Whitepaper zu AWS

DSGVO-Compliance auf AWS

DSGVO-Compliance auf AWS: Whitepaper zu AWS

Table of Contents

DSGVO-Compliance auf AWS

Veröffentlichungsdatum: Dezember 2020 (Dokumentversionen)

Überblick

Dieses Dokument enthält Informationen zu Services und Ressourcen, die Amazon Web Services (AWS) Kunden anbietet, um sie bei der Anpassung an die Anforderungen der Datenschutz-Grundverordnung (DSGVO) zu unterstützen, die für ihre Aktivitäten gelten könnten. Dies beinhaltet die Einhaltung von IT-Sicherheitsstandards, insbesondere die Bestätigungen der Anforderungen Cloud Computing Compliance Controls Catalogue (C5) des BSI, die Einhaltung des Verhaltenskodex für Cloud Infrastructure Services Providers in Europe (CISPE), Steuerungsmöglichkeiten für den Datenzugriff, Protokollierungs- und Überwachungstools, die Verschlüsselung sowie die Schlüsselverwaltung.

Datenschutz-Grundverordnung – Übersicht

Die Datenschutz-Grundverordnung (DSGVO) ist ein europäisches Datenschutzgesetz (Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016), das am 25. Mai 2018 in Kraft trat. Die DSGVO ersetzt die EU-Datenschutzrichtlinie (Richtlinie 95/46/EC). Ziel ist es, die Datenschutzgesetze innerhalb der Europäischen Union (EU) durch ein einziges Datenschutzgesetz zu harmonisieren, das für jeden EU-Mitgliedsstaat verbindlich ist.

Die DSGVO gilt für die gesamte Verarbeitung personenbezogener Daten entweder durch Organisationen, die eine Niederlassung in der EU haben, oder für Organisationen, die personenbezogene Daten von EU-Bürgern verarbeiten, wenn sie Waren oder Dienstleistungen für Einzelpersonen in der EU anbieten oder das Verhalten von EU-Bürgern in der EU überwachen. Unter personenbezogenen Daten sind alle Informationen zu verstehen, die sich auf eine identifizierte natürliche Person beziehen oder anhand derer eine natürliche Person identifiziert werden kann.

Änderungen, die sich mit der DSGVO für in der EU tätige Organisationen ergeben

Einer der wichtigsten Aspekte der DSGVO ist die Harmonisierung des Vorgangs zur Verarbeitung und Nutzung personenbezogener Daten und ihrem sicheren Austausch für EU-Mitgliedsstaaten. Organisationen müssen die Sicherheit der verarbeiteten Daten sowie ihre Compliance mit der DSGVO fortwährend nachweisen. Dazu sind die Implementierung und regelmäßige Prüfung technischer und organisatorischer Maßnahmen sowie Compliance-Richtlinien für die Verarbeitung personenbezogener Daten erforderlich. EU-Aufsichtsbehörden können wegen Verletzung der DSGVO Strafen von bis zu 20 Millionen Euro oder 4 % des jährlichen weltweiten Umsatzes (je nachdem, was höher ausfällt) verhängen.

Wie bereitet sich AWS auf die DSGVO vor?

Unsere Experten für Compliance, Datenschutz und Sicherheit arbeiten mit Kunden aus aller Welt zusammen und beraten sie zur Ausführung von Workloads in der Cloud gemäß der DSGVO. Diese Teams überprüfen auch die Bereitschaft von AWS anhand der Anforderungen der DSGVO.

> **Note**
>
> Alle AWS-Services können in Einklang mit der DSGVO verwendet werden.

Das AWS Data Processing Addendum (DPA)

Der AWS-Vertragsanhang zur DSGVO-konformen Datenverarbeitung (AWS GDPR Data Processing Addendum – GDPR DPA) hilft Kunden, die vertraglichen Verpflichtungen im Rahmen der DSGVO einzuhalten. Das AWS GDPR DPA ist in den Nutzungsbedingungen der AWS-Services integriert und gilt automatisch für alle Kunden weltweit, die sich an die DSGVO halten müssen.

Am 16. Juli 2020 hat der Gerichtshof der Europäischen Union (EuGH) ein Urteil zum EU-US-Datenschutzschild und zu den Standardvertragsklauseln (engl. „standard contractual clauses“, kurz: SCCs), auch als „Modellklauseln“ bezeichnet, gefällt. Der EuGH hat geurteilt, dass das EU-US-Datenschutzschild zur Übertragung personenbezogener Daten aus der Europäischen Union (EU) in die Vereinigten Staaten (USA) nicht mehr gültig ist. In demselben Urteil bestätigte der EuGH jedoch, dass Unternehmen SCCs weiterhin als Mechanismus für die Übertragung von Daten in Länder außerhalb der EU nutzen können.

Nach diesem Urteil können AWS-Kunden und -Partner AWS weiterhin verwenden, um ihre Inhalte in Übereinstimmung mit den EU-Datenschutzgesetzen – einschließlich der Datenschutz-Grundverordnung (DSGVO) – von Europa in die USA und in andere Länder zu übertragen. AWS-Kunden können sich auf die im AWS-Vertragsanhang zur Datenverarbeitung enthaltenen SCCs verlassen, wenn sie ihre Daten DSGVO-konform in Länder außerhalb der Europäischen Union übertragen möchten. Im Zuge der Weiterentwicklung der regulatorischen und gesetzlichen Rahmenbedingungen werden wir daran arbeiten, dass unsere Kunden und Partner weiterhin überall dort, wo sie tätig sind, die Vorteile von AWS nutzen können. Weitere Informationen finden Sie in den häufig gestellten Fragen zum EU-US-Datenschutzschild.

Die Rolle von AWS im Rahmen der DSGVO

Im Rahmen der DSGVO wird AWS sowohl als Datenauftragsverarbeiter als auch als Datenverantwortlicher gesehen.

Gemäß Artikel 32 sind Verantwortliche und Auftragsverarbeiter verpflichtet, „… geeignete technische und organisatorische Maßnahmen“ zu treffen, die „den Stand der Technik, die Implementierungskosten und die Art, den Umfang, und den Zweck der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“ berücksichtigen. Die DSGVO macht konkrete Vorschläge für eventuell erforderliche Sicherheitsmaßnahmen, darunter:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

AWS als Datenauftragsverarbeiter

Wenn Kunden und APN-Partner (AWS Partner Network) die AWS-Services zur Verarbeitung personenbezogener Daten verwenden, agiert AWS als Datenauftragsverarbeiter. Kunden und APN-Partner können die Steuermöglichkeiten, die wir in den AWS-Services zur Verfügung stellen – etwa die für Sicherheitskonfigurationen – für die Verarbeitung personenbezogener Daten nutzen. In diesen Fällen kann der Kunde oder APN-Partner als Datenverantwortlicher oder Datenauftragsverarbeiter und AWS als Datenauftragsverarbeiter oder untergeordneter Datenauftragsverarbeiter agieren. Im AWS-Vertragsanhang zur DSGVO-konformen Datenverarbeitung sind die Verpflichtungen von AWS als Datenauftragsverarbeiter dargelegt.

AWS als Datenverantwortlicher

Wenn AWS personenbezogene Daten erhebt und die Zwecke und Verfahren für ihre Verarbeitung bestimmt, agiert das Unternehmen als Datenverantwortlicher. Wenn AWS z. B. Kontoinformationen für die Kontoregistrierung, die Verwaltung und den Zugriff auf Services oder Kontaktinformationen für das AWS-Konto verarbeitet, um über den Kunden-Support Unterstützung anzubieten, agiert das Unternehmen als Datenverantwortlicher.

Modell zur geteilten Sicherheitszuständigkeit

Dass das System den Anforderungen an Sicherheit und Compliance entspricht, liegt in der Verantwortung von AWS und dem Kunden. Wenn Kunden ihre Computersysteme und Daten in die Cloud verlagern, werden die Verantwortlichkeiten hinsichtlich der Sicherheit zwischen dem Kunden und dem Cloud-Serviceanbieter geteilt. Wenn Kunden in die AWS Cloud wechseln, ist AWS für den Schutz der globalen Infrastruktur verantwortlich, auf der alle in der AWS Cloud angebotenen Services betrieben werden. Bei abstrakten Services wie Amazon S3 und Amazon DynamoDB ist AWS auch für die Sicherheit des Betriebssystems und der Plattform verantwortlich. Kunden und APN-Partner, die entweder als Datenverantwortliche oder als Datenauftragsverarbeiter agieren, sind für

alles verantwortlich, was sie in der Cloud speichern oder mit ihr verbinden. Diese Differenzierung der Verantwortung wird als Sicherheit der Cloud bezeichnet, im Gegensatz zur Sicherheit in der Cloud. Dieses Modell der geteilten Verantwortung kann dazu beitragen, den Betriebsaufwand der Kunden deutlich zu verringern und ihnen die notwendige Flexibilität und Kontrolle für die Bereitstellung ihrer Infrastruktur in der AWS Cloud zu bieten. Weitere Informationen finden Sie im AWS-Modell der geteilten Verantwortung.

Die DSGVO ändert nichts an dem AWS-Modell der geteilten Verantwortung, das für Kunden und APN-Partner, die sich auf die Nutzung von Cloud-Computing-Services konzentrieren, weiterhin relevant ist. Das Modell der geteilten Verantwortung ist ein nützlicher Ansatz, um die unterschiedlichen Verantwortlichkeiten von AWS (als Datenauftragsverarbeiter oder untergeordneter Datenauftragsverarbeiter) und Kunden oder APN-Partnern (als Datenverantwortliche oder Datenauftragsverarbeiter) im Rahmen der DSGVO darzustellen.

Striktes Compliance-Framework und hohe Sicherheitsstandards

Gemäß der DSGVO müssen geeignete technische und organisatorische Maßnahmen „… die Fähigkeit [beinhalten], die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen“ ebenso wie zuverlässige Wiederherstellungs-, Test- und allgemeine Risikomanagementprozesse.

AWS-Compliance-Programm

AWS hat stets hohe Anforderungen an die Sicherheit und Compliance bei den globalen Tätigkeitsfeldern. Die Sicherheit ist seit jeher unsere oberste Priorität, sozusagen die Aufgabe, die vor allen anderen zu erledigen ist. AWS unterzieht sich regelmäßig unabhängigen Bescheinigungsprüfungen durch Dritte, um sicherzustellen, dass die Kontrollaktivitäten wie beabsichtigt funktionieren. Genauer gesagt wird AWS anhand einer Vielzahl globaler und regionaler Sicherheits-Frameworks geprüft, die von Region und Branche abhängen. Derzeit nimmt AWS an über 50 verschiedenen Prüfprogrammen teil.

Die Ergebnisse dieser Prüfungen werden von der Bewertungsstelle dokumentiert und allen AWS-Kunden über AWS Artifact zur Verfügung gestellt. AWS Artifact ist ein kostenloses Self-Service-Portal für den On-Demand-Zugriff auf AWS-Compliance-Berichte. Wenn neue Berichte veröffentlicht werden, sind sie in AWS Artifact verfügbar, sodass Kunden mit sofortigem Zugriff auf neue Berichte jederzeit über die Sicherheit und Compliance von AWS im Bilde sind.

Kunden profitieren von international anerkannten Zertifizierungen und Akkreditierungen, die unsere Compliance mit strikten internationalen Standards unter Beweis stellen. Auf der Liste finden sich beispielsweise ISO 27017 für die Cloud-Sicherheit, ISO 27018 für den Datenschutz in der Cloud, SOC 1, SOC 2 und SOC 3, PCI DSS Level 1 und weitere. AWS unterstützt seine Kunden bei der Einhaltung regionaler Sicherheitsstandards, etwa des Common Cloud Computing Controls Catalogue (C5) des BSI, ein von der Bundesregierung unterstütztes Prüfungsschema.

Weitere Informationen zu den AWS-Zertifizierungsprogrammen, Berichten und Bescheinigungen von Drittanbietern finden Sie unter AWS-Compliance-Programme. Servicespezifische Informationen finden Sie unter AWS-Services in Scope.

Cloud Computing Compliance Controls Catalog (Anforderungskatalog Cloud Computing)

Cloud Computing Compliance Controls Catalog (C5) ist ein von der Bundesregierung unterstütztes Prüfungsschema, das in Deutschland durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgestellt wurde. Anhand des Prüfschemas sollen Organisationen im Rahmen des Eckpunktepapiers Sicherheitsempfehlungen für Cloud-Computing-Anbieter der deutschen Bundesregierung ihre Betriebssicherheit gegen weit verbreitete Cyber-Angriffe unter Beweis stellen.

Die technischen und organisatorischen Maßnahmen des Datenschutzes und die Maßnahmen zur Informationssicherheit zielen auf die Datensicherheit ab, um Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten. C5 definiert Sicherheitsanforderungen, die auch für den Datenschutz relevant sein können. AWS-Kunden und deren Compliance-Berater können das C5-Prüfungsschema als Ressource nutzen, um den Umfang der AWS-Sicherheitsmaßnahmen sowie der ihnen von AWS zur Verfügung gestellten IT-Sicherheitsservices zu verstehen. C5 baut auf dem IT-Grundschutz nach ISO 27001 auf und stellt ein vergleichbares IT-Sicherheitsäquivalent mit zusätzlichen Cloud-spezifischen Kontrollfunktionen dar.

C5 bietet weitere Kontrollfunktionen, die Informationen zum Datenspeicherort, der Servicebereitstellung, dem Gerichtsstand, den existierenden Zertifizierungen, den Offenlegungsverpflichtungen von Informationen und eine ausführliche Beschreibung der Services enthalten. Mittels dieser Informationen können Sie bewerten, wie rechtlichen Vorgaben (z. B. zum Datenschutz), Ihren eigenen Richtlinien oder dem Bedrohungsumfeld im Rahmen Ihrer Nutzung der Cloud-Computing-Services entsprochen werden kann.

Datenzugriffskontrollen

Artikel 25 der DSGVO sieht vor, dass der Verantwortliche „geeignete technische und organisatorische Maßnahmen“ treffen soll, „die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden“. Die im Folgenden benannten Verfahren zur Zugriffssteuerung von AWS können Kunden dabei helfen, diese Vorgaben zu erfüllen, indem sie nur autorisierten Administratoren, Benutzern und Anwendungen den Zugriff auf AWS-Ressourcen und -Kundendaten gewähren.

AWS Identity and Access Management

Wenn Sie ein AWS-Konto erstellen, wird automatisch ein Stammbenutzerkonto für Ihr AWS-Konto erstellt. Dieses Benutzerkonto hat vollständigen Zugriff auf sämtliche AWS-Services und -Ressourcen in Ihrem AWS-Konto. Anstatt dieses Konto für alltägliche Aufgaben zu verwenden, sollten Sie es nur zum anfänglichen Erstellen zusätzlicher Rollen und Benutzerkonten sowie für administrative Aktivitäten verwenden, die dies erfordern. AWS empfiehlt, dass Sie von Anfang an das Prinzip der geringsten Zugriffsrechte anwenden: Definieren Sie verschiedene Benutzerkonten und Rollen für verschiedene Aufgaben und geben Sie den Mindestsatz an Berechtigungen an, der für die Ausführung jeder Aufgabe erforderlich ist. Dieser Ansatz ist ein Mechanismus zur Optimierung eines in der DSGVO eingeführten Schlüsselkonzepts: Datenschutz durch Technik. AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf Ihre AWS-Ressourcen sicher steuern können.

Benutzer und Rollen definieren IAM-Identitäten mit bestimmten Berechtigungen. Ein autorisierter Benutzer kann eine IAM-Rolle übernehmen, um bestimmte Aufgaben auszuführen. Temporäre Anmeldeinformationen werden erstellt, wenn die Rolle übernommen wird. Sie können beispielsweise IAM-Rollen verwenden, um Anwendungen, die in Amazon Elastic Compute Cloud (Amazon EC2) ausgeführt werden, sicher mit temporären Anmeldeinformationen bereitzustellen, die für den Zugriff auf andere AWS-Ressourcen wie Amazon-S3-Buckets und Amazon Relational Database Service (Amazon-RDS)- oder Amazon-DynamoDB-Datenbanken erforderlich sind. In ähnlicher Weise bieten Ausführungsrollen AWS Lambda-Funktionen mit den erforderlichen Berechtigungen für den Zugriff auf andere AWS-Services und -Ressourcen, wie Amazon CloudWatch Logs für das Streaming von Protokollen oder das Lesen einer Nachricht aus einer Amazon Simple Queue Service (Amazon-SQS)-Warteschlange. Wenn Sie eine Rolle erstellen, fügen Sie ihr Richtlinien hinzu, um Autorisierungen zu definieren.

Um Kunden bei der Überwachung von Ressourcenrichtlinien und der Identifizierung von Ressourcen mit öffentlichem oder kontoübergreifendem Zugriff, den sie möglicherweise nicht beabsichtigen, zu unterstützen, kann IAM Access Analyzer aktiviert werden, um umfassende Ergebnisse zu generieren, die Ressourcen identifizieren, auf die von außerhalb eines AWS-Kontos zugegriffen werden kann. IAM Access Analyzer überprüft die Ressourcenrichtlinien auf der Grundlage von mathematischer Logik und Inferenzen, um die von den Richtlinien zugelassenen Zugriffspfade zu ermitteln. IAM Access Analyzer prüft durchgehend auf neue oder aktualisierte Richtlinien und analysiert Berechtigungen, die mit Richtlinien für IAM-Rollen, aber auch für Serviceressourcen wie Amazon-S3-Buckets, AWS Key Management Service (AWS KMS)-Schlüssel, Amazon-SQS-Warteschlangen und Lambda-Funktionen erteilt wurden.

Access Analyzer for S3 benachrichtigt Sie, wenn Buckets so konfiguriert sind, dass jedem im Internet oder anderen AWS-Konten, einschließlich AWS-Konten außerhalb Ihrer Organisation, Zugriff gewährt wird. Wenn Sie einen gefährdeten Bucket in Access Analyzer for Amazon S3 überprüfen, können Sie den gesamten öffentlichen Zugriff auf den Bucket mit einem einzigen Klick blockieren. AWS empfiehlt, den gesamten Zugriff auf Ihre Buckets zu blockieren, es sei denn, Sie benötigen öffentlichen Zugriff, um einen bestimmten Anwendungsfall zu unterstützen. Bevor Sie den gesamten öffentlichen Zugriff blockieren, stellen Sie sicher, dass Ihre Anwendungen ohne öffentlichen Zugriff weiterhin ordnungsgemäß funktionieren. Weitere Informationen finden Sie unter Verwenden von Amazon S3 zum Blockieren des öffentlichen Zugriffs.

IAM stellt auch Informationen zum letzten Zugriff bereit, damit Sie nicht verwendete Berechtigungen identifizieren und sie aus den zugehörigen Prinzipalen entfernen können. Mithilfe der Informationen zum letzten Zugriff können Sie Ihre Richtlinien verfeinern und nur den Zugriff auf die Services und Aktionen gewähren, die benötigt werden. Dies trägt dazu bei, die bewährten Methoden der geringsten Zugriffsrechte besser zu befolgen und anzuwenden. Sie können Informationen zum letzten Zugriff für Entitäten oder Richtlinien anzeigen, die in IAM oder in einer gesamten AWS Organizations-Umgebung vorhanden sind.

Tokens für den vorübergehenden Zugriff mit AWS STS

Sie können mit AWS Security Token Service (AWS STS) die temporären Sicherheitsanmeldeinformationen erstellen und für vertrauenswürdige Benutzer bereitstellen. Darüber wird der Zugriff auf Ihre AWS-Ressourcen gewährt. Temporäre Sicherheitsanmeldeinformationen funktionieren fast genauso wie die langfristigen Zugriffsschlüssel-Anmeldeinformationen, die Sie Ihren IAM-Benutzern zur Verfügung stellen, mit folgenden Unterschieden:

- Temporäre Sicherheitsanmeldeinformationen sind für den kurzfristigen Gebrauch bestimmt. Sie können festlegen, wie lange sie gültig sind, von 15 Minuten bis zu maximal 12 Stunden. Nachdem temporäre Anmeldeinformationen abgelaufen sind, erkennt AWS sie nicht und verweigert den Zugriff von API-Anforderungen, die mit diesen Anmeldeinformationen gestellt werden.
- Temporäre Sicherheitsanmeldeinformationen werden nicht im Benutzerkonto gespeichert. Stattdessen werden sie dynamisch generiert und dem Benutzer auf Anforderung zur Verfügung gestellt. Wenn (oder bevor) temporäre Sicherheitsanmeldeinformationen abgelaufen sind, kann ein Benutzer neue Anmeldeinformationen anfordern, sofern dieser Benutzer über die entsprechenden Berechtigungen verfügt.

Diese Unterschiede bieten die folgenden Vorteile, wenn Sie temporäre Anmeldeinformationen verwenden:

- Sie müssen keine dauerhaften AWS-Anmeldeinformationen verteilen oder in Anwendungen integrieren.
- Temporäre Anmeldeinformationen bilden die Grundlage für den Rollen- und Identitätsverbund. Sie können Benutzern den Zugriff auf Ihre AWS-Ressourcen erteilen, indem Sie eine temporäre AWS-Identität für sie definieren.
- Temporäre Sicherheitsanmeldeinformationen haben eine begrenzte anpassbare Lebensdauer. Aus diesem Grund müssen Sie diese nicht rotieren oder explizit widerrufen, wenn sie nicht mehr benötigt werden. Nachdem die temporären Anmeldeinformationen abgelaufen sind, können sie nicht erneut verwendet werden. Sie können angeben, wie lange die Anmeldeinformationen maximal gültig sind.

Multi-Faktor-Authentifizierung

Für zusätzliche Sicherheit können Sie eine Zwei-Faktor-Authentifizierung zu Ihrem AWS-Konto und IAM-Benutzern hinzufügen. Wenn die Multi-Faktor-Authentifizierung (MFA) aktiviert ist, werden Sie bei der Anmeldung bei der AWS-Managementkonsole aufgefordert, Ihren Benutzernamen und Ihr Passwort (der erste Faktor) sowie eine Authentifizierungsantwort von Ihrem AWS-MFA-Gerät (der zweite Faktor) einzugeben. Sie können die MFA für Ihr AWS-Konto und für einzelne IAM-Benutzer aktivieren, die Sie in Ihrem Konto erstellt haben. Sie können die MFA auch verwenden, um den Zugriff auf AWS-Service-APIs zu kontrollieren.

Sie können beispielsweise eine Richtlinie definieren, die vollen Zugriff auf alle AWS-API-Operationen in Amazon EC2 ermöglicht, aber explizit den Zugriff auf bestimmte API-Operationen – wie

`StopInstances` und `TerminateInstances` – verweigert, wenn der Benutzer nicht mit der MFA authentifiziert ist.

```
        {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Sid”: “AllowAllActionsForEC2”,
                “Effect”: “Allow”,
                “Action”: “ec2:*”,
                “Resource”: “*”
             },
            {
                “Sid”: “DenyStopAndTerminateWhenMFAIsNotPResent”,
                “Effect”: “Deny”,
                “Action”: [
                    “ec2:StopInstances”,
                    “ec2:TerminateInstances”
               ],
               “Resource”: “*”,
               “Conditions”: {
                   “BoolIfExists”: {“aws:MultiFactorAuthPresent”:false}
                }
            }
       }
}
```

Um Ihren Amazon-S3-Buckets eine zusätzliche Sicherheitsebene hinzuzufügen, können Sie MFA Delete konfigurieren, das eine zusätzliche Authentifizierung erfordert, um den Versioning-Status eines Buckets zu ändern und eine Objektversion dauerhaft zu löschen. MFA Delete bietet zusätzliche Sicherheit für den Fall, dass Ihre Sicherheitsanmeldeinformationen nicht mehr vertrauenswürdig sind.

Um MFA Delete zu nutzen, verwenden Sie ein Hardwaregerät oder ein virtuelles MFA-Gerät, um einen Authentifizierungscode zu generieren. Auf der Seite der Multi-Faktor-Authentifizierung finden Sie eine Liste der unterstützten Hardware oder virtuellen MFA-Geräte.

Zugriff auf AWS-Ressourcen

Um den detaillierten Zugriff auf Ihre AWS-Ressourcen zu implementieren, können Sie einzelnen Personen unterschiedliche Berechtigungsebenen für verschiedene Ressourcen gewähren. Sie können beispielsweise nur einigen Benutzern vollständigen Zugriff auf Amazon EC2, Amazon S3, DynamoDB, Amazon Redshift und andere AWS-Services gewähren.

Anderen Benutzern können Sie Lesezugriff auf nur einige Amazon-S3-Buckets, die Berechtigung zum Verwalten von nur einigen Amazon-EC2-Instances oder Zugriff auf nur Ihre Abrechnungsdaten gewähren.

Die folgende Richtlinie ist ein Beispiel für eine Methode, die Sie verwenden können, um alle Aktionen in einem bestimmten Amazon-S3-Bucket zuzulassen und explizit den Zugriff auf jeden AWS-Service zu verweigern, der nicht Amazon S3 ist.

```
      {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Effect”: “Allow”,
                “Action”: “s3:*”,
                “Resource”: [
                     “arn:aws:s3:::bucket-name”,
                     “arn:aws:s3:::bucket-name/*”
                 ],
              },
              {
                “Effect”: “Deny”,
                “NotAction”: “s3:*”,
                “NotResource”: [
                     “arn:aws:s3:::bucket-name”,
                     “arn:aws:s3:::bucket-name/*”
                 ]
               }
            ]
}
```

Sie können eine Richtlinie an ein Benutzerkonto oder eine Rolle anhängen. Weitere Beispiele für IAM-Richtlinien finden Sie unter Beispiele für identitätsbasierte IAM-Richtlinien.

Definieren von Grenzen für den Zugang zu regionalen Services

Als Kunde bleiben Sie der Eigentümer Ihrer Inhalte und können sich entscheiden, welche AWS-Services Ihre Inhalte verarbeiten, speichern und hosten können. AWS greift niemals auf Ihre Inhalte zu oder verwendet diese, ohne Sie vorher um Erlaubnis gebeten zu haben. Auf der Grundlage des Modells der geteilten Verantwortung wählen Sie die AWS-Regionen, in denen Ihre Inhalte gespeichert sind, sodass Sie die AWS-Services an den Orten Ihrer Wahl entsprechend Ihren spezifischen geographischen Anforderungen nutzen können. Wenn Sie beispielsweise sicherstellen möchten, dass sich Ihre Inhalte nur in Europa befinden, können Sie AWS-Services ausschließlich in einer der europäischen AWS-Regionen bereitstellen.

IAM-Richtlinien bieten einen einfachen Mechanismus, um den Zugriff auf Services in bestimmten Regionen zu beschränken. Sie können den IAM-Richtlinien, die Ihren IAM-Prinzipalen angehängt sind, eine globale Bedingung (`aws:RequestedRegion`) hinzufügen, um dies für alle AWS-Services durchzusetzen. Die folgende Richtlinie verwendet beispielsweise das `NotAction`-Element mit dem `Deny`-Effekt, der explizit den Zugriff auf alle Aktionen verweigert, die nicht in der Anweisung aufgeführt sind, wenn die angeforderte Region nicht europäisch ist. Aktionen in den Services CloudFront, IAM, Amazon Route 53 und AWS Support sollten nicht verweigert werden, da dies beliebte globale AWS-Services sind.

```
{
   “Version”: “2012-10-17”,
   “Statement”: [
       {
          “Sid”: “DenyAllOutsideRequestedRegions”,
          “Effect”: “Deny”,
          “NotAction”: [
               “cloudfront:*”,
               “iam:*”,
               ”route53:*”,
               “support:*”
           ],
           “Resource”: “*”,
           “Condition”: {
              “StringNotLike”: {
                  “aws:RequestedRegion”: [
                        “eu-*”
                  ]
               }
```

```
                    }
                }
            ]
}
```

Dieses Beispiel für eine IAM-Richtlinie kann auch als Service Control Policy (SCP, Service-Kontrollrichtlinie) in AWS Organizations implementiert werden, die die Berechtigungsgrenzen definiert, die auf bestimmte AWS-Konten oder Organizational Units (OUs, Organisationseinheiten) innerhalb einer Organisation angewendet werden. Auf diese Weise können Sie den Benutzerzugriff auf regionale Services in komplexen Umgebungen mit mehreren Konten steuern.

Funktionen zur geografischen Einschränkung liegen für neu eingeführte Regionen vor. Regionen, die nach dem 20. März 2019 eingeführt wurden, sind standardmäßig deaktiviert. Sie müssen diese Regionen aktivieren, bevor Sie sie verwenden können. Wenn eine AWS-Region standardmäßig deaktiviert ist, können Sie mithilfe der AWS-Managementkonsole die Region aktivieren und deaktivieren. Indem Sie AWS-Regionen aktivieren und deaktivieren, können Sie steuern, ob Benutzer in Ihrem AWS-Konto auf Ressourcen in dieser Region zugreifen können. Weitere Informationen finden Sie unter Verwalten von AWS-Regionen.

Steuern des Zugriffs auf Webanwendungen und mobile Apps

AWS bietet Services für die Verwaltung der Datenzugriffskontrolle in Kundenanwendungen. Wenn Sie Benutzeranmelde- und Zugriffskontrollfunktionen zu Ihren Webanwendungen und mobilen Apps hinzufügen müssen, können Sie Amazon Cognito verwenden. Amazon-Cognito-Benutzerpools bieten ein sicheres Benutzerverzeichnis, das für Hunderte von Millionen Benutzern skaliert werden kann. Um die Identität Ihrer Benutzer zu schützen, können Sie die Multi-Faktor-Authentifizierung (MFA) für Ihre Benutzerpools verwenden. Sie können auch die adaptive Authentifizierung mit ihrem risikobasierten Modell verwenden, um zu prognostizieren, wann Sie möglicherweise einen anderen Authentifizierungsfaktor benötigen.

Mit Amazon-Cognito-Identitätspools (Verbundidentitäten) können Sie sehen, wer auf Ihre Ressourcen zugegriffen hat und woher der Zugriff stammt (mobile App oder Webanwendung). Sie können diese Informationen verwenden, um IAM-Rollen und -Richtlinien zu erstellen, die den Zugriff auf eine Ressource basierend auf dem Typ des Zugriffsursprungs (mobile App oder Webanwendung) und des Identitätsanbieters erlauben oder verweigern.

Überwachung und Protokollierung

Artikel 30 der DSGVO sieht vor, dass „... jeder Verantwortliche und gegebenenfalls sein Vertreter ein Verzeichnis aller Verarbeitungstätigkeiten führen, die ihrer Verantwortung unterliegen“. Dieser Artikel enthält auch Details darüber, welche Informationen aufgezeichnet werden müssen, wenn Sie die Verarbeitung aller personenbezogenen Daten überwachen. Verantwortliche und Auftragsverarbeiter müssen außerdem Benachrichtigungen über Sicherheitsverletzungen rechtzeitig senden, sodass es wichtig ist, Vorfälle schnell zu erkennen. Zur Erfüllung dieser Auflagen bietet Ihnen AWS die folgenden Überwachungs- und Protokollierungsservices.

Verwalten und Konfigurieren von Komponenten mit AWS Config

AWS Config bietet eine detaillierte Ansicht der Konfiguration vieler Arten von AWS-Ressourcen in Ihrem AWS-Konto. Hierzu zählt auch, wie die Ressourcen zueinander in Verbindung stehen und wie sie in der Vergangenheit konfiguriert wurden. So können Sie erkennen, wie sich die Konfigurationen und Beziehungen mit der Zeit ändern.

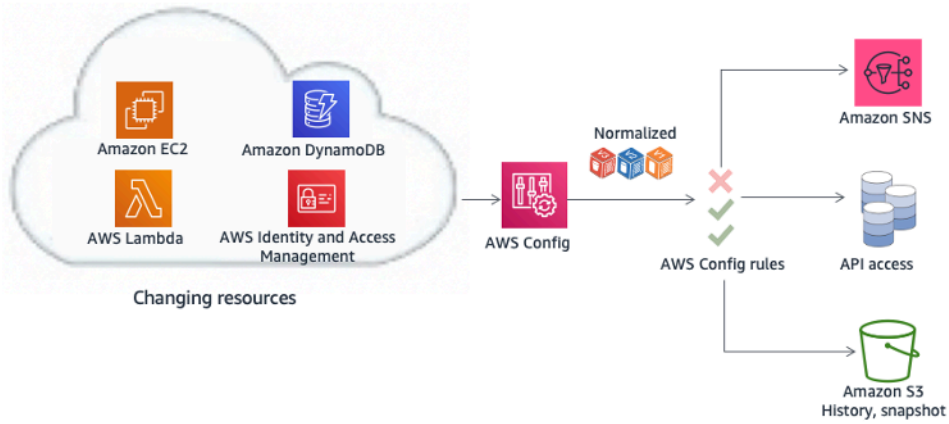

Abbildung 1 – Überwachen der Konfigurationsänderungen im Laufe der Zeit mit AWS Config

Eine AWS-Ressource ist eine Einheit, mit der Sie in AWS arbeiten können, etwa eine EC2-Instance, ein Amazon Elastic Block Store (Amazon-EBS)-Volume, eine Sicherheitsgruppe oder eine Amazon Virtual Private Cloud (Amazon VPC). Eine vollständige Liste der AWS-Ressourcen, die von AWS Config unterstützt werden, finden Sie im Artikel zu den unterstützten AWS-Ressourcentypen.

Mit AWS Config können Sie folgende Aktionen ausführen:

- Ihre AWS-Ressourcenkonfigurationen auswerten, um sicherzustellen, dass die Einstellungen korrekt sind.

- Einen Snapshot der aktuellen Konfigurationen der unterstützten Ressourcen, die Ihrem AWS-Konto zugeordnet sind, anfertigen.
- Konfigurationen von einer oder mehreren Ressourcen in Ihrem Konto abrufen.
- Historische Konfigurationen von einer oder mehreren Ressourcen abrufen.
- Sich eine Benachrichtigung zusenden lassen, wenn eine Ressource erstellt, geändert oder gelöscht wird.
- Beziehungen zwischen Ressourcen anzeigen. Beispielsweise lassen sich alle Ressourcen derselben Sicherheitsgruppe abfragen.

Compliance-Prüfung und -Sicherheitsanalyse

Mit AWS CloudTrail können Sie die AWS-Kontoaktivität kontinuierlich überwachen. Ein Verlauf der AWS-API-Aufrufe für Ihr Konto wird erfasst, einschließlich API-Aufrufen über die AWS-Managementkonsole, AWS SDKs, Befehlszeilen-Tools und die AWS-Services auf höherer Ebene. Sie können identifizieren, welche Benutzer und Konten AWS APIs für Services, die CloudTrail unterstützen, aufgerufen haben, die Quell-IP-Adresse, von der die Aufrufe ausgingen, und wann die Aufrufe aufgetreten sind. Sie können CloudTrail mithilfe der API in Anwendungen integrieren, die Trail-Erstellung für Ihre Organisation automatisieren, den Status Ihrer Trails prüfen und steuern, wie Administratoren die CloudTrail-Protokollierung aktivieren bzw. deaktivieren.

CloudTrail-Protokolle können aus mehreren Regionen und mehreren AWS-Konten in einem einzigen Amazon-S3-Bucket zusammengefasst werden. AWS empfiehlt, dass Sie Protokolle – insbesondere AWS CloudTrail-Protokolle – in einen Amazon-S3-Bucket mit eingeschränktem Zugriff in einem AWS-Konto schreiben, das für die Protokollierung vorgesehen ist (Protokollarchiv). Die Berechtigungen für den Bucket sollten das Löschen der Protokolle verhindern und sie sollten auch im Ruhezustand mithilfe der serverseitigen Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (SSE-S3) oder von AWS KMS verwalteten Schlüsseln (SSE-KMS) verschlüsselt werden. Die Integritätsvalidierung für CloudTrail-Protokolldateien kann verwendet werden, um festzustellen, ob eine Protokolldatei geändert, gelöscht oder nicht verändert wurde, nachdem sie von CloudTrail übermittelt wurde. Diese Funktion wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hash-Funktion und SHA-256 mit RSA für digitale Signaturen. Dadurch ist es computertechnisch schwierig, CT-Protokolldateien unerkannt zu ändern, zu löschen oder zu fälschen. Sie können die AWS-Befehlszeilenschnittstelle (AWS CLI) verwenden, um die Dateien an dem Speicherort zu überprüfen, an den CloudTrail sie übermittelt hat.

In einem Amazon-S3-Bucket aggregierte CloudTrail-Protokolle können für Prüfungszwecke oder zur Fehlerbehebung analysiert werden. Sobald die Protokolle zentralisiert sind, können Sie diese in Security Information and Event Management (SIEM)-Lösungen integrieren oder AWS-Services wie Amazon Athena oder CloudTrail Insights nutzen, um sie zu analysieren und mit Amazon-QuickSight-Dashboards zu visualisieren. Sobald Sie CloudTrail-Protokolle zentralisiert haben, können Sie dasselbe Protokollarchiv-Konto auch verwenden, um Protokolle aus anderen Quellen wie CloudWatch Logs und AWS-Load-Balancern zu zentralisieren.

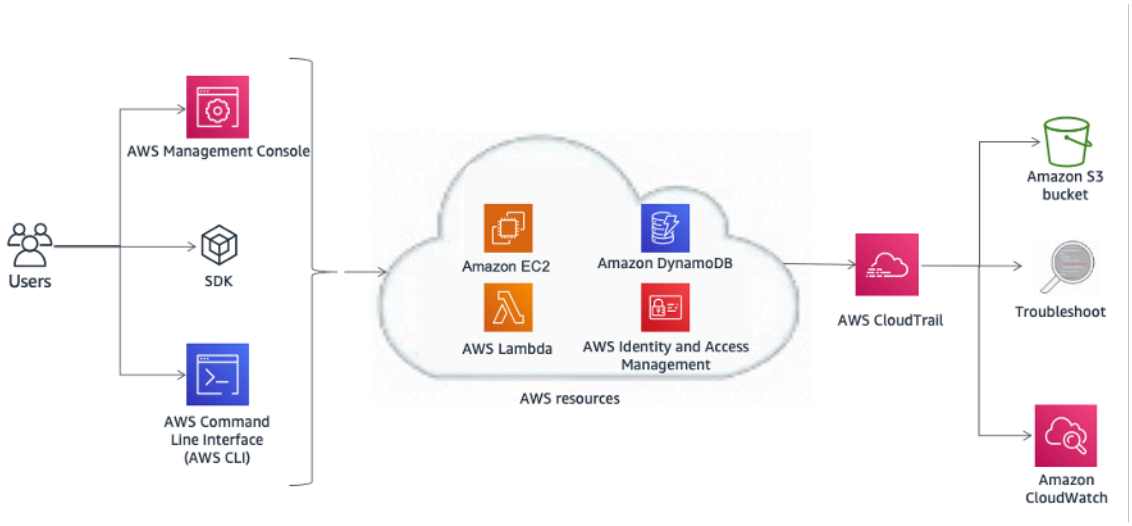

Abbildung 2 – Beispielarchitektur für die Compliance-Prüfung und -Sicherheitsanalyse mit AWS CloudTrail

AWS CloudTrail-Protokolle können auch vorkonfigurierte Amazon-CloudWatch-Ereignisse auslösen. Sie können diese Ereignisse verwenden, um Benutzer oder Systeme darüber zu informieren, dass ein Ereignis eingetreten ist, oder um Korrekturmaßnahmen durchzuführen. Wenn Sie beispielsweise Aktivitäten auf Ihren Amazon-EC2-Instances überwachen möchten, können Sie eine CloudWatch-Ereignisregel erstellen. Wenn eine bestimmte Aktivität auf der Amazon-EC2-Instance stattfindet und das Ereignis in den Protokollen erfasst wird, löst die Regel eine AWS Lambda-Funktion aus, die eine Benachrichtigungs-E-Mail über das Ereignis an den Administrator sendet. (Siehe Abbildung 3.) Die E-Mail enthält Details wie den Zeitpunkt des Ereignisses, welcher Benutzer die Aktion ausgeführt hat, Amazon-EC2-Details und vieles mehr. Im folgenden Diagramm wird die Architektur der Ereignisbenachrichtigung dargestellt.

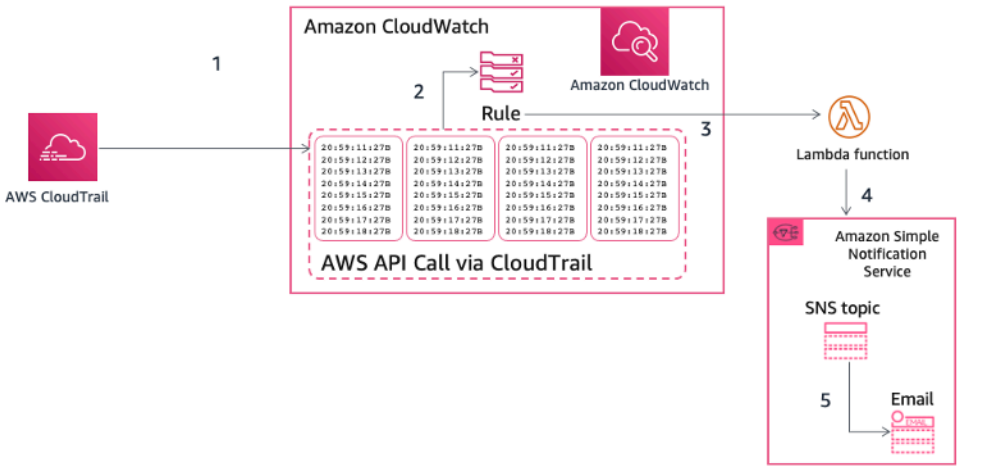

Abbildung 3 – Beispiel einer AWS CloudTrail-Ereignisbenachrichtigung

Erfassen und Verarbeiten von Protokollen

CloudWatch Logs kann verwendet werden, um Ihre Protokolldateien aus Amazon-EC2-Instances, AWS CloudTrail, Route 53 und anderen Quellen zu überwachen, zu speichern und zu öffnen. Weitere Informationen finden Sie auf der Dokumentationsseite AWS-Services, die Protokolle in CloudWatch Logs veröffentlichen.

Zu den Protokollinformationen gehören beispielsweise:

- Individuell festgelegte Protokollierung des Zugriffs auf Amazon-S3-Objekte
- Detaillierte Informationen über Datenströme im Netzwerk durch VPC-Flow Logs
- Regelbasierte Konfigurationsprüfungen und -aktionen mit AWS Config-Regeln
- Filterung und Nachverfolgung von HTTP-Zugriff auf Anwendungen mit Web Application Firewall (WAF)-Funktionen in CloudFront

Benutzerdefinierte Anwendungsmetriken und -protokolle können auch in CloudWatch Logs veröffentlicht werden, indem der CloudWatch-Agent auf Amazon-EC2-Instances oder lokalen Servern installiert wird.

Protokolle können mithilfe von CloudWatch Logs Insights interaktiv analysiert werden, wobei Abfragen durchgeführt werden, damit Sie effizienter und effektiver auf betriebliche Probleme reagieren können.

CloudWatch-Protokolle können durch Konfigurieren von Abonnementfiltern nahezu in Echtzeit verarbeitet und an andere Services wie einen Amazon OpenSearch Service (OpenSearch Service)-Cluster, einen Amazon-Kinesis-Stream, einen Amazon-Kinesis-Data-Firehose-Stream oder Lambda zur benutzerdefinierten Verarbeitung, Analyse oder zum Laden in andere Systeme übermittelt werden.

CloudWatch-Metrikfilter können verwendet werden, um Muster zu definieren, nach denen in Protokolldaten gesucht werden soll, sie in numerische CloudWatch-Metriken umzuwandeln und Alarme basierend auf Ihren Geschäftsanforderungen einzurichten. Wenn Sie beispielsweise der AWS-Empfehlung folgen, den Stammbenutzer nicht für alltägliche Aufgaben zu verwenden, ist es möglich, einen bestimmten CloudWatch-Metrikfilter in einem CloudTrail-Protokoll (an CloudWatch Logs übermittelt) einzurichten, um eine benutzerdefinierte Metrik zu erstellen und einen Alarm zu konfigurieren, um die relevanten Personen zu benachrichtigen, wenn Stamm-Anmeldeinformationen für den Zugriff auf Ihr AWS-Konto verwendet werden.

Protokolle wie Amazon-S3-Serverzugriffsprotokolle, Elastic-Load-Balancing-Zugriffsprotokolle, VPC-Flow-Protokolle und AWS Global Accelerator-Flow-Protokolle können direkt an einen Amazon-S3-Bucket übermittelt werden. Wenn Sie beispielsweise Serverzugriffsprotokolle von Amazon Simple Storage Service aktivieren, erhalten Sie detaillierte Informationen zu den Anfragen, die an Ihren Amazon-S3-Bucket gestellt wurden. Ein Zugriffsprotokoll-Datensatz enthält Details über jede Anfrage, wie beispielsweise den Anfragetyp, die in der Anfrage angegebenen Ressourcen sowie Uhrzeit und Datum der Anfrage. Weitere Informationen zu den Inhalten einer Protokollmeldung finden Sie im Abschnitt Serverzugriff-Protokollformat von Amazon Simple Storage Service im Entwicklerhandbuch zu Amazon Simple Storage Service. Serverzugriffsprotokolle sind für viele Anwendungen nützlich, da sie Bucket-Eigentümern Einblick in die Art der Anfragen bieten, die von Clients erstellt werden, die sich ihrer Kontrolle entziehen. Standardmäßig erfasst Amazon S3 keine Servicezugriffsprotokolle. Wenn Sie die Protokollierung jedoch aktivieren, liefert Amazon S3 normalerweise innerhalb weniger Stunden Zugriffsprotokolle an Ihren S3-Bucket. Wenn Sie eine schnellere Bereitstellung benötigen oder Protokolle an mehrere Ziele liefern müssen, sollten Sie CloudTrail-Protokolle oder eine Kombination aus CloudTrail-Protokollen und Amazon S3 verwenden. Protokolle können im Ruhezustand verschlüsselt werden, indem die standardmäßige Objektverschlüsselung im Ziel-Bucket konfiguriert wird. Die Verschlüsselung der Objekte erfolgt serverseitig mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) oder Kundenmasterschlüsseln (CMKs), die in AWS Key Management Service (AWS KMS) gespeichert sind.

In einem Amazon-S3-Bucket gespeicherte Protokolle können mit Amazon Athena abgefragt und analysiert werden. Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten in S3 mit Standard-SQL analysieren können. Sie können Athena nutzen, um Ad-hoc-Abfragen mit ANSI SQL

durchzuführen, ohne dafür die Daten aggregieren oder in Athena laden zu müssen. Athena kann unstrukturierte, halbstrukturierte und strukturierte Datensätze verarbeiten und lässt sich zur einfachen Visualisierung in Amazon QuickSight integrieren.

Protokolle sind auch eine nützliche Informationsquelle für die automatisierte Bedrohungserkennung. Amazon GuardDuty ist ein Service zur kontinuierlichen Sicherheitsüberwachung, der Ereignisse aus verschiedenen Quellen analysiert und verarbeitet, z. B. VPC Flow Logs, CloudTrail-Verwaltungsereignisprotokolle, CloudTrail-Amazon-S3-Datenereignisprotokolle und DNS-Protokolle. Er verwendet Bedrohungsdaten, z. B. Listen bösartiger IP-Adressen und Domänen, ebenso wie maschinelles Lernen, um unerwartete und potenziell nicht autorisierte bösartige Aktivitäten in Ihrer AWS-Umgebung zu identifizieren. Wenn Sie GuardDuty in einer Region aktivieren, wird sofort mit der Analyse Ihrer CloudTrail-Ereignisprotokolle begonnen. Er nutzt CloudTrail-Verwaltungs- und Amazon S3-Datenereignisse direkt aus CloudTrail über einen unabhängigen und doppelten Ereignisstrom.

Erkennen und Schützen von Daten in großem Umfang mit Amazon Macie

Artikel 32 der DSGVO sieht vor, dass „… der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen sollen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, unter anderem: […]

(b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und Services dauerhaft sicherzustellen;

[…]

(d) ein Verfahren zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“.

Ein fortlaufender Datenklassifizierungsprozess ist entscheidend für die Anpassung der Sicherheitsdatenverarbeitung an die Arten von Daten. Wenn Ihre Organisation sensible Daten verwaltet, überwachen Sie, wo sie sich befinden, schützen Sie sie ordnungsgemäß und stellen Sie Nachweise darüber bereit, dass Sie Datensicherheit und Datenschutz wie erforderlich durchsetzen, um gesetzliche Compliance-Anforderungen zu erfüllen. Um Kunden zu helfen, ihre sensiblen Daten in großem Umfang zu identifizieren und zu schützen, bietet AWS Amazon Macie an, einen vollständig verwalteten Service zur Datensicherheit und zum Datenschutz. Dieser verwendet Musterabgleich- und Machine-Learning-Modelle zur Erkennung von persönlich identifizierbaren Informationen (engl. „personally identifiable information“, kurz: PII), um sensible Daten, die in S3-

Buckets gespeichert sind, zu ermitteln und zu schützen. Amazon Macie scannt diese Buckets und stellt eine Datenkategorisierung dieser mithilfe von verwalteten Datenbezeichnern zur Verfügung, die so konzipiert sind, dass sie mehrere Kategorien sensibler Daten erkennen. Macie kann PII wie vollständiger Name, E-Mail-Adresse, Geburtsdatum, nationale Identifikationsnummer, Steueridentifikations- oder Referenznummer und mehr erkennen. Der Kunde kann benutzerdefinierte Datenbezeichner definieren, die die jeweiligen Szenarien seiner Organisation widerspiegeln (z. B. Kunden-Kontonummern oder interne Datenklassifizierung).

Amazon Macie wertet das Objekt in den Buckets kontinuierlich aus und liefert automatisch eine Zusammenfassung der Ergebnisse (Abbildung 4) für alle entdeckten unverschlüsselten oder öffentlich zugänglichen Daten, die mit der definierten Datenkategorie übereinstimmen. Diese Daten können Warnungen für unverschlüsselte, öffentlich zugängliche Objekte oder Buckets enthalten, die mit AWS-Konten außerhalb der von Ihnen in AWS Organizations definierten Konten geteilt werden. Amazon Macie ist in anderen AWS-Services integriert, z. B. AWS Security Hub, um umsetzbare Sicherheitsergebnisse zu generieren und eine automatische und reaktive Aktion auf das Ergebnis zu ermöglichen (Abbildung 5).

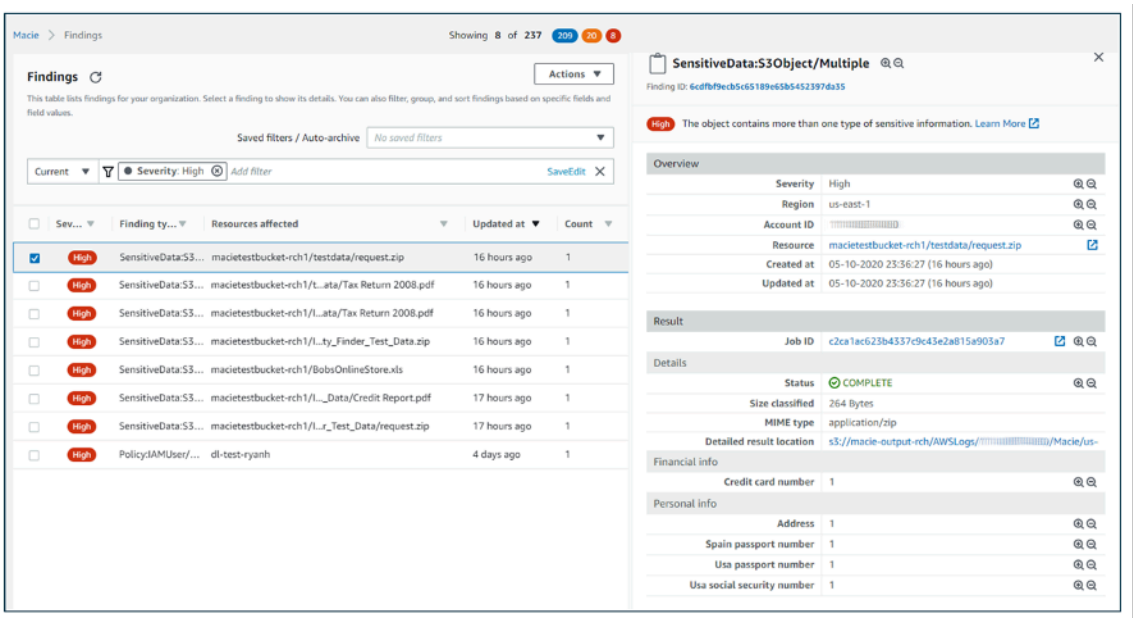

Abbildung 4 – Beispiel für Datenprüfungen und Ergebnisse

Zentrale Sicherheitsverwaltung

Viele Organisationen stehen vor Herausforderungen in Bezug auf die Transparenz und die zentrale Verwaltung ihrer Umgebungen. Wenn Ihre operative Präsenz wächst, kann sich diese Herausforderung noch verschärfen, sofern Sie Ihre Sicherheitskonzepte nicht sorgfältig prüfen.

Mangelndes Wissen in Kombination mit einer dezentralen und ungleichmäßigen Verwaltung von Governance- und Sicherheitsprozessen kann Ihre Umgebung anfällig machen.

AWS bietet Tools, die Ihnen helfen, einige der schwierigsten Anforderungen an IT-Management und -Governance zu erfüllen, sowie Tools zur Unterstützung eines Ansatzes für den Datenschutz durch Technik.

AWS Control Tower bietet eine Methode zur Einrichtung und Steuerung einer neuen sicheren AWS-Umgebung mit mehreren Konten. Es automatisiert die Einrichtung einer Landing Zone, bei der es sich um eine Umgebung mit mehreren Konten handelt, die auf bewährten Entwürfen basiert, und ermöglicht die Verwaltung mit Leitlinien, die Sie aus einer vorgepackten Liste auswählen können. Leitlinien implementieren Governance-Regeln für Sicherheit, Compliance und Betrieb. AWS Control Tower stellt die Identitätsverwaltung mithilfe des AWS IAM Identity Center (IAM Identity Center)-Standardverzeichnisses bereit und ermöglicht die kontenübergreifende Prüfung mithilfe von IAM Identity Center und IAM. Es zentralisiert auch Protokolle von CloudTrail und AWS Config-Protokolle, die in Amazon S3 gespeichert sind.

AWS Security Hub ist ein weiterer Service, der die Zentralisierung unterstützt und die Transparenz einer Organisation verbessern kann. Security Hub zentralisiert und priorisiert Sicherheits- und Compliance-Ergebnisse aus allen AWS-Konten und -Services wie Amazon GuardDuty und Amazon Inspector und kann in Sicherheitssoftware von Drittpartnern integriert werden, um Ihnen zu helfen, Sicherheitstrends zu analysieren und Sicherheitsprobleme mit höchster Priorität zu identifizieren.

Amazon GuardDuty ist ein intelligenter Bedrohungserkennungsservice, mit dem Kunden ihre AWS-Konten und -Workloads sowie in Amazon S3 gespeicherte Daten genauer und einfacher überwachen und schützen können. GuardDuty analysiert Milliarden von Ereignissen in Ihren AWS-Konten aus verschiedenen Quellen, darunter AWS CloudTrail-Verwaltungsereignisse, CloudTrail-Amazon-S3-Datenereignisse, Amazon Virtual Private Cloud Flow Logs und DNS-Protokolle. So erkennt es beispielsweise ungewöhnliche API-Aufrufe, verdächtige abgehende Kommunikation mit bekanntermaßen schädlichen IP-Adressen oder möglichen Datendiebstahl, bei dem DNS-Abfragen als Transportmechanismus genutzt werden. GuardDuty ist in der Lage, genauere Ergebnisse zu liefern, indem es durch Machine Learning unterstützte Bedrohungsinformationen und Drittanbieter-Sicherheitspartner nutzt.

Amazon Inspector ist ein automatisierter Service zur Sicherheitsbewertung, über den bei der Bereitstellung von Anwendungen auf Amazon-EC2-Instances die Sicherheit sowie die Compliance erhöht werden können. Amazon Inspector prüft Anwendungen automatisch auf Lücken, Schwachstellen und Abweichungen von bewährten Methoden. Nach der Durchführung

einer Bewertung erstellt Amazon Inspector eine nach Schweregrad geordnete detaillierte Liste der Sicherheitsergebnisse.

Mit Amazon CloudWatch Events können Sie Ihr AWS-Konto einrichten, um Ereignisse an andere AWS-Konten zu senden oder ein Empfänger für Ereignisse von anderen Konten oder Organisationen zu werden. Dieser Mechanismus kann sehr nützlich sein, um kontenübergreifende Szenarien zur Reaktion auf Vorfälle zu implementieren, indem rechtzeitig Korrekturmaßnahmen ergriffen werden (z. B. durch Aufrufen einer Lambda-Funktion oder Ausführen eines Befehls auf der Amazon-EC2-Instance), wenn ein Sicherheitsvorfall eintritt.

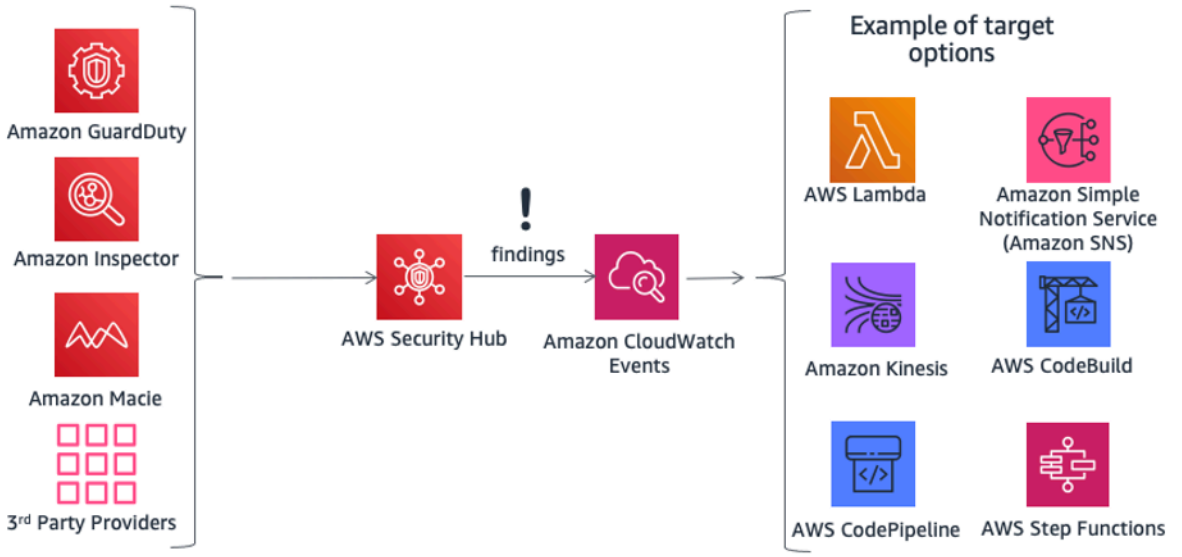

Abbildung 5 – Ergreifen von Maßnahmen mit AWS Security Hub und Amazon CloudWatch Events

AWS Organizations unterstützt Sie bei der zentralen Verwaltung und Steuerung komplexer Umgebungen. Sie können damit den Zugriff, die Compliance und die Sicherheit in einer Umgebung mit mehreren Konten steuern. AWS Organizations unterstützt Service Control Policies (SCPs, Service-Kontrollrichtlinien), die die AWS-Service-Aktionen definieren, die für bestimmte Konten oder Organizational Units (OUs, Organisationseinheiten) innerhalb einer Organisation verfügbar sind.

AWS Systems Manager bietet Ihnen Transparenz und Kontrolle über Ihre Infrastruktur auf AWS. Sie können Betriebsdaten aus mehreren AWS-Services über eine einheitliche Konsole anzeigen und Betriebsaufgaben über sie hinweg automatisieren. Sie können Informationen über die letzten API-Aktivitäten, Änderungen der Ressourcenkonfiguration, Betriebswarnungen, den Softwarebestand und den Status der Patch-Compliance erhalten. Dank der Integration mit anderen AWS-Services können Sie je nach Ihren betrieblichen Anforderungen auch Maßnahmen zu Ressourcen ergreifen, um Ihre Umgebung in einen Compliance-Status zu versetzen.

Durch die Integration von Amazon Inspector in AWS Systems Manager werden Sicherheitsbewertungen beispielsweise vereinfacht und automatisiert, da Sie den Amazon-Inspector-Agent automatisch mit Amazon Elastic Compute Cloud Systems Manager installieren können, wenn eine Amazon-EC2-Instance gestartet wird. Sie können auch automatische Korrekturen für Amazon-Inspector-Ergebnisse durchführen, indem Sie Amazon EC2 System Manager- und Lambda-Funktionen verwenden.

Schutz Ihrer Daten auf AWS

Artikel 32 der DSGVO schreibt vor, dass Organisationen „… geeignete technische und organisatorische Maßnahmen [ergreifen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: … die Pseudonymisierung und Verschlüsselung personenbezogener Daten [...]“. Darüber hinaus müssen Organisationen personenbezogene Daten vor unbefugter Weitergabe und unbefugtem Zugriff schützen“.

Die Verschlüsselung reduziert die mit der Speicherung personenbezogener Daten verbundenen Risiken, da Daten ohne den richtigen Schlüssel nicht lesbar sind. Eine gründliche Verschlüsselungsstrategie kann dazu beitragen, die Auswirkungen verschiedener Sicherheitsereignisse, einschließlich einiger Sicherheitsverletzungen, möglichst gering zu halten.

Verschlüsseln ruhender Daten

Die Verschlüsselung ruhender Daten ist für die Einhaltung gesetzlicher Vorschriften und den Datenschutz entscheidend. Dadurch soll gewährleistet werden, dass sensible Daten, die auf Datenträgern gespeichert werden, für Benutzer oder Anwendungen ohne gültige Zugriffsschlüssel nicht lesbar sind. AWS bietet mehrere Optionen für die Verschlüsselung ruhender Daten und die Verwaltung von Verschlüsselungsschlüsseln. Sie können beispielsweise das AWS Encryption SDK mit einem CMK verwenden, der in AWS KMS erstellt und verwaltet wird, um beliebige Daten zu verschlüsseln.

Verschlüsselte Daten können im Ruhezustand sicher gespeichert und nur von einer Partei mit autorisiertem Zugriff auf den CMK entschlüsselt werden. Als Ergebnis erhalten Sie vertrauliche, durch Envelope verschlüsselte Daten, Richtlinienmechanismen für die Autorisierung und authentifizierte Verschlüsselung sowie die Prüfprotokollierung über AWS CloudTrail. Einige der grundlegenden AWS-Services verfügen über integrierte Verschlüsselungsfunktionen im Ruhezustand, sodass Daten vor dem Schreiben in den nichtflüchtigen Speicher verschlüsselt werden können. So können Sie beispielsweise Amazon-EBS-Volumes verschlüsseln und Amazon-S3-Buckets für die Server-Side Encryption (SSE, serverseitige Verschlüsselung) mithilfe der AES-256-Verschlüsselung konfigurieren. Amazon S3 unterstützt auch die clientseitige Verschlüsselung, mit der Sie Daten verschlüsseln können, bevor Sie diese an Amazon S3 senden. AWS SDKs unterstützen die clientseitige Verschlüsselung, um Verschlüsselungs- und Entschlüsselungsvorgänge von Objekten zu erleichtern. Amazon RDS unterstützt auch die Transparent Data Encryption (TDE, transparente Datenverschlüsselung).

Es ist möglich, Daten in Amazon-EC2-Instance-Speichern von Linux mithilfe integrierter Linux-Bibliotheken zu verschlüsseln. Diese Methode verschlüsselt Dateien transparent und schützt so vertrauliche Daten. Anwendungen, die die Daten verarbeiten, können diese Verschlüsselung auf Datenträgerebene nicht erkennen.

Zur Verschlüsselung der Dateien in Instance-Speichern stehen zwei Methoden zur Verfügung:

- Verschlüsselung auf Datenträgerebene – Bei dieser Methode wird der gesamte Datenträger bzw. der betreffende Datenträgerblock mit mindestens einem Verschlüsselungsschlüssel verschlüsselt. Die Datenträgerverschlüsselung wirkt unterhalb der Dateisystemebene, funktioniert betriebssystemübergreifend und verbirgt Verzeichnis- und Dateiinformationen wie Name und Größe. Verschlüsselndes Dateisystem (Encrypting File System) ist beispielsweise eine Microsoft-Erweiterung des NTFS (New Technology File System) des Betriebssystems Windows NT, die die Datenträgerverschlüsselung übernimmt.
- Verschlüsselung auf Dateisystemebene – Bei dieser Methode werden Dateien und Verzeichnisse verschlüsselt, nicht jedoch der gesamte Datenträger bzw. die gesamte Partition. Die Verschlüsselung auf Dateisystemebene ist dem Dateisystem übergeordnet und somit auf verschiedene Betriebssysteme übertragbar.

Bei Non-Volatile Memory express (NVMe, nichtflüchtigen Memory express)-Instance-Speicher-Volumes auf SSD ist die Verschlüsselung auf Datenträgerebene die Standardoption. Daten in einem NVMe-Instance-Speicher werden mittels einer XTS-AES-256-Blockverschlüsselung verschlüsselt, die in einem Hardwaremodul auf der Instance implementiert ist. Die Verschlüsselungsschlüssel werden mithilfe des Hardwaremoduls erstellt und sind für jedes NVMe-Instance-Speichergerät eindeutig. Alle Verschlüsselungsschlüssel werden zerstört, wenn die Instance angehalten oder beendet wird, und können nicht wiederhergestellt werden. Sie können keine eigenen Verschlüsselungsschlüssel verwenden.

Verschlüsselung während der Übertragung

AWS empfiehlt dringend, Daten während der Übertragung von einem System zum anderen zu verschlüsseln, einschließlich Ressourcen innerhalb und außerhalb von AWS.

Wenn Sie ein AWS-Konto erstellen, wird ihm ein logisch isolierter Abschnitt der AWS Cloud – die Amazon Virtual Private Cloud (Amazon VPC) – bereitgestellt. Dort können Sie AWS-Ressourcen in einem virtuellen Netzwerk starten, das Sie definiert haben. Sie haben die vollständige Kontrolle über Ihre virtuelle Netzwerkumgebung, u. a. beim Auswählen Ihres eigenen IP-Adressbereichs,

dem Erstellen von Subnetzen und der Konfiguration von Routing-Tabellen und Netzwerk-Gateways. Darüber hinaus können Sie eine sichere Hardware Virtual Private Network (VPN)-Verbindung zwischen Ihrem Unternehmensrechenzentrum und Ihrer Amazon VPC einrichten, sodass Sie die AWS Cloud als Erweiterung Ihres Unternehmensrechenzentrums nutzen können.

Zum Schutz der Kommunikation zwischen Ihrer Amazon VPC und Ihrem Unternehmensrechenzentrum sind mehrere VPN-Konnektivitätsoptionen verfügbar und Sie können eine auswählen, die Ihren Anforderungen am besten entspricht. Sie können das AWS Client VPN verwenden, um mithilfe clientbasierter VPN-Services sicheren Zugriff auf Ihre AWS-Ressourcen zu ermöglichen. Sie können auch eine im AWS Marketplace verfügbare Software-VPN-Appliance eines Drittanbieters verwenden, die Sie auf einer Amazon-EC2-Instance in Ihrer Amazon VPC installieren können. Alternativ können Sie eine IPsec-VPN-Verbindung einrichten, um die Kommunikation zwischen Ihrer VPC und Ihrem Remote-Netzwerk zu schützen. Zum Herstellen einer dedizierten, privaten Verbindung zwischen einem Remote-Netzwerk und Ihrer Amazon VPC können Sie AWS Direct Connect verwenden. Sie können diese Verbindung mit einem AWS Site-to-Site VPN kombinieren, um eine durch IPsec verschlüsselte, private Verbindung zu erstellen.

AWS stellt HTTPS-Endpunkte mithilfe des TLS-Protokolls für die Kommunikation bereit, sodass die Verschlüsselung während der Übertragung ermöglicht wird, wenn Sie AWS-APIs verwenden. Sie können den AWS Certificate Manager (ACM)-Service verwenden, um die privaten und öffentlichen Zertifikate zu generieren, zu verwalten und bereitzustellen, mit denen Sie einen verschlüsselten Transport zwischen Systemen für Ihre Workloads einrichten. Elastic Load Balancing ist in ACM integriert und wird zur Unterstützung von HTTPS-Protokollen verwendet. Wenn Ihre Inhalte über Amazon CloudFront verteilt werden, werden verschlüsselte Endpunkte unterstützt.

Verschlüsselungstools

AWS bietet verschiedene hochgradig skalierbare Datenverschlüsselungsservices, -tools und -mechanismen zum Schutz Ihrer in AWS gespeicherten und verarbeiteten Daten. Informationen zur Funktionalität und zum Datenschutz des AWS-Service finden Sie unter AWS-Service-Funktionen für Datenschutzerwägungen.

Kryptografieservices von AWS verwenden eine Vielzahl von Verschlüsselungs- und Speichertechnologien, die darauf ausgelegt sind, die Integrität Ihrer Daten im Ruhezustand oder während der Übertragung zu gewährleisten. AWS bietet vier primäre Tools für kryptografische Operationen.

- AWS Key Management Service (AWS KMS) ist ein von AWS verwalteter Service, der sowohl Masterschlüssel als auch Datenschlüssel generiert und verwaltet. AWS KMS ist in vielen AWS-Services integriert, um die serverseitige Verschlüsselung von Daten mithilfe von AWS KMS-Schlüsseln aus Kundenkonten zu ermöglichen. AWS KMS-Hardwaresicherheitsmodule (HSMs) sind durch das FIPS 140-2 Level 2 validiert.
- AWS CloudHSM bietet HSMs, die durch das FIPS 140-2 Level 3 validiert sind. Sie speichern eine Vielzahl Ihrer selbstverwalteten kryptografischen Schlüssel sicher, einschließlich Master- und Datenschlüsseln.
- AWS-Kryptografieservices und -tools
  - Das AWS Encryption SDK bietet eine clientseitige Verschlüsselungsbibliothek zum Implementieren von Ver- und Entschlüsselungsvorgängen für alle Datentypen.
  - Der Amazon DynamoDB Encryption Client bietet eine clientseitige Verschlüsselungsbibliothek zur Verschlüsselung von Datentabellen, bevor diese an einen Datenbankservice wie Amazon DynamoDB gesendet werden.

AWS Key Management Service

AWS Key Management Service ist ein verwalteter Service, der Ihnen das Erstellen und Steuern der Verschlüsselungsschlüssel erleichtert, die zur Verschlüsselung Ihrer Daten verwendet werden, und nutzt Hardwaresicherheitsmodule (HSMs) zum Schutz der Sicherheit Ihrer Schlüssel. AWS KMS ist in mehreren anderen AWS-Services integriert, um Ihnen zu helfen, die Daten zu schützen, die Sie mit diesen Services speichern. AWS KMS ist auch in AWS CloudTrail integriert, um Ihnen Protokolle der gesamten Schlüsselverwendung für Ihre regulatorischen und Compliance-Anforderungen zur Verfügung zu stellen.

Sie können auf einfache Weise Schlüssel erstellen, importieren und rotieren sowie Verwendungsrichtlinien und Audit-Nutzung über die AWS Management Console oder mit dem AWS SDK oder der AWS CLI definieren.

Die CMKs in AWS KMS, die von Ihnen importiert oder von KMS für Sie erstellt wurden, werden in verschlüsselter Form in sehr robustem Speicher gespeichert, um sicherzustellen, dass sie bei Bedarf verwendet werden können. Sie können festlegen, dass KMS die in KMS erstellten CMKs einmal im Jahr automatisch rotiert. Sie müssen in diesem Fall bereits mit Ihrem Masterschlüssel verschlüsselte Daten nicht nochmals verschlüsseln. Sie müssen ältere Versionen Ihrer CMKs nicht im Auge behalten, da KMS sie für die automatische Entschlüsselung früher verschlüsselter Daten verfügbar hält.

Für jeden CMK in AWS KMS können Sie steuern, wer Zugriff auf diese Schlüssel hat und mit welchen Services sie über eine Reihe von Zugriffskontrollen, einschließlich Erteilungen und Schlüsselrichtlinienbedingungen innerhalb von Schlüsselrichtlinien oder IAM-Richtlinien, verwendet werden können. Sie können auch Schlüssel aus Ihrer eigenen Schlüsselverwaltungsinfrastruktur importieren und in KMS verwenden.

Die folgende Richtlinie verwendet beispielsweise die Bedingung `kms:ViaService`, um die Verwendung eines vom Kunden verwalteten CMK nur für die angegebenen Aktionen zuzulassen, wenn die Anforderung aus Amazon EC2 oder Amazon RDS in einer bestimmten Region (us-west-2) im Auftrag eines bestimmten Benutzers (`ExampleUser`) stammt.

```
        {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Effect”: “Allow”,
                “Principal”: {
                    “AWS”: “arn:aws:iam::111122223333:user/ExampleUser”
                 }
                “Action”: [
                     “kms:Encrypt*”,
                     “kms:Decrypt”,
                     ”kms:ReEncrypt*”,
                     “kms:GenerateDataKey*”,
                     “kms:CreateGrant”,
                     “kms:ListGrants”,
                     “kms:DescribeKey”
                 ],
                 “Resource”: “*”,
                 “Condition”: {
                    “ForAnyValue:StringEquals”: {
                        “kms:ViaService”: [
                              “ec2.us-west-2.amazonaws.com”,
                              “rds.us-west-2.amazonaws.com”
                        ]
                     }
              }
}
```

AWS Service Integration

AWS KMS wurde in eine Reihe von AWS-Services integriert – eine vollständige Liste der integrierten Services finden Sie auf der KMS-Website. Mit diesen Integrationen können Sie AWS KMS-CMKs ganz einfach verwenden, um die Daten zu verschlüsseln, die Sie mit diesen Services speichern. Zusätzlich zur Verwendung eines vom Kunden verwalteten CMK ermöglichen Ihnen einige der integrierten Services die Verwendung eines von AWS verwalteten CMK, der automatisch für Sie erstellt und verwaltet wird, aber nur innerhalb des spezifischen Service verwendet werden kann, der ihn erstellt hat.

Überwachungsmöglichkeiten

AWS CloudTrail zeichnet jede Verwendung eines Schlüssels, den Sie in AWS KMS speichern, in einer Protokolldatei auf, die an den Amazon-S3-Bucket geliefert wird, den Sie in Ihrer Konfiguration von CloudTrail angegeben haben. Die aufgezeichneten Informationen enthalten Details zu Benutzer, Zeit, Datum, ausgeführter Operation und verwendetem Schlüssel.

Sicherheit

AWS KMS wurde entwickelt, um sicherzustellen, dass niemand Zugriff auf Ihre Masterschlüssel hat. Der Service baut auf Systemen auf, die für den Schutz Ihrer Masterschlüssel konzipiert wurden. Dabei werden umfassende Härtungsmethoden eingesetzt: Es werden niemals Klartext-Masterschlüssel auf einem Datenträger gespeichert, sie werden nicht dauerhaft im Arbeitsspeicher gespeichert und es gibt Beschränkungen, welche Systeme auf Hosts zugreifen können, die Schlüssel verwenden. Jeder Zugriff zum Aktualisieren von Software im Service wird über einen Genehmigungsprozess mit mehreren Teilnehmern kontrolliert, der durch eine unabhängige Gruppe bei AWS überwacht und geprüft wird.

Weitere Informationen über AWS KMS finden Sie im Whitepaper zu AWS Key Management Service.

AWS CloudHSM

AWS CloudHSM ist ein Cloud-basiertes Hardwaresicherheitsmodul (HSM), mit dem Sie unternehmerische, vertragliche und regulatorische Compliance-Anforderungen an die Datensicherheit erfüllen können, indem es Ihnen ermöglicht, Ihre Verschlüsselungsschlüssel auf einer durch das FIPS 140-2 Level 3 validierten Hardware zu generieren und zu verwenden.

Mit AWS CloudHSM können Sie die Verschlüsselungsschlüssel und die von HSM durchgeführten kryptografischen Vorgänge steuern.

AWS und AWS Marketplace-Partner bieten eine Vielzahl von Lösungen zum Schutz sensibler Daten innerhalb von AWS. Doch für Anwendungen und Daten, die strengen vertraglichen oder regulatorischen Vorschriften für die Verwaltung kryptografischer Schlüssel unterliegen, ist mitunter zusätzlicher Schutz erforderlich. Bisher bestand die einzige Möglichkeit zum Speichern sensibler Daten (bzw. der Verschlüsselungsschlüssel zum Schutz der sensiblen Daten) möglicherweise in lokalen Rechenzentren. Dies hätte das Migrieren dieser Anwendungen in die Cloud verhindern oder zu starken Performance-Einbußen führen können. Mit AWS CloudHSM können Sie Ihre Verschlüsselungsschlüssel in HSMs schützen, die nach gesetzlichen Standards für die sichere Schlüsselverwaltung entwickelt und validiert wurden. Sie können die für die Datenverschlüsselung verwendeten kryptografischen Schlüssel sicher generieren, speichern und verwalten, um sicherzustellen, dass nur Sie darauf zugreifen können. AWS CloudHSM hilft Ihnen dabei, die strengen Vorschriften für die Schlüsselverwaltung einzuhalten, ohne die Anwendungsleistung zu beeinträchtigen.

Der AWS CloudHSM-Service funktioniert mit Amazon VPC. AWS CloudHSM-Instances werden in Ihrer Amazon VPC mit einer von Ihnen angegebenen IP-Adresse bereitgestellt, die eine einfache und private Netzwerkanbindung an Ihre Amazon-EC2-Instances ermöglicht. Wenn Sie Ihre HSM-Instances in der Nähe Ihrer Amazon-EC2-Instances positionieren, verkürzen Sie die Netzwerklatenz, wodurch sich die Anwendungsleistung verbessern lässt. AWS bietet einen dedizierten und exklusiven (Einzelmandanten-) Zugriff auf HSM-Instances, die von anderen AWS-Kunden isoliert sind. AWS CloudHSM ist in mehreren Regionen und Availability Zones (AZs) verfügbar und ermöglicht Ihnen das Hinzufügen eines sicheren und dauerhaften Schlüsselspeichers für Ihre Anwendungen.

Integration in AWS-Services und Anwendungen von Drittanbietern

Sie können CloudHSM mit Amazon Redshift, Amazon RDS for Oracle oder Anwendungen anderer Anbieter (wie SafeNet Virtual KeySecure) als Vertrauensanker (Root of Trust), Apache (SSL-Terminierung) oder Microsoft SQL Server (transparente Datenverschlüsselung) nutzen. Sie können auch AWS CloudHSM verwenden, wenn Sie eigene Anwendungen schreiben, und die standardmäßigen kryptografischen Bibliotheken wie PKCS#11, Java JCA/JCE und Microsoft CAPI und CNG weiterverwenden.

Aktivitäten überwachen

Wenn Sie aus Sicherheits- oder Compliance-Gründen Ressourcenänderungen nachverfolgen oder Aktivitäten überwachen müssen, können Sie mithilfe von AWS CloudTrail die Verwaltungs-API-Aufrufe über das AWS CloudHSM überprüfen, die in Ihrem Konto erfolgt sind. Darüber hinaus

können Sie Vorgänge auf der HSM-Appliance mithilfe von SYSLOG überwachen oder SYSLOG-Protokollmeldungen an Ihren eigenen Protokollsammler senden.

AWS-Kryptografieservices und -tools

AWS bietet Mechanismen, die eine Vielzahl von kryptografischen Sicherheitsstandards erfüllen, die Sie zur Implementierung der Best-Practice-Verschlüsselung verwenden können. Das AWS Encryption SDK ist eine clientseitige Verschlüsselungsbibliothek, die in Java, Python, C, JavaScript und einer Befehlszeilenschnittstelle verfügbar ist, die Linux, macOS und Windows unterstützt. Es bietet erweiterte Datenschutzfunktionen, einschließlich Algorithmen-Pakete mit sicherem, authentifiziertem, symmetrischem Schlüssel, wie z. B. 256-Bit-AES-GCM mit Schlüsselableitung und Signatur. Da es speziell für Anwendungen entwickelt wurde, die Amazon DynamoDB verwenden, ermöglicht der DynamoDB Encryption Client Benutzern, ihre Tabellendaten zu schützen, bevor sie an die Datenbank gesendet werden. Es überprüft und entschlüsselt auch Daten, wenn sie abgerufen werden. Der Client ist in Java und Python verfügbar.

DM-Crypt-Infrastruktur von Linux

Bei dm-crypt handelt es sich um einen Verschlüsselungsmechanismus für Linux auf Kernelebene, mit dem Benutzer ein verschlüsseltes Dateisystem bereitstellen können. Unter Bereitstellung eines Dateisystems versteht man den Prozess, bei dem ein Dateisystem einem Verzeichnis (Bereitstellungspunkt) zugeordnet wird, wodurch es für das Betriebssystem verfügbar wird. Nach dem Bereitstellen sind sämtliche Dateien eines Dateisystems für Anwendungen (ohne zusätzlichen Interaktionsbedarf) verfügbar. Diese Dateien werden jedoch verschlüsselt, wenn sie auf Datenträgern gespeichert werden.

Der Device Mapper ist eine Infrastruktur innerhalb des Kernel von Linux 2.6 und 3.x. Er bietet eine generische Methode, virtuelle Blockgeräteebenen zu erstellen. Das Verschlüsselungsziel des Device Mappers ermöglicht eine transparente Verschlüsselung von Blockgeräten mithilfe der Verschlüsselungs-API des Kernel. Die Lösung, um die es in diesem Beitrag geht, verwendet dm-crypt in Verbindung mit einem datenträgergestützten Dateisystem, das mit dem Logical Volume Manager (LVM) einem logischen Volume zugeordnet wurde. LVM ermöglicht die Verwaltung des logischen Volumes für den Linux-Kernel.

Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen

Jedes Mal, wenn ein Benutzer oder eine Anwendung versucht, die AWS Management Console, die AWS API oder die AWS CLI zu verwenden, wird eine Anforderung an AWS gesendet. Der AWS-Service empfängt die Anforderung und führt eine Reihe von Schritten aus, um zu bestimmen, ob die Anforderung gemäß einer bestimmten Auswertungslogik für Richtlinien erlaubt oder verweigert werden soll. Mit Ausnahme von Stamm-Anmeldeinformationsanforderungen werden alle Anforderungen in AWS standardmäßig verweigert (die standardmäßige Verweigern-Richtlinie wird angewendet). Das bedeutet, dass alles, was in der Richtlinie nicht ausdrücklich erlaubt ist, verweigert wird. Bei der Definition von Richtlinien und als bewährte Methode empfiehlt AWS, dass Sie das Prinzip der geringsten Zugriffsrechte anwenden, was bedeutet, dass jede Komponente (wie Benutzer, Module oder Services) nur auf die Ressourcen zugreifen kann, die zur Ausführung ihrer Aufgaben erforderlich sind.

Dieser Ansatz steht im Einklang mit Artikel 25 der DSGVO, der vorsieht, dass „der Verantwortliche geeignete technische und organisatorische Maßnahmen“ treffen soll, „die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden“.

AWS bietet auch Tools zur Implementierung der Infrastruktur als Code. Dies ist ein leistungsstarker Mechanismus, um die Sicherheit von Beginn des Entwurfs einer Architektur an einzubeziehen. AWS CloudFormation bietet eine gemeinsame Sprache zur Beschreibung und Bereitstellung aller Infrastrukturressourcen, einschließlich Sicherheitsrichtlinien und -prozesse. Mit diesen Tools und Praktiken wird die Sicherheit zum Bestandteil Ihres Codes und kann gemäß den Anforderungen Ihrer Organisation (mit einem Versionierungssystem) versioniert, überwacht und geändert werden. Dies ermöglicht den Datenschutz durch Technik, da Sicherheitsprozesse und -richtlinien in die Definition Ihrer Architektur einbezogen und auch kontinuierlich durch Sicherheitsmaßnahmen in Ihrer Organisation überwacht werden können.

Wie AWS Ihnen helfen kann

Tabelle 1 – Wie AWS Ihnen bei der DSGVO-Compliance helfen kann

Area	Beschreibung	AWS-Services und -Tools
Striktes Compliance-Framework	Geeignete technische und organisatorische Maßnahmen müssen „die Fähigkeit [beinhalten], die Vertrauli chkeit, Integritä t, Verfügbarkeit und Belastbar keit der Systeme und Dienste im Zusammenhang mit der Verarbeit ung auf Dauer sicherzustellen“.	SOC 1 / SSAE 16 / ISAE 3402 (zuvor SAS 70) / SOC 2 / SOC 3 PCI DSS Level 1 ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018 NIST FIPS 140-2 Common Cloud Computing Controls Catalog (C5, Anforderungskatalog Cloud Computing)
Datenzugr iffskontrolle	Der Verantwor tliche hat „… geeignete technische und organisatorische Maßnahmen “ zu treffen, „die sicherste llen, dass durch Voreinstellung grundsätzlich nur personenb	AWS Identity and Access Management (IAM) Amazon Cognito AWS Shield und AWS WAF AWS Resource Access Manager Amazon CloudFront AWS Organizations AWS CloudTrail

Area	Beschreibung	AWS-Services und -Tools
	ezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden“.	

Area	Beschreibung	AWS-Services und -Tools
Überwachung und Protokollierung	„Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Verantwortung unterliegen.“ „… der Verantwortliche und der Auftragsverarbeiter haben geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten […]“	AWS Config Amazon CloudWatch AWS Control Tower Amazon GuardDuty Amazon Inspector Amazon Macie AWS Systems Manager AWS Security Hub AWS-Tools und SDKs

Area	Beschreibung	AWS-Services und -Tools
Schutz Ihrer Daten auf AWS	Organisationen müssen „geeignete technische und organisatorische Maßnahmen [treffen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: die Pseudonymisierung und Verschlüsselung personenbezogener Daten“.	AWS Certificate Manager AWS CloudHSM AWS Key Management Service

Mitwirkende

An diesem Dokument haben folgende Personen mitgewirkt:

- Tim Anderson, Technical Industry Specialist, Amazon Web Services
- Carmela Gambardella, Public Sector Solutions Architect, Amazon Web Services
- Giuseppe Russo, Security Assurance Manager, Amazon Web Services
- Marta Taggart, Senior Program Manager, Amazon Web Services
- Luca Iannario, Public Sector Solutions Architect, Amazon Web Services

Dokumentversionen

Date (Datum)	Beschreibung
November 2017	Erstveröffentlichung
Dezember 2020	Aktualisiert, um das Hinzufügen neuer AWS-Services und -Funktionen einzuschließen.

Hinweise

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