörden sollten diese das gewünschte Sicherheitsergebnis klar formulieren und den CSPs die Entwicklung der optimalen Techniken zur Realisierung (oder zum Übertreffen) dieser Anforderungen ermöglichen. Die Ausrichtung auf das gewünschte Sicherheitsziel hinter einer bestimmten Anforderung kann die Bundesbehörden dabei unterstützen, sich auf die zu erreichenden Ergebnisse und nicht auf die Umsetzungsdetails zu konzentrieren.

Da Sicherheitsbewertungsprogramme immer ausgereifter und skalierbarer werden, um mit dem rasanten Tempo der Cloud-Features und Sicherheitsinnovationen Schritt zu halten, werden die Details zur Implementierung der Kontrolle im Vergleich zu den Möglichkeiten durch CSPs zunehmend irrelevant. Der gewünschte Endzustand – eine robuste Cloud-Sicherheit, basierend auf einem durch die Sicherheitsergebnisse der Kunden und durch den CSP definierte Sicherheitstechniken definierten Rahmen – kann nur als Ergebnis eines kontinuierlichen Dialogs innerhalb der Cloud-Assurance-Stakeholder-Community erreicht werden. Wir glauben, dass dieser Ansatz eine wesentliche Verbesserung bei der Aufrechterhaltung des Sicherheitsstatus eines CSP darstellen würde.

Zusätzlich zur Bereitstellung einer logisch gleichwertigen Alternativlösung nutzte AWS einen End-to-End-Ansatz und führte Deep-Dive-Sessions durch, um die Sicherheitsbedenken des DoD vollständig zu berücksichtigen. Ausgehend von den im DoD Cloud Computing SRG definierten Kundenanforderungen, führte AWS mehrere Knowledge-Session durch, um das DoD darüber aufzuklären, wie unser dreigliedriger Ansatz den Anforderungen der räumlichen Trennung entspricht. Der externe Gutachter hat unsere Services validiert. Dieser hat ebenfalls an den Sitzungen teilgenommen, um die Richtigkeit unserer Aussagen zu bestätigen und eine risikobasierte Bewertung anzubieten. Diese gemeinsamen Sitzungen waren ein wertvolles und effizientes Mittel, um die Sicherheit sicherzustellen, die Akkreditierung zu beschleunigen und schließlich die IT-Modernisierungsziele des DoD voranzutreiben.

Die Entwicklung des DoD hin zu innovativen Cloud-Lösungen ermutigte uns, die Anforderungen der räumlichen Trennung in der Cloud umzusetzen. Wir verpflichteten uns zu einer kontinuierlichen Zusammenarbeit mit Behörden auf der ganzen Welt, die die Vorzüge und bewährten Methoden der gleichwertigen logischen Trennung des DoD evaluieren.