Implementierung von Sicherheitskontrollen für AWS

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Implementierung von Sicherheitskontrollen für AWS

Table of Contents

Implementierung von Sicherheitskontrollen in AWS

Iqbal Umair, Gurpreet Kaur Cheema, Wasim Hossain, Joseph Nguyen, San Brar und Lucia Vanta, Amazon Web Services (AWS)

Dezember 2023 (Dokumentverlauf)

Sicherheit ist für jedes Unternehmen von entscheidender Bedeutung und stellt eine wichtige Säule des AWS Well-Architected Framework dar. Viele wissen jedoch nicht, wie sie Sicherheitsaspekte berücksichtigen und eine ganzheitliche Strategie für automatisierte Sicherheitstests und Abhilfe für ihre Cloud-Umgebungen entwickeln sollen. Durch die Verwendung von AWS-Services und Tools wie AWS Config, Amazon GuardDuty und AWS CloudFormation können Sie eine Strategie für Sicherheitstests erstellen und diese in Ihre AWS Cloud-Umgebungen integrieren.

Um die Einhaltung der Sicherheitsrichtlinien und -standards Ihres Unternehmens zu unterstützen, sind Sicherheitskontrollen technische oder administrative Integritätsschutzmaßnahmen, die dazu beitragen, die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, zu verhindern, zu erkennen oder zu verringern. Sie dienen dem Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Ressourcen und Daten. Im Folgenden finden Sie Beispiele für Sicherheitskontrollen:

- Implementierung der Multi-Faktor-Authentifizierung für Benutzer, die sich bei einer Anwendung anmelden müssen
- Protokollierung, Überwachung und Abfrage von Aktionen zum Zwecke der Durchführung von Echtzeitprüfungen der Kontoaktivitäten
- Sicherstellen, dass vertrauliche Daten verschlüsselt sind
- Sicherstellen, dass die Protokolle gemäß den Aufbewahrungsrichtlinien Ihres Unternehmens gespeichert werden

Es gibt vier Typen von Sicherheitskontrollen: präventiv, proaktiv, detektivisch und reaktiv. In diesem Handbuch werden die einzelnen Arten ausführlicher beschrieben und der Schwerpunkt liegt auf der Implementierung und Automatisierung dieser Kontrollen in die AWS Cloud. Dieser Leitfaden hilft Ihnen bei der Implementierung kontinuierlicher und proaktiver Sicherheitskontrollen.

Zielgruppe

Dieser Leitfaden richtet sich an Architekten und Sicherheitsingenieure, die für die Implementierung von Sicherheitskontrollen in der AWS Cloud verantwortlich sind. Wenn Ihr Unternehmen keine Sicherheitsrichtlinien, Kontrollziele oder Standards, wie unter Sicherheitskontrollen im Governance-Framework beschrieben, definiert hat, empfehlen wir, diese Governance-Aufgaben umzusetzen, bevor Sie dieses Handbuch umsetzen.

Gezielte Geschäftsergebnisse

Unternehmen nutzen Sicherheitskontrollen, um Risiken für ihre IT-Systeme zu mindern oder ihnen entgegenzuwirken. Kontrollen definieren die grundlegenden Anforderungen, um die wichtigsten Sicherheitsziele eines IT-Programms und seiner Sicherheitsstrategie zu erreichen. Durch die Einrichtung von Kontrollen wird die Sicherheitslage eines Unternehmens verbessert, da sie die Vertraulichkeit, Integrität und Verfügbarkeit seiner Daten und IT-Komponenten schützen. Ohne Kontrollen wäre es schwierig zu wissen, worauf man sich konzentrieren und was man investieren muss, um eine Sicherheitsbasis zu schaffen.

Sicherheitskontrollen können für eine Vielzahl von Szenarien eingesetzt werden. Beispiele hierfür sind die Erfüllung von Anforderungen, die sich aus Risikobewertungen ergeben, die Einhaltung von Industriestandards oder die Einhaltung von Vorschriften. Die Einhaltung der Sicherheitskontrollen zeigt, dass Sie das Risiko für ein System gemessen, das erforderliche Schutzniveau ermittelt und proaktiv Lösungen implementiert haben. Zusätzliche Faktoren, wie Unternehmen, Branche und geografische Lage, können die erforderlichen Sicherheitskontrollen bestimmen.

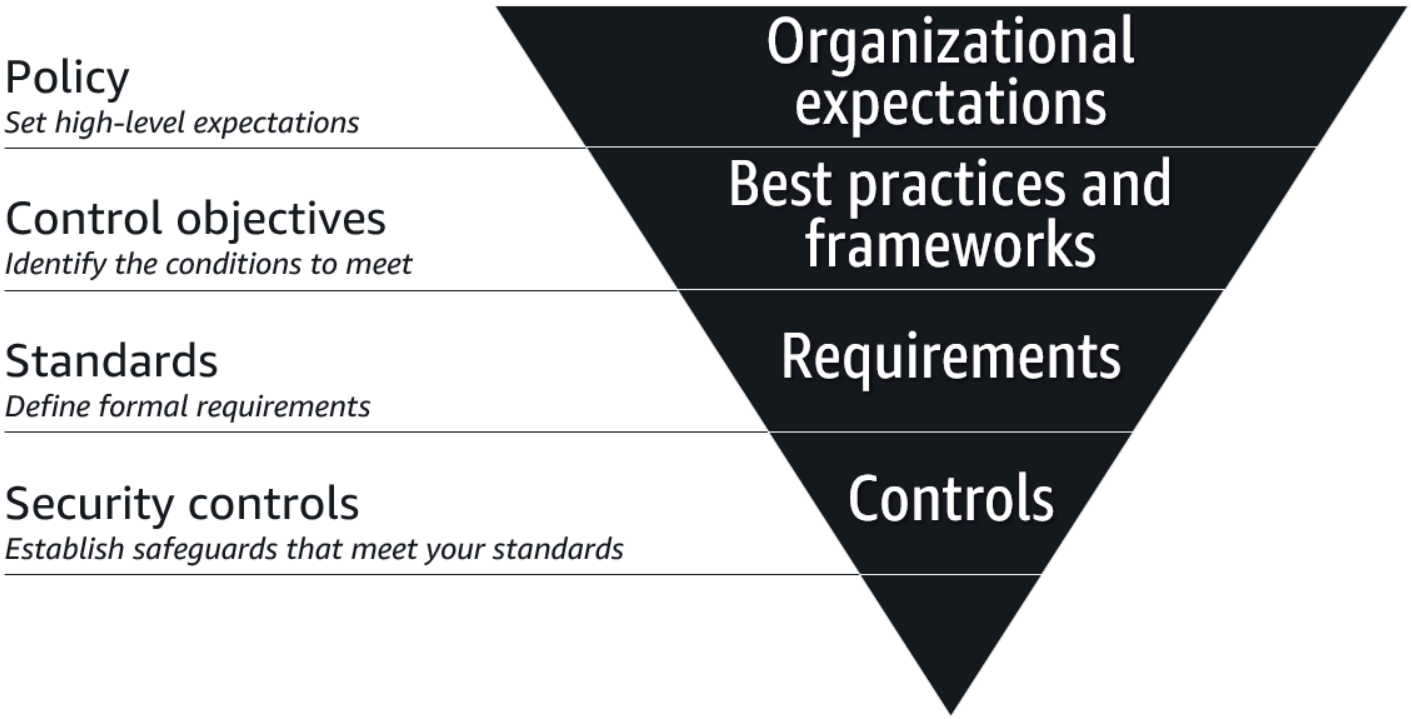
Beispiele für Vorschriften, die hierfür häufig zur Implementierung von Sicherheitskontrollen haben, sind:

- Bei einer Sicherheitsbeurteilung einer Anwendung wurde festgestellt, dass Zugriffskontrollen auf der Grundlage der Sensibilität der verarbeiteten Daten erforderlich sind.
- Sie müssen Sicherheitsstandards wie den Payment Card Industry Data Security Standard (PCI DSS), HIPAA (Health Insurance Portability and Accountability Act) oder das National Institute of Standards and Technology (NIST) einhalten.
- Sie müssen vertrauliche Informationen für Geschäftstransaktionen schützen.
- Ihr Unternehmen hat sich in eine geografische Region ausgedehnt, in der Sicherheitskontrollen erforderlich sind, z. B. eine Region, in der die Einhaltung der Allgemeinen Datenschutzverordnung (DSGVO) erforderlich ist.

Nachdem Sie diesen Leitfaden gelesen haben, sollten Sie mit den vier Arten von Sicherheitskontrollen vertraut sein, verstehen, wie sie Teil Ihres Sicherheits-Governance-Frameworks sind, und bereit sein, mit der Implementierung und Automatisierung von Sicherheitskontrollen in der AWS Cloud zu beginnen.

Sicherheitskontrollen im Governance-Framework

Es ist wichtig, von einer grundlegenden Ebene aus zu planen. Wie fängt man an? Die folgende Abbildung zeigt, wie Sie eine Sicherheits-Governance-Strategie auf der Grundlage von Richtlinien, Kontrollzielen, Standards und Sicherheitskontrollen entwickeln können.



Im Folgenden sind die hierarchischen Komponenten einer Governance-Strategie für Sicherheit aufgeführt:

- Richtlinie – eine Richtlinie ist die Grundlage jeder Cybersicherheits-Governance-Strategie. Es ist ein Dokument, in dem die Erwartungen des Unternehmens dargelegt werden, z. B. gesetzliche, regulatorische oder vertragliche Verpflichtungen, die es erfüllen muss. Die Richtlinien können je nach Branche und Region variieren.
- Ziele der Kontrolle – Ziele der Kontrolle sind Ziele, wie z. B. branchenweit anerkannte bewährte Verfahren, die Ihnen helfen, die Absicht einer Richtlinie zu erreichen. Beim Cloud-Computing setzen viele Unternehmen auf die Cloud Controls Matrix (CCM) (Website der Cloud Security Alliance), welches ein Rahmenwerk für Ziele der Cybersicherheitskontrolle ist.
- Standards – Standards sind formell festgelegte Anforderungen, die ein Kontrollziel erfüllen. Standards können Prozesse, Aktionen oder Konfigurationen beinhalten, und sie sind quantifizierbar, sodass Sie die Leistung anhand des Standards messen können.

- Sicherheitskontrollen – Sicherheitskontrollen sind die technischen oder administrativen Mechanismen, die Sie zur Umsetzung der Standards eingerichtet haben. Alle Sicherheitskontrollen entsprechen Standards, aber nicht alle Standards entsprechen Sicherheitskontrollen. Das Testen von Sicherheitskontrollen dient dazu, zu überwachen und zu messen, ob Sie die definierten Standards tatsächlich einhalten.

Dieser Leitfaden konzentriert sich auf die Gestaltung und Implementierung gängiger Arten von Sicherheitskontrollen in der AWS Cloud.

Typen von Sicherheitskontrollen

Es gibt vier Haupttypen von Sicherheitskontrollen:

- Präventive Kontrollen – Diese Kontrollen sollen verhindern, dass ein Ereignis eintritt.
- Proaktive Kontrollen – Diese Kontrollen sollen die Erstellung von nicht konformen Ressourcen verhindern.
- Detektivische Kontrollen – Diese Steuerelemente dienen der Erkennung, Protokollierung und Warnung, nachdem ein Ereignis eingetreten ist.
- Reaktive Kontrollen – Diese Kontrollen sind so konzipiert, dass sie bei unerwünschten Ereignissen oder Abweichungen von Ihrer Sicherheitsgrundlage Abhilfe schaffen.

Eine effektive Sicherheitsstrategie umfasst alle vier Arten von Sicherheitskontrollen. Präventive Kontrollen sind zwar die erste Verteidigungslinie, um unbefugten Zugriff oder ungewollte Änderungen an Ihrem Netzwerk zu verhindern. Sie müssen jedoch sicherstellen, dass Sie detektivische und reaktive Kontrollen einrichten, damit Sie wissen, wann ein Ereignis eintritt, und sofort geeignete Maßnahmen ergreifen können, um es zu beheben. Die Verwendung proaktiver Kontrollen fügt eine weitere Sicherheitsebene hinzu, da sie die präventiven Kontrollen, die im Allgemeinen strenger sind, ergänzen.

In den folgenden Abschnitten werden die einzelnen Arten von Kontrollen näher beschrieben. Sie erörtern die Ziele, den Implementierungsprozess, die Anwendungsfälle, die technologischen Überlegungen und die angestrebten Ergebnisse der einzelnen Kontrolltypen.

Präventive Kontrollen

Präventive Kontrollen sind Sicherheitskontrollen, die verhindern sollen, dass ein Ereignis eintritt. Diese Leitplanken sind eine erste Verteidigungslinie, um unbefugten Zugriff oder unerwünschte Änderungen an Ihrem Netzwerk zu verhindern. Ein Beispiel für eine präventive Kontrolle ist eine AWS Identity and Access Management (IAM) -Rolle, die nur Lesezugriff hat, da sie dazu beiträgt, unbeabsichtigte Schreibaktionen durch nicht autorisierte Benutzer zu verhindern.

Lesen Sie die folgenden Informationen zu dieser Art von Kontrolle:

- Ziele
- Prozess

- Anwendungsfälle
- Technologie
- Geschäftsergebnisse

Ziele

Der Hauptzweck präventiver Kontrollen besteht darin, die Wahrscheinlichkeit des Eintretens eines Bedrohungsereignisses zu minimieren oder zu vermeiden. Die Kontrolle sollte dazu beitragen, unbefugten Zugriff auf das System zu verhindern und zu verhindern, dass unbeabsichtigte Änderungen das System beeinträchtigen. Präventive Kontrollen haben folgende Ziele:

- Aufgabensegmentierung – Präventive Kontrollen können logische Grenzen setzen, die Rechte einschränken, sodass nur bestimmte Aufgaben in bestimmten Konten oder Umgebungen ausgeführt werden können. Beispiele sind unter anderem:
  - Segmentierung von Workloads auf verschiedene Konten für bestimmte Services
  - Trennung und Aufteilung der Konten in isolierte Produktions-, Entwicklungs- und Testumgebungen
  - Delegieren von Zugriff und Zuständigkeiten an mehrere Entitäten, um bestimmte Funktionen auszuführen, z. B. die Verwendung von IAM-Rollen oder die Übernahme von Rollen, sodass nur bestimmte Aufgabenbereiche bestimmte Aktionen ausführen können
- Zutrittskontrolle – Präventive Kontrollen können den Zugriff auf Ressourcen und Daten in der Umgebung konsistent gewähren oder verweigern. Beispiele sind unter anderem:
  - Verhindern, dass Benutzer ihre vorgesehenen Berechtigungen überschreiten, bekannt als Eskalation von Berechtigungen
  - Beschränkung des Zugriffs auf Anwendungen und Daten auf autorisierte Benutzer und Services
  - Kleinhalten der Administratorgruppe
  - Vermeidung der Verwendung der Anmeldeinformationen des Root-Benutzers
- Durchsetzung – Präventive Kontrollen können Ihrem Unternehmen helfen, seine Richtlinien, Richtlinien und Standards einzuhalten. Beispiele sind unter anderem:
  - Sperrkonfigurationen, die als Mindestsicherheitsbasis dienen
  - Implementierung zusätzlicher Sicherheitsmaßnahmen, wie z. B. Multi-Faktor-Authentifizierung
  - Vermeidung ungewöhnlicher Aufgaben und Aktionen, die von nicht genehmigten Rollen ausgeführt werden

Prozess

Präventive Kontrollzuordnung ist der Prozess, bei dem Kontrollen Anforderungen zugeordnet und diese Kontrollen mithilfe von Richtlinien implementiert werden, indem sie eingeschränkt, deaktiviert oder blockiert werden. Berücksichtigen Sie bei der Zuordnung von Kontrollen deren proaktive Wirkung auf die Umgebung, Ressourcen und Benutzer. Im Folgenden werden die bewährten Methoden für die Zuordnung von Steuerelementen beschrieben:

- Strenge Kontrollen, die eine Aktivität verbieten, sollten Produktionsumgebungen zugeordnet werden, in denen die Aktion Überprüfungs-, Genehmigungs- und Änderungsprozesse erfordert.
- In Entwicklungs- oder geschlossenen Umgebungen gibt es möglicherweise weniger präventive Kontrollen, um die nötige Flexibilität beim Entwickeln und Testen zu gewährleisten.
- Die präventiven Kontrollen werden von der Klassifizierung der Daten, dem Risikoniveau einer Komponente und der Risikomanagement-Richtlinie bestimmt.
- Zuordnung zu bestehenden Frameworks als Nachweis für die Einhaltung von Normen und Vorschriften.
- Implementieren Sie präventive Kontrollen nach geografischem Standort, Umgebung, Konten, Netzwerken, Benutzern, Rollen oder Ressourcen.

Anwendungsfälle

Umgang mit Daten

Es wird eine Rolle erstellt, die auf alle Daten in einem Konto zugreifen kann. Wenn sensible und verschlüsselte Daten vorhanden sind, können übermäßig freigiebige Rechte ein Risiko darstellen, je nachdem, welche Benutzer oder Gruppen die Rolle übernehmen können. Mithilfe einer Schlüsselrichtlinie in AWS Key Management Service (AWS KMS) können Sie steuern, wer Zugriff auf den Schlüssel hat und die Daten entschlüsseln kann.

Rechteeskalation

Wenn Administrator- und Schreibberechtigungen zu breit verteilt sind, kann ein Benutzer die Beschränkungen seiner vorgesehenen Berechtigungen umgehen und sich zusätzliche Rechte gewähren. Der Benutzer, der eine Rolle erstellt und verwaltet, kann eine Berechtigungsgrenze zuordnen, die die maximal zulässigen Rechte für die Rolle definiert.

Lockdown des Workloads

Wenn Ihr Unternehmen voraussichtlich nicht bestimmte Dienste nutzen muss, aktivieren Sie eine Dienststeuerungsrichtlinie, die einschränkt, welche Dienste in den Mitgliedskonten einer Organisation ausgeführt werden können, oder Dienste auf der Grundlage von einschränkt. AWS-Region Durch diese präventive Kontrolle kann das Ausmaß der Auswirkungen verringert werden, wenn es einem Bedrohungsakteur gelingt, ein Konto in Ihrer Organisation zu kompromittieren und darauf zuzugreifen. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien in diesem Handbuch.

Auswirkungen auf andere Anwendungen

Präventive Kontrollen können die Nutzung von Services und Features wie IAM, Verschlüsselung und Protokollierung erzwingen, um die Sicherheitsanforderungen Ihrer Anwendungen zu erfüllen. Sie können diese Kontrollen auch zum Schutz vor Schwachstellen verwenden, indem Sie die Aktionen einschränken, die ein Bedrohungsakteur aufgrund unbeabsichtigter Fehler oder Fehlkonfigurationen ausnutzen kann.

Technologie

Service-Kontrollrichtlinien

Darin AWS Organizations definieren Service Control Policies (SCPs) die maximal verfügbaren Berechtigungen für Mitgliedskonten in einer Organisation. Diese Richtlinien helfen Konten dabei, die Zugriffskontrollrichtlinien der Organisation einzuhalten. Beachten Sie beim Entwerfen von SCPs für Ihre Organisation Folgendes:

- SCPs sind präventive Kontrollen, da sie die maximal zulässigen Berechtigungen für IAM-Rollen und -Benutzer in den Mitgliedskonten der Organisation definieren und durchsetzen.
- SCPs wirken sich nur auf die IAM-Rollen und -Benutzer in den Mitgliedskonten der Organisation aus. Sie wirken sich nicht auf Benutzer und Rollen im Verwaltungskonto der Organisation aus.

Sie können eine SCP detaillierter gestalten, indem Sie die maximalen Berechtigungen für jede AWS-Region definieren.

IAM-IBerechtigungsgrenzen

In AWS Identity and Access Management (IAM) wird eine Berechtigungsgrenze verwendet, um die maximalen Berechtigungen festzulegen, die eine identitätsbasierte Richtlinie einer IAM-Entität

(Benutzern oder Rollen) gewähren kann. Durch eine Berechtigungsgrenze kann eine Entität nur die Aktionen durchführen, die sowohl von den identitätsbasierten Richtlinien als auch den Berechtigungsgrenzen erlaubt werden. Beachten Sie bei der Verwendung von Berechtigungsgrenzen Folgendes:

- Sie können eine AWS verwaltete Richtlinie oder eine vom Kunden verwaltete Richtlinie verwenden, um die Grenze für eine IAM-Entität festzulegen.
- Eine Berechtigungsgrenze gewährt selbst keine Berechtigungen. Die Richtlinie zur Berechtigungsgrenze schränkt die Berechtigungen ein, die der IAM-Entität gewährt werden.

Geschäftsergebnisse

Zeitersparnis

- Durch zusätzliche Automatisierung nach der Einrichtung präventiver Kontrollen können Sie den Bedarf an manuellen Eingriffen und die Häufigkeit von Fehlern reduzieren.
- Die Verwendung von Berechtigungsgrenzen als präventive Kontrolle hilft den Sicherheits- und IAM-Teams, sich auf wichtige Aufgaben wie Verwaltung und Support zu konzentrieren.

Einhaltung gesetzlicher Vorschriften

- Unternehmen müssen möglicherweise interne oder branchenspezifische Vorschriften einhalten. Dabei kann es sich um Regionsbeschränkungen, Benutzer- und Rolleneinschränkungen oder Serviceeinschränkungen handeln. SCPs können Ihnen helfen, die Vorschriften einzuhalten und Strafen bei Verstößen zu vermeiden.

Reduzierung des Risikos

- Mit dem Wachstum nimmt die Anzahl der Anfragen zur Erstellung und Verwaltung neuer Rollen und Richtlinien zu. Es wird immer schwieriger, den Kontext dessen zu verstehen, was erforderlich ist, um die Berechtigungen für jede Anwendung manuell zu erstellen. Die Einrichtung präventiver Kontrollen dient als Grundlage und hilft zu verhindern, dass Benutzer unbeabsichtigte Aktionen ausführen, selbst wenn ihnen versehentlich Zugriff gewährt wurde.
- Die Anwendung präventiver Kontrollen auf Zugriffsrichtlinien bietet eine zusätzliche Ebene zum Schutz von Daten und Komponenten.

Proaktive Kontrollen

Proaktive Kontrollen sind Sicherheitskontrollen, die die Erstellung von nicht konformen Ressourcen verhindern sollen. Diese Kontrollen können die Anzahl der Sicherheitsereignisse reduzieren, die durch reaktive und detektivische Kontrollen behandelt werden. Diese Kontrollen stellen sicher, dass die bereitgestellten Ressourcen konform sind, bevor sie bereitgestellt werden; daher gibt es kein Erkennungsereignis, das eine Reaktion oder Abhilfe erfordert.

Sie könnten z. B. eine detektivische Kontrolle anwenden, die Sie benachrichtigt, wenn ein Amazon Simple Storage Service (Amazon S3)-Bucket öffentlich zugänglich wird. Sie könnten auch über eine reaktive Kontrolle verfügen, die das Problem behebt. Obwohl diese beiden Kontrollen bereits vorhanden sind, können Sie eine weitere Schutzebene hinzufügen, indem Sie eine proaktive Kontrolle hinzufügen. Durch die proaktive Steuerung kann verhindert werden AWS CloudFormation, dass Updates für alle S3-Buckets erstellt werden, für die der öffentliche Zugriff aktiviert ist. Bedrohungsakteure könnten diese Kontrolle immer noch umgehen und Ressourcen außerhalb von einsetzen oder ändern CloudFormation. In diesem Fall würden die detektiven und reaktiven Kontrollen das Sicherheitsereignis beheben.

Lesen Sie die folgenden Informationen zu dieser Art von Kontrolle:

- Ziele
- Prozess
- Anwendungsfälle
- Technologie
- Geschäftsergebnisse

Ziele

- Proaktive Kontrollen helfen Ihnen dabei, Ihre Sicherheitsvorgänge und Qualitätsprozesse zu verbessern.
- Proaktive Kontrollen könnne Ihnen bei der Einhaltung von Sicherheitsrichtlinien, Standards und gesetzlichen Vorschriften oder Compliance-Verpflichtungen helfen.
- Proaktive Kontrollen können die Erstellung von nicht konformen Ressourcen verhindern.
- Proaktive Kontrollen können die Anzahl der Sicherheitserkenntnisse reduzieren.
- Proaktive Kontrollen bieten eine weitere Schutzebene gegen Bedrohungsakteure, die präventive Kontrollen umgehen und versuchen, nicht konforme Ressourcen bereitzustellen.

- In Kombination mit präventiven, detektivischen und reaktiven Kontrollen können proaktive Kontrollen Ihnen helfen, potenzielle Sicherheitsvorfälle zu bewältigen.

Prozess

Proaktive Kontrollen ergänzen präventive Kontrollen. Proaktive Kontrollen verringern das Sicherheitsrisiko Ihres Unternehmens und erzwingen die Bereitstellung von konformen Ressourcen. Diese Kontrollen bewerten die Konformität von Ressourcen, bevor diese erstellt oder aktualisiert werden. Proaktive Kontrollen werden in der Regel mithilfe von CloudFormation Hooks implementiert. Wenn die Ressource die Validierung durch die proaktive Kontrolle nicht besteht, können Sie entweder die Bereitstellung der Ressource ablehnen oder eine Warnmeldung ausgeben. Im Folgenden finden Sie einige Tipps und bewährte Methoden für den Aufbau proaktiver Kontrollen:

- Stellen Sie sicher, dass proaktive Kontrollen den Compliance-Anforderungen Ihres Unternehmens entsprechen.
- Stellen Sie sicher, dass proaktive Kontrollen den bewährten Sicherheitsmethoden für den jeweiligen Service entsprechen.
- Verwenden Sie CloudFormation StackSets oder eine andere Lösung, um proaktive Kontrollen für mehrere AWS-Regionen Konten bereitzustellen.
- Stellen Sie sicher, dass die Warn- oder Fehlermeldung, die mit einer proaktiven Kontrolle verbunden ist, eindeutig und klar ist. Dies hilft Entwicklern, den Grund zu verstehen, warum die Ressource die Bewertung nicht bestanden hat.
- Beginnen Sie bei der Erstellung neuer proaktiver Kontrollen im Beobachtungsmodus. Das bedeutet, dass Sie eine Warnmeldung senden, anstatt die Bereitstellung der Ressource fehlschlagen zu lassen. Dies hilft Ihnen, die Auswirkungen der proaktiven Kontrolle zu verstehen.
- Aktivieren Sie die Protokollierung in Amazon CloudWatch Logs für proaktive Kontrollen.
- Wenn Sie den Aufruf einer bestimmten proaktiven Steuerung überwachen müssen, verwenden Sie eine EventBridge Amazon-Regel und abonnieren Sie Aufrufereignisse für den CloudFormation Hook.

Anwendungsfälle

- Verhindern der Bereitstellung nicht konformer Ressourcen
- Erfüllung von Compliance-Anforderungen

- Verbessern der Codequalität durch Erzwingen der Behebung eines Sicherheitsproblems vor der Bereitstellung
- Verringern der mit der Behebung von Sicherheitsproblemen nach der Bereitstellung verbundenen betrieblichen Ausfallzeiten

Technologie

CloudFormation Hooks

AWS CloudFormationhilft Ihnen dabei, AWS Ressourcen einzurichten, sie schnell und konsistent bereitzustellen und sie während ihres gesamten Lebenszyklus regionsübergreifend AWS-Konten zu verwalten. CloudFormation Hooks bewerten proaktiv die Konfiguration Ihrer CloudFormation Ressourcen, bevor sie bereitgestellt werden. Wenn nicht konforme Ressourcen gefunden werden, wird ein Fehlerstatus zurückgegeben. Je nach Hook-Fehlermodus CloudFormation kann der Vorgang fehlschlagen oder es wird eine Warnung angezeigt, die es dem Benutzer ermöglicht, mit der Bereitstellung fortzufahren. Sie können verfügbare Hooks verwenden oder Ihre eigenen entwickeln.

AWS Control Tower

AWS Control Towerhilft Ihnen bei der Einrichtung und Verwaltung einer Umgebung AWS mit mehreren Konten und befolgt dabei die vorgeschriebenen Best Practices. AWS Control Tower bietet vorkonfigurierte proaktive Steuerungen, die Sie in Ihrer landing zone aktivieren können. Wenn Ihre landing zone mit eingerichtet ist AWS Control Tower, können Sie diese optionalen proaktiven Steuerungen als Ausgangspunkt für Ihre Organisation verwenden. Sie können bei Bedarf zusätzliche, benutzerdefinierte proaktive Kontrollen CloudFormation einbauen.

Geschäftsergebnisse

Weniger menschlicher Aufwand und Fehler

Proaktive Kontrollen verringern das Risiko menschlicher Fehler, die zur Bereitstellung von nicht konformen Ressourcen führen. Sie verringern auch den menschlichen Aufwand in späteren Phasen des Entwicklungszyklus, da sie die Entwickler dazu bringen, die Ressourcensicherheit vor der Bereitstellung zu berücksichtigen. Damit wird die Praxis der Linksverschiebung auf den Aufbau sicherer Ressourcen angewandt, weil sie Compliance früher im Entwicklungszyklus erzwingt.

Geringere Kosten

Es ist im Allgemeinen teurer, ein Sicherheitsproblem nach der Bereitstellung zu beheben. Das Erkennen und Beheben von Problemen zu einem früheren Zeitpunkt im Entwicklungszyklus senkt die Entwicklungskosten.

Zeitersparnis

Da proaktive Kontrollen die Bereitstellung nicht konformer Ressourcen verhindern, reduzieren sie die Zeit, die Sie für die Prüfung und Behebung von Sicherheitsproblemen aufwenden. Sie verringern auch die Anzahl der Sicherheitserkenntnisse, die bei detektivischen Kontrollen erst später im Entwicklungszyklus festgestellt würden.

Einhaltung gesetzlicher Vorschriften

Wenn Ihre Organisation interne oder branchenspezifische Vorschriften einhalten muss, können proaktive Kontrollen Ihnen dabei helfen, konform zu bleiben und Strafen für Verstöße zu vermeiden.

Reduzierung des Risikos

Proaktive Kontrollen helfen Entwicklern dabei, konforme und sicherere Ressourcen bereitzustellen, sodass proaktive Kontrollen das Sicherheitsrisiko für Ihre Organisation verringern.

Detektivische Kontrollen

Detektivische Kontrollen sind Sicherheitskontrollen, die darauf ausgelegt sind, ein Ereignis zu erkennen, zu protokollieren und eine Warnung auszusprechen, nachdem es eingetreten ist. Detektivische Kontrollen sind ein grundlegender Bestandteil des Governance-Frameworks. Diese Leitplanken bilden eine zweite Verteidigungslinie und informieren Sie über Sicherheitsprobleme, die die präventiven Kontrollen umgangen haben.

Sie könnten z. B. eine detektivische Kontrolle anwenden, die erkennt und Sie benachrichtigt, wenn ein Amazon Simple Storage Service (Amazon S3)-Bucket öffentlich zugänglich wird. Möglicherweise verfügen Sie über präventive Kontrollen, die den öffentlichen Zugriff auf S3-Buckets auf Kontoebene und dann den Zugriff über SCPs deaktivieren, aber ein Bedrohungsakteur kann diese präventiven Kontrollen umgehen, indem er sich als Administratorbenutzer anmeldet. In diesen Situationen kann eine detektivische Kontrolle Sie auf die Fehlkonfiguration und die potenzielle Bedrohung aufmerksam machen.

Lesen Sie die folgenden Informationen zu dieser Art von Kontrolle:

Ziele

- Detektivische Kontrollen helfen Ihnen dabei, Ihre Sicherheits- und Qualitätsprozesse zu verbessern.
- Detektivische Kontrollen helfen Ihnen dabei, regulatorische, rechtliche oder Compliance-Verpflichtungen zu erfüllen.
- Detektivische Kontrollen bieten Sicherheitsteams Transparenz, sodass sie auf Sicherheitsprobleme reagieren können, einschließlich hochentwickelter Bedrohungen, die die präventiven Kontrollen umgehen.
- Detektivische Kontrollen können Ihnen dabei helfen, geeignete Maßnahmen für Sicherheitsprobleme und potenzielle Bedrohungen zu finden.

Prozess

Sie implementieren detektivische Kontrollen in zwei Phasen. Zunächst richten Sie das System so ein, dass Ereignisse und Ressourcenstatus an einem zentralen Ort wie Amazon CloudWatch Logs protokolliert werden. Nachdem die zentrale Protokollierung eingerichtet ist, analysieren Sie diese Protokolle, um Anomalien zu erkennen, die auf eine Bedrohung hinweisen könnten. Bei jeder Analyse handelt es sich um eine Kontrolle, die Ihren ursprünglichen Anforderungen und Richtlinien entspricht. Sie können beispielsweise eine detektivische Kontrolle einrichten, die die Protokolle nach einem bestimmten Muster durchsucht und bei Übereinstimmung eine Warnung generiert. Detektivische Kontrollen werden von Sicherheitsteams eingesetzt, um sich einen besseren Überblick über Bedrohungen und Risiken zu verschaffen, denen ihr System ausgesetzt sein könnte.

Anwendungsfälle

Erkennung von verdächtigem Verhalten

Detektivische Kontrollen helfen dabei, ungewöhnliche Aktivitäten zu identifizieren, wie z. B. kompromittierte privilegierte Benutzeranmeldeinformationen oder den Zugriff auf oder die Exfiltration sensibler Daten. Diese Kontrollen sind wichtige reaktive Faktoren, die Ihrem Unternehmen helfen können, den Umfang anomaler Aktivitäten zu identifizieren und zu verstehen.

Aufdeckung von Betrug

Diese Kontrollen helfen dabei, eine Bedrohung innerhalb Ihres Unternehmens zu erkennen und zu identifizieren, z. B. einen Benutzer, der Richtlinien umgeht und nicht autorisierte Transaktionen durchführt.

-Compliance

Detektivische Kontrollen unterstützen Sie bei der Einhaltung von Compliance-Anforderungen wie z. B. dem Payment Card Industry Data Security Standard (PCI DSS) und kann dazu beitragen, Identitätsdiebstahl zu verhindern. Diese Kontrollen können Ihnen helfen, vertrauliche Informationen zu entdecken und zu schützen, die der Einhaltung gesetzlicher Vorschriften unterliegen, wie z. B. personenbezogene Daten.

Automatisierte Analyse

Detektivische Kontrollen können Protokolle automatisch analysieren, um Anomalien und andere Anzeichen für unbefugte Aktivitäten zu erkennen.

Sie können Protokolle aus verschiedenen Quellen automatisch analysieren, z. B. AWS CloudTrail -Protokolle, VPC Flow Log und Domain Name System (DNS)-Protokolle, die Hinweise auf potenziell bösartige Aktivitäten enthalten. Um die Organisation zu erleichtern, können Sie Sicherheitswarnungen oder Ergebnisse von mehreren AWS-Services an einem zentralen Ort zusammenfassen.

Technologie

Ein gängiges Erkennungsinstrument ist die Implementierung eines oder mehrerer Überwachungsservices, die Datenquellen wie Protokolle analysieren können, um Sicherheitsbedrohungen zu identifizieren. In der AWS Cloud können Sie Quellen wie AWS CloudTrail

Protokolle, Amazon S3 S3-Zugriffsprotokolle und Amazon Virtual Private Cloud Cloud-Flow-Protokolle analysieren, um ungewöhnliche Aktivitäten zu erkennen. AWS Sicherheitsdienste wie Amazon GuardDuty, Amazon Detective und Amazon Macie verfügen über integrierte Überwachungsfunktionen. AWS Security Hub

GuardDuty und Security Hub

Amazon GuardDuty verwendet Bedrohungsinformationen, maschinelles Lernen und Techniken zur Erkennung von Anomalien, um Ihre Protokollquellen kontinuierlich auf böswillige oder unbefugte Aktivitäten zu überwachen. Das Dashboard bietet Einblicke in den Zustand Ihrer Workloads und Ihrer AWS-Konten Workloads in Echtzeit. Sie können einen Cloud-Dienst zur Verwaltung der Sicherheitslage integrieren GuardDuty AWS Security Hub, der die Einhaltung von Best Practices überprüft, Warnmeldungen zusammenfasst und automatische Problembehebungen ermöglicht. GuardDuty sendet Ergebnisse an Security Hub, um Informationen zu zentralisieren. Sie können Security Hub auch in SIEM-Lösungen (Security Information and Event Management) integrieren, um die Überwachungs- und Warnfunktionen für Ihre Organisation zu erweitern.

Macie

Amazon Macie ist ein vollständig verwalteter Service für Datensicherheit und Datenschutz, der Machine Learning und Musterabgleich verwendet, um Ihre sensiblen Daten in AWS zu erkennen, zu überwachen und zu schützen. Im Folgenden werden einige der in Macie verfügbaren detektivischen Kontrollen und Features aufgeführt:

- Macie inspiziert das Bucket-Inventar und alle in Amazon S3 gespeicherten Objekte. Diese Informationen können in einer einzigen Dashboard-Ansicht dargestellt werden, was für Transparenz sorgt und Sie bei der Bewertung der Bucket-Sicherheit unterstützt.
- Für die Erkennung sensibler Daten verwendet Macie integrierte, verwaltete Datenkennungen und unterstützt auch benutzerdefinierte Datenkennungen.
- Macie lässt sich nativ in andere AWS-Services AMD-Tools integrieren. Macie gibt beispielsweise Ergebnisse als EventBridge Amazon-Ereignisse aus, die automatisch an Security Hub gesendet werden.

Im Folgenden finden Sie bewährte Methoden für die Konfiguration von detektivischen Kontrollen in Macie:

- Aktivieren Sie Macie für alle Konten. Aktivieren Sie Macie mithilfe des Features zur delegierten Verwaltung für mehrere Konten, indem Sie AWS Organizations verwenden.

- Verwenden Sie Macie, um den Sicherheitsstatus der S3-Buckets in Ihren Konten zu bewerten. Dies trägt dazu bei, Datenverlust zu verhindern, indem Transparenz über den Speicherort und den Zugriff auf Daten bereitgestellt wird. Weitere Informationen finden Sie unter Analyse Ihres Amazon S3 Sicherheitsstatus (Macie-Dokumentation).
- Automatisieren Sie die Erkennung sensibler Daten in Ihren S3-Buckets, indem Sie automatisierte Verarbeitungs- und Datenerkennungsaufträge ausführen und planen. Dadurch werden S3-Buckets regelmäßig auf sensible Daten überprüft.

AWS Config

AWS Configprüft und zeichnet die Einhaltung der Vorschriften der AWS Ressourcen auf. AWS Config erkennt vorhandene AWS Ressourcen und generiert ein vollständiges Inventar zusammen mit den Konfigurationsdetails jeder Ressource. Wenn es Konfigurationsänderungen gibt, zeichnet es diese Änderungen auf und sendet eine Benachrichtigung. Dies kann Ihnen helfen, nicht autorisierte Infrastrukturänderungen zu erkennen und rückgängig zu machen. Sie können AWS verwaltete Regeln verwenden und benutzerdefinierte Regeln erstellen.

Im Folgenden finden Sie bewährte Methoden für die Konfiguration von detektivischen Kontrollen in AWS Config:

- Aktivieren Sie AWS-Region diese Option AWS Config für jedes Mitgliedskonto in der Organisation und für jedes Konto, das Ressourcen enthält, die Sie schützen möchten.
- Richten Sie Amazon Simple Notification Service (Amazon SNS)-Benachrichtigungen für alle Konfigurationsänderungen ein.
- Speichern Sie die Konfigurationsdaten in einem S3-Bucket und verwenden Sie Amazon Athena, um sie zu analysieren.
- Automatisieren Sie die Abhilfe nicht richtlinienkonformer Ressourcen mithilfe von Automation, einer Fähigkeit von AWS Systems Manager.
- Verwenden Sie EventBridge oder Amazon SNS, um Benachrichtigungen über nicht konforme AWS Ressourcen einzurichten.

Trusted Advisor

AWS Trusted Advisor kann als Service für detektivische Kontrollen genutzt werden. Trusted Advisor Identifiziert anhand einer Reihe von Prüfungen Bereiche, in denen Sie Ihre Infrastruktur optimieren, Leistung und Sicherheit verbessern oder Kosten senken können. Trusted Advisor bietet

Empfehlungen auf der Grundlage AWS bewährter Verfahren, anhand derer Sie Ihre Dienste und Ressourcen verbessern können. Business- und Enterprise Support-Pläne bieten Zugriff auf alle verfügbaren Checks für die Säulen des AWS Well-Architected Framework.

Im Folgenden finden Sie bewährte Methoden für die Konfiguration von detektivischen Kontrollen in Trusted Advisor:

- Sehen Sie sich die Zusammenfassung der Prüfungsebenen an
- Implementieren Sie ressourcenspezifische Empfehlungen für Warn- und Fehlerstatus.
- Schauen Sie Trusted Advisor regelmäßig vorbei, um die Empfehlungen aktiv zu überprüfen und umzusetzen.

Amazon Inspector

Amazon Inspector ist ein automatisierter Schwachstellen-Management-Service, der nach seiner Aktivierung Ihre Workloads kontinuierlich auf unbeabsichtigte Netzwerkfreigabe und Software-Schwachstellen durchsucht. Dabei werden die Erkenntnisse zu einer Risikobewertung zusammengefasst, anhand derer Sie die nächsten Schritte festlegen können, z. B. die Behebung oder Bestätigung des Compliance-Status.

Im Folgenden finden Sie bewährte Methoden für die Konfiguration von detektivischen Kontrollen in Amazon Inspector:

- Aktivieren Sie Amazon Inspector für alle Konten und integrieren Sie es in einen EventBridge Security Hub, um Berichte und Benachrichtigungen für Sicherheitslücken zu konfigurieren.
- Priorisieren Sie Abhilfemaßnahmen und andere Maßnahmen auf der Grundlage der Amazon Inspector-Risikobewertung.

Geschäftsergebnisse

Weniger menschlicher Aufwand und Fehler

Sie können Automatisierung erreichen, indem Sie Infrastructure as Code (IaC) verwenden. Die Automatisierung der Bereitstellung und Konfiguration von Überwachungs- und Abhilfeservices und -tools verringert das Risiko manueller Fehler und reduziert den Zeit- und Arbeitsaufwand für die Skalierung dieser detektivischen Kontrollen. Die Automatisierung hilft bei der Entwicklung von Sicherheits-Runbooks und reduziert den manuellen Aufwand für Sicherheitsanalysten. Regelmäßige

Überprüfungen helfen dabei, die Automatisierungstools zu optimieren und die Erkennungskontrollen kontinuierlich zu aktualisieren und zu verbessern.

Geeignete Maßnahmen gegen potenzielle Bedrohungen

Die Erfassung und Analyse von Ereignissen anhand von Protokollen und Metriken ist entscheidend, um Transparenz zu erlangen. Auf diese Weise können Analysten auf Sicherheitsereignisse und potenzielle Bedrohungen reagieren, um Ihre Workloads zu schützen. Da Analysten schnell erkennen können, welche Schwachstellen vorhanden sind, können sie geeignete Maßnahmen ergreifen, um diese zu beheben.

Bessere Reaktion auf Vorfälle und bessere Bearbeitung von Ermittlungen

Die Automatisierung von Tools für detektivische Kontrolle kann die Geschwindigkeit der Erkennung, Untersuchung und Wiederherstellung erhöhen. Automatisierte Warnmeldungen und Benachrichtigungen auf der Grundlage definierter Bedingungen ermöglichen es Sicherheitsanalysten, Nachforschungen anzustellen und angemessen zu reagieren. Diese Einflussfaktoren können Ihnen helfen, den Umfang anomaler Aktivitäten zu identifizieren und zu verstehen.

Reaktive Kontrollen

Reaktive Kontrollen sind Sicherheitskontrollen, die auf die Behebung von unerwünschten Ereignissen oder Abweichungen von der Sicherheitsbasis ausgerichtet sind. Beispiele für technisch reaktive Kontrollen sind das Patchen eines Systems, das Isolieren eines Virus, das Herunterfahren eines Prozesses oder das Neustarten eines Systems.

Lesen Sie die folgenden Informationen zu dieser Art von Kontrolle:

- Ziele
- Prozess
- Anwendungsfälle
- Technologie
- Geschäftsergebnisse

Ziele

- Reaktive Kontrollen können Ihnen dabei helfen, Runbooks für gängige Angriffsarten wie Phishing oder Brute-Force-Angriffe zu erstellen.

- Mit reaktiven Kontrollen können automatisierte Reaktionen auf potenzielle Sicherheitsprobleme implementiert werden.
- Responsive Controls können unbeabsichtigte oder nicht genehmigte Aktionen an AWS Ressourcen, wie z. B. das Löschen unverschlüsselter S3-Buckets, automatisch korrigieren.
- Reaktive Kontrollen können so orchestriert werden, dass sie mit präventiven und detektivischen Kontrollen zusammenarbeiten und so einen ganzheitlichen und proaktiven Ansatz für die Bewältigung potenzieller Sicherheitsvorfälle schaffen.

Prozess

Detektivische Kontrollen sind eine Grundvoraussetzung für die Einrichtung reaktiver Kontrollen. Sie müssen in der Lage sein, das Sicherheitsproblem zu erkennen, bevor Sie es beheben können. Anschließend können Sie eine Richtlinie oder eine Reaktion auf das Sicherheitsproblem festlegen. Im Falle eines Brute-Force-Angriffs würde beispielsweise ein Abhilfeprozess implementiert. Sobald der Abhilfeprozess abgeschlossen ist, kann er automatisiert und mithilfe einer Programmiersprache, z. B. eines Shell-Skripts, als Skript ausgeführt werden.

Überlegen Sie, ob die reaktive Kontrolle einen bestehenden Produktions-Workload unterbrechen könnte. Zum Beispiel, wenn die detektivische Sicherheitskontrolle S3-Buckets dürfen nicht öffentlich zugänglich sein ist und die Abhilfe öffentlichen Zugriff für Amazon S3 ausschalten ist, könnte dies erhebliche Auswirkungen auf Ihr Unternehmen und seine Kunden haben. Wenn der S3-Bucket eine öffentliche Website bedient, kann das Deaktivieren des öffentlichen Zugriffs zu einem Ausfall führen. Datenbanken sind ein ähnliches Beispiel. Wenn eine Datenbank nicht öffentlich über das Internet zugänglich sein darf, kann die Deaktivierung des öffentlichen Zugriffs die Konnektivität zur Anwendung beeinträchtigen.

Anwendungsfälle

- Automatische Reaktion auf erkannte Sicherheitsereignisse
- Automatische Behebung erkannter Sicherheits-Schwachstellen
- Automatisierte Wiederherstellungssteuerung zur Reduzierung von Betriebsausfällen

Technologie

Security Hub

AWS Security Hubsendet automatisch alle neuen Ergebnisse und alle Aktualisierungen vorhandener Ergebnisse als Ereignisse. EventBridge Sie können auch benutzerdefinierte Aktionen erstellen, an die ausgewählte Ergebnisse und Insight-Ergebnisse gesendet EventBridge werden. Sie können so konfigurieren EventBridge , dass auf jeden Ereignistyp reagiert wird. Das Ereignis kann eine AWS Lambda Funktion auslösen, die die Behebungsaktion ausführt.

AWS Config

AWS Configverwendet Regeln, um Ihre AWS Ressourcen zu bewerten, und hilft Ihnen, Ressourcen zu korrigieren, die nicht den Anforderungen entsprechen. AWS Config wendet die Problembehebung mithilfe von Automatisierung an.AWS Systems Manager In Automatisierungsdokumenten definieren Sie die Aktionen, die Sie für Ressourcen ausführen möchten, die als nicht AWS Config richtlinientreu eingestuft werden. Nachdem Sie Automatisierungsdokumente erstellt haben, können Sie sie in Systems Manager über die AWS Management Console oder mithilfe von APIs verwenden. Sie können wählen, ob Sie nicht konforme Ressourcen manuell oder automatisch korrigieren wollen.

Geschäftsergebnisse

Datenverlust minimieren

Nach einem Cybersicherheitsvorfall können reaktionsschnelle Sicherheitskontrollen dazu beitragen, Datenverluste und Schäden am System oder Netzwerk zu minimieren. Reaktionsfähige Kontrollen können auch dazu beitragen, kritische Geschäftssysteme und -prozesse so schnell wie möglich wiederherzustellen und so die Widerstandsfähigkeit Ihrer Workloads zu erhöhen.

Kosten senken

Durch die Automatisierung werden die Personalkosten gesenkt, da die Teammitglieder nicht manuell auf Vorfälle reagieren oder diese auf andere Weise auf einer bestimmten case-by-case Grundlage verwalten müssen.

Nächste Schritte

Nachdem Sie diesen Leitfaden gelesen haben, sollten Sie mit den vier Arten von Sicherheitskontrollen vertraut sein, verstehen, wie sie Teil Ihres Sicherheits-Governance-Frameworks sind, und bereit sein, mit der Implementierung und Automatisierung von Sicherheitskontrollen in der AWS Cloud zu beginnen. Zusätzlich empfehlen wir Ihnen, die Referenzen zu überprüfen, die im Abschnitt Ressourcen enthalten sind.

Wir empfehlen Ihnen außerdem, die folgenden nächsten Schritte zu unternehmen, um die Sicherheit Ihrer Cloud-Infrastruktur zu bewerten und mit der Implementierung von Sicherheitskontrollen zu beginnen:

1. Aktivieren und konfigurieren Sie AWS Security Hub. Als bewährte Methode empfehlen wir Ihnen, die verfügbaren Standardsteuerungen zu aktivieren. Weitere Informationen finden Sie unter Sicherheitsstandards und Kontrollen (Security-Hub-Dokumentation).
2. Aktivieren und konfigurieren Sie AWS Config. Weitere Informationen finden Sie unter Erste Schritte (AWS Config-Dokumentation).
3. Nutzen Sie AWS-Services wie Security Hub, Amazon Macie, AWS Config, AWS Trusted Advisor und Amazon Inspector, um Ihre Organisation und Ihre Kontoinfrastruktur zu bewerten, verbesserungsbedürftige Bereiche zu identifizieren und diese Services zu überprüfen und Empfehlungen abzugeben. Verwenden Sie das Sicherheitsprüfung-Feature in Security Hub, um eine Sicherheitsbewertung für einen Sicherheitsstandard zu generieren. Weitere Informationen finden Sie unter Determining security scores (Security-Hub-Dokumentation).
4. Implementieren Sie präventive, proaktive, detektivische und reaktive Sicherheitskontrollen auf der Grundlage der identifizierten Verbesserungen.
5. Führen Sie eine nachfolgende Sicherheitsbewertung durch, um die Wirksamkeit der implementierten Sicherheitskontrollen zu bewerten. Stellen Sie in Security Hub fest, ob sich der Sicherheitsfaktor verbessert hat. Führen Sie Iterationen durch, um die Sicherheitskontrollen zu verbessern oder neue hinzuzufügen.
6. Legen Sie einen regelmäßigen Rhythmus für die Durchführung von Sicherheitsbeurteilungen fest, z. B. jährlich.

Häufig gestellte Fragen

Worauf sollte ich mich konzentrieren, wenn ich nur begrenzte Zeit und Ressourcen habe und nicht alle diese Steuerungstypen implementieren kann?

Wir empfehlen die Implementierung von AWS Security Hub. Security Hub verfügt über eine Reihe von automatisierten Sicherheitskontrollen, die als bewährte AWS-Standardsicherheitsmethoden für grundlegende Sicherheitsprobleme bezeichnet werden (Security-Hub-Dokumentation). Dies ist eine sorgfältig zusammengestellte Sammlung von bewährten Sicherheitsmethoden, verwaltet von AWS-Sicherheitsexperten. Sie können diese Standardkontrollen entweder kontinuierlich ausführen, wenn Änderungen an den zugehörigen Ressourcen vorgenommen werden, oder in regelmäßigen Abständen. Jede Kontrolle hat einen bestimmten Schweregrad, der Ihnen hilft, Ihre Abhilfemaßnahmen zu priorisieren. Weitere Informationen finden Sie unter Durchführung von Sicherheitsüberprüfungen (Security-Hub-Dokumentation). Wenn Sie AWS Control Tower verwenden, können Sie auch die zugehörigen präventiven, detektivischen und proaktiven Kontrollen überprüfen und aktivieren.

Ressourcen

AWS-Dokumentation

- AWS-Referenzarchitektur für die Sicherheit (AWS-SRA)
- AWS-CAF-Perspektive „Sicherheit“
- Bewährte Methoden für Sicherheit, Identität und Konformität
- Automatisierte Sicherheitsreaktion in AWS (AWS-Lösung)
  - Lösungs-Landingpage
  - Implementierungsleitfaden

AWS-Blog-Posts

- Identity Guide – Präventive Kontrollen mit AWS Identity – SCPs
- Wie man eine Service-Kontrollrichtlinie (SCP) mit Lesezugriff für Konten inAWS Organizations implementiert
- Bewährte Methoden für AWS Organizations-Service-Kontrollrichtlinien in einer Umgebung mit mehreren Konten
- Sorgen Sie mithilfe der Service-Kontrollrichtlinien für die Einhaltung der Vorschriften und stellen Sie sicher, dass diese stets angewendet werden
- Wann und wo sollten IAM-Berechtigungsgrenzen verwendet werden
- Mithilfe von AWS CloudFormation-Hooks proaktiv für die Sicherheit und Konformität Ihrer Ressourcen sorgen

Sonstige Ressourcen

- Cloud Controls Matrix (CCM) (Allianz für Cloud-Sicherheit)
- Beispiele für Berechtigungsgrenzen(GitHub)

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
Proaktive Kontrollen	Wir haben diesem Leitfaden Informationen über proaktive Kontrollen hinzugefügt, einschließlich des Abschnitts Proaktive Kontrollen.	4. Dezember 2023
Erste Veröffentlichung	—	12. Dezember 2022

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 SQL Postgre-Compatible 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 (AmazonRDS) 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 Kundenbeziehungsmanagementsystem (CRM) 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 ein 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

Siehe 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 im Bereich künstliche 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 in der AWS Migrationsstrategie finden Sie im Operations Integration Guide. AIOps

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.

Atomarität, 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 ABACfür AWS in der AWS Identity and Access Management () IAM -Dokumentation.

maßgebliche 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 AWS , das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für die erfolgreiche Umstellung auf die Cloud unterstützt. AWS CAFgliedert 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 AWS CAF bietet es Anleitungen zur Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie AWS CAFauf der Website und im AWS CAFWhitepaper.

AWS Rahmen für die Qualifizierung der Arbeitslast ()AWS WQF

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQFist in AWS Schema Conversion Tool ()AWS SCT enthalten. 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 Anrufe und ähnliche Aktionen 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 Änderungsdaten (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können es CDC für verschiedene Zwecke verwenden, z. B. zur 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-Exzellenzzentrum (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 CCoEBeiträgen 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 — Tätigen Sie grundlegende Investitionen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer landing zone, Definition einerCCoE, 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 or Bitbucket Cloud. Jede Version des Codes wird als Zweig bezeichnet. 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.

Datenbank für das Konfigurationsmanagement () 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 Phase der Migration, die sich CMDB in der Phase der Portfolioerkennung und -analyse befindet.

Konformitätspaket

Eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie zusammenstellen können, um Ihre Compliance- und Sicherheitsüberprüfungen individuell anzupassen. Mithilfe einer Vorlage können Sie ein Conformance Pack als einzelne Einheit in einer AWS-Konto Region oder in einer Organisation bereitstellen. YAML 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 is commonly described as a pipeline. CI/CDkann 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 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.

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 historischer 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.

Sprache zur Datenbankmanipulation (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. DVSMerweitert 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, wie z. B. unbeabsichtigte Fehlkonfigurationen oder ein Malware-Angriff.

Disaster Recovery (DR)

Die Strategie und der Prozess, mit denen Sie Ausfallzeiten und Datenverluste aufgrund einer Katastrophe minimieren. 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 dazu, wie Sie domänengesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Modernizing legacy Microsoft. ASP NET(ASMX) schrittweise 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 der Wertströme 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 Dienst, den Sie in einer virtuellen privaten 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) Prinzipalen erstellen AWS PrivateLink und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktdienst verbinden, indem sie VPC Schnittstellenendpunkte erstellen. Weitere Informationen finden Sie unter Create an Endpoint Service in der Dokumentation zu Amazon Virtual Private Cloud (AmazonVPC).

Unternehmensressourcenplanung (ERP)

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

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 AWS CAF Sicherheitsepen 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

Weitere Informationen finden Sie unter 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. EDAwird 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

Siehe Feinkörnige 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 Regel auf hoher Ebene, die dabei hilft, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Organisationseinheiten zu regeln (). OUs Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Dienststeuerungsrichtlinien 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 in eine Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS for 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 Infrastruktur als Code.

Identitätsbasierte Richtlinie

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

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU Speicherauslastung 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.

eingehend (Eingang) VPC

In einer Architektur AWS mit mehreren Konten, VPC die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. In der AWS Sicherheitsreferenzarchitektur wird empfohlen, Ihr Netzwerkkonto mit eingehenden und ausgehenden Daten sowie Inspektionen einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne 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. Weitere Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektion VPC

In einer Architektur AWS mit mehreren Konten, eine zentrale Architektur, VPC die Inspektionen des Netzwerkverkehrs zwischen VPCs (in demselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. In der AWS Security Reference Architecture wird empfohlen, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr sowie Inspektionen einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne 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 maschinelles Lernen mit. AWS

IoT

Siehe Internet der Dinge.

IT-Informationsbibliothek (ITIL)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITILbietet die Grundlage fürITSM.

IT-Servicemanagement (ITSM)

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 Operations Integration Guide.

ITIL

Weitere Informationen finden Sie in der IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugriffskontrolle () LBAC

Eine Implementierung der obligatorischen Zugriffskontrolle (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.

LBAC

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 in der Dokumentation unter Anwenden von Berechtigungen mit den geringsten Rechten. IAM

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.

Fertigungsleitsystem () 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.

MES

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 Dienst, der über genau definierte Kanäle kommuniziert APIs 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 mithilfe von Lightweight über eine klar definierte Schnittstelle. 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. MAPumfasst 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 von Migration Factory gehören in der Regel Betriebsanalysten 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.

Bewertung des Migrationsportfolios () MPA

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPAbietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, TCO Vergleiche, Analyse der Migrationskosten) sowie Migrationsplanung (Analyse und Datenerfassung von Anwendungen, Gruppierung von Anwendungen, Priorisierung der Migration und Wellenplanung). Das MPATool (Anmeldung erforderlich) steht allen AWS Beratern und APN Partnerberatern kostenlos zur Verfügung.

Bewertung der Eignung für die Migration (MRA)

Der Prozess der Gewinnung von Erkenntnissen über den Cloud-Bereitschaftsstatus eines Unternehmens, der Identifizierung von Stärken und Schwächen und der Erstellung eines Aktionsplans zur Schließung festgestellter Lücken unter Verwendung von AWS CAF. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRAist die erste Phase der AWS Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wird, um einen Workload auf den zu migrieren AWS Cloud. 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

Siehe Origin Access Control.

OAI

Siehe Zugriffsidentität von Origin.

OCM

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 betrieblicher 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 Offene Prozesskommunikation — Einheitliche Architektur.

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 betrieblicher Ebene () OLA

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen, um eine Vereinbarung auf Serviceniveau zu unterstützen (). SLA

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 Einen Trail für eine Organisation erstellen.

Organisatorisches Änderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCMunterstützt Unternehmen bei der Vorbereitung und Umstellung auf neue Systeme und Strategien, indem es die Einführung von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework als Mitarbeiterbeschleunigung bezeichnet, da bei Projekten zur Cloud-Einführung die Geschwindigkeit des Wandels erforderlich ist. Weitere Informationen finden Sie im OCMLeitfaden.

ursprüngliche Zugriffskontrolle (OAC)

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

ursprüngliche Zugriffsidentität () OAI

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie es verwendenOAI, 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, welche eine detailliertere und erweiterte Zugriffskontrolle bietet.

ORR

Siehe Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

ausgehend (Ausgang) VPC

In einer Architektur AWS mit mehreren Konten eine, VPC die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. In der AWS Security Reference Architecture wird empfohlen, Ihr Netzwerkkonto mit eingehenden und ausgehenden Daten und Inspektionen einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

P

Berechtigungsgrenze

Eine IAM Verwaltungsrichtlinie, die den IAM Prinzipalen zugewiesen wird, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie in der IAM Dokumentation unter Grenzen von Berechtigungen.

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 hierfür PII sind Namen, Adressen und Kontaktinformationen.

PII

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 einen AWS-Konto, eine IAM Rolle oder einen Benutzer. Weitere Informationen finden Sie in der IAM Dokumentation unter Principal in Roles (Begriffe und Konzepte).

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 Anfragen für eine Domain und deren Subdomains innerhalb einer oder mehrerer VPCs Domains 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. Diese Steuerelemente scannen Ressourcen, 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, von der Konstruktion, Entwicklung und Markteinführung über Wachstum und Reife bis hin zu Verkauf und Verkauf.

Produktionsumgebung

Siehe Umgebung.

programmierbare Logiksteuerung (PLC)

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.

publish/subscribe (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem Microservice-basierten System kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen MES, 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 SQL relationalen 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

RACIMatrix

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.

RASCIMatrix

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.

Ziel des Wiederherstellungspunkts (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Damit wird festgelegt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Serviceunterbrechung gilt.

Ziel für die Wiederherstellungszeit (RTO)

Die maximal zulässige Verzögerung zwischen der Unterbrechung des Dienstes 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.

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

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 RASCIMatrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACIMatrix 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, die über definierte Zugriffsregeln verfügen. RCACbesteht 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

SAML2.0

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

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 Benutzeranmeldedaten, 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 (SIEM)

Tools und Dienste, die Systeme zur Verwaltung von Sicherheitsinformationen (SIM) und zur Verwaltung 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 EC2 Amazon-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

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

Richtlinie zur Dienststeuerung (SCP)

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

Service-Endpunkt

Der 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.

Vereinbarung zum Servicelevel () 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.

Indikator für das Serviceniveau () SLI

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

Ziel auf Serviceniveau () 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.

zentraler Fehlerpunkt (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.

SLO

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.

SPOF

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 Modernizing legacy MicrosoftASP. NET(ASMX) schrittweise Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in IhremVPC. 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 Netzwerk-Transit-Hub, über den Sie Ihre Netzwerke VPCs und Ihre lokalen Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der Dokumentation unter Was ist ein Transit-Gateway. AWS 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.

VPCPeering

Eine Verbindung zwischen zweiVPCs, die es Ihnen ermöglicht, den Verkehr mithilfe privater IP-Adressen weiterzuleiten. Weitere Informationen finden Sie in der VPC Amazon-Dokumentation unter Was ist VPC Peering.

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.

WORM

Sehen, einmal schreiben, viele lesen.

WQF

Siehe AWSWorkload-Qualifizierungsrahmen.

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 mit einer durchschnittlichen CPU Speicherauslastung von unter 5 Prozent. 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.