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

AWS Prescriptive Guidance

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Prescriptive Guidance: Zero Trust umsetzen: eine Strategie für eine sichere und agile Unternehmenstransformation

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

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
Aus- und Weiterbildung zu Zero Trust 19
Zusammenarbeit und Kommunikation 19
Kontinuierliches Lernen und Verbesserung 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
Best Practices 24
Die wichtigsten Erkenntnisse 28
Nächste Schritte 30
Häufig gestellte Fragen 31
Was ist Zero Trust? 31
Was AWS-Services kann mir bei der Implementierung einer Zero-Trust-Architektur helfen? 31
Wie kann ich die Datensicherheit mit gewährleisten? AWS 31
Kann ich AWS bei den Compliance-Anforderungen in einer Zero-Trust-Umgebung helfen? 31
Gibt es AWS Tools oder Dienste zur Automatisierung der Sicherheit in einer Zero-Trust-Umgebung? 32
Wie kann ich eine kontinuierliche Überwachung und Reaktion auf Vorfälle in einer Zero-Trust-Cloud-Umgebung sicherstellen mit AWS 32
Ressourcen 33
Referenzen 33
Tools 33
Dokumentverlauf 35
..... xxxvi

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 CxOs VPs, andere und Führungskräfte einzubeziehen, um ihre Prioritäten, Bedenken 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 präskriptiven Leitlinien zielen darauf ab CxOs VPs, und Führungskräften eine umfassende Strategie für die Implementierung von ZTA an die Hand zu 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 Identity and Access Management (IAM) AWS Verified Access, Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway und Amazon. GuardDuty Diese Dienste können dazu beitragen, Ressourcen vor unbefugtem Zugriff zu schützen AWS .

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 Zugang auf einer bestimmten need-to-know Basis zu gewähren, in Verbindung mit strengen Kontrollen reduziert die Oberfläche 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 bekannt als Industrial Internet of Things (IIoT), übertragen häufig Telemetrie- und vorausschauende Wartungsinformationen 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. Dazu gehören die Implementierung von just-in-time Zugriffsberechtigungen, rollenbasierten Zugriffskontrollen (RBAC) und regelmäßige Zugriffsprüfungen, 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, softwaredefiniertes Networking (SDN), hostbasierte Firewalls, Netzwerkzugriffskontrolllisten (NACLs) und AWS spezifische Funktionen wie Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen oder implementiert werden. AWS PrivateLink 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 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 Center of Excellence (CCoE), die Überprüfung und Änderung der Sicherheitsabläufe sowie die Zuweisung von Rollen und Verantwortlichkeiten für das Schwachstellenmanagement, die Reaktion auf Vorfälle und die Sicherheitsüberwachung.

Cloud-Kompetenzzentrum

Richten Sie ein CCo E ein, das Leitlinien, bewährte Verfahren und Aufsicht für den Cloud-Betrieb bietet. Ein CCo E ist ein Team oder eine Gruppe von Personen, die für die Erstellung und Umsetzung von Best Practices, Richtlinien und Governance-Richtlinien im Zusammenhang mit der Cloud

verantwortlich sind. Dem CCo E sollten Vertreter verschiedener Geschäftsbereiche und IT-Teams angehören, um die Zusammenarbeit und Abstimmung sicherzustellen. Das CCo E spielt eine entscheidende Rolle dabei, die Einführung der Zero-Trust-Prinzipien in Cloud-gehosteten Workloads voranzutreiben. Das CCo E erleichtert auch den Wissensaustausch innerhalb der Organisation.

Sicherheitsvorgänge

Um den Anforderungen einer Zero-Trust-Umgebung gerecht zu werden, muss die aktuelle Organisation der Sicherheitsvorgänge überprüft und angepasst werden. Zur Verbesserung der Funktionen für Überwachung, Reaktion auf Vorfälle und Bedrohungsinformationen sollten Sie die Einrichtung 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 wichtiger Leistungsindikatoren (KPIs), deren Überwachung und Bewertung sowie die KPIs 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

Festlegung relevanter Leistungskennzahlen (KPIs) zur Bewertung des Erfolgs und der Wirksamkeit der Zero-Trust-Einführung. Anhand dieser KPIs Daten können die Benutzerzufriedenheit, der Fortschritt der Geräte und der Einführung, die Kostensenkung, die Einhaltung von Vorschriften und die Anzahl der Sicherheitsvorfälle gemessen werden. Um die Gesamtentwicklung zu verfolgen und Verbesserungsmöglichkeiten zu finden, sollten diese regelmäßig überwacht und bewertet werden.
KPIs

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 Ihres Unternehmens. Die Förderung einer Zero-Trust-Mentalität beinhaltet die Betonung der folgenden Schlüsselaspekte.

Aus- und Weiterbildung zu Zero Trust

Informieren Sie Ihre Mitarbeiter über die Werte und Vorteile der Zero-Trust-Architektur (ZTA). Erläutern Sie anhand von Schulungen, Workshops und anderen Ressourcen technische und nichttechnische Erläuterungen zu den Konzepten und Ansätzen von ZTA. 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. Fördern Sie die funktionsübergreifende Kommunikation, den Wissensaustausch und den Informationsaustausch, um sicherzustellen, dass jeder den Plan gründlich versteht. Schaffen Sie eine Kultur der gemeinsamen Verantwortung, in der jeder die Bedeutung seines Beitrags zur allgemeinen Sicherheit des Unternehmens anerkennt.

Kontinuierliches Lernen und Verbesserung

Priorisieren Sie kontinuierliches Lernen und Verbessern im Kontext von Zero Trust. Ermutigen Sie Ihre Mitarbeiter, sich über die neuesten Sicherheitstrends, Technologien und Best Practices auf dem Laufenden zu halten. Fördern Sie eine Innovations- und Experimentierkultur, in der die Mitarbeiter ermutigt werden, neue Lösungen und Ansätze zu erforschen, um die Sicherheitslage des Unternehmens zu stärken.

Kennzahlen und Rechenschaftspflicht

Legen Sie klare Kennzahlen und Rechenschaftsmechanismen fest, um die Effektivität der Zero-Trust-Strategie zu messen. Definieren Sie wichtige Leistungsindikatoren (KPIs), die den Sicherheitszielen des Unternehmens entsprechen, und verfolgen Sie regelmäßig die Fortschritte. Machen Sie

Einzelpersonen und Teams für ihre Beiträge 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 die erfolgreiche Einführung und Implementierung von Zero Trust schaffen. Dieser kulturelle Wandel ist unerlässlich, damit jeder im Unternehmen die Bedeutung von Zero Trust versteht und aktiv zu seinem Erfolg beiträgt.

Der nächste Abschnitt befasst sich mit der schrittweisen Einführung von Zero-Trust-Prinzipien und bietet Anleitungen zur praktischen und überschaubaren Umsetzung.

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 Sie sich im Laufe der Zeit ändern ZTAs werden, und überlegen Sie, wie die Entwicklungsteams diese Updates mit minimalem Aufwand oder Unterbrechungen implementieren werden.

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 Verfahren für eine erfolgreiche Implementierung von Zero Trust erörtert und wichtige Überlegungen und Empfehlungen für CxOs VPs, und Führungskräfte behandelt.

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 finden Sie eine Reihe von Best Practices CxOs VPs, die Führungskräften und Führungskräften dabei helfen 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 Sie einen Einführungsplan — Integrieren Sie einen detaillierten Einführungsplan, der den step-by-step Ansatz für die Verlagerung von Workloads, Anwendungen und Daten in die Cloud beschreibt. 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 defense-in-depth Strategie, 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 in Betracht ziehen, z. B. FIDO2 hardwaregestützte Sicherheitsschlüssel, die ein hohes Maß an Authentifizierungssicherheit für Zero Trust bieten und weitreichende Sicherheitsvorteile bieten (z. B. 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 die Zugriffsbereitstellung. just-in-time
- 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 Sie einen Plan zur Einführung von ZTA — Erstellen Sie einen detaillierten Plan, der den step-by-step Ansatz für die Verlagerung von Workloads, Anwendungen und Daten in die Cloud beschreibt. 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. Verwenden Sie für eine effizientere ZTA-Einführung Cloud-native Zero-Trust-Services wie Amazon VPC AWS Verified Access Lattice.
- 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 Cloud-native Sicherheitstools für Bedrohungserkennung, Protokollanalyse und Automatisierung von Incident-Response in Echtzeit, wie Amazon Inspector und Amazon GuardDuty. AWS Security Hub CSPM
- 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 Cloud-native Analyse- und Überwachungstools wie Amazon CloudWatch und, um Erkenntnisse zu sammeln und die Ressourcennutzung, das Kostenmanagement und die Leistung zu optimieren. AWS Security Hub CSPM
- 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.

Was AWS-Services kann mir bei der Implementierung einer Zero-Trust-Architektur helfen?

AWS bietet verschiedene Services, die bei der Implementierung von Zero Trust helfen können AWS Verified Access, wie 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 die Datensicherheit mit gewährleisten? AWS

AWS bietet Dienste wie AWS Key Management Service (AWS KMS) für die Datenverschlüsselung im Ruhezustand und bei der Übertragung, Amazon Virtual Private Cloud (Amazon VPC) für die Netzwerkisolierung und für die sichere Speicherung und AWS Secrets Manager den sicheren Abruf von Anmeldeinformationen.

Kann ich 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 Einhaltung.

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

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

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

AWS bietet Dienste wie Amazon CloudWatch für die Echtzeitüberwachung sowie AWS CloudTrail für die Protokollierung und Analyse an. 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 CCo E, bewährte Methoden zur Erstellung eines effektiven CCo E und vieles mehr.
- Zero Trust on AWS — Diese Seite bietet einen Überblick über die Sicherheitsprinzipien und bewährten Verfahren von Zero Trust in der AWS Umgebung.
- Zero-Trust-Architektur: Eine AWS Perspektive — Dieser Blogbeitrag enthält eine Definition und Leitprinzipien für die Art und Weise, wie Zero Trust implementiert wird AWS.
- AWS Identity and Access Management (IAM) -Benutzerhandbuch — Dieses Handbuch bietet eine umfassende Dokumentation zur Verwaltung von Benutzerzugriffen und -berechtigungen in IAM, einer wichtigen Komponente der Zero-Trust-Architektur.
- AWS Security Hub CSPM— Erfahren Sie mehr über Security Hub CSPM, einen Service, der einen umfassenden Überblick über Sicherheitswarnungen und den Compliance-Status in Ihrem Unternehmen bietet. AWS-Konten
- AWS Well-Architected Framework – lernen Sie das Well-Architected Framework kennen, das Anleitungen zum Aufbau sicherer, leistungsstarker, widerstandsfähiger und effizienter Architekturen in AWS bietet.
- AWS Leitfaden zur Reaktion auf Sicherheitsvorfälle — Dieser Leitfaden bietet einen Überblick über die Grundlagen der Reaktion auf Sicherheitsvorfälle in der Umgebung Ihres Unternehmens. AWS Cloud 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 CSPM
- 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

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.