AWS Referenzarchitektur zum Datenschutz (PRA)AWS

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: AWS Referenzarchitektur zum Datenschutz (PRA)AWS

Table of Contents

AWS Referenzarchitektur zum Datenschutz (AWS PRA)

Amazon Web Services (Mitwirkende)

März 2024 (Verlauf der Dokumente)

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Hinweise

Dieser Leitfaden dient nur zu Informationszwecken. Es handelt sich nicht um eine Rechtsberatung und sollte nicht als Rechtsberatung angesehen werden. AWS fordert seine Kunden auf, sich angemessen beraten zu lassen, wenn es um die Umsetzung von Datenschutz- und Datenschutzregelungen und allgemeiner um die für ihr Unternehmen relevanten Gesetze geht.

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS Produktangebote und Praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWS Produkte oder Dienstleistungen werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt.

Die Verantwortlichkeiten und Verbindlichkeiten AWS gegenüber seinen Kunden werden durch AWS Vereinbarungen geregelt, und dieses Dokument ist weder Teil einer Vereinbarung zwischen AWS und seinen Kunden noch ändert es diese.

Einführung

Die AWS Privacy Reference Architecture (PRA) enthält eine Reihe von Richtlinien, die sich speziell auf das Design und die Konfiguration von Kontrollen beziehen, die den Datenschutz unterstützen. AWS services Dieser Leitfaden kann Ihnen helfen, Entscheidungen über Personen, Prozesse und Technologien zu treffen, die zum Schutz des Datenschutzes in der AWS Cloud

Das Modell der AWS gemeinsamen Verantwortung und der Datenschutz

In der AWS Cloud tragen Sie gemeinsam die Verantwortung für Sicherheit und Einhaltung von AWS. AWS ist für die Sicherheit der Cloud verantwortlich, was bedeutet, dass AWS es für den Schutz der Infrastruktur verantwortlich ist, auf der alle in der Cloud angebotenen Dienste ausgeführt werden AWS Cloud. Sie sind für die Sicherheit in der Cloud verantwortlich, was bedeutet, dass Sie für die Konfiguration und Verwaltung AWS services gemäß den Sicherheits- und Datenschutzanforderungen verantwortlich sind. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

AWS services bietet Funktionen, mit denen Sie Ihre eigenen Datenschutzkontrollen in der Cloud implementieren können, um Ihre Datenschutzanforderungen zu erfüllen. Ihre Verantwortung für den Datenschutz hängt von vielen Faktoren ab, einschließlich der AWS services Art und AWS-Regionen Weise, die Sie wählen, der Integration dieser Dienste in Ihre IT-Umgebung und den Gesetzen und Vorschriften, die für Ihr Unternehmen und Ihre Arbeitslast gelten.

Bei der Nutzung AWS services behalten Sie die Kontrolle über Ihre Inhalte. Insbesondere werden Inhalte als Software (einschließlich Maschinenbilder), Daten, Text, Audio, Video oder Bilder definiert, die Sie oder ein Endbenutzer AWS services in Verbindung mit Ihrem Konto zur Verarbeitung, Speicherung oder zum Hosten an uns übertragen. Dazu gehören auch alle Berechnungsergebnisse, die Sie oder ein Endbenutzer mithilfe dieser Methode ableiten. AWS services Sie sind für die Verwaltung der folgenden Entscheidungen verantwortlich, die unter Ihrer Kontrolle liegen:

- Die Daten, für die Sie sich entscheiden, zu erheben, zu speichern oder zu verarbeiten AWS
- Die AWS services , die Sie mit den Daten verwenden
- Der AWS-Region Ort, an dem Sie Daten sammeln, speichern oder verarbeiten
- Das Format und die Struktur Ihrer Daten und ob sie maskiert, anonymisiert oder verschlüsselt sind
- Wie Sie Ihre kryptografischen Schlüssel für die Verschlüsselung definieren, speichern, rotieren und verwenden
- Wer hat Zugriff auf Ihre Daten und wann hat er Zugriff auf Ihre Daten und wie werden diese Zugriffsrechte gewährt, verwaltet und widerrufen

Sobald Sie das Modell der AWS gemeinsamen Verantwortung verstanden haben und wissen, wie es im Allgemeinen für den Betrieb in der Cloud gilt, müssen Sie herausfinden, wie es für Ihren Anwendungsfall gilt. Je AWS services nachdem, für welches Modell Sie sich entscheiden, wird der Umfang der Konfiguration bestimmt, die Sie im Rahmen der Datenschutzverantwortung

Ihres Unternehmens vornehmen müssen. Ein Service wie Amazon Elastic Compute Cloud (Amazon EC2) wird beispielsweise als Infrastructure as a Service (IaaS) eingestuft. Wenn Sie Amazon EC2 verwenden, müssen Sie daher alle erforderlichen Datenschutzkonfigurationen für Gastbetriebssysteme und für die Anwendungssoftware oder Dienstprogramme durchführen, die Sie auf Ihren EC2-Instances installieren. Wenn Sie einen abstrahierten Service wie Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB verwenden, AWS ist er für die Infrastrukturebene, das Betriebssystem und die Plattformen verantwortlich. Sie sind dafür verantwortlich, die Daten zu verwalten und zu klassifizieren und die Richtlinien zu konfigurieren, die für den Zugriff auf die Endgeräte zum Speichern und Abrufen von Daten verwendet werden. Weitere Informationen darüber, wie Sie AWS Daten und Privatsphäre schützen können, finden Sie unter Datenschutz und Datenschutz unter. AWS

Die AWS PRA verstehen

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

In diesem Abschnitt wird das Verhältnis zwischen der AWS Privacy Reference Architecture (AWS PRA) und anderen AWS Leitlinien beschrieben. In diesem Abschnitt werden auch das allgemeine Layout und die Struktur der Beispielumgebung mit AWS mehreren Konten in der AWS PRA beschrieben.

In diesem Abschnitt werden folgende Themen behandelt:

- Verwendung der AWS PRA und der AWS SRA
- AWS Organizations und die spezielle Kontostruktur
- Operationalisierung von Datenschutzdiensten AWS

Verwendung der AWS PRA und der AWS SRA

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Die AWS PRA bietet Muster, die Kunden bei der Planung grundlegender Datenschutzkontrollen auf Anwendungsebene für ihre Infrastruktur und Workloads als hilfreich empfunden haben. AWS Die AWS Security Reference Architecture (AWS SRA) bietet eine Reihe von Richtlinien für den Aufbau einer Architektur, die die richtigen Sicherheitskontrollen in Ihrer AWS landing zone und Ihren Anwendungen implementiert und unterstützt. Um die in diesem Leitfaden beschriebenen Datenschutzkontrollen festzulegen, geht die AWS PRA von vielen der gleichen grundlegenden Richtlinien und Kontostrukturen aus, die in der AWS SRA beschrieben sind. In der AWS PRA und der AWS SRA werden viele der gleichen Schlüssel detailliert beschrieben. AWS services Dieses Handbuch enthält nur kurze Beschreibungen dieser Dienste. In der AWS SRA erfahren Sie mehr über diese Dienste und deren Verwendung in einem Sicherheitskontext.

Die AWS SRA kann Ihnen helfen, AWS Sicherheitsdienste so zu entwerfen, zu implementieren und zu verwalten, dass sie den AWS empfohlenen Praktiken entsprechen. Sie können die AWS SRA als

eigenständigen Leitfaden oder die AWS SRA und AWS PRA als begleitende Leitfäden verwenden. Viele der in der AWS SRA aufgeführten Sicherheitsrichtlinien können zusammen mit den in der PRA beschriebenen Datenschutzkontrollen befolgt werden. AWS Ähnlich wie bei der Sicherheit gibt es grundlegende Datenschutzüberlegungen, die Sie zu Beginn Ihrer AWS Cloud Reise treffen sollten, da sich diese Entscheidungen auf die Gestaltung der Kontostruktur des Unternehmens auswirken können. Zu den Fragen, die Sie sich stellen könnten, gehören beispielsweise:

- Wie definiert meine Organisation personenbezogene Daten?
- Unterstützt meine Organisation Anwendungen, die personenbezogene Daten verarbeiten?
- Was ist mit Anwendungen, die andere Arten von regulierten Daten verarbeiten?
- Welche Kontrollen auf Organisationsebene kann ich implementieren, um meine Entwickler und Cloud-Techniker so weit wie möglich von personenbezogenen Daten fernzuhalten?
- Wie trenne ich personenbezogene Daten von anderen Datentypen?
- Was sind die Anforderungen meiner Organisation an grenzüberschreitende Datenübertragungen?

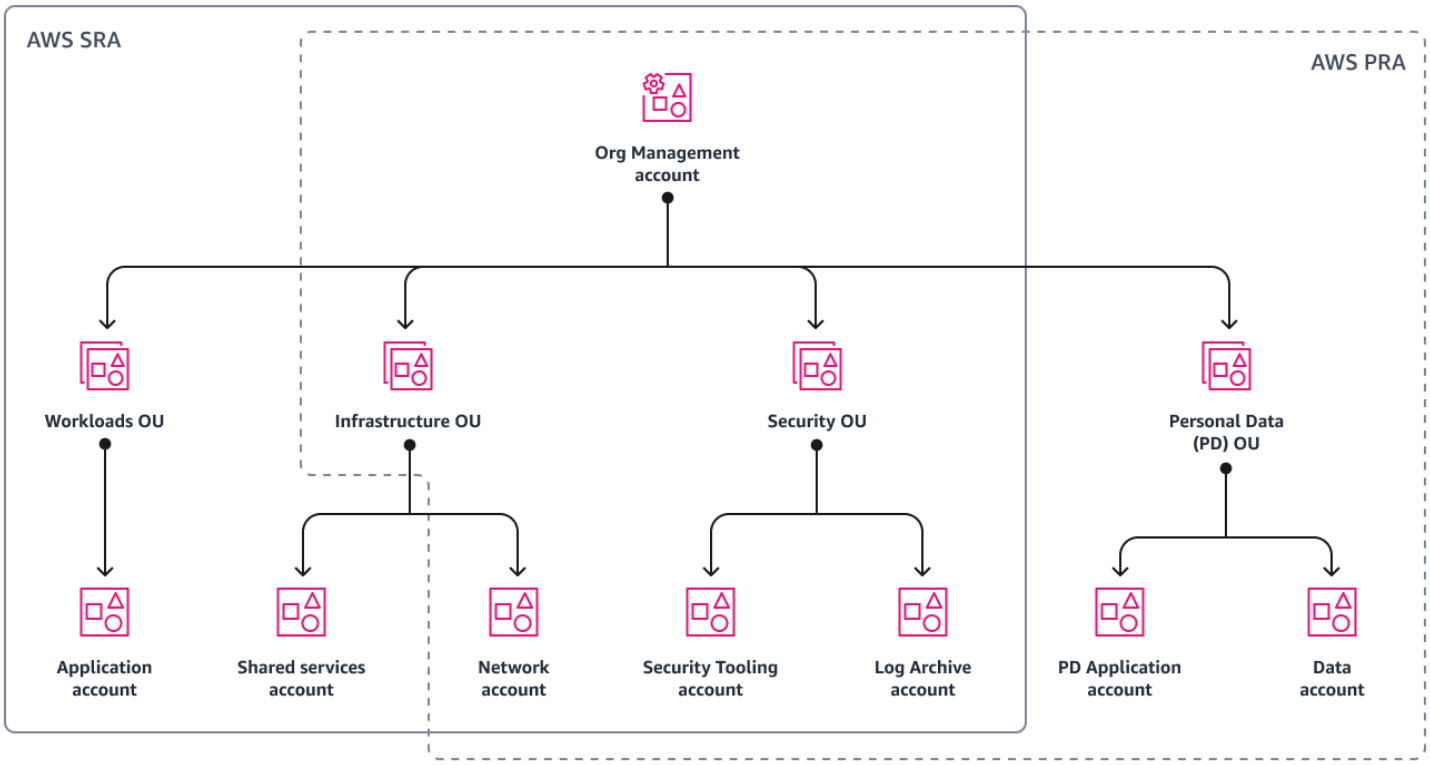
Die Antworten auf viele dieser Fragen können Auswirkungen auf das Design Ihrer Cloud-Umgebung haben, z. B. auf Ihre AWS-Konto Struktur, Richtlinien zur Servicesteuerung und AWS Identity and Access Management (IAM-) Rollen.

AWS Organizations und die spezielle Kontostruktur

> Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

AWS Organizationsist ein Kontoverwaltungsdienst, mit dem Sie mehrere Konten zentral verwalten und verwalten können AWS-Konten. Die Verwendung von AWS Organizations ist die Grundlage für eine gut strukturierte Umgebung mit mehreren AWS Konten. Weitere Informationen finden Sie unter Einrichtung Ihrer Best-Practice-Umgebung. AWS

Das folgende Diagramm zeigt die hochrangige Konto- und Organisationseinheitenstruktur (OU) der AWS PRA. Die Organisationsstruktur der AWS PRA entspricht größtenteils der Organisationsstruktur der AWS SRA.



Zu den Abweichungen von der AWS SRA-Organisation gehören:

- Die AWS PRA fügt die OU für personenbezogene Daten (PD) hinzu, die für die Erfassung, Speicherung und Verarbeitung personenbezogener Daten vorgesehen ist. Diese strukturelle Trennung bietet Flexibilität, sodass Sie spezifische, detaillierte Kontrollen definieren können, um personenbezogene Daten vor unbeabsichtigter Offenlegung zu schützen.
- In der Infrastruktur-OU enthält die AWS PRA derzeit keine zusätzlichen Leitlinien für das Shared Services-Konto, die in der SRA beschrieben sind. AWS
- Die AWS PRA enthält derzeit keine zusätzlichen Leitlinien für die Workloads OU, die in der AWS SRA beschrieben sind. Anwendungen, die personenbezogene Daten erheben oder verarbeiten, befinden sich in speziellen Konten in der PD OU.

Sie können sie AWS Control Towerfür die allgemeine grundlegende Steuerung und die automatisierte Implementierung von Sicherheits- und Datenschutzkontrollen in Ihrem gesamten Unternehmen verwenden. Wenn es heute in Ihrem Unternehmen AWS Control Tower nicht verwendet wird, können Sie dennoch viele der darin enthaltenen Sicherheits- und Datenschutzkontrollen AWS Control Tower, wie z. B. Richtlinien und AWS Config Regeln zur Dienstkontrolle, in den jeweiligen Diensten einsetzen.

Es könnte hilfreich sein, bei der Planung Ihrer Konto- und Organisationsstruktur, einschließlich einer Strategie zur Kontosegmentierung, die Verarbeitung personenbezogener Daten in Betracht zu ziehen. Möglicherweise müssen Sie die Arten von Daten, die Sie verarbeiten, für ihre jeweiligen Anwendungsfälle und die geltenden Gesetze und Vorschriften berücksichtigen. Karteninhaberdaten sind beispielsweise gemäß dem Payment Card Industry Data Security Standard (PCI DSS) geschützt, und geschützte Gesundheitsinformationen können dem Health Insurance Portability and Accountability Act (HIPAA) unterliegen. Möglicherweise möchten Sie überprüfen, welche Umgebungen personenbezogene Daten enthalten, und Ihre Segmentierungsstrategie darauf ausrichten. Eine typische Kundensegmentierungsstrategie kann spezielle Konten beinhalten AWS-Konten , die auf den Softwareentwicklungszyklus (SDLC) abgestimmt sind, wie z. B. spezielle Konten für Entwicklung, Staging oder Qualitätssicherung (QA) und Produktion. Eine solche Segmentierungsstrategie kann ein entscheidender Bestandteil der gesamten Entwurfsdiskussion sein, und Ihre Organisationseinheiten müssen möglicherweise an Ihre spezifischen regulatorischen Anforderungen angepasst werden.

Operationalisierung von Datenschutzdiensten AWS

> Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Für viele ist Datenschutz bereichsübergreifend. Viele verschiedene Teams spielen eine Rolle, darunter Teams für Vorschriften, Compliance und Technik. Wenn Ihr Unternehmen damit begonnen hat, die wichtigsten Personen und Richtlinienkomponenten Ihres Datenschutzprogramms zu definieren, können Sie die Kontrollen mit einem Rahmen zur Einhaltung der Datenschutzbestimmungen abgleichen, um einen konsistenten Betrieb zu gewährleisten. Ein Framework kann als Rubrik für die Implementierung grundlegender und anwendungsspezifischer Datenschutzkontrollen für personenbezogene Daten in Ihrer Umgebung dienen. AWS

Unabhängig vom Framework, das Kunden zur Kategorisierung ihrer Datenschutzanforderungen verwenden, müssen die Teams für die Einhaltung von Datenschutzbestimmungen, die Datenschutzentwicklung und die Anwendungsteams häufig zusammenarbeiten, um die Implementierungsziele zu erreichen. Beispielsweise könnten die Teams für regulatorische Vorschriften und die Einhaltung der Vorschriften die allgemeinen Anforderungen festlegen, und die Konstruktions- und Anwendungsteams konfigurieren AWS services und Funktionen so konfigurieren, dass sie diesen Anforderungen entsprechen. Wenn Sie mit einem Kontrollrahmen beginnen, können Sie präzisere organisatorische und technische Kontrollen definieren.

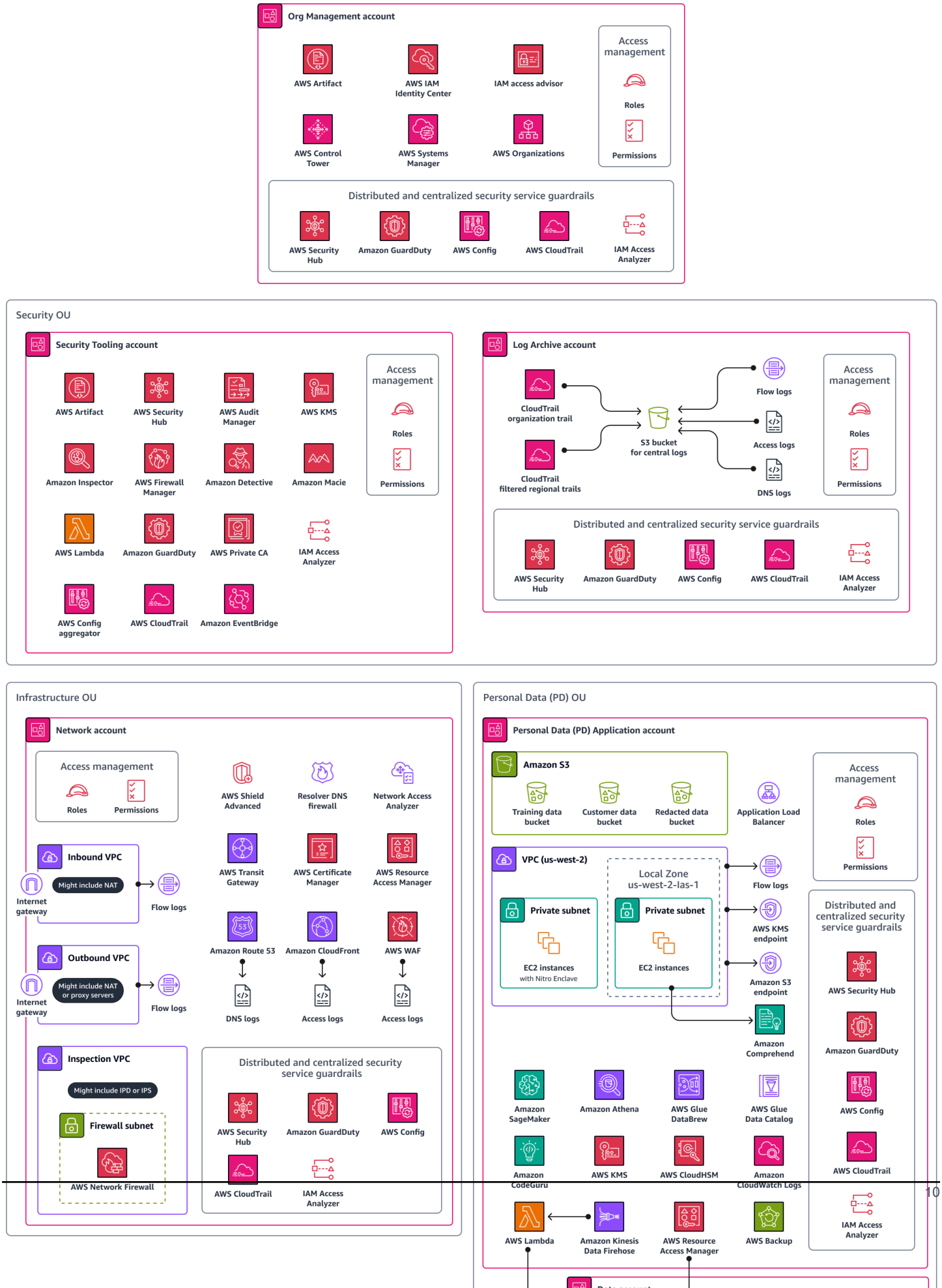
Bei der Definition der technischen Kontrollen AWS services und Funktionen ist eine weitere wichtige Entscheidung, ob eine Kontrolle für die gesamte Organisation, eine Organisationseinheit, ein Konto oder eine bestimmte Ressource gelten soll. Einige Dienste und Funktionen eignen sich hervorragend für die Implementierung von Kontrollen in Ihrem gesamten AWS Unternehmen. Das Blockieren des öffentlichen Zugriffs auf Amazon S3 S3-Buckets ist beispielsweise eine spezifische Kontrolle, die vorzugsweise im Stammverzeichnis der Organisation konfiguriert wird und nicht für jedes Konto einzeln. Ihre Aufbewahrungsrichtlinien können jedoch von Anwendung zu Anwendung variieren, was bedeutet, dass Sie die Kontrolle möglicherweise auf Ressourcenebene anwenden.

Damit Sie den Datenschutz in Ihrem Unternehmen schneller umsetzen können, AWS bietet das Unternehmen Prüfungs- und Compliance-Beratungsdienste für Ihre AWS Workloads an. Weitere Informationen erhalten Sie bei SAS. AWS

Die Referenzarchitektur zum AWS Datenschutz

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Das folgende Diagramm veranschaulicht die AWS Privacy Reference Architecture (AWS PRA). Dies ist ein Beispiel für eine Architektur, die viele datenschutzrelevante AWS services Funktionen miteinander verbindet. Diese Architektur basiert auf einer landing zone, die von regiert wird AWS Control Tower.


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
AWS Control Tower
AWS Systems Manager
AWS Organizations
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
AWS Lambda
Amazon GuardDuty
AWS Private CA
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Access management
Roles
Permissions
Log Archive account
CloudTrail organization trail
CloudTrail filtered regional trails
S3 bucket for central logs
Flow logs
Access logs
DNS logs
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
AWS Transit Gateway
AWS Certificate Manager
AWS Resource Access Manager
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Personal Data (PD) OU
Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application Load Balancer
VPC (us-west-2)
Local Zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Amazon Comprehend
Amazon SageMaker
Amazon Athena
AWS Glue DataBrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

Die AWS PRA umfasst eine serverlose Webarchitektur, die im Anwendungskonto für personenbezogene Daten (PD) gehostet wird. Die Architektur in diesem Konto ist ein Beispiel für einen Workload, der personenbezogene Daten direkt von Verbrauchern sammelt. Bei diesem Workload stellen Benutzer eine Verbindung über eine Webebene her. Die Webebene interagiert mit der Anwendungsebene. Diese Ebene empfängt Eingaben von der Webebene, verarbeitet und speichert die Daten, ermöglicht autorisierten internen Teams und Dritten den Zugriff auf die Daten und archiviert und löscht die Daten schließlich, wenn sie nicht mehr benötigt werden. Die Architektur ist bewusst modular und ereignisgesteuert, um viele der grundlegenden Datenschutztechniken zu demonstrieren, ohne sich mit spezifischen Anwendungsfällen wie Data Lakes, Containern, Datenverarbeitung oder Internet der Dinge (IoT) befassen zu müssen.

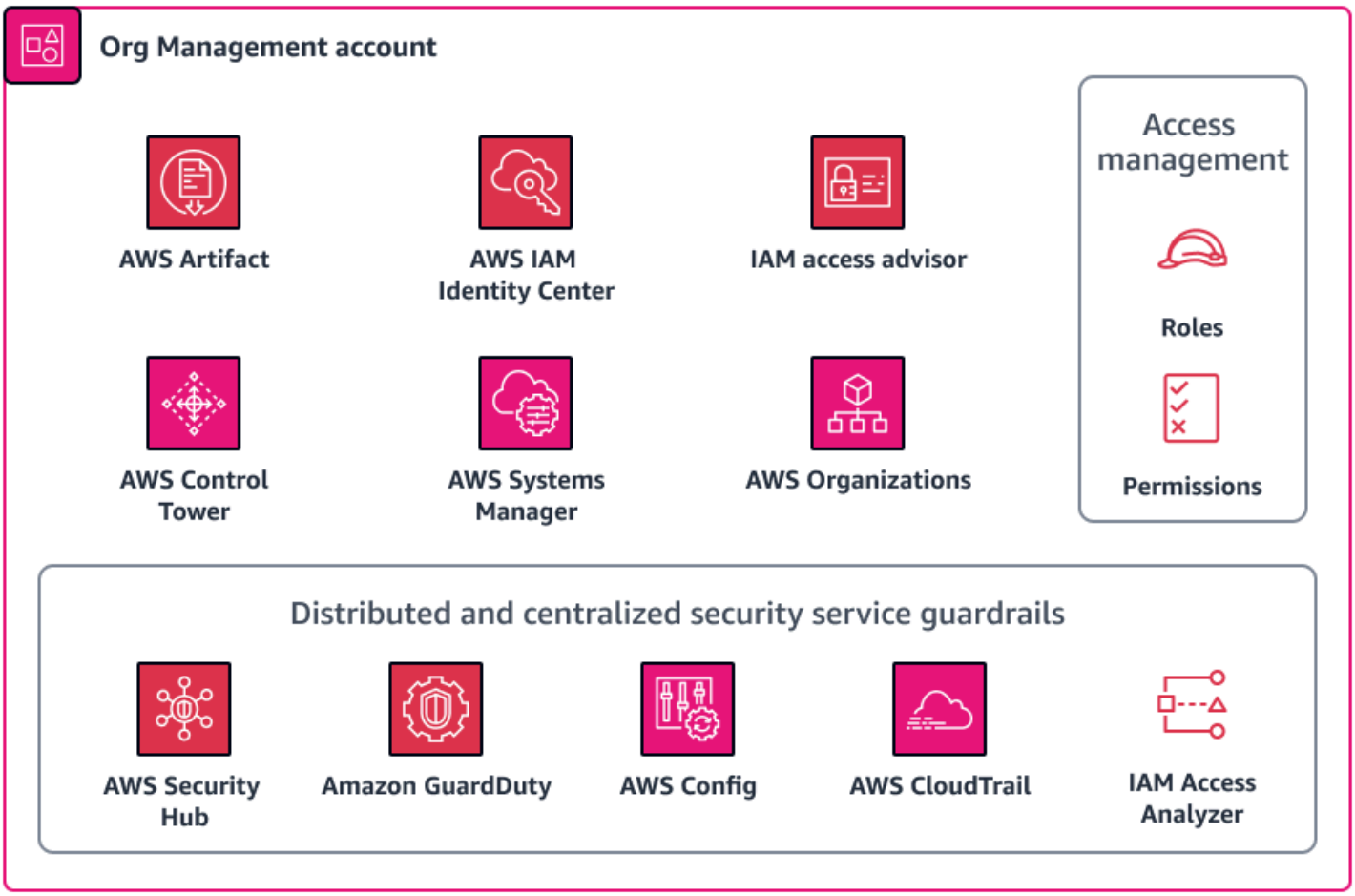
Als Nächstes beschreibt dieser Leitfaden jedes Konto in der Organisation im Detail. Es werden die datenschutzrelevanten Dienste und Funktionen, Überlegungen und Empfehlungen sowie Diagramme für jedes der folgenden Konten beschrieben:

- Konto „Org Management“
- Security OU — Konto für Sicherheitstools
- Security OU — Konto protokollieren
- Infrastruktur-OE – Netzwerkkonto
- Personenbezogene Daten (OU — PD), Anwendungskonto

Konto „Org Management“

> Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Das Org Management-Konto wird in erster Linie verwendet, um Abweichungen in der Ressourcenkonfiguration für die grundlegenden Datenschutzkontrollen für alle Konten in Ihrer Organisation zu verwalten. Verwaltet wird dieses Konto von AWS Organizations. In diesem Konto können Sie auch neue Mitgliedskonten einheitlich einrichten, wobei viele der gleichen Sicherheits- und Datenschutzkontrollen gelten. Weitere Informationen zu diesem Konto finden Sie in der AWS Security Reference Architecture (AWS SRA). Das folgende Diagramm zeigt die AWS Sicherheits- und Datenschutzdienste, die im Org Management-Konto konfiguriert sind.



Dieser Abschnitt enthält detailliertere Informationen zu den folgenden Komponenten AWS services , die in diesem Konto verwendet werden:

- AWS Artifact
- AWS Control Tower
- AWS Organizations

AWS Artifact

AWS Artifactkann Ihnen bei Audits helfen, indem es Dokumente zu AWS Sicherheit und Konformität auf Abruf herunterlädt. Weitere Informationen zur Verwendung dieses Dienstes in einem Sicherheitskontext finden Sie in der AWS Sicherheitsreferenzarchitektur.

Auf AWS service diese Weise können Sie besser verstehen, von welchen Steuerelementen Sie geerbt haben, AWS und bestimmen, welche Kontrollen Sie möglicherweise noch in Ihrer Umgebung implementieren müssen. AWS Artifact bietet Zugriff auf AWS Sicherheits- und Compliance-Berichte,

wie z. B. SOC-Berichte (System and Organization Controls) und PCI-Berichte (Payment Card Industry). Es bietet auch Zugang zu Zertifizierungen von Akkreditierungsstellen in verschiedenen Regionen und Compliance-Branchen, die die Umsetzung und betriebliche Wirksamkeit von Kontrollen bestätigen. AWS Mithilfe dieser AWS Artifact AWS Methode können Sie Ihren Prüfern oder Aufsichtsbehörden die AWS Prüfartefakte als Nachweis für Sicherheitskontrollen zur Verfügung stellen. Die folgenden Berichte könnten nützlich sein, um die Wirksamkeit von AWS Datenschutzkontrollen nachzuweisen:

- SOC 2 Type 2-Datenschutzbericht — Dieser Bericht zeigt die Wirksamkeit von AWS Kontrollen in Bezug auf die Erfassung, Verwendung, Aufbewahrung, Offenlegung und Entsorgung personenbezogener Daten. Weitere Informationen finden Sie in den häufig gestellten Fragen zu SOC.
- SOC 3-Datenschutzbericht — Der SOC 3-Datenschutzbericht ist eine weniger detaillierte Beschreibung der SOC-Datenschutzkontrollen zur allgemeinen Verbreitung.
- Zertifizierungsbericht ISO/IEC 27701:2019 — ISO/IEC 27701:2019 beschreibt Anforderungen und Richtlinien für die Einrichtung und kontinuierliche Verbesserung eines Datenschutz informationsmanagementsystems (PIMS). Dieser Bericht beschreibt den Umfang dieser Zertifizierung und kann als Zertifizierungsnachweis dienen. AWS Weitere Informationen zu dieser Norm finden Sie unter ISO/IEC 27701:2019 (ISO-Website).

AWS Control Tower

AWS Control Towerhilft Ihnen bei der Einrichtung und Verwaltung einer Umgebung mit AWS mehreren Konten, die den vorgeschriebenen bewährten Sicherheitsmethoden folgt. Weitere Informationen zur Verwendung dieses Dienstes in einem Sicherheitskontext finden Sie in der AWS Sicherheitsreferenzarchitektur.

In AWS Control Tower können Sie auch die Implementierung einer Reihe von proaktiven, präventiven und detektiven Kontrollen, auch als Guardrails bezeichnet, automatisieren, die Ihren Anforderungen an die Datenspeicherung und den Datenschutz entsprechen. Sie können beispielsweise Leitplanken festlegen, die die Übertragung von Daten auf nur genehmigte Daten beschränken. AWS-Regionen Für eine noch detailliertere Kontrolle können Sie aus mehr als 17 Leitplanken wählen, die darauf ausgelegt sind, die Datenresidenz zu kontrollieren, wie z. B. Amazon Virtual Private Network (VPN) -Verbindungen verbieten, Internetzugriff für eine Amazon VPC-Instance verbieten und Zugriff auf basierend auf der Anfrage verweigern. AWS AWS-Region Diese Leitplanken bestehen aus einer Reihe von AWS CloudFormation Hooks, Richtlinien zur Servicesteuerung und AWS Config Regeln,

die einheitlich in Ihrem Unternehmen eingesetzt werden können. Weitere Informationen finden Sie in der Dokumentation unter Kontrollen zur Verbesserung des Datenschutzes. AWS Control Tower

AWS Control Tower Enthält eine Reihe von obligatorischen Kontrollen für den Fall, dass Sie Schutzmaßnahmen zum Schutz der Privatsphäre einrichten müssen, die über die Kontrolle der Datenspeicherung hinausgehen. Diese Steuerelemente werden standardmäßig in allen Organisationseinheiten eingesetzt, wenn Sie Ihre landing zone einrichten. Bei vielen dieser Kontrollen handelt es sich um präventive Kontrollen, die auf den Schutz von Protokollen ausgelegt sind, z. B. das Löschen von Protokollarchiven verbieten und die Integritätsprüfung für CloudTrail Protokolldateien aktivieren.

AWS Control Tower ist auch integriert, AWS Security Hub um detektive Kontrollen bereitzustellen. Diese Kontrollen werden als Service-Managed Standard bezeichnet: AWS Control Tower. Sie können diese Kontrollen verwenden, um zu überwachen, ob die Konfiguration von Kontrollen, die den Datenschutz unterstützen, schwankt, z. B. Verschlüsselung im Ruhezustand für Amazon Relational Database Service (Amazon RDS) -Datenbank-Instances.

AWS Organizations

Die AWS PRA dient AWS Organizations zur zentralen Verwaltung aller Konten innerhalb der Architektur. Weitere Informationen finden Sie unter AWS Organizations und die spezielle Kontostruktur in diesem Handbuch. In AWS Organizations können Sie Service Control Policies (SCPs) und Verwaltungsrichtlinien verwenden, um zum Schutz personenbezogener Daten und der Privatsphäre beizutragen.

Service-Kontrollrichtlinien (SCPs)

Service Control Policies (SCPs) sind eine Art von Organisationsrichtlinie, mit der Sie Berechtigungen in Ihrer Organisation verwalten können. Sie bieten eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für AWS Identity and Access Management (IAM) -Rollen und Benutzer im Zielkonto, in der Organisationseinheit (OU) oder in der gesamten Organisation. Sie können SCPs über das Organisationsverwaltungskonto erstellen und anwenden.

Sie können es verwenden AWS Control Tower , um SCPs einheitlich für Ihre Konten bereitzustellen. Weitere Informationen zu den Datenresidenzkontrollen, die Sie beantragen können AWS Control Tower, finden Sie AWS Control Tower in diesem Leitfaden. AWS Control Tower beinhaltet ein umfassendes Angebot an präventiven SCPs. Wenn es in Ihrer Organisation derzeit AWS Control Tower nicht verwendet wird, können Sie diese Kontrollen auch manuell implementieren.

Verwendung von SCPs zur Erfüllung der Anforderungen an die Datenresidenz

Es ist üblich, die Anforderungen an den Wohnsitz personenbezogener Daten zu erfüllen, indem Daten in einer bestimmten geografischen Region gespeichert und verarbeitet werden. Um zu überprüfen, ob die spezifischen Anforderungen einer Jurisdiktion bezüglich des Datenschutzrechts erfüllt sind, empfehlen wir Ihnen, eng mit Ihrem Regulierungsteam zusammenzuarbeiten, um Ihre Anforderungen zu bestätigen. Wenn diese Anforderungen festgelegt wurden, gibt es eine Reihe AWS grundlegender Datenschutzkontrollen, die Ihnen dabei helfen können. Beispielsweise können Sie mithilfe von SCPs einschränken, welche AWS-Regionen Daten verarbeitet und gespeichert werden können. Ein Beispiel für eine Richtlinie finden Sie Beschränken Sie Datenübertragungen zwischen AWS-Regionen in diesem Handbuch.

Verwendung von SCPs zur Beschränkung von API-Aufrufen mit hohem Risiko

Es ist wichtig zu verstehen, für welche Sicherheits- und Datenschutzkontrollen AWS Sie verantwortlich sind und für welche Sie verantwortlich sind. Sie sind beispielsweise für die Ergebnisse von API-Aufrufen verantwortlich, die gegen AWS services die von Ihnen verwendeten APIs gerichtet werden könnten. Sie sind auch dafür verantwortlich, zu verstehen, welche dieser Aufrufe zu Änderungen Ihres Sicherheits- oder Datenschutzes führen könnten. Wenn Sie Bedenken haben, einen bestimmten Sicherheits- und Datenschutzstatus aufrechtzuerhalten, können Sie SCPs aktivieren, die bestimmte API-Aufrufe ablehnen. Diese API-Aufrufe können Auswirkungen haben, wie z. B. die unbeabsichtigte Offenlegung personenbezogener Daten oder Verstöße gegen bestimmte grenzüberschreitende Datenübertragungen. Beispielsweise möchten Sie möglicherweise die folgenden API-Aufrufe verbieten:

- Aktivieren des öffentlichen Zugriffs auf Amazon Simple Storage Service (Amazon S3) -Buckets
- Deaktivierung von Amazon GuardDuty oder Erstellung von Regeln zur Unterdrückung von Datenexfiltrationsergebnissen, wie z. B. der Trojan:EC2/DNS-Entdeckung DataExfiltration
- Regeln zur Datenexfiltration löschen AWS WAF
- Öffentliche Freigabe von Amazon Elastic Block Store (Amazon EBS) -Snapshots
- Ein Mitgliedskonto aus der Organisation entfernen
- Amazon CodeGuru Reviewer von einem Repository trennen

Verwaltungsrichtlinien

Mithilfe der darin AWS Organizations enthaltenen Verwaltungsrichtlinien können Sie die zugehörigen Funktionen zentral konfigurieren AWS services und verwalten. Die Art der von Ihnen ausgewählten Verwaltungsrichtlinien bestimmt, wie sich Richtlinien auf die Organisationseinheiten und Konten

auswirken, die sie erben. Tag-Richtlinien sind ein Beispiel für eine Verwaltungsrichtlinie AWS Organizations , die sich direkt auf den Datenschutz bezieht.

Verwenden von Tag-Richtlinien

Tags sind Schlüsselwertpaare, die Ihnen helfen, AWS Ressourcen zu verwalten, zu identifizieren, zu organisieren, zu suchen und zu filtern. Es kann nützlich sein, Tags anzuwenden, die die Ressourcen in Ihrer Organisation, die personenbezogene Daten verarbeiten, voneinander unterscheiden. Die Verwendung von Tags unterstützt viele der Datenschutzlösungen in diesem Handbuch. Möglicherweise möchten Sie beispielsweise ein Tag anwenden, das die allgemeine Datenklassifizierung der Daten angibt, die in der Ressource verarbeitet oder gespeichert werden. Sie können ABAC-Richtlinien (attribute-based access control) schreiben, die den Zugriff auf Ressourcen beschränken, die über ein bestimmtes Tag oder eine Gruppe von Tags verfügen. In Ihrer Richtlinie könnte beispielsweise festgelegt werden, dass die `SysAdmin` Rolle nicht auf Ressourcen zugreifen kann, die das Tag enthalten. `dataclassification:4` Weitere Informationen und ein Tutorial finden Sie in der IAM-Dokumentation unter Definieren von Berechtigungen für den Zugriff auf AWS Ressourcen auf der Grundlage von Tags. Wenn Ihr Unternehmen Datenaufbewahrungsrichtlinien für alle Backups in vielen Konten verwendet AWS Backup, können Sie außerdem ein Tag hinzufügen, das diese Ressource in den Geltungsbereich dieser Backup-Richtlinie einbezieht.

Tag-Richtlinien helfen Ihnen dabei, einheitliche Tags in Ihrer gesamten Organisation aufrechtzuerhalten. In einer Tag-Richtlinie geben Sie Regeln an, die für Ressourcen gelten, wenn sie markiert sind. Sie können beispielsweise festlegen, dass Ressourcen mit bestimmten Schlüsseln wie `DataClassification` oder gekennzeichnet werden`DataSteward`, und Sie können gültige Fallbehandlungen oder Werte für Schlüssel angeben. Sie können die Durchsetzung auch einsetzen, um zu verhindern, dass nicht konforme Tagging-Anfragen abgeschlossen werden.

Wenn Sie Tags als Kernkomponente Ihrer Datenschutzkontrollstrategie verwenden, sollten Sie Folgendes berücksichtigen:

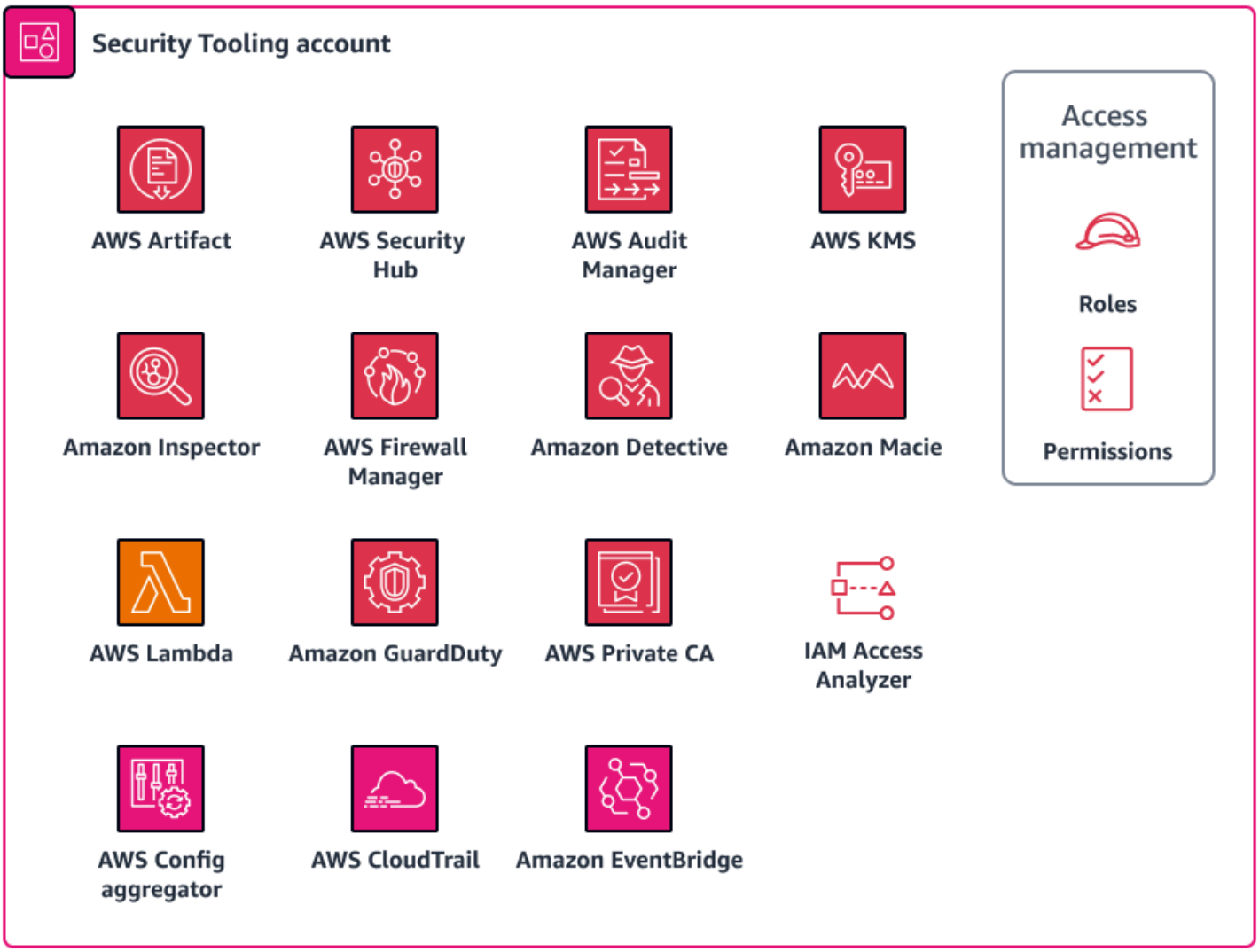
- Bedenken Sie, welche Auswirkungen es hat, personenbezogene Daten oder andere Arten vertraulicher Daten in Tag-Schlüsseln oder -Werten zu platzieren. Wenn Sie technische AWS Unterstützung benötigen, analysieren Sie AWS möglicherweise Tags und andere Ressourcenkennungen, um das Problem zu lösen. In diesem Fall empfiehlt es sich möglicherweise, Tag-Werte zu de-identifizieren und sie anschließend mithilfe eines kundengesteuerten Systems, z. B. eines IT-Servicemanagement-Systems (ITSM), erneut zu identifizieren. AWS empfiehlt, keine personenbezogenen Daten in Tags aufzunehmen.

- Beachten Sie, dass einige Tag-Werte unveränderlich (unveränderbar) gemacht werden müssen, um zu verhindern, dass technische Kontrollen, wie z. B. ABAC-Bedingungen, die auf Tags basieren, umgangen werden.

Security OU — Konto für Sicherheitstools

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Das Security Tooling-Konto ist für den Betrieb grundlegender Sicherheits- und Datenschutzdienste, die Überwachung AWS-Konten und Automatisierung von Sicherheits- und Datenschutzwarnungen und -reaktionen vorgesehen. Weitere Informationen zu diesem Konto finden Sie in der AWS Security Reference Architecture (SRA).AWS Das folgende Diagramm zeigt die AWS Sicherheits- und Datenschutzdienste, die im Security Tooling-Konto konfiguriert sind.



Dieser Abschnitt enthält detailliertere Informationen zu den folgenden Funktionen in diesem Konto:

- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- IAM Access Analyzer
- Amazon Macie

AWS CloudTrail

AWS CloudTrailhilft Ihnen bei der Prüfung der gesamten API-Aktivität in Ihrem AWS-Konto. Wenn Sie alle AWS-Konten Daten aktivieren CloudTrail , AWS-Regionen die personenbezogene Daten

speichern, verarbeiten oder übertragen, können Sie die Verwendung und Offenlegung dieser Daten nachverfolgen. Die AWS Security Reference Architecture empfiehlt, einen Organization Trail zu aktivieren. Dabei handelt es sich um einen einzelnen Trail, der alle Ereignisse für alle Konten in der Organisation protokolliert. Wenn Sie diesen Organisationspfad aktivieren, werden die Protokolldaten mehrerer Regionen jedoch in einem einzigen Amazon Simple Storage Service (Amazon S3) - Bucket im Log Archive-Konto zusammengefasst. Bei Konten, die personenbezogene Daten verarbeiten, kann dies einige zusätzliche Designüberlegungen mit sich bringen. Protokolldatensätze können einige Verweise auf personenbezogene Daten enthalten. Um Ihre Anforderungen an die Datenresidenz und die Datenübertragung zu erfüllen, müssen Sie möglicherweise überdenken, regionsübergreifende Protokolldaten in einer einzigen Region zu aggregieren, in der sich der S3-Bucket befindet. Ihr Unternehmen könnte erwägen, welche regionalen Workloads in den Organisations-Trail aufgenommen oder ausgeschlossen werden sollten. Für Workloads, die Sie aus dem Organisations-Trail ausschließen möchten, könnten Sie erwägen, einen regionsspezifischen Trail zu konfigurieren, der personenbezogene Daten maskiert. Weitere Informationen zum Maskieren personenbezogener Daten finden Sie im Amazon Data Firehose Abschnitt dieses Handbuchs. Letztlich verfügt Ihr Unternehmen möglicherweise über eine Kombination aus Organisationsdaten und regionalen Protokollen, die in einem zentralen Log Archive-Konto zusammengefasst werden.

Weitere Informationen zur Konfiguration eines Trails für einzelne Regionen finden Sie in den Anweisungen zur Verwendung von AWS Command Line Interface (AWS CLI) oder der Konsole. Wenn Sie den Organization Trail erstellen, können Sie eine Opt-in-Einstellung in verwenden AWS Control Tower, oder Sie können den Trail direkt in der CloudTrail Konsole erstellen.

Weitere Informationen zum Gesamtansatz und zur Verwaltung der Zentralisierung von Protokollen und Datenübertragungsanforderungen finden Sie im Zentralisierter Protokollspeicher Abschnitt dieses Handbuchs. Für welche Konfiguration Sie sich auch entscheiden, je nach SRA sollten Sie die Trailverwaltung im Security Tooling-Konto vom Protokollspeicher im Log Archive-Konto trennen. AWS Dieses Design hilft Ihnen bei der Erstellung von Zugriffsrichtlinien mit den geringsten Rechten für diejenigen, die Protokolle verwalten müssen, und für diejenigen, die die Protokolldaten verwenden müssen.

AWS Config

AWS Configbietet einen detaillierten Überblick über die Ressourcen in Ihrem AWS-Konto und deren Konfiguration. Es hilft Ihnen zu erkennen, wie Ressourcen zueinander in Beziehung stehen und wie sich ihre Konfigurationen im Laufe der Zeit geändert haben. Weitere Informationen zur Verwendung dieses Dienstes in einem Sicherheitskontext finden Sie in der AWS Sicherheitsreferenzarchitektur.

In AWS Config können Sie Conformance Packs bereitstellen, bei denen es sich um AWS Config Regelwerke und Abhilfemaßnahmen handelt. Conformance Packs bieten ein Allzweck-Framework, das darauf ausgelegt ist, mithilfe verwalteter oder benutzerdefinierter Regeln Kontrollen im Hinblick auf Datenschutz, Sicherheit, Betrieb und Kostenoptimierung zu ermöglichen. AWS Config Sie können dieses Tool als Teil einer größeren Reihe von Automatisierungstools verwenden, um zu verfolgen, ob Ihre AWS Ressourcenkonfigurationen Ihren eigenen Control-Framework-Anforderungen entsprechen.

Das Konformitätspaket Operational Best Practices for NIST Privacy Framework v1.0 ist auf eine Reihe von datenschutzbezogenen Kontrollen im NIST Privacy Framework abgestimmt. Jede AWS Config Regel gilt für einen bestimmten AWS Ressourcentyp und bezieht sich auf eine oder mehrere NIST Privacy Framework-Kontrollen. Sie können dieses Konformitätspaket verwenden, um die kontinuierliche Einhaltung der Datenschutzbestimmungen für alle Ressourcen in Ihren Konten nachzuverfolgen. Im Folgenden sind einige der Regeln aufgeführt, die in diesem Konformitätspaket enthalten sind:

- `no-unrestricted-route-to-igw`— Diese Regel trägt dazu bei, Datenexfiltration auf der Datenebene zu verhindern, indem sie die VPC-Routentabellen kontinuierlich auf Standard `0.0.0.0/0` - oder `::/0` Ausgangsrouten zu einem Internet-Gateway überwacht. Auf diese Weise können Sie einschränken, wohin internetgebundener Datenverkehr gesendet werden kann, insbesondere wenn es CIDR-Bereiche gibt, von denen bekannt ist, dass sie bösartig sind.
- `encrypted-volumes`— Diese Regel prüft, ob Amazon Elastic Block Store (Amazon EBS) -Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, verschlüsselt sind. Wenn in Ihrem Unternehmen spezifische Kontrollanforderungen gelten, die sich auf die Verwendung von AWS Key Management Service (AWS KMS) -Schlüsseln zum Schutz personenbezogener Daten beziehen, können Sie im Rahmen der Regel spezifische Schlüssel-IDs angeben, um zu überprüfen, ob die Volumes mit einem bestimmten Schlüssel verschlüsselt sind. AWS KMS
- `restricted-common-ports`— Diese Regel prüft, ob Amazon EC2-Sicherheitsgruppen uneingeschränkten TCP-Verkehr zu bestimmten Ports zulassen. Sicherheitsgruppen können Ihnen bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Durch das Blockieren von eingehendem Datenverkehr `0.0.0.0/0` zu gemeinsamen Ports wie TCP 3389 und TCP 21 auf Ihren Ressourcen können Sie den Fernzugriff einschränken.

AWS Config kann sowohl für proaktive als auch für reaktive Konformitätsprüfungen Ihrer AWS Ressourcen verwendet werden. Zusätzlich zur Berücksichtigung der in den Konformitätspaketen

enthaltenen Regeln können Sie diese Regeln sowohl im detektiven als auch im proaktiven Bewertungsmodus verwenden. Auf diese Weise können Datenschutzprüfungen zu einem früheren Zeitpunkt im Softwareentwicklungszyklus implementiert werden, da die Anwendungsentwickler damit beginnen können, Prüfungen vor der Bereitstellung zu integrieren. Sie können beispielsweise Hooks in ihre AWS CloudFormation Vorlagen aufnehmen, die die deklarierte Ressource in der Vorlage anhand aller datenschutzrelevanten AWS Config Regeln überprüfen, für die der proaktive Modus aktiviert ist. Weitere Informationen finden Sie unter AWS Config Rules Now Support Proactive Compliance (AWS Blogbeitrag).

Amazon GuardDuty

AWS bietet mehrere Dienste, die zum Speichern oder Verarbeiten personenbezogener Daten verwendet werden können, wie Amazon S3, Amazon Relational Database Service (Amazon RDS) oder Amazon EC2 mit Kubernetes. Amazon GuardDuty kombiniert intelligente Transparenz mit kontinuierlicher Überwachung, um Indikatoren zu erkennen, die auf eine unbeabsichtigte Offenlegung personenbezogener Daten zurückzuführen sein könnten. Weitere Informationen darüber, wie dieser Service in einem Sicherheitskontext verwendet wird, finden Sie in der AWS Sicherheitsreferenzarchitektur.

Mit GuardDuty können Sie potenziell böswillige, datenschutzrelevante Aktivitäten während des gesamten Lebenszyklus eines Angriffs identifizieren. GuardDuty Kann Sie beispielsweise vor Verbindungen zu Websites auf der schwarzen Liste, ungewöhnlichem Netzwerkportverkehr oder -volumen, DNS-Exfiltration, unerwarteten EC2-Instance-Starts und ungewöhnlichen ISP-Anrufern warnen. Sie können auch so konfigurieren GuardDuty , dass Benachrichtigungen für vertrauenswürdige IP-Adressen aus Ihren eigenen Listen für vertrauenswürdige IP-Adressen und Warnungen vor bekannten bösartigen IP-Adressen aus Ihren eigenen Bedrohungslisten deaktiviert werden.

Wie in der AWS SRA empfohlen, können Sie die Option GuardDuty für alle Benutzer AWS-Konten in Ihrer Organisation aktivieren und das Security Tooling-Konto als GuardDuty delegierter Administrator konfigurieren. GuardDutyfasst Ergebnisse aus dem gesamten Unternehmen in diesem einzigen Konto zusammen. Weitere Informationen finden Sie unter GuardDuty Konten verwalten mit AWS Organizations. Sie können auch in Betracht ziehen, alle datenschutzrelevanten Akteure in den Prozess der Reaktion auf Vorfälle zu identifizieren, von der Erkennung und Analyse bis hin zur Eindämmung und Beseitigung, und sie in alle Vorfälle einzubeziehen, bei denen es zu Datenexfiltration kommen könnte.

IAM Access Analyzer

Viele Kunden möchten stets die Gewissheit haben, dass personenbezogene Daten auf angemessene Weise an vorab zugelassene und vorgesehene Drittanbieter weitergegeben werden und an keine anderen Stellen. Bei einem Datenperimeter handelt es sich um eine Reihe präventiver Schutzmaßnahmen, mit denen nur vertrauenswürdige Identitäten aus den erwarteten Netzwerken auf vertrauenswürdige Ressourcen in Ihrer Umgebung zugreifen können. AWS Bei der Definition von Kontrollen für die unbeabsichtigte und beabsichtigte Offenlegung personenbezogener Daten können Sie vertrauenswürdige Identitäten, vertrauenswürdige Ressourcen und erwartete Netzwerke definieren.

Mit AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) können Unternehmen eine AWS-Konto Vertrauenszone definieren und Warnmeldungen für Verstöße gegen diese Vertrauenszone konfigurieren. IAM Access Analyzer analysiert IAM-Richtlinien, um unbeabsichtigte öffentliche oder kontoübergreifende Zugriffe auf potenziell sensible Ressourcen zu identifizieren und zu beheben. IAM Access Analyzer verwendet mathematische Logik und Inferenz, um umfassende Ergebnisse für Ressourcen zu generieren, auf die von außerhalb zugegriffen werden kann. AWS-Konto Und um auf allzu freizügige IAM-Richtlinien zu reagieren und diese zu korrigieren, können Sie IAM Access Analyzer verwenden, um bestehende Richtlinien anhand von IAM-Best-Practices zu überprüfen und Vorschläge zu unterbreiten. IAM Access Analyzer kann eine IAM-Richtlinie mit den geringsten Rechten generieren, die auf der vorherigen Zugriffsaktivität eines IAM-Prinzipals basiert. Es analysiert CloudTrail Protokolle und generiert eine Richtlinie, die nur die Berechtigungen gewährt, die für die weitere Ausführung dieser Aufgaben erforderlich sind.

Weitere Informationen zur Verwendung von IAM Access Analyzer in einem Sicherheitskontext finden Sie in der AWS Sicherheitsreferenzarchitektur.

Amazon Macie

Amazon Macie ist ein Service, der maschinelles Lernen und Musterabgleich nutzt, um sensible Daten zu erkennen, Einblicke in Datensicherheitsrisiken bietet und Sie dabei unterstützt, den Schutz vor diesen Risiken zu automatisieren. Macie generiert Ergebnisse, wenn es potenzielle Richtlinienverstöße oder Probleme mit der Sicherheit oder dem Datenschutz Ihrer Amazon S3 S3-Buckets feststellt. Macie ist ein weiteres Tool, mit dem Unternehmen Automatisierung implementieren können, um die Einhaltung von Vorschriften zu unterstützen. Weitere Informationen zur Verwendung dieses Dienstes in einem Sicherheitskontext finden Sie in der AWS Sicherheitsreferenzarchitektur.

Macie kann eine große und ständig wachsende Liste vertraulicher Datentypen erkennen, darunter personenbezogene Daten (PII) wie Namen, Adressen und andere identifizierbare Attribute. Sie

können sogar benutzerdefinierte Datenkennungen erstellen, um Erkennungskriterien zu definieren, die der Definition Ihrer Organisation von personenbezogenen Daten entsprechen.

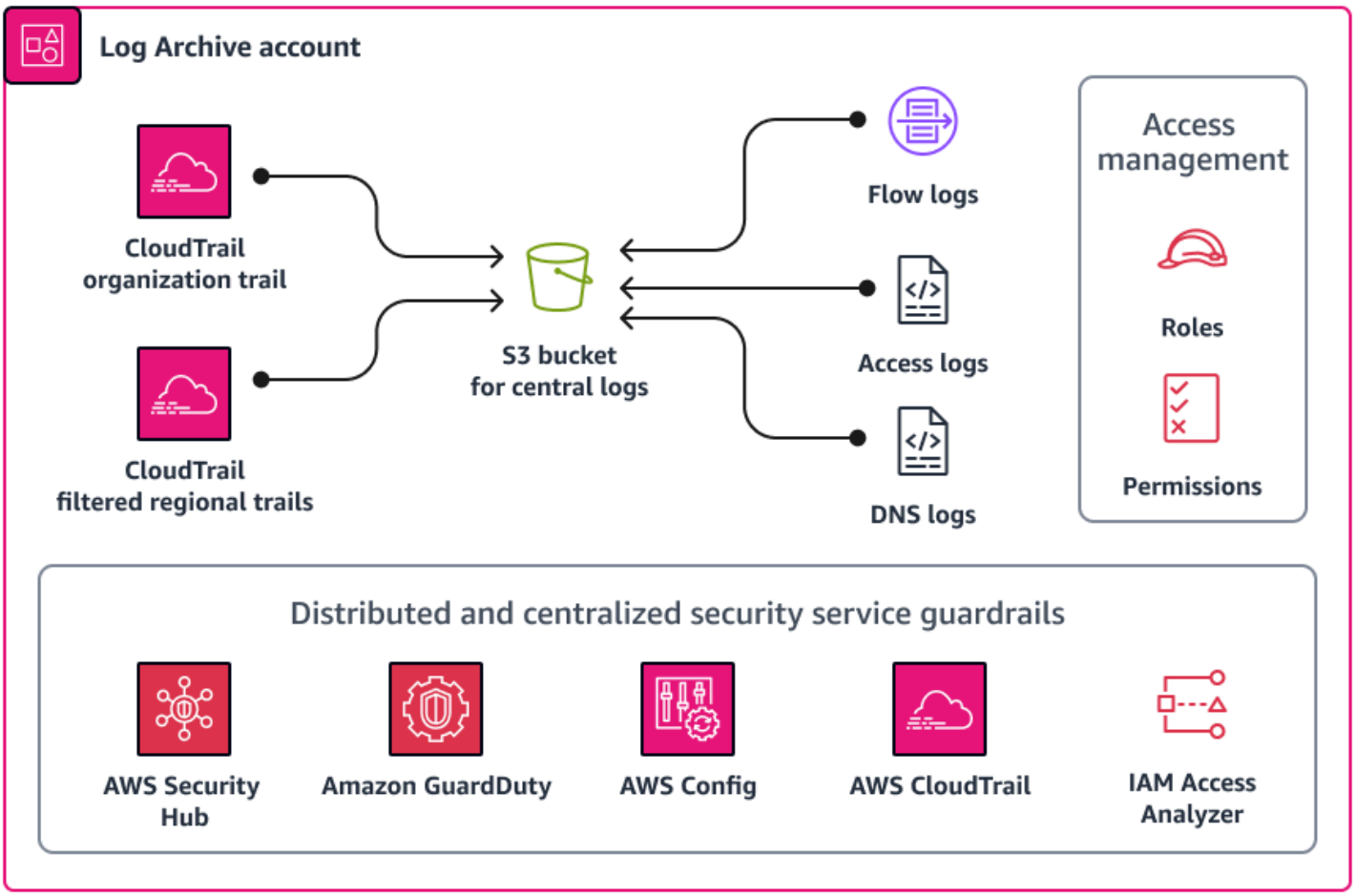
Da Ihr Unternehmen präventive Kontrollen für Ihre Amazon S3 S3-Buckets festlegt, die personenbezogene Daten enthalten, können Sie Macie als Überprüfungsmechanismus verwenden, um kontinuierlich zu überprüfen, wo sich Ihre personenbezogenen Daten befinden und wie sie geschützt sind. Aktivieren Sie zunächst Macie und konfigurieren Sie die automatische Erkennung sensibler Daten. Macie analysiert kontinuierlich Objekte in all Ihren S3-Buckets, kontenübergreifend und. AWS-Regionen Macie generiert und verwaltet eine interaktive Heatmap, die zeigt, wo sich persönliche Daten befinden. Die automatische Erkennungsfunktion für sensible Daten wurde entwickelt, um Kosten zu senken und die Notwendigkeit der manuellen Konfiguration von Discovery-Jobs zu minimieren. Sie können auf der automatischen Erkennungsfunktion vertraulicher Daten aufbauen und Macie verwenden, um automatisch neue Buckets oder neue Daten in vorhandenen Buckets zu erkennen und die Daten dann anhand der zugewiesenen Datenklassifizierungs-Tags zu validieren. Konfigurieren Sie diese Architektur so, dass die entsprechenden Entwicklungs- und Datenschutzteams rechtzeitig über falsch klassifizierte oder nicht klassifizierte Buckets informiert werden.

Sie können Macie für jedes Konto in Ihrer Organisation aktivieren, indem Sie. AWS Organizations Weitere Informationen finden Sie unter Integration und Konfiguration einer Organisation in Amazon Macie.

Security OU — Konto protokollieren

> Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Mit dem Log Archive-Konto zentralisieren Sie Infrastruktur-, Service- und Anwendungsprotokolltypen. Weitere Informationen zu diesem Konto finden Sie in der AWS Security Reference Architecture (AWS SRA). Mit einem speziellen Konto für Protokolle können Sie konsistente Warnmeldungen für alle Protokolltypen einrichten und sicherstellen, dass Incident Responder von einem zentralen Ort aus auf eine Zusammenfassung dieser Protokolle zugreifen können. Sie können auch Sicherheitskontrollen und Richtlinien zur Datenspeicherung von einem zentralen Ort aus einrichten, was den betrieblichen Aufwand für den Datenschutz vereinfachen kann. Das folgende Diagramm zeigt die AWS Sicherheits- und Datenschutzdienste, die im Log Archive-Konto konfiguriert sind.



Zentralisierter Protokollspeicher

Protokolldateien (z. B. AWS CloudTrail Protokolle) können Informationen enthalten, die als personenbezogene Daten betrachtet werden könnten. Einige Organisationen entscheiden sich für die Verwendung eines Organization Trails, um die CloudTrail Logs kontenübergreifend AWS-Regionen und kontenübergreifend an einem zentralen Ort zu sammeln, um die Übersicht zu behalten. Weitere Informationen finden Sie unter AWS CloudTrail in diesem Handbuch. Bei der Implementierung der Zentralisierung von CloudTrail Protokollen werden die Protokolle normalerweise in einem Amazon Simple Storage Service (Amazon S3) -Bucket in einer einzigen Region gespeichert.

Abhängig von der Definition personenbezogener Daten in Ihrem Unternehmen und den geltenden regionalen Datenschutzbestimmungen müssen Sie möglicherweise grenzüberschreitende Datenübertragungen in Betracht ziehen. Wenn Ihr Unternehmen die Datenübertragungsanforderungen der regionalen Datenschutzbestimmungen erfüllen muss, können Ihnen die folgenden Optionen helfen:

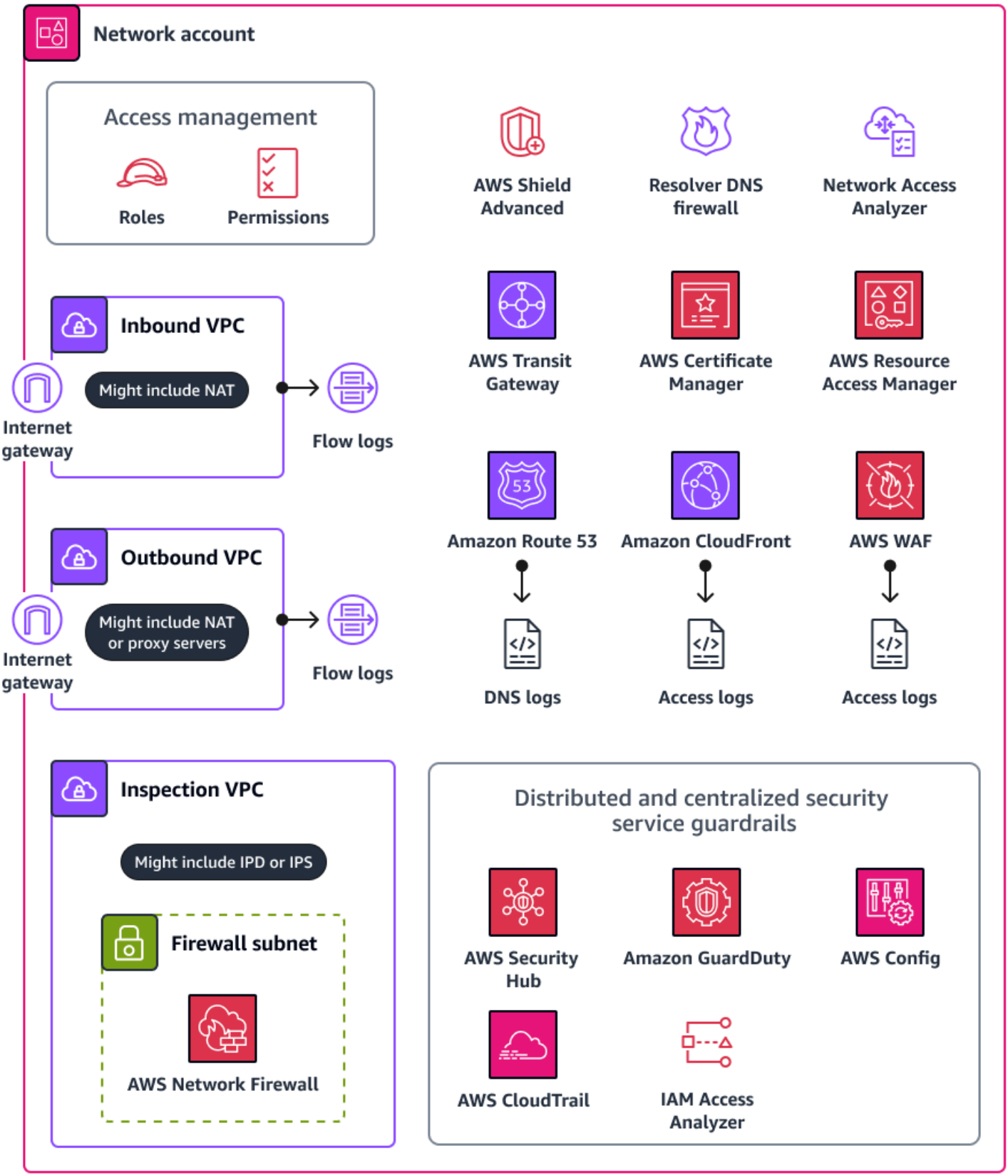
1. Wenn Ihre Organisation Dienste für Datensubjekte in mehreren Ländern anbietet, können Sie sich dafür entscheiden, alle Protokolle in dem Land zu aggregieren, in dem die strengsten Anforderungen an die Datenresidenz gelten. AWS Cloud Wenn Sie beispielsweise in Deutschland tätig sind und dort die strengsten Anforderungen gelten, könnten Sie Daten in einem S3-Bucket aggregieren, `eu-central-1` AWS-Region sodass die in Deutschland gesammelten Daten die Grenzen Deutschlands nicht verlassen. Für diese Option können Sie einen einzelnen Organisationspfad konfigurieren CloudTrail , in dem Logs aus allen Konten und AWS-Regionen in der Zielregion zusammengefasst werden.
2. Redigieren Sie die personenbezogenen Daten, die in der verbleiben müssen, AWS-Region bevor die Daten kopiert und in eine andere Region aggregiert werden. Sie können beispielsweise die personenbezogenen Daten in der Hostregion der Anwendung maskieren, bevor Sie die Protokolle in eine andere Region übertragen. Weitere Informationen zum Maskieren personenbezogener Daten finden Sie im Amazon Data Firehose Abschnitt dieses Handbuchs.

Ermitteln Sie gemeinsam mit Ihrem Rechtsberater, welche personenbezogenen Daten in den Geltungsbereich fallen und welche Übertragungen von Region zu AWS Region zulässig sind.

Infrastruktur-OE – Netzwerkkonto

> Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Im Netzwerkkonto verwalten Sie das Netzwerk zwischen Ihren virtuellen privaten Clouds (VPCs) und dem breiteren Internet. In diesem Konto können Sie umfassende Mechanismen zur Offenlegungskontrolle implementieren, indem Sie AWS Resource Access Manager (AWS RAM) verwenden AWS WAF, um VPC-Subnetze und AWS Transit Gateway -Anhänge gemeinsam zu nutzen, und Amazon verwenden, um die gezielte Nutzung von Diensten CloudFront zu unterstützen. Weitere Informationen zu diesem Konto finden Sie in der AWS Security Reference Architecture (AWS SRA). Das folgende Diagramm zeigt die AWS Sicherheits- und Datenschutzdienste, die im Netzwerkkonto konfiguriert sind.


Network account
Access management
Roles
Permissions
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
Inbound VPC
Might include NAT
Internet gateway
Flow logs
AWS Transit Gateway
AWS Certificate Manager
AWS Resource Access Manager
Amazon Route 53
Amazon CloudFront
AWS WAF
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
DNS logs
Access logs
Access logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

Dieser Abschnitt enthält detailliertere Informationen zu den folgenden Komponenten AWS services , die in diesem Konto verwendet werden:

- Amazon CloudFront
- AWS Resource Access Manager
- AWS Transit Gateway
- AWS WAF

Amazon CloudFront

Amazon CloudFront unterstützt geografische Einschränkungen für Frontend-Anwendungen und Datei-Hosting. CloudFrontkann Inhalte über ein weltweites Netzwerk von Rechenzentren bereitstellen, die als Edge-Standorte bezeichnet werden. Wenn ein Benutzer Inhalte anfordert, die Sie bereitstellen CloudFront, wird die Anfrage an den Edge-Standort weitergeleitet, der die niedrigste Latenz bietet. Weitere Informationen zur Verwendung dieses Dienstes in einem Sicherheitskontext finden Sie in der AWS Sicherheitsreferenzarchitektur.

Sie können CloudFront geografische Beschränkungen verwenden, um zu verhindern, dass Benutzer an bestimmten geografischen Standorten auf Inhalte zugreifen, die Sie über eine CloudFront Distribution verteilen. Weitere Informationen und Konfigurationsoptionen für geografische Einschränkungen finden Sie in der CloudFront Dokumentation unter Beschränken der geografischen Verteilung Ihrer Inhalte.

Sie können auch so konfigurieren CloudFront , dass Zugriffsprotokolle generiert werden, die detaillierte Informationen zu jeder eingehenden Benutzeranfrage enthalten CloudFront . Weitere Informationen finden Sie in der CloudFront Dokumentation unter Konfiguration und Verwendung von Standardprotokollen (Zugriffsprotokollen). Und wenn CloudFront es so konfiguriert ist, dass Inhalte an einer Reihe von Edge-Standorten zwischengespeichert werden, sollten Sie sich überlegen, wo das Caching stattfindet. Für einige Organisationen kann regionsübergreifendes Caching Anforderungen für die grenzüberschreitende Datenübertragung gelten.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) hilft Ihnen dabei, Ihre Ressourcen sicher gemeinsam zu nutzen, AWS-Konten um den betrieblichen Aufwand zu reduzieren und für Transparenz und Überprüfbarkeit zu sorgen. Mit können Unternehmen einschränken AWS RAM, welche AWS Ressourcen mit anderen AWS-Konten innerhalb ihrer Organisation oder mit Konten von Drittanbietern gemeinsam genutzt werden können. Weitere Informationen finden Sie unter

Gemeinsam nutzbare AWS Ressourcen. Im Netzwerkkonto können Sie VPC-Subnetze und Transit-Gateway-Verbindungen gemeinsam nutzen AWS RAM . Wenn Sie AWS RAM eine Datenebenenverbindung mit einer anderen teilen, sollten Sie in Erwägung ziehen AWS-Konto, Prozesse einzurichten, um zu überprüfen, ob die Verbindungen hergestellt und vorab genehmigt wurden. AWS-Regionen

Neben der gemeinsamen Nutzung von VPCs und Transit-Gateway-Verbindungen AWS RAM können auch Ressourcen gemeinsam genutzt werden, die keine ressourcenbasierten IAM-Richtlinien unterstützen. Für einen Workload, der in der Organisationseinheit „Persönliche Daten“ gehostet wird, können Sie AWS RAM damit auf persönliche Daten zugreifen, die sich in einer separaten Organisationseinheit befinden. AWS-Konto Weitere Informationen finden Sie AWS Resource Access Manager im Abschnitt Persönliche Daten OU — PD-Anwendungskonto.

AWS Transit Gateway

Wenn Sie AWS Ressourcen zur Erfassung, Speicherung oder Verarbeitung personenbezogener Daten gemäß den Anforderungen Ihres Unternehmens einsetzen möchten und über AWS-Regionen die entsprechenden technischen Sicherheitsvorkehrungen verfügen, sollten Sie die Implementierung von Schutzmaßnahmen in Betracht ziehen, um unbefugte grenzüberschreitende Datenflüsse auf der Kontroll- und Datenebene zu verhindern. Auf der Kontrollebene können Sie die Nutzung von Regionen und damit den regionsübergreifenden Datenfluss mithilfe von IAM- und Dienststeuerungsrichtlinien einschränken.

Es gibt mehrere Optionen zur Steuerung regionsübergreifender Datenflüsse auf der Datenebene. Sie können beispielsweise Routentabellen, VPC-Peering und AWS Transit Gateway Anlagen verwenden. AWS Transit Gatewayist ein zentraler Hub, der virtuelle private Clouds (VPCs) und lokale Netzwerke verbindet. Als Teil Ihrer größeren AWS-Landezone können Sie die verschiedenen Arten der Datenübertragung berücksichtigen, z. B. über Internet-Gateways AWS-Regionen, durch direktes VPC-zu-VPC-Peering und durch regionsübergreifendes Peering mit. AWS Transit Gateway Sie können beispielsweise Folgendes tun in: AWS Transit Gateway

- Vergewissern Sie sich, dass die Ost-West- und Nord-Süd-Verbindungen zwischen Ihren VPCs und lokalen Umgebungen Ihren Datenschutzanforderungen entsprechen.
- Konfigurieren Sie die VPC-Einstellungen gemäß Ihren Datenschutzanforderungen.
- Verwenden Sie eine Service-Kontrollrichtlinie in AWS Organizations - und IAM-Richtlinien, um Änderungen an Ihren Konfigurationen AWS Transit Gateway und an Ihrer Amazon Virtual Private Cloud (Amazon VPC) -Konfiguration zu verhindern. Ein Beispiel für eine Service-Kontrollrichtlinie finden Sie Änderungen an VPC-Konfigurationen einschränken in diesem Handbuch.

AWS WAF

Um die unbeabsichtigte Offenlegung personenbezogener Daten zu verhindern, können Sie einen defense-in-depth Ansatz für Ihre Webanwendungen verwenden. Sie können Eingabevalidierung und Ratenbegrenzung in Ihre Anwendung integrieren, AWS WAF können aber auch als weitere Verteidigungslinie dienen. AWS WAFist eine Firewall für Webanwendungen, mit der Sie HTTP- und HTTPS-Anfragen überwachen können, die an Ihre geschützten Webanwendungsressourcen weitergeleitet werden. Weitere Informationen zur Verwendung dieses Dienstes in einem Sicherheitskontext finden Sie in der AWS Sicherheitsreferenzarchitektur.

Mit AWS WAF können Sie Regeln definieren und bereitstellen, die nach bestimmten Kriterien suchen. Die folgenden Aktivitäten können mit der unbeabsichtigten Offenlegung personenbezogener Daten verbunden sein:

- Datenverkehr von unbekannten oder bösartigen IP-Adressen oder geografischen Standorten
- Die 10 häufigsten Angriffe des Open Worldwide Application Security Project (OWASP), einschließlich Exfiltrationsangriffen wie SQL-Injection
- Hohe Anforderungsraten
- Allgemeiner Bot-Verkehr
- Inhaltsschaber

Sie können AWS WAF Regelgruppen bereitstellen, die von AWS verwaltet werden. Einige verwaltete Regelgruppen für AWS WAF können verwendet werden, um Bedrohungen für den Datenschutz und persönliche Daten zu erkennen, zum Beispiel:

- SQL-Datenbank — Diese Regelgruppe enthält Regeln, mit denen Anforderungsmuster blockiert werden sollen, die mit der Ausnutzung von SQL-Datenbanken wie SQL-Injection-Angriffen in Verbindung stehen. Ziehen Sie diese Regelgruppe in Betracht, wenn Ihre Anwendung eine Schnittstelle zu einer SQL-Datenbank hat.
- Bekannte fehlerhafte Eingaben — Diese Regelgruppe enthält Regeln zum Blockieren von Anforderungsmustern, die bekanntermaßen ungültig sind und im Zusammenhang mit der Ausnutzung oder Entdeckung von Sicherheitslücken stehen.
- Bot-Kontrolle — Diese Regelgruppe enthält Regeln zur Verwaltung von Anfragen von Bots, die überschüssige Ressourcen verbrauchen, Geschäftskennzahlen verfälschen, Ausfallzeiten verursachen und böswillige Aktivitäten ausführen können.

- Verhinderung von Kontoübernahmen (ATP) — Diese Regelgruppe enthält Regeln, die böswillige Kontoübernahmeversuche verhindern sollen. Diese Regelgruppe untersucht die Anmeldeversuche, die an den Anmeldeendpunkt Ihrer Anwendung gesendet werden.

Personenbezogene Daten (OU — PD), Anwendungskonto

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

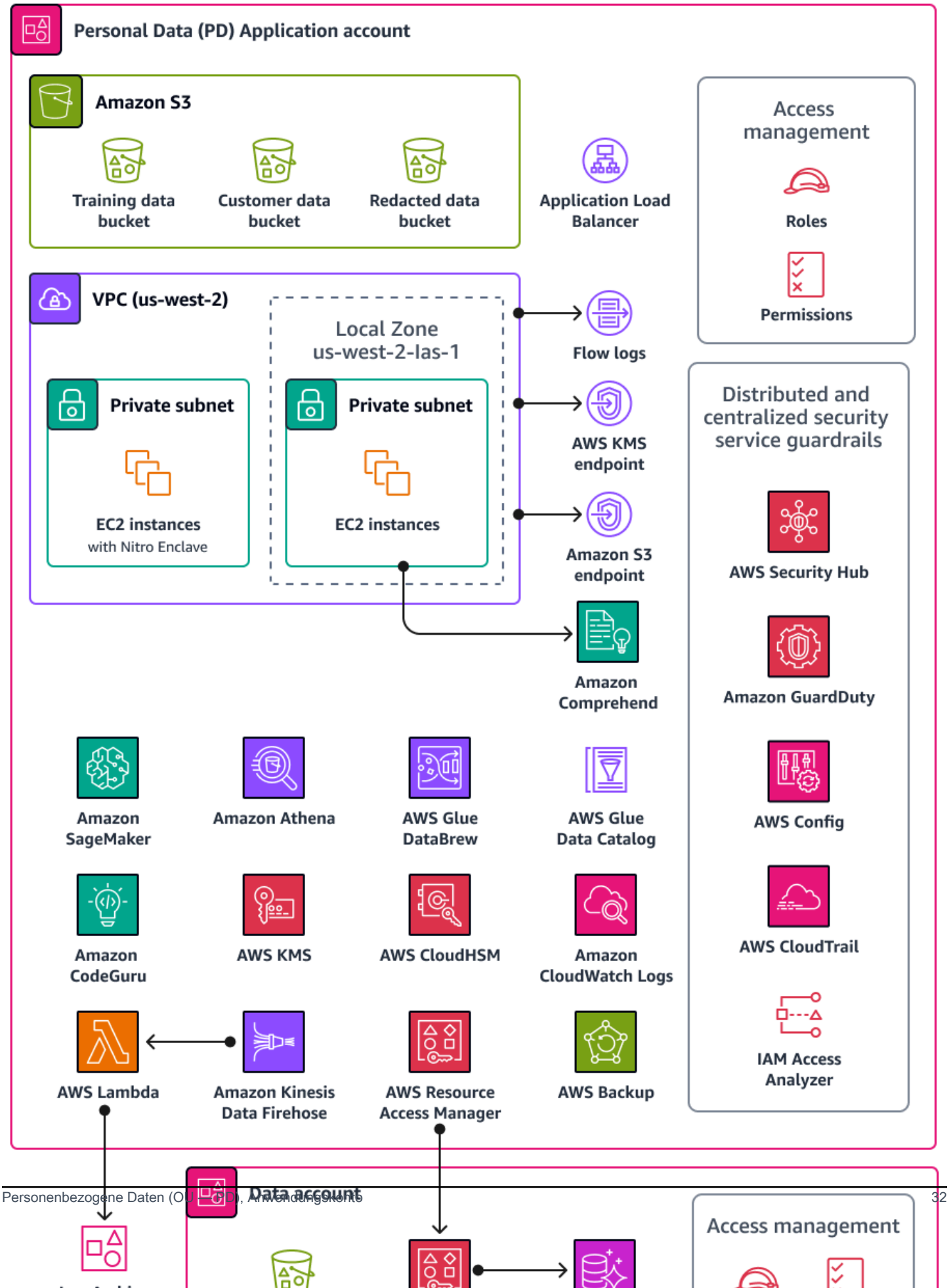
Das Anwendungskonto für personenbezogene Daten (PD) ist der Ort, an dem Ihr Unternehmen Dienste hostet, die personenbezogene Daten erheben und verarbeiten. Insbesondere können Sie in diesem Konto speichern, was Sie als personenbezogene Daten definieren. Die AWS PRA demonstriert anhand einer mehrstufigen serverlosen Webarchitektur eine Reihe von Beispielkonfigurationen für den Datenschutz. Wenn es darum geht, Workloads in einer AWS landing zone zu betreiben, sollten Datenschutzkonfigurationen nicht als one-size-fits-all Lösung betrachtet werden. Ihr Ziel könnte beispielsweise darin bestehen, die zugrunde liegenden Konzepte zu verstehen, zu erfahren, wie sie den Datenschutz verbessern können und wie Ihr Unternehmen Lösungen für Ihre speziellen Anwendungsfälle und Architekturen anwenden kann.

Denn AWS-Konten in Ihrem Unternehmen, das personenbezogene Daten sammelt, speichert oder verarbeitet, können Sie grundlegende AWS Organizations und wiederholbare AWS Control Tower Schutzmaßnahmen verwenden und einsetzen. Die Einrichtung einer eigenen Organisationseinheit (OU) für diese Konten ist von entscheidender Bedeutung. Möglicherweise möchten Sie Schutzmaßnahmen für die Datenresidenz nur auf eine Teilmenge von Konten anwenden, bei denen die Datenspeicherung eine zentrale Entwurfsüberlegung ist. Für viele Organisationen sind dies die Konten, die personenbezogene Daten speichern und verarbeiten.

Ihre Organisation unterstützt möglicherweise ein spezielles Datenkonto, in dem Sie die maßgebliche Quelle Ihrer persönlichen Datensätze speichern. Eine autoritative Datenquelle ist ein Ort, an dem Sie die Primärversion von Daten speichern, die als die zuverlässigste und genaueste Version der Daten angesehen werden kann. Beispielsweise können Sie die Daten aus der autoritativen Datenquelle an andere Speicherorte kopieren, z. B. in Amazon Simple Storage Service (Amazon S3) -Buckets im PD-Anwendungskonto, die zum Speichern von Trainingsdaten, einer Teilmenge von Kundendaten und geschwärzten Daten verwendet werden. Indem Sie diesen Ansatz mit mehreren Konten verwenden, um vollständige und endgültige personenbezogene Datensätze im Datenkonto

von den nachgelagerten Kunden-Workloads im PD-Anwendungskonto zu trennen, können Sie den Umfang der Auswirkungen verringern, die bei einem unbefugten Zugriff auf Ihre Konten entstehen.

Das folgende Diagramm zeigt die AWS Sicherheits- und Datenschutzdienste, die in den Konten PD Application und Data konfiguriert sind.


Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application Load Balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local Zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Amazon Comprehend
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon SageMaker
Amazon Athena
AWS Glue DataBrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
Data account
Access management
Log Archive

Dieser Abschnitt enthält detailliertere Informationen zu den folgenden Elementen AWS services , die in diesen Konten verwendet werden:

- Amazon Athena
- CloudWatch Amazon-Protokolle
- CodeGuru Amazon-Rezensent
- Amazon Comprehend
- Amazon Data Firehose
- AWS Glue
- AWS Key Management Service
- AWS Local Zones
- AWS Nitro-Enklaven
- AWS PrivateLink
- AWS Resource Access Manager
- Amazon SageMaker
- AWS Funktionen, die bei der Verwaltung des Datenlebenszyklus helfen
- AWS-Services und -Funktionen zur Segmentierung von Daten

Amazon Athena

Sie können auch Kontrollen zur Beschränkung von Datenabfragen in Betracht ziehen, um Ihre Datenschutzziele zu erreichen. Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten mithilfe von Standard-SQL direkt in Amazon S3 analysieren können. Sie müssen die Daten nicht in Athena laden; es funktioniert direkt mit den in S3-Buckets gespeicherten Daten.

Ein häufiger Anwendungsfall für Athena ist die Bereitstellung maßgeschneiderter und bereinigter Datensätze für Datenanalyseteams. Wenn die Datensätze personenbezogene Daten enthalten, können Sie den Datensatz bereinigen, indem Sie ganze Spalten mit personenbezogenen Daten maskieren, die für die Datenanalyseteams wenig Wert bieten. Weitere Informationen finden Sie unter Anonymisieren und verwalten Sie Daten in Ihrem Data Lake mit Amazon Athena und AWS Lake Formation (AWS Blogbeitrag).

Wenn Ihr Datentransformationsansatz zusätzliche Flexibilität außerhalb der unterstützten Funktionen in Athena erfordert, können Sie benutzerdefinierte Funktionen definieren, die als benutzerdefinierte

Funktionen (UDF) bezeichnet werden. Sie können UDFs in einer an Athena gesendeten SQL-Abfrage aufrufen, und sie werden dann ausgeführt. AWS Lambda Sie können UDFs in `SELECT` und `FILTER SQL` -Abfragen verwenden, und Sie können mehrere UDFs in derselben Abfrage aufrufen. Aus Datenschutzgründen können Sie UDFs erstellen, die bestimmte Arten der Datenmaskierung durchführen, z. B. nur die letzten vier Zeichen jedes Werts in einer Spalte anzeigen.

CloudWatch Amazon-Protokolle

Amazon CloudWatch Logs hilft Ihnen dabei, die Protokolle all Ihrer Systeme und Anwendungen zu zentralisieren, AWS services sodass Sie sie überwachen und sicher archivieren können. In CloudWatch Logs können Sie eine Datenschutzrichtlinie für neue oder bestehende Protokollgruppen verwenden, um das Risiko der Offenlegung personenbezogener Daten zu minimieren. Mithilfe von Datenschutzrichtlinien können sensible Daten, wie z. B. personenbezogene Daten, in Ihren Protokollen erkannt werden. Die Datenschutzrichtlinie kann diese Daten maskieren, wenn Benutzer über die auf die Protokolle zugreifen AWS Management Console. Wenn Benutzer gemäß der allgemeinen Zweckspezifikation für Ihren Workload direkten Zugriff auf die personenbezogenen Daten benötigen, können Sie diesen Benutzern `logs:Unmask` Berechtigungen zuweisen. Sie können auch eine kontoweite Datenschutzrichtlinie erstellen und diese Richtlinie einheitlich auf alle Konten in Ihrer Organisation anwenden. Dadurch wird die Maskierung standardmäßig für alle aktuellen und future Protokollgruppen in CloudWatch Logs konfiguriert. Wir empfehlen außerdem, Prüfberichte zu aktivieren und sie an eine andere Protokollgruppe, einen Amazon S3 S3-Bucket oder Amazon Data Firehose zu senden. Diese Berichte enthalten eine detaillierte Aufzeichnung der Datenschutzergebnisse für jede Protokollgruppe.

CodeGuru Amazon-Rezensent

Sowohl aus Datenschutz- als auch aus Sicherheitsgründen ist es für viele Unternehmen von entscheidender Bedeutung, dass sie die kontinuierliche Einhaltung der Vorschriften sowohl während der Implementierung als auch nach der Bereitstellung gewährleisten. Die AWS PRA beinhaltet proaktive Kontrollen in den Bereitstellungspipelines für Anwendungen, die personenbezogene Daten verarbeiten. Amazon CodeGuru Reviewer kann potenzielle Fehler erkennen, durch die personenbezogene Daten in Java- und Python-Code offengelegt werden könnten. JavaScript Es bietet Entwicklern Vorschläge zur Verbesserung des Codes. CodeGuru Der Prüfer kann Fehler anhand einer Vielzahl von bewährten Methoden in den Bereichen Sicherheit, Datenschutz und allgemeine Sicherheit identifizieren. Weitere Informationen finden Sie in der Amazon CodeGuru Detector Library. Es wurde für die Zusammenarbeit mit mehreren Quellanbietern entwickelt AWS CodeCommit, darunter Bitbucket und Amazon S3. GitHub Zu den Datenschutzmängeln, die der CodeGuru Prüfer erkennen kann, gehören:

- SQL-Injektion
- Unsichere Cookies
- Fehlende Autorisierung
- Clientseitige Neuverschlüsselung AWS KMS

Amazon Comprehend

Amazon Comprehend ist ein Service zur Verarbeitung natürlicher Sprache (NLP), der maschinelles Lernen nutzt, um wertvolle Erkenntnisse und Zusammenhänge in englischen Textdokumenten aufzudecken. Amazon Comprehend kann personenbezogene Daten in strukturierten, halbstrukturierten oder unstrukturierten Textdokumenten erkennen und redigieren. Weitere Informationen finden Sie unter Persönlich identifizierbare Informationen (PII) in der Amazon Comprehend Comprehend-Dokumentation.

Sie können die AWS-SDKs und die Amazon Comprehend-API verwenden, um Amazon Comprehend in viele Anwendungen zu integrieren. Ein Beispiel ist die Verwendung von Amazon Comprehend zum Erkennen und Redigieren personenbezogener Daten mit Amazon S3 Object Lambda. Organizations können S3 Object Lambda verwenden, um Amazon S3 S3-GET-Anfragen benutzerdefinierten Code hinzuzufügen, um Daten zu ändern und zu verarbeiten, wenn sie an eine Anwendung zurückgegeben werden. S3 Object Lambda kann Zeilen filtern, die Größe von Bildern dynamisch ändern, persönliche Daten redigieren und vieles mehr. Der Code wird von AWS Lambda Funktionen unterstützt und läuft auf einer Infrastruktur, die vollständig verwaltet wird AWS, sodass Sie keine abgeleiteten Kopien Ihrer Daten erstellen und speichern oder Proxys ausführen müssen. Sie müssen Ihre Anwendungen nicht ändern, um Objekte mit S3 Object Lambda zu transformieren. Sie können die `ComprehendPiiRedactionS3Object` Lambda-Funktion verwenden, um persönliche Daten AWS Serverless Application Repository zu redigieren. Diese Funktion verwendet Amazon Comprehend, um Entitäten mit personenbezogenen Daten zu erkennen und diese Entitäten zu redigieren, indem sie durch Sternchen ersetzt werden. Weitere Informationen finden Sie unter Erkennen und Redigieren von PII-Daten mit S3 Object Lambda und Amazon Comprehend in der Amazon S3 S3-Dokumentation.

Da Amazon Comprehend viele Optionen für die Anwendungsintegration über AWS-SDKs bietet, können Sie Amazon Comprehend verwenden, um personenbezogene Daten an vielen verschiedenen Orten zu identifizieren, an denen Sie Daten sammeln, speichern und verarbeiten. Sie können die Funktionen von Amazon Comprehend ML verwenden, um personenbezogene Daten in Anwendungsprotokollen (AWS Blogbeitrag), Kunden-E-Mails, Support-Tickets und mehr zu erkennen

und zu redigieren. Das Architekturdiagramm für das PD-Anwendungskonto zeigt, wie Sie diese Funktion für Anwendungsprotokolle auf Amazon EC2 ausführen können. Amazon Comprehend bietet zwei Redaktionsmodi:

- `REPLACE_WITH_PII_ENTITY_TYPE`ersetzt jede PII-Entität durch ihre Typen. Zum Beispiel würde Jane Doe durch NAME ersetzt werden.
- `MASK`ersetzt die Zeichen in PII-Entitäten durch ein Zeichen Ihrer Wahl (! , #, $,%, &,, oder @). Jane Doe könnte beispielsweise durch **** *** ersetzt werden.

Amazon Data Firehose

Amazon Data Firehose kann verwendet werden, um Streaming-Daten zu erfassen, zu transformieren und in nachgelagerte Dienste wie Amazon Managed Service für Apache Flink oder Amazon S3 zu laden. Firehose wird häufig verwendet, um große Mengen an Streaming-Daten, wie z. B. Anwendungsprotokolle, zu transportieren, ohne dass Verarbeitungspipelines von Grund auf neu erstellt werden müssen.

Sie können Lambda-Funktionen verwenden, um eine benutzerdefinierte oder integrierte Verarbeitung durchzuführen, bevor die Daten flussabwärts gesendet werden. Aus Datenschutzgründen unterstützt diese Funktion die Datenminimierung und Anforderungen an die grenzüberschreitende Datenübertragung. Sie können beispielsweise Lambda und Firehose verwenden, um Protokolldaten aus mehreren Regionen zu transformieren, bevor sie im Log Archive-Konto zentralisiert werden. Weitere Informationen finden Sie unter Biogen: Zentralisierte Protokollierungslösung für mehrere Konten (Video). YouTube Im PD-Anwendungskonto konfigurieren Sie Amazon CloudWatch und die Übertragung von Protokollen AWS CloudTrail an einen Firehose-Lieferstream. Eine Lambda-Funktion transformiert die Protokolle und sendet sie an einen zentralen S3-Bucket im Log Archive-Konto. Sie können die Lambda-Funktion so konfigurieren, dass bestimmte Felder, die personenbezogene Daten enthalten, maskiert werden. Dies trägt dazu bei, die Übertragung personenbezogener Daten zwischen AWS-Regionen den anderen zu verhindern. Durch diesen Ansatz werden die personenbezogenen Daten vor der Übertragung und Zentralisierung maskiert und nicht danach. Bei Anträgen in Jurisdiktionen, die nicht den Anforderungen für die grenzüberschreitende Übertragung unterliegen, ist es in der Regel betrieblich effizienter und kostengünstiger, die Protokolle im Rahmen der organisatorischen Erfassung zusammenzustellen. CloudTrail Weitere Informationen finden Sie AWS CloudTrail im Abschnitt Security OU — Security Tooling-Konto dieses Handbuchs.

AWS Glue

Die Pflege von Datensätzen, die personenbezogene Daten enthalten, ist ein wichtiger Bestandteil von Privacy by Design. Die Daten einer Organisation können in strukturierter, halbstrukturierter oder unstrukturierter Form vorliegen. Personenbezogene Datensätze ohne Struktur können die Durchführung einer Reihe von Maßnahmen zur Verbesserung des Datenschutzes erschweren, darunter die Datenminimierung, das Aufspüren von Daten, die einer einzelnen betroffenen Person im Rahmen einer Anfrage einer betroffenen Person zugeschrieben wurden, die Sicherstellung einer konsistenten Datenqualität und die allgemeine Segmentierung von Datensätzen. AWS Glueist ein vollständig verwalteter ETL-Service (Extrahieren, Transformieren und Laden). Er kann Ihnen helfen, Daten zu kategorisieren, zu bereinigen, anzureichern und zwischen Datenspeichern und Datenströmen zu verschieben. AWS Glue Funktionen sollen Ihnen helfen, Datensätze für Analysen, maschinelles Lernen und Anwendungsentwicklung zu entdecken, vorzubereiten, zu strukturieren und zu kombinieren. Sie können sie verwenden AWS Glue , um zusätzlich zu Ihren vorhandenen Datensätzen eine vorhersehbare und gemeinsame Struktur zu erstellen. AWS Glue Data Catalog AWS Glue DataBrew, und AWS Glue Datenqualität sind AWS Glue Funktionen, die dazu beitragen können, die Datenschutzanforderungen Ihres Unternehmens zu erfüllen.

AWS Glue Data Catalog

AWS Glue Data Cataloghilft Ihnen dabei, verwaltbare Datensätze einzurichten. Der Datenkatalog enthält Verweise auf Daten, die als Quellen und Ziele für Extraktions-, Transformations- und Ladeaufträge (ETL) verwendet werden. AWS Glue Die Informationen im Datenkatalog werden als Metadatentabellen gespeichert, und jede Tabelle gibt einen einzelnen Datenspeicher an. Sie führen einen AWS Glue Crawler aus, um die Daten in einer Vielzahl von Datenspeichertypen zu inventarisieren. Sie fügen dem Crawler integrierte und benutzerdefinierte Klassifikatoren hinzu, und diese Klassifikatoren leiten das Datenformat und das Schema der persönlichen Daten ab. Der Crawler schreibt dann die Metadaten in den Datenkatalog. Eine zentralisierte Metadatentabelle kann es einfacher machen, auf Anfragen von betroffenen Personen (z. B. das Recht auf Löschung) zu reagieren, da sie für Struktur und Vorhersehbarkeit bei unterschiedlichen Quellen personenbezogener Daten in Ihrer Umgebung sorgt. AWS Ein umfassendes Beispiel dafür, wie Sie Data Catalog verwenden können, um automatisch auf diese Anfragen zu antworten, finden Sie unter Umgang mit Datenlöschanfragen in Ihrem Data Lake mit Amazon S3 Find and Forget (AWS Blogbeitrag). Und schließlich ist der Datenkatalog eine AWS Lake FormationSchlüsselkomponente, wenn Ihr Unternehmen die Verwaltung und Bereitstellung eines differenzierten Zugriffs auf Datenbanken, Tabellen, Zeilen und Zellen verwendet. Data Catalog ermöglicht die kontenübergreifende gemeinsame Nutzung von Daten und unterstützt Sie

dabei, mithilfe der tagbasierten Zugriffskontrolle Ihren Data Lake in großem Umfang zu verwalten (Blogbeitrag).AWS

AWS Glue DataBrew

AWS Glue DataBrewunterstützt Sie bei der Bereinigung und Normalisierung von Daten und kann Transformationen an den Daten durchführen, z. B. das Entfernen oder Maskieren personenbezogener Daten und das Verschlüsseln sensibler Datenfelder in Daten-Pipelines. Sie können die Herkunft Ihrer Daten auch visuell abbilden, um die verschiedenen Datenquellen und Transformationsschritte zu verstehen, die die Daten durchlaufen haben. Diese Funktion wird immer wichtiger, da Ihr Unternehmen daran arbeitet, die Herkunft personenbezogener Daten besser zu verstehen und nachzuverfolgen. DataBrew hilft Ihnen dabei, personenbezogene Daten bei der Datenaufbereitung zu maskieren. Sie können im Rahmen der Erstellung von Datenprofilen personenbezogene Daten erkennen und Statistiken erstellen, z. B. die Anzahl der Spalten, die personenbezogene Daten enthalten könnten, und mögliche Kategorien. Anschließend können Sie integrierte Techniken zur umkehrbaren oder irreversiblen Datentransformation verwenden, einschließlich Substitution, Hashing, Verschlüsselung und Entschlüsselung, ohne Code schreiben zu müssen. Sie können die bereinigten und maskierten Datensätze anschließend für Analyse-, Berichts- und Machine-Learning-Aufgaben verwenden. Zu den in verfügbaren Techniken zur Datenmaskierung gehören: DataBrew

- Hashing — Wenden Sie Hashfunktionen auf die Spaltenwerte an.
- Substitution — Ersetzen Sie persönliche Daten durch andere, authentisch aussehende Werte.
- Nullstellen oder Löschen — Ersetzt ein bestimmtes Feld durch einen Nullwert oder löscht die Spalte.
- Ausblenden — Verwenden Sie Zeichenverschlüsselung oder maskieren Sie bestimmte Teile in den Spalten.

Im Folgenden sind die verfügbaren Verschlüsselungstechniken aufgeführt:

- Deterministische Verschlüsselung — Wenden Sie deterministische Verschlüsselungsalgorithmen auf die Spaltenwerte an. Deterministische Verschlüsselung erzeugt immer denselben Chiffretext für einen Wert.
- Probabilistische Verschlüsselung — Wenden Sie probabilistische Verschlüsselungsalgorithmen auf die Spaltenwerte an. Probabilistische Verschlüsselung erzeugt bei jeder Anwendung einen anderen Chiffretext.

Eine vollständige Liste der bereitgestellten Rezepte zur Transformation personenbezogener Daten finden Sie unter DataBrew Rezeptschritte für personenbezogene Daten (PII).

AWS Glue Qualität der Daten

AWS Glue Data Quality hilft Ihnen dabei, die Bereitstellung hochwertiger Daten über Daten-Pipelines proaktiv zu automatisieren und zu operationalisieren, bevor sie an Ihre Datenverbraucher geliefert werden. AWS Glue Data Quality bietet statistische Analysen von Datenqualitätsproblemen in Ihren Daten-Pipelines, kann Warnmeldungen in Amazon EventBridge auslösen und Empfehlungen für Qualitätsregeln zur Behebung aussprechen. AWS Glue Data Quality unterstützt auch die Erstellung von Regeln mit einer domänenspezifischen Sprache, sodass Sie benutzerdefinierte Datenqualitätsregeln erstellen können.

AWS Key Management Service

AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen. AWS KMS verwendet Hardware-Sicherheitsmodule zum Schutz und zur Validierung AWS KMS keys im Rahmen des FIPS 140-2 Cryptographic Module Validation Program. Weitere Informationen zur Verwendung dieses Dienstes in einem Sicherheitskontext finden Sie in der AWS Sicherheitsreferenzarchitektur.

AWS KMS lässt sich in AWS services die meisten Verschlüsselungslösungen integrieren, und Sie können KMS-Schlüssel in Ihren Anwendungen verwenden, die personenbezogene Daten verarbeiten und speichern. Sie können AWS KMS sie verwenden, um eine Vielzahl Ihrer Datenschutzanforderungen zu erfüllen und personenbezogene Daten zu schützen, darunter:

- Mithilfe von vom Kunden verwalteten Schlüsseln haben Sie mehr Kontrolle über Gültigkeitsdauer, Rotation, Ablauf und andere Optionen.
- Verwendung spezieller, vom Kunden verwalteter Schlüssel zum Schutz personenbezogener Daten und Geheimnisse, die den Zugriff auf personenbezogene Daten ermöglichen.
- Definition von Datenklassifizierungsebenen und Benennung von mindestens einem dedizierten, vom Kunden verwalteten Schlüssel pro Ebene. Beispielsweise verfügen Sie möglicherweise über einen Schlüssel zum Verschlüsseln von Betriebsdaten und einen anderen zum Verschlüsseln personenbezogener Daten.
- Verhinderung eines unbeabsichtigten kontoübergreifenden Zugriffs auf KMS-Schlüssel
- Speichern von KMS-Schlüsseln innerhalb derselben Ressource AWS-Konto wie die zu verschlüsselnde Ressource.

- Implementierung der Aufgabentrennung für die Verwaltung und Verwendung von KMS-Schlüsseln. Weitere Informationen finden Sie unter So verwenden Sie KMS und IAM, um unabhängige Sicherheitskontrollen für verschlüsselte Daten in S3 zu aktivieren (AWS Blogbeitrag).
- Durchsetzung der automatischen Schlüsselrotation durch präventive und reaktive Schutzmaßnahmen.

Standardmäßig werden KMS-Schlüssel gespeichert und können nur in der Region verwendet werden, in der sie erstellt wurden. Wenn Ihre Organisation spezielle Anforderungen an Datenresidenz und Datenhoheit stellt, sollten Sie überlegen, ob KMS-Schlüssel für mehrere Regionen für Ihren Anwendungsfall geeignet sind. Schlüssel für mehrere Regionen sind unterschiedliche KMS-Schlüssel für spezielle Zwecke, AWS-Regionen die synonym verwendet werden können. Bei der Erstellung eines regionsübergreifenden Schlüssels werden Ihre wichtigsten Informationen über die AWS-Region Landesgrenzen hinweg transportiert AWS KMS, sodass diese fehlende regionale Abschottung möglicherweise nicht mit den Compliance-Zielen Ihrer Organisation vereinbar ist. Eine Möglichkeit, dieses Problem zu lösen, besteht darin, einen anderen Typ von KMS-Schlüssel zu verwenden, z. B. einen regionsspezifischen, vom Kunden verwalteten Schlüssel.

AWS Local Zones

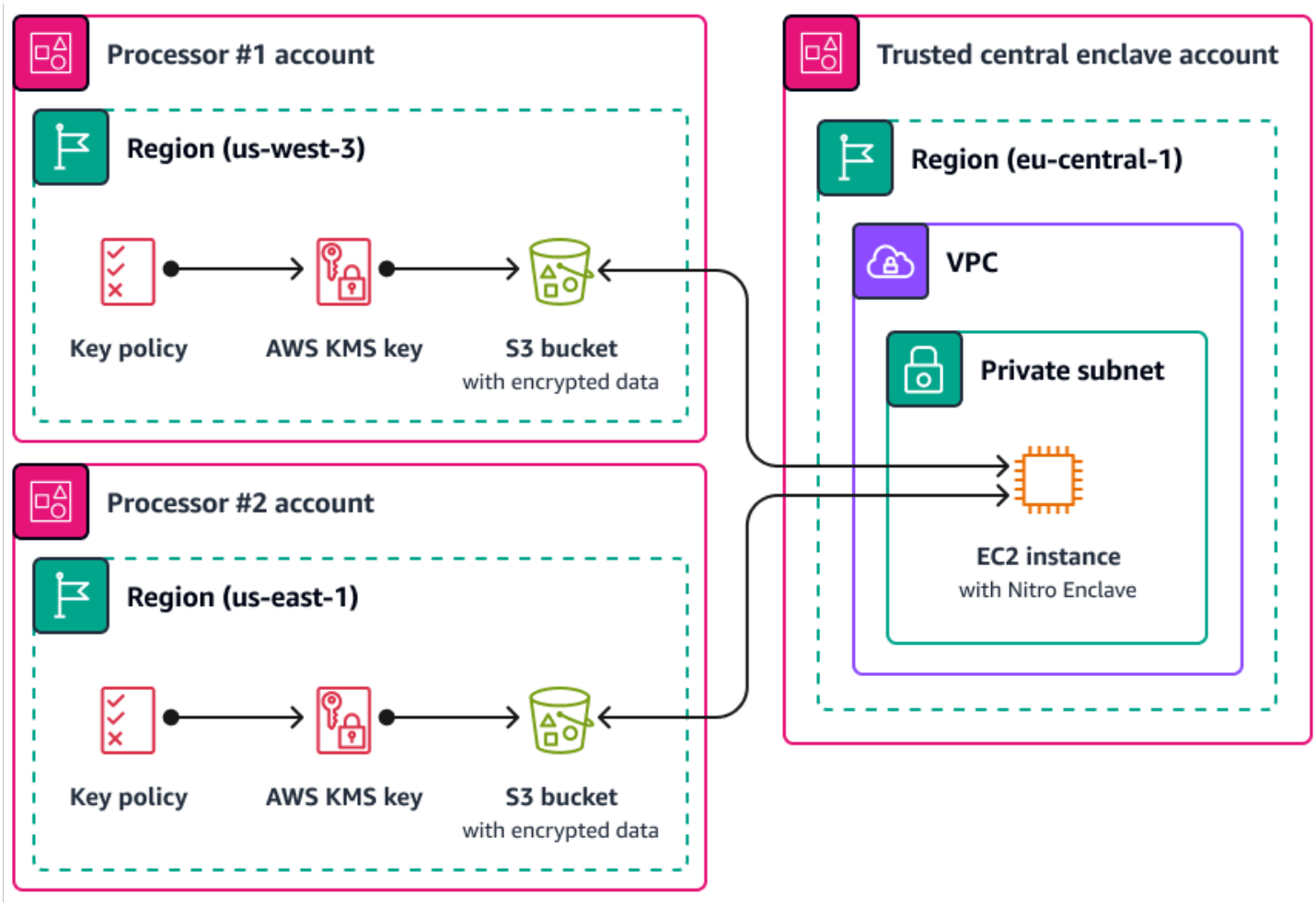
Wenn Sie die Anforderungen an die Datenresidenz erfüllen müssen, können Sie Ressourcen einsetzen, die personenbezogene Daten speichern und verarbeiten, um diese Anforderungen AWS-Regionen zu erfüllen. Sie können auch AWS Local Zones verwenden, um Rechen-, Speicher-, Datenbank- und andere ausgewählte AWS Ressourcen in der Nähe von Ballungs- und Industriezentren zu platzieren. Eine lokale Zone ist eine Erweiterung einer Zone AWS-Region , die sich in geografischer Nähe zu einer großen Metropolregion befindet. Sie können bestimmte Ressourcentypen innerhalb einer lokalen Zone in der Nähe der Region platzieren, der die lokale Zone entspricht. Local Zones können Ihnen dabei helfen, die Anforderungen an die Datenresidenz zu erfüllen, wenn eine Region innerhalb derselben Rechtsordnung nicht verfügbar ist. Wenn Sie Local Zones verwenden, sollten Sie die Datenresidenzkontrollen berücksichtigen, die in Ihrer Organisation implementiert sind. Beispielsweise benötigen Sie möglicherweise ein Steuerelement, um Datenübertragungen von einer bestimmten lokalen Zone in eine andere Region zu verhindern. Weitere Informationen zur Verwendung von SCPs zur Aufrechterhaltung grenzüberschreitender Datenübertragungen finden Sie unter Bewährte Methoden zur Verwaltung der Datenresidenz in AWS Local Zones mithilfe von landing zone Controls (AWS Blogbeitrag).

AWS Nitro-Enklaven

Betrachten Sie Ihre Datensegmentierungsstrategie aus der Perspektive der Verarbeitung, z. B. bei der Verarbeitung personenbezogener Daten mit einem Rechenservice wie Amazon Elastic Compute Cloud (Amazon EC2). Confidential Computing als Teil einer umfassenderen Architekturstrategie kann Ihnen helfen, die Verarbeitung personenbezogener Daten in einer isolierten, geschützten und vertrauenswürdigen CPU-Enklave zu isolieren. Enklaven sind separate, gehärtete und stark eingeschränkte virtuelle Maschinen. AWS Nitro Enclaves ist eine Amazon EC2 EC2-Funktion, mit der Sie diese isolierten Computerumgebungen erstellen können. Weitere Informationen finden Sie unter Das Sicherheitsdesign des AWS Nitro-Systems (Whitepaper).AWS

Nitro Enclaves stellen einen Kernel bereit, der vom Kernel der übergeordneten Instanz getrennt ist. Der Kernel der übergeordneten Instanz hat keinen Zugriff auf die Enklave. Benutzer können weder per SSH noch remote auf die Daten und Anwendungen in der Enklave zugreifen. Anwendungen, die personenbezogene Daten verarbeiten, können in die Enklave eingebettet und so konfiguriert werden, dass sie den Vsock der Enklave verwenden, den Socket, der die Kommunikation zwischen der Enklave und der übergeordneten Instanz erleichtert.

Ein Anwendungsfall, in dem Nitro Enclaves nützlich sein kann, ist die gemeinsame Verarbeitung zwischen zwei Datenprozessoren, die getrennt AWS-Regionen sind und sich möglicherweise nicht gegenseitig vertrauen. Die folgende Abbildung zeigt, wie Sie eine Enklave für die zentrale Verarbeitung, einen KMS-Schlüssel zum Verschlüsseln der personenbezogenen Daten vor dem Senden an die Enklave und eine AWS KMS key Richtlinie verwenden können, mit der überprüft wird, ob die Enklave, die die Entschlüsselung anfordert, die eindeutigen Maße in ihrem Bescheinigungsdokument enthält. Weitere Informationen und Anweisungen finden Sie unter Verwenden der kryptografischen Bescheinigung mit. AWS KMS Ein Beispiel für eine Schlüsselrichtlinie finden Sie Für die Verwendung eines Schlüssels ist eine Bescheinigung erforderlich AWS KMS in diesem Handbuch.



Bei dieser Implementierung haben nur die jeweiligen Datenprozessoren und die zugrunde liegende Enklave Zugriff auf die personenbezogenen Daten im Klartext. Der einzige Ort, an dem die Daten außerhalb der Umgebungen der jeweiligen Datenverarbeiter offengelegt werden, ist die Enklave selbst, die darauf ausgelegt ist, Zugriff und Manipulation zu verhindern.

AWS PrivateLink

Viele Unternehmen möchten die Offenlegung personenbezogener Daten durch nicht vertrauenswürdige Netzwerke einschränken. Wenn Sie beispielsweise den Datenschutz Ihrer gesamten Anwendungsarchitektur verbessern möchten, können Sie Netzwerke nach Datensensitivität segmentieren (ähnlich der logischen und physischen Trennung von Datensätzen, die in diesem AWS-Services und -Funktionen zur Segmentierung von Daten Abschnitt behandelt wird). AWS PrivateLinkhilft Ihnen dabei, unidirektionale, private Verbindungen von Ihren Virtual Private Clouds (VPCs) zu Diensten außerhalb der VPC herzustellen. Damit können Sie dedizierte private Verbindungen zu den Diensten einrichten, die personenbezogene Daten in Ihrer Umgebung speichern oder verarbeiten. Sie müssen keine Verbindung zu öffentlichen Endpunkten herstellen und

diese Daten über nicht vertrauenswürdige öffentliche Netzwerke übertragen. AWS PrivateLink Wenn Sie AWS PrivateLink Dienstendpunkte für die im Leistungsumfang enthaltenen Dienste aktivieren, ist für die Kommunikation kein Internet-Gateway, kein NAT-Gerät, keine öffentliche IP-Adresse, AWS Direct Connect Verbindung oder AWS Site-to-Site VPN Verbindung erforderlich. Wenn Sie eine Verbindung AWS PrivateLink zu einem Dienst herstellen, der Zugriff auf personenbezogene Daten bietet, können Sie VPC-Endpunktrichtlinien und Sicherheitsgruppen verwenden, um den Zugriff gemäß der Datenperimeter-Definition Ihres Unternehmens zu steuern. Ein Beispiel für eine VPC-Endpunktrichtlinie, die nur IAM-Prinzipien und AWS -Ressourcen in einer vertrauenswürdigen Organisation den Zugriff auf einen Service-Endpunkt ermöglicht, finden Sie Für den Zugriff auf VPC-Ressourcen ist eine Organisationsmitgliedschaft erforderlich in diesem Handbuch.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) hilft Ihnen dabei, Ihre Ressourcen sicher gemeinsam zu nutzen, AWS-Konten um den betrieblichen Aufwand zu reduzieren und für Transparenz und Überprüfbarkeit zu sorgen. Bei der Planung Ihrer Strategie zur Segmentierung mehrerer Konten sollten Sie erwägen, persönliche Datenspeicher, die Sie in einem separaten, isolierten Konto speichern, gemeinsam AWS RAM zu nutzen. Sie können diese personenbezogenen Daten zu Verarbeitungszwecken an andere vertrauenswürdige Konten weitergeben. In können Sie Berechtigungen verwalten AWS RAM, die definieren, welche Aktionen für gemeinsam genutzte Ressourcen ausgeführt werden können. Alle API-Aufrufe von AWS RAM sind angemeldet CloudTrail. Sie können Amazon CloudWatch Events auch so konfigurieren, dass Sie automatisch über bestimmte Ereignisse informiert werden AWS RAM, z. B. wenn Änderungen an einer Ressourcenfreigabe vorgenommen werden.

Obwohl Sie viele Arten von AWS Ressourcen mit anderen teilen können, AWS-Konten indem Sie ressourcenbasierte Richtlinien in IAM oder Bucket-Richtlinien in Amazon S3 verwenden, AWS RAM bietet dies mehrere zusätzliche Vorteile für den Datenschutz. AWS bietet Dateneigentümern zusätzliche Transparenz darüber, wie und mit wem die Daten in Ihrem AWS-Konten Unternehmen geteilt werden, einschließlich:

- Die Möglichkeit, eine Ressource mit einer gesamten Organisationseinheit gemeinsam zu nutzen, anstatt Listen mit Konto-IDs manuell zu aktualisieren
- Durchsetzung des Einladungsprozesses für die Initiierung der gemeinsamen Nutzung, wenn das Kundenkonto nicht Teil Ihres Unternehmens ist
- Transparenz darüber, welche spezifischen IAM-Principals Zugriff auf die einzelnen Ressourcen haben

Wenn Sie zuvor eine ressourcenbasierte Richtlinie zur Verwaltung einer Ressourcenfreigabe verwendet haben und diese AWS RAM stattdessen verwenden möchten, verwenden Sie den API-Vorgang. PromoteResourceShareCreatedFromPolicy

Amazon SageMaker

Amazon SageMaker ist ein verwalteter Service für maschinelles Lernen (ML), der Ihnen hilft, ML-Modelle zu erstellen und zu trainieren und sie dann in einer produktionsbereiten gehosteten Umgebung bereitzustellen. SageMaker wurde entwickelt, um die Vorbereitung von Trainingsdaten und die Erstellung von Modellfunktionen zu vereinfachen.

SageMaker Amazon-Modellmonitor

Viele Unternehmen berücksichtigen beim Training von ML-Modellen die Datendrift. Datendrift ist eine signifikante Variation zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine signifikante Änderung der Eingabedaten im Laufe der Zeit. Datendrift kann die Gesamtqualität, Genauigkeit und Fairness von ML-Modellvorhersagen beeinträchtigen. Wenn der statistische Charakter der Daten, die ein ML-Modell während der Produktion erhält, von der Art der Basisdaten abweicht, auf denen es trainiert wurde, kann die Genauigkeit der Vorhersagen abnehmen. Amazon SageMaker Model Monitor kann die Qualität der SageMaker Machine-Learning-Modelle von Amazon in der Produktion kontinuierlich überwachen und die Datenqualität überwachen. Die frühzeitige und proaktive Erkennung von Datenabweichungen kann Ihnen dabei helfen, Korrekturmaßnahmen zu ergreifen, z. B. Modelle neu zu schulen, vorgelagerte Systeme zu prüfen oder Datenqualitätsprobleme zu beheben. Model Monitor kann die Notwendigkeit verringern, Modelle manuell zu überwachen oder zusätzliche Tools zu entwickeln.

Amazon SageMaker Clarify

Amazon SageMaker Clarify bietet Einblicke in Modellverzerrungen und Erklärbarkeit. SageMakerClarify wird häufig bei der Vorbereitung von ML-Modelldaten und in der gesamten Entwicklungsphase verwendet. Entwickler können interessante Attribute wie Geschlecht oder Alter angeben, und SageMaker Clarify führt eine Reihe von Algorithmen aus, um jedes Vorhandensein von Verzerrungen in diesen Attributen zu erkennen. Nach der Ausführung des Algorithmus erstellt SageMaker Clarify einen visuellen Bericht mit einer Beschreibung der Ursachen und Messungen möglicher Verzerrungen, sodass Sie Schritte zur Behebung der Verzerrung identifizieren können. Beispielsweise SageMaker könnten in einem Finanzdatensatz, der nur wenige Beispiele für Geschäftskredite an eine Altersgruppe im Vergleich zu anderen enthält, Ungleichgewichte gekennzeichnet werden, sodass Sie ein Modell vermeiden können, das diese Altersgruppe benachteiligt. Sie können auch bereits trainierte Modelle auf Verzerrungen überprüfen, indem Sie

ihre Prognosen überprüfen und diese ML-Modelle kontinuierlich auf Verzerrungen überprüfen. Schließlich ist SageMaker Clarify in Amazon SageMaker Experiments integriert, um ein Diagramm bereitzustellen, das erklärt, welche Funktionen am meisten zum gesamten Vorhersageprozess eines Modells beigetragen haben. Diese Informationen könnten nützlich sein, um Ergebnisse zur Erklärbarkeit zu erzielen, und sie könnten Ihnen dabei helfen, festzustellen, ob eine bestimmte Modelleingabe mehr Einfluss auf das allgemeine Modellverhalten hat, als sie sollte.

SageMaker Amazon-Modellkarte

Amazon SageMaker Model Card kann Ihnen dabei helfen, wichtige Details zu Ihren ML-Modellen für Governance- und Berichtszwecke zu dokumentieren. Zu diesen Informationen können der Eigentümer des Modells, der allgemeine Zweck, die beabsichtigten Anwendungsfälle, die getroffenen Annahmen, die Risikobewertung eines Modells, Schulungsdetails und Kennzahlen sowie die Bewertungsergebnisse gehören. Weitere Informationen finden Sie unter Modellierbarkeit mit Lösungen für AWS künstliche Intelligenz und Machine Learning (AWS Whitepaper).

AWS Funktionen, die bei der Verwaltung des Datenlebenszyklus helfen

Wenn personenbezogene Daten nicht mehr benötigt werden, können Sie den Lebenszyklus und die time-to-live Richtlinien für Daten in vielen verschiedenen Datenspeichern verwenden. Beachten Sie bei der Konfiguration von Richtlinien zur Datenspeicherung die folgenden Speicherorte, die möglicherweise personenbezogene Daten enthalten:

- Datenbanken wie Amazon DynamoDB und Amazon Relational Database Service (Amazon RDS)
- Amazon-S3-Buckets
- Protokolle von und CloudWatch CloudTrail
- Zwischengespeicherte Daten aus Migrationen in AWS Database Migration Service ()AWS DMS und Projekten AWS Glue DataBrew
- Backups und Schnappschüsse

Mithilfe der folgenden AWS services Funktionen können Sie Richtlinien zur Datenaufbewahrung in Ihren AWS Umgebungen konfigurieren:

- Amazon S3 Lifecycle — Eine Reihe von Regeln, die Aktionen definieren, die Amazon S3 auf eine Gruppe von Objekten anwendet. In der Amazon S3 Lifecyle-Konfiguration können Sie Ablaufaktionen erstellen, die festlegen, wann Amazon S3 abgelaufene Objekte in Ihrem Namen löscht. Weitere Informationen finden Sie unter Verwalten Ihres Speicher-Lebenszyklus.

- Amazon Data Lifecycle Manager — Erstellen Sie in Amazon EC2 eine Richtlinie, die die Erstellung, Aufbewahrung und Löschung von Amazon Elastic Block Store (Amazon EBS) -Snapshots und EBS-gestützten Amazon Machine Images (AMIs) automatisiert.
- DynamoDB Time to Live (TTL) — Definieren Sie einen Zeitstempel pro Element, der festlegt, wann ein Element nicht mehr benötigt wird. Kurz nach dem Datum und der Uhrzeit des angegebenen Zeitstempels löscht DynamoDB das Element aus Ihrer Tabelle.
- Einstellungen für die Aufbewahrung von CloudWatch Protokollen in Logs — Sie können die Aufbewahrungsrichtlinie für jede Protokollgruppe auf einen Wert zwischen 1 Tag und 10 Jahren anpassen.
- AWS Backup— Stellen Sie Datenschutzrichtlinien zentral bereit, um Ihre Backup-Aktivitäten für eine Vielzahl von AWS Ressourcen zu konfigurieren, zu verwalten und zu steuern, darunter S3-Buckets, RDS-Datenbankinstanzen, DynamoDB-Tabellen, EBS-Volumes und vieles mehr. Wenden Sie Backup-Richtlinien auf Ihre AWS Ressourcen an, indem Sie entweder Ressourcentypen angeben oder zusätzliche Granularität bieten, indem Sie sie auf der Grundlage vorhandener Ressourcen-Tags anwenden. Prüfen und dokumentieren Sie die Backup-Aktivitäten von einer zentralen Konsole aus, um die Einhaltung der Backup-Compliance-Anforderungen zu gewährleisten.

AWS-Services und -Funktionen zur Segmentierung von Daten

Datensegmentierung ist der Prozess, bei dem Sie Daten in separaten Containern speichern. Dies kann Ihnen dabei helfen, für jeden Datensatz differenzierte Sicherheits- und Authentifizierungsmaßnahmen vorzusehen und den Umfang der Gefährdung Ihres gesamten Datensatzes zu verringern. Anstatt beispielsweise alle Kundendaten in einer großen Datenbank zu speichern, können Sie diese Daten in kleinere, besser verwaltbare Gruppen unterteilen.

Sie können die physische und logische Trennung verwenden, um personenbezogene Daten zu segmentieren:

- Physische Trennung — Das Speichern von Daten in separaten Datenspeichern oder das Verteilen Ihrer Daten auf separate AWS Ressourcen. Obwohl die Daten physisch getrennt sind, sind beide Ressourcen möglicherweise für dieselben Prinzipale zugänglich. Aus diesem Grund empfehlen wir, die physische Trennung mit der logischen Trennung zu kombinieren.
- Logische Trennung — Das Isolieren von Daten mithilfe von Zugriffskontrollen. Verschiedene Jobfunktionen erfordern unterschiedliche Zugriffsebenen auf Teilmengen personenbezogener

Daten. Ein Beispiel für eine Richtlinie, die eine logische Trennung implementiert, finden Sie Zugriff auf bestimmte Amazon DynamoDB-Attribute gewähren in diesem Handbuch.

Die Kombination aus logischer und physischer Trennung bietet Flexibilität, Einfachheit und Granularität beim Schreiben identitäts- und ressourcenbasierter Richtlinien zur Unterstützung eines differenzierten Zugriffs für verschiedene Aufgabenbereiche. Beispielsweise kann es betrieblich komplex sein, Richtlinien zu erstellen, die verschiedene Datenklassifizierungen logisch in einem einzigen S3-Bucket trennen. Die Verwendung spezieller S3-Buckets für jede Datenklassifizierung vereinfacht die Konfiguration und Verwaltung von Richtlinien.

Beispiele für Datenschutzrichtlinien

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Viele Unternehmen, die mit sensiblen Daten umgehen, verfolgen einen präventiven und vorausschauenden Ansatz, bei dem durchgehend mehrere Ebenen von detektiven und reaktiven Kontrollen implementiert sind. Dieser Abschnitt enthält Beispiele für datenschutzbezogene Richtlinien für AWS Identity and Access Management (IAM), und (). AWS Organizations AWS Key Management Service AWS KMS Diese Richtlinien können Ihrem Unternehmen helfen, verschiedene Datenschutzziele in Bezug auf Nutzung, Offenlegung und grenzüberschreitende Datenübertragung zu erreichen, indem ein präventiver Ansatz verfolgt wird. Auf viele dieser Richtlinien wurde in den vorherigen Abschnitten dieses Handbuchs verwiesen.

Dieser Abschnitt enthält die folgenden Beispielrichtlinien:

- Zugriff von bestimmten IP-Adressen aus erforderlich
- Für den Zugriff auf VPC-Ressourcen ist eine Organisationsmitgliedschaft erforderlich
- Beschränken Sie Datenübertragungen zwischen AWS-Regionen
- Zugriff auf bestimmte Amazon DynamoDB-Attribute gewähren
- Änderungen an VPC-Konfigurationen einschränken
- Für die Verwendung eines Schlüssels ist eine Bescheinigung erforderlich AWS KMS

Zugriff von bestimmten IP-Adressen aus erforderlich

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Diese Richtlinie ermöglicht es dem `john_stiles` Benutzer, IAM-Rollen nur dann anzunehmen, wenn der Anruf von einer IP-Adresse im Bereich `192.0.2.0/24` oder `203.0.113.0/24` kommt. Diese Richtlinie kann dazu beitragen, die unbeabsichtigte Offenlegung personenbezogener Daten und unerwünschte grenzüberschreitende Datenübertragungen zu verhindern. Wenn Ihr Unternehmen beispielsweise Kundenservicemitarbeiter hat, die Zugriff auf personenbezogene Daten benötigen,

möchten Sie vielleicht, dass diese Support-Mitarbeiter nur von Büros aus auf diese Daten zugreifen können, die sich in einer bestimmten Untergruppe befinden. AWS-Regionen

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/john_stiles"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/john_stiles"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24",
            "203.0.113.0/24"
          ]
        }
      }
    }
  ]
}
```

Für den Zugriff auf VPC-Ressourcen ist eine Organisationsmitgliedschaft erforderlich

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Diese VPC-Endpunktrichtlinie ermöglicht nur AWS Identity and Access Management (IAM) - Prinzipalen und Ressourcen der `o-1abcde123` Organisation den Zugriff auf Amazon Personalize

(Amazon S3) -Endpoints. Diese präventive Kontrolle hilft dabei, eine Vertrauenszone einzurichten und den Perimeter personenbezogener Daten zu definieren. Weitere Informationen darüber, wie diese Richtlinie zum Schutz der Privatsphäre und personenbezogener Daten in Ihrem Unternehmen beitragen kann, finden Sie AWS PrivateLink in diesem Leitfaden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyIntendedResourcesAndPrincipals",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-1abcde123",
                    "aws:ResourceOrgID": "o-1abcde123"
                }
            }
        }
    ]
}
```

Beschränken Sie Datenübertragungen zwischen AWS-Regionen

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Mit Ausnahme von zwei Rollen AWS Identity and Access Management (IAM) verweigert diese Dienststeuerungsrichtlinie API-Aufrufe AWS services an AWS-Regionen andere Regionen als `eu-west-1` und. `eu-central-1` Dieses SCP kann dazu beitragen, die Einrichtung von AWS Speicher- und Verarbeitungsdiensten in nicht genehmigten Regionen zu verhindern. Dies kann dazu beitragen, dass personenbezogene Daten AWS services in diesen Regionen insgesamt nicht verarbeitet werden. Diese Richtlinie verwendet einen `NotAction` Parameter, da sie globale AWS-Services wie IAM und Services, die in globale Services integriert sind, wie AWS Key Management Service (AWS KMS) und Amazon CloudFront, berücksichtigt. In den Parameterwerten können Sie diese globalen und andere nicht zutreffende Services als Ausnahmen angeben. Weitere Informationen darüber, wie

diese Richtlinie zum Schutz der Privatsphäre und personenbezogener Daten in Ihrem Unternehmen beitragen kann, finden Sie AWS Organizations in diesem Leitfaden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
```

```
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Zugriff auf bestimmte Amazon DynamoDB-Attribute gewähren

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Bei der Erörterung von Strategien zur physischen und logischen Trennung personenbezogener Daten in Ihrem Unternehmen sollten Sie sich überlegen, welche AWS Speicherservices detaillierte Zugriffskontrollrichtlinien AWS Identity and Access Management (IAM) unterstützen. Die folgende identitätsbasierte Richtlinie ermöglicht nur das Abrufen der `LastLoggedIn` Attribute `UserIDSignUpTime`, und aus einer Amazon DynamoDB-Tabelle mit dem Namen. `Users` Sie könnten diese Richtlinie beispielsweise einer Kundensupport-Rolle zuordnen, anstatt dieser Rolle

Zugriff auf den gesamten persönlichen Datensatz zu gewähren. Weitere Informationen darüber, wie diese Richtlinie zum Schutz der Privatsphäre und personenbezogener Daten in Ihrem Unternehmen beitragen kann, finden Sie AWS-Services und -Funktionen zur Segmentierung von Daten in diesem Leitfaden.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:BatchGetItem",
            "dynamodb:Query",
            "dynamodb:Scan",
            "dynamodb:TransactGetItems"
         ],
         "Resource":[
            "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
         ],
         "Condition":{
            "ForAllValues:StringEquals":{
               "dynamodb:Attributes":[
                  "UserID",
                  "SignUpTime",
                  "LastLoggedIn"
               ]
            },
            "StringEquals":{
               "dynanamodb:Select":[
                  "SPECIFIC_ATTRIBUTES"
               ]
            }
         }
      }
   ]
}
```

Änderungen an VPC-Konfigurationen einschränken

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Nachdem Sie die AWS Infrastruktur entworfen und bereitgestellt haben, die Ihre Anforderungen an die grenzüberschreitende Datenübertragung unterstützt, einschließlich Netzwerkdatenflüsse, möchten Sie möglicherweise Änderungen verhindern. Die folgende Dienststeuerungsrichtlinie trägt dazu bei, Abweichungen oder unbeabsichtigte Änderungen der VPC-Konfiguration zu verhindern. Es verweigert neue Internet-Gateway-Anhänge, VPC-Peering-Verbindungen, Transit-Gateway-Anhänge und neue VPN-Verbindungen. Weitere Informationen darüber, wie diese Richtlinie zum Schutz der Privatsphäre und personenbezogener Daten in Ihrem Unternehmen beitragen kann, finden Sie AWS Transit Gateway in diesem Handbuch.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachInternetGateway",
                "ec2:CreateInternetGateway",
                "ec2:AttachEgressOnlyInternetGateway",
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection",
                "ec2:CreateVpc",
                "ec2:CreateSubnet",
                "ec2:CreateRouteTable",
                "ec2:CreateRoute",
                "ec2:AssociateRouteTable",
                "ec2:ModifyVpcAttribute",
                "ec2:*TransitGateway",
                "ec2:*TransitGateway*",
                "globalaccelerator:Create*",
                "globalaccelerator:Update*"

            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "ArnNotLike": {
```

```
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Für die Verwendung eines Schlüssels ist eine Bescheinigung erforderlich AWS KMS

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Die folgende AWS Key Management Service (AWS KMS) wichtige Richtlinie ermöglicht es AWS Nitro Enclave-Instances, einen KMS-Schlüssel nur zu verwenden, wenn das Bestätigungsdokument der Enklave in der Anfrage den Messungen in der Zustandserklärung entspricht. Diese Richtlinie erlaubt nur vertrauenswürdigen Enklaven, die Daten zu entschlüsseln. Weitere Informationen darüber, wie diese Richtlinie zum Schutz der Privatsphäre und personenbezogener Daten in Ihrer Organisation beitragen kann, finden Sie AWS Nitro-Enklaven in diesem Handbuch. Eine vollständige Liste der AWS KMS Bedingungsschlüssel, die in wichtigen Richtlinien und in AWS Identity and Access Management (IAM-) Richtlinien verwendet werden können, finden Sie unter Bedingungsschlüssel für AWS KMS.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Enable enclave data processing",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:role/data-processing"
         },
         "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey",
```

```
            "kms:GenerateRandom"
         ],
         "Resource": "*",
         "Condition": {
            "StringEqualsIgnoreCase": {
               "kms:RecipientAttestation:ImageSha384":
 "EXAMPLE8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdEXAMPLE",
               "kms:RecipientAttestation:PCR0":
 "EXAMPLEbc2ecbb68ed99a13d7122abfc0666b926a79d5379bc58b9445c84217f59cfdd36c08b2c79552928702EXAM
               "kms:RecipientAttestation:PCR1":
 "EXAMPLE050abf6b993c915505f3220e2d82b51aff830ad14cbecc2eec1bf0b4ae749d311c663f464cde9f718aEXAM
               "kms:RecipientAttestation:PCR2":
 "EXAMPLEc300289e872e6ac4d19b0b5ac4a9b020c98295643ff3978610750ce6a86f7edff24e3c0a4a445f2ff8EXAM
               "kms:RecipientAttestation:PCR3":
 "EXAMPLE11de9baee597508183477f097ae385d4a2c885aa655432365b53b812694e230bbe8e1bb1b8de748fe1EXAM
               "kms:RecipientAttestation:PCR4":
 "EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde479e9f7f512f33e835a0b9023ca51ada02160EXAM
               "kms:RecipientAttestation:PCR8":
 "EXAMPLE34a884328944cd806127c7784677ab60a154249fd21546a217299ccfa1ebfe4fa96a163bf41d3bcfaeEXAM
            }
         }
      }
   ]
}
```

Ressourcen

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

AWS Präskriptive Leitlinien

- AWS Sicherheitsreferenzarchitektur (SRA)AWS

AWS Dokumentation

- Datenschutz (AWS Well-Architected Framework)
- Datenklassifizierung (Whitepaper)AWS
- Amazon Web Services: Risiko und Compliance (AWS Whitepaper)
- Hybride Architekturen zur Erfüllung der Anforderungen an die Verarbeitung personenbezogener Daten (Whitepaper)AWS
- Überblick über die Einhaltung der DSGVO-Vorschriften (Whitepaper AWS)AWS
- Aufbau eines Datenperimeters auf AWS (Whitepaper)AWS
- AWS Dokumentation zur Sicherheit

Andere AWS Ressourcen

- AWS Compliance-Programme
- AWS Modell mit geteilter Verantwortung
- Häufig gestellte Fragen zum Datenschutz
- AWS Dienstleistungen zur Gewährleistung der Sicherheit
- AWS Versprechen digitaler Souveränität: Kontrolle ohne Kompromisse (AWS Blogbeitrag)
- AWS Lernen im Bereich Sicherheit

Mitwirkende

Wir würden uns freuen, von Ihnen zu hören. Bitte geben Sie Feedback zur AWS PRA, indem Sie an einer kurzen Umfrage teilnehmen.

Dieser Leitfaden wurde vom AWS Security Assurance Services-Team verfasst. Wenn Sie Unterstützung bei der Umsetzung der Empfehlungen in diesem Handbuch und bei der Operationalisierung Ihrer Workloads benötigen, wenden Sie sich an das AWS Security Assurance Services-Team.

Die wichtigsten Autoren

- Daniel Nieters, leitender Datenschutzberater AWS
- Amber Welch, AWS leitender Datenschutzberater
- Robert Carter, AWS Technischer Programmmanager

Mitwirkende

- Avik Mukherjee, leitender Sicherheitsberater AWS
- David Bounds, leitender Lösungsarchitekt AWS
- Jeff Lombardo, AWS leitender Architekt für Sicherheitslösungen
- Ram Ramani, AWS leitender Architekt für Sicherheitslösungen
- Vanessa Jacobs, leitende Sicherheitsberaterin AWS

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Signifikante Aktualisierungen	Wir haben durchweg wichtige Aktualisierungen vorgenommen.	26. März 2024
Erste Veröffentlichung	—	2. Oktober 2023

AWS Glossar zu präskriptiven Leitlinien

Im Folgenden finden Sie häufig verwendete Begriffe in Strategien, Leitfäden und Mustern von AWS Prescriptive Guidance. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

Zahlen

7 Rs

Sieben gängige Migrationsstrategien für die Verlagerung von Anwendungen in die Cloud. Diese Strategien bauen auf den 5 Rs auf, die Gartner 2011 identifiziert hat, und bestehen aus folgenden Elementen:

- Faktorwechsel/Architekturwechsel – Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile cloudnativer Feature nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf die Amazon Aurora PostgreSQL-kompatible Edition.
- Plattformwechsel (Lift and Reshape) – Verschieben Sie eine Anwendung in die Cloud und führen Sie ein gewisses Maß an Optimierung ein, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Oracle in der. AWS Cloud
- Neukauf (Drop and Shop) – Wechseln Sie zu einem anderen Produkt, indem Sie typischerweise von einer herkömmlichen Lizenz zu einem SaaS-Modell wechseln. Beispiel: Migrieren Sie Ihr CRM-System (Customer Relationship Management) zu Salesforce.com.
- Hostwechsel (Lift and Shift) – Verschieben Sie eine Anwendung in die Cloud, ohne Änderungen vorzunehmen, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Oracle auf einer EC2-Instanz in der. AWS Cloud
- Verschieben (Lift and Shift auf Hypervisor-Ebene) – Verlagern Sie die Infrastruktur in die Cloud, ohne neue Hardware kaufen, Anwendungen umschreiben oder Ihre bestehenden Abläufe ändern zu müssen. Sie migrieren Server von einer lokalen Plattform zu einem Cloud-Dienst für dieselbe Plattform. Beispiel: Migrieren Sie eine Microsoft Hyper-V Anwendung zu AWS.
- Beibehaltung (Wiederaufgreifen) – Bewahren Sie Anwendungen in Ihrer Quellumgebung auf. Dazu können Anwendungen gehören, die einen umfangreichen Faktorwechsel erfordern und

die Sie auf einen späteren Zeitpunkt verschieben möchten, sowie ältere Anwendungen, die Sie beibehalten möchten, da es keine geschäftliche Rechtfertigung für ihre Migration gibt.

- Außerbetriebnahme – Dekommissionierung oder Entfernung von Anwendungen, die in Ihrer Quellumgebung nicht mehr benötigt werden.

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Weitere Informationen finden Sie unter Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden (mithilfe eines bidirektionalen Replikationstools oder dualer Schreibvorgänge) und beide Datenbanken Transaktionen von miteinander verbundenen Anwendungen während der Migration verarbeiten. Diese Methode unterstützt die Migration in kleinen, kontrollierten Batches, anstatt einen einmaligen Cutover zu erfordern. Es ist flexibler, erfordert aber mehr Arbeit als eine aktiv-passive Migration.

Aktiv-Passiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden, aber nur die Quelldatenbank Transaktionen von verbindenden Anwendungen verarbeitet, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

Aggregatfunktion

Eine SQL-Funktion, die mit einer Gruppe von Zeilen arbeitet und einen einzelnen Rückgabewert für die Gruppe berechnet. Beispiele für Aggregatfunktionen sind `SUM` und`MAX`.

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen mit künstlicher Intelligenz.

Anonymisierung

Der Prozess des dauerhaften Löschens personenbezogener Daten in einem Datensatz. Anonymisierung kann zum Schutz der Privatsphäre beitragen. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten.

Anti-Muster

Eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist.

Anwendungssteuerung

Ein Sicherheitsansatz, bei dem nur zugelassene Anwendungen verwendet werden können, um ein System vor Schadsoftware zu schützen.

Anwendungsportfolio

Eine Sammlung detaillierter Informationen zu jeder Anwendung, die von einer Organisation verwendet wird, einschließlich der Kosten für die Erstellung und Wartung der Anwendung und ihres Geschäftswerts. Diese Informationen sind entscheidend für den Prozess der Portfoliofindung und -analyse und hilft bei der Identifizierung und Priorisierung der Anwendungen, die migriert, modernisiert und optimiert werden sollen.

künstliche Intelligenz (KI)

Das Gebiet der Datenverarbeitungswissenschaft, das sich der Nutzung von Computertechnologien zur Ausführung kognitiver Funktionen widmet, die typischerweise mit Menschen in Verbindung gebracht werden, wie Lernen, Problemlösen und Erkennen von Mustern. Weitere Informationen finden Sie unter Was ist künstliche Intelligenz?

Operationen mit künstlicher Intelligenz (AIOps)

Der Prozess des Einsatzes von Techniken des Machine Learning zur Lösung betrieblicher Probleme, zur Reduzierung betrieblicher Zwischenfälle und menschlicher Eingriffe sowie zur Steigerung der Servicequalität. Weitere Informationen zur Verwendung von AIOps in der AWS -Migrationsstrategie finden Sie im Leitfaden zur Betriebsintegration.

Asymmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung verwendet. Sie können den

öffentlichen Schlüssel teilen, da er nicht für die Entschlüsselung verwendet wird. Der Zugriff auf den privaten Schlüssel sollte jedoch stark eingeschränkt sein.

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

Eine Reihe von Softwareeigenschaften, die die Datenvalidität und betriebliche Zuverlässigkeit einer Datenbank auch bei Fehlern, Stromausfällen oder anderen Problemen gewährleisten.

Attributbasierte Zugriffskontrolle (ABAC)

Die Praxis, detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname zu erstellen. Weitere Informationen finden Sie unter ABAC AWS in der AWS Identity and Access Management (IAM-) Dokumentation.

autoritative Datenquelle

Ein Ort, an dem Sie die primäre Version der Daten speichern, die als die zuverlässigste Informationsquelle angesehen wird. Sie können Daten aus der maßgeblichen Datenquelle an andere Speicherorte kopieren, um die Daten zu verarbeiten oder zu ändern, z. B. zu anonymisieren, zu redigieren oder zu pseudonymisieren.

Availability Zone

Ein bestimmter Standort innerhalb einer AWS-Region , der vor Ausfällen in anderen Availability Zones geschützt ist und kostengünstige Netzwerkkonnektivität mit niedriger Latenz zu anderen Availability Zones in derselben Region bietet.

AWS Framework für die Cloud-Einführung (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für den erfolgreichen Umstieg auf die Cloud unterstützt. AWS AWS CAF unterteilt die Leitlinien in sechs Schwerpunktbereiche, die als Perspektiven bezeichnet werden: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und Betrieb. Die Perspektiven Geschäft, Mitarbeiter und Unternehmensführung konzentrieren sich auf Geschäftskompetenzen und -prozesse, während sich die Perspektiven Plattform, Sicherheit und Betriebsabläufe auf technische Fähigkeiten und Prozesse konzentrieren. Die Personalperspektive zielt beispielsweise auf Stakeholder ab, die sich mit Personalwesen (HR), Personalfunktionen und Personalmanagement befassen. Aus dieser Perspektive bietet AWS CAF Leitlinien für Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQF ist in () enthalten. AWS Schema Conversion Tool AWS SCT Es analysiert Datenbankschemas und Codeobjekte, Anwendungscode, Abhängigkeiten und Leistungsmerkmale und stellt Bewertungsberichte bereit.

B

schlechter Bot

Ein Bot, der Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen soll.

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

Eine einheitliche, interaktive Ansicht des Ressourcenverhaltens und der Interaktionen im Laufe der Zeit. Sie können ein Verhaltensdiagramm mit Amazon Detective verwenden, um fehlgeschlagene Anmeldeversuche, verdächtige API-Aufrufe und ähnliche Vorgänge zu untersuchen. Weitere Informationen finden Sie unter Daten in einem Verhaltensdiagramm in der Detective-Dokumentation.

Big-Endian-System

Ein System, welches das höchstwertige Byte zuerst speichert. Siehe auch Endianness.

Binäre Klassifikation

Ein Prozess, der ein binäres Ergebnis vorhersagt (eine von zwei möglichen Klassen). Beispielsweise könnte Ihr ML-Modell möglicherweise Probleme wie „Handelt es sich bei dieser E-Mail um Spam oder nicht?“ vorhersagen müssen oder „Ist dieses Produkt ein Buch oder ein Auto?“

Bloom-Filter

Eine probabilistische, speichereffiziente Datenstruktur, mit der getestet wird, ob ein Element Teil einer Menge ist.

Blau/Grün-Bereitstellung

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue

Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

Eine Softwareanwendung, die automatisierte Aufgaben über das Internet ausführt und menschliche Aktivitäten oder Interaktionen simuliert. Manche Bots sind nützlich oder nützlich, wie z. B. Webcrawler, die Informationen im Internet indexieren. Einige andere Bots, die als bösartige Bots bezeichnet werden, sollen Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen.

Botnetz

Netzwerke von Bots, die mit Malware infiziert sind und unter der Kontrolle einer einzigen Partei stehen, die als Bot-Herder oder Bot-Operator bezeichnet wird. Botnetze sind der bekannteste Mechanismus zur Skalierung von Bots und ihrer Wirkung.

branch

Ein containerisierter Bereich eines Code-Repositorys. Der erste Zweig, der in einem Repository erstellt wurde, ist der Hauptzweig. Sie können einen neuen Zweig aus einem vorhandenen Zweig erstellen und dann Feature entwickeln oder Fehler in dem neuen Zweig beheben. Ein Zweig, den Sie erstellen, um ein Feature zu erstellen, wird allgemein als Feature-Zweig bezeichnet. Wenn das Feature zur Veröffentlichung bereit ist, führen Sie den Feature-Zweig wieder mit dem Hauptzweig zusammen. Weitere Informationen finden Sie unter Über Branches (GitHub Dokumentation).

Zugang durch Glasbruch

Unter außergewöhnlichen Umständen und im Rahmen eines genehmigten Verfahrens ist dies eine schnelle Methode für einen Benutzer, auf einen Bereich zuzugreifen AWS-Konto , für den er normalerweise keine Zugriffsrechte besitzt. Weitere Informationen finden Sie unter dem Indikator Implementation break-glass procedures in den AWS Well-Architected-Leitlinien.

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

Der Speicherbereich, in dem die am häufigsten abgerufenen Daten gespeichert werden.

Geschäftsfähigkeit

Was ein Unternehmen tut, um Wert zu generieren (z. B. Vertrieb, Kundenservice oder Marketing). Microservices-Architekturen und Entwicklungsentscheidungen können von den Geschäftskapazitäten beeinflusst werden. Weitere Informationen finden Sie im Abschnitt Organisiert nach Geschäftskapazitäten des Whitepapers Ausführen von containerisierten Microservices in AWS.

Planung der Geschäftskontinuität (BCP)

Ein Plan, der die potenziellen Auswirkungen eines störenden Ereignisses, wie z. B. einer groß angelegten Migration, auf den Betrieb berücksichtigt und es einem Unternehmen ermöglicht, den Betrieb schnell wieder aufzunehmen.

C

CAF

Weitere Informationen finden Sie unter Framework für die AWS Cloud-Einführung.

Bereitstellung auf Kanaren

Die langsame und schrittweise Veröffentlichung einer Version für Endbenutzer. Wenn Sie sich sicher sind, stellen Sie die neue Version bereit und ersetzen die aktuelle Version vollständig.

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

Absichtliches Einführen von Ausfällen oder Störungsereignissen, um die Widerstandsfähigkeit eines Systems zu testen. Sie können AWS Fault Injection Service (AWS FIS) verwenden, um Experimente durchzuführen, die Ihre AWS Workloads stress, und deren Reaktion zu bewerten.

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

Ein Kategorisierungsprozess, der bei der Erstellung von Vorhersagen hilft. ML-Modelle für Klassifikationsprobleme sagen einen diskreten Wert voraus. Diskrete Werte unterscheiden sich immer voneinander. Beispielsweise muss ein Modell möglicherweise auswerten, ob auf einem Bild ein Auto zu sehen ist oder nicht.

clientseitige Verschlüsselung

Lokale Verschlüsselung von Daten, bevor das Ziel sie AWS service empfängt.

Cloud-Kompetenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte Transformationen. Weitere Informationen finden Sie in den CCoE-Beiträgen im AWS Cloud Enterprise Strategy Blog.

Cloud Computing

Die Cloud-Technologie, die typischerweise für die Ferndatenspeicherung und das IoT-Gerätemanagement verwendet wird. Cloud Computing ist häufig mit Edge-Computing-Technologie verbunden.

Cloud-Betriebsmodell

In einer IT-Organisation das Betriebsmodell, das zum Aufbau, zur Weiterentwicklung und Optimierung einer oder mehrerer Cloud-Umgebungen verwendet wird. Weitere Informationen finden Sie unter Aufbau Ihres Cloud-Betriebsmodells.

Phasen der Einführung der Cloud

Die vier Phasen, die Unternehmen bei der Migration in der Regel durchlaufen AWS Cloud:

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament – Grundlegende Investitionen tätigen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer Landing Zone, Definition eines CCoE, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen

- Neuentwicklung – Optimierung von Produkten und Services und Innovation in der Cloud

Diese Phasen wurden von Stephen Orban im Blogbeitrag The Journey Toward Cloud-First & the Stages of Adoption im AWS Cloud Enterprise Strategy-Blog definiert. Informationen darüber, wie sie mit der AWS Migrationsstrategie zusammenhängen, finden Sie im Leitfaden zur Vorbereitung der Migration.

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

Ein Ort, an dem Quellcode und andere Komponenten wie Dokumentation, Beispiele und Skripts gespeichert und im Rahmen von Versionskontrollprozessen aktualisiert werden. Zu den gängigen Cloud-Repositorys gehören GitHub oder AWS CodeCommit. Jede Version des Codes wird Zweig genannt. In einer Microservice-Struktur ist jedes Repository einer einzelnen Funktionalität gewidmet. Eine einzelne CI/CD-Pipeline kann mehrere Repositorien verwenden.

Kalter Cache

Ein Puffer-Cache, der leer oder nicht gut gefüllt ist oder veraltete oder irrelevante Daten enthält. Dies beeinträchtigt die Leistung, da die Datenbank-Instance aus dem Hauptspeicher oder der Festplatte lesen muss, was langsamer ist als das Lesen aus dem Puffercache.

Kalte Daten

Daten, auf die selten zugegriffen wird und die in der Regel historisch sind. Bei der Abfrage dieser Art von Daten sind langsame Abfragen in der Regel akzeptabel. Durch die Verlagerung dieser Daten auf leistungsschwächere und kostengünstigere Speicherstufen oder -klassen können Kosten gesenkt werden.

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. AWS Panorama Bietet beispielsweise Geräte an, die CV zu lokalen Kameranetzwerken hinzufügen, und Amazon SageMaker stellt Bildverarbeitungsalgorithmen für CV bereit.

Drift in der Konfiguration

Bei einer Arbeitslast eine Änderung der Konfiguration gegenüber dem erwarteten Zustand. Dies kann dazu führen, dass der Workload nicht mehr richtlinienkonform wird, und zwar in der Regel schrittweise und unbeabsichtigt.

Verwaltung der Datenbankkonfiguration (CMDB)

Ein Repository, das Informationen über eine Datenbank und ihre IT-Umgebung speichert und verwaltet, inklusive Hardware- und Softwarekomponenten und deren Konfigurationen. In der Regel verwenden Sie Daten aus einer CMDB in der Phase der Portfolioerkennung und -analyse der Migration.

Konformitätspaket

Eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie zusammenstellen können, um Ihre Konformitäts- und Sicherheitsprüfungen individuell anzupassen. Mithilfe einer YAML-Vorlage können Sie ein Conformance Pack als einzelne Entität in einer AWS-Konto AND-Region oder unternehmensweit bereitstellen. Weitere Informationen finden Sie in der Dokumentation unter Conformance Packs. AWS Config

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

Der Prozess der Automatisierung der Quell-, Build-, Test-, Staging- und Produktionsphasen des Softwareveröffentlichungsprozesses. CI/CD wird allgemein als Pipeline beschrieben. CI/CD kann Ihnen helfen, Prozesse zu automatisieren, die Produktivität zu steigern, die Codequalität zu verbessern und schneller zu liefern. Weitere Informationen finden Sie unter Vorteile der kontinuierlichen Auslieferung. CD kann auch für kontinuierliche Bereitstellung stehen. Weitere Informationen finden Sie unterKontinuierliche Auslieferung im Vergleich zu kontinuierlicher Bereitstellung.

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

Daten, die in Ihrem Netzwerk stationär sind, z. B. Daten, die sich im Speicher befinden.

Datenklassifizierung

Ein Prozess zur Identifizierung und Kategorisierung der Daten in Ihrem Netzwerk auf der Grundlage ihrer Kritikalität und Sensitivität. Sie ist eine wichtige Komponente jeder Strategie für das Management von Cybersecurity-Risiken, da sie Ihnen hilft, die geeigneten Schutz- und Aufbewahrungskontrollen für die Daten zu bestimmen. Die Datenklassifizierung ist ein Bestandteil

der Sicherheitssäule im AWS Well-Architected Framework. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

Eine signifikante Abweichung zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine signifikante Änderung der Eingabedaten im Laufe der Zeit. Datendrift kann die Gesamtqualität, Genauigkeit und Fairness von ML-Modellvorhersagen beeinträchtigen.

Daten während der Übertragung

Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen.

Datennetz

Ein architektonisches Framework, das verteilte, dezentrale Dateneigentum mit zentraler Verwaltung und Steuerung ermöglicht.

Datenminimierung

Das Prinzip, nur die Daten zu sammeln und zu verarbeiten, die unbedingt erforderlich sind. Durch Datenminimierung im AWS Cloud können Datenschutzrisiken, Kosten und der CO2-Fußabdruck Ihrer Analysen reduziert werden.

Datenperimeter

Eine Reihe präventiver Schutzmaßnahmen in Ihrer AWS Umgebung, die sicherstellen, dass nur vertrauenswürdige Identitäten auf vertrauenswürdige Ressourcen von erwarteten Netzwerken zugreifen. Weitere Informationen finden Sie unter Aufbau eines Datenperimeters auf. AWS

Vorverarbeitung der Daten

Rohdaten in ein Format umzuwandeln, das von Ihrem ML-Modell problemlos verarbeitet werden kann. Die Vorverarbeitung von Daten kann bedeuten, dass bestimmte Spalten oder Zeilen entfernt und fehlende, inkonsistente oder doppelte Werte behoben werden.

Herkunft der Daten

Der Prozess der Nachverfolgung des Ursprungs und der Geschichte von Daten während ihres gesamten Lebenszyklus, z. B. wie die Daten generiert, übertragen und gespeichert wurden.

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen an historischen Daten und werden in der Regel für Abfragen und Analysen verwendet.

Datenbankdefinitionssprache (DDL)

Anweisungen oder Befehle zum Erstellen oder Ändern der Struktur von Tabellen und Objekten in einer Datenbank.

Datenbankmanipulationssprache (DML)

Anweisungen oder Befehle zum Ändern (Einfügen, Aktualisieren und Löschen) von Informationen in einer Datenbank.

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

Mehrere Deep-Learning-Modelle zur Vorhersage kombinieren. Sie können Deep-Ensembles verwenden, um eine genauere Vorhersage zu erhalten oder um die Unsicherheit von Vorhersagen abzuschätzen.

Deep Learning

Ein ML-Teilbereich, der mehrere Schichten künstlicher neuronaler Netzwerke verwendet, um die Zuordnung zwischen Eingabedaten und Zielvariablen von Interesse zu ermitteln.

defense-in-depth

Ein Ansatz zur Informationssicherheit, bei dem eine Reihe von Sicherheitsmechanismen und -kontrollen sorgfältig in einem Computernetzwerk verteilt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks und der darin enthaltenen Daten zu schützen. Wenn Sie diese Strategie anwenden AWS, fügen Sie mehrere Steuerelemente auf verschiedenen Ebenen der AWS Organizations Struktur hinzu, um die Ressourcen zu schützen. Ein defense-in-depth Ansatz könnte beispielsweise Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselung kombinieren.

delegierter Administrator

In AWS Organizations kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren, um die Konten der Organisation und die Berechtigungen für diesen Dienst zu verwalten. Dieses Konto

wird als delegierter Administrator für diesen Service bezeichnet. Weitere Informationen und eine Liste kompatibler Services finden Sie unter Services, die mit AWS Organizations funktionieren in der AWS Organizations -Dokumentation.

Bereitstellung

Der Prozess, bei dem eine Anwendung, neue Feature oder Codekorrekturen in der Zielumgebung verfügbar gemacht werden. Die Bereitstellung umfasst das Implementieren von Änderungen an einer Codebasis und das anschließende Erstellen und Ausführen dieser Codebasis in den Anwendungsumgebungen.

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, ein Ereignis zu erkennen, zu protokollieren und zu warnen, nachdem ein Ereignis eingetreten ist. Diese Kontrollen stellen eine zweite Verteidigungslinie dar und warnen Sie vor Sicherheitsereignissen, bei denen die vorhandenen präventiven Kontrollen umgangen wurden. Weitere Informationen finden Sie unter Detektivische Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken konzipiert wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um durch den Softwareentwicklungsprozess Mehrwert zu schaffen und zu steigern.

digitaler Zwilling

Eine virtuelle Darstellung eines realen Systems, z. B. eines Gebäudes, einer Fabrik, einer Industrieanlage oder einer Produktionslinie. Digitale Zwillinge unterstützen vorausschauende Wartung, Fernüberwachung und Produktionsoptimierung.

Maßtabelle

In einem Sternschema eine kleinere Tabelle, die Datenattribute zu quantitativen Daten in einer Faktentabelle enthält. Bei Attributen von Dimensionstabellen handelt es sich in der Regel um Textfelder oder diskrete Zahlen, die sich wie Text verhalten. Diese Attribute werden häufig zum Einschränken von Abfragen, zum Filtern und zur Kennzeichnung von Ergebnismengen verwendet.

Katastrophe

Ein Ereignis, das verhindert, dass ein Workload oder ein System seine Geschäftsziele an seinem primären Einsatzort erfüllt. Diese Ereignisse können Naturkatastrophen, technische Ausfälle oder das Ergebnis menschlichen Handelns sein, z. B. unbeabsichtigte Fehlkonfigurationen oder Malware-Angriffe.

Notfallwiederherstellung (DR)

Die Strategie und der Prozess, die Sie zur Minimierung von Ausfallzeiten und Datenverlusten aufgrund einer Katastrophe anwenden. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder Kerngeschäftszielen verknüpft werden, denen jede Komponente dient. Dieses Konzept wurde von Eric Evans in seinem Buch Domaingesteuertes Design: Bewältigen der Komplexität im Herzen der Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domaingesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

DR

Siehe Disaster Recovery.

Erkennung von Driften

Verfolgung von Abweichungen von einer Basiskonfiguration Sie können es beispielsweise verwenden, AWS CloudFormation um Abweichungen bei den Systemressourcen zu erkennen, oder Sie können AWS Control Tower damit Änderungen in Ihrer landing zone erkennen, die sich auf die Einhaltung von Governance-Anforderungen auswirken könnten.

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

Edge-Computing

Die Technologie, die die Rechenleistung für intelligente Geräte an den Rändern eines IoT-Netzwerks erhöht. Im Vergleich zu Cloud Computing kann Edge Computing die Kommunikationslatenz reduzieren und die Reaktionszeit verbessern.

Verschlüsselung

Ein Rechenprozess, der Klartextdaten, die für Menschen lesbar sind, in Chiffretext umwandelt.

Verschlüsselungsschlüssel

Eine kryptografische Zeichenfolge aus zufälligen Bits, die von einem Verschlüsselungsalgorithmus generiert wird. Schlüssel können unterschiedlich lang sein, und jeder Schlüssel ist so konzipiert, dass er unvorhersehbar und einzigartig ist.

Endianismus

Die Reihenfolge, in der Bytes im Computerspeicher gespeichert werden. Big-Endian-Systeme speichern das höchstwertige Byte zuerst. Little-Endian-Systeme speichern das niedrigwertigste Byte zuerst.

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

Ein System, das wichtige Geschäftsprozesse (wie Buchhaltung, MES und Projektmanagement) für ein Unternehmen automatisiert und verwaltet.

Envelope-Verschlüsselung

Der Prozess der Verschlüsselung eines Verschlüsselungsschlüssels mit einem anderen Verschlüsselungsschlüssel. Weitere Informationen finden Sie unter Envelope-Verschlüsselung in der AWS Key Management Service (AWS KMS) -Dokumentation.

Umgebung

Eine Instance einer laufenden Anwendung. Die folgenden Arten von Umgebungen sind beim Cloud-Computing üblich:

- Entwicklungsumgebung – Eine Instance einer laufenden Anwendung, die nur dem Kernteam zur Verfügung steht, das für die Wartung der Anwendung verantwortlich ist. Entwicklungsumgebungen werden verwendet, um Änderungen zu testen, bevor sie in höhere Umgebungen übertragen werden. Diese Art von Umgebung wird manchmal als Testumgebung bezeichnet.
- Niedrigere Umgebungen – Alle Entwicklungsumgebungen für eine Anwendung, z. B. solche, die für erste Builds und Tests verwendet wurden.
- Produktionsumgebung – Eine Instance einer laufenden Anwendung, auf die Endbenutzer zugreifen können. In einer CI/CD-Pipeline ist die Produktionsumgebung die letzte Bereitstellungsumgebung.
- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsthemen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit, Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS -Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

Der Prozess der Analyse eines Datensatzes, um seine Hauptmerkmale zu verstehen. Sie sammeln oder aggregieren Daten und führen dann erste Untersuchungen durch, um Muster zu

finden, Anomalien zu erkennen und Annahmen zu überprüfen. EDA wird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

F

Faktentabelle

Die zentrale Tabelle in einem Sternschema. Sie speichert quantitative Daten über den Geschäftsbetrieb. In der Regel enthält eine Faktentabelle zwei Arten von Spalten: Spalten, die Kennzahlen enthalten, und Spalten, die einen Fremdschlüssel für eine Dimensionstabelle enthalten.

schnell scheitern

Eine Philosophie, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu verkürzen. Dies ist ein wichtiger Bestandteil eines agilen Ansatzes.

Grenze zur Fehlerisolierung

Dabei handelt es sich um eine Grenze AWS Cloud, z. B. eine Availability Zone AWS-Region, eine Steuerungsebene oder eine Datenebene, die die Auswirkungen eines Fehlers begrenzt und die Widerstandsfähigkeit von Workloads verbessert. Weitere Informationen finden Sie unter Grenzen zur AWS Fehlerisolierung.

Feature-Zweig

Siehe Zweig.

Features

Die Eingabedaten, die Sie verwenden, um eine Vorhersage zu treffen. In einem Fertigungskontext könnten Feature beispielsweise Bilder sein, die regelmäßig von der Fertigungslinie aus aufgenommen werden.

Bedeutung der Feature

Wie wichtig ein Feature für die Vorhersagen eines Modells ist. Dies wird in der Regel als numerischer Wert ausgedrückt, der mit verschiedenen Techniken wie Shapley Additive Explanations (SHAP) und integrierten Gradienten berechnet werden kann. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit:AWS.

Featuretransformation

Daten für den ML-Prozess optimieren, einschließlich der Anreicherung von Daten mit zusätzlichen Quellen, der Skalierung von Werten oder der Extraktion mehrerer Informationssätze aus einem einzigen Datenfeld. Das ermöglicht dem ML-Modell, von den Daten profitieren. Wenn Sie beispielsweise das Datum „27.05.2021 00:15:37“ in „2021“, „Mai“, „Donnerstag“ und „15“ aufschlüsseln, können Sie dem Lernalgorithmus helfen, nuancierte Muster zu erlernen, die mit verschiedenen Datenkomponenten verknüpft sind.

FGAC

Weitere Informationen finden Sie unter detaillierter Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

Die Verwendung mehrerer Bedingungen, um eine Zugriffsanfrage zuzulassen oder abzulehnen.

Flash-Cut-Migration

Eine Datenbankmigrationsmethode, bei der eine kontinuierliche Datenreplikation durch Erfassung von Änderungsdaten verwendet wird, um Daten in kürzester Zeit zu migrieren, anstatt einen schrittweisen Ansatz zu verwenden. Ziel ist es, Ausfallzeiten auf ein Minimum zu beschränken.

G

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

Bei Amazon eine Option CloudFront, um zu verhindern, dass Benutzer in bestimmten Ländern auf Inhaltsverteilungen zugreifen. Sie können eine Zulassungsliste oder eine Sperrliste verwenden, um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie in der Dokumentation unter Beschränkung der geografischen Verteilung Ihrer Inhalte. CloudFront

Gitflow-Workflow

Ein Ansatz, bei dem niedrigere und höhere Umgebungen unterschiedliche Zweige in einem Quellcode-Repository verwenden. Der Gitflow-Workflow gilt als veraltet, und der Trunk-basierte Workflow ist der moderne, bevorzugte Ansatz.

Greenfield-Strategie

Das Fehlen vorhandener Infrastruktur in einer neuen Umgebung. Bei der Einführung einer Neuausrichtung einer Systemarchitektur können Sie alle neuen Technologien ohne Einschränkung der Kompatibilität mit der vorhandenen Infrastruktur auswählen, auch bekannt als Brownfield. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Integritätsschutz

Eine allgemeine Regel, die dabei hilft, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Organisationseinheiten (OUs) zu regeln. Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die eine andere Datenbank-Engine verwendet (z. B. Oracle zu Amazon Aurora). Eine heterogene Migration ist in der Regel Teil einer Neuarchitektur, und die Konvertierung des Schemas kann eine komplexe Aufgabe sein. AWS bietet AWS SCT, welches bei Schemakonvertierungen hilft.

hohe Verfügbarkeit (HA)

Die Fähigkeit eines Workloads, im Falle von Herausforderungen oder Katastrophen kontinuierlich und ohne Eingreifen zu arbeiten. HA-Systeme sind so konzipiert, dass sie automatisch ein Failover durchführen, gleichbleibend hohe Leistung bieten und unterschiedliche Lasten und Ausfälle mit minimalen Leistungseinbußen bewältigen.

historische Modernisierung

Ein Ansatz zur Modernisierung und Aufrüstung von Betriebstechnologiesystemen (OT), um den Bedürfnissen der Fertigungsindustrie besser gerecht zu werden. Ein Historian ist eine Art von Datenbank, die verwendet wird, um Daten aus verschiedenen Quellen in einer Fabrik zu sammeln und zu speichern.

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank zu einer Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS für SQL Server). Eine homogene Migration ist in der Regel Teil eines Hostwechsels oder eines Plattformwechsels. Sie können native Datenbankserviceprogramme verwenden, um das Schema zu migrieren.

heiße Daten

Daten, auf die häufig zugegriffen wird, z. B. Echtzeitdaten oder aktuelle Translationsdaten. Für diese Daten ist in der Regel eine leistungsstarke Speicherebene oder -klasse erforderlich, um schnelle Abfrageantworten zu ermöglichen.

Hotfix

Eine dringende Lösung für ein kritisches Problem in einer Produktionsumgebung. Aufgrund seiner Dringlichkeit wird ein Hotfix normalerweise außerhalb des typischen DevOps Release-Workflows erstellt.

Hypercare-Phase

Unmittelbar nach dem Cutover, der Zeitraum, in dem ein Migrationsteam die migrierten Anwendungen in der Cloud verwaltet und überwacht, um etwaige Probleme zu beheben. In der Regel dauert dieser Zeitraum 1–4 Tage. Am Ende der Hypercare-Phase überträgt das Migrationsteam in der Regel die Verantwortung für die Anwendungen an das Cloud-Betriebsteam.

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

Eine Richtlinie, die einem oder mehreren IAM-Prinzipalen zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU- und Arbeitsspeicherauslastung zwischen 5 und 20 Prozent über einen Zeitraum von 90 Tagen. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen oder sie On-Premises beizubehalten.

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

Ein Modell, das eine neue Infrastruktur für Produktionsworkloads bereitstellt, anstatt die bestehende Infrastruktur zu aktualisieren, zu patchen oder zu modifizieren. Unveränderliche Infrastrukturen sind von Natur aus konsistenter, zuverlässiger und vorhersehbarer als veränderliche Infrastrukturen. Weitere Informationen finden Sie in der Best Practice Deploy using immutable infrastructure im AWS Well-Architected Framework.

Eingehende (ingress) VPC

In einer Architektur AWS mit mehreren Konten ist dies eine VPC, die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

Industrie 4.0

Ein Begriff, der 2016 von Klaus Schwab eingeführt wurde und sich auf die Modernisierung von Fertigungsprozessen durch Fortschritte in den Bereichen Konnektivität, Echtzeitdaten, Automatisierung, Analytik und KI/ML bezieht.

Infrastruktur

Alle Ressourcen und Komponenten, die in der Umgebung einer Anwendung enthalten sind.

Infrastructure as Code (IaC)

Der Prozess der Bereitstellung und Verwaltung der Infrastruktur einer Anwendung mithilfe einer Reihe von Konfigurationsdateien. IaC soll Ihnen helfen, das Infrastrukturmanagement zu zentralisieren, Ressourcen zu standardisieren und schnell zu skalieren, sodass neue Umgebungen wiederholbar, zuverlässig und konsistent sind.

Industrielles Internet der Dinge (IIoT)

Einsatz von mit dem Internet verbundenen Sensoren und Geräten in Industriesektoren wie Fertigung, Energie, Automobilindustrie, Gesundheitswesen, Biowissenschaften und Landwirtschaft. Mehr Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektions-VPC

In einer Architektur AWS mit mehreren Konten eine zentralisierte VPC, die Inspektionen des Netzwerkverkehrs zwischen VPCs (in derselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Internet of Things (IoT)

Das Netzwerk verbundener physischer Objekte mit eingebetteten Sensoren oder Prozessoren, das über das Internet oder über ein lokales Kommunikationsnetzwerk mit anderen Geräten und Systemen kommuniziert. Weitere Informationen finden Sie unter Was ist IoT?

Interpretierbarkeit

Ein Merkmal eines Modells für Machine Learning, das beschreibt, inwieweit ein Mensch verstehen kann, wie die Vorhersagen des Modells von seinen Eingaben abhängen. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für Machine Learning mit AWS.

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITIL bietet die Grundlage für ITSM.

T service management (ITSM, IT-Servicemanagement)

Aktivitäten im Zusammenhang mit der Gestaltung, Implementierung, Verwaltung und Unterstützung von IT-Services für eine Organisation. Informationen zur Integration von Cloud-Vorgängen mit ITSM-Tools finden Sie im Leitfaden zur Betriebsintegration.

BIS

Weitere Informationen finden Sie in der IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

Eine Implementierung der Mandatory Access Control (MAC), bei der den Benutzern und den Daten selbst jeweils explizit ein Sicherheitslabelwert zugewiesen wird. Die Schnittmenge zwischen der Benutzersicherheitsbeschriftung und der Datensicherheitsbeschriftung bestimmt, welche Zeilen und Spalten für den Benutzer sichtbar sind.

Landing Zone

Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, die skalierbar und sicher ist. Dies ist ein Ausgangspunkt, von dem aus Ihre Organisationen Workloads und Anwendungen schnell und mit Vertrauen in ihre Sicherheits- und Infrastrukturumgebung starten und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Weitere Informationen finden Sie unter Label-basierte Zugriffskontrolle.

Geringste Berechtigung

Die bewährte Sicherheitsmethode, bei der nur die für die Durchführung einer Aufgabe erforderlichen Mindestberechtigungen erteilt werden. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

Ein System, welches das niedrigwertigste Byte zuerst speichert. Siehe auch Endianness.

Niedrigere Umgebungen

Siehe Umwelt.

M

Machine Learning (ML)

Eine Art künstlicher Intelligenz, die Algorithmen und Techniken zur Mustererkennung und zum Lernen verwendet. ML analysiert aufgezeichnete Daten, wie z. B. Daten aus dem Internet der Dinge (IoT), und lernt daraus, um ein statistisches Modell auf der Grundlage von Mustern zu erstellen. Weitere Informationen finden Sie unter Machine Learning.

Hauptzweig

Siehe Filiale.

Malware

Software, die entwickelt wurde, um die Computersicherheit oder den Datenschutz zu gefährden. Malware kann Computersysteme stören, vertrauliche Informationen durchsickern lassen oder sich unbefugten Zugriff verschaffen. Beispiele für Malware sind Viren, Würmer, Ransomware, Trojaner, Spyware und Keylogger.

verwaltete Dienste

AWS services für die die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betrieben werden, und Sie greifen auf die Endgeräte zu, um Daten zu speichern und abzurufen. Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB sind Beispiele für Managed Services. Diese werden auch als abstrakte Dienste bezeichnet.

Manufacturing Execution System (MES)

Ein Softwaresystem zur Nachverfolgung, Überwachung, Dokumentation und Steuerung von Produktionsprozessen, bei denen Rohstoffe in der Fertigung zu fertigen Produkten umgewandelt werden.

MAP

Siehe Migration Acceleration Program.

Mechanismus

Ein vollständiger Prozess, bei dem Sie ein Tool erstellen, die Akzeptanz des Tools vorantreiben und anschließend die Ergebnisse überprüfen, um Anpassungen vorzunehmen. Ein Mechanismus ist ein Zyklus, der sich im Laufe seiner Tätigkeit selbst verstärkt und verbessert. Weitere Informationen finden Sie unter Aufbau von Mechanismen im AWS Well-Architected Framework.

Mitgliedskonto

Alle AWS-Konten außer dem Verwaltungskonto, die Teil einer Organisation in sind. AWS Organizations Ein Konto kann jeweils nur einer Organisation angehören.

DURCHEINANDER

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

Ein leichtes machine-to-machine (M2M) -Kommunikationsprotokoll, das auf dem Publish/Subscribe-Muster für IoT-Geräte mit beschränkten Ressourcen basiert.

Microservice

Ein kleiner, unabhängiger Service, der über klar definierte APIs kommuniziert und in der Regel kleinen, eigenständigen Teams gehört. Ein Versicherungssystem kann beispielsweise Microservices beinhalten, die Geschäftsfunktionen wie Vertrieb oder Marketing oder Subdomains wie Einkauf, Schadenersatz oder Analytik zugeordnet sind. Zu den Vorteilen von Microservices gehören Agilität, flexible Skalierung, einfache Bereitstellung, wiederverwendbarer Code und Ausfallsicherheit. Weitere Informationen finden Sie unter Integration von Microservices mithilfe serverloser Dienste. AWS

Microservices-Architekturen

Ein Ansatz zur Erstellung einer Anwendung mit unabhängigen Komponenten, die jeden Anwendungsprozess als Microservice ausführen. Diese Microservices kommunizieren über eine klar definierte Schnittstelle mithilfe einfacher APIs. Jeder Microservice in dieser Architektur kann aktualisiert, bereitgestellt und skaliert werden, um den Bedarf an bestimmten Funktionen einer Anwendung zu decken. Weitere Informationen finden Sie unter Implementierung von Microservices auf. AWS

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAP umfasst eine Migrationsmethode für die methodische Durchführung von Legacy-Migrationen sowie eine Reihe von Tools zur Automatisierung und Beschleunigung gängiger Migrationsszenarien.

Migration in großem Maßstab

Der Prozess, bei dem der Großteil des Anwendungsportfolios in Wellen in die Cloud verlagert wird, wobei in jeder Welle mehr Anwendungen schneller migriert werden. In dieser Phase werden die bewährten Verfahren und Erkenntnisse aus den früheren Phasen zur Implementierung einer Migrationsfabrik von Teams, Tools und Prozessen zur Optimierung der Migration von Workloads durch Automatisierung und agile Bereitstellung verwendet. Dies ist die dritte Phase der AWS - Migrationsstrategie.

Migrationsfabrik

Funktionsübergreifende Teams, die die Migration von Workloads durch automatisierte, agile Ansätze optimieren. Zu den Teams in der Migrationsabteilung gehören in der Regel Betriebsabläufe, Geschäftsanalysten und Eigentümer, Migrationsingenieure, Entwickler und DevOps Experten, die in Sprints arbeiten. Zwischen 20 und 50 Prozent eines Unternehmensanwendungsportfolios bestehen aus sich wiederholenden Mustern, die durch einen Fabrik-Ansatz optimiert werden können. Weitere Informationen finden Sie in Diskussion über Migrationsfabriken und den Leitfaden zur Cloud-Migration-Fabrik in diesem Inhaltssatz.

Migrationsmetadaten

Die Informationen über die Anwendung und den Server, die für den Abschluss der Migration benötigt werden. Für jedes Migrationsmuster ist ein anderer Satz von Migrationsmetadaten erforderlich. Beispiele für Migrationsmetadaten sind das Zielsubnetz, die Sicherheitsgruppe und AWS das Konto.

Migrationsmuster

Eine wiederholbare Migrationsaufgabe, in der die Migrationsstrategie, das Migrationsziel und die verwendete Migrationsanwendung oder der verwendete Migrationsservice detailliert beschrieben werden. Beispiel: Rehost-Migration zu Amazon EC2 mit AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung, Migrationspriorisierung und Wellenplanung). Das MPA-Tool (Anmeldung erforderlich) steht allen AWS Beratern und APN-Partnerberatern kostenlos zur Verfügung.

Migration Readiness Assessment (MRA)

Der Prozess, bei dem mithilfe des AWS CAF Erkenntnisse über den Cloud-Bereitschaftsstatus eines Unternehmens gewonnen, Stärken und Schwächen identifiziert und ein Aktionsplan zur Schließung festgestellter Lücken erstellt wird. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRA ist die erste Phase der AWS - Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wurde, um einen Workload auf den AWS Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Sie Ihr Unternehmen, um umfangreiche Migrationen zu beschleunigen.

ML

Siehe maschinelles Lernen.

Modernisierung

Umwandlung einer veralteten (veralteten oder monolithischen) Anwendung und ihrer Infrastruktur in ein agiles, elastisches und hochverfügbares System in der Cloud, um Kosten zu senken, die Effizienz zu steigern und Innovationen zu nutzen. Weitere Informationen finden Sie unter Strategie zur Modernisierung von Anwendungen in der AWS Cloud.

Bewertung der Modernisierungsfähigkeit

Eine Bewertung, anhand derer festgestellt werden kann, ob die Anwendungen einer Organisation für die Modernisierung bereit sind, Vorteile, Risiken und Abhängigkeiten identifiziert und ermittelt wird, wie gut die Organisation den zukünftigen Status dieser Anwendungen unterstützen kann. Das Ergebnis der Bewertung ist eine Vorlage der Zielarchitektur, eine Roadmap, in der die Entwicklungsphasen und Meilensteine des Modernisierungsprozesses detailliert beschrieben werden, sowie ein Aktionsplan zur Behebung festgestellter Lücken. Weitere Informationen finden Sie unter Evaluierung der Modernisierungsbereitschaft von Anwendungen in der AWS Cloud.

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

Ein Prozess, der dabei hilft, Vorhersagen für mehrere Klassen zu generieren (wobei eines von mehr als zwei Ergebnissen vorhergesagt wird). Ein ML-Modell könnte beispielsweise fragen: „Ist dieses Produkt ein Buch, ein Auto oder ein Telefon?“ oder „Welche Kategorie von Produkten ist für diesen Kunden am interessantesten?“

veränderbare Infrastruktur

Ein Modell, das die bestehende Infrastruktur für Produktionsworkloads aktualisiert und modifiziert. Für eine verbesserte Konsistenz, Zuverlässigkeit und Vorhersagbarkeit empfiehlt das AWS Well-Architected Framework die Verwendung einer unveränderlichen Infrastruktur als bewährte Methode.

O

OAC

Weitere Informationen finden Sie unter Origin Access Control.

OAI

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

Eine Migrationsmethode, bei der der Quell-Workload während des Migrationsprozesses heruntergefahren wird. Diese Methode ist mit längeren Ausfallzeiten verbunden und wird in der Regel für kleine, unkritische Workloads verwendet.

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

Ein machine-to-machine (M2M) -Kommunikationsprotokoll für die industrielle Automatisierung. OPC-UA bietet einen Interoperabilitätsstandard mit Datenverschlüsselungs-, Authentifizierungs- und Autorisierungsschemata.

Vereinbarung auf Betriebsebene (OLA)

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen zu liefern, um ein Service Level Agreement (SLA) zu unterstützen.

Überprüfung der Betriebsbereitschaft (ORR)

Eine Checkliste mit Fragen und zugehörigen bewährten Methoden, die Ihnen helfen, Vorfälle und mögliche Ausfälle zu verstehen, zu bewerten, zu verhindern oder deren Umfang zu reduzieren. Weitere Informationen finden Sie unter Operational Readiness Reviews (ORR) im AWS Well-Architected Framework.

Betriebstechnologie (OT)

Hardware- und Softwaresysteme, die mit der physischen Umgebung zusammenarbeiten, um industrielle Abläufe, Ausrüstung und Infrastruktur zu steuern. In der Fertigung ist die Integration

von OT- und Informationstechnologie (IT) -Systemen ein zentraler Schwerpunkt der Industrie 4.0-Transformationen.

Betriebsintegration (OI)

Der Prozess der Modernisierung von Abläufen in der Cloud, der Bereitschaftsplanung, Automatisierung und Integration umfasst. Weitere Informationen finden Sie im Leitfaden zur Betriebsintegration.

Organisationspfad

Ein Pfad, der von erstellt wird und in AWS CloudTrail dem alle Ereignisse für alle AWS-Konten in einer Organisation protokolliert werden. AWS Organizations Diese Spur wird in jedem AWS-Konto , der Teil der Organisation ist, erstellt und verfolgt die Aktivität in jedem Konto. Weitere Informationen finden Sie in der CloudTrail Dokumentation unter Erstellen eines Pfads für eine Organisation.

Organisatorisches Veränderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCM hilft Organisationen dabei, sich auf neue Systeme und Strategien vorzubereiten und auf diese umzustellen, indem es die Akzeptanz von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework aufgrund der Geschwindigkeit des Wandels, der bei Projekten zur Cloud-Einführung erforderlich ist, als Mitarbeiterbeschleunigung bezeichnet. Weitere Informationen finden Sie im OCM-Handbuch.

Ursprungszugriffskontrolle (OAC)

In CloudFront, eine erweiterte Option zur Zugriffsbeschränkung, um Ihre Amazon Simple Storage Service (Amazon S3) -Inhalte zu sichern. OAC unterstützt alle S3-Buckets insgesamt AWS-Regionen, serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) sowie dynamische `PUT` und `DELETE` Anfragen an den S3-Bucket.

Ursprungszugriffsidentität (OAI)

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie OAI verwenden, CloudFront erstellt es einen Principal, mit dem sich Amazon S3 authentifizieren kann. Authentifizierte Principals können nur über eine bestimmte Distribution auf Inhalte in einem S3-Bucket zugreifen. CloudFront Siehe auch OAC, das eine detailliertere und verbesserte Zugriffskontrolle bietet.

ODER

Siehe Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

P

Berechtigungsgrenze

Eine IAM-Verwaltungsrichtlinie, die den IAM-Prinzipalen zugeordnet ist, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitys in der IAM-Dokumentation.

persönlich identifizierbare Informationen (PII)

Informationen, die, wenn sie direkt betrachtet oder mit anderen verwandten Daten kombiniert werden, verwendet werden können, um vernünftige Rückschlüsse auf die Identität einer Person zu ziehen. Beispiele für personenbezogene Daten sind Namen, Adressen und Kontaktinformationen.

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

Eine Reihe vordefinierter Schritte, die die mit Migrationen verbundenen Aufgaben erfassen, z. B. die Bereitstellung zentraler Betriebsfunktionen in der Cloud. Ein Playbook kann die Form von Skripten, automatisierten Runbooks oder einer Zusammenfassung der Prozesse oder Schritte annehmen, die für den Betrieb Ihrer modernisierten Umgebung erforderlich sind.

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

Ein Objekt, das Berechtigungen definieren (siehe identitätsbasierte Richtlinie), Zugriffsbedingungen spezifizieren (siehe ressourcenbasierte Richtlinie) oder die maximalen Berechtigungen für alle Konten in einer Organisation definieren kann AWS Organizations (siehe Dienststeuerungsrichtlinie).

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht. Weitere Informationen finden Sie unter Datenpersistenz in Microservices aktivieren.

Portfoliobewertung

Ein Prozess, bei dem das Anwendungsportfolio ermittelt, analysiert und priorisiert wird, um die Migration zu planen. Weitere Informationen finden Sie in Bewerten der Migrationsbereitschaft.

predicate

Eine Abfragebedingung, die `true` oder zurückgibt`false`, was üblicherweise in einer Klausel vorkommt. `WHERE`

Prädikat Pushdown

Eine Technik zur Optimierung von Datenbankabfragen, bei der die Daten in der Abfrage vor der Übertragung gefiltert werden. Dadurch wird die Datenmenge reduziert, die aus der relationalen Datenbank abgerufen und verarbeitet werden muss, und die Abfrageleistung wird verbessert.

Präventive Kontrolle

Eine Sicherheitskontrolle, die verhindern soll, dass ein Ereignis eintritt. Diese Kontrollen stellen eine erste Verteidigungslinie dar, um unbefugten Zugriff oder unerwünschte Änderungen an Ihrem Netzwerk zu verhindern. Weitere Informationen finden Sie unter Präventive Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz durch Design

Ein Ansatz in der Systemtechnik, der den Datenschutz während des gesamten Engineering-Prozesses berücksichtigt.

Privat gehostete Zonen

Ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und ihre Subdomains innerhalb einer oder mehrerer VPCs reagieren soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive Steuerung

Eine Sicherheitskontrolle, die den Einsatz nicht richtlinienkonformer Ressourcen verhindern soll. Mit diesen Steuerelementen werden Ressourcen gescannt, bevor sie bereitgestellt werden. Wenn die Ressource nicht mit der Steuerung konform ist, wird sie nicht bereitgestellt. Weitere Informationen finden Sie im Referenzhandbuch zu Kontrollen in der AWS Control Tower Dokumentation und unter Proaktive Kontrollen unter Implementierung von Sicherheitskontrollen am AWS.

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, vom Design, der Entwicklung und Markteinführung über Wachstum und Reife bis hin zur Markteinführung und Markteinführung.

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

In der Fertigung ein äußerst zuverlässiger, anpassungsfähiger Computer, der Maschinen überwacht und Fertigungsprozesse automatisiert.

Pseudonymisierung

Der Prozess, bei dem persönliche Identifikatoren in einem Datensatz durch Platzhalterwerte ersetzt werden. Pseudonymisierung kann zum Schutz der Privatsphäre beitragen. Pseudonymisierte Daten gelten weiterhin als personenbezogene Daten.

veröffentlichen/abonnieren (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen, den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

Eine Reihe von Schritten, wie Anweisungen, die für den Zugriff auf die Daten in einem relationalen SQL-Datenbanksystem verwendet werden.

Abfrageplanregression

Wenn ein Datenbankserviceoptimierer einen weniger optimalen Plan wählt als vor einer bestimmten Änderung der Datenbankumgebung. Dies kann durch Änderungen an Statistiken, Beschränkungen, Umgebungseinstellungen, Abfrageparameter-Bindungen und Aktualisierungen der Datenbank-Engine verursacht werden.

R

RACI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

Ransomware

Eine bösartige Software, die entwickelt wurde, um den Zugriff auf ein Computersystem oder Daten zu blockieren, bis eine Zahlung erfolgt ist.

RASCI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

Eine Kopie einer Datenbank, die nur für Lesezwecke verwendet wird. Sie können Abfragen an das Lesereplikat weiterleiten, um die Belastung auf Ihrer Primärdatenbank zu reduzieren.

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Dies bestimmt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Betriebsunterbrechung angesehen wird.

Wiederherstellungszeitziel (RTO)

Die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes.

Refaktorierung

Siehe 7 Rs.

Region

Eine Sammlung von AWS Ressourcen in einem geografischen Gebiet. Jeder AWS-Region ist isoliert und unabhängig von den anderen, um Fehlertoleranz, Stabilität und Belastbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann.

Regression

Eine ML-Technik, die einen numerischen Wert vorhersagt. Zum Beispiel, um das Problem „Zu welchem Preis wird dieses Haus verkauft werden?“ zu lösen Ein ML-Modell könnte ein lineares Regressionsmodell verwenden, um den Verkaufspreis eines Hauses auf der Grundlage bekannter Fakten über das Haus (z. B. die Quadratmeterzahl) vorherzusagen.

rehosten

Siehe 7 Rs.

Veröffentlichung

In einem Bereitstellungsprozess der Akt der Förderung von Änderungen an einer Produktionsumgebung.

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

Die Fähigkeit einer Anwendung, Störungen zu widerstehen oder sich von ihnen zu erholen. Hochverfügbarkeit und Notfallwiederherstellung sind häufig Überlegungen bei der Planung der Ausfallsicherheit in der. AWS Cloud Weitere Informationen finden Sie unter AWS Cloud Resilienz.

Ressourcenbasierte Richtlinie

Eine mit einer Ressource verknüpfte Richtlinie, z. B. ein Amazon-S3-Bucket, ein Endpunkt oder ein Verschlüsselungsschlüssel. Diese Art von Richtlinie legt fest, welchen Prinzipalen der Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen.

RACI-Matrix (verantwortlich, rechenschaftspflichtig, konsultiert, informiert)

Eine Matrix, die die Rollen und Verantwortlichkeiten aller an Migrationsaktivitäten und Cloud-Operationen beteiligten Parteien definiert. Der Matrixname leitet sich von den in der Matrix definierten Zuständigkeitstypen ab: verantwortlich (R), rechenschaftspflichtig (A), konsultiert (C) und informiert (I). Der Unterstützungstyp (S) ist optional. Wenn Sie Unterstützung einbeziehen, wird die Matrix als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Reaktive Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, die Behebung unerwünschter Ereignisse oder Abweichungen von Ihren Sicherheitsstandards voranzutreiben. Weitere Informationen finden Sie unter Reaktive Kontrolle in Implementieren von Sicherheitskontrollen in AWS.

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Drehung

Der Vorgang, bei dem ein Geheimnis regelmäßig aktualisiert wird, um es einem Angreifer zu erschweren, auf die Anmeldeinformationen zuzugreifen.

Zugriffskontrolle für Zeilen und Spalten (RCAC)

Die Verwendung einfacher, flexibler SQL-Ausdrücke mit definierten Zugriffsregeln. RCAC besteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel der Wiederherstellungszeit.

Runbook

Eine Reihe manueller oder automatisierter Verfahren, die zur Ausführung einer bestimmten Aufgabe erforderlich sind. Diese sind in der Regel darauf ausgelegt, sich wiederholende Operationen oder Verfahren mit hohen Fehlerquoten zu rationalisieren.

S

SAML 2.0

Ein offener Standard, den viele Identitätsanbieter (IdPs) verwenden. Diese Funktion ermöglicht föderiertes Single Sign-On (SSO), sodass sich Benutzer bei den API-Vorgängen anmelden AWS Management Console oder die AWS API-Operationen aufrufen können, ohne dass Sie einen Benutzer in IAM für alle in Ihrer Organisation erstellen müssen. Weitere Informationen zum SAML-2.0.-basierten Verbund finden Sie unter Über den SAML-2.0-basierten Verbund in der IAM-Dokumentation.

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder Benutzeranmeldeinformationen, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Was ist in einem Secrets Manager Manager-Geheimnis? in der Secrets Manager Manager-Dokumentation.

Sicherheitskontrolle

Ein technischer oder administrativer Integritätsschutz, der die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, verhindert, erkennt oder einschränkt. Es gibt vier Haupttypen von Sicherheitskontrollen: präventiv, detektiv, reaktionsschnell und proaktiv.

Härtung der Sicherheit

Der Prozess, bei dem die Angriffsfläche reduziert wird, um sie widerstandsfähiger gegen Angriffe zu machen. Dies kann Aktionen wie das Entfernen von Ressourcen, die nicht mehr benötigt werden, die Implementierung der bewährten Sicherheitsmethode der Gewährung geringster Berechtigungen oder die Deaktivierung unnötiger Feature in Konfigurationsdateien umfassen.

System zur Verwaltung von Sicherheitsinformationen und Ereignissen (security information and event management – SIEM)

Tools und Services, die Systeme für das Sicherheitsinformationsmanagement (SIM) und das Management von Sicherheitsereignissen (SEM) kombinieren. Ein SIEM-System sammelt, überwacht und analysiert Daten von Servern, Netzwerken, Geräten und anderen Quellen, um Bedrohungen und Sicherheitsverletzungen zu erkennen und Warnmeldungen zu generieren.

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer Amazon EC2 EC2-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

Verschlüsselung von Daten am Zielort durch denjenigen AWS service , der sie empfängt.

Service-Kontrollrichtlinie (SCP)

Eine Richtlinie, die eine zentrale Kontrolle über die Berechtigungen für alle Konten in einer Organisation in AWS Organizations ermöglicht. SCPs definieren Integritätsschutz oder legen Grenzwerte für Aktionen fest, die ein Administrator an Benutzer oder Rollen delegieren kann. Sie können SCPs als Zulassungs- oder Ablehnungslisten verwenden, um festzulegen, welche Services oder Aktionen zulässig oder verboten sind. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Richtlinien zur Dienststeuerung.

Service-Endpunkt

Die URL des Einstiegspunkts für einen AWS service. Sie können den Endpunkt verwenden, um programmgesteuert eine Verbindung zum Zielservice herzustellen. Weitere Informationen finden Sie unter AWS service -Endpunkte in der Allgemeine AWS-Referenz.

Service Level Agreement (SLA)

Eine Vereinbarung, in der klargestellt wird, was ein IT-Team seinen Kunden zu bieten verspricht, z. B. in Bezug auf Verfügbarkeit und Leistung der Services.

Service-Level-Indikator (SLI)

Eine Messung eines Leistungsaspekts eines Dienstes, z. B. seiner Fehlerrate, Verfügbarkeit oder Durchsatz.

Service-Level-Ziel (SLO)

Eine Zielkennzahl, die den Zustand eines Dienstes darstellt, gemessen anhand eines Service-Level-Indikators.

Modell der geteilten Verantwortung

Ein Modell, das die Verantwortung beschreibt, mit der Sie gemeinsam AWS für Cloud-Sicherheit und Compliance verantwortlich sind. AWS ist für die Sicherheit der Cloud verantwortlich, wohingegen Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

Ein Fehler in einer einzelnen, kritischen Komponente einer Anwendung, der das System stören kann.

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

Ein Muster für die Skalierung und Beschleunigung von Modernisierungsprojekten. Sobald neue Features und Produktversionen definiert werden, teilt sich das Kernteam auf, um neue Produktteams zu bilden. Dies trägt zur Skalierung der Fähigkeiten und Services Ihrer Organisation bei, verbessert die Produktivität der Entwickler und unterstützt schnelle Innovationen. Weitere Informationen finden Sie unter Schrittweiser Ansatz zur Modernisierung von Anwendungen in der AWS Cloud.

SPOTTEN

Siehe Single Point of Failure.

Sternschema

Eine Datenbank-Organisationsstruktur, die eine große Faktentabelle zum Speichern von Transaktions- oder Messdaten und eine oder mehrere kleinere dimensionale Tabellen zum Speichern von Datenattributen verwendet. Diese Struktur ist für die Verwendung in einem Data Warehouse oder für Business Intelligence-Zwecke konzipiert.

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie

unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in Ihrer VPC. Ein Subnetz muss sich in einer einzigen Availability Zone befinden.

Aufsichtskontrolle und Datenerfassung (SCADA)

In der Fertigung ein System, das Hardware und Software zur Überwachung von Sachanlagen und Produktionsabläufen verwendet.

Symmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der denselben Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet.

synthetisches Testen

Testen eines Systems auf eine Weise, die Benutzerinteraktionen simuliert, um potenzielle Probleme zu erkennen oder die Leistung zu überwachen. Sie können Amazon CloudWatch Synthetics verwenden, um diese Tests zu erstellen.

T

tags

Schlüssel-Wert-Paare, die als Metadaten für die Organisation Ihrer Ressourcen dienen. AWS Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen.

Zielvariable

Der Wert, den Sie in überwachtem ML vorhersagen möchten. Dies wird auch als Ergebnisvariable bezeichnet. In einer Fertigungsumgebung könnte die Zielvariable beispielsweise ein Produktfehler sein.

Aufgabenliste

Ein Tool, das verwendet wird, um den Fortschritt anhand eines Runbooks zu verfolgen. Eine Aufgabenliste enthält eine Übersicht über das Runbook und eine Liste mit allgemeinen Aufgaben, die erledigt werden müssen. Für jede allgemeine Aufgabe werden der geschätzte Zeitaufwand, der Eigentümer und der Fortschritt angegeben.

Testumgebungen

Siehe Umgebung.

Training

Daten für Ihr ML-Modell bereitstellen, aus denen es lernen kann. Die Trainingsdaten müssen die richtige Antwort enthalten. Der Lernalgorithmus findet Muster in den Trainingsdaten, die die Attribute der Input-Daten dem Ziel (die Antwort, die Sie voraussagen möchten) zuordnen. Es gibt ein ML-Modell aus, das diese Muster erfasst. Sie können dann das ML-Modell verwenden, um Voraussagen für neue Daten zu erhalten, bei denen Sie das Ziel nicht kennen.

Transit-Gateway

Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre VPCs und On-Premises-Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der AWS Transit Gateway Dokumentation unter Was ist ein Transit-Gateway.

Stammbasierter Workflow

Ein Ansatz, bei dem Entwickler Feature lokal in einem Feature-Zweig erstellen und testen und diese Änderungen dann im Hauptzweig zusammenführen. Der Hauptzweig wird dann sequentiell für die Entwicklungs-, Vorproduktions- und Produktionsumgebungen erstellt.

Vertrauenswürdiger Zugriff

Gewährung von Berechtigungen für einen Dienst, den Sie angeben, um Aufgaben in Ihrer Organisation AWS Organizations und in deren Konten in Ihrem Namen auszuführen. Der vertrauenswürdige Service erstellt in jedem Konto eine mit dem Service verknüpfte Rolle, wenn diese Rolle benötigt wird, um Verwaltungsaufgaben für Sie auszuführen. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Verwendung AWS Organizations mit anderen AWS Diensten.

Optimieren

Aspekte Ihres Trainingsprozesses ändern, um die Genauigkeit des ML-Modells zu verbessern. Sie können das ML-Modell z. B. trainieren, indem Sie einen Beschriftungssatz generieren, Beschriftungen hinzufügen und diese Schritte dann mehrmals unter verschiedenen Einstellungen wiederholen, um das Modell zu optimieren.

Zwei-Pizzen-Team

Ein kleines DevOps Team, das Sie mit zwei Pizzen ernähren können. Eine Teamgröße von zwei Pizzen gewährleistet die bestmögliche Gelegenheit zur Zusammenarbeit bei der Softwareentwicklung.

U

Unsicherheit

Ein Konzept, das sich auf ungenaue, unvollständige oder unbekannte Informationen bezieht, die die Zuverlässigkeit von prädiktiven ML-Modellen untergraben können. Es gibt zwei Arten von Unsicherheit: Epistemische Unsicherheit wird durch begrenzte, unvollständige Daten verursacht, wohingegen aleatorische Unsicherheit durch Rauschen und Randomisierung verursacht wird, die in den Daten liegt. Weitere Informationen finden Sie im Leitfaden Quantifizieren der Unsicherheit in Deep-Learning-Systemen.

undifferenzierte Aufgaben

Diese Arbeit wird auch als Schwerstarbeit bezeichnet. Dabei handelt es sich um Arbeiten, die zwar für die Erstellung und den Betrieb einer Anwendung erforderlich sind, aber dem Endbenutzer keinen direkten Mehrwert bieten oder keinen Wettbewerbsvorteil bieten. Beispiele für undifferenzierte Aufgaben sind Beschaffung, Wartung und Kapazitätsplanung.

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

Ein Vorgang zur Datenbankwartung, bei dem die Datenbank nach inkrementellen Aktualisierungen bereinigt wird, um Speicherplatz zurückzugewinnen und die Leistung zu verbessern.

Versionskontrolle

Prozesse und Tools zur Nachverfolgung von Änderungen, z. B. Änderungen am Quellcode in einem Repository.

VPC-Peering

Eine Verbindung zwischen zwei VPCs, mit der Sie den Datenverkehr mithilfe von privaten IP-Adressen weiterleiten können. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

Ein Software- oder Hardwarefehler, der die Sicherheit des Systems gefährdet.

W

Warmer Cache

Ein Puffer-Cache, der aktuelle, relevante Daten enthält, auf die häufig zugegriffen wird. Die Datenbank-Instance kann aus dem Puffer-Cache lesen, was schneller ist als das Lesen aus dem Hauptspeicher oder von der Festplatte.

warme Daten

Daten, auf die selten zugegriffen wird. Bei der Abfrage dieser Art von Daten sind mäßig langsame Abfragen in der Regel akzeptabel.

Fensterfunktion

Eine SQL-Funktion, die eine Berechnung für eine Gruppe von Zeilen durchführt, die sich in irgendeiner Weise auf den aktuellen Datensatz beziehen. Fensterfunktionen sind nützlich für die Verarbeitung von Aufgaben wie die Berechnung eines gleitenden Durchschnitts oder für den Zugriff auf den Wert von Zeilen auf der Grundlage der relativen Position der aktuellen Zeile.

Workload

Ein Workload ist eine Sammlung von Ressourcen und Code, die einen Unternehmenswert bietet, wie z. B. eine kundenorientierte Anwendung oder ein Backend-Prozess.

Workstream

Funktionsgruppen in einem Migrationsprojekt, die für eine bestimmte Reihe von Aufgaben verantwortlich sind. Jeder Workstream ist unabhängig, unterstützt aber die anderen Workstreams im Projekt. Der Portfolio-Workstream ist beispielsweise für die Priorisierung von Anwendungen, die Wellenplanung und die Erfassung von Migrationsmetadaten verantwortlich. Der Portfolio-Workstream liefert diese Komponenten an den Migrations-Workstream, der dann die Server und Anwendungen migriert.

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Weitere Informationen finden Sie unter AWS Workload Qualification Framework.

einmal schreiben, viele lesen (WORM)

Ein Speichermodell, das Daten ein einziges Mal schreibt und verhindert, dass die Daten gelöscht oder geändert werden. Autorisierte Benutzer können die Daten so oft wie nötig lesen, aber sie können sie nicht ändern. Diese Datenspeicherinfrastruktur gilt als unveränderlich.

Z

Zero-Day-Exploit

Ein Angriff, in der Regel Malware, der eine Zero-Day-Sicherheitslücke ausnutzt.

Zero-Day-Sicherheitslücke

Ein unfehlbarer Fehler oder eine Sicherheitslücke in einem Produktionssystem. Bedrohungsakteure können diese Art von Sicherheitslücke nutzen, um das System anzugreifen. Entwickler werden aufgrund des Angriffs häufig auf die Sicherheitsanfälligkeit aufmerksam.

Zombie-Anwendung

Eine Anwendung, deren durchschnittliche CPU- und Arbeitsspeichernutzung unter 5 Prozent liegt. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.