Zero Trust umsetzen: eine Strategie für eine sichere und agile Unternehmenstransformation

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Zero Trust umsetzen: eine Strategie für eine sichere und agile Unternehmenstransformation

Table of Contents

Einführung 1
Prozesse der Entscheidungsfindung 1
Gezielte Geschäftsergebnisse 4
Verbesserter Sicherheitsstatus 4
Reibungslose Cloud-Einführung 4
Compliance und Ausrichtung an gesetzlichen Vorschriften 4
Verbesserter Datenschutz 5
Effiziente Vorfallreaktion 5
Verbesserte Produktivität der Belegschaft 6
Ermöglichen der digitalen Transformation 6
Zusammenfassung des Abschnitts 7
Zero-Trust-Prinzipien 8
Verifizieren und authentifizieren 8
Zugriff mit geringster Berechtigung 8
Mikrosegmentierung 8
Kontinuierliche Überwachung und Analysen 9
Automatisierung und Orchestrierung 9
Autorisierung 10
Zusammenfassung des Abschnitts 10
ZTA-Schlüsselkomponenten 11
Identity and Access Management 11
Secure Access Service Edge 11
Verhinderung von Datenverlust 11
Verwaltung von Sicherheitsinformationen und Ereignissen 12
Katalog zum Eigentum an Unternehmensressourcen 12
Einheitliche Endpunktverwaltung 12
Richtlinienbasierte Durchsetzungspunkte 13
Zusammenfassung des Abschnitts 13
Organisatorische Bereitschaft 14
Ausrichtung der Führungsebene und Kommunikation 14
Kompetenzentwicklung und Schulung 15
Organisatorische Struktur und Rollen 15
IT-Infrastruktur und -Architektur 16
Risikomanagement, Governance und Änderungskontrolle 16

Überwachung und Auswertung ... 17
Zusammenfassung des Abschnitts ... 18
Zero-Trust-Mentalität ... 19
Zero Trust Aus- und Weiterbildung ... 19
Zusammenarbeit und Kommunikation ... 19
Kontinuierliches Lernen und Verbessern ... 19
Kennzahlen und Rechenschaftspflicht ... 19
Zusammenfassung des Abschnitts ... 20
Schrittweiser Ansatz ... 21
Phase 1: Bewertung und Planung ... 21
Phase 2: Pilotierung und Implementierung ... 22
Phase 3: Überwachung und kontinuierliche Verbesserung ... 23
Zusammenfassung des Abschnitts ... 23
Bewährte Methoden ... 24
Die wichtigsten Erkenntnisse ... 28
Nächste Schritte ... 30
Häufig gestellte Fragen ... 31
Was ist Zero Trust? ... 31
Welche AWS-Services können mir bei der Implementierung einer Zero-Trust-Architektur helfen? ... 31
Wie kann ich mit AWS für Datensicherheit sorgen? ... 31
Kann AWS bei den Compliance-Anforderungen in einer Zero-Trust-Umgebung helfen? ... 31
Gibt es AWS-Tools oder -Services zur Automatisierung der Sicherheit in einer Zero-Trust-Umgebung? ... 32
Wie kann ich mit AWS eine kontinuierliche Überwachung und Reaktion auf Vorfälle in einer Zero-Trust-Cloud-Umgebung sicherstellen? ... 32
Ressourcen ... 33
Referenzen ... 33
Tools ... 33
Dokumentverlauf ... 35
Glossar ... 36
... 36
A ... 37
B ... 40
C ... 42
D ... 46

E 50
F 52
G 54
H 55
I 56
L 59
M 60
O 64
P 67
Q 70
R 70
S 73
T 77
U 79
V 79
W 80
Z 81
..... lxxxii

Zero Trust umsetzen: eine Strategie für eine sichere und agile Unternehmenstransformation

Greg Gooden, Amazon Web Services (AWS)

Dezember 2023 (Dokumentverlauf)

Sicherheit hat für Unternehmen heute mehr denn je oberste Priorität. Dies ermöglicht eine Vielzahl von Vorteilen, von der Aufrechterhaltung des Vertrauens ihrer Kunden über die Verbesserung der Mobilität ihrer Mitarbeiter bis hin zur Erschließung neuer digitaler Geschäftsmöglichkeiten. Dabei stellen sie sich immer wieder eine uralte Frage: Was sind die optimalen Muster, um das richtige Maß an Sicherheit und Verfügbarkeit für meine Systeme und Daten zu gewährleisten? Die moderne Antwort auf diese Frage wird zunehmend mit dem Begriff „Zero Trust“ beschrieben.

Die Zero-Trust-Architektur (ZTA) ist ein konzeptionelles Modell und ein zugehöriger Satz von Mechanismen, die darauf ausgerichtet sind, Sicherheitskontrollen für digitale Ressourcen bereitzustellen, die nicht ausschließlich oder grundlegend von herkömmlichen Netzwerkkontrollen oder Netzwerkperimetern abhängen. Stattdessen werden Netzwerkkontrollen um Identität, Gerät, Verhalten und andere umfangreiche Kontexte und Signale erweitert, um detailliertere, intelligentere, anpassungsfähigere und kontinuierlichere Zugriffsentscheidungen zu treffen. Durch die Implementierung eines ZTA-Modells können Sie eine sinnvolle nächste Iteration der kontinuierlichen Weiterentwicklung der Cybersicherheit und insbesondere der tiefgreifenden Verteidigungskonzepte erreichen.

Prozesse der Entscheidungsfindung

Die Umsetzung einer ZTA-Strategie erfordert sorgfältige Planung und Entscheidungsfindung. Dabei müssen verschiedene Faktoren bewertet und mit den Unternehmenszielen in Einklang gebracht werden. Zu den wichtigsten Entscheidungsprozessen für den Einstieg in die ZTA gehören:

1. Einbindung von Stakeholdern. Es ist wichtig, andere CXOs, VPs und Führungskräfte einzubeziehen, um deren Prioritäten, Anliegen und Visionen für die Sicherheitslage Ihres Unternehmens zu verstehen. Indem Sie die wichtigsten Interessengruppen von Anfang an einbeziehen, können Sie die ZTA-Implementierung auf die allgemeinen strategischen Ziele abstimmen und die notwendige Unterstützung und Ressourcen gewinnen.

2. Risikobewertung. Die Durchführung einer umfassenden Risikobewertung hilft bei der Identifizierung von Problemen, übermäßiger Angriffsfläche und kritischen Vermögenswerten, was Ihnen hilft, fundierte Entscheidungen über Sicherheitskontrollen und Investitionen zu treffen. Bewerten Sie die aktuelle Sicherheitslage Ihres Unternehmens, identifizieren Sie potenzielle Schwachstellen und setzen Sie Prioritäten für Verbesserungsmaßnahmen auf der Grundlage der für Ihre Branche und Ihr Betriebsumfeld spezifischen Risikolandschaft.
3. Technologiebewertung: Die Bewertung der bestehenden Technologielandschaft des Unternehmens und die Ermittlung von Lücken hilft bei der Auswahl geeigneter Tools und Lösungen, die den ZTA-Prinzipien entsprechen. Diese Bewertung sollte eine gründliche Analyse der folgenden Punkte beinhalten:
   - Netzwerkarchitektur
   - Identitäts- und Zugriffsverwaltungssysteme
   - Authentifizierungs- und Autorisierungsmechanismen
   - Einheitliche Endpunktverwaltung
   - Tools und Prozesse für den Ressourcenbesitz
   - Verschlüsselungstechnologien
   - Überwachungs- und Protokollierungsfunktionen
   - Die Wahl des richtigen Technologie-Stacks ist entscheidend für den Aufbau eines robusten ZTA-Modells.
4. Änderungsmanagement: Es ist wichtig, die kulturellen und organisatorischen Auswirkungen der Einführung eines ZTA-Modells zu erkennen. Die Implementierung von Verfahren zum Änderungsmanagement trägt dazu bei, einen reibungslosen Übergang und die Akzeptanz im gesamten Unternehmen sicherzustellen. Dazu gehört die Aufklärung von Mitarbeitern über die Grundsätze und Vorteile von ZTA, die Schulung in den neuen Sicherheitspraktiken und die Förderung einer sicherheitsbewussten Kultur, die Verantwortlichkeit und kontinuierliches Lernen fördert.

Diese vorgeschriebene Anleitung soll CXOs, VPs und Führungskräften eine umfassende Strategie für die Implementierung von ZTA an die Hand geben. Es werden die wichtigsten Aspekte von ZTA behandelt, darunter die folgenden:

- Organisatorische Bereitschaft
- Stufenweiser Ansatz zur Einführung
- Zusammenarbeit mit Interessenvertretern

- Bewährte Methoden für eine sichere und agile Unternehmenstransformation

Wenn Sie diese Anleitung befolgen, kann sich Ihr Unternehmen in der ZTA-Landschaft zurechtfinden und erfolgreiche Ergebnisse auf Ihrem Weg zur Sicherheit in der Amazon Web Services (AWS)-Cloud erzielen. AWS bietet eine Vielzahl von Services, mit denen Sie eine ZTA implementieren können, z. B. AWS Verified Access, AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway und Amazon GuardDuty. Diese Services können helfen, AWS-Ressourcen vor unbefugtem Zugriff zu schützen.

Gezielte Geschäftsergebnisse

In diesem Abschnitt geht es um die voraussichtlichen Ergebnisse im Zusammenhang mit der Definition und Implementierung einer Zero-Trust-Architektur in Ihrer gesamten Organisation.

Verbesserter Sicherheitsstatus

Durch die Einführung der Zero-Trust-Prinzipien ist Ihre Organisation in der Lage, die Sicherheitslage zu stärken, Sicherheitsrisiken zu minimieren und Ihre Cloud-Infrastruktur und Daten zu schützen. Das Zero-Trust-Grundprinzip, den Zugriff auf der Grundlage des Need-to-know-Prinzips zu gewähren, reduziert in Verbindung mit strengen Kontrollen die Angriffsfläche erheblich und begrenzt die potenziellen Auswirkungen von Sicherheitsereignissen. Dieser proaktive Ansatz hilft Organisationen, neuen Sicherheitsrisiken immer einen Schritt voraus zu sein, und trägt dazu bei, die Vertraulichkeit, Integrität und Verfügbarkeit von Ressourcen zu gewährleisten.

Reibungslose Cloud-Einführung

Die Entwicklung eines klar definierten Einführungsplans für die Zero-Trust-Architektur (ZTA) trägt dazu bei, einen reibungslosen und erfolgreichen Übergang zur Cloud-Umgebung sicherzustellen. Die ZTA-Prinzipien orientieren sich eng an den bewährten Methoden zur Cloud-Sicherheit, da sie Organisationen eine solide Grundlage bieten, um die Vorteile von Cloud-Computing sicher zu nutzen. Die Einbeziehung der ZTA-Prinzipien von Beginn an hilft Ihrer Organisation dabei, die Cloud-Architektur so zu gestalten, dass Sicherheit ein zentrales Element ist.

Compliance und Ausrichtung an gesetzlichen Vorschriften

Die Implementierung von ZTA-Praktiken hilft Ihrer Organisation dabei, branchenspezifische und regulatorische Anforderungen und Standards einzuhalten. ZTA fördert von Natur aus das Prinzip der geringsten Berechtigung und setzt strenge Zugriffskontrollen durch. Zugriffskontrollen werden häufig durch Vorschriften wie den folgenden geregelt:

- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS).

Durch die Einführung von Zero Trust trägt Ihre Organisation dazu bei, das Engagement für Datenschutz, Privatsphäre und die Einhaltung gesetzlicher Vorschriften unter Beweis zu stellen und gleichzeitig das Risiko von Strafen oder Reputationsschäden zu minimieren.

Verbesserter Datenschutz

Organisationen können vertrauliche Daten während des gesamten Cloud-Einführungsprozesses schützen, indem sie Datenverschlüsselung, Zugriffskontrollen und regelmäßige Sicherheitsbewertungen implementieren. Ihre Organisation kann die folgenden spezifischen Schritte ergreifen:

- Datenverschlüsselung – Bei der Datenverschlüsselung werden Klartextdaten in Geheimtext verschlüsselt, wobei ein Schlüssel erforderlich ist, um die Daten wieder zu entschlüsseln und in die ursprüngliche Klartextform zu bringen. Dadurch wird es für Unbefugte erheblich schwieriger, auf sensible Daten zuzugreifen, selbst wenn sie an eine Kopie der Daten gelangen.
- Zugriffskontrollen – Zugriffskontrollen schränken ein, wer auf sensible Daten zugreifen kann und was die Person damit tun kann. Dies wird durch die Zuweisung von Benutzerrollen und Berechtigungen sowie durch die Verwendung der Multi-Faktor-Authentifizierung oder von anderen Methoden zur Überprüfung der Benutzeridentität erreicht.
- Regelmäßige Sicherheitsbewertungen – regelmäßige Sicherheitsbewertungen können Organisationen dabei unterstützen, Sicherheitsprobleme zu erkennen, anzugehen und proaktiv zu beheben. Diese Bewertungen können von internen Sicherheitsteams oder von externen Sicherheitsfirmen durchgeführt werden.

Zero-Trust-Architekturen verfolgen einen umfassenden Datenschutzansatz, indem sie eine Reihe von Sicherheitsmaßnahmen implementieren. Zu diesen Maßnahmen gehören eine starke Authentifizierung, die Datenverschlüsselung und detaillierte Zugriffskontrollen. Dieser Ansatz minimiert das Risiko datenbezogener Sicherheitsereignisse und schützt sensible Informationen vor unbefugtem Zugriff.

Effiziente Vorfallreaktion

Organisationen können Sicherheitsereignisse schneller und effektiver erkennen und darauf reagieren, indem sie Frameworks für die Überwachung und Vorfallsreaktion in der Cloud-Umgebung einrichten. In Zero-Trust-Architekturen haben die kontinuierliche Überwachung, die Integration von Bedrohungsinformationen und Echtzeiteinblicke in Benutzeraktivitäten, Netzwerkverkehr

und Systemverhalten große Bedeutung. Sicherheitsteams sind dann in der Lage, proaktiv Sicherheitsereignisse zu identifizieren und einzudämmen. Dieser Ansatz reduziert die Zeit, die für die Erkennung und Behebung potenzieller Probleme erforderlich ist, und minimiert die Auswirkungen auf den Geschäftsbetrieb. Wichtige Punkte sind u. a. folgende:

- Testen – unabhängig davon, welches Framework oder welche Methode Ihre Organisation für die Reaktion auf Vorfälle verwendet, sollten Sie Ihren Plan zur Reaktion auf Vorfälle regelmäßig testen. Theoretische Übungen, Simulationen und Red Teaming bieten die Möglichkeit, die Reaktion auf Vorfälle in realistischen Umgebungen zu üben, Tools- und Fähigkeitslücken aufzudecken und die Erfahrung und das Selbstvertrauen der an der Vorfallsreaktion Beteiligten zu stärken.
- Überwachung – überwachen Sie Ihre Cloud-Umgebungen kontinuierlich, um Anzeichen ungewöhnlicher Aktivitäten zu erkennen. Dazu steht Ihnen eine Vielzahl von Tools und Techniken zur Verfügung, z. B. Protokollanalysen, Netzwerküberwachung und Schwachstellenscans.
- Integration von Bedrohungsinformationen – integrieren Sie Bedrohungsinformationen in Ihre Frameworks für Überwachung und Vorfallreaktion. Dies hilft Ihrer Organisation, Bedrohungen schneller und effektiver zu erkennen und darauf zu reagieren.
- Transparenz in Echtzeit – um Sicherheitsvorfälle schnell zu erkennen und darauf zu reagieren, benötigt Ihre Organisation Echtzeitinformationen zu Benutzeraktivitäten, Netzwerkverkehr und Systemverhalten.
- Proaktive Identifizierung und Abwehr – durch die proaktive Identifizierung und Abwehr von Sicherheitsvorfällen kann Ihre Organisation die Zeit für die Erkennung und Abwehr potenzieller Bedrohungen reduzieren und so die Auswirkungen auf den Geschäftsbetrieb minimieren.

Verbesserte Produktivität der Belegschaft

Die Belegschaft von heute benötigt Flexibilität, um ihre Arbeit von immer mehr Standorten, Geräten und Zeiten aus erledigen zu können. Durch die Implementierung eines ZTA können Sie diese Anforderungen erfüllen und die Mobilität, Produktivität und Zufriedenheit der Mitarbeiter verbessern, während Sie gleichzeitig die Sicherheitslage der Organisation aufrechterhalten oder verbessern.

Ermöglichen der digitalen Transformation

Organisationen streben im Rahmen der digitalen Transformation zunehmend die Vernetzung von Geräten, Maschinen, Einrichtungen, Infrastrukturen und Prozessen außerhalb des traditionellen Netzwerkperimeters an. Geräte für das Internet der Dinge (IoT) und die Betriebstechnologie (OT,

auch als Industrial Internet of Things oder IIoT bezeichnet) übertragen Telemetrie- und prädiktive Wartungsinformationen häufig direkt in die Cloud. Um Workloads zu schützen, erfordert dies die Anwendung von Sicherheitskontrollen, die über den herkömmlichen Perimeteransatz hinausgehen.

Zusammenfassung des Abschnitts

Wenn Sie sich auf diese gezielten Geschäftsergebnisse konzentrieren, kann Ihre Organisation das Potenzial von ZTA voll ausschöpfen und Ihre Sicherheitslage in der Cloud stärken. Diese Ergebnisse müssen unbedingt mit spezifischen Unternehmenszielen in Einklang gebracht, auf die individuellen Geschäftsanforderungen zugeschnitten und regelmäßig auf ihre Wirksamkeit hin bewertet werden, um eine kontinuierliche Verbesserung voranzutreiben.

Grundlegendes zu Zero-Trust-Prinzipien

Die Zero-Trust-Architektur (ZTA) basiert auf einer Reihe von Kernprinzipien, die die Grundlage des Sicherheitsmodells bilden. Das Verständnis dieser Prinzipien ist für Unternehmen, die eine ZTA-Strategie effektiv umsetzen möchten, von entscheidenderBedeutung. In diesem Abschnitt werden die Kernprinzipien von ZTA behandelt.

Verifizieren und authentifizieren

Das Verifizierungs- und Authentifizierungsprinzip unterstreicht die Bedeutung einer starken Identifizierung und Authentifizierung für Prinzipale aller Typen, einschließlich Benutzern, Maschinen und Geräten. ZTA erfordert eine kontinuierliche Verifizierung der Identitäten und des Authentifizierungsstatus während einer Sitzung, idealerweise bei jeder Anfrage. Sie verlässt sich nicht nur auf herkömmliche Netzwerkstandorte oder -kontrollen. Dazu gehört die Implementierung einer modernen, starken Multi-Faktor-Authentifizierung (MFA) und die Auswertung zusätzlicher Umgebungs- und Kontextsignale während der Authentifizierungsprozesse. Durch die Einführung dieses Prinzips können Unternehmen sicherstellen, dass Entscheidungen zur Ressourcenautorisierung auf den bestmöglichen Identitätsdaten basieren.

Zugriff mit geringster Berechtigung

Das Prinzip der geringsten Berechtigung bedeutet, dass der Zugriff auf die für die Erfüllung der Aufgaben erforderlichen Ressourcen auf ein Minimum beschränkt wird. Durch die Anwendung des Prinzips der geringsten Berechtigung können Unternehmen differenzierte Zugriffskontrollen durchsetzen, sodass Prinzipale nur auf die Ressourcen zugreifen können, die sie zur Erfüllung ihrer Aufgaben und Verantwortlichkeiten benötigen. Dies beinhaltet die Implementierung von Just-in-Time-Zugriffsberechtigungen, rollenbasierten Zugriffskontrollen (RBAC) und regelmäßigen Zugriffsüberprüfungen, um die Oberfläche und das Risiko eines unbefugten Zugriffs zu minimieren.

Mikrosegmentierung

Mikrosegmentierung ist eine Netzwerksicherheitsstrategie, bei der ein Netzwerk in kleinere, isolierte Segmente unterteilt wird, um bestimmte Datenverkehrsflüsse zu autorisieren. Sie können Mikrosegmentierung erreichen, indem Sie Workload-Grenzen schaffen und strenge Zugriffskontrollen zwischen verschiedenen Segmenten durchsetzen.

Mikrosegmentierung kann durch Netzwerkvirtualisierung, softwaredefinierte Netzwerke (SDN), hostbasierte Firewalls, Netzwerk-Zugriffskontrolllisten (NACLs) und AWS-spezifische Funktionen wie Amazon Elastic Compute Cloud (Amazon EC2)-Sicherheitsgruppen oder AWS PrivateLink implementiert werden. Segmentierungs-Gateways kontrollieren den Datenverkehr zwischen Segmenten, um den Zugriff explizit zu autorisieren. Mikrosegmentierung und Segmentierungs-Gateways helfen Unternehmen, unnötige Pfade durch das Netzwerk einzuschränken, insbesondere solche, die zu kritischen Systemen und Daten führen.

Kontinuierliche Überwachung und Analysen

Kontinuierliche Überwachung und Analysen umfassen die Erfassung, Analyse und Korrelation von sicherheitsrelevanten Ereignissen und Daten in der gesamten Unternehmensumgebung. Durch die Implementierung robuster Überwachungs- und Analysetools kann Ihr Unternehmen Sicherheitsdaten und Telemetriedaten auf konvergente Weise auswerten.

Dieses Prinzip unterstreicht die Bedeutung der Einsicht in das Benutzerverhalten, den Netzwerkverkehr und die Systemaktivitäten, um Anomalien und potenzielle Sicherheitsereignisse zu erkennen. Fortschrittliche Technologien wie Verwaltung von Sicherheitsinformationen und Ereignissen (Security Information and Event Management, SIEM), Analyse des Benutzer- und Entitätsverhaltens (User and Entity Behaviour Analytics, UEBA) und Plattformen für Bedrohungsinformationen spielen eine entscheidende Rolle bei der kontinuierlichen Überwachung und proaktiven Bedrohungserkennung.

Automatisierung und Orchestrierung

Automatisierung und Orchestrierung helfen Unternehmen dabei, Sicherheitsprozesse zu rationalisieren, manuelle Eingriffe zu reduzieren und die Reaktionszeiten zu verbessern. Durch die Automatisierung von routinemäßigen Sicherheitsaufgaben und die Nutzung von Orchestrierungsfunktionen kann Ihr Unternehmen konsistente Sicherheitsrichtlinien durchsetzen und schnell auf Sicherheitsereignisse reagieren. Zu diesem Prinzip gehört auch die Automatisierung von Prozessen zur Bereitstellung und Aufhebung von Zugriffsrechten, um eine zeitnahe und genaue Verwaltung von Benutzerberechtigungen zu gewährleisten. Durch Automatisierung und Orchestrierung kann Ihr Unternehmen die betriebliche Effizienz verbessern, menschliche Fehler reduzieren und Ressourcen auf strategischere Sicherheitsinitiativen konzentrieren.

Autorisierung

In einer ZTA sollte jede Anfrage für den Zugriff auf eine Ressource ausdrücklich durch einen Gating-Durchsetzungspunkt genehmigt werden. Neben der authentifizierten Identität sollten die Autorisierungsrichtlinien zusätzlichen Kontext berücksichtigen, z. B. Zustand und Status des Geräts, Verhaltensmuster, Ressourcenklassifizierung und Netzwerkfaktoren. Der Autorisierungsprozess sollte diesen konvergierten Kontext anhand der entsprechenden Zugriffsrichtlinien bewerten, die für die Ressource, auf die zugegriffen wird, relevant sind. Optimalerweise können Machine-Learning-Modelle eine dynamische Ergänzung zu den deklarativen Richtlinien darstellen. Wenn diese Modelle eingesetzt werden, sollten sie sich nur auf zusätzliche Einschränkungen konzentrieren und keinen Zugriff gewähren, der nicht explizit festgelegt wurde.

Zusammenfassung des Abschnitts

Durch die Einhaltung dieser Kernprinzipien der ZTA können Unternehmen ein robustes Sicherheitsmodell aufbauen, das der Vielfalt der modernen Unternehmensumgebung gerecht wird. Die Umsetzung dieser Prinzipien erfordert einen umfassenden Ansatz, der Technologie, Prozesse und Menschen kombiniert, um eine Zero-Trust-Mentalität zu erreichen und eine robuste Sicherheitslage zu schaffen.

Schlüsselkomponenten einer Zero-Trust-Architektur

Zur effektiven Umsetzung einer Zero-Trust-Architektur (ZTA)-Strategie muss Ihr Unternehmen die Schlüsselkomponenten verstehen, aus denen eine ZTA besteht. Diese Komponenten arbeiten zusammen, um ein umfassendes Sicherheitsmodell, das den Zero-Trust-Prinzipien entspricht, kontinuierlich zu verbessern. In diesem Abschnitt werden diese Schlüsselkomponenten einer ZTA behandelt.

Identity and Access Management

Identitäts- und Zugriffsverwaltung bildet die Grundlage einer ZTA, indem sie eine zuverlässige Benutzerauthentifizierung und grobe Zugriffskontrollmechanismen bietet. Es umfasst Technologien wie Single Sign-On (SSO), Multi-Faktor-Authentifizierung (MFA) sowie Lösungen für Governance und Verwaltung von Identitäten. Identitäts- und Zugriffsmanagement bietet ein hohes Maß an Authentifizierungssicherheit und wichtige Rahmenbedingungen, die für Zero-Trust-Autorisierungsentscheidungen unerlässlich sind. Gleichzeitig handelt es sich bei ZTA um ein Sicherheitsmodell, bei dem der Zugriff auf Anwendungen und Ressourcen pro Benutzer, pro Gerät und pro Sitzung gewährt wird. Dies trägt dazu bei, Unternehmen vor unbefugtem Zugriff zu schützen, selbst wenn die Anmeldeinformationen eines Benutzers kompromittiert werden.

Secure Access Service Edge

Secure Access Service Edge (SASE) ist ein neuer Ansatz für die Netzwerksicherheit, bei dem Netzwerk- und Sicherheitsfunktionen in einem einzigen, cloudbasierten Dienst virtualisiert, kombiniert und verteilt werden. SASE bietet sicheren Zugriff auf Anwendungen und Ressourcen, unabhängig vom Standort des Benutzers.

SASE umfasst eine Vielzahl von Sicherheitsfeatures, wie z. B. sichere Web-Gateways, Firewall-as-a-Service und Zero Trust Network Access (ZTNA). Diese Features wirken zusammen, um Unternehmen vor einer Vielzahl von Bedrohungen zu schützen, darunter Malware, Phishing und Ransomware.

Verhinderung von Datenverlust

Technologien zur Verhinderung von Datenverlust (Data Loss Prevention, DLP) können Unternehmen dabei helfen, sensible Daten vor unbefugter Offenlegung zu schützen. DLP-Lösungen überwachen

und kontrollieren Daten in Bewegung und im Ruhezustand. Dies hilft Unternehmen bei der Definition und Durchsetzung von Richtlinien, die datenbezogene Sicherheitsereignisse verhindern, und trägt dazu bei, dass sensible Informationen im gesamten Netzwerk geschützt bleiben.

Verwaltung von Sicherheitsinformationen und Ereignissen

Lösungen für die Verwaltung von Sicherheitsinformationen und Ereignissen (Security Information and Event Management, SIEM) sammeln, aggregieren und analysieren Sicherheitsereignisprotokolle aus verschiedenen Quellen in der gesamten Infrastruktur eines Unternehmens. Sie können diese Daten nutzen, um Sicherheitsvorfälle zu erkennen, die Reaktion auf Vorfälle zu erleichtern und Einblicke in potenzielle Bedrohungen und Schwachstellen zu erhalten.

Speziell für ZTA ist die Fähigkeit einer SIEM-Lösung, zusammenhängende Telemetriedaten von verschiedenen Sicherheitssystemen zu korrelieren und zu verstehen, entscheidend für eine verbesserte Erkennung von und Reaktion auf anormale Muster.

Katalog zum Eigentum an Unternehmensressourcen

Um den Zugriff auf Unternehmensressourcen ordnungsgemäß gewähren zu können, muss ein Unternehmen über ein zuverlässiges System verfügen, das diese Ressourcen katalogisiert und vor allem festhält, wem sie gehören. Diese Informationsquelle muss Workflows bereitstellen, die Zugriffsanfragen, die damit verbundenen Genehmigungsentscheidungen und deren regelmäßige Bestätigungen erleichtern. Mit der Zeit wird diese Informationsquelle die Antworten auf die Frage „Wer darf auf was zugreifen?“ innerhalb der Organisation enthalten. Sie können die Antworten sowohl für die Autorisierung als auch für die Prüfung und Einhaltung von Vorschriften nutzen.

Einheitliche Endpunktverwaltung

Neben der strengen Authentifizierung des Benutzers muss eine ZTA auch den Zustand des Geräts des Benutzers berücksichtigen, um zu bewerten, ob der Zugriff auf Unternehmensdaten und -ressourcen sicher ist. Eine Plattform für einheitliche Endpunktverwaltung (Unified Endpoint Management, UEM) bietet die folgenden Funktionen:

- Gerätebereitstellung
- Kontinuierliche Konfiguration und Patchverwaltung
- Sicherheits-Baselining

- Telemetrieberichte
- Bereinigung und Außerbetriebnahme von Geräten

Richtlinienbasierte Durchsetzungspunkte

In einer ZTA sollte der Zugriff auf jede Ressource ausdrücklich durch einen richtlinienbasierten Durchsetzungspunkt genehmigt werden. Anfangs können diese Durchsetzungspunkte auf bestehenden Durchsetzungspunkten in bestehenden Netzwerk- und Identitätssystemen basieren. Die Durchsetzungspunkte können schrittweise leistungsfähiger gemacht werden, indem das breitere Spektrum an Kontext und Signalen berücksichtigt wird, das die ZTA bietet. Längerfristig sollte Ihr Unternehmen ZTA-spezifische Durchsetzungspunkte implementieren, die mit konvergentem Kontext arbeiten, Signalanbieter konsistent integrieren, einen umfassenden Richtliniensatz beibehalten und mit Informationen aus kombinierten Telemetriedaten erweitert werden.

Zusammenfassung des Abschnitts

Das Verständnis dieser Schlüsselkomponenten ist für Organisationen, die die Einführung einer ZTA planen, von entscheidender Bedeutung. Durch die Implementierung dieser Komponenten und deren Integration in ein kohärentes Sicherheitsmodell kann Ihre Organisation ein starkes Sicherheitsniveau aufbauen, das auf den Prinzipien von Zero Trust basiert. Die folgenden Abschnitte befassen sich mit den organisatorischen Voraussetzungen, den Ansätzen für eine schrittweise Einführung und bewährten Methoden, die Sie bei der erfolgreichen Implementierung von ZTA in Ihrer Organisation unterstützen.

Bewertung der organisatorischen Bereitschaft zur Einführung von Zero Trust

Die Einführung einer neuen Architekturstrategie ist ein bedeutendes Unterfangen, das eine sorgfältige Planung und die Berücksichtigung von organisatorischen Faktoren erfordert. Dieser Abschnitt befasst sich mit den wichtigsten Überlegungen zur organisatorischen Bereitschaft für die Einführung von Zero Trust in Ihrem Unternehmen. Wenn Sie diese Überlegungen berücksichtigen, kann Ihr Unternehmen den Weg für eine stärkere und erfolgreichere Sicherheitslage ebnen.

Ausrichtung der Führungsebene und Kommunikation

Die Ausrichtung der Führungsebene und die Kommunikation sind für die erfolgreiche Umsetzung von Zero Trust unerlässlich. Die Führungsebene muss die Vorteile von Zero Trust und die erforderlichen Ressourcen verstehen. Führungskräfte müssen auch bereit sein, Änderungen an der Unternehmenskultur und den Prozessen vorzunehmen. Die Kommunikation mit den Mitarbeitern ist notwendig, um Vertrauen und Akzeptanz aufzubauen. Mitarbeiter müssen verstehen, warum das Unternehmen Zero Trust einführt, was es für sie bedeutet und wie sie dazu beitragen können. Die Kommunikation sollte offen, transparent und fortlaufend sein.

Unterstützung und Akzeptanz durch die Führungsebene

Für eine erfolgreiche Implementierung der Zero-Trust-Architektur (ZTA) ist es von entscheidender Bedeutung, wichtige Stakeholder und Führungskräfte über die Ziele, Vorteile und Erfolgskriterien der Architektur aufzuklären. Vermitteln Sie die Bedeutung der Zero-Trust-Prinzipien für die Verbesserung der Sicherheit und der geschäftlichen Flexibilität, indem Sie von der traditionellen perimeterbasierten Sicherheit zu einem detaillierteren, benutzerzentrierten Ansatz übergehen. Durch die Umstellung auf diesen Ansatz kann sich Ihr Unternehmen schneller an Veränderungen und Bedrohungen anpassen. Die Zustimmung der Führungskräfte gibt den Ton für das Unternehmen vor und hilft, mögliche Widerstände gegen Veränderungen zu überwinden.

Transparente Kommunikation

Pflegen Sie während des gesamten Prozesses der Zero-Trust-Einführung eine offene und transparente Kommunikation mit den Mitarbeitern. Erläutern Sie die Gründe, Vorteile und erwarteten Ergebnisse der Einführung und gehen Sie auf Bedenken umgehend ein. Informieren Sie sich regelmäßig über den Stand der Implementierung. Dadurch wird die Akzeptanz erhöht, Widerstand abgebaut und Vertrauen aufgebaut.

Kompetenzentwicklung und Schulung

Nachdem die Führungsebene abgestimmt und die Kommunikation offen ist, ist es wichtig, die Fähigkeiten und das Wissen der Mitarbeiter, die Zero Trust umsetzen sollen, zu entwickeln. Dazu gehört, dass sie die Zero-Trust-Prinzipien verstehen und wissen, wie sie sie bei ihrer Arbeit umsetzen und wie sie auf Sicherheitsvorfälle reagieren können. Bieten Sie Schulungs- und Entwicklungsmöglichkeiten an, damit die Mitarbeiter diese Fähigkeiten erwerben können.

Cloudwissen und -kompetenzen

Bewerten Sie die Kompetenzen und Wissenslücken des Unternehmens in Bezug auf Cloudtechnologien und Zero-Trust-Prinzipien. Bieten Sie Schulungs- und Entwicklungsprogramme an, um Mitarbeiter weiterzubilden und sie mit dem nötigen Fachwissen auszustatten, damit sie in einer cloudorientierten Zero-Trust-Umgebung effektiv arbeiten können. Fördern Sie eine Kultur des kontinuierlichen Lernens, um mit den sich weiterentwickelnden Technologien und Sicherheitspraktiken Schritt zu halten.

Sicherheitskultur und -bewusstsein

Bewerten Sie die Sicherheitskultur des Unternehmens. Beurteilen Sie den Grad des Sicherheitsbewusstseins der Mitarbeiter, ihr Verständnis für bewährte Sicherheitspraktiken und ihre Einhaltung von Richtlinien und Verfahren. Ermitteln Sie etwaige Lücken im Sicherheitswissen. Erwägen Sie die Durchführung von Schulungsprogrammen zum Sicherheitsbewusstsein, um die Mitarbeiter über die Bedeutung von Zero Trust und ihre Rolle bei der Aufrechterhaltung einer sicheren Umgebung zu informieren.

Organisatorische Struktur und Rollen

Um Zero Trust erfolgreich umzusetzen, müssen Sie eine effektive Organisationsstruktur und Rollenverteilung einrichten. Dazu gehören die Einrichtung eines Cloud-Kompetenzzentrums (CCoE), die Überprüfung und Anpassung der Sicherheitsabläufe sowie die Zuweisung von Rollen und Verantwortlichkeiten für das Schwachstellenmanagement, die Reaktion auf Vorfälle und die Sicherheitsüberwachung.

Cloud-Kompetenzzentrum

Richten Sie ein CCoE ein, um Leitfäden, bewährte Methoden und die Aufsicht über den Cloudbetrieb zu gewährleisten. Ein CCoE ist ein Team oder eine Gruppe von Personen, die für die Erstellung und Umsetzung von bewährten Methoden, Leitlinien und Governance-Richtlinien für die Cloud

verantwortlich sind. Dem CCoE sollten Vertreter aus verschiedenen Geschäftsbereichen und IT-Teams angehören, um die Zusammenarbeit und Abstimmung zu gewährleisten. Das CCoE spielt eine entscheidende Rolle bei der Einführung von Zero-Trust-Prinzipien für in der Cloud gehostete Workloads. Das CCoE erleichtert auch den Wissensaustausch innerhalb des Unternehmens.

Sicherheitsvorgänge

Um den Anforderungen einer Zero-Trust-Umgebung gerecht zu werden, muss die aktuelle Organisation der Sicherheitsvorgänge überprüft und angepasst werden. Um die Überwachung, die Reaktion auf Vorfälle und die Fähigkeiten zur Bedrohungsanalyse zu verbessern, sollten Sie die Implementierung von Security Operations Centern (SOCs) oder Managed Security Service Providern (MSSPs) in Betracht ziehen. Legen Sie Rollen und Verantwortlichkeiten für das Schwachstellenmanagement, die Reaktion auf Vorfälle und die Sicherheitsüberwachung fest. Ein gut funktionierender Prozess zur Reaktion auf Vorfälle ist entscheidend dafür, dass kleinere Sicherheitsvorfälle schnell erkannt und behoben werden können, um die Abfolge der Ereignisse zu unterbrechen. Auf diese Weise wird verhindert, dass aus einem geringfügigen Ereignis ein schwerwiegenderes Ereignis wird.

IT-Infrastruktur und -Architektur

Untersuchen Sie die IT-Architektur und -Infrastruktur Ihres Unternehmens auf Einschränkungen oder Abhängigkeiten, die die Einführung eines Zero-Trust-Ansatzes beeinträchtigen könnten. Stellen Sie fest, ob die derzeitigen Anwendungen und Systeme mit den erforderlichen Komponenten der Zero-Trust-Architektur kompatibel sind. Analysieren Sie, ob Verbesserungen oder Anpassungen der Infrastruktur erforderlich sind, um die erfolgreiche Bereitstellung von Zero-Trust-Prinzipien zu unterstützen. Überlegen Sie für jede Anwendung bzw. jedes System, ob Zero Trust am besten direkt oder im Rahmen eines größeren Modernisierungsprojekts implementiert wird.

Risikomanagement, Governance und Änderungskontrolle

Um Zero Trust erfolgreich zu implementieren, müssen Sie wirksame Prozesse für Risikomanagement, Governance und Änderungskontrolle einrichten. Dazu gehören die Abstimmung des Risikomanagements auf die Zero-Trust-Prinzipien, die Entwicklung eines Plans zur Reaktion auf Vorfälle, die Zusammenarbeit mit den Rechts- und Compliance-Abteilungen und die Einrichtung eines Prozesses zur Änderungskontrolle.

Risikomanagement

Untersuchen Sie die in Ihrem Unternehmen geltende Risikomanagementstrategie und stellen Sie fest, inwieweit sie den Zero-Trust-Prinzipien entspricht. Analysieren Sie die Effizienz der derzeitigen Systeme zur Reaktion auf Vorfälle, Sicherheitsmaßnahmen und Risikobewertungsverfahren. Stellen Sie fest, welche Bereiche verbessert werden müssen, um der Zero-Trust-Strategie zu entsprechen. Beginnen Sie mit der Entwicklung eines automatisierten Systems zur Reaktion auf Vorfälle oder eines Frameworks für kontinuierliche Überwachung und Analyse, um die Lösungsgeschwindigkeit zu erhöhen.

Prozesse zur Änderungskontrolle

Um sicherzustellen, dass alle cloudbezogenen Änderungen den Sicherheits- und Compliance-Anforderungen entsprechen, sollten Sie effektive Änderungskontrollverfahren einführen. Führen Sie ein systematisches Änderungsmanagementverfahren ein, das eine Analyse der Sicherheitskonfiguration, Risikobewertungen, Genehmigungen und Dokumentation umfasst. Überprüfen Sie Aktualisierungen häufig, um die Integrität der Zero-Trust-Architektur zu wahren.

Überwachung und Auswertung

Um Zero Trust erfolgreich umzusetzen, muss Ihr Unternehmen seine Sicherheitslage kontinuierlich überwachen und auswerten. Dazu gehören die Festlegung von Leistungskennzahlen (Key Performance Indicators, KPIs), die Überwachung und Bewertung der KPIs sowie die Förderung einer Kultur der kontinuierlichen Verbesserung. Durch die Befolgung dieser Schritte können Unternehmen sicherstellen, dass ihre Zero-Trust-Implementierung erfolgreich ist und dass sie stets an der Verbesserung ihrer Sicherheit arbeiten.

Leistungskennzahlen

Legen Sie einschlägige Leistungskennzahlen (Key Performance Indicators, KPIs) fest, um den Erfolg und die Wirksamkeit der Zero-Trust-Implementierung zu messen. Diese KPIs können die Zufriedenheit der Benutzer, den Fortschritt bei der Ausrüstung und der Einführung, die Kostenreduzierung, die Einhaltung von Vorschriften und die Anzahl der Sicherheitsvorfälle messen. Um die Gesamtentwicklung zu verfolgen und Verbesserungsmöglichkeiten zu finden, sollten Sie diese KPIs regelmäßig überwachen und auswerten.

Kontinuierliche Verbesserung

Die Einrichtung von Systemen zur Einholung von Meinungen und Erkenntnissen der Beteiligten trägt dazu bei, eine Kultur der kontinuierlichen Verbesserung zu fördern. Ermutigen Sie die Mitarbeiter,

Gedanken und Vorschläge zur Verbesserung der Sicherheit, Effektivität und Benutzerfreundlichkeit der Cloudumgebung einzubringen. Nutzen Sie diesen Input, um Verfahren zu rationalisieren, Sicherheitsmaßnahmen zu verbessern und Innovationen anzustoßen.

Zusammenfassung des Abschnitts

Durch die Berücksichtigung dieser organisatorischen und kulturellen Überlegungen kann Ihr Unternehmen ein günstiges Umfeld für die Einführung eines Zero-Trust-Sicherheitsmodells in der Cloud schaffen. Der nächste Abschnitt befasst sich mit der schrittweisen Einführung von Zero-Trust-Prinzipien und bietet Anleitungen zur praktischen und überschaubaren Umsetzung.

Kultivierung einer Zero-Trust-Mentalität

Die Implementierung von Zero Trust geht über technische Implementierungen hinaus. Es erfordert einen kulturellen Wandel innerhalb Ihrer Organisation. Zur Förderung einer Zero-Trust-Mentalität müssen die folgenden Schlüsselaspekte betont werden.

Zero Trust Aus- und Weiterbildung

Informieren Sie Ihre Mitarbeiter über die Werte und Vorteile der Zero-Trust-Architektur (ZTA). Bieten Sie technische und nichttechnische Erklärungen zu ZTA-Konzepten und -Ansätzen im Rahmen von Schulungen, Workshops und anderen Ressourcen an. Ermutigen Sie die Mitarbeiter, sich ihrer Verantwortung bei der Einführung und Aufrechterhaltung eines Zero-Trust-Sicherheitsparadigmas bewusst zu sein.

Zusammenarbeit und Kommunikation

Fördern Sie die Zusammenarbeit und Transparenz zwischen allen Teams und Abteilungen, die an der ZTA-Implementierung beteiligt sind. Um sicherzustellen, dass alle ein gründliches Verständnis des Plans haben, fördern Sie die funktionsübergreifende Kommunikation, den Wissensaustausch und den Informationsaustausch. Schaffen Sie eine Kultur der gemeinsamen Verantwortung, in der jeder die Bedeutung seines Beitrags zur allgemeinen Sicherheit des Unternehmens anerkennt.

Kontinuierliches Lernen und Verbessern

Priorisieren Sie kontinuierliches Lernen und Verbessern im Kontext von Zero Trust. Ermutigen Sie die Mitarbeiter, über die neuesten Sicherheitstrends, Technologien und Best Practices auf dem Laufenden zu bleiben. Pflegen Sie eine Kultur der Innovation und des Experimentierens, in der die Mitarbeiter ermutigt werden, neue Lösungen und Ansätze zu erkunden, um die Sicherheitslage des Unternehmens zu stärken.

Kennzahlen und Rechenschaftspflicht

Richten Sie klare Kennzahlen und Rechenschaftsmechanismen ein, um die Effektivität der Zero-Trust-Strategie zu messen. Definieren Sie wichtige Leistungsindikatoren (KPIs), die mit den Sicherheitszielen des Unternehmens übereinstimmen, und verfolgen Sie regelmäßig die Fortschritte.

Machen Sie Einzelpersonen und Teams für ihren Beitrag zur Umsetzung und Aufrechterhaltung der Zero-Trust-Prinzipien zur Rechenschaft.

Zusammenfassung des Abschnitts

Durch die Berücksichtigung dieser Aspekte und die Pflege einer Zero-Trust-Mentalität können Unternehmen eine solide Grundlage für eine erfolgreiche Einführung und Implementierung von Zero Trust schaffen. Dieser kulturelle Wandel ist unerlässlich, um allen Mitarbeitern des Unternehmens zu helfen, die Bedeutung von Zero Trust zu verstehen und aktiv zu seinem Erfolg beizutragen.

Im nächsten Abschnitt werden Ansätze zur schrittweisen Einführung untersucht und Hinweise zur schrittweisen Umsetzung der Zero-Trust-Prinzipien auf praktische und überschaubare Weise gegeben.

Schrittweiser Ansatz für Zero Trust

Die Einführung einer Zero-Trust-Architektur (ZTA) erfordert eine sorgfältige Planung und Implementierung. Wir empfehlen eine schrittweise Einführung, um einen reibungslosen Übergang zu gewährleisten und Störungen des Geschäftsbetriebs zu minimieren. Dieser Abschnitt enthält Hinweise zu den wichtigsten Phasen bei der Einführung einer ZTA.

Phase 1: Bewertung und Planung

Die erste Phase der Zero-Trust-Implementierung ist die Bewertung und Planung. Diese Phase ist entscheidend für den Erfolg der gesamten Implementierung, da sie die Identifizierung und Beseitigung von Lücken in der aktuellen Sicherheitslage Ihres Unternehmens beinhaltet. Indem Sie sich die Zeit nehmen, Ihren aktuellen Zustand zu bewerten und Ihre Sicherheitsziele zu definieren, können Sie den Grundstein für eine erfolgreiche Zero Trust-Implementierung legen.

Gleichzeitig ist eine vollkommen vollständige und genaue Bewertung nicht immer realistisch. Um eine Lähmung der Analyse zu vermeiden, die Sie daran hindert, zu weiteren Phasen überzugehen, sollten Sie bereit sein, zu segmentieren oder ein gewisses Maß an Unvollkommenheit in Kauf zu nehmen.

1. Bewertung des aktuellen Zustands: Führen Sie eine Bewertung Ihrer bestehenden Sicherheitsinfrastruktur, Richtlinien und Kontrollen durch. Identifizieren Sie potenzielle Schwachstellen, Sicherheitslücken und Bereiche, in denen die Umsetzung der Zero-Trust-Prinzipien Verbesserungen bringen kann.
2. Definition von Sicherheitszielen: Definieren Sie auf der Grundlage der Erkenntnisse der Bewertung des aktuellen Zustands Sicherheitsziele, die mit den Prinzipien von Zero Trust übereinstimmen. Diese Sicherheitsziele sollten auch mit der allgemeinen Sicherheitsstrategie Ihres Unternehmens übereinstimmen und identifizierte Schwachstellen und Lücken beheben.
3. Entwerfen der Architektur: Entwickeln Sie eine ZTA, die die Sicherheitsziele Ihres Unternehmens unterstützt. Diese Architektur sollte die notwendigen Komponenten wie Identitäts- und Zugriffsverwaltungslösungen, Netzwerksegmentierungsmechanismen und kontinuierliche Überwachungssysteme umfassen. Die Architektur sollte außerdem skalierbar und anpassungsfähig sein und künftiges Wachstum und technologische Fortschritte berücksichtigen können. Idealerweise sollte diese Architektur in einem Format dargestellt werden, das von den Teams, die für die Implementierung verantwortlich sind, leicht genutzt werden kann, wie z. B. eine AWS CloudFormation-Vorlage, und nicht nur als Dokument oder Diagramm.

4. Einbindung von Stakeholdern: Beziehen Sie alle Stakeholder ein, einschließlich der Geschäftsbereiche, IT-Teams und Sicherheitsteams, um Erkenntnisse zu gewinnen und ihre Ziele mit dem ZTA-Implementierungsplan abzustimmen. Fördern Sie die Zusammenarbeit und Kommunikation, um ein gemeinsames Verständnis für die Vorteile und Anforderungen des Zero-Trust-Ansatzes zu schaffen.

Phase 2: Pilotierung und Implementierung

Die zweite Phase der Implementierung von Zero Trust besteht aus der Pilotierung und Implementierung. In dieser Phase wird die ZTA in einer kleinen, kontrollierten Umgebung getestet und dann schrittweise in Ihrem gesamten Unternehmen eingeführt. Es ist wichtig, die Mitarbeiter über die neuen Sicherheitsmaßnahmen und ihre Rolle bei der Aufrechterhaltung einer Zero-Trust-Umgebung zu informieren.

1. Pilotieren der Bereitstellung: Testen Sie die ZTA in einer kleinen, kontrollierten Umgebung. Implementieren Sie die notwendigen Komponenten und Sicherheitskontrollen, die in der Architekturentwurfsphase definiert wurden. Überwachen Sie die Pilotbereitstellung genau, sammeln Sie Feedback und nehmen Sie gegebenenfalls Anpassungen vor. Seien Sie darauf vorbereitet, zu Beginn des Prozesses flexibel zu sein, wenn Zero Trust von einer hypothetischen Übung zu einem Projekt wird, mit dem Sie echte Erfahrungen sammeln.
2. Iterative Bereitstellung: Beginnen Sie auf der Grundlage der Erfahrungen aus dem Pilotprojekt mit der iterativen Bereitstellung von Zero Trust im gesamten Unternehmen. Bauen Sie eine Dynamik durch einen Schwungradeffekt auf, der keine umfangreiche Kampagne erfordert, um eine kritische Bereitstellungsmasse zu erreichen. Heben Sie sich Führungsaufträge oder Eskalationen für den weiteren Verlauf der Einführung auf, wo sie erforderlich sein könnten.
3. Bereitstellung von Benutzerschulungen und Sensibilisierung: Informieren Sie Ihre Mitarbeiter über die neuen Sicherheitsmaßnahmen und ihre Rolle bei der Aufrechterhaltung einer Zero-Trust-Umgebung. Betonen Sie die Bedeutung sicherer Praktiken, wie z. B. sichere Passwörter, Multi-Faktor-Authentifizierung und regelmäßige Sicherheitsupdates.
4. Änderungsmanagement: Erstellen Sie einen umfassenden Plan für das Änderungsmanagement, um die organisatorischen und kulturellen Veränderungen zu bewältigen, die mit der Einführung von Zero Trust einhergehen. Vermitteln Sie den Mitarbeitern die Vorteile und Gründe für die Einführung und gehen Sie auf Bedenken und Widerstände ein. Bieten Sie fortlaufend Unterstützung und Beratung, um einen reibungslosen Übergang zu ermöglichen.

Phase 3: Überwachung und kontinuierliche Verbesserung

Die dritte und letzte Phase der Zero-Trust-Implementierung ist die Überwachung und kontinuierliche Verbesserung. In dieser Phase geht es darum, ein umfassendes Überwachungs- und Analyseprogramm einzurichten, einen umfassenden Plan zur Reaktion auf Vorfälle zu erstellen und regelmäßig Feedback von Interessengruppen und Benutzern einzuholen.

1. Kontinuierliche Überwachung: Richten Sie ein umfassendes Überwachungs- und Analyseprogramm ein, um die Sicherheitslage kontinuierlich zu bewerten und mögliche Anomalien zu erkennen. Verwenden Sie fortschrittliche Sicherheitstools und -technologien, um das Benutzerverhalten, den Netzwerkverkehr und die Systemaktivitäten zu überwachen.
2. Planen der Reaktion auf Vorfälle und deren Behebung: Erstellen Sie einen umfassenden Plan für die Reaktion auf Vorfälle, der sich an den Zero-Trust-Prinzipien orientiert. Legen Sie klare Eskalationspfade fest, definieren Sie Rollen und Verantwortlichkeiten und implementieren Sie nach Möglichkeit automatisierte Mechanismen zur Reaktion auf Vorfälle. Testen und aktualisieren Sie den Plan zur Reaktion auf Vorfälle regelmäßig.
3. Einholen von Feedback und Auswertung:: Holen Sie regelmäßig Feedback von Interessengruppen und Benutzern ein, um Erkenntnisse über die Effektivität der Zero-Trust-Architektur (ZTA) zu gewinnen. Führen Sie regelmäßige Aus- und Bewertungen durch, um die Auswirkungen auf die Sicherheitslage, die betriebliche Effizienz und die Benutzererfahrung zu messen. Nutzen Sie das Feedback und die Bewertungsergebnisse, um Verbesserungsmöglichkeiten zu identifizieren. Rechnen Sie damit, dass sich Ihre ZTAs im Laufe der Zeit ändern werden, und überlegen Sie, wie die Entwicklungsteams diese Aktualisierungen mit minimalem Aufwand oder Unterbrechungen implementieren können.

Zusammenfassung des Abschnitts

Wenn Sie diesen Ansatz der schrittweisen Einführung verfolgen, können Unternehmen effektiv zu einer ZTA übergehen und dabei Risiken und Unterbrechungen minimieren. Im nächsten Abschnitt werden bewährte Methoden für eine erfolgreiche Zero-Trust-Implementierung erörtert, wobei die wichtigsten Überlegungen und Empfehlungen für CxOs, VPs und leitende Angestellte behandelt werden.

Bewährte Methoden für den Erfolg mit Zero Trust

Die erfolgreiche Einführung der Zero-Trust-Architektur (ZTA) erfordert einen strategischen Ansatz und die Einhaltung bewährter Methoden. In diesem Abschnitt werden eine Reihe von bewährten Methoden vorgestellt, die CXOs, VPs und Führungskräfte dabei unterstützen sollen, ihre Zero-Trust-Einführung erfolgreich zu gestalten. Wenn Sie diesen Empfehlungen folgen, kann Ihre Organisation ein solides Sicherheitsfundament schaffen und die Vorteile eines Zero-Trust-Ansatzes nutzen:

- Klare Definition von Zielen – definieren Sie klar die Ziele und gewünschten Geschäftsergebnisse des Cloud-Betriebs. Richten Sie diese Ziele an den Prinzipien von Zero Trust aus, um eine solide Sicherheitsgrundlage zu schaffen und gleichzeitig Unternehmenswachstum und Innovation zu ermöglichen.
- Durchführung einer umfassenden Bewertung – führen Sie eine umfassende Bewertung der aktuellen IT-Infrastruktur, der Anwendungen und der Datenbestände durch. Identifizieren Sie Abhängigkeiten, technische Probleme und mögliche Kompatibilitätsprobleme. Diese Bewertung dient als Grundlage für den Einführungsplan und hilft bei der Priorisierung von Workloads auf der Grundlage von Kritikalität, Komplexität und geschäftlichen Auswirkungen.
- Entwickeln eines Einführungsplans – binden Sie einen detaillierten Einführungsplan ein, der das schrittweise Vorgehen für die Migration von Workloads, Anwendungen und Daten in die Cloud skizziert. Definieren Sie Einführungsphasen, Zeitpläne und Abhängigkeiten. Binden Sie wichtige Stakeholder ein und weisen Sie Ressourcen entsprechend zu.
- Entwicklung von Anfang an – Ihre Fähigkeit, authentisch darzustellen, wie Zero Trust in Ihrer Organisation aussehen wird, wird erheblich gestärkt, wenn Sie mit dem Aufbau und der Implementierung begonnen haben (anstatt diese nur zu analysieren und darüber zu sprechen).
- Einholen finanzieller Unterstützung durch die Geschäftsleitung – Sichern Sie sich die finanzielle Förderung und Unterstützung der Zero-Trust-Implementierung. Bitten Sie andere C-Level-Führungskräfte, sich für die Initiative einzusetzen und die erforderlichen Ressourcen bereitzustellen. Das Engagement der Führungsebene ist unerlässlich, um die kulturellen und organisatorischen Veränderungen voranzutreiben, die für eine erfolgreiche Umsetzung erforderlich sind.
- Implementieren eines Governance-Frameworks – schaffen Sie ein Governance-Framework, das Rollen, Verantwortlichkeiten und Entscheidungsprozesse für die Implementierung von Zero Trust definiert. Legen Sie die Rechenschaftspflicht und die Eigenverantwortung für Sicherheitskontrollen, Risikomanagement und Compliance klar fest. Überprüfen und aktualisieren Sie das Governance-Framework regelmäßig, um es an wechselnde Sicherheitsanforderungen anzupassen.

- Unterstützen der funktionsübergreifenden Zusammenarbeit – fördern Sie die Zusammenarbeit und Kommunikation zwischen verschiedenen Geschäftsbereichen, IT-Teams und Sicherheitsteams. Schaffen Sie eine Kultur der gemeinsamen Verantwortung, um die Abstimmung und Koordination während der gesamten Zero-Trust-Implementierung zu fördern. Unterstützen Sie häufige Kommunikation, den Wissensaustausch und gemeinsame Problemlösungen.
- Schützen Ihrer Daten und Anwendungen – Bei Zero Trust geht es nicht nur darum, dass Endbenutzer auf Ressourcen und Anwendungen zugreifen. Die Zero-Trust-Prinzipien sollten auch innerhalb und zwischen Workloads implementiert werden. Wenden Sie dieselben technischen Prinzipien an – starke Identität, Mikrosegmentierung und Autorisierung –, indem Sie auch den gesamten verfügbaren Kontext innerhalb des Rechenzentrums nutzen.
- Umfassender Schutz – implementieren Sie eine umfassende Verteidigungsstrategie, indem Sie mehrere Ebenen von Sicherheitskontrollen verwenden. Kombinieren Sie verschiedene Sicherheitstechnologien wie die Multi-Faktor-Authentifizierung (MFA), Netzwerksegmentierung, Verschlüsselung und Erkennung von Anomalien, um umfassenden Schutz zu bieten. Stellen Sie sicher, dass jede Ebene die anderen ergänzt, um ein starkes Abwehrsystem zu schaffen.
- Anfordern einer starken Authentifizierung – Erzwingen Sie starke Authentifizierungsmechanismen wie MFA für alle Benutzer, die auf alle Ressourcen zugreifen. Im Idealfall sollten Sie moderne MFA wie hardwarebasierte FIDO2-Sicherheitsschlüssel in Betracht ziehen, die ein hohes Maß an Authentifizierungssicherheit für Zero Trust bieten und weitreichende Sicherheitsvorteile bieten (z. B. den Schutz vor Phishing).
- Zentralisieren und Verbessern der Autorisierung – autorisieren Sie gezielt jeden Zugriffsversuch. Abhängig von den Protokollspezifikationen sollte dies pro Verbindung oder pro Anfrage erfolgen. Die Autorisierung pro Anfrage ist ideal. Nutzen Sie den gesamten verfügbaren Kontext, einschließlich Identitäts-, Geräte-, Verhaltens- und Netzwerkinformationen, um detailliertere, anpassungsfähigere und ausgefeiltere Autorisierungsentscheidungen zu treffen.
- Nutzen des Prinzips der geringsten Berechtigung – implementieren Sie das Prinzip der geringsten Berechtigung, um Benutzern die Mindestzugriffsrechte zu gewähren, die für die Erfüllung ihrer Aufgaben erforderlich sind. Überprüfen und aktualisieren Sie die Zugriffsberechtigungen regelmäßig auf der Grundlage von Aufgabenbereichen, Zuständigkeiten und Geschäftsanforderungen. Implementieren Sie eine Just-in-Time-Zugriffsbereitstellung.
- Verwenden einer privilegierten Zugriffsverwaltung – implementieren Sie eine PAM-Lösung (Privileged Access Management), um privilegierte Konten zu schützen und das Risiko eines unbefugten Zugriffs auf kritische Systeme zu verringern. PAM-Lösungen bieten Funktionen für privilegierte Zugriffskontrollen, Sitzungsaufzeichnung und Prüfung, damit Ihre Organisation vertrauliche Daten und Systeme schützen kann.

- Nutzen der Mikrosegmentierung – teilen Sie Ihr Netzwerk in kleinere, isoliertere Segmente auf. Verwenden Sie die Mikrosegmentierung, um strenge Zugriffskontrollen zwischen Segmenten auf der Grundlage von Benutzerrollen, Anwendungen oder Datensensitivität durchzusetzen. Bemühen Sie sich, alle unnötigen Netzwerkpfade zu eliminieren, insbesondere wenn sie zu Daten führen.
- Überwachen von und Reagieren auf Sicherheitswarnungen – implementieren Sie ein umfassendes Programm zur Sicherheitsüberwachung und Reaktion auf Vorfälle in der Cloud-Umgebung. Verwenden Sie cloudnative Sicherheitstools und -dienste, um Bedrohungen in Echtzeit zu erkennen, Protokolle zu analysieren und die Reaktion auf Vorfälle zu automatisieren. Richten Sie klare Verfahren zur Reaktion auf Vorfälle ein, führen Sie regelmäßige Sicherheitsbewertungen durch und überwachen Sie Vorgänge kontinuierlich, um Anomalien oder verdächtige Aktivitäten zu erkennen.
- Nutzen der kontinuierlichen Überwachung – implementieren Sie eine kontinuierliche Überwachung, um Sicherheitsvorfälle schnell und effektiv zu erkennen und darauf zu reagieren. Verwenden Sie fortschrittliche Sicherheitsanalysetools, um das Benutzerverhalten, den Netzwerkverkehr und die Systemaktivitäten zu überwachen. Automatisieren Sie Warnungen und Benachrichtigungen, um die rechtzeitige Reaktion auf Vorfälle zu gewährleisten.
- Fördern einer Kultur der Sicherheit und Compliance – fördern Sie eine Kultur der Sicherheit und Compliance in der gesamten Organisation. Informieren Sie die Mitarbeiter über bewährte Sicherheitsverfahren, die Bedeutung der Einhaltung von Zero-Trust-Prinzipien und die Rolle der Mitarbeiter bei der Aufrechterhaltung einer sicheren Cloud-Umgebung. Führen Sie regelmäßige Schulungen zum Sicherheitsbewusstsein durch, um zu gewährleisten, dass die Mitarbeiter auf Social Engineering achten und sich ihrer Verantwortung in Bezug auf Datenschutz und Privatsphäre bewusst sind.
- Verwenden von Social-Engineering-Simulationen – führen Sie Social-Engineering-Simulationen durch, um die Anfälligkeit der Benutzer für Social-Engineering-Angriffe zu bewerten. Entwickeln Sie anhand der Ergebnisse der Simulationen individuelle Schulungsprogramme, um die Benutzer stärker zu sensibilisieren und auf potenzielle Bedrohungen zu reagieren.
- Fördern der kontinuierlichen Weiterbildung – etablieren Sie eine Kultur der kontinuierlichen Aus- und Weiterbildung, indem Sie fortlaufende Sicherheitsschulungen und Ressourcen bereitstellen. Halten Sie die Benutzer über die Entwicklung von bewährten Methoden für die Sicherheit auf dem Laufenden. Ermutigen Sie die Benutzer, wachsam zu bleiben und verdächtige Aktivitäten umgehend zu melden.
- Kontinuierliche Bewertung und Optimierung – untersuchen Sie die Cloud-Umgebung regelmäßig auf Verbesserungsmöglichkeiten. Verwenden Sie cloudnative Tools, um die Ressourcennutzung

und Leistung zu überwachen, und führen Sie Schwachstellenanalysen und Penetrationstests durch, um Schwachstellen zu erkennen und zu beheben.

- Einrichten eines Governance- und Compliance-Frameworks – entwickeln Sie ein Governance- und Compliance-Framework, um sicherzustellen, dass Ihre Organisation Branchenstandards und gesetzliche Anforderungen einhält. Legen Sie in diesem Framework Richtlinien, Verfahren und Kontrollen fest, um Daten und Systeme vor unbefugtem Zugriff, unbefugter Nutzung, Offenlegung, Störung, Änderung oder Zerstörung zu schützen. Implementieren Sie Mechanismen zur Nachverfolgung und Berichterstattung in Bezug auf Compliance-Kennzahlen, führen Sie regelmäßige Audits durch und beheben Sie etwaige Verstöße umgehend.
- Fördern der Zusammenarbeit und des Wissensaustausches – fördern Sie die Zusammenarbeit und den Wissensaustausch zwischen den Teams, die an der Einführung von ZTA beteiligt sind. Dies erreichen Sie, indem Sie die funktionsübergreifende Kommunikation und Zusammenarbeit zwischen IT-, Sicherheits- und Geschäftsbereichen fördern. Ihre Organisation kann außerdem Foren, Workshops und Sitzungen zum Wissensaustausch einrichten, um das Verständnis zu fördern, Herausforderungen anzugehen und Erfahrungen auszutauschen, die während des Einführungsprozesses gesammelt wurden.

Die wichtigsten Erkenntnisse

In diesem Leitfaden wurden die wesentlichen Aspekte der Entwicklung einer erfolgreichen Strategie für eine Zero-Trust-Architektur (ZTA) erkundet. Dieser Abschnitt fasst die wichtigsten Erkenntnisse aus der vorgeschriebenen Anleitung zusammen:

- Verstehen der Zero-Trust-Prinzipien – Zero Trust ist ein konzeptionelles Modell und ein zugehöriger Satz von Mechanismen, die darauf ausgerichtet sind, Sicherheitskontrollen für digitale Ressourcen bereitzustellen, die nicht ausschließlich oder grundlegend von herkömmlichen Netzwerkkontrollen oder Netzwerkperimetern abhängen. Stattdessen werden Netzwerkkontrollen um Identität, Gerät, Verhalten und andere umfangreiche Kontexte und Signale erweitert, um detailliertere, intelligentere, anpassungsfähigere und kontinuierlichere Zugriffsentscheidungen zu treffen. Machen Sie sich mit den Kernprinzipien von Zero Trust vertraut, wie z. B. geringste Berechtigung, Mikrosegmentierung, kontinuierliche Authentifizierung und adaptive Autorisierung.
- Klare Definition von Zielen – definieren Sie klar die Ziele und gewünschten Geschäftsergebnisse der ZTA-Einführung. Richten Sie diese Ziele an den Prinzipien von Zero Trust aus, um für eine solide Sicherheitsgrundlage zu sorgen und gleichzeitig Unternehmenswachstum und Innovation zu ermöglichen.
- Durchführung umfassender Bewertungen – führen Sie eine gründliche Bewertung Ihrer bestehenden IT-Infrastruktur, Anwendungen und Datenbestände durch. Identifizieren Sie Abhängigkeiten, technische Schulden und Kompatibilitätsprobleme, um Ihre Einführungsstrategie zu optimieren.
- Entwickeln eines Plans für die ZTA-Einführung – erstellen Sie einen detaillierten Plan, der das schrittweise Vorgehen für die Migration von Workloads, Anwendungen und Daten in die Cloud skizziert. Berücksichtigen Sie dabei Faktoren wie Compliance-Anforderungen und Anwendungsmodernisierung.
- Implementierung einer robusten ZTA – entwerfen und implementieren Sie eine ZTA, die differenzierte Zugriffskontrollen, starke Authentifizierungsmechanismen und eine kontinuierliche Überwachung durchsetzt. Für eine effizientere ZTA-Einführung sollten Sie cloudnative Zero-Trust-Services wie AWS Verified Access und Amazon VPC Lattice verwenden.
- Priorisieren der Sicherheit von Daten und Anwendungen – wenden Sie Zero-Trust-Prinzipien – starke Identität, Mikrosegmentierung und Autorisierung – an, um den gesamten verfügbaren Kontext bereitzustellen. Verwenden Sie diesen Kontext für Benutzer, die auf Systeme und Ressourcen zugreifen, sowie für den Kommunikations- und Datenfluss innerhalb und zwischen Back-End-Komponenten.

- Einrichten von Frameworks für die Überwachung und Reaktion auf Vorfälle – implementieren Sie robuste Funktionen zur Sicherheitsüberwachung und Reaktion auf Vorfälle in der Cloudumgebung. Verwenden Sie cloudnative Sicherheitstools für die Erkennung von Bedrohungen in Echtzeit, die Protokollanalyse und die Automatisierung der Reaktion auf Vorfälle, wie Amazon Inspector, AWS Security Hub und Amazon GuardDuty.
- Fördern einer Kultur der Sicherheit und Compliance – fördern Sie eine Kultur des Sicherheitsbewusstseins und der Compliance in der gesamten Organisation. Informieren Sie Mitarbeiter über bewährte Sicherheitsmethoden und ihre Rolle bei der Aufrechterhaltung einer sicheren Cloudumgebung.
- Kontinuierliche Bewertung und Optimierung – bewerten Sie regelmäßig die Cloudumgebung, die Sicherheitskontrollen und die betrieblichen Prozesse. Verwenden Sie cloudnative Analyse- und Überwachungstools wie Amazon CloudWatch und AWS Security Hub, um Erkenntnisse zu sammeln und die Ressourcennutzung, das Kostenmanagement und die Leistung zu optimieren.
- Einrichten von Governance- und Compliance-Frameworks – entwickeln Sie Governance- und Compliance-Frameworks, die Branchenstandards und gesetzlichen Anforderungen entsprechen. Definieren Sie Richtlinien, Verfahren und Kontrollen, um die Einhaltung von Sicherheits-, Datenschutz- und Compliance-Standards zu gewährleisten.

Nächste Schritte

Die Einführung einer Zero-Trust-Architektur (ZTA) ist eine der sichersten Methoden, um die Position Ihres Unternehmens zu verbessern und Risiken zu reduzieren. Diese vorgeschriebene Anleitung hat Ihnen einen umfassenden Plan für die Implementierung von Zero Trust an die Hand gegeben, vom Verständnis der Grundsätze über die Beurteilung Ihrer Bereitschaft bis hin zur Implementierung der erforderlichen Komponenten.

Die nächsten Schritte in diesem Workstream oder Bereich umfassen Folgendes:

- Umsetzung des Einführungsplans
- Implementieren von ZTA
- Durchführung regelmäßiger Sicherheitsbewertungen
- Kontinuierliche Optimierung der Cloud-Umgebung und der Sicherheitskontrollen

ZTA ist ein fortlaufender Prozess, der eine ständige Überwachung, Bewertung und Anpassung erfordert, um eine solide Sicherheitsgrundlage zu gewährleisten. Wenn Sie die in diesem Leitfaden beschriebenen bewährten Methoden befolgen, kann Ihr Unternehmen seine Sicherheitslage verbessern, die Einhaltung von Vorschriften gewährleisten und sensible Daten schützen.

Häufig gestellte Fragen

Dieser Abschnitt gibt Antworten auf häufig gestellte Fragen zum Entwurf und zur Implementierung einer Zero-Trust-Architektur (ZTA).

Was ist Zero Trust?

Zero Trust ist ein konzeptionelles Modell und ein zugehöriger Satz von Mechanismen, die darauf ausgerichtet sind, Sicherheitskontrollen für digitale Ressourcen bereitzustellen, die nicht ausschließlich oder grundlegend von herkömmlichen Netzwerkkontrollen oder Netzwerkperimetern abhängen. Stattdessen werden Netzwerkkontrollen um Identität, Gerät, Verhalten und andere umfangreiche Kontexte und Signale erweitert, um detailliertere, intelligentere, anpassungsfähigere und kontinuierlichere Zugriffsentscheidungen zu treffen.

Welche AWS-Services können mir bei der Implementierung einer Zero-Trust-Architektur helfen?

AWS bietet verschiedene Services, die bei der Implementierung von Zero Trust helfen können, wie AWS Verified Access, AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway und Amazon GuardDuty.

Wie kann ich mit AWS für Datensicherheit sorgen?

AWS bietet Services wie AWS Key Management Service (AWS KMS) für Datenverschlüsselung im Ruhezustand und bei der Übertragung, Amazon Virtual Private Cloud (Amazon VPC) für Netzwerkisolierung und AWS Secrets Manager für das sichere Speichern und Abrufen von Anmeldeinformationen.

Kann AWS bei den Compliance-Anforderungen in einer Zero-Trust-Umgebung helfen?

Ja, AWS verfügt über Compliance-Programme und -Services zur Erfüllung verschiedener regulatorischer Anforderungen. AWS Artifact bietet Zugriff auf AWS-Compliance-Berichte und AWS Config unterstützt die kontinuierliche Überwachung und Bewertung der Compliance.

Gibt es AWS-Tools oder -Services zur Automatisierung der Sicherheit in einer Zero-Trust-Umgebung?

AWS bietet Services wie AWS Security Hub zur Zentralisierung und Automatisierung von Sicherheitsergebnissen, sowie AWS Config-Regeln für die Definition und Durchsetzung von Sicherheitsrichtlinien.

Wie kann ich mit AWS eine kontinuierliche Überwachung und Reaktion auf Vorfälle in einer Zero-Trust-Cloud-Umgebung sicherstellen?

AWS bietet Services wie Amazon CloudWatch für die Überwachung in Echtzeit sowie AWS CloudTrail für die Protokollierung und Analyse. Bewährte Methoden zur Reaktion auf Vorfälle finden Sie im Leitfaden zur Reaktion auf Sicherheitsvorfälle in AWS.

Ressourcen

Referenzen

- What is a cloud center of excellence and why should your organization create one? – dieser Blogbeitrag bietet einen Überblick über CCoE, bewährte Methoden für die Einrichtung eines effektiven CCoE und mehr.
- Zero Trust in AWS – diese Seite bietet einen Überblick über die Zero-Trust-Sicherheitsprinzipien und bewährte Methoden in der AWS-Umgebung.
- Zero Trust architecture: An AWS perspective – dieser Blogbeitrag enthält eine Definition und Leitprinzipien für die Art und Weise, wie Zero Trust bei AWS umgesetzt wird.
- Leitfaden zu AWS Identity and Access Management (IAM) – dieser Leitfaden bietet eine umfassende Dokumentation zur Verwaltung von Benutzerzugriff und -berechtigungen in IAM, einer entscheidenden Komponente der Zero-Trust-Architektur.
- AWS Security Hub – erfahren Sie mehr über Security Hub, einen Service, der einen umfassenden Überblick über Sicherheitswarnungen und den Compliance-Status Ihrer AWS-Konten bietet.
- AWS Well-Architected Framework – lernen Sie das Well-Architected Framework kennen, das Anleitungen zum Aufbau sicherer, leistungsstarker, widerstandsfähiger und effizienter Architekturen in AWS bietet.
- Leitfaden zur Reaktion auf Sicherheitsvorfälle in AWS – dieser Leitfaden bietet einen Überblick über die Grundlagen der Reaktion auf Sicherheitsvorfälle in der AWS Cloud-Umgebung Ihrer Organisation. Er bietet einen Überblick über Konzepte zur Cloudsicherheit und zur Reaktion auf Vorfälle und identifiziert Cloudfunktionen, -services und -mechanismen, die Kunden zur Verfügung stehen, die auf Sicherheitsprobleme reagieren.

Tools

- Amazon API Gateway
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config

- Amazon GuardDuty
- AWS Identity and Access Management
- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub
- AWS Verified Access

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
Hinzugefügte Aktualisierungen	Es wurden Informationen zum Abschnitt Key components of a zero trust architecture hinzugefügt, Änderungen im Abschnitt Assessing organizational readiness for Zero Trust adoption vorgenommen, Informationen zum Abschnitt Best Practices hinzugefügt und Änderungen an den häufig gestellten Fragen vorgenommen.	4. Dezember 2023
Erste Veröffentlichung	—	19. Juni 2023

AWS Glossar zu präskriptiven Leitlinien

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

Zahlen

7 Rs

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

- Faktorwechsel/Architekturwechsel – Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile cloudnativer Feature nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf die Amazon Aurora 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.