AWS Well-Architected Framework

Säule der Sicherheit

Säule der Sicherheit: AWS Well-Architected Framework

Table of Contents

Säule „Sicherheit“ – AWS Well-Architected Framework

Veröffentlichungsdatum: 6. November 2024 (Dokumentversionen)

Das vorliegende Dokument befasst sich schwerpunktmäßig mit der Säule „Sicherheit“ des AWS Well-Architected Framework. Es bietet Anleitungen, die Ihnen helfen, bewährte Methoden und aktuelle Empfehlungen für das Design, die Bereitstellung und die Wartung sicherer AWS-Workloads anzuwenden.

Einführung

Das AWS Well-Architected Framework unterstützt Sie dabei, die Vor- und Nachteile der Entscheidungen nachzuvollziehen, die Sie beim Aufbau von Workloads in AWS treffen. Das Framework hilft Ihnen, aktuelle bewährte Architekturmethoden für den Entwurf und Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Workloads in der Cloud zu ermitteln. Es bietet Ihnen die Möglichkeit, Ihre Workload auf die Einhaltung bewährter Methoden zu prüfen und Verbesserungspotenzial zu identifizieren. Wir sind der Meinung, dass eine gute Workload-Architektur die Wahrscheinlichkeit für den geschäftlichen Erfolg deutlich erhöht.

Das Framework basiert auf den folgenden sechs Säulen:

- Operational Excellence
- Sicherheit
- Zuverlässigkeit
- Leistungseffizienz
- Kostenoptimierung
- Nachhaltigkeit

Dieses Whitepaper konzentriert sich auf die Säule „Sicherheit“. Indem Sie den aktuellen AWS-Empfehlungen folgen, können Sie sicherstellen, dass Sie die geschäftlichen und regulatorischen Anforderungen zu erfüllen. Dieses Dokument richtet sich an Nutzer in technologischen Rollen, z. B. CTOs (Chief Technology Officers), CSOs/CISOs (Chief Information Security Officers), Architekten, Entwickler und Mitglieder von Betriebsteams.

Sie erfahren darin mehr über die aktuellen Empfehlungen und Strategien von AWS für die Entwicklung sicherer Cloud-Architekturen. Auf Details zur Implementierung oder Architekturmuster

wird in diesem Whitepaper nicht eingegangen. Sie finden darin jedoch Verweise auf entsprechende Ressourcen mit diesen Informationen. Mit den Methoden in diesem Whitepaper können Sie Architekturen erstellen, die Ihre Daten und Systeme schützen, den Zugriff steuern und bei Sicherheitsereignissen automatisch reagieren.

Sicherheitsgrundlagen

Die Sicherheitssäule beschreibt, wie Sie Cloud-Technologien nutzen können, um Daten, Systeme und Komponenten so zu schützen, dass Ihre Sicherheitslage verbessert werden kann. Dieses Dokument bietet eine umfassende Anleitung mit den bewährten Methoden für den Aufbau sicherer Workloads in AWS.

Designprinzipien

Die Cloud bietet zahlreiche Möglichkeiten zur Verbesserung Ihrer Workload-Sicherheit:

- Implementieren einer starken Identitätsgrundlage: Etablieren Sie das Prinzip der geringsten Berechtigung und erzwingen Sie die Trennung von Pflichten durch eine entsprechende Autorisierung für jede Interaktion mit Ihren AWS-Ressourcen. Zentralisieren Sie die Identitätsverwaltung und vermeiden Sie die Abhängigkeit von langfristigen statischen Anmeldeinformationen.
- Sicherstellen der Nachverfolgbarkeit: Überwachen, melden und prüfen Sie Aktionen und Änderungen in Ihrer Umgebung in Echtzeit. Integrieren Sie die Protokoll- und Metrikerfassung in Systeme, um automatisch zu untersuchen und Maßnahmen zu ergreifen.
- Sicherheit auf allen Ebenen: Etablieren Sie eine Abwehrstrategie mit mehreren Sicherheitsmechanismen. Wenden Sie diesen auf allen Ebenen an (z. B. Netzwerkgrenzen, VPC, Lastverteilung, alle Instances und Datenverarbeitungsservices, Betriebssystem, Anwendung und Code).
- Automatisieren bewährter Sicherheitsverfahren: Mithilfe automatisierter softwarebasierter Sicherheitsmechanismen können Sie Ihr System sicher, schnell und kosteneffektiv skalieren. Erstellen Sie sichere Architekturen, einschließlich implementierter Kontrollen, die als Code in versionsgesteuerten Vorlagen definiert und verwaltet werden.
- Schutz von Daten während der Übertragung und im Ruhezustand: Klassifizieren Sie Ihre Daten nach Sensibilität und nutzen sie Mechanismen wie Verschlüsselung, Tokenisierung der Daten und Zugriffskontrolle.
- Trennen von Benutzern und Daten: Nutzen Sie Mechanismen und Tools, um den direkten Zugriff auf Daten zu minimieren/verhindern und das manuelle Verarbeiten Ihrer Daten zu reduzieren. Sie reduzieren dadurch das Risiko, dass sensible Daten verloren gehen, geändert werden oder anderweitigen Benutzerfehlern unterliegen.

- Vorbereitung auf Sicherheitsereignisse: Seien Sie auf Vorfälle vorbereitet. Richten Sie entsprechend Ihren organisatorischen Anforderungen ein Verfahren zum Vorfallmanagement sowie Richtlinien für die Überprüfung ein. Simulieren Sie Vorfallreaktionen und nutzen Sie automatisierbare Tools, um die Erkennung, Untersuchung und Wiederherstellung zu beschleunigen.

Definition

Sicherheit in der Cloud umfasst sieben Bereiche:

- Sicherheitsgrundlagen
- Identity and Access Management
- Erkennung
- Schutz der Infrastruktur
- Datenschutz
- Vorfallreaktion
- Anwendungssicherheit

Gemeinsame Verantwortlichkeit

Sicherheit und Compliance stellen eine übergreifende Verantwortlichkeit zwischen AWS und dem Kunden dar. Durch dieses gemeinsame Modell kann der Kunde entlastet werden, da AWS die Komponenten vom Host-Betriebssystem und der Virtualisierungsebene bis hin zur physischen Sicherheit der Einrichtungen, in denen der Service läuft, betreibt, verwaltet und kontrolliert. Der Kunde übernimmt Verantwortung für das Gastbetriebssystem und dessen Verwaltung (einschließlich Updates und Sicherheits-Patches) und andere damit verbundene Anwendungssoftware zusätzlich zur Konfiguration der von AWS bereitgestellten Firewall für die Sicherheitsgruppe. Kunden sollten sich gut überlegen, welche Services sie auswählen, da ihre Verantwortlichkeit von den genutzten Services, von deren Integration in ihre IT-Umgebung sowie von den geltenden Gesetzen und Vorschriften abhängt. Diese geteilte Verantwortung bietet auch die nötige Flexibilität und Kundenkontrolle für eine Bereitstellung. Wie im folgenden Diagramm dargestellt, wird diese Differenzierung der Verantwortung als Sicherheit „der“ Cloud bezeichnet, im Gegensatz zur Sicherheit „in“ der Cloud.

AWS-Verantwortlichkeit „Sicherheit der Cloud“: AWS ist für den Schutz der Infrastruktur verantwortlich, in der alle in der AWS angebotenen Services ausgeführt werden. Diese Infrastruktur besteht aus der Hardware, Software, dem Netzwerk und den Einrichtungen, auf und in denen AWS Cloud-Services ausgeführt werden.

Kundenverantwortlichkeit „Sicherheit in der Cloud“: Die Kundenverantwortlichkeit wird durch die AWS-Cloud-Services bestimmt, die ein Kunde auswählt. Dadurch wird der Umfang der Konfiguration bestimmt, die der Kunde im Rahmen seiner Sicherheitsverantwortung durchführen muss. Ein Service wie Amazon Elastic Compute Cloud (Amazon EC2) wird beispielsweise als Infrastructure as a Service (IaaS) kategorisiert und erfordert als solcher, dass der Kunde alle notwendigen Aufgaben der Sicherheitskonfiguration und -verwaltung übernimmt. Kunden, die eine Amazon-EC2-Instance einsetzen, sind für die Verwaltung des Gastbetriebssystems (einschließlich Updates und Sicherheitspatches), für die Anwendungssoftware oder Dienstprogramme, die vom Kunden auf den Instances installiert wurden, sowie für die Konfiguration der von AWS bereitgestellten Firewall (Sicherheitsgruppe genannt) auf jeder Instance verantwortlich. Für abstrakte Services wie Amazon S3 und Amazon DynamoDB betreibt AWS die Infrastrukturebene, das Betriebssystem und die Plattformen. Kunden greifen auf die Endpunkte zu, um Daten zu speichern und abzurufen. Die Kunden sind für die Verwaltung ihrer Daten (einschließlich Verschlüsselungsoptionen), die Klassifizierung ihrer Assets und die Verwendung von IAM-Tools zur Anwendung der entsprechenden Berechtigungen verantwortlich.

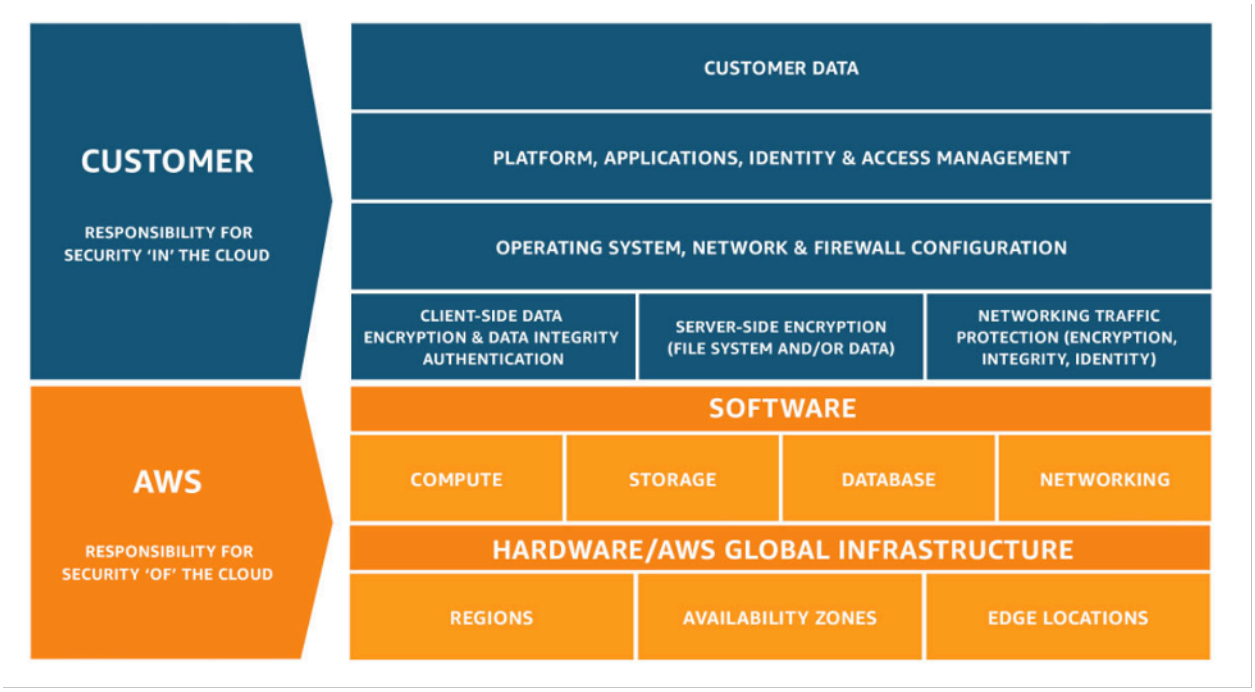


Abbildung 1: Das AWS-Modell der geteilten Verantwortung

Das Modell der geteilten Verantwortung von Kunde/AWS kann auch auf IT-Kontrollen ausgedehnt werden. Genauso wie die Verantwortung für den Betrieb der IT-Umgebung zwischen AWS und seinen Kunden geteilt wird, wird auch die Verwaltung, der Betrieb und die Überprüfung der IT-Kontrollen geteilt. AWS kann dazu beitragen, den Kunden bei der Bedienung der Mechanismen zu entlasten, indem es die Mechanismen verwaltet, die mit der in der AWS-Umgebung eingesetzten physischen Infrastruktur verbunden sind und zuvor vom Kunden verwaltet wurden. Da jede Kundenumgebung in AWS anders bereitgestellt wird, können Kunden vom Verlagern der Verwaltung bestimmter IT-Mechanismen an AWS profitieren, was zu einer (neuen) verteilten Kontrollumgebung führt. Die Kunden können dann die ihnen zur Verfügung stehenden AWS-Kontroll- und Konformitätsdokumente nutzen, um ihre Kontrollbewertungs- und -überprüfungsverfahren nach Bedarf durchzuführen. Nachfolgend finden Sie Beispiele für Kontrollen, die von AWS, AWS-Kunden oder von beiden verwaltet werden.

Vererbte Kontrollen: Kontrollen, die von AWS vollständig auf den Kunden übergehen.

- Physische und Umgebungskontrollen

Geteilte Kontrollen: Kontrollen, die für die Infrastruktur- und die Kundenebene gelten, allerdings in vollständig voneinander getrennten Kontexten oder Perspektiven. Bei einer geteilten Kontrolle werden die Anforderungen an die Infrastruktur von AWS bereitgestellt, und der Kunde muss seine eigene Kontrollimplementierung im Rahmen der Nutzung der AWS-Services bereitstellen. Beispiele sind unter anderem:

- Patch Management: AWS ist für das Patchen und Beheben von Fehlern innerhalb der Infrastruktur zuständig. Die Kunden sind für das Patchen ihres Gastbetriebssystems und ihrer Anwendungen verantwortlich.
  - Für AWS Managed Services, die auf Single-Tenant-Architekturen ausgeführt werden (wie Amazon ElastiCache, Amazon RDS und Amazon OpenSearch Service), wird die Verantwortung für das Patch-Management wie folgt aufgeteilt:
    - AWSVerantwortung: Identifizieren Sie Schwachstellen, entwickeln und validieren Sie Patches, veröffentlichen Sie Patches im Rahmen der Patching-SLA des Services und benachrichtigen Sie Kunden über verfügbare Updates über den dokumentierten Benachrichtigungsmechanismus des Services.
    - Verantwortung des Kunden: Überprüfen Sie die verfügbaren Updates und vereinfachen Sie das Patchen, indem Sie Wartungsfenster auswählen, Service-Updates installieren oder erforderliche Neustarts innerhalb der von AWS mitgeteilten Zeitrahmen planen.

  - Für AWS Managed Services, die auf Multi-Tenant-Architekturen ausgeführt werden (wie Amazon ElastiCache Serverless, Amazon DynamoDB und Amazon S3), wird die Verantwortung für das Patch-Management wie folgt aufgeteilt:
    - AWS-Verantwortung: Wenden Sie Patches an, ohne dass Aktionen seitens Kunden erforderlich sind.
    - Verantwortung des Kunden: Lesen Sie die Patch- und Wartungsdokumentation für jeden von ihnen verwendeten, von AWS verwalteten Service, um mehr über die spezifischen Benachrichtigungsmechanismen, Wartungsfensteroptionen und die verfügbaren Update-Anwendungsprozesse zu erfahren.
- Konfigurationsmanagement AWS verwaltet die Konfiguration seiner Infrastrukturgeräte. Die Kunden sind für die Konfiguration ihrer eigenen Gastbetriebssysteme, Datenbanken und Anwendungen verantwortlich.
- Sensibilisierung und Schulung AWS schult AWS-Mitarbeiter. Die Kunden müssen ihre eigenen Mitarbeiter schulen.

Kundenspezifisch: Kontrollen, die alleine in der Verantwortung des Kunden liegen und auf der Anwendung basieren, die er innerhalb von AWS-Services bereitstellt. Beispiele sind unter anderem:

- Services- und Kommunikationsschutz oder Zonensicherheit, die einen Kunden dazu verpflichten können, Daten innerhalb bestimmter Sicherheitsumgebungen weiterzuleiten oder in Zonen zu fassen.

Governance

Die Sicherheits-Governance als Teil des Gesamtkonzepts soll die Unternehmensziele unterstützen, indem sie Richtlinien und Kontrollziele für das Risikomanagement festlegt. Erreichen Sie ein Risikomanagement, indem Sie einen mehrschichtigen Ansatz für Sicherheitskontrollziele verfolgen – jede Schicht baut auf der vorherigen auf. Das Verständnis des AWS-Modells der geteilten Verantwortung ist die Grundlage für Ihre Arbeit. Dieses Wissen schafft Klarheit darüber, wofür Sie auf Kundenseite verantwortlich sind und was Sie von AWS übernehmen. Eine nützliche Ressource ist AWS Artifact, die Ihnen On-Demand-Zugriff auf die Sicherheits- und Compliance-Berichte von AWS und ausgewählte Online-Vereinbarungen bietet.

Erfüllen Sie die meisten Ihrer Kontrollziele auf der nächsten Ebene. Hier befindet sich die plattformübergreifende Fähigkeit. Zu dieser Ebene gehören beispielsweise der Prozess der AWS-Kontovergabe, die Integration mit einem Identitätsanbieter wie AWS IAM Identity Center und

die gemeinsamen aufdeckenden Kontrollen. Einige der Ergebnisse des Plattform-Governance-Prozesses sind ebenfalls hier zu finden. Wenn Sie einen neuen AWS-Service verwenden möchten, aktualisieren Sie die Service-Kontrollrichtlinien (SCPs) im Service von AWS Organizations, um den Integritätsschutz für die anfängliche Verwendung des Services bereitzustellen. Sie können andere SCPs verwenden, um gemeinsame Sicherheitskontrollziele zu implementieren, die oft als Sicherheitsinvarianten bezeichnet werden. Dies sind Kontrollziele oder Konfigurationen, die Sie auf mehrere Konten, Organisationseinheiten oder die gesamte AWS-Organisation anwenden. Typische Beispiele sind die Begrenzung der Regionen, in denen die Infrastruktur ausgeführt wird, oder die Verhinderung der Deaktivierung von aufdeckenden Kontrollen. Diese mittlere Ebene enthält auch kodifizierte Richtlinien wie Konfigurationsregeln oder Prüfungen in Pipelines.

Die oberste Ebene ist der Ort, an dem die Produktteams ihre Kontrollziele erreichen. Dies liegt daran, dass die Implementierung in den Anwendungen erfolgt, die von den Produktteams kontrolliert werden. Dabei kann es sich um die Implementierung einer Eingabevalidierung in einer Anwendung handeln oder um die Sicherstellung, dass die Identität zwischen Microservices korrekt weitergegeben wird. Auch wenn das Produktteam Besitzer der Konfiguration ist, kann es dennoch einige Fähigkeiten von der mittleren Ebene erben.

Wo auch immer Sie die Kontrolle durchführen, das Ziel ist das gleiche: Risikomanagement. Es gibt eine Reihe von Frameworks für das Risikomanagement, die für bestimmte Branchen, Regionen oder Technologien gelten. Ihr Hauptziel: Hervorhebung des Risikos anhand der Wahrscheinlichkeit und der Folgen. Dies ist das inhärente Risiko. Sie können dann ein Kontrollziel definieren, das entweder die Wahrscheinlichkeit oder die Folgen oder beides verringert. Wenn Sie dann eine Kontrolle durchführen, können Sie sehen, wie hoch das daraus resultierende Risiko sein wird. Dies ist das Restrisiko. Kontrollziele können sich auf eine oder mehrere Workloads beziehen. Das folgende Diagramm zeigt eine typische Risikomatrix. Die Wahrscheinlichkeit basiert auf der Häufigkeit früherer Vorfälle und die Folgen auf den finanziellen, rufschädigenden und zeitlichen Kosten des Ereignisses.

Likelihood	Risk Level				
Very Likely	Low	Medium	High	Critical	Critical
Likely	Low	Medium	Medium	High	Critical
Possible	Low	Low	Medium	Medium	High
Unlikely	Low	Low	Medium	Medium	High
Very unlikely	Low	Low		Medium	High
Consequence	Minimal	Low	Medium	High	Severe

Abbildung 2: Wahrscheinlichkeitsmatrix der Risikoebenen

AWS-Kontoverwaltung und -trennung

Wir empfehlen, Workloads in separaten Konten zu organisieren und Konten basierend auf Funktionen, Compliance-Anforderungen oder einer gemeinsamen Gruppe von Kontrollen zu gruppieren, anstatt die Berichtsstruktur Ihres Unternehmens zu spiegeln. In AWS sind Konten eine harte Grenze. Beispielsweise wird eine Trennung auf Kontoebene dringend empfohlen, um Produktions-Workloads von Entwicklungs- und Test-Workloads zu isolieren.

Zentrale Verwaltung von Konten: AWS Organizations automatisiert die Erstellung und Verwaltung von AWS-Konten und die Kontrolle dieser Konten nach ihrer Erstellung. Wenn Sie ein Konto über AWS Organizations erstellen, ist es wichtig, die E-Mail-Adresse zu berücksichtigen, die Sie verwenden, da dies der Root-Benutzer ist, der das Zurücksetzen des Passworts ermöglicht. Mit Organizations können Sie Konten in Organisationseinheiten (OUs) gruppieren, die je nach Anforderungen und Zweck der Workload unterschiedliche Umgebungen darstellen können.

Zentrale Einrichtung von Kontrollen: Kontrollieren Sie, was Ihre AWS-Konten tun können, indem Sie nur bestimmte Services, Regionen und Serviceaktionen auf der entsprechenden Ebene zulassen. Mit AWS Organizations können Sie Service-Kontrollrichtlinien (SCPs) verwenden, um Integritätsschutzfunktionen mit Berechtigungen auf der Ebene der Organisation, der Organisationseinheit oder des Kontos anzuwenden, die für alle AWS Identity and Access Management (IAM)-Benutzer und -Rollen gelten. Sie können beispielsweise eine SCP anwenden, die Benutzer daran hindert, Ressourcen in Regionen zu starten, die Sie nicht explizit zugelassen haben. AWS Control Tower bietet eine vereinfachte Möglichkeit, mehrere Konten einzurichten und zu verwalten. Es automatisiert die Einrichtung von Konten in Ihrer AWS-Organisation, automatisiert die Bereitstellung, wendet Integritätsschutz an (einschließlich Verhinderung und Erkennung) und stellt Ihnen ein Dashboard für Sichtbarkeit zur Verfügung.

Zentrale Konfiguration von Services und Ressourcen: Mit AWS Organizations können Sie AWS-Services, konfigurieren, die für alle Ihre Konten gelten. Sie können beispielsweise die zentrale Protokollierung aller in Ihrer Organisation durchgeführten Aktionen mithilfe von AWS CloudTrail konfigurieren und verhindern, dass Mitgliedskonten die Protokollierung deaktivieren. Sie können auch Daten für Regeln, die Sie mit AWS Config definiert haben, zentral aggregieren, sodass Sie Ihre Workloads auf Compliance prüfen und schnell auf Änderungen reagieren können. Mit AWS CloudFormation StackSets können Sie AWS CloudFormation-Stacks in Ihrer Organisation über Konten und OEs hinweg zentral verwalten. Auf diese Weise können Sie automatisch ein neues Konto bereitstellen, um Ihre Sicherheitsanforderungen zu erfüllen.

Verwenden Sie das Feature „Delegierte Verwaltung“ der Sicherheitsservices, um die für die Verwaltung verwendeten Konten vom organisatorischen Abrechnungskonto (Verwaltung) zu trennen. Mehrere AWS-Services, wie GuardDuty, Security Hub und AWS-Config, unterstützen die Integration mit AWS-Organisationen, einschließlich der Zuweisung eines bestimmten Kontos für Verwaltungsfunktionen.

Best Practices

- SEC01-BP01 Trennen von Workloads mithilfe von Konten
- SEC01-BP02 Schutz des Konto-Root-Benutzers und seiner Eigenschaften

SEC01-BP01 Trennen von Workloads mithilfe von Konten

Sorgen Sie mit einer Mehrkonten-Strategie für wirksamen Integritätsschutz und Isolierungen zwischen Umgebungen (etwa Produktion, Entwicklung und Test) sowie Workloads. Die Trennung auf Kontoebene wird nachdrücklich angeraten, da diese für die wirksame Isolierung für Sicherheits-, Fakturierungs- und Zugriffszwecke sorgt.

Gewünschtes Ergebnis: eine Kontostruktur, die Cloud-Vorgänge, nicht zusammengehörige Workloads und Umgebungen in separaten Konten voneinander isoliert, sodass die Sicherheit in der gesamten Cloud-Infrastruktur verbessert wird.

Typische Anti-Muster:

- Platzierung mehrerer nicht zusammengehöriger Workloads mit unterschiedlicher Datensensitivität in einem einzigen Konto
- Schlecht definierte Organizational Unit (OU, Organisationseinheit)-Struktur

Vorteile der Nutzung dieser bewährten Methode:

- Geringere Auswirkungen bei versehentlichen Zugriffen auf eine Workload
- Zentrale Verwaltung des Zugriffes auf AWS-Services, Ressourcen und Regionen
- Wahrung der Sicherheit der Cloud-Infrastruktur durch Richtlinien und die zentralisierte Verwaltung von Sicherheitsservices
- Automatisierte Kontoerstellung und Wartungsprozesse
- Zentralisierte Prüfung Ihrer Infrastruktur auf Compliance- und regulatorische Anforderungen

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

AWS-Konten bieten eine Sicherheitsisolierungsgrenze zwischen Workloads oder Ressourcen, die auf unterschiedlichen Sensitivitätsstufen operieren. AWS bietet Tools, mit denen Sie Ihre umfangreichen Cloud-Workloads über eine Mehrkonten-Strategie verwalten und so die Isolierungsgrenze nutzen können. Erläuterungen der Konzepte, Muster und der Implementierung einer Mehrkonten-Strategie in AWS finden Sie unter Organizing Your AWS Environment Using Multiple Accounts.

Wenn Sie mehrere AWS-Konten zentral verwalten, sollten Ihre Konten in einer gemäß den Ebenen der Organisationseinheiten (OEs) definierten Hierarchie organisiert sein. Dadurch können Sicherheitskontrollen anhand der OEs und der Mitgliedskonten organisiert und auf diese angewendet werden, was eine konsistente präventive Kontrolle der Mitgliedskonten in der Organisation ermöglicht. Die Sicherheitskontrollen werden weitergegeben, sodass Sie nach verfügbaren Berechtigungen für Mitgliedskonten auf unteren Ebenen der OE-Hierarchie filtern können. Ein gutes Design macht sich diese Weitergabe zunutze, um die Anzahl und die Komplexität der Sicherheitsrichtlinien, die für die erwünschten Sicherheitskontrollen für jedes Mitgliedskonto erforderlich sind, zu reduzieren.

AWS Organizations und AWS Control Tower sind zwei Services, mit denen Sie diese Mehrkontenstruktur in Ihrer AWS-Umgebung implementieren und verwalten können. AWS Organizations ermöglicht die Organisation von Konten in einer von einer oder mehreren OE-Ebenen definierten Hierarchie, wobei jede OE eine Reihe von Mitgliedskonten enthält. Service-Kontrollrichtlinien (SCPs) ermöglichen einem Organisationsadministrator die Einrichtung detaillierter präventiver Kontrollen für Mitgliedskonten und AWS Config kann verwendet werden, um proaktive und erkennende Kontrollen für Mitgliedskonten zu aktivieren. Viele AWS-Services lassen sich in AWS Organizations integrieren und bieten so delegierte administrative Kontrollen und führen servicespezifische Aufgaben für alle Mitgliedskonten in der Organisation durch.

Auf der Ebene über AWS Organizations ermöglicht AWS Control Tower die Einrichtung bewährter Methoden mit einem Klick für eine AWS-Mehrkontenumgebung mit einer Landing Zone. Die Landing Zone ist der Einstiegspunkt für die Mehrkonten-Umgebung, eingerichtet von Control Tower. Control Tower bietet mehrere Vorteile gegenüber AWS Organizations. Hier sind drei Vorteile, die die Kontoverwaltung verbessern:

- Integrierter verpflichtender Integritätsschutz, der automatisch auf für die Organisation zugelassene Konten angewendet wird

- Optionaler Integritätsschutz, der für einen bestimmten Satz von OEs aktiviert und deaktiviert werden kann
- AWS Control Tower Account Factory bietet eine automatisierte Bereitstellung von Konten mit vorab genehmigten Baselines und Konfigurationsoptionen innerhalb Ihrer Organisation.

Implementierungsschritte

1. Entwurf einer Struktur für Organisationseinheiten: Eine ordnungsgemäß gestaltete Struktur für Organisationseinheiten reduziert den Verwaltungsaufwand für die Erstellung und Wahrung von Service-Kontrollrichtlinien und anderen Sicherheitskontrollen. Ihre Struktur für Organisationseinheiten sollte an Ihre geschäftlichen Anforderungen, die Sensitivität der Daten und die Workload-Struktur angepasst sein.
2. Erstellen einer Landing Zone für Ihre Mehrkontenumgebung: Eine Landing Zone bietet eine konsistente Sicherheits- und Infrastrukturbasis, über die Ihre Organisation Workloads schnell entwickeln, starten und bereitstellen kann. Sie können eine individuell erstellte Landing ZoneAWS Control Tower oder für die Orchestrierung Ihrer Umgebung verwenden.
3. Einrichtung von Integritätsschutz: Implementieren Sie konsistenten Integritätsschutz für Ihre Umgebung über Ihre Landing Zone. AWS Control Tower bietet eine Liste verpflichtender und optionaler Kontrollen, die bereitgestellt werden können. Verpflichtende Kontrollen werden automatisch bereitgestellt, wenn Control Tower implementiert wird. Überprüfen Sie die Liste nachdrücklich empfohlener sowie optionaler Kontrollen und implementieren Sie diejenigen, die Ihren Anforderungen entsprechen.
4. Einschränken des Zugriffs auf neu hinzugefügte Regionen: Für neue AWS-Regionen werden IAM-Ressourcen, z. B. Benutzer und Rollen, nur an die von Ihnen angegebenen Regionen weitergegeben. Dieser Vorgang kann über die Konsole durchgeführt werden, wenn Sie Control Tower verwenden, oder durch die Anpassung von IAM-Berechtigungsrichtlinien in AWS Organizations.
5. Erwägen der Verwendung von AWS CloudFormation StackSets: StackSets helfen dabei, Ressourcen wie IAM-Richtlinien, -Rollen und -Gruppen aus einer genehmigten Vorlage in verschiedenen AWS-Konten-Konten und Regionen bereitzustellen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC02-BP04 Verlassen auf einen zentralen Identitätsanbieter

Zugehörige Dokumente:

- AWS Control Tower
- AWS-Richtlinien für Sicherheitsprüfungen
- IAM Best Practices
- Use CloudFormation StackSets to provision resources across multiple AWS-Konten and regions
- Organizations – Häufig gestellte Fragen
- AWS Organizations-Terminologie und -Konzepte
- Best Practices for Service Control Policies in an AWS Organizations Multi-Account Environment
- AWS Referenzhandbuch zur Kontoverwaltung
- Organisieren Sie Ihre AWS-Umgebung mit mehreren Konten

Zugehörige Videos:

- Enable AWS adoption at scale with automation and governance
- Security Best Practices the Well-Architected Way
- Building and Governing Multiple Accounts using AWS Control Tower
- Enable Control Tower for Existing Organizations

SEC01-BP02 Schutz des Konto-Root-Benutzers und seiner Eigenschaften

Der Root-Benutzer ist in einem AWS-Konto der Benutzer mit den meisten Berechtigungen und vollständigem administrativem Zugriff auf alle Ressourcen in dem Konto und kann in manchen Fällen nicht von Sicherheitsrichtlinien eingeschränkt werden. Die Deaktivierung des programmatischen Zugriffs auf den Root-Benutzer, die Einrichtung geeigneter Kontrollen für den Root-Benutzer und das Vermeiden der routinemäßigen Verwendung des Root-Benutzers senken die Risiken einer unbeabsichtigten Offenlegung der Anmeldeinformationen des Root-Benutzers und daraus resultierender ernsthafter Probleme für die Cloud-Umgebung.

Gewünschtes Ergebnis: Das Sichern des Root-Benutzers hilft dabei, die Gefahr zu verringern, dass versehentliche oder beabsichtigte Schäden durch den Missbrauch der Anmeldeinformationen des Root-Benutzers entstehen. Die Einrichtung erkennender Kontrollen kann auch für die Benachrichtigung der richtigen Personen sorgen, wenn Aktionen unter Verwendung des Root-Benutzers durchgeführt werden.

Typische Anti-Muster:

- Verwendung des Root-Benutzers für andere Aufgaben als die wenigen, für die Root-Benutzer-Anmeldeinformationen erforderlich sind
- Versäumnis, Notfallpläne regelmäßig zu testen, um das Funktionieren kritischer Infrastrukturen, Prozesse und des Personals während eines Notfalls zu überprüfen.
- ausschließliche Berücksichtigung des typischen Kontoanmeldungsprozesses und keine Berücksichtigung alternativer Kontowiederherstellungsverfahren
- keine Behandlung von DNS, E-Mail-Servern und Telefonanbietern als Teil des kritischen Sicherheitsperimeters, da diese in den Kontowiederherstellungsabläufen verwendet werden

Vorteile der Nutzung dieser bewährten Methode: Der Schutz des Zugriffs auf den Root-Benutzer stärkt das Vertrauen dazu, dass Aktionen in Ihrem Konto kontrolliert und überwacht werden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

AWS bietet zahlreiche Tools für den Schutz Ihres Kontos. Da einige dieser Maßnahmen aber nicht standardmäßig aktiviert sind, müssen Sie sie selbst implementieren. Betrachten Sie diese Empfehlungen als grundlegende Schritte für den Schutz Ihres AWS-Konto. Bei der Implementierung dieser Schritte ist es wichtig, dass Sie einen Prozess für die kontinuierliche Bewertung und Überwachung der Sicherheitskontrollen einrichten.

Wenn Sie ein AWS-Konto anlegen, beginnen Sie mit einer Identität, mit der Sie auf alle mit dem Konto verbundenen AWS-Services und -Ressourcen zugreifen können. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Sie können sich als Stammbenutzer mit der E-Mail-Adresse und dem Passwort anmelden, die Sie bei der Erstellung des Kontos verwendet haben. Da der AWS-Root-Benutzer erweiterte Zugriffsrechte hat, müssen Sie die Verwendung des AWS-Root-Benutzers auf die Aufgaben beschränken, für die er ausdrücklich erforderlich ist. Die Anmeldeinformationen des Root-Benutzers müssen sehr gut geschützt werden, und für den Root-Benutzer des AWS-Konto sollte immer die Multi-Faktor-Authentifizierung (MFA) genutzt werden.

Zusätzlich zum normalen Authentifizierungsablauf bei der Anmeldung als Root-Benutzer mit einem Benutzernamen, Passwort und einem Gerät zur Multi-Faktor-Authentifizierung (MFA) gibt es Kontowiederherstellungsabläufe für die Anmeldung Ihres AWS-Konto als Root-Benutzer mit Zugriff auf die mit Ihrem Konto verbundene E-Mail-Adresse und die Telefonnummer. Daher ist es ebenso

wichtig, das E-Mail-Konto des Root-Benutzers, an das die Wiederherstellungs-E-Mail gesendet wird, und die mit dem Konto verknüpfte Telefonnummer zu sichern. Denken Sie auch an mögliche zirkuläre Abhängigkeiten, bei denen die zum Root-Benutzer gehörende E-Mail-Adresse auf E-Mail-Servern oder Domain Name Service (DNS)-Ressourcen von demselben AWS-Konto gehostet wird.

Bei Verwendung von AWS Organizations gibt es mehrere AWS-Konten, die jeweils einen Root-Benutzer haben. Ein Konto fungiert als Verwaltungskonto und mehrere Ebenen von Mitgliedskonten können dann darunter hinzugefügt werden. Priorisieren Sie den Schutz des Root-Benutzers Ihres Verwaltungskontos und kümmern Sie sich dann um diejenigen der Mitgliedskonten. Die Strategie zum Schutz des Root-Benutzers Ihres Verwaltungskontos kann sich von der für die Root-Benutzer der Mitgliedskonten unterscheiden und Sie können präventive Sicherheitskontrollen für die Root-Benutzer Ihrer Mitgliedskonten einrichten.

Implementierungsschritte

Die folgenden Implementierungsschritte werden für die Einrichtung der Kontrollen für den Root-Benutzer empfohlen. Gegebenenfalls verweisen die Empfehlungen auf CIS AWS Foundations Benchmark, Version 1.4.0. Konsultieren Sie zusätzlich zu diesen Schritten die Richtlinien zu bewährten Methoden für AWS für den Schutz Ihres AWS-Konto und Ihrer Ressourcen.

Präventive Kontrollen

1. Richten Sie genaue Kontaktinformationen für das Konto ein.
    a. Diese Informationen werden für die Abläufe zur Wiederherstellung verlorener Passwörter, verlorener MFA-Gerätekonten und für die kritische sicherheitsrelevante Kommunikation mit Ihrem Team verwendet.
    b. Verwenden Sie eine von ihrer Unternehmensdomain gehostete E-Mail-Adresse, vorzugsweise eine Verteilerliste, als E-Mail-Adresse des Root-Benutzers. Die Verwendung einer Verteilerliste anstelle einer einzelnen E-Mail-Adresse sorgt für zusätzliche Redundanz und Kontinuität beim Zugriff auf das Root-Konto über längere Zeiträume hinweg.
    c. Die in den Kontaktinformationen angegebene Telefonnummer sollte eine für diesen Zweck speziell eingerichtete und sichere Telefonnummer sein. Diese Telefonnummer sollte nicht eingetragen sein oder an andere weitergegeben werden.
2. Erstellen Sie keine Zugriffsschlüssel für den Root-Benutzer. Wenn Zugriffsschlüssel vorhanden sind, entfernen Sie diese (CIS 1.4).
    a. Entfernen Sie alle langfristigen programmatischen Anmeldeinformationen (Zugriffs- und geheime Schlüssel) für den Root-Benutzer.

   b. Wenn bereits Zugriffsschlüssel für den Root-Benutzer vorhanden sind, sollten Prozesse, die diese Schlüssel verwenden, so umgestaltet werden, dass sie temporäre Zugriffsschlüssel von einer AWS Identity and Access Management (IAM)-Rolle verwenden; löschen Sie dann die Zugriffsschlüssel des Root-Benutzers.

3. Ermitteln Sie, ob Sie Anmeldeinformationen für den Root-Benutzer speichern müssen.
   a. Wenn Sie AWS Organizations zum Erstellen neuer Mitgliedskonten verwenden, wird das ursprüngliche Passwort für den Root-Benutzer in neuen Mitgliedskonten auf einen zufälligen Wert festgelegt, der Ihnen nicht angezeigt wird. Erwägen Sie die Nutzung der Passwortrücksetzung von Ihrem AWS-Organization-Verwaltungskonto, um bei Bedarf Zugriff auf das Mitgliedskonto zu erhalten.
   b. Für Standalone-AWS-Konten oder das AWS-Organization-Verwaltungskonto sollten Sie Anmeldeinformationen für den Root-Benutzer erstellen und sicher speichern. Verwenden Sie MFA für den Root-Benutzer.
4. Aktivieren Sie präventive Kontrollen für Root-Benutzer von Mitgliedskonten in AWS-Mehrkonten-Umgebungen.
   a. Erwägen Sie die präventive Sicherheitsvorkehrung Erstellung von Zugriffsschlüsseln für den Root-Benutzer nicht zulassen für Mitgliedskonten.
   b. Erwägen Sie die Aktivierung der präventiven Sicherheitsmaßnahme Aktionen als Root-Benutzer nicht zulassen für Mitgliedskonten.
5. Wenn Sie Anmeldeinformationen für den Root-Benutzer benötigen:
   a. Verwenden Sie ein komplexes Passwort.
   b. Aktivieren Sie Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer, besonders für AWS Organizations-Verwaltungskonten (Bezahlerkonten) (CIS 1.5).
   c. Erwägen Sie die Nutzung von Hardware-MFA-Geräten für Resilienz und Sicherheit, da Einweggeräte auf MFA-Funktionen begrenzt sind und so die Wahrscheinlichkeit verringern, dass die Geräte mit Ihren MFA-Codes für andere Zwecke verwendet werden. Stellen Sie sicher, dass batteriebetriebene MFA-Geräte regelmäßig ausgetauscht werden. (CIS 1.6)
      - Befolgen Sie zur Konfiguration der MFA für den Root-Benutzer die Anleitungen für die Aktivierung einer virtuellen MFA oder eines Hardware-MFA-Geräts.
   d. Erwägen Sie die Nutzung mehrerer MFA-Geräte als Sicherung. Pro Konto sind bis zu 8 MFA-Geräte zulässig.
      - Beachten Sie, dass die Verwendung von mehr als einem MFA-Gerät für den Root-Benutzer automatisch den Ablauf für die Wiederherstellung Ihres Kontos bei Verlust des MFA-Geräts deaktiviert.

e. Speichern Sie das Passwort in sicherer Weise, und beachten Sie zirkuläre Abhängigkeiten bei der elektronischen Speicherung des Passworts. Speichern Sie das Passwort nicht so, dass Zugriff auf dasselbe AWS-Konto erforderlich wäre, um es abzurufen.

6. Optional: Erwägen Sie die Einrichtung einer periodischen Passwortrotation für den Root-Benutzer.
   - Bewährte Methoden für die Verwaltung von Anmeldeinformationen hängen von Ihren jeweiligen regulatorischen und Richtlinienanforderungen ab. Durch MFA geschützte Root-Benutzer sind nicht auf das Passwort als einzigen Authentifizierungsfaktor angewiesen.
   - Die regelmäßige Änderung des Root-Benutzer-Passworts senkt das Risiko, dass ein unbeabsichtigt offengelegtes Passwort missbraucht werden kann.

Detektivische Kontrollen

- Erstellen Sie Alarme, um die Verwendung der Root-Anmeldeinformationen zu erkennen (CIS 1.7). Amazon GuardDuty kann die Nutzung der API-Anmeldeinformationen des Root-Benutzers überwachen und Sie über das Ergebnis von RootCredentialUsage benachrichtigen.
- Evaluieren und implementieren Sie die im Konformitätspaket der Säule „Sicherheit“ der AWS Well Architected für AWS Config enthaltenen aufdeckenden Kontrollen oder, falls Sie AWS Control Tower verwenden, die nachdrücklich empfohlenen Kontrollen, die in Control Tower verfügbar sind.

Operative Anleitung

- Legen Sie fest, wer in der Organisation Zugriff auf die Root-Benutzer-Anmeldeinformationen haben sollte.
  - Verwenden Sie eine Zwei-Personen-Regel, damit keine einzelne Person Zugang zu allen erforderlichen Anmeldeinformationen und zur MFA hat, um sich Root-Benutzer-Zugriff zu verschaffen.
  - Stellen Sie sicher, dass die Organisation – und nicht nur eine einzelne Person – die Kontrolle über die mit dem Konto verbundene Telefonnummer und das entsprechende E-Mail-Alias hat (diese werden für die Passwort- und die MFA-Rücksetzung verwendet).
- Verwenden Sie nur im Ausnahmefall den Root-Benutzer (CIS 1.7).
  - Der AWS-Root-Benutzer darf nicht für alltägliche Aktivitäten verwendet werden, auch nicht für administrative. Melden Sie sich nur dann als Root-Benutzer an, wenn Sie AWS-Aufgaben durchführen müssen, für die der Root-Benutzer erforderlich ist. Alle anderen Aktionen sollten von anderen Benutzern mit den entsprechenden Rollen durchgeführt werden.

- Prüfen Sie regelmäßig, ob der Zugriff auf den Root-Benutzer funktioniert, um Prozeduren vor dem Eintreten von Notsituationen zu testen, die die Verwendung der Root-Benutzer-Anmeldeinformationen erfordern.
- Prüfen Sie regelmäßig, ob die mit dem Konto verbundene E-Mail-Adresse und die unter Alternative Kontakte aufgeführten E-Mail-Adressen funktionieren. Überwachen Sie diese E-Mail-Posteingänge auf etwaige Sicherheitsmitteilungen von <abuse@amazon.com>. Stellen Sie auch sicher, dass alle mit dem Konto verbundenen Telefonnummern funktionieren.
- Bereiten Sie Notfallreaktionsprozeduren vor, um auf den Missbrauch des Root-Kontos reagieren zu können. Weitere Informationen zum Aufbau einer Sicherheitsstrategie für Ihr AWS-Konto-Konto finden Sie im AWS-Reaktionsleitfaden für Sicherheitsvorfälle und in den bewährten Methoden im Abschnitt zu Vorfallreaktionen im Whitepaper zur Säule „Sicherheit“.

Ressourcen

Zugehörige bewährte Methoden:

- SEC01-BP01 Trennen von Workloads mithilfe von Konten
- SEC02-BP01 Verwenden von starken Anmeldemechanismen
- SEC03-BP02 Gewähren des Zugriffs mit den geringsten Berechtigungen
- SEC03-BP03 Einrichtung eines Notfallzugriffprozesses
- SEC10-BP05 Vorab bereitgestellter Zugriff

Zugehörige Dokumente:

- AWS Control Tower
- AWS-Richtlinien für Sicherheitsprüfungen
- IAM Best Practices
- Amazon GuardDuty – Warnung bei Verwendung der Root-Anmeldeinformationen
- Schritt-für-Schritt-Anleitung zur Überwachung der Verwendung von Root-Anmeldeinformationen mit CloudTrail
- Zur Verwendung mit genehmigte MFA-Token AWS
- Implementieren von „Break Glass“-Zugriff in AWS
- Top 10 security items to improve in your AWS-Konto
- What do I do if I notice unauthorized activity in my AWS-Konto?

Zugehörige Videos:

- Enable AWS adoption at scale with automation and governance
- Security Best Practices the Well-Architected Way
- Limiting use of AWS root credentials from AWS re:inforce 2.022 – Security best practices with AWS IAM

Sicheres Betreiben Ihrer Workloads

Das sichere Betreiben von Workloads deckt den gesamten Lebenszyklus einer Workload ab, vom Design über die Erstellung bis hin zur Ausführung und zur laufenden Verbesserung. Eine der Möglichkeiten zur Verbesserung Ihrer Fähigkeit, sicher in der Cloud zu arbeiten, ist ein organisatorischer Ansatz für die Governance. Governance ist die Art und Weise, wie Entscheidungen konsequent geleitet werden, ohne dass sie allein vom guten Urteilsvermögen der beteiligten Personen abhängen. Ihr Governance-Modell und -Prozess ist die Art und Weise, wie Sie die Frage beantworten: „Woher weiß ich, dass die Kontrollziele für eine bestimmte Workload erfüllt werden und für diese Workload angemessen sind?“ Ein einheitlicher Ansatz für die Entscheidungsfindung beschleunigt die Bereitstellung von Workloads und trägt dazu bei, die Messlatte für die Sicherheitskapazität in Ihrem Unternehmen höher zu legen.

Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an. Wenn Sie über AWS- und Branchenempfehlungen sowie Bedrohungsinformationen auf dem Laufenden bleiben, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Die Automatisierung von Sicherheitsprozessen, Tests und Validierung hilft Ihnen, Ihre Sicherheitsvorgänge zu skalieren.

Die Automatisierung ermöglicht die Konsistenz und Wiederholbarkeit von Prozessen. Menschen sind in vielen Dingen gut, aber immer wieder das Gleiche zu tun, ohne Fehler zu machen, gehört nicht dazu. Selbst bei gut geschriebenen Runbooks besteht die Gefahr, dass die Mitarbeiter sich wiederholende Aufgaben nicht konsequent ausführen. Dies gilt vor allem dann, wenn die Mitarbeiter verschiedene Aufgaben haben und dann auf ungewohnte Alarme reagieren müssen. Die Automatisierung hingegen reagiert jedes Mal auf dieselbe Weise. Der beste Weg zur Bereitstellung von Anwendungen ist die Automatisierung. Der Code, mit dem die Bereitstellung ausgeführt wird, kann getestet und dann zur Durchführung der Bereitstellung verwendet werden. Dies erhöht

das Vertrauen in den Veränderungsprozess und verringert das Risiko einer fehlgeschlagenen Veränderung.

Um zu überprüfen, ob die Konfiguration Ihren Kontrollzielen entspricht, testen Sie die Automatisierung und die bereitgestellte Anwendung zunächst in einer Nicht-Produktionsumgebung. Auf diese Weise können Sie die Automatisierung testen, um nachzuweisen, dass sie alle Schritte korrekt ausgeführt hat. Außerdem erhalten Sie frühzeitiges Feedback im Entwicklungs- und Bereitstellungszyklus, was die Nacharbeit reduziert. Um die Wahrscheinlichkeit von Bereitstellungsfehlern zu verringern, sollten Sie Konfigurationsänderungen durch Code und nicht durch Personen vornehmen. Wenn Sie eine Anwendung erneut bereitstellen müssen, wird dies durch die Automatisierung erheblich erleichtert. Wenn Sie zusätzliche Kontrollziele definieren, können Sie diese einfach zur Automatisierung für alle Workloads hinzufügen.

Anstatt dass die Eigentümer der einzelnen Workloads in die für ihre Workloads spezifische Sicherheit investieren müssen, sparen Sie Zeit durch die Nutzung gemeinsamer Funktionen und Komponenten. Einige Beispiele für Services, die von mehreren Teams genutzt werden können, sind der Prozess der AWS-Kontoerstellung, die zentrale Identität von Personen, die gemeinsame Konfiguration der Protokollierung sowie die Erstellung von AMI- und Container-Basis-Images. Dieser Ansatz kann Entwicklern dabei helfen, die Zykluszeiten für die Workloads zu verkürzen und die Ziele der Sicherheitskontrolle konsequent einzuhalten. Wenn die Teams kohärenter arbeiten, können Sie die Kontrollziele validieren und den Beteiligten besser über Ihre Kontrollsituation und Risikolage berichten.

Best Practices

- SEC01-BP03 Identifizieren und Validieren von Kontrollzielen
- SEC01-BP04 Sicherstellen der Aktualität von Informationen zu Sicherheitsbedrohungen
- SEC01-BP05 Verringern des Umfangs der Sicherheitsverwaltung
- SEC01-BP06 Automatisieren der Bereitstellung von Standard-Sicherheitskontrollen
- SEC01-BP07 Identifizieren von Bedrohungen und Priorisieren von Abhilfemaßnahmen unter Verwendung eines Bedrohungsmodells
- SEC01-BP08 Regelmäßiges Bewerten und Implementieren neuer Sicherheitsservices und -features

SEC01-BP03 Identifizieren und Validieren von Kontrollzielen

Entsprechend Ihren Compliance-Anforderungen und Risiken, die aus Ihrem Bedrohungsmodell identifiziert werden, können Sie die Kontrollziele und Kontrollen ableiten und validieren, die Sie für Ihre Workload benötigen. Die laufende Validierung von Kontrollzielen und Kontrollen hilft Ihnen, die Effektivität der Risikominderung zu messen.

Gewünschtes Ergebnis: Die Kontrollziele Ihres Unternehmens sind klar definiert und auf Ihre Compliance-Anforderungen abgestimmt. Kontrollen werden durch Automatisierung und Richtlinien implementiert und durchgesetzt und kontinuierlich auf ihre Wirksamkeit bei der Erreichung Ihrer Ziele überprüft. Die Belege für die Wirksamkeit sowohl zu einem bestimmten Zeitpunkt als auch über einen bestimmten Zeitraum hinweg sind jederzeit für Prüfer abrufbar.

Typische Anti-Muster:

- Regulatorische Anforderungen, Markterwartungen und Branchenstandards für verlässliche Sicherheit sind in Ihrem Unternehmen nicht hinreichend vertraut.
- Ihr Framework für die Cybersicherheit und Ihre Kontrollziele sind nicht an den Anforderungen Ihres Unternehmens ausgerichtet.
- Die Implementierung der Kontrollen ist nicht messbar auf Ihre Kontrollziele ausgerichtet.
- Sie verwenden keine Automatisierung zur Berichterstattung über die Wirksamkeit Ihrer Kontrollen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Es gibt zahlreiche gängige Frameworks für die Cybersicherheit, die die Grundlage für Ihre Sicherheitskontrollziele bilden können. Berücksichtigen Sie die regulatorischen Anforderungen, die Markterwartungen und die Branchenstandards für Ihr Unternehmen, um festzustellen, welches Framework Ihre Anforderungen am besten erfüllt. Beispiele hierfür sind u. a. AICPA SOC 2, HITRUST, PCI-DSS, ISO 27001 und NIST SP 800-53.

Für die von Ihnen festgelegten Kontrollziele sollten Sie verstehen, wie die von Ihnen in Anspruch genommenen AWS-Services Ihnen helfen, diese Ziele zu erreichen. Unter AWS Artifact finden Sie Dokumentationen und Berichte, die auf Ihre Zielframeworks abgestimmt sind. Darin wird der Verantwortungsbereich von AWS beschrieben. Ferner können Sie dort Anleitungen erhalten, in denen der verbleibende Umfang, für den Sie verantwortlich sind, beschrieben wird. Weitere

servicespezifische Anleitungen, die sich an verschiedenen Regelwerken orientieren, finden Sie unter AWS Customer Compliance Guides.

Während Sie die Kontrollen zur Erreichung Ihrer Ziele definieren, kodifizieren Sie die Durchsetzung mithilfe von präventiven Kontrollen und automatisieren die Abschwächung mithilfe von detektivischen Kontrollen. Verhindern Sie nicht konforme Ressourcenkonfigurationen und Aktionen in AWS Organizations mithilfe von Service-Kontrollrichtlinien (SCPs). Implementieren Sie Regeln in AWS Config zur Überwachung und Berichterstattung über nicht konforme Ressourcen und wechseln Sie dann zu einem Durchsetzungsmodell, sobald Sie von deren Verhalten überzeugt sind. Wenn Sie vordefinierte und verwaltete Regeln bereitstellen möchten, die sich an Ihren Cybersicherheits-Rahmenbedingungen orientieren, sollten Sie die Verwendung von AWS Security Hub CSPM-Standards als erste Wahl in Betracht ziehen. Der Standard „Foundational Service Best Practices (FSBP)“ von AWS und der CIS-AWS-Foundations-Benchmark sind gute Ausgangspunkte mit Kontrollen, die auf zahlreiche Ziele ausgerichtet sind, die in mehreren Standardframeworks gemeinsam genutzt werden. In Fällen, in denen Security Hub CSPM nicht intrinsisch die gewünschten Kontrollmeldungen verfügt, kann es durch AWS Config-Konformitätspakete ergänzt werden.

Verwenden Sie APN-Partnerpakete, die vom Global Security and Compliance Acceleration (GSCA)-Team von AWS empfohlen werden, um bei Bedarf Unterstützung von Sicherheitsberatern, Beratungsagenturen, Beweissammlungs- und Berichtssystemen, Prüfern und anderen ergänzenden Services zu erhalten.

Implementierungsschritte

1. Bewerten Sie gängige Frameworks für Cybersicherheit und richten Sie Ihre Kontrollziele an den ausgewählten Frameworks aus.
2. Beschaffen Sie sich mithilfe von AWS Artifact einschlägige Unterlagen über Leitlinien und Verantwortlichkeiten für Ihr Framework. Machen Sie sich klar, welche Teile der Compliance in den AWS-Bereich des Modells der gemeinsamen Verantwortung fallen und für welche Teile Sie verantwortlich sind.
3. Verwenden Sie SCPs, Ressourcenrichtlinien, Rollenvertrauensrichtlinien und andere Maßnahmen für den Integritätsschutz, um nicht konforme Ressourcenkonfigurationen und Aktionen zu verhindern.
4. Evaluieren Sie die Implementierung von Security-Hub-CSPM-Standards und AWS Config-Konformitätspaketen, die mit Ihren Kontrollzielen übereinstimmen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC03-BP01 Definieren von Zugriffsanforderungen
- SEC04-BP01 Konfigurieren der Service- und Anwendungsprotokollierung
- SEC07-BP01 Verstehen Ihres Schemas zur Datenklassifizierung
- OPS01-BP03 Bewerten der Governance-Anforderungen
- OPS01-BP04 Bewerten der Compliance-Anforderungen
- PERF01-BP05 Verwenden von Richtlinien und Referenzarchitekturen
- COST02-BP01 Entwickeln von Richtlinien auf Basis Ihrer Organisationsanforderungen

Zugehörige Dokumente:

- AWS Customer Compliance Guides

Zugehörige Tools:

- AWS Artifact

SEC01-BP04 Sicherstellen der Aktualität von Informationen zu Sicherheitsbedrohungen

Bleiben Sie auf dem Laufenden über die neuesten Bedrohungen und Abhilfemaßnahmen, indem Sie Veröffentlichungen zu Bedrohungsdaten und Datenfeeds der Branche auf Aktualisierungen verfolgen. Prüfen Sie Angebote für verwaltete Services, die automatisch auf der Grundlage der neuesten Bedrohungsdaten aktualisiert werden.

Gewünschtes Ergebnis: Sie bleiben auf dem Laufenden, da die Branchenpublikationen mit den neuesten Bedrohungen und Empfehlungen aktualisiert werden. Sie nutzen die Automatisierung, um potenzielle Schwachstellen und Gefährdungen zu erkennen, während Sie neue Bedrohungen identifizieren. Sie ergreifen Maßnahmen zur Eindämmung dieser Bedrohungen. Sie übernehmen AWS-Services, die automatisch mit den neuesten Bedrohungsdaten aktualisiert werden.

Typische Anti-Muster:

- Kein zuverlässiger und wiederholbarer Mechanismus, um über die neuesten Bedrohungsdaten informiert zu sein
- Manuelle Bestandsführung Ihres Technologieportfolios, Ihrer Workloads und Abhängigkeiten, was menschliches Eingreifen im Hinblick auf potenzielle Schwachstellen und Gefährdungen erfordert
- Fehlende Mechanismen zur Aktualisierung Ihrer Workloads und Abhängigkeiten auf die neuesten verfügbaren Versionen, die bekannte Bedrohungsabwehrmaßnahmen bieten

Vorteile der Nutzung dieser bewährten Methode: Die Verwendung von Bedrohungsdatenquellen, um auf dem Laufenden zu bleiben, verringert das Risiko, wichtige Änderungen in der Bedrohungslandschaft zu verpassen, die sich auf Ihr Unternehmen auswirken können. Wenn Sie Ihre Workloads und deren Abhängigkeiten automatisiert auf potenzielle Schwachstellen oder Gefährdungen prüfen, diese erkennen und beheben, können Sie Risiken im Vergleich zu manuellen Alternativen schnell und vorhersehbar eindämmen. Dies trägt dazu bei, Zeit und Kosten im Zusammenhang mit der Behebung von Schwachstellen zu kontrollieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Verfolgen Sie vertrauenswürdige Veröffentlichungen zu Bedrohungsdaten, um über die Bedrohungslandschaft auf dem Laufenden zu bleiben. Konsultieren Sie die Wissensdatenbank von MITRE ATT&CK. Hier finden Sie Dokumentationen über bekannte gegnerische Taktiken, Techniken und Verfahren (Tactics, Techniques and Procedures, TTPs). Informieren Sie sich in der MITRE-Liste Common Vulnerabilities and Exposures (CVE) über bekannte Schwachstellen in Produkten, auf die Sie angewiesen sind. Verstehen Sie kritische Risiken für Webanwendungen mit dem populären Projekt OWASP Top 10 des Open Worldwide Application Security Project (OWASP).

Bleiben Sie auf dem Laufenden über AWS-Sicherheitsereignisse und empfohlene Abhilfemaßnahmen mit AWS-Sicherheitsberichten für CVEs.

Um den Gesamtaufwand für die Aktualisierung zu reduzieren, sollten Sie AWS-Services nutzen. Diese beziehen die neue Bedrohungsdaten im Laufe der Zeit automatisch ein. Zum Beispiel behält Amazon GuardDuty den Überblick über die Bedrohungsdaten der Branche, um anormale Verhaltensweisen und Bedrohungssignaturen in Ihren Konten zu erkennen. Amazon Inspector hält automatisch eine Datenbank mit den CVEs auf dem neuesten Stand. Diese Datenbank wird für die kontinuierlichen Scan-Features verwendet. Sowohl AWS WAF als auch AWS Shield Advanced bieten verwaltete Regelgruppen, die automatisch aktualisiert werden, wenn neue Bedrohungen auftauchen.

Informationen zum automatisierten Flottenmanagement und Patching finden Sie unter Säule „Operative Exzellenz“ – Well-Architected-Framework

Implementierungsschritte

- Abonnieren Sie Updates für Bedrohungsinformationen, die für Ihr Unternehmen und Ihre Branche relevant sind. Abonnieren Sie die AWS-Sicherheitsberichte.
- Erwägen Sie die Einführung von Services, die neue Bedrohungsdaten automatisch einbeziehen, wie Amazon GuardDuty und Amazon Inspector.
- Erstellen Sie eine Flottenmanagement- und Patching-Strategie, die sich an den bewährten Methoden der der Säule „Operative Exzellenz“ des Well-Architected-Framework“ orientiert.

Ressourcen

Zugehörige bewährte Methoden:

- SEC01-BP07 Identifizieren von Bedrohungen und Priorisieren von Abhilfemaßnahmen unter Verwendung eines Bedrohungsmodells
- OPS01-BP05 Bewerten der Bedrohungsszenarien
- OPS11-BP01 Implementieren eines Prozesses für die kontinuierliche Verbesserung

SEC01-BP05 Verringern des Umfangs der Sicherheitsverwaltung

Ermitteln Sie, ob Sie Ihren Sicherheitsumfang reduzieren können, indem Sie AWS-Services verwenden, die die Verwaltung bestimmter Kontrollen in AWS verlagern (verwaltete Services). Mit diesen Services können Sie Ihre Wartungsaufgaben im Bereich Sicherheit reduzieren, z. B. die Bereitstellung der Infrastruktur, die Einrichtung von Software, Patches oder Sicherungen.

Gewünschtes Ergebnis: Sie berücksichtigen den Umfang Ihrer Sicherheitsverwaltung bei der Auswahl von AWS-Services für Ihre Workload. Die Kosten für den Verwaltungsaufwand und die Wartungsaufgaben (die Gesamtbetriebskosten (Total Cost of Ownership, TCO) werden gegen die Kosten der von Ihnen ausgewählten Services abgewogen. Hinzu kommen weitere Überlegungen im Rahmen von Well-Architected. Sie integrieren die Kontroll- und Compliance-Dokumentation von AWS in Ihre Kontrollbewertungs- und Verifizierungsverfahren.

Typische Anti-Muster:

- Bereitstellung von Workloads ohne gründliches Verständnis des Modells der geteilten Verantwortung für die von Ihnen ausgewählten Services
- Hosten von Datenbanken und anderen Technologien auf virtuellen Maschinen, ohne einen entsprechenden verwalteten Service evaluiert zu haben
- Nichtberücksichtigung von Sicherheitsverwaltungsaufgaben bei den Gesamtbetriebskosten des Hostings von Technologien auf virtuellen Maschinen im Vergleich zu verwalteten Serviceoptionen

Vorteile der Nutzung dieser bewährten Methode: Der Einsatz von verwalteten Services kann Ihren Gesamtaufwand für die Verwaltung der betrieblichen Sicherheitskontrollen verringern, was Ihre Sicherheitsrisiken und Gesamtbetriebskosten reduzieren kann. Die Zeit, die Sie sonst für bestimmte Sicherheitsaufgaben aufwenden müssten, können Sie in Aufgaben investieren, die Ihrem Unternehmen einen größeren Nutzen bringen. Verwaltete Services können auch den Umfang Ihrer Compliance-Anforderungen reduzieren, indem sie einige Kontrollanforderungen in AWS verlagern.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Es gibt mehrere Möglichkeiten, wie Sie die Komponenten Ihrer Workload in AWS integrieren können. Die Installation und der Betrieb von Technologien auf Amazon-EC2-Instances erfordert häufig, dass Sie den größten Teil der gesamten Sicherheitsverantwortung übernehmen. Um den Aufwand für die Durchführung bestimmter Kontrollen zu verringern, sollten Sie von AWS verwaltete Services identifizieren, die den Umfang Ihrer Seite des Modells der geteilten Verantwortung verringern, und verstehen, wie Sie diese in Ihrer bestehenden Architektur nutzen können. Beispiele sind die Verwendung von Amazon Relational Database Service (Amazon RDS) für die Bereitstellung von Datenbanken, Amazon Elastic Kubernetes Service (Amazon EKS) oder Amazon Elastic Container Service (Amazon ECS) für die Orchestrierung von Containern oder die Verwendung von Serverless-Optionen. Überlegen Sie bei der Entwicklung neuer Anwendungen, welche Services dazu beitragen können, den Zeit- und Kostenaufwand für die Implementierung und Verwaltung von Sicherheitskontrollen zu reduzieren.

Auch Compliance-Anforderungen können bei der Auswahl von Services eine Rolle spielen. Verwaltete Services können die Einhaltung einiger Anforderungen in AWS verlagern. Sprechen Sie mit Ihrem Compliance-Team darüber, inwieweit es sich mit der Prüfung der von Ihnen betriebenen und verwalteten Services und der Annahme von Kontrollerklärungen in den entsprechenden Audit-Berichten von AWS wohl fühlt. Sie können die in AWS Artifact gefundenen Audit-Artefakte Ihren Prüfern oder Regulierungsbehörden als Nachweis für AWS-Sicherheitskontrollen vorlegen. Sie

können beim Design Ihrer Architektur auch die Hinweise zur Verantwortung verwenden, die in einigen AWS-Audit-Artefakten enthalten sind, zusammen mit den AWS Customer Compliance Guides. Dieser Leitfaden hilft Ihnen, die zusätzlichen Sicherheitskontrollen zu bestimmen, die Sie einrichten sollten, um die spezifischen Anwendungsfälle Ihres Systems zu unterstützen.

Wenn Sie verwaltete Services nutzen, sollten Sie mit dem Prozess der Aktualisierung ihrer Ressourcen auf neuere Versionen vertraut sein (z. B. die Aktualisierung der Version einer von Amazon RDS verwalteten Datenbank oder einer Laufzeit einer Programmiersprache für eine AWS Lambda-Funktion). Auch wenn der verwaltete Service diesen Vorgang für Sie durchführt, sind Sie für die Konfiguration des Zeitpunkts der Aktualisierung und die Auswirkungen auf Ihren Betrieb selbst verantwortlich. Tools wie AWS Health können Ihnen helfen, diese Updates in Ihren Umgebungen zu verfolgen und zu verwalten.

Implementierungsschritte

1. Bewerten Sie die Komponenten Ihrer Workload, die durch einen verwalteten Service ersetzt werden können.
   a. Wenn Sie eine Workload zu AWS migrieren, sollten Sie den geringeren Verwaltungsaufwand (Zeit und Kosten) und die Verringerung des Risikos berücksichtigen, wenn Sie folgende Optionen für Ihren Workload bewerten: Hostwechsel, Faktorwechsel, Plattformwechsel, erneute Erstellung oder Ersatz. Manchmal können zusätzliche Investitionen zu Beginn einer Migration auf lange Sicht erhebliche Einsparungen bringen.
2. Ziehen Sie die Implementierung von verwalteten Services wie Amazon RDS in Betracht, anstatt Ihre eigenen Technologiebereitstellungen zu installieren und zu verwalten.
3. Verwenden Sie die Anleitung zur Verantwortung in AWS Artifact, um die Sicherheitskontrollen zu bestimmen, die Sie für Ihre Workload einrichten sollten.
4. Führen Sie ein Inventar der genutzten Ressourcen und halten Sie sich über neue Services und Ansätze auf dem Laufenden, um neue Möglichkeiten zur Reduzierung des Umfangs zu ermitteln.

Ressourcen

Zugehörige bewährte Methoden:

- PERF02-BP01 Auswählen der besten Datenverarbeitungsoptionen für Ihre Workload
- PERF03-BP01 Verwenden eines speziell entwickelten Datenspeichers, der die Datenzugriffs- und Speicheranforderungen am besten unterstützt
- SUS05-BP03 Verwenden verwalteter Services

Zugehörige Dokumente:

- Planned lifecycle events for AWS Health

Zugehörige Tools:

- AWS Health
- AWS Artifact
- AWS Customer Compliance Guides

Zugehörige Videos:

- How do I migrate to an Amazon RDS or Aurora MySQL DB instance using AWS DMS?
- AWS re:Invent 2.023 - Manage resource lifecycle events at scale with AWS Health

SEC01-BP06 Automatisieren der Bereitstellung von Standard-Sicherheitskontrollen

Wenden Sie bei der Entwicklung und Bereitstellung von Sicherheitskontrollen, die in Ihren AWS-Umgebungen Standard sind, moderne DevOps-Verfahren an. Definieren Sie Standard-Sicherheitskontrollen und -konfigurationen mithilfe von Infrastructure as Code (IaC)-Vorlagen, erfassen Sie Änderungen in einem Versionskontrollsystem, testen Sie Änderungen als Teil einer CI/CD-Pipeline und automatisieren Sie die Bereitstellung von Änderungen in Ihren AWS-Umgebungen.

Gewünschtes Ergebnis: IaC-Vorlagen erfassen standardisierte Sicherheitskontrollen und übergeben sie an ein Versionskontrollsystem. CI/CD-Pipelines sind an Stellen vorhanden, die Änderungen erkennen und das Testen und Bereitstellen Ihrer AWS-Umgebungen automatisieren. Mechanismen zum Integritätsschutz erkennen und warnen vor Fehlkonfigurationen in Vorlagen, bevor die Bereitstellung erfolgt. Workloads werden in Umgebungen bereitgestellt, in denen Standardkontrollen vorhanden sind. Die Teams können genehmigte Servicekonfigurationen über einen Selfservice-Mechanismus bereitstellen. Die Strategien zur Gewährleistung der Sicherheit bei der Sicherung und Wiederherstellung von Kontrollkonfigurationen, Skripten und zugehörigen Daten sind etabliert.

Typische Anti-Muster:

- Manuelle Änderungen an Ihren Standard-Sicherheitskontrollen über eine Webkonsole oder eine Befehlszeilenschnittstelle.

- Sich darauf verlassen, dass die einzelnen Workload-Teams die von einem zentralen Team festgelegten Kontrollen manuell umsetzen.
- Sich auf ein zentrales Sicherheitsteam verlassen, das auf Anfrage eines Workload-Teams Kontrollen auf Workload-Ebene bereitstellt.
- Erlauben, dass dieselben Personen oder Teams Automatisierungsskripte für die Sicherheitskontrolle entwickeln, testen und bereitstellen, ohne dass eine angemessene Aufgabentrennung oder gegenseitige Kontrolle stattfindet.

Vorteile der Nutzung dieser bewährten Methode: Die Verwendung von Vorlagen zur Definition Ihrer Standard-Sicherheitskontrollen ermöglicht es Ihnen, Änderungen im Laufe der Zeit mithilfe eines Versionskontrollsystems zu verfolgen und zu vergleichen. Der Einsatz von Automatisierung zum Testen und Bereitstellen von Änderungen schafft Standardisierung und Vorhersehbarkeit, erhöht die Chancen auf eine erfolgreiche Bereitstellung und reduziert manuelle, sich wiederholende Aufgaben. Durch die Bereitstellung eines Selfservice-Mechanismus für Workload-Teams zur Bereitstellung genehmigter Services und Konfigurationen wird das Risiko von Fehlkonfigurationen und Missbrauch verringert. Das hilft ihnen auch dabei, Kontrollen früher in den Entwicklungsprozess einzubauen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Wenn Sie die in SEC01-BP01 Trennen von Workloads mithilfe von Konten beschriebenen Methoden befolgen, erhalten Sie am Ende mehrere AWS-Konten-Konten für verschiedene Umgebungen, die Sie mit AWS Organizations verwalten. Auch wenn jede dieser Umgebungen und Workloads unterschiedliche Sicherheitskontrollen erfordert, können Sie einige Sicherheitskontrollen in Ihrer Organisation standardisieren. Beispiele hierfür sind die Integration zentraler Identitätsanbieter, die Definition von Netzwerken und Firewalls und die Konfiguration von Standardorten für die Speicherung und Analyse von Protokollen. Analog zur Anwendung von Infrastructure as Code (IaC) zur Anwendung der gleichen strikten Vorgehensweise bei der Entwicklung von Anwendungscode auf die Bereitstellung der Infrastruktur können Sie IaC auch zur Definition und Bereitstellung Ihrer Standard-Sicherheitskontrollen verwenden.

Definieren Sie Ihre Sicherheitskontrollen nach Möglichkeit deklarativ, wie z. B. in AWS CloudFormation, und speichern Sie sie in einem Versionskontrollsystem. Nutzen Sie DevOps-Methoden, um die Bereitstellung Ihrer Kontrollen zu automatisieren und so besser vorhersehbare Releases, automatisierte Tests mit Tools wie AWS CloudFormation Guard und die Erkennung von Abweichungen zwischen Ihren bereitgestellten Kontrollen und der gewünschten Konfiguration zu

ermöglichen. Sie können Services wie AWS CodePipeline, AWS CodeBuild und AWS CodeDeploy verwenden, um eine CI/CD-Pipeline zu erstellen. Berücksichtigen Sie die Hinweise in Organizing Your AWS Environment Using Multiple Accounts, um diese Services in eigenen Konten separat von anderen Bereitstellungspipelines zu konfigurieren.

Sie können auch Vorlagen definieren, um die Definition und Bereitstellung von AWS-Konten, Services und Konfigurationen zu standardisieren. Diese Technik ermöglicht es einem zentralen Sicherheitsteam, diese Definitionen zu verwalten und sie den Workload-Teams über einen Selfservice-Ansatz zur Verfügung zu stellen. Eine Möglichkeit, dies zu erreichen, ist die Verwendung von Service Catalog, wo Sie Vorlagen als Produkte veröffentlichen können, die Workload-Teams in ihre eigenen Pipeline-Bereitstellungen einbinden können. Wenn Sie AWS Control Tower verwenden, sind einige Vorlagen und Kontrollen als Ausgangspunkt verfügbar. Control Tower bietet zudem die Funktion Account Factory, mit der Workload-Teams neue AWS-Konten-Konten unter Verwendung der von Ihnen definierten Standards erstellen können. Mit dieser Funktion sind Sie nicht mehr auf ein zentrales Team angewiesen, das neue Konten genehmigt und anlegt, wenn diese von Ihren Workload-Teams als notwendig erachtet werden. Sie benötigen diese Konten möglicherweise, um verschiedene Workload-Komponenten zu isolieren, z. B. aufgrund ihrer Funktion, der Sensibilität der verarbeiteten Daten oder ihres Verhaltens.

Implementierungsschritte

1. Legen Sie fest, wie Sie Ihre Vorlagen in einem Versionskontrollsystem speichern und pflegen wollen.
2. Erstellen Sie CI/CD-Pipelines zum Testen und Bereitstellen Ihrer Vorlagen. Definieren Sie Tests, um zu prüfen, ob Fehlkonfigurationen vorliegen und ob die Vorlagen den Standards Ihres Unternehmens entsprechen.
3. Erstellen Sie einen Katalog mit standardisierten Vorlagen für Workload-Teams zur Bereitstellung von AWS-Konten und -Services gemäß Ihren Anforderungen.
4. Implementieren Sie sichere Sicherungs- und Wiederherstellungsstrategien für die Konfiguration Ihrer Kontrollen, Skripte und zugehörigen Daten.

Ressourcen

Zugehörige bewährte Methoden:

- OPS05-BP01 Verwendung von Versionskontrolle
- OPS05-BP04 Einsatz von Systemen zur Build- und Bereitstellungsverwaltung

- REL08-BP05 Automatisieren von Änderungen
- SUS06-BP01 Einführen von Methoden, die schnelle Verbesserungen für die Nachhaltigkeit ermöglichen

Zugehörige Dokumente:

- Organisieren Sie Ihre AWS-Umgebung mit mehreren Konten

Zugehörige Beispiele:

- Automate account creation, and resource provisioning using Service Catalog, AWS Organizations, and AWS Lambda
- Strengthen the DevOps pipeline and protect data with AWS Secrets Manager, AWS KMS, and AWS Certificate Manager

Zugehörige Tools:

- AWS CloudFormation Guard
- Landing Zone Accelerator in AWS

SEC01-BP07 Identifizieren von Bedrohungen und Priorisieren von Abhilfemaßnahmen unter Verwendung eines Bedrohungsmodells

Führen Sie Bedrohungsmodellierungen zur Identifizierung und Pflege eines aktuellen Registers potenzieller Bedrohungen und entsprechender Abhilfemaßnahmen für Ihre Workload durch. Priorisieren Sie Ihre Bedrohungen und passen Sie Ihre Sicherheitskontrollen an, um zu verhindern, zu erkennen und zu reagieren. Überarbeiten und halten Sie diese Methoden im Kontext Ihrer Workload und der sich entwickelnden Sicherheitslandschaft aktuell.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Was versteht man unter Bedrohungsmodellierung?

„Bedrohungsmodellierung dient der Identifizierung, Kommunikation und dem Verständnis von Bedrohungen und Abhilfemaßnahmen im Kontext des Schutzes von etwas Wertvollem.“ – The Open Web Application Security Project (OWASP) über Bedrohungsmodellierung für Anwendungen

Wozu dient die Bedrohungsmodellierung?

Systeme sind komplex und werden mit der Zeit immer komplexer und leistungsfähiger. Gleichzeitig liefern sie immer mehr geschäftlichen Wert und verbessern die Kundenzufriedenheit und -bindung. Dies bedeutet, dass Entscheidungen zum IT-Design immer mehr Anwendungsfälle berücksichtigen müssen. Diese Komplexität und die zunehmende Zahl der Anwendungsfälle macht unstrukturierte Konzepte ineffektiv, wenn es um das Erkennen und Bekämpfen von Bedrohungen geht. Stattdessen wird ein systematisches Konzept benötigt, das die potenziellen Bedrohungen für ein System aufführen und Abhilfemaßnahmen benennen und priorisieren kann, um sicherzustellen, dass die begrenzten Ressourcen einer Organisation in maximaler Weise in der Lage sind, die Sicherheitslage des Systems insgesamt zu verbessern.

Die Bedrohungsmodellierung dient zum Aufbau eines solchen systematischen Konzepts, damit Probleme frühzeitig im Designprozess erkannt und angegangen werden können, so lange Abhilfemaßnahmen noch mit niedrigen relativen Kosten und geringem Aufwand verbunden sind, was später im Lebenszyklus nicht mehr der Fall ist. Dieses Konzept entspricht dem Branchenprinzip des Shift-Left-Sicherheitsansatzes. Letztendlich ist die Bedrohungsmodellierung in den Risikomanagementprozess einer Organisation integriert und hilft mit einem auf Bedrohungen ausgerichteten Konzept bei Entscheidungen dazu, welche Kontrollmechanismen zu implementieren sind.

Wann sollte eine Bedrohungsmodellierung durchgeführt werden?

Beginnen Sie mit der Bedrohungsmodellierung so früh wie möglich im Lebenszyklus Ihrer Workload. Dies gibt Ihnen die benötigte Flexibilität im Umgang mit den identifizierten Bedrohungen. Wie bei Softwarebugs gilt auch hier: Je früher Sie Bedrohungen identifizieren, desto kostengünstiger ist es, sie zu beheben. Ein Bedrohungsmodell ist ein lebendiges Dokument, dass stetig weiterentwickelt werden sollte, während sich Ihre Workloads verändern. Überprüfen Sie regelmäßig Ihre Bedrohungsmodelle, vor allem bei größeren Änderungen, bei Änderungen der Bedrohungslandschaft, oder wenn Sie neue Features oder Services einführen.

Implementierungsschritte

Wie wird die Bedrohungsmodellierung durchgeführt?

Es gibt viele verschiedene Möglichkeiten zur Durchführung von Bedrohungsmodellierungen. Ähnlich wie bei Programmiersprachen gibt es Vor- und Nachteile und Sie sollten den Ansatz wählen, der für Sie am besten funktioniert. Ein Konzept besteht darin, mit Shostack's 4 Question Frame for Threat Modeling zu beginnen, das aus offenen Fragen besteht, die Ihre Bedrohungsmodellierung strukturieren:

1. Woran arbeiten wir?

   Diese Frage dient dazu, das von Ihnen aufgebaute System sowie die sicherheitsrelevanten Details zu diesem System zu verstehen. Für die Beantwortung dieser Frage ist es üblich, ein Modell oder Diagramm zur Visualisierung dessen aufzustellen, was aufgebaut wird, etwa in Gestalt eines Datenflussdiagramms. Das Aufschreiben von Annahmen und wichtigen Details zum System hilft ebenfalls beim Verständnis des Umfangs. Dadurch können sich alle, die zum Bedrohungsmodell beitragen, auf dasselbe konzentrieren und zeitraubende Umwege über irrelevante Themen (wie etwa veraltete Versionen des Systems) vermeiden. Wenn Sie beispielsweise eine Web-Anwendung erstellen, ist es wahrscheinlich nicht relevant, sich um die Bedrohungsmodellierung im Zusammenhang mit der Bootsequenz für Browser-Clients in vertrauenswürdigen Betriebssystemen zu kümmern, da Sie darauf ohnehin keinen Einfluss haben.
2. Was kann schief gehen?

   Hier identifizieren Sie die Bedrohungen für Ihr System. Bedrohungen sind versehentliche oder beabsichtigte Handlungen oder Ereignisse, die unerwünschte Folgen haben und die Sicherheit Ihres Systems beeinträchtigen können. Ohne ein klares Verständnis dessen, was schief gehen kann, haben Sie keine Möglichkeit, etwas dagegen zu unternehmen.

   Es gibt keine kanonische Liste dessen, was schief gehen kann. Die Erstellung dieser Liste erfordert Brainstorming und die Zusammenarbeit all Ihrer Teammitglieder und der relevanten Beteiligten an der Bedrohungsmodellierung. Sie können das Brainstorming unterstützen, indem Sie ein Modell zur Identifizierung von Bedrohungen verwenden, z. B. STRIDE, das verschiedene Kategorien zur Bewertung anbietet: Spoofing, Manipulation, Zurückweisung, Offenlegung von Informationen, Denial of Service und Erhöhung der Berechtigung. Dazu sollten Sie zur Inspiration vorhandene Listen und Forschungsergebnisse heranziehen, etwa die OWASP Top 10, den HiTrust Threat Catalog und den eigenen Bedrohungskatalog Ihrer Organisation.
3. Wie gehen wir damit um?

   Wie schon bei der vorherigen Frage gibt es auch hier keine kanonische Liste möglicher Abhilfemaßnahmen. Die Inputs für diesen Schritt sind die identifizierten Bedrohungen, Akteure und Verbesserungsbereiche aus dem vorherigen Schritt.

Sicherheit und Compliance unterliegen der geteilten Verantwortung zwischen Ihnen und AWS. Der Frage „Wie gehen wir damit um?“ sollte unbedingt die Frage „Wer ist für die Maßnahmen verantwortlich?“ angeschlossen werden. Das Verständnis der Verantwortungsverteilung zwischen Ihnen und AWS hilft Ihnen bei der Anpassung der Bedrohungsmodellierung an die Abhilfemaßnahmen, die Ihrer Kontrolle unterliegen und in der Regel aus einer Kombination aus AWS-Servicekonfigurationsoptionen und Ihren eigenen systemspezifischen Abhilfemaßnahmen bestehen.

Für den AWS-Teil der geteilten Verantwortung werden Sie feststellen, dass AWS-Services in den Bereich vieler Compliance-Programme fallen. Diese Programme helfen Ihnen, sich mit den zuverlässigen Kontrollmöglichkeiten bei AWS zur Sicherheitswahrung und Compliance in der Cloud vertraut zu machen. Die Audit-Berichte dieser Programme stehen für AWS-Kunden von AWS Artifact zum Download zur Verfügung.

Unabhängig davon, welche AWS-Services Sie nutzen, gibt es immer ein Element der Kundenverantwortung, und an diese Verantwortungen angepasste Abhilfemaßnahmen sollten Teil Ihres Bedrohungsmodells sein. Für Sicherheitskontrollabhilfen für die AWS-Services selbst sollten Sie die Implementierung von Sicherheitskontrollen über Domains hinweg erwägen, einschließlich Domains wie Identitäts- und Zugriffsmanagement (Authentifizierung und Autorisierung), Datenschutz (im Ruhezustand und während der Übertragung), Infrastruktursicherheit, Protokollierung und Überwachung. Die Dokumentation für jeden AWS-Service enthält ein spezielles Sicherheitskapitel mit Anleitungen zu den Sicherheitskontrollen, die Abhilfemaßnahmen unterstützen können. Wichtig ist, dass Sie den Code, den Sie schreiben, und dessen Abhängigkeiten berücksichtigen und an Kontrollen denken, die Sie für den Umgang mit den damit verbundenen Bedrohungen implementieren können. Bei diesen Kontrollen könnte es sich um Dinge wie Eingabevalidierung, Sitzungsabwicklung und Umgang mit Grenzen handeln. Oft ist der Löwenanteil der Bedrohungen mit benutzerdefiniertem Code verbunden, konzentrieren Sie sich also besonders darauf.

4. Haben wir gute Arbeit geleistet?

   Ihr Team und die Organisation verfolgen das Ziel, die Qualität der Bedrohungsmodelle und die Geschwindigkeit zu verbessern, mit der Sie die Bedrohungsmodellierung im Laufe der Zeit durchführen. Diese Verbesserungen werden durch eine Kombination von Praxis, Lernen, Lehren und Prüfen ermöglicht. Um dies zu vertiefen und praktisch umzusetzen, sollten Sie und Ihr Team den Trainingskurs zum Thema Korrekte Bedrohungsmodellierung für Builder oder den dazugehörigen Workshop absolvieren. Wenn Sie nach Anleitungen zur Integration der Bedrohungsmodellierung in den Anwendungsentwicklungslebenszyklus Ihrer Organisation suchen,

beachten Sie auch den Beitrag zum Thema Bedrohungsmodellierungskonzepte im AWS-Blog zu Sicherheit.

Threat Composer

Zur Unterstützung und Anleitung bei der Erstellung von Bedrohungsmodellen können Sie das Threat Composer-Tool verwenden, das darauf ausgerichtet ist, bei der Erstellung von Bedrohungsmodellen die Zeit bis zur Wertschöpfung zu verkürzen. Das Tool hilft Ihnen bei den folgenden Aufgaben:

- Verfassen nützlicher, an Bedrohungsgrammatik ausgerichtete Bedrohungsanweisungen, die in einem natürlichen, nicht-linearen Arbeitsablauf funktionieren.
- Generieren Sie ein für Menschen lesbares Bedrohungsmodell.
- Generieren Sie ein maschinenlesbares Bedrohungsmodell, damit Sie Bedrohungsmodelle wie Code behandeln können.
- Mit dem Insights-Dashboard können Sie schnell Bereiche identifizieren, in denen die Qualität und die Abdeckung verbessert werden müssen.

Für weitere Informationen rufen Sie Threat Composer auf und wechseln Sie zum systemdefinierten Beispielarbeitsbereich.

Ressourcen

Zugehörige bewährte Methoden:

- SEC01-BP03 Identifizieren und Validieren von Kontrollzielen
- SEC01-BP04 Sicherstellen der Aktualität von Informationen zu Sicherheitsbedrohungen
- SEC01-BP05 Verringern des Umfangs der Sicherheitsverwaltung
- SEC01-BP08 Regelmäßiges Bewerten und Implementieren neuer Sicherheitsservices und -features

Zugehörige Dokumente:

- How to approach threat modeling (AWS-Blog zum Thema Sicherheit)
- NIST: Guide to Data-Centric System Threat modeling

Zugehörige Videos:

- AWS Summit ANZ 2021 - How to approach threat modeling
- AWS Summit ANZ 2.022 - Scaling security – Optimise for fast and secure delivery

Zugehörige Schulungen:

- Threat modeling the right way for builders – virtuelle AWS Skill Builder-Schulung zum Selbststudium
- Threat modeling the right way for builders – AWS Workshop

Zugehörige Tools:

- Threat Composer

SEC01-BP08 Regelmäßiges Bewerten und Implementieren neuer Sicherheitsservices und -features

Bewerten und implementieren Sie Sicherheitsservices und -features von AWS und AWS-Partnern, mit denen Sie die Sicherheitsstrategie für Ihre Workload weiterentwickeln können.

Gewünschtes Ergebnis: Sie verfügen über eine Standardmethode, die Sie über neue Features und Services informiert, die von AWS und AWS-Partnern veröffentlicht werden. Sie bewerten, wie sich diese neuen Funktionen auf das Design der aktuellen und neuen Kontrollen für Ihre Umgebungen und Workloads auswirken.

Typische Anti-Muster:

- Sie abonnieren keine Blogs und RSS-Feeds von AWS, um schnell von relevanten neuen Features und Servicesn zu erfahren
- Sie verlassen sich auf Nachrichten und Updates über Sicherheitsservices und Features aus zweiter Hand
- Sie halten AWS-Benutzer in Ihrer Organisation nicht dazu an, sich über die neuesten Updates zu informieren

Vorteile der Nutzung dieser bewährten Methode: Indem Sie sich über neue Sicherheitsservices und Features auf dem Laufenden halten, können Sie fundierte Entscheidungen über die Implementierung von Kontrollen in Ihren Cloud-Umgebungen und Workloads treffen. Diese Quellen tragen dazu bei,

das Bewusstsein für die sich entwickelnde Sicherheitslandschaft zu schärfen und zu zeigen, wie AWS-Services zum Schutz vor neuen und aufkommenden Bedrohungen genutzt werden können.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

Implementierungsleitfaden

AWS informiert Kunden über neue Sicherheitsservices und Features über verschiedene Kanäle:

- AWS Neuerungen bei
- AWS News Blog
- AWS Blog zum Thema Sicherheit
- AWS Sicherheitsberichte
- AWS Überblick über die -Dokumentation

Sie können ein Thema der AWS Daily Feature Updates mit Amazon Simple Notification Service (Amazon SNS) abonnieren, um eine umfassende tägliche Zusammenfassung der Updates zu erhalten. Einige Sicherheitsservices wie Amazon GuardDuty und AWS Security Hub CSPM bieten ihre eigenen SNS-Themen an, um über neue Standards, Erkenntnisse und andere Aktualisierungen für diese speziellen Services informiert zu bleiben.

Neue Services und Features werden auch auf Konferenzen, Veranstaltungen und Webinaren, die jedes Jahr rund um den Globus stattfinden, angekündigt und im Detail beschrieben. Besonders interessant ist dabei die jährliche Sicherheitskonferenz AWS re:Inforce und die breiter angelegte Konferenz AWS re:Invent. In den bereits erwähnten AWS-Nachrichtenkanälen werden diese Konferenzankündigungen über Sicherheit und andere Services geteilt, und Sie können sich Deep Dive Breakout Sessions online auf dem YouTube-Kanal AWS Events ansehen.

Sie können auch Ihr AWS-Konto-Team nach den neuesten Updates und Empfehlungen für Sicherheitsservices fragen. Sie können Ihr Team über das Verkaufssupport-Formular erreichen, wenn Ihnen dessen direkte Kontaktinformationen nicht vorliegen. Gleichermaßen erhalten Sie, wenn Sie AWS Enterprise-Support abonniert haben, wöchentliche Updates von Ihrem Technical Account Manager (TAM) und können ein regelmäßiges Review-Meeting mit ihm vereinbaren.

Implementierungsschritte

1. Abonnieren Sie die verschiedenen Blogs und Bulletins mit Ihrem bevorzugten RSS-Reader oder die SNS-Thema Daily Features Updates.

2. Überlegen Sie, welche AWS-Veranstaltungen Sie besuchen sollten, um sich aus erster Hand über neue Features und Services zu informieren.
3. Vereinbaren Sie Besprechungen mit Ihrem AWS-Konto-Team für alle Fragen zur Aktualisierung von Sicherheitsservices und -features.
4. Ziehen Sie in Erwägung, den Enterprise Support zu abonnieren, um regelmäßige Konsultationen mit einem Technical Account Manager (TAM) zu erhalten.

Ressourcen

Zugehörige bewährte Methoden:

- PERF01-BP01 Informieren über verfügbare Cloud-Services und -Features
- COST01-BP07 Verfolgen neuer Serviceversionen

Identity and Access Management

Gewähren Sie Ihren Benutzern und Anwendungen Zugriff auf die Ressourcen in Ihren AWS-Konten, um AWS-Services nutzen zu können. Wenn Sie mehr Workloads in AWS ausführen, benötigen Sie eine robuste Identitätsverwaltung und Berechtigungen, um sicherzustellen, dass die richtigen Personen unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. AWS bietet eine große Auswahl an Funktionen, die Sie bei der Verwaltung Ihrer menschlichen und maschinellen Identitäten und deren Berechtigungen unterstützen. Die bewährten Methoden für diese Funktionen sind in zwei Hauptbereiche unterteilt.

Themen

Identitätsverwaltung

Es gibt zwei Arten von Identitäten, die Sie für den Betrieb von sicheren AWS-Workloads verwalten müssen.

- Menschliche Identitäten: Die menschlichen Identitäten, die Zugriff auf Ihre AWS-Umgebungen und -Anwendungen benötigen, können in drei Gruppen eingeteilt werden: Belegschaft, Dritte und Benutzer.

  Zur Gruppe Belegschaft gehören Administratoren, Entwickler und Betreiber, die Mitglieder Ihrer Organisation sind. Diese benötigen Zugriff, um Ihre AWS-Ressourcen verwalten, erstellen und betreiben zu können.

  Dritte sind externe Mitarbeiter wie Auftragnehmer, Anbieter oder Partner. Diese interagieren im Rahmen ihrer Zusammenarbeit mit Ihrer Organisation mit Ihren AWS-Ressourcen.

  Benutzer sind die Nutzer Ihrer Anwendungen. Diese greifen über Webbrowser, Client-Anwendungen, Mobil-Apps oder interaktive Befehlszeilentools auf Ihre AWS-Ressourcen zu.
- Maschinenidentitäten: Ihre Workload-Anwendungen, betrieblichen Tools und Komponenten benötigen eine Identität, um Anforderungen an AWS-Services zu stellen, z. B. um Daten zu lesen. Zu diesen Identitäten gehören auch Maschinen, die in Ihrer AWS-Umgebung ausgeführt werden, wie z. B. Amazon-EC2-Instances oder AWS Lambda-Funktionen. Sie können auch

Maschinenidentitäten für externe Parteien oder Maschinen außerhalb von AWS verwalten, die Zugriff auf Ihre AWS-Umgebung benötigen.

Bewährte Methoden

- SEC02-BP01 Verwenden von starken Anmeldemechanismen
- SEC02-BP02 Verwenden von temporären Anmeldeinformationen
- SEC02-BP03 Sicheres Speichern und Verwenden von Secrets
- SEC02-BP04 Verlassen auf einen zentralen Identitätsanbieter
- SEC02-BP05 Regelmäßiges Überprüfen und Rotieren von Anmeldeinformationen
- SEC02-BP06 Nutzen von Benutzergruppen und Attributen

SEC02-BP01 Verwenden von starken Anmeldemechanismen

Anmeldungen (Authentifizierung unter Verwendung von Anmeldeinformationen) können risikobehaftet sein, wenn nicht Mechanismen wie die Multi-Faktor-Authentifizierung (MFA) verwendet werden, besonders in Situationen, in denen Anmeldeinformationen unbeabsichtigt offengelegt wurden oder leicht zu erraten sind. Verwenden Sie starke Anmeldemechanismen in Form von MFA und Richtlinien für sichere Passwörter, um diese Risiken zu reduzieren.

Gewünschtes Ergebnis: Reduzieren Sie das Risiko eines unbeabsichtigten Zugriffs auf Anmeldeinformationen in AWS, indem Sie starke Anmeldemechanismen für AWS Identity and Access Management (IAM)-Benutzer, den AWS-KontoRoot-Benutzer, AWS IAM Identity Center und externe Identitätsanbieter verwenden. Dies bedeutet das Erfordern von MFA, das Durchsetzen von Richtlinien zur Verwendung starker Passwörter und das Erkennen anomaler Anmeldeverhaltensweisen.

Typische Anti-Muster:

- Keine Durchsetzung einer Richtlinie zur Verwendung starker Passwörter für Ihre Identitäten, einschließlich komplexer Passwörter und MFA.
- Gemeinsame Nutzung derselben Anmeldeinformationen durch mehrere Benutzer.
- Keine Verwendung von detektivischen Kontrollen für verdächtige Anmeldevorgänge.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Es gibt mehrere Möglichkeiten zur Anmeldung bei AWS für menschliche Identitäten. Eine bewährte AWS-Methode besteht darin, einen zentralisierten Identitätsanbieter mit Verbundverfahren (direkter SAML-2.0-Verbund zwischen AWS IAM und dem zentralisierten Identitätsanbieter oder Verwendung von AWS IAM Identity Center) für die Authentifizierung bei AWS zu verwenden. Richten Sie in diesem Fall einen sicheren Anmeldevorgang mit Ihrem Identitätsanbieter oder Microsoft Active Directory ein.

Wenn Sie ein AWS-Konto zum ersten Mal einrichten, beginnen Sie mit einem Root-Benutzer für das AWS-Konto. Sie sollten den Root-Benutzer nur verwenden, um den Zugriff für Ihre Benutzer einzurichten (und für Aufgaben, für die der Root-Benutzer erforderlich ist). Es ist wichtig, die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer des Kontos sofort nach dem Öffnen Ihres AWS-Kontos zu aktivieren und den Root-Benutzer unter Berücksichtigung des AWS-Leitfadens für bewährte Methoden zu sichern.

AWS IAM Identity Center wurde für Belegschaftsbenutzer konzipiert. Sie können Benutzeridentitäten innerhalb des Service erstellen und verwalten und den Anmeldevorgang mit MFA sichern. AWS Cognito dagegen wurde für Customer Identity and Access Management (CIAM) entwickelt, das Benutzerpools und Identitätsanbieter für externe Benutzeridentitäten in Ihren Anwendungen bereitstellt.

Wenn Sie in AWS IAM Identity Center Benutzer erstellen, sollten Sie den Anmeldevorgang in diesem Service schützen und MFA aktivieren. Für externe Benutzeridentitäten in Ihren Anwendungen können Sie Amazon-Cognito-Benutzerpools verwenden und den Anmeldevorgang in diesem Service oder über einen der unterstützten Identitätsanbieter in Amazon-Cognito-Benutzerpools sichern.

Darüber hinaus können Sie für Benutzer in AWS IAM Identity Center unter Verwendung von AWS Verified Access eine zusätzliche Sicherheitsebene bereitstellen, indem Sie die Identität der Benutzers und den Gerätestatus überprüfen, bevor ihnen Zugriff auf AWS-Ressourcen gewährt wird.

Wenn Sie AWS Identity and Access Management (IAM)-Benutzer verwenden, sichern Sie den Anmeldevorgang mit IAM.

Sie können AWS IAM Identity Center und den direkten IAM-Verbund gleichzeitig verwenden, um den Zugriff auf AWS zu verwalten. Sie können den IAM-Verbund für die Verwaltung des Zugriffs auf die AWS-Managementkonsole und die Services und IAM Identity Center für die Verwaltung des Zugriffs auf Geschäftsanwendungen wie QuickSight oder Amazon Q Business verwenden.

Unabhängig vom Anmeldeverfahren ist es wichtig, eine strenge Anmelderichtlinie durchzusetzen.

Implementierungsschritte

Es folgen allgemeine Empfehlungen für starke Anmeldeverfahren. Die tatsächlichen Einstellungen, die Sie konfigurieren, sollten Ihren Unternehmensrichtlinien oder einem Standard wie NIST 800-63 entsprechen.

- MFA erforderlich. Es ist eine bewährte IAM-Methode, MFA für menschliche Identitäten und Workloads zu erfordern. Die Aktivierung von MFA bietet eine zusätzliche Sicherheitsebene, die verlangt, dass Benutzer Anmeldeinformationen und ein Einmalpasswort (OTP) oder eine kryptographisch verifizierte und generierte Zeichenfolge von einem Hardware-Gerät vorlegen.
- Verlangen Sie eine Mindestlänge für Passwörter als primären Faktor für die Passwortstärke.
- Verlangen Sie Passwortkomplexität, um das Erraten von Passwörtern zu erschweren.
- Ermöglichen Sie Benutzern, ihre eigenen Passwörter zu ändern.
- Erstellen Sie individuelle Identitäten anstelle gemeinsam genutzter Anmeldeinformationen. Da Sie individuelle Identitäten erstellen, können Sie jedem Benutzer eindeutige Anmeldeinformationen zuordnen. Individuelle Benutzer bieten die Möglichkeit, die Aktivität der einzelnen Benutzer zu prüfen.

Empfehlungen für IAM Identity Center:

- IAM Identity Center bietet bei Verwendung des Standardverzeichnisses eine vordefinierte Passwortrichtlinie, die Anforderungen an die Länge, Komplexität und Wiederverwendung von Passwörtern festlegt.
- Aktivieren Sie MFA und konfigurieren Sie die kontextsensitive oder „always-on“-Einstellung für MFA, wenn die Identitätsquelle das Standardverzeichnis, AWS Managed Microsoft AD oder AD Connector ist.
- Erlauben Sie Benutzern, ihre eigenen MFA-Geräte zu registrieren.

Empfehlungen für Verzeichnisse der Amazon Cognito-Benutzerpools:

- Konfigurieren Sie die Einstellungen für die Passwortstärke.
- Erfordern Sie MFA für Benutzer.
- Verwenden Sie die erweiterten Sicherheitseinstellungen der Amazon Cognito-Benutzerpools für Features wie die adaptive Authentifizierung, mit der verdächtige Anmeldungen blockiert werden können.

Empfehlungen für IAM-Benutzer:

- Idealerweise verwenden Sie IAM Identity Center oder den direkten Verbund. Möglicherweise benötigen Sie aber auch IAM-Benutzer. Legen Sie in diesem Fall eine Passwortrichtlinie für IAM-Benutzer fest. Sie können die Passwortrichtlinie verwenden, um Anforderungen wie die Mindestlänge zu definieren oder ob das Passwort nicht-alphanumerische Zeichen beinhalten sollte.
- Erstellen Sie eine IAM-Richtlinie, um die MFA-Anmeldung zu erzwingen, sodass Benutzer ihre eigenen Passwörter und MFA-Geräte verwalten können.

Ressourcen

Zugehörige bewährte Methoden:

- SEC02-BP03 Sicheres Speichern und Verwenden von Secrets
- SEC02-BP04 Verlassen auf einen zentralen Identitätsanbieter
- SEC03-BP08 Sicheres gemeinsames Nutzen von Ressourcen in Ihrer Organisation

Zugehörige Dokumente:

- Passwortrichtlinie von AWS IAM Identity Center
- Passwortrichtlinie für IAM-Benutzer
- Festlegen des Passworts des AWS-Konto-Root-Benutzers
- Amazon-Cognito-Passwortrichtlinie
- AWS-Anmeldeinformationen
- Bewährte IAM-Sicherheitsmethoden

Zugehörige Videos:

- Verwaltung von Benutzerberechtigungen in großem Umfang mit AWS IAM Identity Center
- Beherrschen der Identität auf jeder Ebene

SEC02-BP02 Verwenden von temporären Anmeldeinformationen

Bei Authentifizierungen jeder Art, sollten am besten temporäre anstelle langfristiger Anmeldeinformationen verwendet werden, um Risiken zu reduzieren oder zu eliminieren, etwa durch die unbeabsichtigte Offenlegung, die Weitergabe oder den Diebstahl von Anmeldeinformationen.

Gewünschtes Ergebnis: Um das Risiko langfristiger Anmeldeinformationen zu verringern, sollten Sie nach Möglichkeit sowohl für menschliche als auch für maschinelle Identitäten temporäre Anmeldeinformationen verwenden. Langfristige Anmeldeinformationen sind mit vielen Risiken verbunden. So kann es beispielsweise zu einer Offenlegung durch Uploads in öffentliche Repositorys kommen. Durch die Verwendung temporärer Anmeldeinformationen können Sie die Gefahr, dass Anmeldeinformationen kompromittiert werden, deutlich senken.

Typische Anti-Muster:

- Entwickler verwenden langfristige Zugriffsschlüssel von IAM-Benutzern, anstatt sich temporäre Anmeldeinformationen per Verbund von der CLI zu beschaffen.
- Entwickler betten langfristige Zugriffsschlüssel in ihren Code ein und laden diese in öffentliche Git-Repositorys hoch.
- Entwickler betten langfristige Zugriffsschlüssel in Mobil-Apps ein, die dann in App-Stores verfügbar gemacht werden.
- Benutzer geben langfristige Zugriffsschlüssel an andere Benutzer weiter, oder Mitarbeiter verlassen das Unternehmen und besitzen weiterhin langfristige Zugriffsschlüssel.
- Es werden langfristige Zugriffsschlüssel für Maschinenidentitäten genutzt, obwohl temporäre Anmeldeinformationen verwendet werden könnten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Verwenden Sie temporäre anstelle langfristiger Anmeldeinformationen für alle AWS-API- und -CLI-Anfragen. API- und CLI-Anfragen an AWS-Services müssen in fast allen Fällen mit AWS-Zugriffsschlüsseln signiert werden. Diese Anfragen können mit temporären oder langfristigen Anmeldeinformationen signiert werden. Langfristige Anmeldeinformationen – auch als langfristige Zugriffsschlüssel bezeichnet – sollten Sie nur verwenden, wenn Sie einen IAM-Benutzer oder den AWS-Konto-Root-Benutzer verwenden. Wenn Sie auf andere Weise einen Verbund mit AWS herstellen oder eine IAM-Rolle übernehmen, werden temporäre Anmeldeinformationen generiert. Selbst wenn Sie mit Anmeldeinformationen auf die AWS-Managementkonsole zugreifen, werden für

Sie temporäre Anmeldeinformationen für Aufrufe von AWS-Services generiert. Es gibt nur wenige Situationen, in denen Sie langfristige Anmeldeinformationen benötigen, und fast alle Aufgaben lassen sich mit temporären Anmeldeinformationen erledigen.

Das Vermeiden der Verwendung langfristiger zugunsten temporärer Anmeldeinformationen sollte von einer Strategie zur Reduzierung der Verwendung von IAM-Benutzern gegenüber Verbundverfahren und IAM-Rollen begleitet werden. Zwar wurden früher IAM-Benutzer für menschliche und maschinelle Identitäten verwendet, wir empfehlen heute jedoch, dies nicht mehr zu tun, um die mit der Verwendung langfristiger Zugriffsschlüssel verbundenen Risiken zu vermeiden.

Implementierungsschritte

Menschliche Identitäten

Für Identitäten der Belegschaft wie Mitarbeiter, Administratoren, Entwickler und Bediener:

- Wir empfehlen Ihnen, sich auf einen zentralen Identitätsanbieter zu verlassen und menschliche Benutzer aufzufordern, den Verbund mit einem Identitätsanbieter zu verwenden, um mit temporären Anmeldeinformationen auf AWS zuzugreifen. Der Verbund für Ihre Benutzer kann entweder in Form eines direkten Verbunds mit jedem AWS-Konto oder unter Verwendung von AWS IAM Identity Center und dem Identitätsanbieter Ihrer Wahl erfolgen. Ein Verbund bietet eine Reihe von Vorteilen gegenüber der Verwendung von IAM-Benutzern und eliminiert langfristige Anmeldeinformationen. Ihre Benutzer können auch temporäre Anmeldeinformationen über die Befehlszeile für den direkten Verbund oder mithilfe von IAM Identity Center anfordern. Dies bedeutet, dass es nur wenige Anwendungsfälle gibt, für die IAM-Benutzer oder langfristige Anmeldeinformationen für Ihre Benutzer erforderlich sind.

Für externe Identitäten:

- Wenn Sie Dritten – etwa Software as a Service (SaaS)-Anbietern – Zugriff auf Ressourcen in Ihrem AWS-Konto gewähren, können Sie kontoübergreifende Rollen und ressourcenbasierte Richtlinien verwenden. Darüber hinaus können Sie den Flow zum Erteilen von Client-Anmeldeinformationen in Amazon Cognito OAuth 2.0 für B2B-SaaS-Kunden oder -Partner verwenden.

Benutzeridentitäten, die über Web-Browser, Client-Anwendungen, mobile Apps oder interaktive Befehlszeilentools auf Ihre AWS-Ressourcen zugreifen:

- Wenn Sie Anwendungen für Verbraucher oder Kunden Zugriff auf Ihre AWS-Ressourcen gewähren müssen, können Sie Amazon Cognito-Identitätspools oder Amazon Cognito-Benutzerpools

verwenden, um temporäre Anmeldeinformationen bereitzustellen. Die Berechtigungen für die Anmeldeinformationen werden über IAM-Rollen konfiguriert. Darüber hinaus können Sie eine separate IAM-Rolle mit beschränkten Berechtigungen für Gastbenutzer anlegen, die nicht authentifiziert wurden.

Maschinenidentitäten

Für Maschinenidentitäten müssen Sie möglicherweise langfristige Anmeldeinformationen verwenden. In diesen Fällen sollten Sie Workloads auffordern, temporäre Anmeldeinformationen mit IAM-Rollen für den Zugriff auf AWS zu verwenden.

- Für Amazon Elastic Compute Cloud (Amazon EC2) können Sie Rollen für Amazon EC2 verwenden.
- AWS Lambda ermöglicht es Ihnen, eine Lambda-Ausführungsrolle zu konfigurieren, um dem Service Berechtigungen zu gewähren, die die Ausführung von AWS-Aktionen mit temporären Anmeldeinformationen erlauben. Es gibt zahlreiche ähnliche Modelle für AWS-Services zum Gewähren temporärer Anmeldeinformationen mit IAM-Rollen.
- Für IoT-Geräte können Sie den AWS IoT Core-Anmeldeinformationsanbieter verwenden, um temporäre Anmeldeinformationen anzufordern.
- Für On-Premises-Systeme oder Systeme, die außerhalb von AWS ausgeführt werden und Zugriff auf AWS-Ressourcen benötigen, können Sie IAM Roles Anywhere verwenden.

Es gibt Szenarien, in denen temporäre Anmeldeinformationen nicht unterstützt werden und langfristige Anmeldeinformationen verwendet werden müssen. In diesen Situationen sollten diese Anmeldeinformationen regelmäßig überprüft und rotiert und Zugriffsschlüssel regelmäßig rotiert werden. Bei stark eingeschränkten Zugriffsschlüsseln für IAM-Benutzer sollten Sie die folgenden zusätzlichen Sicherheitsmaßnahmen in Betracht ziehen:

- Erteilung stark eingeschränkter Berechtigungen:
  - Halten Sie sich an das Prinzip der geringsten Berechtigung (machen Sie konkrete Angaben zu Aktionen, Ressourcen und Bedingungen).
  - Erwägen Sie, dem IAM-Benutzer nur die Operation „AssumeRole“ für eine bestimmte Rolle zu gewähren. Abhängig von der On-Premises-Architektur hilft dieser Ansatz, die langfristigen IAM-Anmeldeinformationen zu isolieren und zu sichern.
- Beschränken Sie die zulässigen Netzwerkquellen und IP-Adressen in der Vertrauensrichtlinie für IAM-Rollen.

- Überwachen Sie die Nutzung und richten Sie Warnmeldungen bei ungenutzten Berechtigungen oder missbräuchlicher Verwendung ein (unter Verwendung der Metrikfilter und Alarme von AWS CloudWatch Logs).
- Setzen Sie Berechtigungsgrenzen durch (Service-Kontrollrichtlinien (SCPs) und Berechtigungsgrenzen ergänzen sich gegenseitig – SCPs sind weniger stark differenziert, Berechtigungsgrenzen dagegen stärker differenziert).
- Implementieren Sie einen Prozess zur Bereitstellung und sicheren Speicherung der Anmeldeinformationen (in einem On-Premises-Tresor).

Einige weitere Optionen für Szenarien, in denen langfristige Anmeldeinformationen erforderlich sind:

- Erstellen Ihrer eigenen API für die Token-Vergabe (mit Amazon API Gateway).
- In Situationen, in denen Sie langfristige Anmeldeinformationen oder andere Anmeldeinformationen als AWS-Zugriffsschlüssel verwenden müssen (z. B. Datenbankanmeldungen), können Sie einen Service verwenden, der für die Verwaltung von Secrets konzipiert ist, wie etwa AWS Secrets Manager. Secrets Manager vereinfacht die Verwaltung, Rotation und sichere Speicherung verschlüsselter Secrets. Viele AWS-Services unterstützen eine direkte Integration mit Secrets Manager.
- Für Multi-Cloud-Integrationen können Sie einen Identitätsverbund auf der Grundlage Ihrer Quell-CSP-Anmeldeinformationen (CSP = Credential Service Provider) verwenden (siehe AWS STS AssumeRoleWithWebIdentity).

Weitere Informationen zum Austauschen von langfristigen Anmeldeinformationen finden Sie unter Rotieren der Zugriffsschlüssel

Ressourcen

Zugehörige bewährte Methoden:

- SEC02-BP03 Sicheres Speichern und Verwenden von Secrets
- SEC02-BP04 Verlassen auf einen zentralen Identitätsanbieter
- SEC03-BP08 Sicheres gemeinsames Nutzen von Ressourcen in Ihrer Organisation

Zugehörige Dokumente:

- Temporäre Sicherheitsanmeldeinformationen

- AWS Anmeldedaten
- Bewährte IAM-Sicherheitsmethoden
- IAM-Rollen
- IAM Identity Center
- Identitätsanbieter und Verbund
- Rotieren der Zugriffsschlüssel
- Partnerlösungen im Bereich Sicherheit: Zugriff und Zugriffssteuerung
- Der Stammbenutzer des AWS-Kontos
- Zugriff auf AWS über eine native Workload-Identität der Google Cloud Platform
- Zugriff auf AWS-Ressourcen von Mandanten von Microsoft Entra ID mit AWS -Security-Token-Service

Zugehörige Videos:

- Verwaltung von Benutzerberechtigungen in großem Umfang mit AWS IAM Identity Center
- Beherrschen der Identität auf jeder Ebene

SEC02-BP03 Sicheres Speichern und Verwenden von Secrets

Eine Workload muss ihre Identität automatisch gegenüber Datenbanken, Ressourcen und Services von Drittanbietern authentifizieren können. Dazu dienen geheime Zugriffsanmeldeinformationen wie etwa API-Zugriffsschlüssel, Passwörter und OAuth-Tokens. Die Verwendung eines dedizierten Services zur Speicherung, Verwaltung und Rotation der Anmeldeinformationen hilft dabei, die Gefahr der Kompromittierung dieser Anmeldeinformationen zu verringern.

Gewünschtes Ergebnis: Implementierung eines Mechanismus zur sicheren Verwaltung von Anmeldeinformationen für Anwendungen, mit dem die folgenden Ziele erreicht werden:

- Identifikation der für die Workload erforderlichen Secrets
- Reduzierung der Anzahl der erforderlichen langfristigen Anmeldeinformationen durch ihren Austausch gegen kurzfristige Anmeldeinformationen, wo dies möglich ist
- Einrichtung der sicheren Speicherung und der automatischen Rotation der verbleibenden langfristigen Anmeldeinformationen
- Überwachung des Zugriffs auf in der Workload vorhandene Secrets

- Kontinuierliche Beobachtung, um sicherzustellen, dass im Rahmen des Entwicklungsprozesses keine Secrets in den Quellcode eingebettet werden
- Reduzieren der Gefahr unbeabsichtigter Offenlegungen von Anmeldeinformationen

Typische Anti-Muster:

- Keine Rotation der Anmeldeinformationen
- Speichern langfristiger Anmeldeinformationen in Quellcode oder Konfigurationsdateien
- Speichern von Anmeldeinformationen im Ruhezustand ohne Verschlüsselung

Vorteile der Nutzung dieser bewährten Methode:

- Secrets werden im Ruhezustand und während der Übertragung verschlüsselt gespeichert.
- Der Zugriff auf Anmeldeinformationen erfolgt über eine API (stellen Sie sich das als Automaten zum Verkauf von Anmeldeinformationen vor).
- Der Zugriff (Lese- und Schreibzugriff) auf Anmeldeinformationen wird geprüft und protokolliert.
- Trennung möglicher Problemquellen: Die Rotation der Anmeldeinformationen wird von einer separaten Komponente vorgenommen, die vom Rest der Architektur isoliert werden kann.
- Secrets werden automatisch bei Bedarf an Softwarekomponenten verteilt und die Rotation erfolgt an einem zentralen Ort.
- Der Zugriff auf Anmeldeinformationen kann detailliert kontrolliert werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Früher wurden Anmeldeinformationen für die Authentifizierung bei Datenbanken, APIs von Dritten, Tokens und andere Secrets möglicherweise in eingebettetem Quellcode oder in Umgebungsdateien gespeichert. AWS bietet mehrere Mechanismen, um diese Anmeldeinformationen sicher zu speichern, sie automatisch zu rotieren und ihre Verwendung zu prüfen.

Das beste Verfahren für die Verwaltung von Secrets besteht darin, den Anweisungen zum Entfernen, Ersetzen und Rotieren zu folgen. Die sichersten Anmeldeinformationen sind diejenigen, die Sie nicht speichern, verwalten oder handhaben müssen. Möglicherweise gibt es Anmeldeinformationen, die für die Funktion der Workload nicht mehr benötigt werden und sicher entfernt werden können.

Bei Anmeldeinformationen, die für die korrekte Funktion der Workload weiterhin benötigt werden, besteht die Möglichkeit, langfristige Anmeldeinformationen durch temporäre oder kurzfristige zu ersetzen. So könnten Sie beispielsweise anstelle der Hartkodierung eines geheimen AWS-Zugriffsschlüssels diese langfristigen Anmeldeinformationen durch temporäre unter Verwendung von IAM-Rollen ersetzen.

Manche langfristigen Secrets können möglicherweise nicht entfernt oder ersetzt werden. Diese Secrets können in einem Service wie AWS Secrets Manager gespeichert werden, wo sie zentral gespeichert, verwaltet und regelmäßig rotiert werden können.

Eine Prüfung des Quellcodes und der Konfigurationsdateien des Workloads kann verschiedene Arten von Anmeldeinformationen aufdecken. Die folgende Tabelle fasst Strategien für den Umgang mit gängigen Arten von Anmeldeinformationen zusammen:

Anmeldeinformationstyp	Beschreibung	Empfohlene Strategie
IAM-Zugriffsschlüssel	AWS-IAM-Zugriff und geheime Schlüssel, die zur Übernahme von IAM-Rollen innerhalb einer Workload verwendet werden	Ersetzen: Verwenden Sie stattdessen IAM-Rollen, die den Datenverarbeitungs-Instances zugewiesen sind (z. B. Amazon EC2 oder AWS Lambda). Fragen Sie zwecks Interoperabilität mit Drittanbietern, die Zugriff auf Ressourcen in Ihrem AWS-Konto benötigen, ob diese den kontoübergreifenden AWS-Zugriff unterstützen. Erwägen Sie für mobile Apps die Verwendung temporäre r Anmeldeinformationen über Amazon-Cognito-Identitätspools (Verbundi dentitäten). Für Workloads , die außerhalb von AWS ausgeführt werden, sollten Sie IAM Roles Anywhere oder AWSSystems Manager Hybrid

Anmeldeinformationstyp	Beschreibung	Empfohlene Strategie
		Activations in Betracht ziehen. Beachten Sie für Container die Informationen unter IAM-Rolle für Amazon-ECS-Aufgaben oder IAM-Rolle für Amazon-EKS-Knoten.
SSH-Schlüssel	Private Secure-Shell-Schlüssel, mit denen Sie sich manuell oder im Rahmen eines automatisierten Prozesses bei Linux EC2-Instances anmelden können	Ersetzen: Verwenden Sie AWS Systems Manager oder EC2 Instance Connect, um mithilfe von IAM-Rollen programmgesteuerten und menschlichen Zugriff auf EC2-Instances zu ermöglichen.
Anwendungs- und Datenbank anmeldeinformationen	Passwörter – einfache Textzeichenfolge	Rotation: Speichern Sie Anmeldeinformationen in AWS Secrets Manager und richten Sie nach Möglichkeit eine automatische Rotation ein.
Amazon-RDS- und Aurora-Administratordatenbank-Anmeldeinformationen	Passwörter – einfache Textzeichenfolge	Ersetzen: Verwenden Sie die Secrets Manager-Integration mit Amazon RDS oder Amazon Aurora. Darüber hinaus können einige RDS-Datenbanktypen in einigen Anwendungsfällen IAM-Rollen anstelle von Passwörtern verwenden. Weitere Informationen hierzu finden Sie unter IAM-Datenbankauthentifizierung.

Anmeldeinformationstyp	Beschreibung	Empfohlene Strategie
OAuth-Token	Geheime Token – einfache Textzeichenfolge	Rotiation: Speichern Sie Token in AWS Secrets Manager und konfigurieren Sie die automatische Rotation.
API-Token und Schlüssel	Geheime Token – einfache Textzeichenfolge	Rotation: Speichern Sie diese Daten in AWS Secrets Manager und richten Sie nach Möglichkeit eine automatische Rotation ein.

Ein typisches Anti-Muster ist die Einbettung von IAM-Zugriffsschlüsseln in Quellcode, Konfigurationsdateien oder Mobil-Apps. Wenn für die Kommunikation mit einem AWS-Service ein IAM-Zugriffsschlüssel erforderlich ist, verwenden Sie temporäre (kurzfristige) Sicherheitsanmeldeinformationen. Diese kurzfristigen Anmeldeinformationen können über IAM-Rollen für EC2-Instances, Ausführungsrollen für Lambda-Funktionen, Cognito-IAM-Rollen für den mobilen Benutzerzugriff und IoT-Core-Richtlinien für IoT-Geräte bereitgestellt werden. Wenn Sie Schnittstellen zu Drittanbietern nutzen, sollten Sie eher den Zugriff auf eine IAM-Rolle mit dem erforderlichen Zugriff auf die Ressourcen Ihres Kontos delegieren, als einen IAM-Benutzer zu konfigurieren und dem Drittanbieter den geheimen Zugriffsschlüssel für diesen Benutzer zu senden.

Es gibt viele Fälle, in denen die Workload die Speicherung von Secrets erfordert, die für die Zusammenarbeit mit anderen Services und Ressourcen erforderlich sind. AWS Secrets Manager wurde speziell für die sichere Verwaltung dieser Anmeldeinformationen sowie für die Speicherung, Verwendung und Rotation von API-Token, Passwörtern und anderen Anmeldeinformationen entwickelt.

AWS Secrets Manager bietet fünf wichtige Funktionen, um die sichere Speicherung und Verarbeitung vertraulicher Anmeldeinformationen zu gewährleisten: Verschlüsselung im Ruhezustand, Verschlüsselung während der Übertragung, umfassende Prüfungen, detaillierte Zugriffskontrolle und erweiterbare Rotation von Anmeldeinformationen. Andere Secret-Verwaltungsservices von AWS-Partnern oder lokal entwickelte Lösungen mit ähnlichen Funktionen und Sicherungen sind ebenfalls akzeptabel.

Wenn Sie ein Secret abrufen, können Sie die clientseitigen Caching-Komponenten von Secrets Manager verwenden, um es für die zukünftige Verwendung zwischenzuspeichern. Das Abrufen eines gecacheten Secrets ist schneller als das Abrufen aus Secrets Manager. Da für den Aufruf von Secrets-Manager-APIs Kosten anfallen, kann die Verwendung eines Caches zudem Ihre Kosten senken. Alle Möglichkeiten zum Abrufen von Secrets finden Sie unter Abrufen von Secrets.

> **Note**
>
> Bei einigen Sprachen müssen Sie möglicherweise Ihre eigene In-Memory-Verschlüsselung für das clientseitige Caching implementieren.

Implementierungsschritte

1. Identifizieren Sie Codepfade, die hartkodierte Anmeldeinformationen enthalten, mithilfe von automatisierten Tools wie Amazon CodeGuru.
   a. Scannen Sie Ihre Code-Repositorys mit Amazon CodeGuru. Sobald die Überprüfung abgeschlossen ist, filtern Sie in CodeGuru nach Type=Secrets, um problematische Codezeilen zu finden.
2. Identifizieren Sie Anmeldeinformationen, die entfernt oder ersetzt werden können.
   a. Identifizieren Sie Anmeldeinformationen, die nicht mehr benötigt werden, und markieren Sie sie zum Entfernen.
   b. Ersetzen Sie AWS-Geheimschlüssel, die in Quellcode eingebettet sind, durch IAM-Rollen, die mit den erforderlichen Ressourcen verbunden sind. Wenn sich ein Teil Ihres Workloads außerhalb von AWS befindet, für den Zugriff auf AWS-Ressourcen jedoch IAM-Anmeldeinformationen erforderlich sind, sollten Sie IAM Roles Anywhere oder AWS Systems Manager Hybrid Activations in Betracht ziehen.
3. Integrieren Sie für andere langfristige Secrets von Dritten, die die Rotationsstrategie erfordern, Secrets Manager in Ihren Code, um die externen Secrets zur Laufzeit abzurufen.
   a. Die CodeGuru-Konsole kann auf der Grundlage der erkannten Anmeldeinformationen automatisch ein Secret in Secrets Manager erstellen.
   b. Integrieren Sie den Secret-Abruf von Secrets Manager in Ihren Anwendungscode.
      i. Serverless-Lambda-Funktionen können eine sprachunabhängige Lambda-Erweiterung verwenden.
      ii. Für EC2-Instances oder -Container stellt AWS clientseitigen Beispielcode zum Abrufen von Secrets aus Secrets Manager in verschiedenen gängigen Programmiersprachen bereit.

4. Prüfen Sie Ihre Codebasis regelmäßig und wiederholen Sie dies, um sicherzustellen, dass dem Code keine neuen Secrets hinzugefügt wurden.
   a. Erwägen Sie die Verwendung eines Tools wie git-secrets, um zu verhindern, dass neue Secrets in Ihr Quellcode-Repository geladen werden.
5. Überwachen Sie die Aktivitäten von Secrets Manager auf Anzeichen für eine unerwartete Nutzung, unangemessenen Secret-Zugriff oder Versuche, Secrets zu löschen.
6. Reduzieren Sie menschliche Interaktionen mit Anmeldeinformationen. Schränken Sie den Zugriff zum Lesen, Schreiben und Ändern von Anmeldeinformationen auf eine für diesen Zweck dedizierte IAM-Rolle ein und erlauben Sie die Übernahme dieser Rolle nur einem kleinen Teil der betrieblichen Nutzer.

Ressourcen

Zugehörige bewährte Methoden:

- SEC02-BP02 Verwenden von temporären Anmeldeinformationen
- SEC02-BP05 Regelmäßiges Überprüfen und Rotieren von Anmeldeinformationen

Zugehörige Dokumente:

- Erste Schritte mit AWS Secrets Manager
- Identitätsanbieter und Verbund
- Amazon CodeGuru: Einführung in Secrets Detector
- Wie AWS Secrets ManagerAWS Key Management Service verwendet
- Ver- und Entschlüsselung von Secrets in Secrets Manager
- Blogeinträge zu Secrets Manager
- Amazon RDS kündigt Integration mit AWS Secrets Manager an

Zugehörige Videos:

- Bewährte Methoden zum Verwalten, Abrufen und Rotieren von Secrets in großem Maßstab
- Finden von hartkodierten Secrets mit Amazon CodeGuru Secrets Detector
- Sicherung von Secrets für hybride Workloads mit AWS Secrets Manager

Zugehörige Workshops:

- Speichern, Abrufen und Verwalten von vertraulichen Anmeldeinformationen in AWS Secrets Manager
- AWS-Systems-Manager-Hybridaktivierungen

SEC02-BP04 Verlassen auf einen zentralen Identitätsanbieter

Verlassen Sie sich im Zusammenhang mit Identitäten für Ihre Belegschaft (Mitarbeiter und Auftragnehmer) auf einen Identitätsanbieter, mit dem Sie Identitäten zentral verwalten können. Dadurch ist es einfacher, den Zugriff über mehrere Anwendungen und Systeme hinweg zu verwalten, da Sie den Zugriff von einem einzigen Standort aus erstellen, zuweisen, verwalten, widerrufen und überwachen.

Gewünschtes Ergebnis: Sie verfügen über einen zentralen Identitätsanbieter, mit dem Sie Benutzer im Unternehmen, Authentifizierungsrichtlinien (z. B. die Anforderung einer Multi-Faktor-Authentifizierung, MFA) und die Autorisierung für Systeme und Anwendungen zentral verwalten (z. B. die Zuweisung von Zugriffsberechtigungen auf Grundlage der Gruppenmitgliedschaft oder der Attribute eines Benutzers). Die Benutzer in Ihrer Belegschaft melden sich beim zentralen Identitätsanbieter an und bilden einen Verbund (Single Sign-On) mit internen und externen Anwendungen, sodass sich die Benutzer nicht mehrere Anmeldeinformationen merken müssen. Ihr Identitätsanbieter ist in Ihre Personalverwaltungssysteme integriert, sodass Personaländerungen automatisch mit Ihrem Identitätsanbieter synchronisiert werden. Wenn beispielsweise jemand Ihr Unternehmen verlässt, können Sie den Zugriff auf alle Anwendungen und Systeme im Verbund (einschließlich AWS) widerrufen. Sie haben die detaillierte Auditprotokollierung in Ihrem Identitätsanbieter aktiviert und überwachen diese Protokolle auf ungewöhnliches Benutzerverhalten.

Typische Anti-Muster:

- Sie verwenden keinen Verbund mit Single-Sign-On. Die Benutzer in Ihrer Belegschaft erstellen separate Benutzerkonten und Anmeldeinformationen für mehrere Anwendungen und Systeme.
- Sie haben den Lebenszyklus von Identitäten für Benutzer in Ihrer Belegschaft nicht automatisiert, indem Sie beispielsweise Ihren Identitätsanbieter in Ihre Personalverwaltungssysteme integriert haben. Wenn ein Benutzer Ihre Organisation verlässt oder die Position wechselt, folgen Sie einem manuellen Prozess, um seine Datensätze in mehreren Anwendungen und Systemen zu löschen oder zu aktualisieren.

Vorteile der Nutzung dieser bewährten Methode: Durch die Verwendung eines zentralen Identitätsanbieters haben Sie die Möglichkeit, Benutzeridentitäten und Richtlinien für Ihre Mitarbeiter von einem zentralen Ort aus zu verwalten, Benutzern und Gruppen Zugriff auf Anwendungen zuzuweisen und die Anmeldeaktivitäten der Benutzer zu überwachen. Wenn ein Benutzer die Position wechselt, werden durch die Integration in Ihre Personalverwaltungssysteme Änderungen mit dem Identitätsanbieter synchronisiert und die ihm zugewiesenen Anwendungen und Berechtigungen werden automatisch aktualisiert. Wenn ein Benutzer Ihre Organisation verlässt, wird seine Identität automatisch im Identitätsanbieter deaktiviert, wodurch ihm der Zugriff auf Anwendungen und Systeme im Verbund entzogen wird.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Leitfaden für Benutzer in der Belegschaft, die auf AWS zugreifen Benutzer in der Belegschaft, wie z. B. Mitarbeiter und Auftragnehmer in Ihrer Organisation, benötigen möglicherweise Zugriff auf AWS über die AWS-Managementkonsole oder die AWS Command Line Interface (AWS CLI), um ihre Aufgaben auszuführen. Sie können diesen Benutzern Zugriff auf AWS gewähren, indem Sie einen Verbund von Ihrem zentralen Identitätsanbieter zu AWS auf zwei Ebenen einrichten: ein direkter Verbund mit jedem AWS-Konto oder ein Verbund mit mehreren Konten in Ihrer AWS-Organisation.

Um die Benutzer in Ihrem Unternehmen direkt mit jedem AWS-Konto zu verbinden, können Sie einen zentralen Identitätsanbieter für den Verbund mit AWS Identity and Access Management in diesem Konto verwenden. Dank der Flexibilität von IAM können Sie für jedes AWS-Konto einen separaten SAML-2.0- oder OpenID Connect (OIDC)-Identitätsanbieter aktivieren und Verbundbenutzerattribute für die Zugriffskontrolle verwenden. Die Benutzer in Ihrer Belegschaft verwenden ihren Webbrowser, um sich beim Identitätsanbieter anzumelden, indem sie ihre Anmeldeinformationen (wie Passwörter und MFA-Tokencodes) angeben. Der Identitätsanbieter gibt eine SAML-Zusicherung an den Browser aus, die an die Anmelde-URL der AWS-Managementkonsole gesendet wird. Dies ermöglicht den Benutzern das Single Sign-On (SSO) bei der AWS-Managementkonsole, indem sie eine IAM-Rolle annehmen. Ihre Benutzer können auch temporäre AWS-API-Anmeldeinformationen für die Verwendung in der AWS CLI oder AWS-SDKs aus AWS STS abrufen, indem sie mithilfe einer SAML-Zusicherung des Identitätsanbieters die IAM-Rolle übernehmen.

Um die Benutzer Ihrer Belegschaft mit mehreren Konten in Ihrer AWS-Organisation zu verbinden, können Sie mithilfe von AWS IAM Identity Center den Zugriff Ihrer Mitarbeiter auf AWS-Konten und Anwendungen zentral verwalten. Sie aktivieren Identity Center für Ihre Organisation und konfigurieren Ihre Identitätsquelle. IAM Identity Center stellt ein Standard-Identitätsquellenverzeichnis bereit, mit dem Sie Ihre Benutzer und Gruppen verwalten können. Alternativ können Sie eine externe

Identitätsquelle auswählen, indem Sie mithilfe von SAML 2.0 eine Verbindung zu Ihrem externen Identitätsanbieter herstellen und Benutzer und Gruppen mithilfe von SCIM automatisch bereitstellen oder mithilfe von Directory Service eine Verbindung zu Ihrem Microsoft AD-Verzeichnis herstellen. Sobald eine Identitätsquelle konfiguriert wurde, können Sie Benutzern und Gruppen Zugriff auf AWS-Konten zuweisen, indem Sie Richtlinien nach dem Prinzip der geringsten Berechtigung in Ihren Berechtigungssätzen definieren. Die Benutzer Ihrer Belegschaft können sich über Ihren zentralen Identitätsanbieter authentifizieren, um sich beim AWS-Zugriffsportal anzumelden und sich per Single Sign-On bei AWS-Konten und den ihnen zugewiesenen Cloud-Anwendungen zu authentifizieren. Ihre Benutzer können AWS CLI v2 konfigurieren, um sich bei Identity Center zu authentifizieren und Anmeldeinformationen für die Ausführung von AWS CLI-Befehlen zu erhalten. Identity Center ermöglicht auch den Single-Sign-On-Zugriff auf AWS-Anwendungen wie Amazon SageMaker AI Studio und AWS IoT-SiteWise-Monitor-Portalen.

Nachdem Sie die obigen Anweisungen befolgt haben, müssen die Benutzer in Ihrer Belegschaft bei der Verwaltung von Workloads in AWS für den normalen Betrieb keine IAM-Benutzer und -Gruppen mehr verwenden. Stattdessen werden Ihre Benutzer und Gruppen außerhalb von AWS verwaltet, und Benutzer können als Verbundidentität auf AWS-Ressourcen zugreifen. Verbundidentitäten verwenden die von ihrem zentralen Identitätsanbieter definierten Gruppen. Sie sollten IAM-Gruppen, IAM-Benutzer und langlebige Benutzeranmeldeinformationen (Passwörter und Zugriffsschlüssel), die in Ihren AWS-Konten nicht mehr benötigt werden, identifizieren und entfernen. Sie können mithilfe von IAM-Berichten zu Anmeldeinformationen nach ungenutzten Anmeldeinformationen suchen, die entsprechenden IAM-Benutzer löschen und IAM-Gruppen löschen. Sie können auf Ihre Organisation eine Service-Kontrollrichtlinie (SCP) anwenden, die die Erstellung neuer IAM-Benutzer und -Gruppen verhindert, und so den Zugriff auf AWS über Verbundidentitäten erzwingen.

> **Note**
>
> Sie sind für die Rotation der SCIM-Zugriffstoken verantwortlich, wie in der Dokumentation zur automatischen Bereitstellung beschrieben. Darüber hinaus liegt die Rotation der Zertifikate, die Ihren Identitätsverbund unterstützen, in Ihrer Verantwortung.

Leitfaden für Benutzer Ihrer Anwendungen Sie können die Identitäten der Benutzer Ihrer Anwendungen, z. B. einer mobilen App, mithilfe von Amazon Cognito als zentralem Identitätsanbieter verwalten. Amazon Cognito ermöglicht die Authentifizierung, Autorisierung und Benutzerverwaltung für Ihre Web- und Mobil-Apps. Amazon Cognito bietet einen Identitätsspeicher, der auf Millionen von Benutzern skaliert werden kann, unterstützt den Identitätsverbund für soziale Netzwerke und Unternehmen und bietet erweiterte Sicherheitsfeatures zum Schutz Ihrer Benutzer und

Ihres Unternehmens. Sie können Ihre benutzerdefinierte Web- oder Mobilanwendung in Amazon Cognito integrieren, um Ihren Anwendungen innerhalb von Minuten Benutzerauthentifizierung und Zugriffskontrolle hinzuzufügen. Amazon Cognito basiert auf offenen Identitätsstandards wie SAML und Open ID Connect (OIDC), unterstützt verschiedene Compliance-Vorschriften und lässt sich in Frontend- und Backend-Entwicklungsressourcen integrieren.

Implementierungsschritte

Schritte für Benutzer im Unternehmen, die auf AWS zugreifen

- Erstellen Sie für die Benutzer in Ihrer Belegschaft unter Verwendung eines zentralen Identitätsanbieters einen Verbund mit AWS. Nutzen Sie dabei einen der folgenden Ansätze:
  - Verwenden Sie IAM Identity Center, um Single Sign-On für mehrere AWS-Konten in Ihrer AWS-Organisation zu aktivieren, indem Sie einen Verbund mit Ihrem Identitätsanbieter erstellen.
  - Verwenden Sie IAM, um Ihren Identitätsanbieter direkt mit jedem AWS-Konto zu verbinden und so einen differenzierten Verbundzugriff zu ermöglichen.
- Identifizieren und entfernen Sie IAM-Benutzer und -Gruppen, die durch Verbundidentitäten ersetzt werden.

Schritte für Benutzer Ihrer Anwendungen

- Verwenden Sie Amazon Cognito als zentralen Identitätsanbieter für Ihre Anwendungen.
- Integrieren Sie Ihre benutzerdefinierten Anwendungen mithilfe von OpenID Connect und OAuth mit Amazon Cognito. Sie können Ihre benutzerdefinierten Anwendungen mithilfe der Amplify-Bibliotheken entwickeln, die einfache Schnittstellen für die Integration in eine Vielzahl von AWS-Services bieten, z. B. Amazon Cognito für die Authentifizierung.

Ressourcen

Zugehörige bewährte Methoden:

- SEC02-BP06 Nutzen von Benutzergruppen und Attributen
- SEC03-BP02 Gewähren des Zugriffs mit den geringsten Berechtigungen
- SEC03-BP06 Zugriffsverwaltung basierend auf dem Lebenszyklus

Zugehörige Dokumente:

- Identitätsverbund in AWS
- Bewährte Methoden für die Sicherheit in IAM
- Bewährte Methoden für AWS Identity and Access Management
- Erste Schritte mit der delegierten Administration von IAM Identity Center
- Verwenden von vom Kunden verwalteten Richtlinien in IAM Identity Center für fortgeschrittene Anwendungsfälle
- AWS CLI v2: Anbieter von IAM Identity Center-Anmeldeinformationen

Zugehörige Videos:

- AWS re:Inforce 2022 – AWS Identity and Access Management (IAM) Vertiefung
- AWS re:Invent 2022 – Vereinfachen des vorhandenen Mitarbeiterzugriffs mit IAM Identity Center
- AWS re:Invent 2018: Beherrschen der Identität auf jeder Ebene

Zugehörige Beispiele:

- Workshop: Verwenden von AWS IAM Identity Center für eine robuste Identitätsverwaltung

Zugehörige Tools:

- AWS-Kompetenzpartner für Sicherheit: Identitäts- und Zugriffsverwaltung
- saml2aws

SEC02-BP05 Regelmäßiges Überprüfen und Rotieren von Anmeldeinformationen

Prüfen und rotieren Sie Anmeldeinformationen regelmäßig, um die Zeit zu begrenzen, für die diese zum Zugriff auf Ihre Ressourcen genutzt werden können. Langfristig gültige Anmeldeinformationen sind mit Risiken verbunden, die durch die regelmäßige Rotation dieser Informationen reduziert werden können.

Gewünschtes Ergebnis: Implementieren Sie die Rotation von Anmeldeinformationen, um die Risiken zu verringern, die mit der Nutzung von langfristigen Anmeldeinformationen verbunden sind. Prüfen und korrigieren Sie regelmäßig fehlende Compliance mit Richtlinien zur Rotation von Anmeldeinformationen.

Typische Anti-Muster:

- Keine Prüfung der Verwendung von Anmeldeinformationen
- Unnötiges Verwenden langfristiger Anmeldeinformationen
- Verwendung langfristiger Anmeldeinformationen, ohne diese regelmäßig zu rotieren

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Wenn Sie sich nicht auf temporäre Anmeldeinformationen verlassen können und langfristige Anmeldeinformationen benötigen, prüfen Sie die Anmeldeinformationen, um sicherzustellen, dass definierte Kontrollen wie Multi-Faktor-Authentifizierung (MFA)) erzwungen und regelmäßig rotiert werden sowie über die entsprechende Zugriffsebene verfügen.

Eine regelmäßige Validierung, vorzugsweise durch ein automatisiertes Tool, ist notwendig, um zu überprüfen, ob die richtigen Kontrollen angewendet werden. Für Personenidentitäten sollten Sie festlegen, dass Benutzer ihre Passwörter regelmäßig ändern und anstelle von Zugriffsschlüsseln temporäre Anmeldeinformationen verwenden. Wenn Sie von AWS Identity and Access Management (IAM) Benutzern zu zentralen Identitäten wechseln, können Sie einen Bericht zu Anmeldeinformationen erstellen, um Ihre Benutzer zu überprüfen.

Wir empfehlen außerdem, dass Sie MFA in Ihrem Identitätsanbieter erzwingen. Sie können AWS-Config-Regeln einrichten oder AWS Security Hub CSPM Security Stands verwenden, um zu überwachen, ob Benutzer MFA konfiguriert haben. Erwägen Sie die Nutzung von IAM Roles Anywhere zur Bereitstellung temporärer Anmeldeinformationen für Maschinenidentitäten. In Situationen, in denen die Verwendung von IAM-Rollen und temporären Anmeldeinformationen nicht möglich ist, ist eine häufige Prüfung und Rotation von Zugriffsschlüsseln erforderlich.

Implementierungsschritte

- Regelmäßige Prüfung der Anmeldeinformationen: Die Prüfung der in Ihrem Identitätsanbieter und in IAM konfigurierten Identitäten hilft bei der Sicherstellung, dass nur autorisierte Identitäten Zugriff auf Ihre Workload haben. Solche Identitäten können unter anderem IAM-Benutzer, Benutzer von AWS IAM Identity Center, Active-Directory-Benutzer oder Benutzer in einem anderen vorgelagerten Identitätsanbieter sein. Entfernen sie beispielsweise Personen, die die Organisation verlassen. Entfernen Sie auch kontoübergreifende Rollen, die nicht mehr erforderlich sind. Sie benötigen einen Prozess zum regelmäßigen Prüfen von Berechtigungen für die Services, auf die eine IAM-

Entität zugreift. Dadurch können Sie die Richtlinien identifizieren, die Sie ändern müssen, um nicht genutzte Berechtigungen zu entfernen. Verwenden Sie Berichte zu Anmeldeinformationen und AWS Identity and Access Management Access Analyzer, um IAM-Anmeldeinformationen und -Berechtigungen zu überprüfen. Sie können Amazon CloudWatch verwenden, um Alarme für bestimmte API-Aufrufe einzurichten, die in Ihrer AWS-Umgebung erfolgen. Amazon GuardDuty kann Sie auch vor unerwarteten Aktivitäten warnen, die auf einen übermäßig freizügigen Zugriff oder einen unbeabsichtigten Zugriff auf IAM-Anmeldeinformationen hindeuten können.

- Anmeldeinformationen regelmäßig rotieren: Wenn Sie keine temporären Anmeldeinformationen verwenden können, rotieren Sie langfristige IAM-Zugriffsschlüssel regelmäßig (spätestens nach jeweils 90 Tagen). Wenn ein Zugriffsschlüssel ohne Ihr Wissen kompromittiert wurde, wird dadurch begrenzt, für wie lange die Anmeldeinformationen zum Zugriff auf Ihre Ressourcen genutzt werden können. Informationen zum Austauschen von Zugriffsschlüsseln für IAM-Benutzer finden Sie unter Rotieren der Zugriffsschlüssel.
- IAM-Berechtigungen überprüfen: Um die Sicherheit Ihres AWS-Kontos zu erhöhen, sollten Sie Ihre IAM-Richtlinien regelmäßig überprüfen und überwachen. Stellen Sie sicher, dass die Richtlinien dem Prinzip der geringsten Berechtigung entsprechen.
- Automatisierung der Erstellung und Aktualisierung von IAM-Ressourcen erwägen: IAM Identity Center automatisiert viele IAM-Aufgaben, etwa die Rollen- und Richtlinienverwaltung. Alternativ können Sie mit AWS CloudFormation die Bereitstellung von IAM-Ressourcen – einschließlich Rollen und Richtlinien – automatisieren. So lässt sich die Zahl menschlicher Fehler verringern, da die Vorlagen verifiziert und ihre Versionen kontrolliert werden können.
- IAM Roles Anywhere verwenden, um IAM-Benutzer für Maschinenidentitäten zu ersetzen: Mit IAM Roles Anywhere können Sie Rollen in Bereichen verwenden, in denen dies bisher nicht möglich war, z. B. auf On-Premises-Servern. IAM Roles Anywhere verwendet ein vertrauenswürdiges X.509-Zertifikat zur Authentifizierung gegenüber AWS und zum Erhalt temporärer Anmeldeinformationen. Mit IAM Roles Anywhere müssen Sie diese Anmeldeinformationen nicht mehr rotieren, da sie nicht mehr in Ihrer On-Premises-Umgebung gespeichert werden. Beachten Sie, dass Sie das X.509-Zertifikat beobachten und gegen Ende seiner Gültigkeitsdauer austauschen müssen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC02-BP02 Verwenden von temporären Anmeldeinformationen
- SEC02-BP03 Sicheres Speichern und Verwenden von Secrets

Zugehörige Dokumente:

- Erste Schritte mit AWS Secrets Manager
- IAM Best Practices
- Identitätsanbieter und Verbund
- Partnerlösungen im Bereich Sicherheit: Zugriff und Zugriffssteuerung
- Temporäre Sicherheitsanmeldeinformationen
- Abrufen von Berichten zu Anmeldeinformationen für Ihr AWS-Konto

Zugehörige Videos:

- Bewährte Methoden zum Verwalten, Abrufen und Rotieren von Secrets in großem Maßstab
- Verwaltung von Benutzerberechtigungen in großem Umfang mit AWS IAM Identity Center
- Beherrschen der Identität auf jeder Ebene

SEC02-BP06 Nutzen von Benutzergruppen und Attributen

Die Definition von Berechtigungen nach Benutzergruppen und Attributen trägt dazu bei, die Anzahl und Komplexität von Richtlinien zu reduzieren, sodass das Prinzip der geringsten Berechtigung einfacher umgesetzt werden kann. Sie können Benutzergruppen verwenden, um die Berechtigungen für viele Personen an einem Ort zu verwalten, basierend auf der Funktion, die sie in Ihrer Organisation innehaben. Attribute, wie z. B. Abteilung, Projekt oder Standort, können eine zusätzliche Ebene des Berechtigungsumfangs bieten, wenn Personen eine ähnliche Funktion ausüben, jedoch für unterschiedliche Teilmengen von Ressourcen.

Gewünschtes Ergebnis: Sie können Änderungen der Berechtigungen auf alle Benutzer anwenden, die eine bestimmte Funktion ausführen. Die Gruppenzugehörigkeit und -attribute regeln die Benutzerberechtigungen, sodass Sie die Berechtigungen nicht mehr auf der Ebene der einzelnen Benutzer verwalten müssen. Die Gruppen und Attribute, die Sie in Ihrem Identitätsanbieter (IDP) definieren, werden automatisch an Ihre AWS-Umgebungen weitergegeben.

Typische Anti-Muster:

- Verwaltung von Berechtigungen für einzelne Benutzer und Duplizierung für viele Benutzer.
- Definition von Gruppen auf einer zu hohen Ebene, Gewährung von zu weitreichenden Berechtigungen.

- Die Definition von Gruppen auf einer zu granularen Ebene, was zu Doppelarbeit und Verwirrung über die Mitgliedschaft führt.
- Verwendung von Gruppen mit doppelten Berechtigungen für Teilmengen von Ressourcen, wenn stattdessen Attribute verwendet werden können.
- Keine Verwaltung von Gruppen, Attributen und Mitgliedschaften über einen standardisierten Identitätsanbieter, der in Ihre AWS-Umgebungen integriert ist.
- Verwenden von Rollenverkettung bei der Verwendung von Sitzungen von AWS IAM Identity Center

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

AWS-Berechtigungen werden in Dokumenten definiert, die als Richtlinien bezeichnet werden und einem Prinzipal zugeordnet sind, z. B. einem Benutzer, einer Gruppe, einer Rolle oder einer Ressource. Sie können das Berechtigungsmanagement skalieren, indem Sie die Zuweisungen von Berechtigungen (Gruppe, Berechtigungen, Konto) auf der Grundlage von Aufgabenfunktion, Workload und SDLC-Umgebung organisieren. So können Sie für Ihre Mitarbeiter Gruppen definieren, die auf der Funktion basieren, die Ihre Benutzer in Ihrer Organisation innehaben, und nicht auf den Ressourcen, auf die sie zugreifen. Beispielsweise kann einer WebAppDeveloper-Gruppe eine Richtlinie für die Konfiguration von Services wie Amazon CloudFront innerhalb eines Entwicklungskontos angehängt sein. Eine `AutomationDeveloper`-Gruppe hat möglicherweise einige Berechtigungen, die sich mit der `WebAppDeveloper`-Gruppe überschneiden. Diese gemeinsamen Berechtigungen können in einer separaten Richtlinie erfasst und beiden Gruppen zugeordnet werden. Dadurch ist es nicht erforderlich, dass Benutzer beider Funktionen zu einer `CloudFrontAccess`-Gruppe gehören.

Zusätzlich zu Gruppen können Sie Attribute verwenden, um den Zugriff festzulegen. Sie können beispielsweise ein Projekt-Attribut für Benutzer in Ihrer `WebAppDeveloper`-Gruppe nutzen, damit die Benutzer nur auf Ressourcen ihres Projekts zugreifen können. Mit dieser Technik entfällt die Notwendigkeit, für Anwendungsentwickler, die an verschiedenen Projekten arbeiten, unterschiedliche Gruppen einzurichten, wenn ihre Berechtigungen ansonsten identisch sind. Die Art und Weise, wie Sie sich auf Attribute in Berechtigungsrichtlinien beziehen, hängt von deren Quelle ab, d. h. ob sie als Teil Ihres Verbundprotokolls (wie SAML, OIDC oder SCIM), als benutzerdefinierte SAML-Assertions oder innerhalb von IAM Identity Center definiert sind.

Implementierungsschritte

1. Legen Sie fest, wo Sie Gruppen und Attribute definieren wollen:

   a. Anhand der Anleitung unter SEC02-BP04 Verlassen auf einen zentralen Identitätsanbieter können Sie festlegen, ob Sie Gruppen und Attribute innerhalb Ihres Identitätsanbieters, innerhalb von IAM Identity Center oder mithilfe von IAM-Benutzergruppen in einem bestimmten Konto definieren müssen.

2. Definieren von Gruppen:
   a. Legen Sie Ihre Gruppen je nach Funktion und Umfang des erforderlichen Zugriffs fest. Erwägen Sie die Verwendung einer hierarchischen Struktur oder von Benennungskonventionen, um Gruppen effektiv zu organisieren.
   b. Wenn Sie innerhalb von IAM Identity Center definieren, erstellen Sie Gruppen und ordnen Sie die gewünschte Zugriffsebene mithilfe von Berechtigungsgruppen zu.
   c. Wenn Sie die Definition innerhalb eines externen Identitätsanbieters vornehmen, stellen Sie fest, ob der Anbieter das SCIM-Protokoll unterstützt und erwägen Sie die Aktivierung der automatischen Bereitstellung innerhalb von IAM Identity Center. Diese Funktion synchronisiert die Erstellung, Mitgliedschaft und Löschung von Gruppen zwischen Ihrem Anbieter und IAM Identity Center.
3. Definieren von Attributen:
   a. Wenn Sie einen externen Identitätsanbieter verwenden, bieten sowohl das SCIM- als auch das SAML 2.0-Protokoll standardmäßig bestimmte Attribute. Zusätzliche Attribute können mithilfe von SAML-Zusicherungen unter Verwendung des `https://aws.amazon.com/SAML/Attributes/PrincipalTag`-Attributnamens definiert und übergeben werden. Schritte zum Definieren und Konfigurieren von benutzerdefinierten Attributen finden Sie in der Dokumentation Ihres Identitätsanbieters.
   b. Wenn Sie Rollen innerhalb von IAM Identity Center definieren, aktivieren Sie das Feature attributbasierte Zugriffskontrolle (ABAC) und definieren Sie die Attribute nach Bedarf. Ziehen Sie Attribute in Betracht, die zur Struktur oder zur Ressourcen-Tagging-Strategie Ihres Unternehmens passen.

Wenn Sie eine IAM-Rollenverkettung von IAM-Rollen benötigen, die über das IAM Identity Center übernommen wurden, werden Werte wie `source-identity` und `principal-tags` nicht weitergegeben. Weitere Informationen finden Sie unter Aktivieren und Konfigurieren von Attributen für die Zugriffskontrolle.

1. Legen Sie den Umfang von Berechtigungen basierend auf Gruppen und Attributen fest:
   a. Erwägen Sie, Bedingungen in Ihre Genehmigungsrichtlinien aufzunehmen, die die Attribute Ihres Prinzipals mit den Attributen der Ressourcen vergleichen, auf die zugegriffen wird. Sie

können beispielsweise eine Bedingung so definieren, dass der Zugriff auf eine Ressource nur dann gewährt wird, wenn der Wert eines `PrincipalTag`-Bedingungsschlüssels mit dem Wert eines `ResourceTag`-Schlüssels mit demselben Namen übereinstimmt.

b. Beachten Sie bei der Definition von ABAC-Richtlinien die Hinweise in den bewährten Methoden und Beispielen für die ABAC-Autorisierung.

c. Überprüfen und aktualisieren Sie Ihre Gruppen- und Attributstruktur regelmäßig, wenn sich die Anforderungen Ihres Unternehmens weiterentwickeln, um ein optimales Berechtigungsmanagement sicherzustellen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC02-BP04 Verlassen auf einen zentralen Identitätsanbieter
- SEC03-BP02 Gewähren des Zugriffs mit den geringsten Berechtigungen
- COST02-BP04 Implementieren von Gruppen und Rollen

Zugehörige Dokumente:

- IAM Best Practices
- Verwaltung von Identitäten in IAM Identity Center
- Wofür wird ABAC in AWS verwendet?
- ABAC in IAM Identity Center
- Beispiele für ABAC-Richtlinien

Zugehörige Videos:

- Verwaltung von Benutzerberechtigungen in großem Umfang mit AWS IAM Identity Center
- Beherrschen der Identität auf jeder Ebene

Berechtigungsverwaltung

Verwalten Sie Berechtigungen zum Steuern des Zugriffs für menschliche Identitäten und Maschinenidentitäten, die Zugriff auf AWS und Ihre Workloads benötigen. Berechtigungen steuern,

wer unter welchen Bedingungen worauf zugreifen kann. Legen Sie Berechtigungen für bestimmte menschliche oder Maschinenidentitäten fest, um Zugriff auf bestimmte Service-Aktionen für bestimmte Ressourcen zu gewähren. Sie können auch Bedingungen angeben, die erfüllt sein müssen, damit der Zugriff gewährt wird.

Es gibt eine Reihe von Möglichkeiten, Zugriff auf verschiedene Arten von Ressourcen zu gewähren. Eine Möglichkeit ist die Verwendung verschiedener Richtlinienarten.

Identitätsbasierte Richtlinien in IAM sind verwaltete Richtlinien oder Inline-Richtlinien und werden IAM-Identitäten, einschließlich Benutzern, Gruppen oder Rollen, angefügt. Mit diesen Richtlinien können Sie festlegen, welche Aktionen diese Identität durchführen darf (ihre Berechtigungen). Identitätsbasierte Richtlinien können weiter unterteilt werden.

Verwaltete Richtlinien – Dies sind eigenständige, identitätsbasierte Richtlinien, die Sie an mehrere Benutzer, Gruppen und Rollen in Ihrem AWS-Konto anfügen können. Es gibt zwei Typen von verwalteten Richtlinien:

- Verwaltete AWS-Richtlinien –Verwaltete Richtlinien, die von AWS erstellt und verwaltet werden.
- Vom Kunden verwaltete Richtlinien – Dies sind verwaltete Richtlinien, die Sie in Ihrem AWS-Konto erstellen und verwalten. Vom Kunden verwaltete Richtlinien bieten eine genauere Kontrolle über Ihre Richtlinien als von AWS verwaltete Richtlinien.

Verwaltete Richtlinien sind die bevorzugte Methode für die Anwendung von Berechtigungen. Sie können jedoch auch Inline-Richtlinien verwenden, die Sie direkt zu einem einzelnen Benutzer, einer Gruppe oder einer Rolle hinzufügen. Bei Inline-Richtlinien besteht eine strikte Eins-zu-Eins-Beziehung zwischen einer Richtlinie und einer Identität. Inline-Richtlinien werden gelöscht, wenn Sie die Identität löschen.

In den meisten Fällen sollten Sie Ihre eigenen, vom Kunden verwalteten Richtlinien erstellen und dabei dem Prinzip der geringsten Berechtigung folgen.

Ressourcenbasierten Richtlinien sind an eine Ressource angefügt. Eine S3-Bucket-Richtlinie ist zum Beispiel eine ressourcenbasierte Richtlinie. Diese Richtlinien erteilen einem Prinzipal, der sich in demselben Konto wie die Ressource oder in einem anderen Konto befinden kann, eine Berechtigung. Eine Liste der Services, die ressourcenbasierte Richtlinien unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren.

Berechtigungsgrenzen verwenden eine verwaltete Richtlinie, um die maximalen Berechtigungen festzulegen, die ein Administrator festlegen kann. Auf diese Weise können Sie die Fähigkeit zum

Erstellen und Verwalten von Berechtigungen an Entwickler delegieren, z. B. die Erstellung einer IAM-Rolle, aber die Berechtigungen, die diese erteilen können, einschränken, sodass sie ihre Berechtigungen nicht mit den erstellten Berechtigungen erweitern können.

Die attributbasierte Zugriffskontrolle (ABAC) in AWS ermöglicht es Ihnen, Berechtigungen basierend auf Attributen, sogenannten Tags, zu erteilen. Diese Tags können an IAM-Prinzipale (Benutzer oder Rollen) und an AWS-Ressourcen angefügt werden. Administratoren können wiederverwendbare IAM-Richtlinien erstellen, die Berechtigungen basierend auf den Attributen des IAM-Prinzipals anwenden. Als Administrator können Sie beispielsweise eine einzelne IAM-Richtlinie verwenden, um Entwicklern in Ihrer Organisation Zugriff auf AWS-Ressourcen zu gewähren, die mit ihren Projekt-Tags übereinstimmen. Wenn das Entwicklerteam Ressourcen zu Projekten hinzufügt, werden Berechtigungen automatisch basierend auf Attributen angewendet. Damit entfällt die Notwendigkeit von Richtlinienaktualisierungen für jede neue Ressource.

Service-Kontrollrichtlinien (SCP) für Organisationen definieren die maximalen Berechtigungen für Kontomitglieder einer Organisation oder Organisationseinheit (OE). SCPs schränken Berechtigungen ein, die identitätsbasierte Richtlinien oder ressourcenbasierte Richtlinien Entitäten (Benutzern oder Rollen) innerhalb des Kontos erteilen, aber sie gewähren keine Berechtigungen.

Sitzungsrichtlinien nehmen eine Rolle oder einen Verbundbenutzer an. Übergeben Sie Sitzungsrichtlinien, wenn Sie die AWS-CLI- oder AWS-API-Sitzungsrichtlinien verwenden, um die Berechtigungen einzuschränken, die die identitätsbasierten Richtlinien der Rolle oder des Benutzers für die Sitzung gewähren. Sitzungsrichtlinien beschränken Berechtigungen für eine erstellte Sitzung, aber sie gewähren keine Berechtigungen. Weitere Informationen finden Sie unter Sitzungsrichtlinien

Bewährte Methoden

- SEC03-BP01 Definieren von Zugriffsanforderungen
- SEC03-BP02 Gewähren des Zugriffs mit den geringsten Berechtigungen
- SEC03-BP03 Einrichtung eines Notfallzugriffprozesses
- SEC03-BP04 Kontinuierliche Reduzierung der Berechtigungen
- SEC03-BP05 Definieren eines Integritätsschutzes für Berechtigungen in Ihrer Organisation
- SEC03-BP06 Zugriffsverwaltung basierend auf dem Lebenszyklus
- SEC03-BP07 Analysieren des öffentlichen und kontoübergreifenden Zugriffs
- SEC03-BP08 Sicheres gemeinsames Nutzen von Ressourcen in Ihrer Organisation
- SEC03-BP09 Sicheres Teilen von Ressourcen mit Dritten

SEC03-BP01 Definieren von Zugriffsanforderungen

Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.

Typische Anti-Muster:

- Hartkodierung oder Speicherung von geheimen Daten in Ihrer Anwendung
- Gewähren individueller Berechtigungen für jeden Benutzer
- Verwendung langlebiger Anmeldeinformationen

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.

Der reguläre Zugriff auf AWS-Konten innerhalb einer Organisation sollte über den Verbundzugriff oder einen zentralen Identitätsanbieter bereitgestellt werden. Sie sollten auch Ihr Identitätsmanagement zentralisieren und sicherstellen, dass es ein etabliertes Verfahren zur Integration des AWS-Zugriffs in den Zugriffslebenszyklus der Mitarbeiter gibt Wenn beispielsweise ein Mitarbeiter in eine Rolle mit einer anderen Zugriffsstufe wechselt, sollte sich auch dessen Gruppenmitgliedschaft so ändern, dass die neuen Zugriffsanforderungen berücksichtigt werden.

Legen Sie bei der Definition der Zugriffsanforderungen für nicht menschliche Identitäten fest, welche Anwendungen und Komponenten Zugriff benötigen und wie die Berechtigungen gewährt werden. Eine empfohlene Vorgehensweise ist die Verwendung von nach dem Modell der geringsten Berechtigung entwickelten IAM-Rollen. AWS Verwaltete Richtlinien bieten vordefinierte IAM-Richtlinien für die meisten typischen Anwendungsfälle.

AWS-Services wie AWS Secrets Manager und AWS Systems Manager Parameter Store können Ihnen dabei helfen, Secrets sicher von der Anwendung oder dem Workload zu entkoppeln. In Secrets Manager können Sie die automatische Rotation Ihrer Anmeldeinformationen einrichten. Mit Systems Manager können Sie auf Parameter in Ihren Skripts, Befehlen, SSM-Dokumenten, Konfigurations-

und Automatisierungsworkflows verweisen, indem Sie den bei der Erstellung des Parameters angegebenen eindeutigen Namen verwenden.

Sie können AWS IAM Roles Anywhere verwenden, um temporäre Sicherheitsanmeldeinformationen in IAM für Workloads abzurufen, die außerhalb von AWS ausgeführt werden. Ihre Workloads können dieselben IAM-Richtlinien und IAM-Rollen verwenden, die Sie auch bei AWS-Anwendungen für den Zugriff auf AWS-Ressourcen verwenden.

Verwenden Sie nach Möglichkeit kurzfristige temporäre anstelle langfristiger statischer Anmeldeinformationen. Für Szenarien, in denen Sie -Benutzer mit programmgeteuertem Zugriff und langfristigen Anmeldeinformationen benötigen, verwenden Sie die Informationen über die letzte Nutzung von Zugriffsschlüsseln, um die Zugriffsschlüssel zu rotieren und zu entfernen.

Benutzer benötigen programmgesteuerten Zugriff, wenn sie außerhalb der AWS-Managementkonsole mit AWS interagieren möchten. Die Vorgehensweise, um programmgesteuerten Zugriff zu gewähren, hängt davon ab, welcher Benutzertyp auf zugreift AWS.

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Empfohlen) Verwenden Sie Konsolen-Anmeldeinformationen als temporäre Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS-SDKs oder AWS-APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zur AWS CLI finden Sie unter Anmeldung für lokale AWS-Entwicklung im AWS Command Line Interface-Benutzerhandbuch. • Informationen zu AWS-SDKs finden Sie unter Anmeldung für lokale AWS-Entwicklung im Referenzhandbuch zu AWS-SDKs und -Tools.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS-SDKs oder AWS-APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zur AWS CLI finden Sie unter Konfigurieren der AWS CLI für die Verwendung von AWS IAM Identity Center im AWS Command Line Interface-Benutzerhandbuch. • Informationen zu AWS-SDKs, Tools und AWS-APIs finden Sie unter IAM-Identity-Center-Authentifizierung im Referenzhandbuch zu AWS-SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS-SDKs oder AWS-APIs zu signieren.	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS-Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS-SDKs oder AWS-APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zur AWS CLI finden Sie unter Authentifizierung mit IAM-Benutzer-Anmeldeinformationen im AWS Command Line Interface-Benutzerhandbuch. • Informationen zu AWS-SDKs und Tools finden Sie unter Authentifizierung mit langfristigen Anmeldeinformationen im Referenzhandbuch zu AWS-SDKs und Tools. • Informationen zu AWS-APIs finden Sie unter Verwalten von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Ressourcen

Zugehörige Dokumente:

- Attributbasierte Zugriffskontrolle (ABAC)
- AWS IAM Identity Center
- IAM Roles Anywhere
- AWS Verwaltete -Richtlinien für IAM Identity Center
- AWS IAM-Richtlinienbedingungen

- IAM-Anwendungsfälle
- Entfernen unnötiger Anmeldeinformationen
- Arbeiten mit -Richtlinien
- Steuerung des Zugriffs auf AWS-Ressourcen auf der Grundlage von AWS-Konto, OU oder Organisation
- Identifizieren, Arrangieren und Verwalten von geheimen Daten mithilfe der erweiterten Suche in AWS Secrets Manager

Zugehörige Videos:

- Experte für IAM-Richtlinien in unter 60 Minuten
- Trennung von Pflichten, geringste Berechtigung, Delegierung und CI/CD
- Optimieren des Identitäts- und Zugriffsmanagements für Innovation

SEC03-BP02 Gewähren des Zugriffs mit den geringsten Berechtigungen

Gewähren Sie nur den Zugriff, den Benutzer benötigen, um bestimmte Aktionen auf bestimmten Ressourcen unter bestimmten Bedingungen durchzuführen. Nutzen Sie Gruppen und Identitätsattribute, um Berechtigungen dynamisch in großem Umfang festzulegen, anstatt Berechtigungen für einzelne Benutzer zu definieren. Sie können beispielsweise einer Gruppe von Entwicklern den Zugriff erlauben, nur die Ressourcen für ihr Projekt zu verwalten. So ist sichergestellt, dass einem Entwickler, der nicht mehr am Projekt arbeitet, automatisch der Zugriff entzogen wird, ohne dass die zugrunde liegenden Zugriffsrichtlinien geändert werden müssen.

Gewünschtes Ergebnis: Benutzer verfügen nur über die Berechtigungen, die für ihre Arbeit erforderlich sind. Sie verwenden separate AWS-Konten, um Entwickler von Produktionsumgebungen zu isolieren. Wenn Entwickler für bestimmte Aufgaben auf Produktionsumgebungen zugreifen müssen, wird ihnen nur für die Dauer dieser Aufgaben eingeschränkter und kontrollierter Zugriff gewährt. Ihr Zugriff auf die Produktion wird sofort aufgehoben, nachdem sie die erforderlichen Arbeiten abgeschlossen haben. Sie führen regelmäßige Überprüfungen der Berechtigungen durch und widerrufen sie umgehend, wenn sie nicht mehr benötigt werden, z. B. wenn ein Benutzer die Rolle wechselt oder das Unternehmen verlässt. Sie beschränken Administratorrechte auf eine kleine, vertrauenswürdige Gruppe, um das Risiko zu verringern. Sie gewähren Maschinen- oder Systemkonten nur die Mindestberechtigungen, die zur Ausführung der vorgesehenen Aufgaben erforderlich sind.

Typische Anti-Muster:

- Sie gewähren Benutzern standardmäßig Administratorberechtigungen.
- Sie verwenden das Root-Benutzerkonto für tägliche Aktivitäten.
- Sie erstellen übermäßig permissive Richtlinien ohne angemessene Beschränkung des Geltungsbereichs.
- Ihre Berechtigungen werden nur selten überprüft, was dazu führt, dass sie ständig erweitert werden.
- Sie verlassen sich ausschließlich auf die attributbasierte Zugriffskontrolle, wenn es um die Isolierung von Umgebungen oder die Verwaltung von Berechtigungen geht.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Das Prinzip der geringsten Berechtigung besagt, dass Identitäten nur die kleinstmögliche Menge von Aktionen ausführen dürfen, die zur Durchführung einer bestimmten Aufgabe erforderlich sind. Dies schafft ein Gleichgewicht zwischen Benutzerfreundlichkeit, Effizienz und Sicherheit. Die Anwendung dieses Prinzips trägt dazu bei, den unbeabsichtigten Zugriff zu beschränken und nachzuverfolgen, wer auf welche Ressourcen zugreifen kann. IAM-Benutzer und -Rollen verfügen standardmäßig über keine Berechtigungen. Der Root-Benutzer hat standardmäßig vollen Zugriff und sollte streng kontrolliert, überwacht und nur für Aufgaben verwendet werden, die Root-Zugriff erfordern.

Mithilfe von IAM-Richtlinien können ausdrücklich Berechtigungen für IAM-Rollen oder bestimmte Ressourcen erteilt werden. So können beispielsweise identitätsbasierte Richtlinien an IAM-Gruppen angefügt werden, während S3-Buckets von ressourcenbasierten Richtlinien kontrolliert werden können.

Wenn Sie eine IAM-Richtlinie erstellen, können Sie die Serviceaktionen, Ressourcen und Bedingungen angeben, die erfüllt sein müssen, damit AWS den Zugriff erlaubt oder verweigert. AWS unterstützt eine Vielzahl von Bedingungen, mit denen Sie den Zugriff einschränken können. Mithilfe des Bedingungsschlüssels PrincipalOrgID können Sie beispielsweise Aktionen ablehnen, wenn der Anforderer nicht zu Ihrer AWS-Organisation gehört.

Sie können auch Anforderungen kontrollieren, die AWS-Services in Ihrem Namen stellen, etwa das Erstellen einer AWS Lambda-Funktion durch AWS CloudFormation. Dazu verwenden Sie den Bedingungsschlüssel CalledVia. Sie können unterschiedliche Richtlinientypen in Ebenen organisieren, um ein umfassendes Verteidigungskonzept aufzubauen und die Berechtigungen

Ihrer Benutzer insgesamt zu begrenzen. Sie können auch Beschränkungen in Bezug darauf festlegen, welche Berechtigungen unter welchen Umständen erteilt werden können. Sie können Ihren Workload-Teams beispielsweise gestatten, ihre eigenen IAM-Richtlinien für die von ihnen erstellten Systeme zu erstellen; es muss aber auch eine Berechtigungsgrenze festgelegt werden, um die maximalen Berechtigungen zu beschränken, die sie gewähren können.

Implementierungsschritte

- Richtlinien für die geringste Berechtigung implementieren: Weisen Sie IAM-Gruppen und -Rollen Zugriffsrichtlinien mit geringsten Berechtigungen zu, die an den von Ihnen definierten Tätigkeitsbereich der Benutzer angepasst sind.
- Entwicklungs- und Produktionsumgebungen durch separate AWS-Konten trennen: Verwenden Sie separate AWS-Konten für Entwicklungs- und Produktionsumgebungen und kontrollieren Sie den Zugriff zwischen diesen Umgebungen mithilfe von Servicekontrollrichtlinien, Ressourcen- und Identitätsrichtlinien.
- Grundlegende Richtlinien für die API-Nutzung: Eine Möglichkeit, die erforderlichen Berechtigungen zu ermitteln, ist die Überprüfung von AWS CloudTrail-Protokollen. Diese Prüfung ermöglicht es Ihnen, Berechtigungen zu erstellen, die auf die Aktionen zugeschnitten sind, die der Benutzer tatsächlich in AWS ausführt. IAM Access Analyzer kann automatisch IAM-Richtlinien auf der Grundlage von Zugriffsaktivitäten generieren. Sie können IAM Access Advisor auf Organisations- oder Kontoebene verwenden, um die zuletzt abgerufenen Informationen für eine bestimmte Richtlinie nachzuverfolgen.
- Die Verwendung von AWS-verwalteten Richtlinien für Tätigkeitsbereiche erwägen: Wenn Sie mit der Erstellung detaillierter Berechtigungsrichtlinien beginnen, kann es nützlich sein, AWS-verwaltete Richtlinien für gängige Positionen wie Fakturierungsmitarbeiter, Datenbankadministratoren und Datenwissenschaftler zu verwenden. Diese Richtlinien können helfen, den Zugriff der Benutzer einzuschränken, während Sie festlegen, wie die Richtlinien für die geringste Berechtigung implementiert werden sollen.
- Unnötige Berechtigungen entfernen: Erkennen und entfernen Sie nicht genutzte IAM-Entitäten, Anmeldeinformationen und Berechtigungen, um das Prinzip der geringsten Berechtigung durchzusetzen. Sie können IAM Access Analyzer verwenden, um externen und nicht genutzten Zugriff zu identifizieren, und die Richtliniengenerierung von IAM Access Analyzer kann zur Optimierung der Berechtigungsrichtlinien beitragen.
- Sicherstellen, dass Benutzer eingeschränkten Zugriff auf Produktionsumgebungen haben: Benutzer sollten nur Zugriff auf Produktionsumgebungen haben, wenn es sich um einen gültigen Anwendungsfall handelt. Nachdem der Benutzer die konkreten Aufgaben ausgeführt hat, für die

Zugriff auf die Produktionsumgebung erforderlich war, sollte der Zugriff widerrufen werden. Die Beschränkung des Zugriffs auf Produktionsumgebungen hilft, unbeabsichtigte Vorkommnisse mit Auswirkungen auf die Produktion zu verhindern und das Ausmaß der Auswirkungen eines unbeabsichtigten Zugriffs zu verringern.

- Berechtigungsgrenzen erwägen:: Eine Berechtigungsgrenze ist ein Feature für eine verwaltete Richtlinie, das die maximalen Berechtigungen festlegt, die mit einer identitätsbasierten Richtlinie einer IAM-Entität erteilt werden können. Durch eine Berechtigungsgrenze kann eine Entität nur die Aktionen durchführen, die sowohl von den identitätsbasierten Richtlinien als auch den Berechtigungsgrenzen erlaubt werden.
- Den Zugriff mithilfe von attributbasierter Zugriffskontrolle und Ressourcentags verfeinern Die attributbasierte Zugriffskontrolle (ABAC) mithilfe von Ressourcentags kann, sofern sie unterstützt wird, zur Verfeinerung von Berechtigungen verwendet werden. Sie können ein ABAC-Modell verwenden, das Prinzipal-Tags mit Ressourcen-Tags vergleicht, um den Zugriff auf der Grundlage der von Ihnen definierten benutzerdefinierten Dimensionen zu verfeinern. Dieses Konzept kann die Berechtigungsrichtlinien in Ihrer Organisation vereinfachen und ihre Anzahl reduzieren.
  - Es wird empfohlen, ABAC nur für die Zugriffskontrolle zu verwenden, wenn sowohl die Prinzipale als auch die Ressourcen zu Ihrer AWS-Organisation gehören. Externe Parteien können dieselben Tag-Namen und Werte wie Ihre Organisation für ihre eigenen Prinzipale und Ressourcen verwenden. Wenn Sie sich bei der Gewährung des Zugriffs für Prinzipale oder Ressourcen von externen Parteien ausschließlich auf diese Name-Wert-Paare stützen, kann es vorkommen, dass Sie nicht beabsichtigte Berechtigungen erteilen.
- Service-Kontrollrichtlinien für AWS Organizations verwenden: Service-Kontrollrichtlinien steuern zentral die maximal verfügbaren Berechtigungen für Mitgliedskonten in Ihrer Organisation. Wichtig ist, dass Sie mithilfe von Service-Kontrollrichtlinien die Root-Benutzerberechtigungen in Mitgliedskonten einschränken können. Ziehen Sie auch die Verwendung von AWS Control Tower in Betracht, das präskriptive verwaltete Kontrollen zur Bereicherung von AWS Organizations bietet. Sie können auch Ihre eigenen Kontrollen in Control Tower definieren.
- Eine Lebenszyklusrichtlinie für Benutzer für Ihre Organisation einrichten: Benutzer-Lebenszyklusrichtlinien definieren Aufgaben, die ausgeführt werden, wenn Benutzer in AWS hinzugefügt werden, ihre Rolle oder ihren Aufgabenbereich ändern oder sie keinen Zugriff auf AWS mehr benötigen. Führen Sie bei jedem Schritt im Lebenszyklus eines Benutzers Berechtigungsprüfungen durch, um sicherzustellen, dass die Berechtigungen angemessen restriktiv sind und keine schleichenden Berechtigungserweiterungen stattfinden.
- Einen regelmäßigen Zeitplan einrichten, um die Berechtigungen zu überprüfen und alle nicht benötigten Berechtigungen zu entfernen: Sie sollten den Benutzerzugriff regelmäßig überprüfen,

um sicherzustellen, dass Benutzer keinen übermäßigen Zugriff haben. AWS Config und IAM Access Analyzer können Sie bei der Prüfung der Benutzerberechtigungen unterstützen.

- Job-Rollen-Matrix erstellen: Eine Job-Rollen-Matrix stellt die verschiedenen Rollen und Zugriffsebenen, die in Ihrem AWS-System erforderlich sind, grafisch dar. Mithilfe einer Job-Rollen-Matrix können Sie Berechtigungen auf der Grundlage von Benutzerzuständigkeiten in Ihrer Organisation definieren und trennen. Verwenden Sie Gruppen, anstatt Berechtigungen direkt auf einzelne Benutzer oder Rollen anzuwenden.

Ressourcen

Zugehörige Dokumente:

- Gewähren der geringsten Berechtigung
- Berechtigungsgrenzen für IAM-Entitäten
- Techniken zum Erstellen von IAM-Richtlinien mit geringsten Berechtigungen
- IAM Access Analyzer erleichtert die Implementierung geringster Berechtigungen durch die Generierung von IAM-Richtlinien auf der Grundlage der Zugriffsaktivitäten
- Delegieren der Berechtigungsverwaltung an Entwickler mithilfe von IAM-Berechtigungsgrenzen
- Verfeinern von Berechtigungen mithilfe der Informationen zum letzten Zugriff
- IAM-Richtlinienarten und wann sie verwendet werden sollten
- Testen von IAM-Richtlinien mit dem IAM-Richtliniensimulator
- Integritätsschutz in AWS Control Tower
- Zero-Trust-Architekturen: Eine AWS-Perspektive
- Implementieren des Prinzips der geringsten Berechtigung mit CloudFormation StackSets
- Attributbasierte Zugriffskontrolle (ABAC)
- Reduzieren des Richtlinienbereichs durch Anzeigen der Benutzeraktivität
- Anzeigen des Rollenzugriffs
- Verwenden Sie Tagging, um Ihre Umgebung zu organisieren und die Verantwortlichkeit zu fördern
- AWS-Strategien für das Tagging
- Taggen von AWS-Ressourcen

Zugehörige Videos:

- Berechtigungsmanagement der nächsten Generation
- Zero Trust: Eine AWS-Perspektive

SEC03-BP03 Einrichtung eines Notfallzugriffprozesses

Erstellen Sie einen Prozess, der im unwahrscheinlichen Fall eines Problems mit Ihrem zentralen Identitätsanbieter den Notfallzugriff auf Ihre Workloads ermöglicht.

Sie müssen Prozesse für verschiedene Ausfallmodi entwerfen, die zu einem Notfallereignis führen können. Unter normalen Umständen verbinden sich die Benutzer Ihrer Belegschaft beispielsweise über einen zentralen Identitätsanbieter (SEC02-BP04) mit der Cloud, um ihre Workloads zu verwalten. Wenn der zentrale Identitätsanbieter jedoch ausfällt oder die Konfiguration für den Verbund in der Cloud geändert wird, können sich die Benutzer in Ihrem Unternehmen möglicherweise nicht mit der Cloud verbinden. Ein Prozess für den Notfallzugriff ermöglicht autorisierten Administratoren den Zugriff auf Ihre Cloud-Ressourcen über alternative Verfahren (z. B. eine alternative Form des Verbunds oder direkter Benutzerzugriff), um Probleme mit Ihrer Verbundkonfiguration oder Ihren Workloads zu beheben. Der Prozess für den Notfallzugriff wird verwendet, bis der normale Verbundmechanismus wiederhergestellt ist.

Gewünschtes Ergebnis:

- Sie haben die Ausfallmodi definiert und dokumentiert, die als Notfall gelten: Berücksichtigen Sie dabei Ihre normalen Abläufe und die Systeme, auf die Ihre Benutzer angewiesen sind, um ihre Workloads zu verwalten. Überlegen Sie, wie jede dieser Abhängigkeiten ausfallen und zu einer Notsituation führen kann. Möglicherweise finden Sie die Fragen und bewährten Methoden in der Säule der Zuverlässigkeit hilfreich, um Ausfallarten zu identifizieren und widerstandsfähigere Systeme zu entwickeln, bei denen die Wahrscheinlichkeit von Ausfällen geringer ist.
- Sie haben die Schritte dokumentiert, die befolgt werden müssen, um einen Ausfall als Notfall zu identifizieren. Sie können beispielsweise festlegen, dass Ihre Identitätsadministratoren den Status Ihrer primären und Standby-Identitätsanbieter überprüfen müssen und, falls beide nicht verfügbar sind, ein Notfallereignis für den Ausfall eines Identitätsanbieters feststellen.
- Sie haben einen Prozess für den Notfallzugriff definiert, der für jeden Notfall- oder Ausfallmodus spezifisch ist. Wenn Sie hier möglichst detaillierte Informationen angeben, kann dies der Neigung Ihrer Benutzer entgegenwirken, einen allgemeinen Prozess für alle Arten von Notfällen zu stark zu nutzen. Ihre Prozesse für den Notfallzugriff beschreiben die Umstände, unter denen ein Prozess jeweils verwendet werden sollte, und umgekehrt Situationen, in denen der Prozess nicht verwendet werden sollte. In diesem Fall wird auf alternative Prozesse hingewiesen, die zutreffen können.

- Ihre Prozesse sind mit detaillierten Anweisungen und Playbooks, die schnell und effizient befolgt werden können, gut dokumentiert. Denken Sie daran, dass ein Notfallereignis Stress für Ihre Benutzer bedeuten kann und dass sie unter extremem Zeitdruck stehen können. Gestalten Sie Ihren Prozess daher so einfach wie möglich.

Typische Anti-Muster:

- Sie verfügen nicht über gut dokumentierte und gut getestete Prozesse für den Notfallzugriff. Ihre Benutzer sind nicht auf einen Notfall vorbereitet und nutzen improvisierte Prozesse, wenn er eintritt.
- Ihre Prozesse für den Notfallzugriff hängen von denselben Systemen (z. B. einem zentralen Identitätsanbieter) ab wie Ihre normalen Zugriffsmechanismen. Das bedeutet, dass der Ausfall eines solchen Systems sowohl Ihre normalen Zugriffsmechanismen als auch Ihre Notfallzugriffsmechanismen betrifft und Ihre Fähigkeit zur Wiederherstellung nach dem Ausfall beeinträchtigen kann.
- Ihre Prozesse für den Notfallzugriff werden in Situationen verwendet, die keine Notfälle sind. Ein Beispiel könnte sein, dass Ihre Benutzer Prozesse für den Notfallzugriff häufig missbrauchen, da es für sie einfacher ist, Änderungen direkt vorzunehmen, als Änderungen über eine Pipeline einzureichen.
- Ihre Prozesse für den Notfallzugriff generieren nicht genügend Protokolle, um sie zu überwachen, oder die Protokolle werden nicht so überwacht, dass Sie bei einem möglichen Missbrauch der Prozesse gewarnt werden.

Vorteile der Nutzung dieser bewährten Methode:

- Durch gut dokumentierte und gut getestete Prozesse für den Notfallzugriff können Sie die Zeit reduzieren, die Ihre Benutzer benötigen, um auf ein Notfallereignis zu reagieren und es zu beheben. Dies kann zu kürzeren Ausfallzeiten und einer höheren Verfügbarkeit der Services führen, die Sie für Ihre Kunden bereitstellen.
- Sie können jede Notfallzugriffsanfrage verfolgen und unbefugte Versuche, den Prozess für Nicht-Notfallereignisse zu missbrauchen, erkennen und darauf hinweisen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Dieser Abschnitt enthält Richtlinien zur Erstellung von Prozessen für den Notfallzugriff für verschiedene Ausfallmodi im Zusammenhang mit Workloads, die in AWS bereitgestellt werden. Zunächst finden Sie allgemeine Leitlinien, die für alle Ausfallmodi gelten, und danach spezifische Anleitungen für die verschiedenen Arten von Ausfallmodi.

Allgemeine Leitlinien für alle Ausfallmodi

Beachten Sie beim Entwerfen eines Prozesses für den Notfallzugriff für einen Ausfallmodus Folgendes:

- Dokumentieren Sie die Voraussetzungen und Annahmen für den Prozess: Wann soll der Prozess verwendet werden und wann nicht? Es ist hilfreich, den Ausfallmodus detailliert zu beschreiben und Annahmen zu dokumentieren, z. B. den Zustand anderer verwandter Systeme. Der Prozess für den Ausfallmodus 2 geht beispielsweise davon aus, dass der Identitätsanbieter verfügbar ist, aber die Konfiguration in AWS geändert wurde oder abgelaufen ist.
- Erstellen Sie im Voraus Ressourcen, die für den Notfallzugriffsprozess benötigt werden (SEC10-BP05). Erstellen Sie beispielsweise vorab das AWS-Konto für den Notfallzugriff mit IAM-Benutzern und -Rollen sowie die kontoübergreifenden IAM-Rollen in allen Workload-Konten. So wird sichergestellt, dass diese Ressourcen bereit und verfügbar sind, wenn ein Notfallereignis eintritt. Durch die Vorab-Erstellung von Ressourcen sind Sie nicht von APIs der AWS-Steuerebene (zum Erstellen und Ändern von AWS-Ressourcen verwendet) abhängig, die im Notfall möglicherweise nicht verfügbar sind. Darüber hinaus müssen Sie durch die Vorab-Erstellung von IAM-Ressourcen keine potenziellen Verzögerungen aufgrund der letztendlichen Datenkonsisten berücksichtigen.
- Schließen Sie Prozesse für den Notfallzugriff in Ihre Vorfallmanagementpläne ein (SEC10-BP02). Dokumentieren Sie, wie Notfallereignisse nachverfolgt und an andere in Ihrem Unternehmen, z. B. an Peer-Teams, Führungskräfte und gegebenenfalls extern an Kunden und Geschäftspartner, kommuniziert werden sollen.
- Definieren Sie den Prozess für Notfallzugriffsanfragen in Ihrem bestehenden Workflow-System für Serviceanfragen, falls eines vorhanden ist. In der Regel können Sie mit solchen Workflow-Systemen Eingabeformulare erstellen, um Informationen zur Anfrage zu erfassen, die Anfrage in jeder Phase des Workflows zu verfolgen und sowohl automatisierte als auch manuelle Genehmigungsschritte hinzuzufügen. Ordnen Sie jede Anfrage einem entsprechenden Notfallereignis zu, das in Ihrem Vorfallmanagement-System verfolgt wird. Mit einem einheitlichen System für Notfallzugriffe können Sie diese Anfragen in einem zentralen System verfolgen, Nutzungstrends analysieren und Ihre Prozesse verbessern.

- Stellen Sie sicher, dass Ihre Notfallzugriffsprozesse nur von autorisierten Benutzern initiiert werden können, und legen Sie fest, dass Genehmigungen von Kollegen oder Führungskräften des Benutzers erforderlich sind. Der Genehmigungsprozess sollte sowohl während als auch außerhalb der Geschäftszeiten funktionieren. Definieren Sie, wie Genehmigungsanfragen sekundäre Genehmiger berücksichtigen, falls die primären Genehmiger nicht verfügbar sind, und wie sie in Ihrer Managementkette nach oben eskaliert werden, bis sie genehmigt wurden.
- Implementieren Sie robuste Protokollierungs-, Überwachungs- und Warnmechanismen für den Notfallzugriffsprozess und die entsprechenden Mechanismen. Generieren Sie detaillierte Auditprotokolle für alle erfolgreichen und fehlgeschlagenen Versuche, Notfallzugriff zu erhalten. Korrelieren Sie die Aktivität mit laufenden Notfallereignissen aus Ihrem Vorfallmanagement-System und senden Sie Benachrichtigungen, wenn Aktionen außerhalb der erwarteten Zeiträume erfolgen oder wenn das Notfallzugriffskonto während des normalen Betriebs verwendet wird. Auf das Notfallkonto sollte nur in Notfällen zugegriffen werden, da Break-Glass-Verfahren als Hintertür betrachtet werden sollten. Integrieren Sie dies in Ihr SIEM-Tool (Security Information and Event Management) oder AWS Security Hub CSPM, um alle Aktivitäten während der Notfallzugriffsphase zu melden und zu überprüfen. Sobald Sie zum normalen Betrieb zurückkehren, rotieren Sie die Anmeldeinformationen für den Notfallzugriff automatisch und benachrichtigen Sie die zuständigen Teams.
- Testen Sie die Notfallzugriffsprozesse regelmäßig, um sicherzustellen, dass die Schritte klar sind und die richtigen Zugriffsebenen schnell und effizient gewährt werden. Ihre Notfallzugriffsprozesse sollten im Rahmen von Incident-Response-Simulationen (SEC10-BP07) und Notfallwiederherstellungs-Tests (REL13-BP03) getestet werden.

Ausfallmodus 1: Der für den Verbund mit AWS verwendete Identitätsanbieter ist nicht verfügbar

Wie in SEC02-BP04 Verlassen auf einen zentralen Identitätsanbieter beschrieben, wird empfohlen, sich auf einen zentralen Identitätsanbieter zu verlassen, der die Benutzer Ihres Unternehmens verbindet, um den Zugriff auf AWS-Konten zu gewähren. Sie können mit IAM Identity Center einen Verbund für mehrere AWS-Konten in Ihrer AWS-Organisation implementieren oder einzelne AWS-Konten mit IAM verbinden. In beiden Fällen authentifizieren sich die Benutzer in Ihrer Belegschaft beim zentralen Identitätsanbieter, bevor sie zu einem AWS-Anmeldeendpunkt für das Single Sign-On weitergeleitet werden.

Im unwahrscheinlichen Fall, dass der zentrale Identitätsanbieter nicht verfügbar ist, können sich die Benutzer Ihrer Belegschaft nicht mit AWS-Konten verbinden oder ihre Workloads verwalten. In einem solchen Notfall können Sie einen Notfallzugriffsprozess für eine kleine Gruppe von Administratoren einrichten, die auf AWS-Konten zugreifen dürfen, um kritische Aufgaben auszuführen, die nicht

warten können, bis die zentralen Identitätsanbieter wieder online sind. Nehmen Sie beispielsweise an, dass Ihr Identitätsanbieter für 4 Stunden nicht verfügbar ist und während dieses Zeitraums die Obergrenzen einer Amazon EC2 Auto Scaling-Gruppe in einem Produktionskonto geändert werden müssen, um einen unerwarteten Anstieg des Kundendatenverkehrs zu bewältigen. Ihre Notfalladministratoren sollten den Notfallzugriffsprozess befolgen, um Zugriff auf das spezifische AWS-Konto in der Produktion zu erhalten und die erforderlichen Änderungen vorzunehmen.

Der Notfallzugriffsprozess basiert auf einem vorab erstellten AWS-Konto für den Notfallzugriff, das ausschließlich für den Notfallzugriff verwendet wird und über AWS-Ressourcen (wie IAM-Rollen und IAM-Benutzer) zur Unterstützung des Notfallzugriffsprozesses verfügt. Während des normalen Betriebs sollte niemand auf das Notfallzugriffskonto zugreifen. Sie müssen dieses Konto auf Missbrauch überwachen und ggf. Warnungen senden (weitere Informationen finden Sie im vorherigen Abschnitt mit allgemeinen Leitlinien).

Das Notfallzugriffskonto verfügt über IAM-Notfallzugriffsrollen mit der Berechtigung, kontoübergreifende Rollen in den AWS-Konten anzunehmen, für die Notfallzugriff erforderlich ist. Diese IAM-Rollen sind vordefiniert und mit Vertrauensrichtlinien konfiguriert, die den IAM-Rollen des Notfallkontos vertrauen.

Der Notfallzugriffsprozess kann einen der folgenden Ansätze verwenden:

- Sie können im Notfallzugriffskonto vorab eine Gruppe von IAM-Benutzern mit zugehörigen sicheren Passwörtern und MFA-Token für Ihre Notfalladministratoren erstellen. Diese IAM-Benutzer verfügen über Berechtigungen, die IAM-Rollen anzunehmen, die dann den kontoübergreifenden Zugriff auf das AWS-Konto ermöglichen, für das der Notfallzugriff erforderlich ist. Wir empfehlen, so wenige solcher Benutzer wie möglich zu erstellen und jeden Benutzer einem einzelnen Notfalladministrator zuzuweisen. Während eines Notfalls meldet sich ein Notfalladministrator mit seinem Passwort und seinem MFA-Tokencode beim Notfallzugriffskonto an, wechselt zur IAM-Notfallzugriffsrolle im Notfallkonto und wechselt schließlich zur IAM-Notfallzugriffsrolle im Workload-Konto, um die für den Notfall erforderliche Änderungsaktion durchzuführen. Der Vorteil dieses Ansatzes besteht darin, dass jeder IAM-Benutzer einem Notfalladministrator zugewiesen ist und Sie anhand der CloudTrail-Ereignisse feststellen können, welcher Benutzer sich angemeldet hat. Der Nachteil ist, dass Sie mehrere IAM-Benutzer mit den zugehörigen langlebigen Passwörtern und MFA-Token verwalten müssen.
- Sie können den Root-Benutzer des AWS-Kontos für den Notfallzugriff verwenden, um sich beim Notfallzugriffskonto anzumelden, die IAM-Rolle für den Notfallzugriff anzunehmen und dann die kontoübergreifende Rolle im Workload-Konto anzunehmen. Wir empfehlen, ein sicheres Passwort und mehrere MFA-Token für den Root-Benutzer festzulegen. Wir empfehlen außerdem, das

Passwort und die MFA-Token in einem sicheren Vault für Unternehmensanmeldeinformationen zu speichern, der eine starke Authentifizierung und Autorisierung erzwingt. Sie sollten das Passwort und die Faktoren zum Zurücksetzen des MFA-Tokens sichern: Legen Sie die E-Mail-Adresse für das Konto auf eine E-Mail-Verteilerliste fest, die von Ihren Cloud-Sicherheitsadministratoren überwacht wird. Legen Sie die Telefonnummer des Kontos auf eine gemeinsam genutzte Telefonnummer fest, die ebenfalls von Sicherheitsadministratoren überwacht wird. Der Vorteil dieses Ansatzes besteht darin, dass nur ein Satz von Root-Benutzeranmeldeinformationen verwaltet werden muss. Der Nachteil ist, dass sich mehrere Administratoren als Root-Benutzer anmelden können, da es sich um einen gemeinsam genutzten Benutzer handelt. Sie müssen die Protokollereignisse für den Unternehmens-Vault überprüfen, um festzustellen, welcher Administrator das Passwort für den Root-Benutzer ausgecheckt hat.

Ausfallmodus 2: Die Konfiguration des Identitätsanbieters in AWS wurde geändert oder ist abgelaufen

Um den Verbund der Benutzer in Ihrem Unternehmen mit AWS-Konten zu ermöglichen, können Sie IAM Identity Center mit einem externen Identitätsanbieter konfigurieren oder einen IAM-Identitätsanbieter erstellen (SEC02-BP04). In der Regel konfigurieren Sie diese, indem Sie ein XML-Dokument mit SAML-Metadaten importieren, das von Ihrem Identitätsanbieter bereitgestellt wird. Das XML-Metadatendokument enthält ein X.509-Zertifikat, das einem privaten Schlüssel entspricht, mit dem der Identitätsanbieter seine SAML-Zusicherungen signiert.

Diese Konfigurationen auf AWS-Seite können versehentlich von einem Administrator geändert oder gelöscht werden. In einem anderen Szenario läuft das in AWS importierte X.509-Zertifikat möglicherweise ab und eine neue XML-Metadatendatei mit einem neuen Zertifikat wurde noch nicht in AWS importiert. In beiden Szenarien kann der Verbund mit AWS für die Benutzer Ihrer Belegschaft unterbrochen werden, was zu einem Notfall führt.

In einem solchen Notfall können Sie Ihren Identitätsadministratoren Zugriff auf AWS gewähren, um die Verbundprobleme zu beheben. Ihr Identitätsadministrator verwendet beispielsweise den Notfallzugriffsprozess, um sich beim AWS-Konto für den Notfallzugriff anzumelden. Er wechselt zu einer Rolle im Identity Center-Administratorkonto und aktualisiert die Konfiguration des externen Identitätsanbieters, indem er das aktuelle XML-Dokument mit SAML-Metadaten von Ihrem Identitätsanbieter importiert, um den Verbund wieder zu aktivieren. Sobald der Verbund wiederhergestellt ist, verwenden die Benutzer in Ihrer Belegschaft weiter den normalen Betriebsprozess, um sich mit ihren Workload-Konten zu verbinden.

Sie können die oben für Ausfallmodus 1 beschriebenen Vorgehensweisen befolgen, um einen Notfallzugriffsprozess zu erstellen. Sie können Ihren Identitätsadministratoren Berechtigungen

nach dem Prinzip der geringsten Berechtigung gewähren, sodass sie nur auf das Identity Center-Administratorkonto zugreifen und nur in diesem Konto Aktionen für Identity Center ausführen können.

Ausfallmodus 3: Störung von Identity Center

Für den unwahrscheinlichen Fall einer Störung von IAM Identity Center oder einer AWS-Region empfehlen wir, eine Konfiguration einzurichten, mit der Sie temporären Zugriff auf die AWS-Managementkonsole gewähren können.

Der Notfallzugriffsprozess verwendet einen direkten Verbund von Ihrem Identitätsanbieter zu IAM in einem Notfallkonto. Einzelheiten zu den Prozess- und Entwurfsüberlegungen finden Sie im Artikel zum Einrichten des Notfallzugriffs auf die AWS-Managementkonsole.

Implementierungsschritte

Allgemeine Schritte für alle Ausfallmodi

- Erstellen Sie ein AWS-Konto speziell für Notfallzugriffsprozesse. Erstellen Sie vorab die für das Konto benötigten IAM-Ressourcen wie IAM-Rollen oder IAM-Benutzer und optional IAM-Identitätsanbieter. Erstellen Sie außerdem vorab kontoübergreifende IAM-Rollen in den AWS-Konten für die Workload mit Vertrauensbeziehungen zu den entsprechenden IAM-Rollen im Notfallzugriffskonto. Sie können CloudFormation-StackSets mit AWS Organizations verwenden, um solche Ressourcen in den Mitgliedskonten Ihrer Organisation zu erstellen.

- Erstellen Sie AWS Organizations-Service-Kontrollrichtlinien (SCP), um das Löschen und Ändern der kontoübergreifenden IAM-Rollen in den AWS-Konten der Mitglieder zu verweigern.
- Aktivieren Sie CloudTrail für das AWS-Konto für den Notfallzugriff und senden Sie die Trail-Ereignisse an einen zentralen S3-Bucket im AWS-Konto für die Protokollerfassung. Wenn Sie AWS Control Tower verwenden, um Ihre AWS-Umgebung mit mehreren Konten einzurichten und zu verwalten, ist für jedes Konto, das Sie mit AWS Control Tower erstellen oder in AWS Control Tower registrieren, CloudTrail standardmäßig aktiviert und wird an einen S3-Bucket in einem dedizierten AWS-Konto für das Protokollarchiv gesendet.
- Überwachen Sie die Aktivitäten des Notfallzugriffskontos, indem Sie EventBridge-Regeln erstellen, die bei der Anmeldung in der Konsole und bei API-Aktivitäten durch die IAM-Notfallrollen greifen. Senden Sie Benachrichtigungen an Ihr Security Operations Center, wenn Aktivitäten außerhalb eines laufenden Notfallereignisses stattfinden, das in Ihrem Vorfallmanagement-System nachverfolgt wurde.

Zusätzliche Schritte für Ausfallmodus 1 (Der für den Verbund mit AWS verwendete Identitätsanbieter ist nicht verfügbar) und Ausfallmodus 2 (Die Konfiguration des Identitätsanbieters in AWS wurde geändert oder ist abgelaufen)

- Erstellen Sie vorab Ressourcen, je nachdem, welchen Mechanismus Sie für den Notfallzugriff wählen:
  - IAM-Benutzer verwenden: Erstellen Sie vorab die IAM-Benutzer mit sicheren Passwörtern und den zugehörigen MFA-Geräten.
  - Root-Benutzer des Notfallkontos verwenden: Konfigurieren Sie den Root-Benutzer mit einem sicheren Passwort und speichern Sie das Passwort im Unternehmens-Vault für Anmeldeinformationen. Ordnen Sie dem Root-Benutzer mehrere physische MFA-Geräte zu und bewahren Sie die Geräte an Orten auf, zu denen die Mitglieder Ihres Notfalladministratorteams schnell Zugang haben.

Zusätzliche Schritte für den Ausfallmodus 3 (Störung von Identity Center

- Erstellen Sie wie im Artikel zum Einrichten des Notfallzugriffs auf die AWS-Managementkonsole erläutert im AWS-Konto für den Notfallzugriff einen IAM-Identitätsanbieter, um den direkten SAML-Verbund von Ihrem Identitätsanbieter aus zu ermöglichen.
- Erstellen Sie Notfalleinsatzgruppen in Ihrem Identitätsanbieter ohne Mitglieder.
- Erstellen Sie IAM-Rollen, die den Notfalleinsatzgruppen im Notfallzugriffskonto entsprechen.

Ressourcen

Zugehörige bewährte Methoden für Well-Architected:

- SEC02-BP04 Verlassen auf einen zentralen Identitätsanbieter
- SEC03-BP02 Gewähren des Zugriffs mit den geringsten Berechtigungen
- SEC10-BP02 Entwickeln von Vorfallmanagementplänen
- SEC10-BP07 Durchführen von Gamedays

Zugehörige Dokumente:

- Artikel zum Einrichten des Notfallzugriffs auf die AWS-Managementkonsole
- Aktivieren von Zugriff auf die für SAML-2.0-Verbundbenutzer AWS-Managementkonsole

- Break Glass“-Zugriff

Zugehörige Videos:

- AWS re:Invent 2022 – Vereinfachen des vorhandenen Mitarbeiterzugriffs mit IAM Identity Center
- AWS re:Inforce 2022 – AWS Identity and Access Management (IAM) Vertiefung

Zugehörige Beispiele:

- AWS Rolle „Break Glass
- AWS Customer Playbook Framework
- AWS Beispiele von Playbooks für die Vorfallsreaktion

SEC03-BP04 Kontinuierliche Reduzierung der Berechtigungen

Wenn Ihre Teams bestimmen, welchen Zugriff sie benötigen, entfernen Sie unnötige Berechtigungen und erstellen Sie Überprüfungsprozesse, damit jederzeit dem Prinzip der geringsten Berechtigung entsprochen wird. Überwachen Sie Ihre Identitäten kontinuierlich und entfernen Sie ungenutzte Identitäten und Berechtigungen für den Zugriff von Menschen und Maschinen.

Gewünschtes Ergebnis: Die Genehmigungsrichtlinien sollten dem Prinzip der geringsten Berechtigung entsprechen. Wenn Zuständigkeiten und Rollen immer besser definiert werden, müssen Sie Ihre Berechtigungsrichtlinien prüfen, um unnötige Berechtigungen zu entfernen. Dieses Konzept verringert die Auswirkungen, wenn Anmeldeinformationen versehentlich offengelegt werden oder wenn anderweitig ohne Genehmigung darauf zugegriffen wird.

Typische Anti-Muster:

- Standardmäßige Gewährung von Administratorberechtigungen für Benutzer
- Erstellung übermäßig großzügiger Richtlinien, jedoch ohne vollständige Administratorberechtigungen
- Aufbewahrung von Berechtigungsrichtlinien, nachdem sie nicht mehr benötigt werden

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Wenn Teams und Projekte gerade erst mit der Arbeit beginnen, können lockere Richtlinien verwendet werden, um Innovationen und Agilität zu unterstützen. So könnten beispielsweise Entwickler in einer Entwicklungs- und Testumgebung Zugang zu einer breiten Palette von AWS-Services erhalten. Wir empfehlen, den Zugriff kontinuierlich zu prüfen und auf Services und Serviceaktionen einzuschränken, die für die anstehende Aufgabe wirklich benötigt werden. Wir empfehlen diese Evaluierung für menschliche und für maschinelle Identitäten. Maschinenidentitäten, manchmal auch als System- oder Servicekonten bezeichnet, sind Identitäten, die AWS den Zugriff auf Anwendungen oder Server ermöglichen. Dieser Zugriff ist besonders in einer Produktionsumgebung wichtig, in der übermäßig lockere Zugriffsregeln weitreichende Auswirkungen haben und möglicherweise Kundendaten offen legen könnten.

AWS bietet mehrere Verfahren zur Unterstützung der Identifizierung nicht verwendeter Benutzer, Rollen, Berechtigungen und Anmeldeinformationen. AWS kann auch bei der Analyse von Zugriffsaktivitäten von IAM-Benutzern und -Rollen helfen, darunter ebenfalls Analysen zu zugehörigen Zugriffsschlüsseln sowie zum Zugriff auf AWS-Ressourcen wie etwa Objekten in Amazon S3-Buckets. Die Generierung von Richtlinien mit AWS Identity and Access Management Access Analyzer kann Ihnen bei der Erstellung restriktiver Berechtigungsrichtlinien auf der Grundlage der Services und Aktionen helfen, mit denen ein Prinzipal tatsächlich interagiert. Die attributbasierte Zugriffskontrolle (ABAC) kann zur Vereinfachung der Berechtigungsverwaltung beitragen, da Sie Benutzern anhand ihrer Attribute Berechtigungen erteilen können, anstatt jedem Benutzer direkt Berechtigungsrichtlinien zuzuweisen.

Implementierungsschritte

- AWS Identity and Access Management Access Analyzer verwenden: IAM Access Analyzer hilft Ihnen, die Ressourcen in Ihrer Organisation und Ihren Konten zu identifizieren, die mit einer externen Entität geteilt werden (z. B. Amazon Simple Storage Service (Amazon S3)-Buckets oder IAM-Rollen).
- Das Generieren von IAM Access Analyzer-Richtlinien verwenden: Mit dem Generieren von IAM Access Analyzer-Richtlinien können Sie detaillierte Berechtigungsrichtlinien erstellen, die auf der Zugriffsaktivität eines IAM-Benutzers oder einer IAM-Rolle basieren.
- Vor der Produktionsphase Berechtigungen in weniger kritischen Umgebungen testen: Verwenden Sie zunächst die weniger kritischen Sandbox- und Entwicklungsumgebungen, um die für verschiedene Tätigkeitsbereiche erforderlichen Berechtigungen mit IAM Access Analyzer zu testen. Verschärfen und validieren Sie dann schrittweise diese Berechtigungen in allen Test-, Qualitätssicherungs- und Staging-Umgebungen, bevor Sie sie für die Produktion anwenden.

In den weniger kritischen Umgebungen können zunächst lockerere Berechtigungen gelten, da Service-Kontrollrichtlinien (SCPs) Integritätsschutz durchsetzen, indem sie die maximal erteilten Berechtigungen einschränken.

- Einen akzeptablen Zeitrahmen und eine akzeptable Nutzungsrichtlinie für IAM-Benutzer und -Rollen festlegen: Verwenden Sie den Zeitstempel des letzten Zugriffs, um ungenutzte Benutzer und Rollen zu identifizieren und sie zu entfernen. Überprüfen Sie die Informationen zum letzten Service- und Aktionszugriff überprüfen, um Berechtigungen für bestimmte Benutzer und Rollen zu identifizieren und festzulegen. Sie können beispielsweise Informationen zum letzten Zugriff verwenden, um die spezifischen Amazon S3-Aktionen zu identifizieren, die Ihre Anwendungsrolle erfordert, und den Zugriff der Rolle auf diese Aktionen beschränken. Features für die zuletzt abgerufenen Informationen sind in der AWS-Managementkonsole und programmgesteuert verfügbar, damit Sie sie in Ihre Infrastruktur-Workflows und automatisierten Tools integrieren können.
- Protokollierung von Datenereignissen in AWS CloudTrail erwägen: Standardmäßig protokolliert CloudTrail keine Datenereignisse wie Amazon S3-Aktivitäten auf Objektebene (zum Beispiel `GetObject` und `DeleteObject`) oder Amazon DynamoDB-Tabellenaktivitäten (zum Beispiel `PutItem` und `DeleteItem`). Erwägen Sie die Verwendung der Protokollierung dieser Ereignisse, um zu ermitteln, welche Benutzer und Rollen Zugriff auf bestimmte Amazon S3-Objekte oder DynamoDB-Tabellenelemente benötigen.

Ressourcen

Zugehörige Dokumente:

- Gewähren der geringsten Berechtigung
- Entfernen unnötiger Anmeldeinformationen
- Was ist AWS CloudTrail?
- Arbeiten mit -Richtlinien
- Protokollierung und Überwachung in DynamoDB
- Verwenden der CloudTrail-Ereignisprotokollierung für Amazon S3-Buckets und -Objekte
- Abrufen von Berichten zu Anmeldeinformationen für Ihr AWS-Konto

Zugehörige Videos:

- Experte für IAM-Richtlinien in unter 60 Minuten

- Trennung von Pflichten, geringste Berechtigung, Delegierung und CI/CD
- AWS re:Inforce 2022 – AWS Identity and Access Management (IAM) Vertiefung

SEC03-BP05 Definieren eines Integritätsschutzes für Berechtigungen in Ihrer Organisation

Verwenden Sie Maßnahmen zum Integritätsschutz, um den Umfang der verfügbaren Berechtigungen, die Prinzipalen gewährt werden können, einzuschränken. Die Bewertungskette für Genehmigungsrichtlinien umfasst Ihren Integritätsschutz, um bei Autorisierungsentscheidungen die effektiven Berechtigungen eines Prinzipals zu bestimmen. Sie können Maßnahmen zum Integritätsschutz mit einem ebenenbasierten Ansatz definieren. Wenden Sie einige Maßnahmen zum Integritätsschutz allgemein für Ihre gesamte Organisation an und andere granular auf Sitzungen mit temporärem Zugriff.

Gewünschtes Ergebnis: Die Umgebungen sind durch die Verwendung separater AWS-Konten klar voneinander abgegrenzt. Service-Kontrollrichtlinien (SCP) werden verwendet, um organisationsweite Maßnahmen zum Integritätsschutz zu definieren. Umfassender angelegte Maßnahmen zu Integritätsschutz werden auf den Hierarchieebenen festgelegt, die der Root Ihrer Organisation am nächsten sind, und strengerer Integritätsschutz wird näher an der Ebene der einzelnen Konten festgelegt.

Sofern unterstützt, definieren Ressourcenrichtlinien die Bedingungen, die ein Prinzipal erfüllen muss, um Zugriff auf eine Ressource zu erhalten. Die Ressourcenrichtlinien schränken auch den Umfang der erlaubten Aktionen ein, wo dies angebracht ist. Berechtigungsgrenzen werden auf Prinzipale verteilt, die Workload-Berechtigungen verwalten und die Verwaltung von Berechtigungen an einzelne Workload-Besitzer delegieren.

Typische Anti-Muster:

- AWS-Konten für Mitglieder werden innerhalb einer AWS-Organisation erstellt, ohne dass SCPs verwendet werden, um die Nutzung und die für ihre Root-Anmeldeinformationen verfügbaren Rechte einzuschränken.
- Zuweisung von Berechtigungen auf der Grundlage der geringsten Berechtigung, aber kein Integritätsschutz für die maximale Anzahl von Berechtigungen, die gewährt werden können
- Sie verlassen sich bei der Einschränkung von Berechtigungen auf die implizite Ablehnungsgrundlage von AWS IAM und vertrauen darauf, dass Richtlinien keine unerwünschte ausdrückliche Genehmigungsberechtigung gewähren.

- Mehrere Workload-Umgebungen im selben AWS-Konto ausführen und sich dann auf Mechanismen wie VPCs, Tags oder Ressourcenrichtlinien verlassen, um Berechtigungsgrenzen durchzusetzen

Vorteile der Nutzung dieser bewährten Methode: Durch den Integritätsschutz für Berechtigungen kann das Vertrauen gestärkt werden, dass keine unerwünschten Berechtigungen erteilt werden können, selbst wenn eine Berechtigungsrichtlinie dies versucht. Dies kann die Definition und Verwaltung von Berechtigungen vereinfachen, da der maximale Umfang der zu berücksichtigenden Berechtigungen reduziert wird.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Wir empfehlen Ihnen, einen ebenenbasierten Ansatz zu verwenden, um für Maßnahmen für den Integritätsschutz für Ihre Organisation zu definieren. Dieser Ansatz reduziert systematisch die maximale Anzahl der möglichen Berechtigungen, wenn weitere Ebenen hinzugefügt werden. So können Sie den Zugriff nach dem Prinzip der geringsten Berechtigung gewähren und das Risiko eines unbeabsichtigten Zugriffs aufgrund einer falschen Konfiguration der Richtlinie verringern.

Der erste Schritt zur Einrichtung zum Integritätsschutz ist die Isolierung Ihrer Workloads und Umgebungen in getrennten AWS-Konten. Prinzipale eines Kontos können ohne ausdrückliche Genehmigung nicht auf Ressourcen in einem anderen Konto zugreifen, selbst wenn sich beide Konten in derselben AWS-Organisation oder derselben Organisationseinheit (OE) befinden. Sie können OEs verwenden, um Konten zu gruppieren, die Sie als eine Einheit verwalten möchten.

Der nächste Schritt besteht darin, die maximale Anzahl von Berechtigungen zu reduzieren, die Sie Prinzipalen innerhalb der Mitgliedskonten Ihrer Organisation erteilen können. Zu diesem Zweck können Sie Service-Kontrollrichtlinien (SCP) verwenden, die Sie entweder auf eine Organisationseinheit oder ein Konto anwenden können. SCPs können allgemeine Zugriffskontrollen durchsetzen, etwa die Beschränkung des Zugriffs auf bestimmte AWS-Regionen, die Verhinderung des Löschens von Ressourcen oder die Deaktivierung potenziell riskanter Serviceaktionen. SCPs, die Sie auf das Root-Verzeichnis Ihrer Organisation anwenden, wirken sich nur auf die Mitgliedskonten aus, nicht auf das Verwaltungskonto. SCPs regeln nur die Prinzipale innerhalb Ihrer Organisation. Ihre SCPs regeln keine Prinzipale außerhalb Ihrer Organisation, die auf Ihre Ressourcen zugreifen.

Wenn Sie AWS Control Tower verwenden, können Sie die Steuerungen und Landing Zones als Grundlage für Ihren Integritätsschutz für Berechtigungen und Ihre Multi-Konten-Umgebung nutzen. Die Landing Zones bieten eine vorkonfigurierte, sichere Basisumgebung mit getrennten

Konten für verschiedene Workloads und Anwendungen. Der Integritätsschutz setzt verbindliche Kontrollen in Bezug auf Sicherheit, Betrieb und Compliance durch eine Kombination aus Service-Kontrollrichtlinien (SCPs), AWS Config-Regeln und anderen Konfigurationen durch. Bei der Verwendung von Integritätsschutz und Landing Zones im Control Tower zusammen mit SCPs, die für die Kundenorganisation spezifisch sind, ist es jedoch kritisch, die in der AWS-Dokumentation beschriebenen Best Practices zu befolgen, um Konflikte zu vermeiden und eine angemessene Steuerung sicherzustellen. Detaillierte Empfehlungen zur Verwaltung von SCPs, Konten und Organisationseinheiten (OUs) in einer Control-Tower-Umgebung finden Sie in der AWS Control Tower-Anleitung für AWS Organizations.

Wenn Sie sich an diese Empfehlungen halten, können Sie den Integritätsschutz, die Landing Zones und die benutzerdefinierten SCPs von Control Tower effektiv nutzen. Gleichzeitig vermeiden Sie potenzielle Konflikte und stellen eine angemessene Verwaltung und Kontrolle Ihrer AWS-Umgebung mit mehreren Konten sicher.

Ein weiterer Schritt besteht darin, mithilfe von IAM-Ressourcenrichtlinien die verfügbaren Aktionen festzulegen, die Sie für die zugehörigen Ressourcen ausführen können – zusammen mit allen Bedingungen, die der aktuelle Prinzipal erfüllen muss. Dies kann so breit gefasst sein, dass alle Aktionen zugelassen werden, solange der Prinzipal Teil Ihrer Organisation ist (unter Verwendung des Bedingungsschlüssels PrincipalOrgID), oder so detailliert sein, dass nur bestimmte Aktionen einer bestimmten IAM-Rolle zugelassen werden. Sie können einen ähnlichen Ansatz mit Bedingungen in IAM-Rollenvertrauensrichtlinien verfolgen. Wenn eine Vertrauensrichtlinie für eine Ressource oder Rolle explizit einen Prinzipal im selben Konto wie die Rolle oder Ressource benennt, die sie regelt, benötigt dieser Prinzipal keine angehängte IAM-Richtlinie, die dieselben Berechtigungen gewährt. Wenn der Prinzipal ein anderes Konto hat als die Ressource, dann benötigt der Prinzipal eine angehängte IAM-Richtlinie, die diese Berechtigungen gewährt.

Oft möchte ein Workload-Team die für seine Workload erforderlichen Berechtigungen verwalten. Dazu muss es möglicherweise neue IAM-Rollen und Berechtigungsrichtlinien erstellen. Sie können den maximalen Umfang der Berechtigungen erfassen, die das Team innerhalb einer IAM-Berechtigungsgrenze gewähren darf, und dieses Dokument einer IAM-Rolle zuordnen, mit der das Team dann seine IAM-Rollen und -Berechtigungen verwalten kann. Dieser Ansatz kann dem Team die nötige Flexibilität bieten, die Aufgaben zu erledigen, und gleichzeitig die Risiken reduzieren, die durch einen IAM-Verwaltungszugriff entstehen.

Ein detaillierterer Schritt ist die Implementierung von Techniken zur Verwaltung des privilegierten Zugriffs (PAM) und zur Verwaltung des vorübergehend erhöhten Zugriffs (TEAM). Ein Beispiel für PAM ist die Anforderung an Prinzipale, sich mehrfach zu authentifizieren, bevor sie privilegierte

Aktionen durchführen. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs. TEAM benötigt eine Lösung, die die Genehmigung und den Zeitrahmen verwaltet, in dem ein Prinzipal erweiterten Zugriff haben darf. Eine Möglichkeit besteht darin, den Prinzipal vorübergehend in die Vertrauensrichtlinie für eine IAM-Rolle aufzunehmen, die über einen erweiterten Zugriff verfügt. Ein anderer Ansatz besteht darin, im Normalbetrieb die einem Prinzipal durch eine IAM-Rolle gewährten Berechtigungen mithilfe einer Sitzungsrichtlinie einzuschränken und diese Einschränkung dann während des genehmigten Zeitfensters vorübergehend aufzuheben. Weitere Informationen zu Lösungen, die AWS und ausgewählte Partner validiert haben, finden Sie unter Temporärer erweiterter Zugriff.

Implementierungsschritte

1. Isolieren Sie Ihre Workloads und Umgebungen in separaten AWS-Konten.
2. Verwenden Sie SCPs, um die maximale Anzahl von Berechtigungen zu reduzieren, die Prinzipalen innerhalb der Mitgliedskonten Ihrer Organisation gewährt werden können.
   a. Bei der Definition von SCPs zur Reduzierung der maximalen Anzahl von Berechtigungen, die Prinzipalen innerhalb der Mitgliedskonten Ihrer Organisation gewährt werden können, können Sie zwischen einer Zulassungsliste und einer Verweigerungsliste wählen. Die Zulassungslistenstrategie gibt explizit die zulässigen Zugriffe an und blockiert implizit alle anderen Zugriffe. Die Verweigerungslistenstrategie gibt explizit die unzulässigen Zugriffe an und lässt standardmäßig alle anderen Zugriffe zu. Beide Strategien haben Vor- und Nachteile. Die Entscheidung ist von den spezifischen Anforderungen und vom Risikomodell Ihres Unternehmens abhängig. Weitere Informationen finden Sie unter Strategie für die Verwendung von SCPs.
   b. Sehen Sie sich auch die Beispiele für Service-Kontrollrichtlinien an, um zu verstehen, wie Sie SCPs effektiv konstruieren können.
3. Verwenden Sie IAM-Ressourcenrichtlinien, um den Geltungsbereich einzugrenzen und Bedingungen für zulässige Aktionen auf Ressourcen festzulegen. Verwenden Sie Bedingungen in IAM-Rollenvertrauensrichtlinien, um Einschränkungen für die Übernahme von Rollen zu erstellen.
4. Weisen Sie IAM-Berechtigungsgrenzen zu IAM-Rollen zu, die Workload-Teams dann zur Verwaltung ihrer eigenen Workload-IAM-Rollen und -Berechtigungen verwenden können.
5. Evaluieren Sie PAM- und TEAM-Lösungen auf der Grundlage Ihrer Bedürfnisse.

Ressourcen

Zugehörige Dokumente:

- Datenperimeter in AWS
- Einrichten des Berechtigungs-Integritätsschutzes mithilfe von Datenperimetern
- Auswertungslogik für Richtlinien

Zugehörige Beispiele:

- Beispiele für Service-Kontrollrichtlinie

Zugehörige Tools:

- AWS Lösung: Temporäre erweiterte Zugriffsverwaltung
- Validierte Sicherheitspartnerlösungen für TEAM

SEC03-BP06 Zugriffsverwaltung basierend auf dem Lebenszyklus

Überwachen Sie die Berechtigungen, die Ihren Prinzipalen (Benutzern, Rollen und Gruppen) während ihres gesamten Lebenszyklus in Ihrer Organisation gewährt werden, und passen Sie sie an. Passen Sie die Gruppenmitgliedschaften an, wenn Benutzer ihre Rolle ändern, und entfernen Sie den Zugriff, wenn ein Benutzer die Organisation verlässt.

Gewünschtes Ergebnis: Sie überwachen und passen die Berechtigungen während des gesamten Lebenszyklus der Prinzipale innerhalb der Organisation an und reduzieren so das Risiko unnötiger Rechte. Sie gewähren den entsprechenden Zugriff, wenn Sie einen Benutzer anlegen. Sie ändern den Zugriff, wenn sich die Aufgaben des Benutzers ändern, und Sie entfernen den Zugriff, wenn der Benutzer nicht mehr aktiv ist oder die Organisation verlassen hat. Sie verwalten Änderungen an Ihren Benutzern, Rollen und Gruppen zentral. Sie verwenden die Automatisierung, um Änderungen in Ihren AWS-Umgebungen zu verbreiten.

Typische Anti-Muster:

- Sie erteilen Identitäten im Voraus übermäßige oder weitreichende Zugriffsrechte, die über das zunächst erforderliche Maß hinausgehen.
- Sie überprüfen und ändern die Zugriffsberechtigungen nicht, wenn sich Rollen und Verantwortlichkeiten der Identitäten im Laufe der Zeit ändern.
- Sie entfernen aktive Zugriffsberechtigungen nicht von inaktiven oder beendeten Identitäten. Dies erhöht das Risiko eines unbefugten Zugriffs.

- Sie nutzen keine Automatisierung, um den Lebenszyklus von Identitäten zu verwalten.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Verwalten Sie die Zugriffsprivilegien, die Sie Identitäten (z. B. Benutzern, Rollen, Gruppen) gewähren, sorgfältig und passen Sie sie im Laufe ihres Lebenszyklus an. Dieser Lebenszyklus umfasst die anfängliche Onboarding-Phase, laufende Änderungen der Rollen und Verantwortlichkeiten und schließlich das Offboarding oder die Kündigung. Verwalten Sie den Zugriff proaktiv je nach Stadium des Lebenszyklus, um die richtige Zugriffsstufe zu erhalten. Halten Sie sich an das Prinzip der geringsten Berechtigung, um Risiken durch übermäßige oder unnötige Zugriffsberechtigungen zu verringern.

Sie können den Lebenszyklus von IAM-Benutzern direkt innerhalb des AWS-Konto oder durch den Verbund Ihres Identitätsanbieters für Mitarbeiter mit AWS IAM Identity Center verwalten. Für IAM-Benutzer können Sie innerhalb des AWS-Konto Benutzer und die damit verbundenen Berechtigungen erstellen, ändern und löschen. Für Verbundbenutzer können Sie IAM Identity Center verwenden, um ihren Lebenszyklus zu verwalten. Hierzu synchronisieren Sie Benutzer- und Gruppeninformationen aus dem Identitätsanbieter Ihrer Organisation über das Protokoll System for Cross-domain Identity Management (SCIM).

SCIM ist ein offenes Standardprotokoll für die automatisierte Bereitstellung und Deprovisionierung von Benutzeridentitäten über verschiedene Systeme hinweg. Durch die Integration Ihres Identitätsanbieters mit IAM Identity Center unter Verwendung von SCIM können Sie Benutzer- und Gruppeninformationen automatisch synchronisieren und so sicherstellen, dass Zugriffsberechtigungen auf der Grundlage von Änderungen in der maßgeblichen Identitätsquelle Ihrer Organisation gewährt, geändert oder entzogen werden.

Wenn sich die Rollen und Zuständigkeiten der Mitarbeiter in Ihrer Organisation ändern, passen Sie ihre Zugriffsrechte entsprechend an. Sie können die Berechtigungssätze von IAM Identity Center verwenden, um verschiedene Job-Rollen oder -Verantwortlichkeiten zu definieren und sie mit den entsprechenden IAM-Richtlinien und -Berechtigungen zu verknüpfen. Wenn sich die Rolle eines Mitarbeiters ändert, können Sie die ihm zugewiesenen Berechtigungen aktualisieren, um die neuen Verantwortlichkeiten zu berücksichtigen. Vergewissern Sie sich, dass sie über den erforderlichen Zugriff verfügen, und halten Sie sich dabei an das Prinzip der geringsten Berechtigung.

Implementierungsschritte

1. Definieren und dokumentieren Sie einen Lebenszyklusprozess für die Zugriffsverwaltung, einschließlich Verfahren für die Gewährung des Erstzugriffs, regelmäßige Überprüfungen und das Offboarding.
2. Implementieren Sie IAM-Rollen, -Gruppen und -Berechtigungsgrenzen, um den Zugriff kollektiv zu verwalten und die maximal zulässigen Zugriffsstufen durchzusetzen.
3. Führen Sie eine Integration mit einem Anbieter von Verbundidentitäten (z. B. Microsoft Active Directory, Okta, Ping Identity) als autoritativer Quelle für Benutzer- und Gruppeninformationen mit IAM Identity Center durch.
4. Verwenden Sie das SCIM-Protokoll, um Benutzer- und Gruppeninformationen aus dem Identitätsanbieter mit dem Identitätsspeicher von IAM Identity Center zu synchronisieren.
5. Erstellen Sie in IAM Identity Center Berechtigungssätze, die verschiedene Jobrollen oder Verantwortlichkeiten in Ihrer Organisation repräsentieren. Definieren Sie die entsprechenden IAM-Richtlinien und -Berechtigungen für jeden Berechtigungssatz.
6. Führen Sie regelmäßige Zugriffsüberprüfungen, sofortigen Zugriffsentzug und eine kontinuierliche Verbesserung des Lebenszyklusprozesses der Zugriffsverwaltung ein.
7. Schulung und Sensibilisierung der Mitarbeiter für die bewährten Methoden der Zugriffsverwaltung.

Ressourcen

Zugehörige bewährte Methoden:

- SEC02-BP04 Verlassen auf einen zentralen Identitätsanbieter

Zugehörige Dokumente:

- Verwaltung Ihrer Identitätsquelle
- Verwaltung von Identitäten in IAM Identity Center
- Verwenden von AWS Identity and Access Management Access Analyzer
- Generieren von IAM Access Analyzer-Richtlinien

Zugehörige Videos:

- AWS re:Inforce 2023 – Temporäre erweiterte Zugriffsverwaltung mit AWS IAM Identity Center

- AWS re:Invent 2022 – Vereinfachen des vorhandenen Mitarbeiterzugriffs mit IAM Identity Center
- AWS re:Invent 2022 – Nutzung der Leistungsfähigkeit von IAM-Richtlinien und Einschränken der Berechtigungen mit Access Analyzer

SEC03-BP07 Analysieren des öffentlichen und kontoübergreifenden Zugriffs

Überwachen Sie kontinuierlich Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff betreffen. Beschränken Sie den öffentlichen und kontoübergreifenden Zugriff ausschließlich auf Ressourcen, die diese Art von Zugriff benötigen.

Gewünschtes Ergebnis: Sie wissen, welche Ihrer AWS-Ressourcen für welche Benutzer freigegeben sind. Überwachen und prüfen Sie kontinuierlich Ihre freigegebenen Ressourcen, um sicherzustellen, dass sie nur für autorisierte Prinzipale freigegeben sind.

Typische Anti-Muster:

- Fehlendes Inventar gemeinsam genutzter Ressourcen
- Nichtbefolgung eines Prozesses zur Genehmigung von kontoübergreifendem oder öffentlichem Zugriff auf Ressourcen

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

Implementierungsleitfaden

Wenn sich Ihr Konto in AWS Organizations befindet, können Sie den Zugriff auf Ressourcen der gesamten Organisation, bestimmten Organisationseinheiten oder einzelnen Konten gewähren. Wenn Ihr Konto nicht zu einer Organisation gehört, können Sie Ressourcen für einzelne Konten freigeben. Sie können direkten kontoübergreifenden Zugriff gewähren, indem Sie ressourcenbasierte Richtlinien verwenden (z. B. die Richtlinien für Amazon Simple Storage Service (Amazon S3)-Buckets) oder indem Sie einem Prinzipal in einem anderen Konto erlauben, eine IAM-Rolle in Ihrem Konto zu übernehmen. Verifizieren Sie bei der Verwendung von Ressourcenrichtlinien, dass der Zugriff nur autorisierten Prinzipalen gewährt wird. Definieren Sie einen Prozess für die Genehmigung aller Ressourcen, die öffentlich verfügbar sein müssen.

AWS Identity and Access Management Access Analyzer nutzt nachweisbare Sicherheit, um alle Zugriffspfade zu einer Ressource von außerhalb ihres Kontos zu identifizieren. Es überprüft Ressourcenrichtlinien kontinuierlich und meldet Ergebnisse des öffentlichen und kontoübergreifenden Zugriffs, um Ihnen die Analyse potenziell umfassender Zugriffe zu erleichtern. Ziehen Sie die

Konfiguration von IAM Access Analyzer mit AWS Organizations in Betracht, um Transparenz für alle Ihre Konten zu gewährleisten. Mit IAM Access Analyzer können Sie zudem eine Vorschau der Ergebnisse anzeigen, bevor Sie Ressourcenberechtigungen bereitstellen. So können Sie sicherstellen, dass mit den Richtlinienänderungen nur der beabsichtigte öffentliche und kontoübergreifende Zugriff auf Ihre Ressourcen gewährt wird. Wenn Sie den Zugriff auf mehrere Konten planen, können Sie mithilfe von Vertrauensrichtlinien steuern, in welchen Fällen eine Rolle übernommen werden kann. Sie könnten beispielsweise den `PrincipalOrgId`-Bedingungsschlüssel verwenden, um Versuche, eine Rolle von außerhalb Ihres AWS Organizations zu übernehmen, abzulehnen.

AWS Config kann falsch konfigurierte Ressourcen melden und mithilfe von AWS Config-Richtlinienprüfungen Ressourcen erkennen, für die ein öffentlicher Zugriff konfiguriert ist. Services wie AWS Control Tower und AWS Security Hub CSPM vereinfachen die Bereitstellung von detektivischen Kontrollen und Integritätsschutz über AWS Organizations hinweg, um öffentlich zugängliche Ressourcen zu identifizieren und zu korrigieren. AWS Control Tower hat beispielsweise einen verwalteten Integritätsschutz, der erkennen kann, ob Amazon-EBS-Snapshots von AWS-Konten wiederhergestellt werden können.

Implementierungsschritte

- Die Verwendung von AWS Config für AWS Organizations erwägen: Mit AWS Config können Sie die Ergebnisse mehrerer Konten in einem AWS Organizations in einem delegierten Administratorkonto zusammenfassen. Dies bietet einen umfassenden Überblick und ermöglicht die kontoübergreifende Bereitstellung von AWS-Config-Regeln, um öffentlich zugängliche Ressourcen zu erkennen.
- AWS Identity and Access Management Access Analyzer konfigurieren: IAM Access Analyzer hilft Ihnen, die Ressourcen in Ihrer Organisation und in Ihren Konten zu identifizieren, die für eine externe Entität freigegeben wurden, z. B. Amazon S3-Buckets oder IAM-Rollen.
- Automatische Abhilfemaßnahmen in AWS Config verwenden, um auf Änderungen an der Konfiguration des öffentlichen Zugriffs von Amazon S3-Buckets zu reagieren: Sie können die Einstellungen zum Blockieren des öffentlichen Zugriffs für Amazon S3-Buckets automatisch aktivieren.
- Überwachung und Warnmeldungen implementieren, um festzustellen, ob Amazon S3-Buckets öffentlich geworden sind: Überwachung und Warnmeldungen müssen aktiviert sein, damit erkannt werden kann, wenn Amazon S3 Block Public Access deaktiviert wird und ob Amazon S3-Buckets öffentlich geworden sind. Wenn Sie AWS Organizations verwenden, können Sie außerdem eine Service-Kontrollrichtlinie erstellen, die Änderungen an den Amazon-S3-Richtlinien für den

öffentlichen Zugriff verhindert. AWS Trusted Advisor sucht nach Amazon-S3-Buckets mit offenen Zugriffsberechtigungen. Bucket-Berechtigungen, die allen Benutzern den Zugriff zum Hochladen/Löschen einräumen, bergen ein hohes Potenzial für Sicherheitsrisiken, da alle Personen Elemente in einem Bucket hinzufügen, ändern oder löschen können. Bei der Prüfung durch Trust Advisor werden explizite Bucket-Berechtigungen und zugeordnete Bucket-Richtlinien geprüft, die die Bucket-Berechtigungen möglicherweise überschreiben. Sie können auch mit AWS Config Ihre Amazon S3-Buckets für den öffentlichen Zugriff überwachen. Weitere Informationen finden Sie unter How AWS Config to Monitor for and Respond to Amazon S3 Buckets Allowing Public Access.

Bei der Überprüfung der Zugriffskontrollen für Amazon-S3-Buckets ist es wichtig, die Art der darin gespeicherten Daten zu berücksichtigen. Amazon Macie ist ein Service, mit dem Sie sensible Daten wie persönlich identifizierbare Informationen (PII), geschützte Gesundheitsinformationen (PHI, Protected Health Information) und Anmeldeinformationen wie private Schlüssel oder AWS-Zugriffsschlüssel entdecken und schützen können.

Ressourcen

Zugehörige Dokumente:

- Verwenden von AWS Identity and Access Management Access Analyzer
- Bibliothek von AWS Control Tower-Kontrollen
- AWS Foundational Security Best Practices-Standard
- AWS Config Von verwaltete Regeln
- AWS Trusted Advisor-Referenz prüfen
- Überwachen von AWS Trusted Advisor-Prüfungsergebnissen mit Amazon EventBridge
- Verwalten von AWS Config-Regeln für alle Konten in Ihrer Organisation
- AWS Config und AWS Organizations
- Ihr AMI für die Verwendung in Amazon EC2 öffentlich verfügbar machen

Zugehörige Videos:

- Bewährte Methoden für den Schutz Ihrer Mehrkonten-Umgebung
- Tiefer Einblick in IAM Access Analyzer

SEC03-BP08 Sicheres gemeinsames Nutzen von Ressourcen in Ihrer Organisation

Wenn die Anzahl der Workloads zunimmt, müssen Sie möglicherweise den Zugriff auf Ressourcen in diesen Workloads ausweiten oder diese Ressourcen mehrfach über mehrere Konten hinweg zugänglich machen. Möglicherweise haben Sie Konstrukte zur Untergliederung Ihrer Umgebung, etwa für Entwicklungs-, Test- und Produktionsumgebungen. Solche Trennungskonstrukte schränken Sie jedoch nicht in der Lage ein, sicher zu teilen. Durch die gemeinsame Nutzung sich überschneidender Ressourcen können Sie übermäßigen betrieblichen Aufwand reduzieren und eine konsistente Umgebung schaffen, ohne dass Sie raten müssen, was Sie vielleicht versäumt haben, wenn Sie eine Ressource mehrmals erstellen.

Gewünschtes Ergebnis: Vermeiden Sie den unbeabsichtigten Zugriff, indem Sie sichere Methoden verwenden, um Ressourcen innerhalb Ihrer Organisation zu teilen, und unterstützen Sie Ihre Initiative zur Verhinderung von Datenverlust. Reduzieren Sie Ihren organisatorischen Aufwand gegenüber der Verwaltung einzelner Komponenten, senken Sie die Zahl von Fehlern durch das manuelle mehrmalige Erstellen identischer Ressourcen, und steigern Sie die Skalierbarkeit Ihrer Workloads. Sie können von kürzeren Lösungszeiten in Szenarien mit mehreren Fehlerpunkten profitieren und Ihr Vertrauen in die Bestimmung erhöhen, wann eine Komponente nicht mehr benötigt wird. Verbindliche Anleitungen zur Analyse extern gemeinsam genutzter Ressourcen finden Sie unter SEC03-BP07 Analysieren des öffentlichen und kontoübergreifenden Zugriffs.

Typische Anti-Muster:

- Fehlen eines Prozesses für die kontinuierliche Überwachung und die automatische Benachrichtigung bei unerwarteten externen Freigaben
- Fehlen einer Basislinie dazu, was freigegeben werden sollte und was nicht
- Die standardmäßige Verwendung einer sehr offenen Richtlinie, anstatt Ressourcen explizit freizugeben, wenn sie benötigt werden
- Manuelle Erstellung grundlegender Ressourcen bei Bedarf, die sich überlappen

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Gestalten Sie Ihre Zugriffskontrollen und -muster so, dass die Nutzung freigegebener Ressourcen kontrolliert wird und nur mit vertrauenswürdigen Entitäten möglich ist. Überwachen Sie freigegebene

Ressourcen, prüfen Sie kontinuierlich den Zugriff darauf und erhalten Sie Benachrichtigungen bei unangemessenen oder unerwarteten Freigaben. Lesen Sie Analysieren des öffentlichen und kontoübergreifenden Zugriffs, um eine Governance einzurichten, mit der Sie den externen Zugriff auf diejenigen Ressourcen beschränken können, die ihn benötigen, und um einen Prozess zur kontinuierlichen Überwachung und automatischen Warnung einzurichten.

Die kontoübergreifende gemeinsame Nutzung innerhalb von AWS Organizations wird durch eine Reihe von AWS-Services unterstützt, etwa AWS Security Hub CSPM, Amazon GuardDuty und AWS Backup. Diese Services ermöglichen die Freigabe von Daten für ein zentrales Konto, ihre Zugänglichkeit von einem zentralen Konto aus sowie die Verwaltung von Ressourcen und Daten von einem zentralen Konto aus. Beispielsweise kann AWS Security Hub CSPM Ergebnisse von einzelnen Konten auf ein zentrales Konto übertragen, wo Sie alle Ergebnisse einsehen können. AWS Backup kann eine Sicherungskopie einer Ressource kontoübergreifend freigeben. Sie können mit AWS Resource Access Manager (AWS RAM) weitere gängige Ressourcen freigeben, z. B. VPC-Subnetze und Transit-Gateway-Anhänge, AWS Network Firewall oder Amazon-SageMaker-AI-Pipelines.

Um Ihr Konto so zu beschränken, dass nur Ressourcen innerhalb Ihrer Organisation gemeinsam genutzt werden, verwenden Sie Service-Kontrollrichtlinien (SCP), um den Zugriff auf externe Prinzipale zu verhindern. Kombinieren Sie bei der gemeinsamen Nutzung von Ressourcen identitätsbasierte Kontrollen und Netzwerkkontrollen, um einen Datenperimeter für Ihre Organisation zu schaffen, der zum Schutz vor unbeabsichtigtem Zugriff beiträgt. Ein Datenperimeter ist ein Satz von präventiven Maßnahmen zum Integritätsschutz, die dabei helfen, sicherzustellen, dass nur vertrauenswürdige Identitäten aus erwarteten Netzwerken auf vertrauenswürdige Ressourcen zugreifen. Diese Kontrollen begrenzen, welche Ressourcen gemeinsam genutzt werden, und verhindern die gemeinsame Nutzung oder Offenlegung von Ressourcen, die nicht zugelassen werden sollten. Als Teil Ihres Datenperimeters können Sie beispielsweise VPC-Endpunktrichtlinien und die `AWS:PrincipalOrgId`-Bedingung verwenden, um sicherzustellen, dass die Identitäten, die auf Ihre Amazon S3-Buckets zugreifen, zu Ihrer Organisation gehören. Es ist wichtig zu beachten, dass SCPs nicht für servicebezogene Rollen oder AWS-Service-Prinzipale gelten.

Wenn Sie Amazon S3 verwenden, deaktivieren Sie ACLs für Ihren Amazon S3-Bucket und definieren Sie die Zugriffskontrolle mithilfe von IAM-Richtlinien. Zum Beschränken des Zugriffs auf Amazon-S3-Inhalte von Amazon CloudFront aus migrieren Sie von der Ursprungszugriffsidentität (OAI) zur Ursprungszugriffssteuerung (OAC), die zusätzliche Features wie die serverseitige Verschlüsselung mit AWS Key Management Service unterstützen.

In manchen Fällen möchten Sie möglicherweise die Freigabe von Ressourcen außerhalb Ihrer Organisation zulassen oder einer Drittpartei den Zugriff auf Ihre Ressourcen gewähren. Verbindliche

Anleitungen zur Verwaltung von Berechtigungen für die externe gemeinsame Nutzung von Ressourcen finden Sie unter Verwaltung von Berechtigungen.

Implementierungsschritte

1. Verwendung von AWS Organizations: AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer von Ihnen erstellten und zentral verwalteten Organisation konsolidieren können. Sie können Ihre Konten in Organisationseinheiten (OUs) gruppieren und jeder OU unterschiedliche Richtlinien zuweisen, um Ihre Budget-, Sicherheits- und Compliance-Anforderungen zu erfüllen. Sie können auch steuern, wie AWS-Services für künstliche Intelligenz (KI) und Machine Learning (ML) Daten erfassen und speichern können, und die Mehrkonten-Verwaltung der mit Organizations integrierten AWS-Services verwenden.
2. Integration von AWS Organizations mit AWS-Services: Wenn Sie einen AWS-Service zur Ausführung von Aufgaben in Ihrem Namen in den Mitgliedskonten Ihrer Organisation verwenden, erstellt AWS Organizations in jedem Mitgliedskonto eine serviceverknüpfte IAM-Rolle (SLR, Service-linked Role) für den jeweiligen Service. Sie sollten den vertrauenswürdigen Zugriff mit der AWS-Managementkonsole, den AWS-APIs oder der AWS CLI verwalten. Verbindliche Anleitungen zur Aktivierung des vertrauenswürdigen Zugriffs finden Sie unter Verwendung von AWS Organizations mit anderen AWS-Services und unter AWS-Services, die Sie mit Organizations verwenden können.
3. Einrichtung eines Datenperimeters: Ein Datenperimeter schafft eine klare Grenze zwischen Vertrauen und Zuständigkeit. In AWS wird er in der Regel als Ihre AWS-Organisation dargestellt, die von AWS Organizations verwaltet wird, zusammen mit allen On-Premises-Netzwerken oder -Systemen, die auf Ihre AWS-Ressourcen zugreifen. Das Ziel des Datenperimeters besteht darin, zu überprüfen, ob der Zugriff erlaubt ist, wenn die Identität und die Ressource vertrauenswürdig sind und es sich um ein erwartetes Netzwerk handelt. Die Einrichtung eines Datenperimeters ist jedoch kein Einheitslösung für alle. Evaluieren und übernehmen Sie die im Whitepaper „Perimeter in AWS erstellen“ erläuterten Kontrollziele auf der Grundlage Ihrer spezifischen Sicherheitsrisikomodelle und -anforderungen. Sie sollten Ihre individuelle Risikosituation sorgfältig abwägen und die Perimeterkontrollen implementieren, die Ihren Sicherheitsanforderungen entsprechen.
4. Gemeinsame Nutzung von Ressourcen in AWS-Services und entsprechende Einschränkung: Viele AWS-Services ermöglichen es Ihnen, Ressourcen mit einem anderen Konto gemeinsam zu nutzen oder eine Ressource in einem anderen Konto als Ziel zu verwenden, z. B. Amazon Machine Images (AMIs) und AWS Resource Access Manager (AWS RAM). Beschränken Sie die `ModifyImageAttribute`-API auf die Angabe der vertrauenswürdigen Konten, mit denen das AMI geteilt werden soll. Geben Sie bei der Verwendung von AWS RAM die

`ram:RequestedAllowsExternalPrincipals`-Bedingung an, um die gemeinsame Nutzung nur auf Ihre Organisation zu beschränken, sodass der Zugriff durch nicht vertrauenswürdige Identitäten verhindert wird. Verbindliche Hinweise und Überlegungen finden Sie unter Gemeinsame Nutzung von Ressourcen und externe Ziele.

5. Verwendung von AWS RAM für die sichere gemeinsame Nutzung in einem Konto oder mit anderen AWS-Konten: AWS RAM unterstützt die sichere gemeinsame Nutzung der Ressourcen, die Sie erstellt haben, mit Rollen und Benutzern in Ihrem Konto sowie mit anderen AWS-Konten. In einer Mehrkonten-Umgebung ermöglicht AWS RAM die einmalige Erstellung einer Ressource und ihre Freigabe für andere Konten. Dies reduziert Ihren operationalen Aufwand und sorgt für Konsistenz, Transparenz und Prüfbarkeit durch Integrationen mit Amazon CloudWatch und AWS CloudTrail, die bei Verwendung eines kontoübergreifenden Zugriffs nicht möglich sind.

   Wenn Sie über Ressourcen verfügen, die Sie zuvor mithilfe einer ressourcenbasierten Richtlinie gemeinsam genutzt haben, können Sie die `PromoteResourceShareCreatedFromPolicy`-API oder eine gleichwertige Lösung verwenden, um die gemeinsame Nutzung auf eine vollständige AWS RAM-Ressourcenfreigabe hochzustufen.

   In manchen Fällen müssen Sie möglicherweise weitere Schritte unternehmen, um Ressourcen freizugeben. Um beispielsweise einen verschlüsselten Snapshot zu teilen, müssen Sie einen AWS KMS-Schlüssel freigeben.

Ressourcen

Zugehörige bewährte Methoden:

- SEC03-BP07 Analysieren des öffentlichen und kontoübergreifenden Zugriffs
- SEC03-BP09 Sicheres Teilen von Ressourcen mit Dritten
- SEC05-BP01 Erstellen von Netzwerkebenen

Zugehörige Dokumente:

- Bucket-Besitzer gewährt kontoübergreifende Berechtigung für Objekte, die er nicht besitzt
- Verwendung von Vertrauensrichtlinien mit IAM
- Erstellen von Datenperimetern in AWS
- Verwenden einer externen ID, um Dritten Zugriff auf Ihre AWS-Ressourcen zu gewähren
- AWS-Services, die Sie mit AWS Organizations verwenden können

- Einrichtung eines Datenperimeters in AWS: Nur vertrauenswürdigen Identitäten den Zugriff auf Unternehmensdaten gestatten

Zugehörige Videos:

- Granulärer Zugriff mit AWS Resource Access Manager
- Schutz Ihres Datenperimeters mit VPC-Endpunkten
- Einrichten eines Datenperimeters in AWS

Zugehörige Tools:

- Beispiele für Richtlinien für Datenperimeter

SEC03-BP09 Sicheres Teilen von Ressourcen mit Dritten

Die Sicherheit Ihrer Cloud-Umgebung endet nicht bei Ihrer Organisation. Möglicherweise stützt sich Ihre Organisation auf eine Drittpartei, um einen Teil Ihrer Daten zu verwalten. Das Berechtigungsmanagement für das von Dritten verwaltete System sollte dem Prinzip des Just-in-time-Zugriffs und dem der geringsten Berechtigung mit temporären Anmeldeinformationen folgen. Durch die enge Zusammenarbeit mit einer Drittpartei können Sie die möglichen Auswirkungen und das Risiko unbeabsichtigter Zugriffe gemeinsam senken.

Gewünschtes Ergebnis: Sie vermeiden die Verwendung von langfristigen AWS Identity and Access Management (IAM)-Anmeldeinformationen wie Zugriffsschlüsseln und geheimen Schlüsseln, da diese bei Missbrauch ein Sicherheitsrisiko darstellen. Stattdessen verwenden Sie IAM-Rollen und temporäre Anmeldeinformationen, um Ihre Sicherheitslage zu verbessern und den operativen Aufwand für die Verwaltung langfristiger Anmeldeinformationen zu minimieren. Wenn Sie Dritten Zugriff erteilen, verwenden Sie eine universell eindeutige Kennung (UUID, Universally Unique Identifier) als externe ID in der IAM-Vertrauensrichtlinie und lassen die IAM-Richtlinien an die Rolle unter Ihrer Kontrolle angefügt, um einen Zugriff mit geringsten Berechtigungen sicherzustellen. Eine verbindliche Anleitung für die Analyse extern freigegebener Ressourcen finden Sie unter SEC03-BP07 Analysieren des öffentlichen und kontoübergreifenden Zugriffs.

Typische Anti-Muster:

- Verwendung der Standard-IAM-Vertrauensrichtlinie ohne Bedingungen
- Verwenden langfristiger IAM-Anmeldeinformationen und Zugriffsschlüssel

- Wiederverwendung externer IDs

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Möglicherweise möchten Sie die Freigabe von Ressourcen außerhalb von AWS Organizations zulassen oder einer Drittpartei den Zugriff auf Ihr Konto gewähren. So könnte etwa eine Drittpartei eine Überwachungslösung bereitstellen, die auf Ressourcen in Ihrem Konto zugreifen muss. In solchen Fällen sollten Sie eine kontoübergreifende IAM-Rolle erstellen, die nur über die von der Drittpartei benötigten Berechtigungen verfügt. Definieren Sie außerdem eine Vertrauensrichtlinie mithilfe der externen ID-Bedingung. Wenn eine externe ID verwendet wird, können Sie oder die Drittpartei eine eindeutige ID für jede(n) Kunden, Drittpartei oder Tenancy generieren. Die eindeutige ID sollte nach ihrer Erstellung ausschließlich von Ihnen kontrolliert werden. Die Drittpartei muss einen Prozess implementieren, durch den die externe ID in sicherer, prüfbarer und reproduzierbarer Weise dem Kunden zugeordnet wird.

Sie können IAM Roles Anywhere auch verwenden, um IAM-Rollen für Anwendungen außerhalb von AWS zu verwalten, die AWS-APIs verwenden.

Wenn die Drittpartei keinen Zugriff mehr auf Ihre Umgebung benötigt, entfernen Sie die Rolle. Vermeiden Sie die Weitergabe langfristiger Anmeldeinformationen an Dritte. Informieren Sie sich über andere AWS-Services zur Unterstützung von Freigaben, z. B. AWS Well-Architected Tool, der das Freigeben eines Workloads für andereAWS-Konten unterstützt, und AWSResource Access Manager, der Ihnen hilft, eine AWS-Ressource in Ihrem Besitz auf sichere Weise für andere Konten freizugeben.

Implementierungsschritte

1. Verwenden Sie kontoübergreifende Rollen, um Zugriff auf externe Konten zu gewähren. Kontoübergreifende Rollen reduzieren die Menge vertraulicher Informationen, die von externen Konten und Dritten gespeichert werden, um ihre Kunden zu betreuen. Kontoübergreifende Rollen ermöglichen die sichere Gewährung des Zugriffs auf AWS-Ressourcen in Ihrem Konto für Drittparteien wie AWS-Partner oder andere Konten in Ihrer Organisation. Gleichzeitig wird die Möglichkeit gewahrt, diesen Zugriff zu verwalten und zu überprüfen. Möglicherweise stellt Ihnen die Drittpartei Dienstleistungen aus einer hybriden Infrastruktur heraus bereit oder ruft Daten zu einem anderen Standort ab. Mit IAM Roles Anywhere können Ihre Drittanbieter-Workloads sicher mit Ihren AWS-Workloads interagieren und die Notwendigkeit für langfristige Anmeldeinformationen weiter reduzieren.

Sie sollten keine langfristigen Anmeldeinformationen oder Benutzern zugeordnete Zugriffsschlüssel verwenden, um externen Zugriff auf Konten zu erteilen. Verwenden Sie stattdessen kontoübergreifende Rollen, um kontoübergreifenden Zugriff zu gewähren.

2. Führen Sie Due-Diligence-Prüfungen durch und sorgen Sie für einen sicheren Zugriff für SaaS-Drittanbieter. Führen Sie bei der Freigabe von Ressourcen für SaaS-Drittanbieter eine gründliche Due-Diligence-Prüfung durch, um sicherzustellen, dass diese beim Zugriff auf Ihre AWS-Ressourcen sicher und verantwortungsbewusst vorgehen. Evaluieren Sie ihr Modell der gemeinsamen Verantwortung, um zu verstehen, welche Sicherheitsmaßnahmen diese Drittanbieter bereitstellen und für welche Bereiche Sie verantwortlich sind. Stellen Sie sicher, dass die SaaS-Anbieter über einen sicheren und überprüfbaren Prozess für den Zugriff auf Ihre Ressourcen verfügen, einschließlich der Verwendung externer IDs und des Prinzips des geringsten Zugriffs. Die Verwendung externer IDs trägt dazu bei, das Confused-Deputy-Problem zu lösen.

   Implementieren Sie Sicherheitskontrollen, um einen sicheren Zugriff und die Einhaltung des Prinzips der geringsten Berechtigung sicherzustellen, wenn Sie SaaS-Drittanbietern Zugriff erteilen. Dies kann die Verwendung von externen IDs, Universally Unique Identifiers (UUIDs) und IAM-Vertrauensrichtlinien umfassen, die den Zugriff auf das unbedingt Notwendige einschränken. Arbeiten Sie eng mit dem SaaS-Anbieter zusammen, um sichere Zugriffsmechanismen einzurichten, den Zugriff auf Ihre AWS-Ressourcen regelmäßig zu überprüfen und Audits durchzuführen, um die Einhaltung Ihrer Sicherheitsanforderungen sicherzustellen.

3. Verwenden Sie vom Kunden bereitgestellte langfristige Anmeldeinformationen nicht mehr. Beenden Sie die Verwendung langfristiger Anmeldeinformationen, und verwenden Sie kontoübergreifende Rollen oder IAM Roles Anywhere. Wenn Sie langfristige Anmeldeinformationen verwendet müssen, formulieren Sie einen Plan für die Migration rollenbasierter Zugriffe. Einzelheiten zur Verwaltung von Schlüsseln finden Sie unter Identitätsverwaltung. Sie sollten außerdem zusammen mit Ihrem AWS-Konto-Team und dem Drittanbieter ein Runbook für die Risikominderung erstellen. Verbindliche Anleitungen für Reaktionen auf Sicherheitsvorfälle und die Minderung ihrer potenziellen Auswirkungen finden Sie unter Vorfallsreaktion.

4. Stellen Sie sicher, dass die Einrichtung über verbindliche Anleitungen verfügt oder automatisiert ist. Die externe ID wird nicht als Secret behandelt, ihr Wert darf aber nicht leicht zu erraten sein wie etwa eine Telefonnummer, ein Name oder eine Konto-ID. Machen Sie die externe ID zu einem schreibgeschützten Feld, damit sie nicht für illegitime Einrichtungen geändert werden kann.

Die externe ID kann von Ihnen oder von der Drittpartei generiert werden. Richten Sie einen Prozess ein, um festzulegen, wer für die Generierung der ID verantwortlich ist. Unabhängig von der Entität, die die externe ID erstellt, setzt die Drittpartei Eindeutigkeit und Formate in konsistenter Weise für alle Kunden durch.

Die Richtlinie, die für den kontoübergreifenden Zugriff in Ihren Konten erstellt wurde, muss dem Prinzip der geringsten Berechtigung entsprechen. Die Drittpartei muss ein Rollenrichtliniendokument oder einen automatisierten Einrichtungsmechanismus bereitstellen, der eine AWS CloudFormation-Vorlage oder ein Äquivalent verwendet. Dies reduziert die Gefahr von Fehlern durch die manuelle Erstellung von Richtlinien und bietet einen Überwachungspfad. Weitere Informationen zur Verwendung einer AWS CloudFormation-Vorlage zum Erstellen kontoübergreifender Rollen finden Sie unter Kontoübergreifende Rollen.

Die Drittpartei muss einen automatisierten und prüfbaren Einrichtungsmechanismus bereitstellen. Sie sollten jedoch die Einrichtung der Rolle automatisieren, indem Sie das Rollenrichtliniendokument verwenden, das den erforderlichen Zugriff angibt. Sie sollten mithilfe der AWS CloudFormation-Vorlage oder einer gleichwertigen Methode Änderungen überwachen. Die Erkennung von Abweichungen sollte Teil dieser Überwachung sein.

5. Berücksichtigen Sie Änderungen. Ihre Kontostruktur und Ihr Bedarf an einer Drittpartei bzw. deren Serviceangebots können sich über Nacht ändern. Sie sollten Änderungen und Ausfälle antizipieren und mit den richtigen Personen, Prozessen und Technologielösungen entsprechend planen. Prüfen Sie regelmäßig das von Ihnen bereitgestellte Zugriffsniveau und implementieren Sie Erkennungsverfahren, die Sie auf unerwartete Änderungen aufmerksam machen. Überwachen und prüfen Sie die Verwendung der externen Rolle und den Datenspeicher der externen IDs. Sie sollten darauf vorbereitet sein, den Zugriff der Drittpartei temporär oder dauerhaft zu widerrufen, wenn sich unerwartete Änderungen oder Zugriffsmuster ergeben. Messen Sie auch die Auswirkungen Ihrer Widerrufaktion, einschließlich der dafür benötigten Zeit, der involvierten Personen, der Kosten und der Auswirkungen auf andere Ressourcen.

   Verbindliche Anleitungen zu Erkennungsmethoden finden Sie unter Bewährte Methoden zur Erkennung.

Ressourcen

Zugehörige bewährte Methoden:

- SEC02-BP02 Verwenden von temporären Anmeldeinformationen

- SEC03-BP05 Definieren eines Integritätsschutzes für Berechtigungen in Ihrer Organisation
- SEC03-BP06 Zugriffsverwaltung basierend auf dem Lebenszyklus
- SEC03-BP07 Analysieren des öffentlichen und kontoübergreifenden Zugriffs
- SEC04 Erkennung

Zugehörige Dokumente:

- Bucket-Besitzer gewährt kontoübergreifende Berechtigung für Objekte, die er nicht besitzt
- Verwenden von Vertrauensrichtlinien mit IAM-Rollen
- Delegieren des Zugriffs für AWS-Konten mithilfe von IAM-Rollen
- Wie greife ich mithilfe von IAM auf Ressourcen in einem anderen AWS-Konto zu?
- Bewährte Methoden für die Sicherheit in IAM
- Logik für die kontoübergreifende Richtlinienauswertung
- Verwenden einer externen ID beim Erteilen von Zugriff auf Ihre AWS-Ressourcen für Dritte
- Sammeln von Informationen in AWS CloudFormation-Ressourcen, die in externen Konten mit benutzerdefinierten Ressourcen erstellt wurden
- Sichere Verwendung einer externen ID für den Zugriff auf AWS-Konten im Besitz anderer Benutzer
- Erweitern von IAM-Rollen auf Workloads außerhalb von IAM mithilfe von IAM Roles Anywhere

Zugehörige Videos:

- Wie erteile ich Benutzern oder Rollen in einem separaten AWS-Konto Zugriff auf mein AWS-Konto?
- AWS re:Invent 2018: Experte für IAM-Richtlinien in unter 60 Minuten
- AWS Knowledge Center Live: Bewährte IAM-Methoden und Entwurfsentscheidungen

Zugehörige Beispiele:

- Kontenübergreifenden Zugriff auf Amazon DynamoDB konfigurieren
- AWS STS Network Query Tool

Erkennung

Die Erkennung besteht aus zwei Teilen: der Erkennung von unerwarteten oder unerwünschten Konfigurationsänderungen und der Erkennung von unerwartetem Verhalten. Der erste Teil kann an mehreren Stellen im Lebenszyklus einer Anwendung erfolgen. Durch die Verwendung von Infrastruktur als Code (z. B. eine CloudFormation-Vorlage) können Sie vor der Bereitstellung einer Workload durch die Implementierung von Prüfungen in den CI/CD-Pipelines oder der Versionskontrolle auf unerwünschte Konfigurationen prüfen. Wenn Sie dann eine Workload in Nicht-Produktions- und Produktionsumgebungen bereitstellen, können Sie die Konfiguration mit nativen AWS-, Open-Source- oder AWS-Partner-Tools überprüfen. Diese Prüfungen können sich auf Konfigurationen beziehen, die nicht den Sicherheitsgrundsätzen oder bewährten Methoden entsprechen oder auf Änderungen, die zwischen einer getesteten und einer bereitgestellten Konfiguration vorgenommen wurden. Bei einer laufenden Anwendung können Sie überprüfen, ob die Konfiguration auf unerwartete Weise geändert wurde, auch außerhalb einer bekannten Bereitstellung oder eines automatischen Skalierungsereignisses.

Für den zweiten Teil der Erkennung, das unerwartete Verhalten, können Sie Tools verwenden oder eine Warnung ausgeben, wenn eine bestimmte Art von API-Aufrufen zunimmt. Mit Amazon GuardDuty können Sie gewarnt werden, wenn unerwartete und potenziell unbefugte oder böswillige Aktivitäten in Ihren AWS-Konten auftreten. Sie sollten auch explizit auf mutierende API-Aufrufe achten, von denen Sie nicht erwarten würden, dass sie in Ihrer Workload verwendet werden, sowie auf API-Aufrufe, die die Sicherheitslage verändern.

Die Erkennung ermöglicht es Ihnen, eine potenzielle Sicherheitsfehlkonfiguration, eine Bedrohung oder ein unerwartetes Verhalten zu identifizieren. Die Kontrollmechanismen sind ein wesentlicher Bestandteil des Sicherheitslebenszyklus. Sie können zur Unterstützung von Qualitätssicherungsverfahren, zur Einhaltung gesetzlicher Vorgaben und Pflichten sowie zur Erkennung und Abwehr von Bedrohungen genutzt werden. Es gibt unterschiedliche Erkennungsmechanismen. Protokolle von Ihrer Workload können beispielsweise auf Exploits analysiert werden, die verwendet werden. Sie sollten regelmäßig die Erkennungsmechanismen im Zusammenhang mit Ihrer Workload überprüfen, um sicherzustellen, dass Sie die internen und externen Richtlinien und Anforderungen erfüllen. Automatisierte Warnungen und Benachrichtigungen sollten auf definierten Bedingungen basieren, damit Ihre Teams oder Tools Untersuchungen vornehmen können. Diese Mechanismen sind wichtige reaktive Faktoren, die es Ihrer Organisation ermöglichen, den Umfang anomaler Aktivitäten zu ermitteln und zu verstehen.

In AWS gibt es eine Reihe von Ansätzen, die Sie in Zusammenhang mit aufdeckenden Mechanismen verwenden können. Die folgenden Abschnitte beschreiben die Verwendung dieser Ansätze:

Bewährte Methoden

- SEC04-BP01 Konfigurieren der Service- und Anwendungsprotokollierung
- SEC04-BP02 Erfassen von Protokollen, Erkenntnissen und Metriken an standardisierten Orten
- SEC04-BP03 Korrelieren und Anreichern von Sicherheitswarnmeldungen
- SEC04-BP04 Initiieren von Abhilfemaßnahmen für nicht konforme Ressourcen

SEC04-BP01 Konfigurieren der Service- und Anwendungsprotokollierung

Bewahren Sie Protokolle zu Sicherheitsereignissen von Services und Anwendungen auf. Dies ist ein grundlegendes Sicherheitsprinzip für Prüfungs-, Untersuchungs- und betriebliche Anwendungsfälle und eine übliche Sicherheitsanforderung gemäß Governance-, Risiko- und Compliance (GRC)-Standards, -Richtlinien und -Prozeduren.

Gewünschtes Ergebnis: Eine Organisation sollte in der Lage sein, Sicherheitsereignisprotokolle in zuverlässiger und konsistenter Weise sowie zeitnah aus AWS-Services und -Anwendungen abzurufen, wenn diese für einen internen Prozess oder eine Verpflichtung wie etwa die Reaktion auf einen Sicherheitsvorfall benötigt werden. Erwägen Sie die Zentralisierung von Protokollen für bessere betriebliche Ergebnisse.

Typische Anti-Muster:

- Protokolle werden dauerhaft gespeichert oder zu früh gelöscht.
- Jeder kann auf die Protokolle zugreifen.
- Für die Verwaltung und Verwendung von Protokollen werden ausschließlich manuelle Prozesse genutzt.
- Alle Arten von Protokollen werden gespeichert, nur für den Fall, dass sie benötigt werden.
- Die Protokollintegrität wird nur bei Bedarf geprüft.

Vorteile der Nutzung dieser bewährten Methode: Implementieren Sie einen Mechanismus für die Ursachenanalyse (RCA) für Sicherheitsvorfälle sowie eine Evidenzquelle für Ihre Governance-, Risiko- und Compliance-Anforderungen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Bei einer Sicherheitsuntersuchung oder in anderen bedarfsabhängigen Anwendungsfällen müssen Sie relevante Protokolle konsultieren können, um alle Aspekte und den Zeitrahmen des Vorfalls zu verstehen. Protokolle werden auch für die Generierung von Alarmen benötigt, die darauf hinweisen, dass bestimmte Ereignisse vorgekommen sind. Es ist sehr wichtig, Abfrage-, Abruf- sowie Benachrichtigungsmechanismen auszuwählen, zu aktivieren, zu speichern und einzurichten.

Implementierungsschritte

- Wählen und aktivieren Sie Protokollquellen. Vor einer Sicherheitsuntersuchung müssen Sie relevante Protokolle erfassen, um die Aktivitäten in einem AWS-Konto retroaktiv rekonstruieren zu können. Wählen und aktivieren Sie für Ihre Workloads relevante Protokollquellen.

  Die Kriterien für die Auswahl der Protokollquelle sollten auf den Anwendungsfällen Ihres Unternehmens basieren. Richten Sie einen Trail für jedes AWS-Konto-Konto mit AWS CloudTrail oder einen AWS Organizations-Trail ein, und konfigurieren Sie dafür einen Amazon S3-Bucket.

  AWS CloudTrail ist ein Protokollservice, der API-Aufrufe an ein AWS-Konto verfolgt und AWS-Serviceaktivitäten erfasst. Dieser ist standardmäßig mit einer 90-tägigen Aufbewahrung von Managementereignissen aktiviert, die über den CloudTrail-Ereignisverlauf mit der AWS-Managementkonsole, der AWS CLI oder einem AWS-SDK abgerufen werden können. Für längere Aufbewahrungszeiten und Abrufbarkeit von Datenereignissen erstellen Sie einen CloudTrail-Trail und verbinden diesen mit einem Amazon S3-Bucket sowie optional mit einer Amazon CloudWatch-Protokollgruppe. Sie können auch einen CloudTrail-Lake erstellen, der CloudTrail-Protokolle bis zu sieben Jahre lang aufbewahrt und eine SQL-basierte Abfragemöglichkeit bietet.

  AWS empfiehlt, dass Kunden, die eine VPC nutzen, Netzwerkdatenverkehr- und DNS-Protokolle mit VPC Flow Logs und Amazon Route 53 Resolver Query Logs einrichten und diese per Stream zu einem Amazon S3-Bucket oder einer CloudWatch-Protokollgruppe leiten. Sie können ein VPC-Flow-Protokoll für eine VPC, ein Subnetz oder eine Netzwerkschnittstelle erstellen. Für VPC-Flow-Protokolle können Sie wählen, wie und wo Flow-Protokolle verwendet werden sollen, um Kosten zu sparen.

  AWS CloudTrail CloudTrail-Protokolle, VPC-Flow-Protokolle und Route 53 Resolver Query Logs sind die grundlegenden Protokollquellen zur Unterstützung von Sicherheitsuntersuchungen in AWS. Sie können auch Amazon Security Lake verwenden, um diese Protokolldaten zu erfassen,

zu normalisieren und im Apache Parquet-Format und mit dem Open Cybersecurity Schema Framework (OCSF) zu speichern, das Abfragen ermöglicht. Security Lake unterstützt auch andere AWS-Protokolle sowie Protokolle aus Drittquellen.

AWS-Services können Protokolle generieren, die von den grundlegenden Protokollquellen nicht erfasst werden, wie etwa Protokolle von Elastic Load Balancing, AWS WAF-Protokolle, Recorder-Protokolle von AWS Config, Amazon GuardDuty-Erkenntnisse, Amazon Elastic Kubernetes Service (Amazon EKS)-Prüfprotokolle sowie Instance-Betriebssystem- und Anwendungsprotokolle von Amazon EC2. Eine vollständige Liste von Protokoll- und Überwachungslösungen finden Sie unter Anhang A: Definitionen der Cloud-Funktionen – Protokollierung und Ereignisse in der Anleitung zur Reaktion auf AWS-Sicherheitsvorfälle.

- Untersuchen Sie die Protokollierungsmöglichkeiten für jede(n) AWS-Service und -Anwendung: Jede(r) AWS-Service und -Anwendung bietet Optionen für die Speicherung von Protokollen, jeweils mit eigenen Aufbewahrungs- und Lebenszyklus-Funktionen. Die beiden verbreitetsten Protokollspeicherservices sind Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch. Für lange Aufbewahrungszeiten wird die Verwendung von Amazon S3 empfohlen, wegen seiner Kosteneffektivität und der flexiblen Lebenszyklus-Funktionen. Wenn die primäre Protokollierungsoption Amazon CloudWatch Logs sind, sollten Sie erwägen, weniger häufig benötigte Protokolle in Amazon S3 zu archivieren.
- Wählen Sie den Protokollspeicher aus: Die Wahl des Protokollspeichers hängt generell vom verwendeten Abfragetool, den Aufbewahrungsfunktionen, der Vertrautheit damit und den Kosten ab. Die wichtigsten Optionen für die Protokollspeicherung sind ein Amazon S3-Bucket oder eine CloudWatch-Protokollgruppe.

  Ein Amazon S3-Bucket bietet kosteneffektiven und dauerhaften Speicher mit optionaler Lebenszyklusrichtlinie. In Amazon S3-Buckets gespeicherte Protokolle können mit Services wie Amazon Athena abgefragt werden.

  Eine CloudWatch-Protokollgruppe bietet dauerhaften Speicher und eine integrierte Abfragemöglichkeit über CloudWatch Logs Insights.
- Legen Sie die benötigte Aufbewahrungszeit für Protokolle fest: Wenn Sie einen Amazon S3-Bucket oder eine CloudWatch-Protokollgruppe für die Speicherung von Protokollen verwenden, müssen Sie adäquate Lebenszyklen für jede Protokollquelle einrichten, um Speicher- und Abrufkosten zu optimieren. Normalerweise haben Kunden Protokolle zwischen drei Monaten bis einem Jahr für Abfragen verfügbar, bei einer Gesamtaufbewahrungszeit von bis zu sieben Jahren. Die Wahl von Verfügbarkeit und Aufbewahrungszeit sollte sich nach Ihren Sicherheitsanforderungen und einer Kombination aus gesetzlichen, regulatorischen und unternehmensinternen Vorschriften richten.

- Aktivieren Sie die Protokollierung für jede(n) AWS-Service und -Anwendung mit korrekten Aufbewahrungs- und Lebenszyklusrichtlinien: Suchen Sie für alle AWS-Services oder -Anwendungen in Ihrer Organisation nach den entsprechenden Anleitungen zur Protokollkonfiguration:
  - Konfigurieren eines AWS CloudTrail-Trails
  - Konfigurieren von VPC-Flow-Protokollen
  - Konfigurieren des Amazon GuardDuty-Erkenntnisexports
  - Konfigurieren der AWS Config-Aufzeichnung
  - Konfigurieren des AWS WAF-Datenverkehrs von WAF
  - Konfigurieren der Netzwerkdatenverkehrsprotokolle von AWS Network Firewall
  - Konfigurieren der Zugriffsprotokolle von Elastic Load Balancing
  - Konfigurieren von Resolver-Abfrageprotokollen von Amazon Route 53
  - Konfigurieren von Amazon RDS-Protokollen
  - Konfigurieren von Amazon EKS-Steuerebenenprotokollen
  - Konfigurieren eines Amazon CloudWatch-Agenten für Amazon EC2-Instances und On-Premises-Server
- Wählen und implementieren Sie Abfragemechanismen für Ihre Protokolle: Für Protokollabfragen können Sie CloudWatch Logs Insights für in CloudWatch-Protokollgruppen gespeicherte Daten sowie Amazon Athena und Amazon OpenSearch Service für in Amazon S3 gespeicherte Daten verwenden. Sie können auch Abfragetools von Drittanbietern wie etwa den SIEM (Security Information and Event Management)-Service verwenden.

  Bei der Auswahl eines Tools zur Protokollabfrage sollten Sie die Personen, die Prozesse und die Technologieaspekte Ihrer Sicherheitsoperationen berücksichtigen. Wählen Sie ein Tool, das betriebliche, geschäftliche und sicherheitsrelevante Aspekte berücksichtigt und langfristig sowohl zugänglich als auch wartbar ist. Denken Sie daran, dass Tools zur Protokollabfrage optimal funktionieren, wenn die Anzahl der zu durchsuchenden Protokolle im Rahmen der Limits des jeweiligen Tools liegt. Es ist nicht ungewöhnlich, aus Kostengründen oder aufgrund technischer Einschränkungen mehrere Abfragetools zu verwenden.

  Beispielsweise können Sie ein SIEM-Tool eines Drittanbieters für Abfragen der letzten 90 Datentage, aber aufgrund der Protokollerfassungskosten für SIEM Athena für Abfragen verwenden, die darüber hinaus gehen. Prüfen Sie unabhängig von der Implementierung, ob Ihr Konzept die Anzahl der für die Maximierung der operationalen Effizienz erforderlichen Tools minimiert, besonders für Untersuchungen von Sicherheitsvorfällen.

- Verwenden Sie Protokolle für Benachrichtigungen: AWS bietet verschiedene Benachrichtigungsmöglichkeiten über mehrere Sicherheitsservices:
  - AWS Config überwacht und zeichnet Ihre AWS-Ressourcenkonfigurationen auf. Darüber hinaus ermöglicht es Ihnen, die Auswertung und Korrektur der gewünschten Konfigurationen zu automatisieren.
  - Amazon GuardDuty ist ein Bedrohungserkennungsservice, der kontinuierlich nach schädlichen Aktivitäten und nicht autorisierten Verhaltensweisen sucht, um Ihre AWS-Konten und Ihre Workloads zu schützen. GuardDuty erfasst, aggregiert und analysiert Informationen aus Quellen wie AWS CloudTrail-Verwaltungs- und Datenereignissen, DNS-Protokollen, VPC-Flow-Protokollen und Amazon EKS-Prüfprotokollen. GuardDuty ruft unabhängige Datenströme direkt von CloudTrail, VPC-Flow-Protokollen, DNS-Abfrageprotokollen und Amazon EKS ab. Sie müssen keine Amazon S3-Bucket-Richtlinien verwalten oder die Art und Weise der Erfassung und Speicherung von Protokollen verändern. Es wird jedoch empfohlen, diese Protokolle für Ihre eigenen Untersuchungs- und Compliance-Zwecke aufzubewahren.
  - AWS Security Hub CSPM bietet einen zentralen Ort, an dem Ihre Sicherheitswarnungen oder Ergebnisse von mehreren AWS-Services und optionalen Produkten von Drittanbietern aggregiert, organisiert und priorisiert werden. So erhalten Sie einen umfassenden Überblick über Sicherheitswarnungen und den Compliance-Status.

  Sie können auch benutzerdefinierte Alarm-Engines für Sicherheitsalarme verwenden, die von diesen Services nicht abgedeckt werden, bzw. für bestimmte Alarme, die für Ihre Umgebung relevante sind. Informationen zur Erstellung dieser Alarm- und Erkennungsmechanismen finden Sie unter „Detection“ im AWS Security Incident Response Guide.

Ressourcen

Zugehörige bewährte Methoden:

- SEC04-BP02 Erfassen von Protokollen, Erkenntnissen und Metriken an standardisierten Orten
- SEC07-BP04 Definieren eines skalierbaren Datenlebenszyklusmanagements
- SEC10-BP06 Vorabbereitstellen von Tools

Zugehörige Dokumente:

- AWS Security Incident Response Guide
- Erste Schritte mit Amazon Security Lake

- Getting started: Amazon CloudWatch Logs

Zugehörige Videos:

- AWS re:Invent 2.022 - Introducing Amazon Security Lake

Zugehörige Beispiele:

- Assisted Log Enabler for AWS
- AWS Security Hub CSPM Findings Historical Export

SEC04-BP02 Erfassen von Protokollen, Erkenntnissen und Metriken an standardisierten Orten

Sicherheitsteams stützen sich auf Protokolle und Erkenntnisse, um Ereignisse zu analysieren, die auf unbefugte Aktivitäten oder unbeabsichtigte Änderungen hindeuten könnten. Um diese Analyse zu rationalisieren, sollten Sie Sicherheitsprotokolle und Ergebnisse an standardisierten Orten erfassen. Dies macht Datenpunkte von Interesse für die Korrelation verfügbar und kann die Integration von Tools vereinfachen.

Gewünschtes Ergebnis: Sie verfügen über einen standardisierten Ansatz zum Sammeln, Analysieren und Visualisieren von Protokolldaten, Erkenntnissen und Metriken. Sicherheitsteams können Sicherheitsdaten über verschiedene Systeme hinweg effizient korrelieren, analysieren und visualisieren, um potenzielle Sicherheitsereignisse zu erkennen und Anomalien zu identifizieren. Systeme für Sicherheitsinformation und Ereignisverwaltung (Security Information and Event Management, SIEM) oder andere Mechanismen sind integriert, um Protokolldaten abzufragen und zu analysieren, damit Sie zeitnah auf Sicherheitsereignisse reagieren, diese verfolgen und eskalieren können.

Typische Anti-Muster:

- Teams besitzen und verwalten eigenständig Protokolle und Metriksammlungen, die nicht mit der Protokollierungsstrategie der Organisation übereinstimmen.
- Teams verfügen nicht über angemessene Zugriffskontrollen, um die Sichtbarkeit und Veränderung der erfassten Daten einzuschränken.

- Teams regeln ihre Sicherheitsprotokolle, Erkenntnisse und Metriken nicht als Teil ihrer Richtlinie zur Datenklassifizierung.
- Teams vernachlässigen bei der Konfiguration von Datensammlungen die Anforderungen an die Datenhoheit und die Lokalisierung.

Vorteile der Nutzung dieser bewährten Methode: Eine standardisierte Protokollierungslösung zur Erfassung und Abfrage von Protokolldaten und -ereignissen verbessert die aus den darin enthaltenen Informationen gewonnenen Erkenntnisse. Die Konfiguration eines automatisierten Lebenszyklus für die gesammelten Protokolldaten kann die durch die Speicherung von Protokollen entstehenden Kosten reduzieren. Sie können eine fein abgestufte Zugriffskontrolle für die gesammelten Protokollinformationen einrichten, je nachdem, wie sensibel die Daten sind und welche Zugriffsmuster Ihre Teams benötigen. Sie können Tools integrieren, um die Daten zu korrelieren, zu visualisieren und Erkenntnisse daraus abzuleiten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Die zunehmende AWS-Nutzung innerhalb einer Organisation führt zu einer wachsenden Anzahl von verteilten Workloads und Umgebungen. Jeder dieser Workloads und jede dieser Umgebungen generiert Daten über die darin stattfindenden Aktivitäten. Die Erfassung und lokale Speicherung dieser Daten stellt eine Herausforderung für den Sicherheitsbetrieb dar. Sicherheitsteams verwenden Tools wie Sicherheitsinformations- und Ereignisverwaltungssysteme (SIEM), um Daten aus verteilten Quellen zu sammeln und Korrelations-, Analyse- und Reaktionsabläufe durchzuführen. Dies erfordert die Verwaltung einer komplexen Reihe von Berechtigungen für den Zugriff auf die verschiedenen Datenquellen und einen zusätzlichen Aufwand beim Betrieb der Extract, Transform, Load (ETL)-Prozesse.

Um diese Herausforderungen zu bewältigen, sollten Sie alle relevanten Quellen von Sicherheitsprotokolldaten in einem Protokollarchiv-Konto zusammenfassen, wie in Organisieren Ihrer AWS-Umgebung mittels mehrerer Konten beschrieben. Dazu gehören alle sicherheitsrelevanten Daten aus Ihrem Workload und Protokolle, die AWS-Services erzeugen, wie AWS CloudTrail, AWS WAF, Elastic Load Balancing und Amazon Route 53. Es hat mehrere Vorteile, diese Daten an standardisierten Orten in einem separaten AWS-Konto mit entsprechenden kontoübergreifenden Berechtigungen zu erfassen. Diese Vorgehensweise hilft, die Manipulation von Protokollen in gefährdeten Workloads und Umgebungen zu verhindern, bietet einen einzigen Integrationspunkt für zusätzliche Tools und bietet ein einfacheres Modell für die Konfiguration der Datenaufbewahrung

und des Lebenszyklus. Bewerten Sie die Auswirkungen der Datenhoheit, der Compliance-Bereiche und anderer Vorschriften, um festzustellen, ob mehrere Speicherorte für Sicherheitsdaten und Aufbewahrungsfristen erforderlich sind.

Um die Erfassung und Standardisierung von Protokollen und Erkenntnissen zu erleichtern, bewerten Sie Amazon Security Lake in Ihrem Protokollarchiv-Konto. Sie können Security Lake so konfigurieren, dass Daten aus gängigen Quellen wie CloudTrail, Route 53, Amazon EKS und VPC Flow Logs automatisch aufgenommen werden. Außerdem können Sie AWS Security Hub CSPM auch als Datenquelle in Security Lake konfigurieren, sodass Sie Erkenntnisse aus anderen AWS-Services wie Amazon GuardDuty und Amazon Inspector mit Ihren Protokolldaten korrelieren können. Ferner haben Sie die Möglichkeit, Datenquellen von Drittanbietern zu integrieren oder eigene Datenquellen zu konfigurieren. Alle Integrationen standardisieren Ihre Daten in das Open Cybersecurity Schema Framework (OCSF)-Format und werden in Amazon S3-Buckets als Parquet-Dateien gespeichert, sodass keine ETL-Verarbeitung erforderlich ist.

Die Speicherung von Sicherheitsdaten an standardisierten Orten bietet erweiterte Analysemöglichkeiten. AWS empfiehlt Ihnen die Bereitstellung von Tools für Sicherheitsanalysen, die in einer AWS-Umgebung arbeiten, in einem Security-Tooling-Konto, das von Ihrem Protokollarchiv-Konto getrennt ist. Dieser Ansatz ermöglicht es Ihnen, Kontrollen in der Tiefe zu implementieren, um die Integrität und Verfügbarkeit der Protokolle und des Protokollverwaltungsprozesses zu schützen, und zwar unabhängig von den Tools, die auf sie zugreifen. Erwägen Sie die Nutzung von Services wie Amazon Athena, um On-Demand-Abfragen durchzuführen, die mehrere Datenquellen miteinander in Beziehung setzen. Sie können auch Visualisierungstools wie QuickSight integrieren. KI-gestützte Lösungen werden zunehmend verfügbar und können Funktionen wie die Übersetzung von Erkenntnissen in für Menschen lesbare Zusammenfassungen und Interaktion in natürlicher Sprache übernehmen. Diese Lösungen lassen sich oft leichter integrieren, wenn ein standardisierter Datenspeicher für Abfragen zur Verfügung steht.

Implementierungsschritte

1. Erstellen Sie die Konten „Protokollarchiv“ und „Security Tooling
   a. Erstellen Sie mit AWS Organizations Organizations die Konten „Protokollarchiv“ und „Security Tooling“ unter einer Sicherheitsorganisationseinheit. Wenn Sie AWS Control Tower zur Verwaltung Ihrer Organisation verwenden, werden die Konten für Protokollarchiv und Security Tooling automatisch für Sie erstellt. Konfigurieren Sie bei Bedarf Rollen und Berechtigungen für den Zugriff auf diese Konten und deren Verwaltung.
2. Konfigurieren Sie Ihre standardisierten Speicherorte für Sicherheitsdaten

   a. Legen Sie Ihre Strategie für die Erstellung standardisierter Sicherheitsdatenorte fest. Sie können dies durch Optionen wie allgemeine Data-Lake-Architekturansätze, Datenprodukte von Drittanbietern oder Amazon Security Lake erreichen. AWS empfiehlt, dass Sie Sicherheitsdaten von AWS-Regionen-Regionen erfassen, die für Ihre Konten aktiviert sind, auch wenn sie nicht aktiv genutzt werden.

3. Konfigurieren Sie die Veröffentlichung von Datenquellen an Ihren standardisierten Standorten
   a. Identifizieren Sie die Quellen für Ihre Sicherheitsdaten und konfigurieren Sie sie so, dass sie an Ihren standardisierten Standorten veröffentlicht werden. Evaluieren Sie Optionen für den automatischen Export von Daten in das gewünschte Format im Gegensatz zu solchen, bei denen ETL-Prozesse entwickelt werden müssen. Mit Amazon Security Lake können Sie Daten aus unterstützten AWS-Quellen und integrierten Drittsystemen sammeln.
4. Konfigurieren Sie Tools für den Zugriff auf Ihre standardisierten Speicherorte
   a. Konfigurieren Sie Tools wie Amazon Athena, QuickSight oder Lösungen von Drittanbietern, um den erforderlichen Zugriff auf Ihre standardisierten Standorte zu erhalten. Konfigurieren Sie diese Tools so, dass sie über das Security Tooling-Konto mit kontoübergreifendem Zugriff auf das Protokollarchiv-Konto arbeiten, sofern zutreffend. Erstellen Sie Subscriber in Amazon Security Lake, um diesen Tools Zugriff auf Ihre Daten zu erteilen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC01-BP01 Trennen von Workloads mithilfe von Konten
- SEC07-BP04 Definieren eines skalierbaren Datenlebenszyklusmanagements
- SEC08-BP04 Durchsetzen der Zugriffskontrolle
- OPS08-BP02 Analysieren von Workload-Protokollen

Zugehörige Dokumente:

- AWS Whitepapers: Organizing Your AWS Environment Using Multiple Accounts
- AWS Prescriptive Guidance: AWS Security Reference Architecture (AWS SRA)
- AWS Prescriptive Guidance: Logging and monitoring guide for application owners

Zugehörige Beispiele:

- Aggregierung, Suche und Visualisierung von Protokolldaten aus verteilten Quellen mit Amazon Athena und QuickSight
- Visualisieren von Ergebnissen von Amazon Security Lake mit QuickSight
- Generate AI powered insights for Amazon Security Lake using Amazon SageMaker AI Studio and Amazon Bedrock
- Identify cybersecurity anomalies in your Amazon Security Lake data using Amazon SageMaker AI
- Ingest, transform, and deliver events published by Amazon Security Lake to Amazon OpenSearch Service
- Simplify AWS CloudTrail log analysis with natural language query generation in CloudTrail Lake

Zugehörige Tools:

- Amazon Security Lake
- Amazon Security Lake-Partnerintegrationen
- Open Cybersecurity Schema Framework (OCSF)
- Amazon Athena
- Schnell
- Amazon Bedrock

SEC04-BP03 Korrelieren und Anreichern von Sicherheitswarnmeldungen

Unerwartete Aktivitäten können mehrere Sicherheitswarnmeldungen aus verschiedenen Quellen auslösen, die eine weitere Korrelation und Anreicherung erfordern, um den gesamten Kontext zu verstehen. Implementieren Sie die automatische Korrelation und Anreicherung von Sicherheitswarnmeldungen, um eine genauere Identifizierung von Vorfällen und eine bessere Reaktion darauf zu ermöglichen.

Gewünschtes Ergebnis: Da die Aktivitäten in Ihren Workloads und Umgebungen unterschiedliche Warnmeldungen erzeugen, korrelieren automatische Mechanismen die Daten und reichern sie mit zusätzlichen Informationen an. Diese Vorverarbeitung ermöglicht ein detaillierteres Verständnis des Ereignisses, was Ihren Ermittlern hilft, die Kritikalität des Ereignisses zu bestimmen und festzustellen, ob es sich um einen Vorfall handelt, der eine formelle Reaktion erfordert. Dieses Verfahren entlastet Ihre Überwachungs- und Untersuchungsteams.

Typische Anti-Muster:

- Verschiedene Personengruppen untersuchen Erkenntnisse und Warnmeldungen, die von verschiedenen Systemen generiert werden, sofern nicht durch Anforderungen der Aufgabentrennung etwas anderes vorgeschrieben ist.
- Ihre Organisation leitet alle Sicherheitserkenntnisse und -warnmeldungen an Standardspeicherorte weiter, verlangt aber von den Ermittlern, dass sie diese manuell korrelieren und anreichern.
- Sie verlassen sich ausschließlich auf die Intelligenz von Bedrohungserkennungssystemen, um über Erkenntnisse zu berichten und die Kritikalität zu bestimmen.

Vorteile der Nutzung dieser bewährten Methode: Die automatische Korrelation und Anreicherung von Warnmeldungen trägt dazu bei, die gesamte kognitive Belastung und die manuelle Datenaufbereitung zu reduzieren, die Ihre Ermittler benötigen. Diese Methode kann die Zeit verkürzen, die benötigt wird, um festzustellen, ob es sich bei dem Ereignis um einen Vorfall handelt, und eine formelle Reaktion einzuleiten. Zusätzlicher Kontext hilft Ihnen auch, den wahren Schweregrad eines Ereignisses genau zu bewerten, da er höher oder niedriger sein kann, als eine einzelne Warnmeldung vermuten lässt.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

Implementierungsleitfaden

Sicherheitswarnmeldungen können von vielen verschiedenen Quellen innerhalb von AWS stammen, darunter:

- Services wie Amazon GuardDuty, AWS Security Hub CSPM, Amazon Macie, Amazon Inspector, AWS Config, AWS Identity and Access Management Access Analyzer und Network Access Analyzer
- Warnmeldungen aus der automatisierten Analyse von AWS-Service-, Infrastruktur- und Anwendungsprotokollen, z. B. von Security Analytics for Amazon OpenSearch Service.
- Warnungen als Reaktion auf Änderungen in Ihrer Abrechnungsaktivität aus Quellen wie Amazon CloudWatch, Amazon EventBridge oder AWS Budgets.
- Quellen von Drittanbietern wie Threat Intelligence Feeds und Security Partner Solutions vom AWS Partner Network
- Kontakt durch AWS-Vertrauen und -Sicherheit oder andere Quellen, wie Kunden oder interne Mitarbeiter.

- Verwenden Sie den Threat Technique Catalog von AWS (TTC), um das Verhalten von Bedrohungsakteuren anhand von Indicator of Compromise (IoC) zu identifizieren und zu korrelieren. Der TTC ist eine Erweiterung des MITRE ATT&CK-Frameworks und kategorisiert alle bekannten und beobachteten Verhaltensweisen und Techniken von Bedrohungsakteuren, die sich gegen AWS-Ressourcen richten.

In ihrer grundlegendsten Form enthalten Warnmeldungen Informationen darüber, wer (Prinzipal oder Identität) was (die Aktion, die ergriffen wird) im Hinblick worauf (Ressourcen, die betroffen sind) tut. Ermitteln Sie für jede dieser Quellen, ob es Möglichkeiten gibt, Zuordnungen zwischen den Identifikatoren für diese Identitäten, Aktionen und Ressourcen als Grundlage für die Durchführung von Korrelationen zu erstellen. Dies kann in Form einer Integration von Quellen für Warnmeldungen mit einem SIEM-Tool (Security Information and Event Management) erfolgen, das eine automatische Korrelation für Sie durchführt, oder durch den Aufbau eigener Datenpipelines und -verarbeitung oder durch eine Kombination aus beidem.

Ein Beispiel für einen Dienst, der eine Korrelation für Sie durchführen kann, ist Amazon Detective. Detective nimmt laufend Warnmeldungen aus verschiedenen AWS- und Drittquellen auf und nutzt verschiedene Formen von Informationen, um eine visuelle Grafik ihrer Beziehungen zur Unterstützung von Ermittlungen zusammenzustellen.

Während die anfängliche Kritikalität eines Alarms eine Hilfe für die Priorisierung ist, bestimmt der Kontext, in dem der Alarm auftrat, seine wahre Kritikalität. Zum Beispiel kann Amazon GuardDuty die Warnmeldung ausgeben, dass eine Amazon EC2-Instance innerhalb Ihres Workloads einen unerwarteten Domain-Namen abfragt. GuardDuty könnte dieser Warnmeldung von sich aus eine niedrige Kritikalität zuweisen. Eine automatische Korrelation mit anderen Aktivitäten zum Zeitpunkt der Warnmeldung könnte jedoch aufdecken, dass mehrere hundert EC2-Instances von derselben Identität bereitgestellt wurden, was die Gesamtbetriebskosten erhöht. In diesem Fall würde dieser korrelierte Ereigniskontext zur Veröffentlichung einer neuen Sicherheitswarnung führen. Die Kritikalität wird möglicherweise als hoch festgelegt, was die weiteren Maßnahmen beschleunigen würde.

Implementierungsschritte

1. Identifizieren Sie Quellen für Informationen zu Sicherheitswarnmeldungen. Verstehen Sie, wie Warnmeldungen aus diesen Systemen Identität, Aktion und Ressourcen darstellen, um festzustellen, wo eine Korrelation möglich ist.

2. Richten Sie einen Mechanismus zur Erfassung von Warnmeldungen aus verschiedenen Quellen ein. Ziehen Sie zu diesem Zweck Services wie Security Hub CSPM, EventBridge und CloudWatch in Betracht.
3. Identifizieren Sie Quellen für die Korrelation und Anreicherung von Daten. Zu den Beispielquellen gehören AWS CloudTrail, VPC-Flow-Protokolle, Route-53-Resolver-Protokolle sowie Infrastruktur- und Anwendungsprotokolle. Einige oder alle dieser Protokolle können über eine einzige Integration mit Amazon Security Lake verwendet werden.
4. Integrieren Sie Ihre Warnmeldungen mit Ihren Datenkorrelations- und -anreicherungsquellen, um detailliertere Kontexte für Sicherheitsereignisse zu erstellen und die Kritikalität zu ermitteln.
    a. Amazon Detective, SIEM-Tools oder andere Lösungen von Drittanbietern können ein gewisses Maß an Erfassung, Korrelation und Anreicherung automatisch durchführen.
    b. Sie können auch AWS-Services nutzen, um Ihre eigenen zu erstellen. Sie können zum Beispiel eine AWS Lambda-Funktion aufrufen, um eine Amazon Athena-Abfrage von AWS CloudTrail oder Amazon Security Lake auszuführen, und die Ergebnisse in EventBridge veröffentlichen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC10-BP03 Vorbereiten forensischer Funktionen
- OPS08-BP04 Erstellen umsetzbarer Warnmeldungen
- REL06-BP03 Senden von Benachrichtigungen (Verarbeitung und Benachrichtigung in Echtzeit)

Zugehörige Dokumente:

- AWS Security Incident Response Guide

Zugehörige Beispiele:

- How to enrich AWS Security Hub CSPM findings with account metadata

Zugehörige Tools:

- Amazon Detective
- Amazon EventBridge

- AWS Lambda
- Amazon Athena

SEC04-BP04 Initiieren von Abhilfemaßnahmen für nicht konforme Ressourcen

Ihre detektivischen Kontrollen können Sie auf Ressourcen aufmerksam machen, die nicht mit Ihren Konfigurationsanforderungen übereinstimmen. Sie können programmatisch definierte Abhilfemaßnahmen einleiten, entweder manuell oder automatisch, um diese Ressourcen zu korrigieren und mögliche Auswirkungen zu minimieren. Wenn Sie Abhilfemaßnahmen programmatisch definieren, können Sie sofort und konsequent handeln.

Automatisierung kann zwar den Sicherheitsbetrieb verbessern, aber Sie sollten die Automatisierung sorgfältig implementieren und verwalten. Schaffen Sie geeignete Überwachungs- und Kontrollmechanismen, um zu überprüfen, ob die automatisierten Antworten effektiv und genau sind und mit den Organisationsrichtlinien und der Risikobereitschaft übereinstimmen.

Gewünschtes Ergebnis: Sie definieren Standards für die Ressourcenkonfiguration und die Schritte zur Behebung, wenn festgestellt wird, dass die Ressourcen nicht konform sind. Wo immer möglich, haben Sie Abhilfemaßnahmen programmatisch definiert, sodass sie entweder manuell oder durch Automatisierung eingeleitet werden können. Es gibt Erkennungssysteme, die nicht konforme Ressourcen identifizieren und Warnungen in zentralisierten Tools veröffentlichen, die von Ihrem Sicherheitspersonal überwacht werden. Diese Tools unterstützen die Durchführung Ihrer programmatischen Korrekturen, entweder manuell oder automatisch. Automatische Abhilfemaßnahmen verfügen über angemessene Überwachungs- und Kontrollmechanismen, um ihre Verwendung zu steuern.

Typische Anti-Muster:

- Sie implementieren Automatisierung, versäumen es aber, Abhilfemaßnahmen gründlich zu testen und zu validieren. Dies kann unbeabsichtigte Folgen haben, wie z. B. die Unterbrechung legitimer Geschäftsabläufe oder die Instabilität des Systems.
- Sie verbessern die Reaktionszeiten und Verfahren durch Automatisierung, aber ohne angemessene Überwachung und Mechanismen, die bei Bedarf menschliches Eingreifen und Urteilsvermögen ermöglichen.
- Sie verlassen sich ausschließlich auf Abhilfemaßnahmen, anstatt Abhilfemaßnahmen als Teil eines umfassenderen Programms zur Reaktion auf Vorfälle und zur Wiederherstellung zu nutzen.

Vorteile der Nutzung dieser bewährten Methode: Automatische Abhilfemaßnahmen können schneller auf Fehlkonfigurationen reagieren als manuelle Prozesse. So können Sie potenzielle Auswirkungen auf Ihr Unternehmen minimieren und das Zeitfenster für unbeabsichtigte Nutzungen verringern. Wenn Sie Abhilfemaßnahmen programmatisch definieren, werden sie konsistent angewendet, was das Risiko menschlicher Fehler verringert. Die Automatisierung kann auch eine größere Anzahl von Alarmen gleichzeitig verarbeiten, was besonders in Umgebungen von großem Maßstab wichtig ist.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Wie unter SEC01-BP03 Identifizieren und Validieren von Kontrollzielen beschrieben, können Services wie AWS Config und AWS Security Hub CSPM Ihnen dabei helfen, die Konfiguration der Ressourcen in Ihren Konten auf die Einhaltung Ihrer Anforderungen zu überwachen. Wenn nicht konforme Ressourcen erkannt werden, können Services wie AWS Security Hub CSPM bei der angemessenen Weiterleitung von Warnmeldungen und der Behebung von Problemen helfen. Diese Lösungen bieten einen zentralen Ort für Ihre Sicherheitsbeauftragten, um Probleme zu überwachen und Korrekturmaßnahmen zu ergreifen.

Zusätzlich zu AWS Security Hub CSPM führte AWS Security Hub Advanced ein. Dieser Service, der auf der re:Invent 2025 angekündigt wurde, verändert die Art und Weise, wie Unternehmen ihre kritischsten Sicherheitsprobleme priorisieren und in großem Umfang reagieren, um ihre Cloud-Umgebungen zu schützen. Der erweiterte Security Hub verwendet jetzt fortschrittliche Analytik, um Sicherheitssignale in Ihrer Cloud-Umgebung automatisch zu korrelieren, anzureichern und zu priorisieren. Security Hub lässt sich nahtlos in Amazon GuardDuty, Amazon Inspector, Amazon Macie und AWS Security Hub CSPM integrieren. Korrelierte Erkenntnisse in Security Hub können zu einem völlig neuen Ergebnis führen, das als „Bedrohungserkenntnis“ bezeichnet wird. Dazu gehört ein angenommener Angriffspfad, der auf den in jeder Ressource gefundenen Schwachstellen basiert.

Einige Situationen, in denen Ressourcen nicht konform sind, können zwar einzigartig sein und erfordern menschliches Urteilsvermögen, um Abhilfe zu schaffen. Für andere Fälle gibt es jedoch eine Standardreaktion, die Sie programmatisch definieren können. Eine Standardreaktion auf eine falsch konfigurierte VPC-Sicherheitsgruppe könnte zum Beispiel darin bestehen, die unzulässigen Regeln zu entfernen und den Eigentümer zu benachrichtigen. Antworten können in AWS Lambda-Funktionen, in AWS-Systems-Manager-Automation-Dokumenten oder durch andere von Ihnen bevorzugte Code-Umgebungen definiert werden. Vergewissern Sie sich, dass die Umgebung in der Lage ist, sich bei AWS zu authentifizieren, indem Sie eine IAM-Rolle mit der geringsten Berechtigung verwenden, die für die Durchführung von Korrekturmaßnahmen erforderlich ist.

Sobald Sie die gewünschte Abhilfemaßnahme definiert haben, können Sie festlegen, wie Sie diese einleiten möchten. AWS Config kann Abhilfemaßnahmen für Sie einleiten. Wenn Sie Security Hub CSPM verwenden, können Sie dies über benutzerdefinierte Aktionen tun, wodurch die Erkenntnisinformationen in Amazon EventBridge veröffentlicht werden. Eine EventBridge-Regel kann dann Ihre Abhilfe einleiten. Sie können die Fehlerbehebungen in Security Hub CSPM für die automatische oder manuelle Ausführung konfigurieren.

Für programmatische Abhilfemaßnahmen empfehlen wir Ihnen, umfassende Protokolle und Audits für die durchgeführten Maßnahmen sowie deren Ergebnisse zu führen. Prüfen und analysieren Sie diese Protokolle, um die Effektivität der automatisierten Prozesse zu bewerten und Verbesserungsmöglichkeiten zu identifizieren. Erfassen Sie Protokolle in Amazon CloudWatch Logs und Abhilfeergebnisse als Erkenntnisse in Security Hub CSPM.

Als Ausgangspunkt sollten Sie Automatische Sicherheitsreaktion in AWS verwenden, das über vorgefertigte Abhilfemaßnahmen zur Behebung häufiger Sicherheitsfehlkonfigurationen verfügt.

Implementierungsschritte

1. Analysieren und priorisieren Sie Warnmeldungen.
    a. Konsolidieren Sie Sicherheitswarnungen von verschiedenen AWS-Services in Security Hub CSPM für eine zentrale Übersicht, Priorisierung und Abhilfe.
2. Entwickeln Sie Abhilfemaßnahmen.
    a. Verwenden Sie Services wie Systems Manager und AWS Lambda, um programmatische Korrekturen durchzuführen.
3. Konfigurieren Sie, wie Abhilfemaßnahmen eingeleitet werden.
    a. Definieren Sie mithilfe von Systems Manager benutzerdefinierte Aktionen, die Erkenntnisse an EventBridge veröffentlichen. Konfigurieren Sie diese Aktionen so, dass sie manuell oder automatisch ausgelöst werden.
    b. Sie können auch Amazon Simple Notification Service (SNS) verwenden, um Benachrichtigungen und Warnmeldungen an relevante Beteiligte (wie das Sicherheitsteam oder das Vorfallsreaktionsteam) zu senden, damit diese bei Bedarf manuell eingreifen oder eskalieren können.
4. Prüfen und analysieren Sie die Protokolle der Abhilfemaßnahmen auf Wirksamkeit und Verbesserung.
    a. Senden Sie die Protokollausgabe an CloudWatch Logs. Erfassen Sie die Ergebnisse als Erkenntnisse in Security Hub CSPM.

Ressourcen

Zugehörige bewährte Methoden:

- SEC06-BP03 Reduzieren der manuellen Verwaltung und des interaktiven Zugriffs

Zugehörige Dokumente:

- AWS Security Incident Response Guide - Detection

Zugehörige Beispiele:

- Automatisierte Sicherheitsreaktion in AWS
- Monitor EC2 instance key pairs using AWS Config
- Create AWS Config custom rules by using AWS CloudFormation Guard policies
- Automatically remediate unencrypted Amazon RDS DB instances and clusters

Zugehörige Tools:

- AWS Systems Manager Automation
- Automatisierte Sicherheitsreaktion in AWS

Schutz der Infrastruktur

Der Schutz der Infrastruktur umfasst Kontrollmethoden, z. B. die Tiefenverteidigung, die notwendig sind, um bewährte Methoden und organisatorische oder gesetzliche Verpflichtungen zu erfüllen. Die Nutzung dieser Methoden ist für erfolgreiche, kontinuierliche Betriebsabläufe sowohl in der Cloud als auch lokal ausschlaggebend.

Der Schutz der Infrastruktur ist ein wichtiger Bestandteil eines Informationssicherheitsprogramms. Sie schützen dadurch die Systeme und Services innerhalb Ihrer Workload vor unbeabsichtigten und nicht autorisierten Zugriffen sowie potenziellen Schwachstellen. Sie definieren beispielsweise Vertrauensgrenzen (z. B. Netzwerk- und Kontogrenzen), Systemsicherheitskonfiguration und -wartung (z. B. Härtung, Minimierung und Patching), Betriebssystemauthentifizierung und Autorisierungen (z. B. Benutzer, Schlüssel und Zugriffsebenen) und andere geeignete Durchsetzungsmechanismen für Richtlinien (z. B. Firewalls für Webanwendungen und/oder API-Gateways).

Regionen, Availability Zones, AWS Local Zones und AWS Outposts

Stellen Sie sicher, dass Sie vertraut sind mit Regionen, Availability Zones, AWS Local Zones und AWS Outposts, die Bestandteile der sicheren globalen AWS-Infrastruktur sind.

Das Konzept von AWS beruht auf Regionen, bei denen es sich um physische Standorte auf der ganzen Welt handelt, in denen wir Rechenzentren als Cluster zusammenfassen. Wir nennen jede Gruppe logischer Rechenzentren eine Availability Zone (AZ). Jede AWS-Region besteht aus mehreren isolierten und räumlich getrennten AZs innerhalb eines geografischen Gebiets. Wenn Sie Anforderungen an die Datenresidenz haben, können Sie die AWS-Region wählen, die sich in der Nähe Ihres gewünschten Standorts befindet. Sie behalten volle Kontrolle und Rechte über die Regionen bei, in denen Ihre Daten sich physisch befinden; was hilfreich sein kann Ihre regionalen Anforderungen an Compliance und Datenresidenz zu erfüllen. Jede AZ verfügt über eine unabhängige Stromversorgung, Kühlung und physische Sicherheit. Wenn eine Anwendung auf mehrere AZs aufgeteilt ist, sind Sie besser isoliert und vor Problemen wie Stromausfällen, Blitzeinschlägen, Tornados, Erdbeben usw. geschützt. AZs sind physisch durch eine deutliche Entfernung von vielen Kilometern voneinander getrennt, liegen aber alle in einem Umkreis von 100 km voneinander. Alle AZs in einer AWS-Region sind über ein Netzwerk mit hoher Bandbreite und niedriger Latenz miteinander verbunden, wobei vollständig redundante, dedizierte Metro-Glasfasern verwendet werden, die einen hohen Durchsatz und eine niedrige Latenz zwischen den AZs ermöglichen. Der gesamte Datenverkehr zwischen den AZs ist verschlüsselt. AWS-Kunden, die Wert auf hohe Verfügbarkeit legen, können ihre Anwendungen so konzipieren, dass sie in mehreren

AZs laufen, um eine noch größere Fehlertoleranz zu erreichen. AWS- Regionen erfüllen die höchsten Anforderungen an Sicherheit, Compliance und Datenschutz.

AWS Local Zones bringen Datenverarbeitungs-, Speicher-, Datenbank- und andere ausgewählte AWS-Services näher an die Endnutzer heran. Mit AWS Local Zones können Sie problemlos anspruchsvolle Anwendungen ausführen, die Latenzzeiten im einstelligen Millisekundenbereich für Ihre Endbenutzer erfordern, wie z. B. die Erstellung von Medien- und Unterhaltungsinhalten, Echtzeitspiele, Reservoirsimulationen, die Automatisierung von Elektronikdesign und Machine Learning. Jeder Standort einer AWS Local Zone ist eine Erweiterung einer AWS-Region, in der Sie Ihre latenzempfindlichen Anwendungen unter Verwendung von AWS-Services wie Amazon EC2, Amazon VPC, Amazon EBS, Amazon File Storage und Elastic Load Balancing in geografischer Nähe zu den Endbenutzern ausführen können. AWS Local Zones bieten eine sichere Verbindung mit hoher Bandbreite zwischen lokalen Workloads und denjenigen, die in der AWS-Region ausgeführt werden. So können Sie über dieselben APIs und Toolsets nahtlos auf die gesamte Palette der Services in der Region zugreifen.

AWS Outposts bringen native AWS-Services, Infrastruktur und Betriebsmodelle in praktisch jedes Rechenzentrum, jede Co-Location-Umgebung und jede On-Premises-Einrichtung. Sie können dieselben AWS-APIs, Tools und Infrastrukturen sowohl On-Premises als auch in der AWS-Cloud nutzen, um ein wirklich konsistentes Hybrid-Erlebnis zu bieten. AWS Outposts ist für vernetzte Umgebungen konzipiert und kann zur Unterstützung von Workloads eingesetzt werden, die aufgrund geringer Latenzzeiten oder lokaler Datenverarbeitungsanforderungen On-Premises bleiben müssen.

AWS bietet eine Reihe von Ansätzen zum Schutz der Infrastruktur. In den nächsten Abschnitten werden folgende Ansätze erläutert.

Themen

Schutz von Netzwerken

Benutzer, sowohl Ihre Mitarbeiter als auch Ihre Kunden, können sich überall befinden. Sie müssen sich von traditionellen Modellen verabschieden, bei denen Sie allem und jedem vertrauen, das Zugang zu Ihrem Netzwerk hat. Wenn Sie dem Prinzip folgen, Sicherheit auf allen Ebenen anzuwenden, setzen Sie einen Zero-Trust-Ansatz um. Zero-Trust-Sicherheit ist ein Modell, bei dem

Anwendungskomponenten oder Microservices als voneinander getrennt betrachtet werden und keine Komponente oder kein Microservice anderen vertraut.

Die sorgfältige Verwaltung Ihres Netzwerkdesigns bildet die Grundlage, um Ressourcen innerhalb Ihrer Workload zu isolieren und einzugrenzen. Da viele Ressourcen in Ihrer Workload in einer VPC ausgeführt werden und die Sicherheitseigenschaften übernehmen, ist es wichtig, dass das Design automatisierte Inspektions- und Schutzmechanismen unterstützt wird. Für Workloads, welche außerhalb einer VPC mit Edge-Services oder Serverless ausgeführt werden, bestehen vereinfachte bewährte Methoden. Spezifische Anleitungen zur Serverless-Sicherheit finden Sie unter AWS Well-Architected Serverless Application Lens.

Bewährte Methoden

- SEC05-BP01 Erstellen von Netzwerkebenen
- SEC05-BP02 Kontrollieren des Datenverkehrsflusses innerhalb Ihrer Netzwerkebenen
- SEC05-BP03 Implementieren Sie einen inspektionsbasierten Schutz
- SEC05-BP04 Automatisieren Sie den Netzwerkschutz

SEC05-BP01 Erstellen von Netzwerkebenen

Segmentieren Sie Ihre Netzwerktopologie in verschiedene Ebenen, die auf logischen Gruppierungen Ihrer Workload-Komponenten entsprechend ihrer Datensensibilität und Zugriffsanforderungen basieren. Unterscheiden Sie zwischen Komponenten, auf die vom Internet aus zugegriffen werden muss, wie z. B. öffentliche Web-Endpunkte, und solchen, die nur intern erreichbar sein müssen, wie z. B. Datenbanken.

Gewünschtes Ergebnis: Die Ebenen Ihres Netzwerks sind Teil eines ganzheitlichen, tiefgreifenden Sicherheitsansatzes, der die Identitätsauthentifizierungs- und Autorisierungsstrategie Ihrer Workloads ergänzt. Je nach Sensibilität der Daten und den Zugriffsanforderungen werden Ebenen mit entsprechenden Verkehrsfluss- und Kontrollmechanismen eingerichtet.

Typische Anti-Muster:

- Sie erstellen alle Ressourcen in einem einzigen VPC oder Subnetz.
- Sie erstellen Ihre Netzwerkebenen ohne Rücksicht auf die Anforderungen an die Datensensibilität, das Verhalten der Komponenten oder die Funktionalität.
- Sie verwenden VPCs und Subnetze als Standards für alle Aspekte der Netzwerkebenen und berücksichtigen nicht, wie verwaltete AWS-Services Ihre Topologie beeinflussen.

Vorteile der Nutzung dieser bewährten Methode: Die Einrichtung von Netzwerkebenen ist der erste Schritt, um unnötige Pfade durch das Netzwerk einzuschränken, insbesondere solche, die zu kritischen Systemen und Daten führen. Dadurch wird es für Unbefugte schwieriger, sich Zugriff auf Ihr Netzwerk zu verschaffen und zu weiteren Ressourcen darin zu navigieren. Diskrete Netzwerkebenen reduzieren den Umfang der Analyse für Inspektionssysteme, z. B. für die Erkennung von Eindringlingen oder die Verhinderung von Malware, vorteilhaft. Dadurch wird das Potenzial für Fehlalarme und unnötigen Verarbeitungsaufwand reduziert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Beim Entwurf einer Workload-Architektur ist es üblich, die Komponenten je nach ihrer Verantwortlichkeit in verschiedene Ebenen aufzuteilen. Eine Webanwendung kann zum Beispiel eine Präsentationsebene, eine Anwendungsebene und eine Datenebene haben. Bei der Gestaltung Ihrer Netzwerktopologie können Sie einen ähnlichen Ansatz wählen. Die zugrunde liegenden Netzwerkkontrollen können dazu beitragen, die Anforderungen Ihres Workloads an den Datenzugriff durchzusetzen. In einer dreistufigen Webanwendungsarchitektur können Sie zum Beispiel Ihre statischen Präsentationsebenendateien in Amazon S3 speichern und sie von einem Content Delivery Network (CDN) wie Amazon CloudFront aus bereitstellen. Die Anwendungsebene kann öffentliche Endpunkte haben, die ein Application Load Balancer (ALB) in einem Amazon VPC-öffentlichen Subnetz (ähnlich einer demilitarisierten Zone oder DMZ) bedient, während die Backend-Services in privaten Subnetzen bereitgestellt werden. Die Datenebene, die Ressourcen wie Datenbanken und gemeinsam genutzte Dateisysteme hostet, kann sich in anderen privaten Subnetzen befinden als die Ressourcen Ihrer Anwendungsebene. An jeder dieser Ebenengrenzen (CDN, öffentliches Subnetz, privates Subnetz) können Sie Kontrollen bereitstellen, die es nur autorisiertem Datenverkehr erlauben, diese Grenzen zu überqueren.

Ähnlich wie bei der Modellierung von Netzwerkebenen auf der Grundlage des funktionalen Zwecks der Komponenten Ihres Workloads sollten Sie auch die Sensibilität der verarbeiteten Daten berücksichtigen. Wenn Sie das Beispiel der Webanwendung verwenden, kann es sein, dass alle Ihre Workload-Services innerhalb der Anwendungsebene angesiedelt sind, während verschiedene Services Daten mit unterschiedlichen Sensibilitätsstufen verarbeiten. In diesem Fall kann die Aufteilung der Anwendungsebene durch mehrere private Subnetze, verschiedene VPCs in demselben AWS-Konto oder sogar verschiedene VPCs in verschiedenen AWS-Konten für jede Stufe der Datensensibilität je nach Ihren Kontrollanforderungen angemessen sein.

Eine weitere Überlegung für Netzwerkebenen ist die Verhaltenskonsistenz der Komponenten Ihres Workloads. Um das Beispiel fortzusetzen: In der Anwendungsebene haben Sie möglicherweise

Services, die Eingaben von Endbenutzern oder externen Systemintegrationen akzeptieren, die von Natur aus risikoreicher sind als die Eingaben für andere Services. Beispiele sind das Hochladen von Dateien, das Ausführen von Skripten, das Scannen von E-Mails und so weiter. Die Unterbringung dieser Services in einer eigenen Netzwerkebene hilft dabei, eine stärkere Isolationsgrenze um sie herum zu schaffen, und kann verhindern, dass ihr einzigartiges Verhalten falsche positive Alarme in Inspektionssystemen erzeugt.

Berücksichtigen Sie bei Ihrer Planung, wie die Nutzung von AWS verwalteten Services Ihre Netzwerktopologie beeinflusst. Erfahren Sie, wie Services wie Amazon VPC Lattice die Interoperabilität Ihrer Workload-Komponenten über Netzwerkebenen hinweg erleichtern können. Wenn Sie AWS Lambda verwenden, sollten Sie die Bereitstellung in Ihren VPC-Subnetzen vornehmen, es sei denn, es gibt besondere Gründe, die dagegen sprechen. Bestimmen Sie, wo VPC-Endpunkte und AWS PrivateLink die Einhaltung von Sicherheitsrichtlinien, die den Zugriff auf Internet-Gateways beschränken, vereinfachen können.

Implementierungsschritte

1. Überprüfen Sie Ihre Workload-Architektur. Gruppieren Sie Komponenten und Services logisch nach den Funktionen, die sie erfüllen, nach der Sensibilität der verarbeiteten Daten und nach ihrem Verhalten.
2. Für Komponenten, die auf Anfragen aus dem Internet reagieren, sollten Sie Load Balancer oder andere Proxys verwenden, um öffentliche Endpunkte bereitzustellen. Erkunden Sie die Verlagerung der Sicherheitskontrollen durch den Einsatz von verwalteten Services wie CloudFront, Amazon API Gateway, Elastic Load Balancing und AWS Amplify zum Hosten öffentlicher Endpunkte.
3. Für Komponenten, die in Datenverarbeitungsumgebungen ausgeführt werden, wie Amazon EC2-Instances, AWS Fargate-Container oder Lambda-Funktionen, stellen Sie diese in privaten Subnetzen bereit, und zwar basierend auf Ihren Gruppen aus dem ersten Schritt.
4. Für vollständig verwaltete AWS-Services, wie Amazon DynamoDB, Amazon Kinesis oder Amazon SQS, sollten Sie VPC-Endpunkte als Standard für den Zugriff über private IP-Adressen verwenden.

Ressourcen

Zugehörige bewährte Methoden:

- REL02 Planen der Netzwerktopologie

- PERF04-BP01 Verstehen der Auswirkungen des Netzwerks auf die Leistung

Zugehörige Videos:

- AWS re:Invent 2.023 - AWS networking foundations

Zugehörige Beispiele:

- VPC-Beispiele
- Greifen Sie privat auf Container-Anwendungen auf Amazon ECS zu, indem Sie AWS Fargate, AWS PrivateLink und einen Network Load Balancer verwenden
- Serve static content in an Amazon S3 bucket through a VPC by using Amazon CloudFront

SEC05-BP02 Kontrollieren des Datenverkehrsflusses innerhalb Ihrer Netzwerkebenen

Verwenden Sie innerhalb der einzelnen Ebenen Ihres Netzwerks eine weitere Segmentierung, um den Datenverkehr auf die für die einzelnen Workloads erforderlichen Flüsse zu beschränken. Konzentrieren Sie sich zunächst auf die Kontrolle des Datenverkehrs zwischen dem Internet oder anderen externen Systemen eines Workloads und Ihrer Umgebung (Nord-Süd-Verkehr). Betrachten Sie anschließend die Ströme zwischen verschiedenen Komponenten und Systemen (Ost-West-Verkehr).

Gewünschtes Ergebnis: Sie lassen nur die Netzwerkflüsse zu, die für die Kommunikation der Komponenten Ihrer Workloads untereinander, mit ihren Clients und mit allen anderen Services, von denen sie abhängig sind, erforderlich sind. Ihr Design berücksichtigt Überlegungen wie öffentlichen im Vergleich zu privatem Ingress und Egress, Datenklassifizierung, regionale Vorschriften und Protokollanforderungen. Wo immer es möglich ist, bevorzugen Sie Punkt-zu-Punkt-Flüsse gegenüber Netzwerk-Peering im Rahmen des Prinzips der geringsten Berechtigung.

Typische Anti-Muster:

- Sie verfolgen bei der Netzwerksicherheit einen Perimeter-basierten Ansatz und kontrollieren den Datenverkehr nur an den Grenzen Ihrer Netzwerkebenen.
- Sie gehen davon aus, dass der gesamte Verkehr innerhalb einer Netzwerkebene authentifiziert und autorisiert ist.

- Sie kontrollieren entweder den eingehenden oder den ausgehenden Datenverkehr, aber nicht beide.
- Sie verlassen sich bei der Authentifizierung und Autorisierung des Datenverkehrs ausschließlich auf Ihre Workload-Komponenten und Netzwerkkontrollen.

Vorteile der Nutzung dieser bewährten Methode: Diese Vorgehensweise trägt dazu bei, das Risiko unbefugter Bewegungen innerhalb Ihres Netzwerks zu verringern, und fügt Ihren Workloads eine zusätzliche Autorisierungsebene hinzu. Durch die Kontrolle des Datenverkehrs können Sie den Umfang der Auswirkungen eines Sicherheitsvorfalls begrenzen und die Erkennung und Reaktion beschleunigen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Netzwerkebenen helfen zwar bei der Abgrenzung von Komponenten Ihres Workloads, die eine ähnliche Funktion, eine ähnliche Datensensibilität und ein ähnliches Verhalten aufweisen. Sie können jedoch eine wesentlich feinere Ebene der Datenverkehrskontrolle schaffen, indem Sie Techniken zur weiteren Segmentierung von Komponenten innerhalb dieser Ebenen einsetzen, die dem Prinzip der geringsten Berechtigung folgen. Innerhalb von AWS werden Netzwerkebenen in erster Linie über Subnetze entsprechend den IP-Adressbereichen innerhalb eines Amazon VPC definiert. Ebenen können auch über verschiedene VPCs definiert werden, z. B. für die Gruppierung von Microservice-Umgebungen nach Business Domain. Wenn Sie mehrere VPCs verwenden, vermitteln Sie das Routing mit einem AWS Transit Gateway. Dies ermöglicht zwar die Kontrolle des Datenverkehrs auf Layer-4-Ebene (IP-Adressen- und Portbereiche) mithilfe von Sicherheitsgruppen und Routing-Tabellen, aber Sie können mit zusätzlichen Services, wie AWS PrivateLink, Amazon Route 53-Resolver-DNS-Firewall, AWS Network Firewall und AWS WAF weitere Kontrolle erlangen.

Verstehen und inventarisieren Sie den Datenfluss und die Kommunikationsanforderungen Ihrer Workloads in Bezug auf verbindungsauslösende Parteien, Ports, Protokolle und Netzwerkebenen. Prüfen Sie die verfügbaren Protokolle für den Verbindungsaufbau und die Datenübertragung, um diejenigen auszuwählen, die Ihre Schutzanforderungen erfüllen (z. B. HTTPS statt HTTP). Erfassen Sie diese Anforderungen sowohl an den Grenzen Ihrer Netzwerke als auch innerhalb jeder Ebene. Sobald diese Anforderungen identifiziert sind, prüfen Sie die Möglichkeiten, um nur den erforderlichen Datenverkehr an jedem Verbindungspunkt zuzulassen. Ein guter Ausgangspunkt ist die Verwendung von Sicherheitsgruppen innerhalb Ihrer VPC, da sie an Ressourcen angehängt werden können, die eine Elastic-Network-Schnittstelle (ENI) verwenden, wie Amazon EC2-Instances, Amazon ECS-

Aufgaben, Amazon EKS-Pods oder Amazon RDS-Datenbanken. Im Gegensatz zu einer Layer-4-Firewall kann eine Sicherheitsgruppe eine Regel haben, die den Datenverkehr einer anderen Sicherheitsgruppe anhand ihrer Kennung zulässt, wodurch Aktualisierungen minimiert werden, wenn sich die Ressourcen innerhalb der Gruppe im Laufe der Zeit ändern. Sie können den Datenverkehr auch mithilfe von Sicherheitsgruppen nach eingehenden und ausgehenden Regeln filtern.

Wenn sich der Datenverkehr zwischen VPCs bewegt, ist es üblich, VPC-Peering für einfaches Routing oder AWS Transit Gateway für komplexes Routing zu verwenden. Mit diesen Ansätzen erleichtern Sie den Datenverkehrsfluss zwischen dem Bereich der IP-Adressen des Quell- und des Zielnetzwerks. Wenn Ihr Workload jedoch nur Datenverkehrsflüsse zwischen bestimmten Komponenten in verschiedenen VPCs erfordert, sollten Sie eine Punkt-zu-Punkt-Verbindung mit AWS PrivateLink verwenden. Bestimmen Sie dazu, welcher Service als Produzent und welcher als Verbraucher fungieren soll. Stellen Sie einen kompatiblen Load Balancer für den Produzenten bereit, schalten Sie PrivateLink entsprechend ein und akzeptieren Sie dann eine Verbindungsanfrage des Verbrauchers. Dem Produzenten-Service wird dann eine private IP-Adresse aus der VPC des Verbrauchers zugewiesen, die der Verbraucher für nachfolgende Anfragen verwenden kann. Dieser Ansatz reduziert die Notwendigkeit, die Netzwerke zu peeren. Beziehen Sie die Kosten für die Datenverarbeitung und den Load Balancer in die Bewertung von PrivateLink mit ein.

Sicherheitsgruppen und PrivateLink tragen zwar dazu bei, den Fluss zwischen den Komponenten Ihrer Workloads zu kontrollieren. Eine weitere wichtige Überlegung ist jedoch, wie Sie kontrollieren können, auf welche DNS-Domains Ihre Ressourcen zugreifen dürfen (falls überhaupt). Abhängig von der DHCP-Konfiguration Ihrer VPCs können Sie zwei verschiedene AWS-Services für diesen Zweck in Betracht ziehen. Die meisten Kunden verwenden den standardmäßigen Route 53-Resolver DNS-Service (auch Amazon-DNS-Server oder AmazonProvidedDNS genannt), der für VPCs unter der +2-Adresse ihres CIDR-Bereichs verfügbar ist. Mit diesem Ansatz können Sie DNS-Firewall-Regeln erstellen und diese mit Ihrer VPC verknüpfen, die festlegen, welche Aktionen für die von Ihnen bereitgestellten Domain-Listen durchgeführt werden sollen.

Wenn Sie nicht den Route 53-Resolver verwenden, oder wenn Sie den Resolver mit tieferen Prüf- und Flusskontrollfunktionen als der Domain-Filterung ergänzen wollen, sollten Sie die Bereitstellung eines AWS Network Firewall erwägen. Dieser Service prüft einzelne Pakete anhand von zustandslosen oder zustandsbehafteten Regeln, um zu entscheiden, ob der Datenverkehr verweigert oder zugelassen werden soll. Einen ähnlichen Ansatz können Sie für die Filterung des eingehenden Internetdatenverkehrs zu Ihren öffentlichen Endpunkten mit AWS WAF verfolgen. Weitere Hinweise zu diesen Services finden Sie unter SEC05-BP03 Implementieren eines prüfungsbasierten Schutzes.

Implementierungsschritte

1. Identifizieren Sie die erforderlichen Datenflüsse zwischen den Komponenten Ihrer Workloads.
2. Wenden Sie mehrere Kontrollen mit einem Ansatz der Tiefenverteidigung sowohl für den eingehenden als auch für den ausgehenden Datenverkehr an, einschließlich der Verwendung von Sicherheitsgruppen und Routing-Tabellen.
3. Verwenden Sie Firewalls, um eine feinkörnige Kontrolle über den Netzwerkverkehr in, aus und zwischen Ihren VPCs zu definieren, wie z. B. die Route 53 Resolver DNS Firewall, AWS Network Firewall und AWS WAF. Erwägen Sie den Einsatz von AWS Firewall Manager für die zentrale Konfiguration und Verwaltung Ihrer Firewall-Regeln in Ihrer Organisation.

Ressourcen

Zugehörige bewährte Methoden:

- REL03-BP01 Segmentierung Ihres Workloads
- SEC09-BP02 Erzwingen einer Verschlüsselung bei der Übertragung

Zugehörige Dokumente:

- Security best practices for your VPC
- AWS Network Optimization Tips
- Guidance for Network Security on AWS
- Secure your VPC's outbound network traffic in the AWS Cloud

Zugehörige Tools:

- AWS Firewall Manager

Zugehörige Videos:

- AWS Transit Gateway reference architectures for many VPCs
- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield
- AWS re:Inforce 2023: Firewalls and where to put them

SEC05-BP03 Implementieren Sie einen inspektionsbasierten Schutz

Richten Sie Kontrollpunkte für den Datenverkehr zwischen Ihren Netzwerkebenen ein, um sicherzustellen, dass die Daten während der Übertragung den erwarteten Kategorien und Mustern entsprechen. Analysieren Sie Datenverkehrsströme, Metadaten und Muster, um Ereignisse effektiver zu identifizieren, zu erkennen und darauf zu reagieren.

Gewünschtes Ergebnis: Der Datenverkehr, der zwischen Ihren Netzwerkebenen verläuft, wird geprüft und autorisiert. Entscheidungen über das Zulassen oder Verweigern von Zugriffen beruhen auf expliziten Regeln, Informationen über Bedrohungen und Abweichungen vom Grundverhalten. Der Schutz wird strenger, je näher der Datenverkehr an sensible Daten heranrückt.

Typische Anti-Muster:

- Ausschließlich auf Firewall-Regeln vertrauen, die auf Ports und Protokollen basieren, und Vorteile intelligenter Systeme außer Acht lassen
- Firewall-Regeln auf der Grundlage bestimmter aktueller Bedrohungsmuster erstellen, die sich ändern können
- Überprüfung des Datenverkehrs auf den Übergang von privaten zu öffentlichen Subnetzen oder von öffentlichen Subnetzen zum Internet beschränken
- Keine Basisansicht Ihres Netzwerkdatenverkehrs haben, die Sie auf Verhaltensanomalien hin überprüfen können

Vorteile der Nutzung dieser bewährten Methode: Prüfungssysteme ermöglichen es Ihnen, intelligente Regeln zu erstellen, z. B. den Datenverkehr nur dann zuzulassen oder zu verweigern, wenn bestimmte Bedingungen in den Datenverkehrsdaten vorliegen. Profitieren Sie von verwalteten Regelsätzen von AWS und Partnern, die auf den neuesten Bedrohungsinformationen basieren, da sich die Bedrohungslandschaft im Laufe der Zeit ändert. Dadurch verringert sich der Aufwand für die Pflege von Regeln und die Suche nach Indikatoren für eine Gefährdung, wodurch das Potenzial für Fehlalarme reduziert wird.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Verschaffen Sie sich mithilfe anderer Firewalls und Intrusion Prevention-Systeme (IPS) AWS Network Firewall, die Sie hinter einem Gateway Load Balancer () einsetzen können, eine genaue Kontrolle über Ihren AWS Marketplace statusbehafteten und statusfreien Netzwerkverkehr. GWLBAWS

Network Firewall unterstützt Suricata-kompatible Open-Source-Spezifikationen, um Ihre Workloads zu schützen. IPS

AWS Network Firewall Sowohl die Lösungen als auch die von Anbietern, die A verwenden, GWLB unterstützen unterschiedliche Bereitstellungsmodelle für Inline-Inspektionen. Sie können beispielsweise Inspektionen auf VPC Einzelbasis durchführen, sie in Form einer zentralen Inspektion durchführen oder sie in einem Hybridmodell einsetzenVPC, bei dem der Ost-West-Verkehr durch eine Inspektion fließt VPC und der Interneteingang einzeln geprüft wird. VPC Eine weitere Überlegung ist, ob die Lösung das Entpacken von Transport Layer Security (TLS) unterstützt, wodurch eine Deep Packet Inspection für Datenflüsse, die in beide Richtungen initiiert werden, ermöglicht wird. Weitere Informationen und ausführliche Details zu diesen Konfigurationen finden Sie im Leitfaden für AWS Network Firewall Best Practices.

Wenn Sie Lösungen verwenden, die out-of-band Inspektionen durchführen, z. B. die PCAP-Analyse von Paketdaten von Netzwerkschnittstellen, die im Promiscuous-Modus arbeiten, können Sie die Verkehrsspiegelung konfigurieren. VPC Gespiegelter Datenverkehr wird auf die verfügbare Bandbreite Ihrer Schnittstellen angerechnet und unterliegt denselben Datenübertragungsgebühren wie nicht gespiegelter Datenverkehr. Sie können sehen, ob virtuelle Versionen dieser Appliances auf dem verfügbar sind AWS Marketplace, was möglicherweise die Inline-Bereitstellung hinter einem unterstützt. GWLB

Schützen Sie Ihre Anwendung bei Komponenten, die über HTTP basierte Protokolle abgewickelt werden, mit einer Webanwendungs-Firewall (WAF) vor häufigen Bedrohungen. AWS WAFist eine Firewall für Webanwendungen, mit der Sie Anfragen, die Ihren konfigurierbaren Regeln entsprechen, überwachen und blockieren HTTP können, bevor sie an Amazon API Gateway CloudFront, Amazon AWS AppSync oder einen Application Load Balancer gesendet werden. Ziehen Sie Deep Packet Inspection in Betracht, wenn Sie den Einsatz Ihrer Webanwendungs-Firewall evaluieren, da Sie bei einigen Anwendungen den Vorgang TLS vor der Datenverkehrsinspektion beenden müssen. Zu Beginn können Sie AWS WAF es Von AWS verwaltete Regelnin Kombination mit Ihren eigenen Integrationen verwenden oder bestehende Partnerintegrationen verwenden.

Mit können Sie AWS WAF, AWS Shield Advanced AWS Network Firewall, und VPC Amazon-Sicherheitsgruppen in Ihrer gesamten AWS Organisation zentral verwalten AWS Firewall Manager.

Implementierungsschritte

1. Stellen Sie fest, ob Sie die Inspektionsregeln breit fassen könnenVPC, z. B. durch eine Inspektion, oder ob Sie einen detaillierteren VPC Ansatz benötigen.
2. Für Inline-Prüfungslösungen:

   a. Falls Sie diese verwenden AWS Network Firewall, erstellen Sie Regeln, Firewall-Richtlinien und die Firewall selbst. Sobald diese konfiguriert sind, können Sie den Datenverkehr an den Endpunkt der Firewall leiten, um die Prüfung zu aktivieren.

   b. Wenn Sie eine Appliance eines Drittanbieters mit einem Gateway Load Balancer (GWLB) verwenden, stellen Sie Ihre Appliance in einer oder mehreren Availability Zones bereit und konfigurieren Sie sie. Erstellen Sie dann Ihren GWLB Endpunktdienst und konfigurieren Sie das Routing für Ihren Datenverkehr.

3. Für out-of-band Inspektionslösungen:

   1. Aktivieren Sie VPC Traffic Mirroring auf Schnittstellen, an denen eingehender und ausgehender Datenverkehr gespiegelt werden soll. Sie können EventBridge Amazon-Regeln verwenden, um eine AWS Lambda Funktion aufzurufen, mit der die Verkehrsspiegelung auf Schnittstellen aktiviert wird, wenn neue Ressourcen erstellt werden. Richten Sie die Sitzungen zur Datenverkehrsspiegelung auf den Network Load Balancer vor Ihrer Appliance, der den Datenverkehr verarbeitet.

4. Für Lösungen für eingehenden Internetdatenverkehr:

   a. Um zu konfigurieren AWS WAF, konfigurieren Sie zunächst eine Web-Zugriffskontrollliste (WebACL). Das Web ACL ist eine Sammlung von Regeln mit einer seriell verarbeiteten Standardaktion (ALLOWoderDENY), die definiert, wie Sie mit dem Datenverkehr WAF umgehen. Sie können Ihre eigenen Regeln und Gruppen erstellen oder AWS verwaltete Regelgruppen in Ihrem Web ACL verwenden.

   b. Sobald Ihr Web konfiguriert ACL ist, verknüpfen Sie das Web ACL mit einer AWS Ressource (wie einem Application Load Balancer, einem API Gateway oder einer CloudFront Distribution) RESTAPI, um mit dem Schutz des Webverkehrs zu beginnen.

Ressourcen

Zugehörige Dokumente:

- What is Traffic Mirroring?
- Implementing inline traffic inspection using third-party security appliances
- AWS Network Firewall Beispielarchitekturen mit Routing
- Zentralisierte Inspektionsarchitektur mit AWS Gateway Load Balancer und AWS Transit Gateway

Zugehörige Beispiele:

- Best practices for deploying Gateway Load Balancer
- TLSInspektionskonfiguration für verschlüsselten Ausgangsverkehr und AWS Network Firewall

Zugehörige Tools:

- AWS Marketplace IDS/IPS

SEC05-BP04 Automatisieren Sie den Netzwerkschutz

Automatisieren Sie die Implementierung Ihrer Netzwerkschutzmaßnahmen mithilfe von DevOps Methoden wie Infrastructure as Code (IaC) und CI/CD-Pipelines. Diese Praktiken können Ihnen helfen, Änderungen an Ihrem Netzwerkschutz über ein Versionskontrollsystem zu verfolgen, den Zeitaufwand für die Bereitstellung von Änderungen zu reduzieren und zu erkennen, wenn Ihr Netzwerkschutz von der gewünschten Konfiguration abweicht.

Gewünschtes Ergebnis: Sie definieren Netzwerkschutzmaßnahmen mit Vorlagen und übertragen diese in ein Versionskontrollsystem. Automatisierte Pipelines werden initiiert, wenn neue Änderungen vorgenommen werden, die ihre Prüfung und Bereitstellung orchestrieren. Richtlinienprüfungen und andere statische Tests dienen der Validierung von Änderungen vor der Bereitstellung. Sie stellen die Änderungen in einer Staging-Umgebung bereit, um zu überprüfen, ob die Kontrollen wie erwartet funktionieren. Die Bereitstellung in Ihrer Produktionsumgebung erfolgt ebenfalls automatisch, sobald die Kontrollen genehmigt sind.

Typische Anti-Muster:

- Darauf vertrauen, dass die einzelnen Workload-Teams ihren kompletten Netzwerkstack, Schutzmaßnahmen und Automatisierungen selbst definieren Keine zentrale Veröffentlichung von Standardaspekten des Netzwerkstapels und der Schutzmechanismen für Workload-Teams zur Nutzung
- Auf ein zentrales Netzwerkteam vertrauen, das alle Aspekte des Netzwerks, der Schutzmaßnahmen und der Automatisierungen definiert Verzicht auf die Delegation von Workload-spezifischen Aspekten des Netzwerkstacks und der Schutzmaßnahmen an das Team des Workloads
- Beibehalten eines ausgewogenen Verhältnisses zwischen Zentralisierung und Delegation zwischen einem Netzwerkteam und Workload-Teams, aber keine Anwendung konsistenter Test- und Bereitstellungsstandards über Ihre IaC-Vorlagen und CI/CD-Pipelines hinweg Unterlassen der Erfassung erforderlicher Konfigurationen in Tools, die Ihre Vorlagen auf Einhaltung überprüfen

Vorteile der Nutzung dieser bewährten Methode: Durch die Verwendung von Vorlagen zur Definition Ihres Netzwerkschutzes können Sie Änderungen im Laufe der Zeit mit einem Versionskontrollsystem verfolgen und vergleichen. Der Einsatz von Automatisierung zum Testen und Bereitstellen von Änderungen schafft Standardisierung und Vorhersehbarkeit, erhöht die Chancen auf eine erfolgreiche Bereitstellung und reduziert die sich wiederholenden manuellen Konfigurationen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Eine Reihe von Netzwerkschutzmaßnahmen, die in SEC05-BP02 Steuern Sie den Datenfluss innerhalb Ihrer Netzwerkschichten und SEC 05-BP03 Implementieren Sie inspektionsbasierten Schutz beschrieben sind, verfügen über verwaltete Regelsysteme, die automatisch auf der Grundlage der neuesten Bedrohungsinformationen aktualisiert werden können. Beispiele für den Schutz Ihrer Web-Endgeräte sind AWS WAF verwaltete Regeln und automatische Abwehr auf Anwendungsebene.AWS Shield Advanced DDoS Verwenden Sie von AWS Network Firewall verwaltete Regelgruppen, um auch bei Domain-Listen mit geringer Reputation und Bedrohungssignaturen auf dem Laufenden zu bleiben.

Neben verwalteten Regeln empfehlen wir Ihnen, DevOps Methoden zur Automatisierung der Bereitstellung Ihrer Netzwerkressourcen, Schutzmaßnahmen und der von Ihnen festgelegten Regeln zu verwenden. Sie können diese Definitionen in AWS CloudFormation oder einem anderen Infrastructure as Code (IaC)-Tool Ihrer Wahl erfassen, sie an ein Versionskontrollsystem übergeben und sie über CI/CD-Pipelines bereitstellen. Nutzen Sie diesen Ansatz, um die traditionellen Vorteile der DevOps Verwaltung Ihrer Netzwerkkontrollen zu nutzen, z. B. vorhersehbarere Versionen, automatisierte Tests mit Tools wie AWS CloudFormation Guardund die Erkennung von Abweichungen zwischen Ihrer bereitgestellten Umgebung und der gewünschten Konfiguration.

Basierend auf den Entscheidungen, die Sie im Rahmen von SEC05-BP01 Create Network Layers getroffen haben, verfolgen Sie möglicherweise einen zentralen Managementansatz für die Erstellung von NetzwerkschichtenVPCs, die für Eingangs-, Ausgangs- und Inspektionsabläufe vorgesehen sind. Wie in der AWS Sicherheitsreferenzarchitektur (AWS SRA) beschrieben, können Sie diese VPCs in einem speziellen Netzwerkinfrastrukturkonto definieren. Sie können ähnliche Techniken verwenden, um zentral die von Ihren Workloads in anderen Konten VPCs verwendeten Sicherheitsgruppen, AWS Network Firewall Bereitstellungen, Route 53-Resolver-Regeln und DNS Firewall-Konfigurationen sowie andere Netzwerkressourcen zu definieren. Sie können diese Ressourcen mit Ihren anderen Konten mit AWS Resource Access Manager teilen. Mit diesem Ansatz können Sie das automatisierte Testen und die Bereitstellung Ihrer Netzwerkkontrollen für das Netzwerkkonto vereinfachen, da Sie nur ein Ziel verwalten müssen. Sie können dies in einem hybriden Modell tun, bei dem Sie bestimmte

Kontrollen zentral bereitstellen und gemeinsam nutzen und andere Kontrollen an die einzelnen Workload-Teams und ihre jeweiligen Konten delegieren.

Implementierungsschritte

1. Legen Sie fest, welche Aspekte des Netzwerks und des Schutzes zentral definiert werden und welche Ihre Workload-Teams verwalten können.
2. Erstellen Sie Umgebungen zum Testen und Bereitstellen von Änderungen an Ihrem Netzwerk und dessen Schutzmaßnahmen. Verwenden Sie zum Beispiel ein Netzwerk-Testkonto und ein Netzwerk-Produktionskonto.
3. Legen Sie fest, wie Sie Ihre Vorlagen in einem Versionskontrollsystem speichern und pflegen wollen. Speichern Sie zentrale Vorlagen in einem Repository, das sich von den Workload-Repositories unterscheidet, während Workload-Vorlagen in Repositories gespeichert werden können, die speziell für diesen Workload gelten.
4. Erstellen Sie CI/CD-Pipelines zum Testen und Bereitstellen von Vorlagen. Definieren Sie Tests, um zu prüfen, ob Fehlkonfigurationen vorliegen und ob die Vorlagen den Standards Ihres Unternehmens entsprechen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC01-BP06 Automatisieren Sie die Implementierung von Standard-Sicherheitskontrollen

Zugehörige Dokumente:

- AWS Security Reference Architecture - Network account

Zugehörige Beispiele:

- AWS Deployment Pipeline Reference Architecture
- NetDevSecOpszur Modernisierung von Netzwerkinstallationen AWS
- Integration von AWS CloudFormation Sicherheitstests und Berichten AWS Security Hub CSPMAWS CodeBuild

Zugehörige Tools:

- AWS CloudFormation
- AWS CloudFormation Guard
- cfn_nag

Schutz der Datenverarbeitung

Zu den Rechenressourcen gehören u. a. EC2-Instances, Container, AWS-Lambda-Funktionen, Datenbankservices und IoT-Geräte. Jeder dieser Typen von Datenverarbeitungsressourcen erfordert unterschiedliche Ansätze, um sie zu schützen. Sie haben jedoch gemeinsame Strategien, die Sie in Betracht ziehen müssen: tiefgehende Sicherheit, Schwachstellenmanagement, Verringerung der Angriffsfläche, Automatisierung von Konfiguration und Betrieb und Durchführung von Aktionen aus der Ferne. In diesem Abschnitt finden Sie eine allgemeine Anleitung zum Schutz Ihrer Datenverarbeitungsressourcen für wichtige Services. Es ist wichtig, dass Sie für jeden verwendeten AWS-Service die spezifischen Sicherheitsempfehlungen in der Dokumentation des Services überprüfen.

Bewährte Methoden

- SEC06-BP01 Schwachstellenmanagement
- SEC06-BP02 Bereitstellen von Rechenleistung aus gehärteten Images
- SEC06-BP03 Reduzieren der manuellen Verwaltung und des interaktiven Zugriffs
- SEC06-BP04 Softwareintegrität validieren
- SEC06-BP05 Automatisieren des Datenverarbeitungsschutzes

SEC06-BP01 Schwachstellenmanagement

Überprüfen und Patchen Sie Ihren Code, Ihre Abhängigkeiten und Ihre Infrastruktur häufig auf Schwachstellen, um sich vor neuen Bedrohungen zu schützen.

Gewünschtes Ergebnis: Sie verfügen über eine Lösung, die Ihren Workload kontinuierlich auf Software-Schwachstellen, potenzielle Fehler und unbeabsichtigte Netzwerkrisiken überprüft. Sie haben Prozesse und Verfahren eingerichtet, um diese Schwachstellen basierend auf Risikobewertungskriterien zu identifizieren, zu priorisieren und zu beheben. Darüber hinaus haben Sie eine automatisierte Patch-Verwaltung für Ihre Datenverarbeitungs-Instances implementiert. Ihr Programm für das Schwachstellenmanagement ist in Ihren Softwareentwicklungszyklus integriert und bietet Lösungen zum Scannen Ihres Quellcodes in der CI/CD-Pipeline.

Typische Anti-Muster:

- Fehlen eines Programms für das Schwachstellenmanagement
- Durchführung von System-Patches ohne Berücksichtigung des Schweregrads oder der Risikovermeidung
- Verwendung von Software nach dem vom Anbieter angegebenen Lebenszyklusenddatum
- Bereitstellung von Code für die Produktion, bevor dieser auf Sicherheitsprobleme untersucht wurde

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Das Schwachstellenmanagement ist ein wichtiger Aspekt bei der Aufrechterhaltung einer sicheren und robusten Cloud-Umgebung. Es umfasst einen umfassenden Prozess, der Sicherheitsscans, die Identifizierung und Priorisierung von Problemen sowie Patch-Operationen zur Behebung der identifizierten Schwachstellen umfasst. Die Automatisierung spielt in diesem Prozess eine zentrale Rolle, da sie das kontinuierliche Scannen von Workloads auf potenzielle Probleme und unbeabsichtigte Netzwerkrisiken sowie die Durchführung von Abhilfemaßnahmen ermöglicht.

Das AWS-Modell der gemeinsamen Verantwortung ist ein Basiskonzept, das dem Schwachstellenmanagement zugrunde liegt. Gemäß diesem Modell ist AWS für die Sicherung der zugrunde liegenden Infrastruktur verantwortlich, einschließlich Hardware, Software, Netzwerk und der Einrichtungen, in denen AWS-Services ausgeführt werden. Umgekehrt sind Sie für die Sicherung Ihrer Daten, die Sicherheitskonfigurationen und die Verwaltungsaufgaben im Zusammenhang mit Services wie Amazon-EC2-Instances und Amazon-S3-Objekten verantwortlich.

AWS bietet verschiedene Services zur Unterstützung von Programmen für das Schwachstellenmanagement an. Amazon Inspector scannt AWS Workloads kontinuierlich auf Software-Schwachstellen und unbeabsichtigte Netzwerkzugriffe, während AWSSystems Manager Patch Manager die Verwaltung von Patches für Amazon-EC2-Instances unterstützt. Diese Services können mit AWS Security Hub CSPM integriert werden, einem Service für das Management der Cloud-Sicherheit. Dieser Service automatisiert AWS-Sicherheitsprüfungen, zentralisiert Sicherheitswarnungen und stellt eine umfassende Übersicht über die Sicherheitslage einer Organisation bereit. Darüber hinaus verwendet Amazon CodeGuru Security Analysen des statischen Codes, um während der Entwicklungsphase potenzielle Probleme in Java- und Python-Anwendungen zu erkennen.

Durch die Integration von Verfahren für das Schwachstellenmanagement in den Software-Entwicklungszyklus können Sie Schwachstellen proaktiv beseitigen, bevor sie in Produktionsumgebungen eingeführt werden. Dies reduziert das Risiko von Sicherheitsvorfällen und die potenziellen Auswirkungen von Schwachstellen.

Implementierungsschritte

1. Machen Sie sich mit dem Modell der geteilten Verantwortung vertraut: Informieren Sie sich über das AWS-Modell der geteilten Verantwortung, um Ihre Verantwortung für die Sicherung Ihrer Workloads und Daten in der Cloud zu verstehen. AWS ist für die Sicherheit der zugrunde liegenden Cloud-Infrastruktur verantwortlich, während Sie für die Sicherheit Ihrer Anwendungen und Daten sowie der genutzten Services verantwortlich sind.
2. Implementieren Sie Schwachstellenscans: Konfigurieren Sie einen Service für das Scannen von Schwachstellen, z. B. Amazon Inspector, um Ihre Datenverarbeitungs-Instances (z. B. virtuelle Maschinen, Container oder Serverless-Funktionen) automatisch auf Software-Schwachstellen, potenzielle Fehler und unbeabsichtigte Netzwerkrisiken zu scannen.
3. Richten Sie Prozesse für das Schwachstellenmanagement ein: Definieren Sie Prozesse und Verfahren für die Identifizierung, Priorisierung und Behebung von Schwachstellen. Dies kann die Einrichtung von Zeitplänen für das regelmäßige Scannen auf Sicherheitslücken, die Festlegung von Kriterien für die Risikobewertung und die Definition von Zeitplänen für die Behebung basierend auf dem Schweregrad der Schwachstelle umfassen.
4. Richten Sie eine Patch–Verwaltung ein: Verwenden Sie einen Service für die Verwaltung von Patches, um das Patchen Ihrer Datenverarbeitungs-Instances zu automatisieren, sowohl für Betriebssysteme als auch für Anwendungen. Sie können den Service für das Scannen von Instances auf fehlende Patches und das automatische Installieren von Patches nach Zeitplan konfigurieren. Ziehen Sie AWS Systems Manager Patch Manager in Betracht, um diese Funktionalität bereitzustellen.
5. Konfigurieren Sie einen Malware-Schutz: Implementieren Sie Mechanismen für die Erkennung bösartiger Software in Ihrer Umgebung. Sie können beispielsweise Tools wie Amazon GuardDuty verwenden, um EC2- und EBS-Volumes hinsichtlich Malware zu analysieren, Malware zu erkennen und vor Malware zu warnen. GuardDuty kann auch neu zu Amazon S3 hochgeladene Objekte auf potenzielle Malware oder Viren scannen und Maßnahmen ergreifen, um sie vor der Aufnahme in nachgelagerte Prozesse zu isolieren.
6. Integrieren Sie Schwachstellen-Scans in CI/CD-Pipelines: Wenn Sie eine CI/CD-Pipeline für Ihre Anwendungsbereitstellung verwenden, sollten Sie Tools zum Scannen auf Schwachstellen in Ihre

Pipeline integrieren. Tools wie Amazon CodeGuru Security und Open-Source-Optionen können Quellcode, Abhängigkeiten und Artefakte auf potenzielle Sicherheitsprobleme scannen.

7. Konfigurieren Sie einen Service für die Überwachung der Sicherheit: Richten Sie einen Service für die Überwachung der Sicherheit ein, z. B. AWS Security Hub CSPM, um einen umfassenden Überblick über Ihren Sicherheitsstatus über verschiedene Cloud-Services hinweg zu erhalten. Der Service sollte Erkenntnisse zur Sicherheit aus verschiedenen Quellen sammeln und sie in einem standardisierten Format anzeigen, um Priorisierung und Behebung zu vereinfachen.
8. Implementieren Sie Penetrationstests für Webanwendungen: Wenn es sich bei Ihrer Anwendung um eine Webanwendung handelt und Ihre Organisation über die erforderlichen Kompetenzen verfügt oder externe Unterstützung erhalten kann, sollten Sie die Implementierung von Penetrationstests für Webanwendungen in Betracht ziehen, um potenzielle Schwachstellen in Ihrer Anwendung zu identifizieren.
9. Automatisieren Sie mit „Infrastructur as Code“: Verwenden Sie Infrastructure as Code (IAC)-Tools, z. B. AWS CloudFormation, um die Bereitstellung und Konfiguration Ihrer Ressourcen zu automatisieren, einschließlich der zuvor genannten Sicherheitsservices. Dieses Verfahren hilft, eine konsistentere und standardisierte Ressourcenarchitektur für mehrere Konten und Umgebungen zu erstellen.
10. Überwachung und kontinuierliche Verbesserung: Überwachen Sie kontinuierlich die Effektivität Ihres Programms für das Schwachstellenmanagement und verbessern Sie es wie notwendig. Überprüfen Sie die Sicherheitserkenntnisse, bewerten Sie die Effektivität Ihrer Abhilfemaßnahmen und passen Sie Ihre Prozesse und Tools entsprechend an.

Ressourcen

Zugehörige Dokumente:

- AWS Systems Manager
- Security Overview of AWS Lambda
- Amazon CodeGuru
- Improved, Automated Vulnerability Management for Cloud Workloads with a New Amazon Inspector
- Automate vulnerability management and remediation in AWS using Amazon Inspector and AWS Systems Manager – Part 1

Zugehörige Videos:

- Securing Serverless and Container Services
- Security best practices for the Amazon EC2 instance metadata service

SEC06-BP02 Bereitstellen von Rechenleistung aus gehärteten Images

Bieten Sie weniger Möglichkeiten für einen unbeabsichtigten Zugriff auf Ihre Laufzeitumgebungen, indem Sie sie über gehärtete Images bereitstellen. Beziehen Sie Laufzeit-Abhängigkeiten wie Container-Images und Anwendungsbibliotheken nur von vertrauenswürdigen Registern und überprüfen Sie deren Signaturen. Erstellen Sie Ihre eigenen privaten Register, um vertrauenswürdige Images und Bibliotheken für die Verwendung in Ihren Build- und Bereitstellungsprozessen zu speichern.

Gewünschtes Ergebnis: Ihre Datenverarbeitungsressourcen werden über gehärtete Baseline-Images bereitgestellt. Sie rufen externe Abhängigkeiten, wie Container-Images und Anwendungsbibliotheken, nur aus vertrauenswürdigen Registern ab und überprüfen deren Signaturen. Diese werden in privaten Registern gespeichert, auf die Ihre Build- und Bereitstellungsprozesse verweisen können. Sie überprüfen und aktualisieren Images und Abhängigkeiten regelmäßig, um sich vor neu entdeckten Schwachstellen zu schützen.

Typische Anti-Muster:

- Abrufen von Images und Bibliotheken aus vertrauenswürdigen Registern, ohne deren Signaturen zu überprüfen oder Schwachstellen zu scannen, bevor sie eingesetzt werden
- Härtung von Images, ohne sie regelmäßig auf neue Schwachstellen zu testen oder auf die neueste Version zu aktualisieren
- Installation oder Nichtentfernung von Softwarepaketen, die während des erwarteten Lebenszyklus des Images nicht benötigt werden
- Vertrauen auf Patches als einzige Methode, um Datenverarbeitungsressourcen in der Produktion auf dem neuesten Stand zu halten Die alleinige Verwendung von Patches kann immer noch dazu führen, dass Datenverarbeitungsressourcen im Laufe der Zeit von dem gehärteten Standard abweichen. Patches sind außerdem nicht in der Lage, Malware zu entfernen, die möglicherweise von einem Bedrohungsakteur während eines Sicherheitsvorfalls installiert wurde.

Vorteile der Nutzung dieser bewährten Methode: Das Härten von Images trägt dazu bei, die Anzahl der in Ihrer Laufzeitumgebung verfügbaren Pfade zu reduzieren, die unbeabsichtigten Zugriff auf

nicht autorisierte Benutzer oder Services ermöglichen können. Auch das Ausmaß der Auswirkungen eines unbeabsichtigten Zugriffs kann damit verringert werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Um Ihre Systeme abzusichern, sollten Sie mit den neuesten Versionen von Betriebssystemen, Container-Images und Anwendungsbibliotheken beginnen. Wenden Sie Patches auf bekannte Probleme an. Reduzieren Sie das System auf ein Minimum, indem Sie nicht benötigte Anwendungen, Services, Gerätetreiber, Standardbenutzer und andere Anmeldeinformationen entfernen. Ergreifen Sie alle weiteren erforderlichen Maßnahmen, wie z. B. das Deaktivieren von Ports, um eine Umgebung zu schaffen, die nur über die von Ihren Workloads benötigten Ressourcen und Fähigkeiten verfügt. Von dieser Baseline aus können Sie dann Software, Agenten oder andere Prozesse installieren, die Sie für Zwecke wie die Überwachung des Workloads oder die Verwaltung von Schwachstellen benötigen.

Sie können die Belastung durch die Abhärtung von Systemen verringern, indem Sie sich an Anleitungen von vertrauenswürdigen Quellen wie dem Center for Internet Security (CIS) und den Security Technical Implementation Guides () der Defense Information Systems Agency (DISA) halten. STIGs Wir empfehlen Ihnen, mit einem Amazon Machine Image (AMI) zu beginnen, das von AWS oder einem APN Partner veröffentlicht wurde, und den AWS EC2Image Builder zu verwenden, um die Konfiguration gemäß einer geeigneten Kombination von CIS und STIG Kontrollen zu automatisieren.

Zwar sind gehärtete Images und EC2 Image Builder Builder-Rezepte verfügbar, die die CIS DISA STIG Oder-Empfehlungen anwenden, aber Sie stellen möglicherweise fest, dass Ihre Software aufgrund ihrer Konfiguration nicht erfolgreich ausgeführt werden kann. In diesem Fall können Sie von einem nicht gehärteten Basis-Image ausgehen, Ihre Software installieren und dann schrittweise CIS Kontrollen anwenden, um deren Wirkung zu testen. Testen Sie bei allen CIS Kontrollen, die die Ausführung Ihrer Software verhindern, ob Sie stattdessen die detaillierteren Empfehlungen zur Absicherung implementieren können. DISA Behalten Sie den Überblick über die verschiedenen CIS Steuerungen und DISA STIG Konfigurationen, die Sie erfolgreich anwenden können. Verwenden Sie diese, um Ihre Rezepte für die Bildhärtung in EC2 Image Builder entsprechend zu definieren.

Für containerisierte Workloads sind gehärtete Images von Docker im öffentlichen Repository von Amazon Elastic Container Registry () ECR verfügbar. Sie können EC2 Image Builder verwenden, um Container-Images gleichzeitig AMIs zu härten.

Ähnlich wie bei Betriebssystemen und Container-Images können Sie Codepakete (oder Bibliotheken) mithilfe von Tools wie pip, npm, Maven und aus öffentlichen Repositorys abrufen. NuGet Wir

empfehlen Ihnen, Code-Pakete zu verwalten, indem Sie private Repositorys, wie z. B. innerhalb von AWS CodeArtifact, mit vertrauenswürdigen öffentlichen Repositorys verbinden. Diese Integration kann das Abrufen, Speichern und Aufbewahren von Paketen für Sie übernehmen. up-to-date Ihre Anwendungsentwicklungsverfahren können dann die neueste Version dieser Pakete zusammen mit Ihrer Anwendung abrufen und testen. Dabei kommen Techniken wie Software Composition Analysis (SCA), Static Application Security Testing (SAST) und Dynamic Application Security Testing (DAST) zum Einsatz.

Vereinfachen Sie für serverlose Workloads, die verwenden AWS Lambda, die Verwaltung von Paketabhängigkeiten mithilfe von Lambda-Schichten. Verwenden Sie Lambda-Ebenen, um einen Satz von Standardabhängigkeiten, die von verschiedenen Funktionen gemeinsam genutzt werden, in einem eigenständigen Archiv zu konfigurieren. Sie können Ebenen mithilfe eines eigenen Build-Prozesses erstellen und verwalten, sodass Ihre Funktionen auf zentrale Weise erhalten bleiben. up-to-date

Implementierungsschritte

- Härten des Betriebssystems: Verwenden Sie Basis-Images aus vertrauenswürdigen Quellen als Grundlage für den Aufbau Ihres gehärteten SystemsAMIs. Verwenden Sie EC2Image Builder, um die auf Ihren Images installierte Software anzupassen.
- Härten von containerisierten Ressourcen: Konfigurieren Sie containerisierte Ressourcen so, dass sie den bewährten Methoden im Bereich Sicherheit entsprechen. Wenn Sie Container verwenden, implementieren Sie ECRImage Scanning in Ihrer Build-Pipeline und regelmäßig anhand Ihres Image-Repositorys, um CVEs in Ihren Containern danach zu suchen.
- Wenn Sie die serverlose Implementierung mit verwenden AWS Lambda, verwenden Sie Lambda-Schichten, um Anwendungsfunktionscode und gemeinsam genutzte abhängige Bibliotheken zu trennen. Konfigurieren Sie die Codesignierung für Lambda, um sicherzustellen, dass nur vertrauenswürdiger Code in Ihren Lambda-Funktionen ausgeführt wird.

Ressourcen

Zugehörige bewährte Methoden:

- OPS05-BP05 Führen Sie das Patch-Management durch

Zugehörige Videos:

- Tauchen Sie tief in die Sicherheit ein AWS Lambda

Zugehörige Beispiele:

- AMIMit EC2 Image Builder schnell STIG baukonform erstellen
- Building better container images
- Using Lambda layers to simplify your development process
- Entwickeln und implementieren Sie AWS Lambda Ebenen mit dem Serverless Framework
- Aufbau einer end-to-end AWS DevSecOps CI/CD-Pipeline mit Open Source SCA und Tools SAST DAST

SEC06-BP03 Reduzieren der manuellen Verwaltung und des interaktiven Zugriffs

Nutzen Sie Automatisierung für die Bereitstellung, Konfiguration, Wartung und Untersuchung, wo immer dies möglich ist. Erwägen Sie den manuellen Zugriff auf Datenverarbeitungsressourcen in Notfällen oder in sicheren (Sandbox-)Umgebungen, wenn keine Automatisierung möglich ist.

Gewünschtes Ergebnis: Programmatische Skripte und Automatisierungsdokumente (Runbooks) erfassen autorisierte Aktionen in Ihren Datenverarbeitungsressourcen. Diese Runbooks werden entweder automatisch durch Systeme zur Erkennung von Änderungen oder manuell ausgelöst, wenn ein menschliches Urteilsvermögen erforderlich ist. Der direkte Zugriff auf Datenverarbeitungsressourcen wird nur in Notfällen gewährt, wenn keine Automatisierung verfügbar ist. Alle manuellen Aktivitäten werden protokolliert und in einen Überprüfungsprozess einbezogen, um Ihre Automatisierungsmöglichkeiten kontinuierlich zu verbessern.

Typische Anti-Muster:

- Interaktiver Zugriff auf Amazon EC2-Instances mit Protokollen wie SSH oder RDP.
- Verwalten einzelner Benutzeranmeldungen wie `/etc/passwd` oder lokaler Windows-Benutzer.
- Gemeinsame Nutzung eines Passworts oder privaten Schlüssels für den Zugriff auf eine Instance durch mehrere Benutzer.
- Manuelles Installieren von Software und Erstellen oder Aktualisieren von Konfigurationsdateien.
- Manuelles Aktualisieren oder Patchen von Software.
- Einloggen in eine Instance, um Probleme zu beheben.

Vorteile der Nutzung dieser bewährten Methode: Die Durchführung automatisierter Aktionen hilft Ihnen, das betriebliche Risiko unbeabsichtigter Änderungen und Fehlkonfigurationen zu verringern. Durch das Entfernen von Secure Shell (SSH) und Remote Desktop Protocol (RDP) für den interaktiven Zugriff wird der Umfang des Zugriffs auf Ihre Datenverarbeitungsressourcen reduziert. Damit wird ein gängiger Weg für unbefugte Aktionen abgeschnitten. Die Erfassung Ihrer Aufgaben zur Verwaltung von Datenverarbeitungsressourcen in Automatisierungsdokumenten und programmatischen Skripten bietet einen Mechanismus, mit dem Sie den gesamten Umfang der autorisierten Aktivitäten bis ins kleinste Detail definieren und überprüfen können.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Das Protokollieren einer Instance ist eine klassische Methode der Systemverwaltung. Nach der Installation des Server-Betriebssystems würden sich die Benutzer normalerweise manuell anmelden, um das System zu konfigurieren und die gewünschte Software zu installieren. Während der Lebensdauer des Servers melden sich die Benutzer möglicherweise an, um Software-Updates durchzuführen, Patches anzuwenden, Konfigurationen zu ändern und Probleme zu beheben.

Der manuelle Zugriff birgt jedoch eine Reihe von Risiken. Er erfordert einen Server, der auf Anfragen achtet, wie z. B. einen SSH- oder RDP-Service, der einen potenziellen Pfad für unbefugten Zugriff darstellen kann. Außerdem erhöht sich dadurch das Risiko menschlicher Fehler bei der Durchführung manueller Schritte. Diese können zu Störungen des Workloads, zur Beschädigung oder Zerstörung von Daten oder zu anderen Sicherheitsproblemen führen. Der menschliche Zugriff erfordert außerdem Schutzmaßnahmen gegen die Weitergabe von Anmeldeinformationen, was zusätzlichen Verwaltungsaufwand bedeutet.

Um diese Risiken abzuschwächen, können Sie eine agentenbasierte Remotezugriffslösung implementieren, wie z. B. AWS Systems Manager. AWS Systems Manager Systems Manager-Agent (SSM Agent) initiiert einen verschlüsselten Kanal und ist daher nicht darauf angewiesen, auf von außen initiierte Anfragen zu achten. Erwägen Sie, SSM Agent so zu konfigurieren, dass er diesen Kanal über einen VPC-Endpunkt aufbaut.

Systems Manager gibt Ihnen eine fein abgestufte Kontrolle darüber, wie Sie mit Ihren verwalteten Instances interagieren können. Sie legen fest, welche Automatisierungen ausgeführt werden sollen, wer sie ausführen darf und wann sie ausgeführt werden können. Systems Manager ist in der Lage, Patches anzuwenden, Software zu installieren und Konfigurationsänderungen ohne interaktiven Zugriff auf die Instance vorzunehmen. Systems Manager kann außerdem den Zugriff auf eine entfernte Shell ermöglichen und jeden während der Sitzung aufgerufenen Befehl und seine Ausgabe

in Protokollen und Amazon S3 protokollieren. AWS CloudTrail zeichnet Aufrufe von Systems Manager-APIs zur Überprüfung auf.

Implementierungsschritte

1. Installieren Sie AWS Systems Manager Agent (SSM Agent) auf Ihren Amazon EC2-Instances. Prüfen Sie, ob der SSM-Agent als Teil Ihrer AMI-Basiskonfiguration enthalten ist und automatisch gestartet wird.
2. Überprüfen Sie, ob die IAM-Rollen, die mit Ihren EC2-Instance-Profilen verbunden sind, die verwaltete IAM-Richtlinie `AmazonSSMManagedInstanceCore` enthalten.
3. Deaktivieren Sie SSH, RDP und andere Remotezugriffsservices, die auf Ihren Instances ausgeführt werden. Sie können dies tun, indem Sie Skripte ausführen, die im Abschnitt Benutzerdaten Ihrer Startvorlagen konfiguriert sind, oder indem Sie mit Tools wie EC2 Image Builder angepasste AMIs erstellen.
4. Vergewissern Sie sich, dass die für Ihre EC2-Instances geltenden Ingress-Regeln der Sicherheitsgruppe keinen Zugriff auf Port 22/tcp (SSH) oder Port 3389/tcp (RDP) zulassen. Implementieren Sie die Erkennung und Alarmierung bei falsch konfigurierten Sicherheitsgruppen mit Services wie AWS Config.
5. Definieren Sie entsprechende Automatisierungen, Runbooks und Run Commands in Systems Manager. Verwenden Sie IAM-Richtlinien, um festzulegen, wer diese Aktionen durchführen darf und unter welchen Bedingungen sie erlaubt sind. Testen Sie diese Automatisierungen gründlich in einer nicht produktiven Umgebung. Rufen Sie diese Automatisierungen bei Bedarf auf, anstatt interaktiv auf die Instance zuzugreifen.
6. Verwenden Sie AWS Systems Manager Session Manager, um bei Bedarf interaktiven Zugriff auf Instances zu ermöglichen. Aktivieren Sie die Protokollierung der Sitzungsaktivitäten, um einen Audit Trail zu erstellen, in Amazon CloudWatch Logs oder Amazon S3.

Ressourcen

Zugehörige bewährte Methoden:

- REL08-BP04 Bereitstellung mit einer unveränderlichen Infrastruktur

Zugehörige Beispiele:

- Replacing SSH access to reduce management and security overhead with AWS Systems Manager

Zugehörige Tools:

- AWS Systems Manager

Zugehörige Videos:

- Controlling User Session Access to Instances in AWS Systems Manager Session Manager

SEC06-BP04 Softwareintegrität validieren

Verwenden Sie die kryptografische Überprüfung, um die Integrität von Software-Artefakten (einschließlich Images) zu überprüfen, die Ihr Workload verwendet. Signieren Sie Ihre Software kryptografisch, um sie vor unbefugten Änderungen in Ihren Computerumgebungen zu schützen.

Gewünschtes Ergebnis: Alle Artefakte werden aus vertrauenswürdigen Quellen bezogen. Die Zertifikate der Website des Anbieters sind validiert. Heruntergeladene Artefakte werden anhand ihrer Signaturen kryptographisch verifiziert. Ihre eigene Software ist kryptografisch signiert und wird von Ihren Computerumgebungen überprüft.

Typische Anti-Muster:

- Vertrauen auf die Websites seriöser Anbieter, um Software-Artefakte zu erhalten, aber Hinweise zum Ablauf von Zertifikaten ignorieren Fortfahren mit dem Herunterladen, ohne zu bestätigen, dass die Zertifikate gültig sind
- Validieren der Zertifikate von Anbieter-Websites, aber keine kryptografische Überprüfung der heruntergeladenen Artefakte von diesen Websites
- Prüfen der Integrität von Software ausschließlich anhand von Digests oder Hashes Hashes stellen sicher, dass Artefakte gegenüber der ursprünglichen Version nicht verändert wurden, aber sie bestätigen nicht ihre Quelle.
- Nicht signieren Ihrer eigene Software, Ihres eigenen Codes oder Ihrer eigenen Bibliotheken, selbst wenn Sie sie nur in Ihren eigenen Bereitstellungen verwenden.

Vorteile der Nutzung dieser bewährten Methode: Die Überprüfung der Integrität von Artefakten, von denen Ihr Workload abhängt, hilft zu verhindern, dass Malware in Ihre Computerumgebungen eindringt. Das Signieren Ihrer Software schützt Sie davor, dass sie von Unbefugten in Ihrer Computerumgebung ausgeführt wird. Sichern Sie Ihre Softwarelieferkette durch Signieren und Verifizieren von Code.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Betriebssystem-Images, Container-Images und Code-Artefakte werden oft mit verfügbaren Integritätsprüfungen verteilt, z. B. durch einen Digest oder Hash. Diese ermöglichen es den Clients, die Integrität zu überprüfen, indem sie ihren eigenen Hash der Nutzdaten berechnen und überprüfen, ob er mit dem veröffentlichten Hash übereinstimmt. Diese Überprüfungen helfen zwar dabei, sicherzustellen, dass die Nutzdaten nicht manipuliert wurden, aber sie bestätigen nicht, dass die Nutzdaten von der ursprünglichen Quelle (ihrer Herkunft) stammen. Zur Überprüfung der Herkunft ist ein Zertifikat erforderlich, das eine vertrauenswürdige Stelle ausstellt, um das Artefakt digital zu signieren.

Wenn Sie in Ihrem Workload eine heruntergeladene Software oder Artefakte verwenden, prüfen Sie, ob der Anbieter einen öffentlichen Schlüssel für die Überprüfung der digitalen Signatur bereitstellt. Hier sind einige Beispiele dafür, wie AWS einen öffentlichen Schlüssel und Verifizierungsanweisungen für die von uns veröffentlichte Software bereitstellt:

- EC2Image Builder: Überprüfen Sie die Signatur des AWS TOE Installationsdownloads
- AWS Systems Manager: Überprüfung der Signatur des Agenten SSM
- Amazon CloudWatch: Überprüfung der Signatur des CloudWatch Agentenpakets

Integrieren Sie die Überprüfung digitaler Signaturen in die Prozesse, die Sie zum Abrufen und Härten von Images verwenden, wie unter SEC06-BP02 Bereitstellung von Rechenleistung aus gehärteten Images beschrieben.

Sie können AWS Signer verwenden, um die Überprüfung von Signaturen sowie Ihren eigenen Lebenszyklus der Codesignatur für Ihre eigene Software und Artefakte zu verwalten. Sowohl AWS Lambda als auch Amazon Elastic Container Registry bieten Integrationen mit Signer, um die Signaturen Ihres Codes und Ihrer Images zu überprüfen. Mit den Beispielen im Abschnitt Ressourcen können Sie Signer in Ihre Continuous Integration und Delivery (CI/CD) Pipelines einbinden, um die Überprüfung von Signaturen und die Signierung Ihres eigenen Codes und Ihrer Images zu automatisieren.

Ressourcen

Zugehörige Dokumente:

- Cryptographic Signing for Containers

- Bewährte Methoden zur Sicherung Ihrer Pipeline für die Erstellung von Container-Images mithilfe von AWS Signer
- Ankündigung von Container Image Signing with AWS Signer und Amazon EKS
- Codesignatur konfigurieren für AWS Lambda
- Best practices and advanced patterns for Lambda code signing
- Codesignatur mit AWS Certificate Manager privater CA und AWS Key Management Service asymmetrischen Schlüsseln

Zugehörige Beispiele:

- Automatisieren Sie die Lambda-Code-Signierung mit Amazon CodeCatalyst und AWS Signer
- Signieren und Validieren von OCI Artefakten mit AWS Signer

Zugehörige Tools:

- AWS Lambda
- AWS Signer
- AWS Certificate Manager
- AWS Key Management Service
- AWS CodeArtifact

SEC06-BP05 Automatisieren des Datenverarbeitungsschutzes

Automatisieren Sie den Datenverarbeitungsschutz, um das Erfordernis menschlichen Eingreifens zu reduzieren. Nutzen Sie automatisierte Scans, um potenzielle Probleme in Ihren Datenverarbeitungsressourcen zu erkennen und mit automatisierten programmatischen Reaktionen oder Flottenmanagement-Vorgängen zu beheben. Integrieren Sie die Automatisierung in Ihre CI/CD-Prozesse, um vertrauenswürdige Workloads mit aktuellen Abhängigkeiten bereitzustellen.

Gewünschtes Ergebnis: Automatisierte Systeme führen alle Scans und Patches von Datenverarbeitungsressourcen durch. Sie verwenden die automatische Überprüfung, um sicherzustellen, dass Software-Images und Abhängigkeiten aus vertrauenswürdigen Quellen stammen und nicht manipuliert wurden. Workloads werden automatisch auf aktuelle Abhängigkeiten geprüft und signiert, um die Vertrauenswürdigkeit in AWS-Datenverabeitungsumgebungen zu

gewährleisten. Automatisierte Abhilfemaßnahmen werden eingeleitet, wenn nicht konforme Ressourcen entdeckt werden.

Typische Anti-Muster:

- Verfolgen des Ansatzes einer unveränderlichen Infrastruktur, aber ohne eine Lösung für Notfall-Patches oder den Austausch von Produktionssystemen
- Verwenden von Automatisierung, um falsch konfigurierte Ressourcen zu korrigieren, ohne dass ein manueller Überschreibungsmechanismus vorhanden ist Es können Situationen entstehen, in denen Sie die Anforderungen anpassen müssen, und es kann sein, dass Sie die Automatisierungen aussetzen müssen, bis Sie diese Änderungen vorgenommen haben.

Vorteile der Nutzung dieser bewährten Methode: Die Automatisierung kann das Risiko des unbefugten Zugriffs und der Nutzung Ihrer Datenverarbeitungsressourcen verringern. Sie hilft zu verhindern, dass Fehlkonfigurationen in Produktionsumgebungen gelangen, und Fehlkonfigurationen zu erkennen und zu beheben, wenn sie auftreten. Die Automatisierung hilft auch bei der Erkennung von unbefugtem Zugriff und der Nutzung von Datenverarbeitungsressourcen, um Ihre Reaktionszeit zu verkürzen. Dies wiederum kann den Gesamtumfang der Auswirkungen des Problems verringern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Sie können die in den Methoden der Sicherheitssäule beschriebenen Automatisierungen zum Schutz Ihrer Datenverarbeitungsressourcen anwenden. In SEC06-BP01 Schwachstellenmanagement wird beschrieben, wie Sie Amazon Inspector sowohl in Ihren CI/CD-Pipelines als auch für die kontinuierliche Überprüfung Ihrer Laufzeitumgebungen auf bekannte CVEs (Common Vulnerabilities and Exposures) einsetzen können. Sie können AWSSystems Manager verwenden, um Patches anzuwenden oder neue Images über automatisierte Runbooks bereitzustellen, damit Ihre Computerflotte stets mit der neuesten Software und den neuesten Bibliotheken ausgestattet ist. Nutzen Sie diese Techniken, um den Bedarf an manuellen Prozessen und interaktivem Zugriff auf Ihre Datenverarbeitungsressourcen zu reduzieren. Weitere Informationen finden Sie unter Reduzieren der manuellen Verwaltung und des interaktiven Zugriffs.

Die Automatisierung spielt auch eine Rolle bei der Bereitstellung von Workloads, die vertrauenswürdig sind. Dies wird in SEC06-BP02 Bereitstellen von Datenverarbeitung über gehärtete Images und SEC06-BP04 Validieren der Softwareintegrität beschrieben. Sie können Services wie EC2 Image Builder, AWS Signer, AWS CodeArtifact und Amazon Elastic Container Registry (ECR)

verwenden, um gehärtete und genehmigte Images und Code-Abhängigkeiten herunterzuladen, zu überprüfen, zu erstellen und zu speichern. Neben Inspector kann jeder von ihnen eine Rolle in Ihrem CI/CD-Prozess spielen, sodass Ihr Workload nur dann in die Produktion geht, wenn sichergestellt ist, dass seine Abhängigkeiten aktuell sind und aus vertrauenswürdigen Quellen stammen. IIhr Workload ist außerdem signiert, damit AWS-Datenverarbeitungsumgebungen wie AWS Lambda und Amazon Elastic Kubernetes Service (EKS) überprüfen können, dass er nicht manipuliert wurde, bevor sie ihn ausführen.

Über diese präventiven Kontrollen hinaus können Sie die Automatisierung auch bei den detektivischen Kontrollen für Ihre Datenverarbeitungsressourcen einsetzen. Ein Beispiel: AWS Security Hub CSPM bietet den Standard NIST 800-53 Rev. 5, der Prüfungen wie [EC2.8] EC2 instances should use Instance Metadata Service Version 2 (IMDSv2) enthält. IMDSv2 verwendet die Techniken der Sitzungsauthentifizierung, des Blockierens von Anfragen, die einen X-Forwarded-For HTTP-Header enthalten, und eine Netzwerk-TTL von 1, um den von externen Quellen stammenden Datenverkehr zum Abrufen von Informationen über die EC2-Instance zu stoppen. Diese Prüfung in Security Hub CSPM kann erkennen, wenn EC2 Instances IMDSv1 verwenden und eine automatische Abhilfe einleiten. Weitere Informationen zur automatisierten Erkennung und zu Abhilfemaßnahmen finden Sie unter SEC04-BP04 Initiieren von Abhilfemaßnahmen für nicht konforme Ressourcen.

Implementierungsschritte

1. Automatisieren Sie die Erstellung sicherer, konformer und gehärteter AMIs mit EC2 Image Builder. Sie können Images erstellen, die Kontrollen aus den Center for Internet Security (CIS)-Benchmarks oder Security Technical Implementation Guide (STIG)-Standards aus Basis- AWS und APN-Partner-Images enthalten.
2. Automatische Konfigurationsverwaltung. Erzwingen und validieren Sie sichere Konfigurationen in Ihren Datenverarbeitungsressourcen automatisch. Verwenden Sie dazu einen Service oder ein Tool zur Konfigurationsverwaltung.
   a. Automatisiertes Konfigurationsmanagement mit AWS Config
   b. Automatisiertes Sicherheits- und Compliance-Management mit AWS Security Hub CSPM
3. Automatisieren Sie das Patchen oder Ersetzen von Amazon Elastic Compute Cloud (Amazon EC2)-Instances. AWS Systems Manager Patch Manager automatisiert das Patchen verwalteter Instances mit sicherheitsrelevanten und anderen Arten von Updates. Sie können Patchmanager verwenden, um Patches sowohl für Betriebssysteme als auch für Anwendungen durchzuführen.
   a. AWS Systems Manager Patch Manager
4. Automatisieren Sie das Scannen von Datenverarbeitungsressourcen auf häufige Schwachstellen und Gefährdungen (CVEs) und betten Sie Sicherheitsscan-Lösungen in Ihre Build-Pipeline ein.

   a. Amazon Inspector
   b. ECR Image Scanning
5. Ziehen Sie Amazon GuardDuty für die automatische Erkennung von Malware und Bedrohungen in Betracht, um Datenverarbeitungsressourcen zu schützen. GuardDuty kann außerdem mögliche Probleme identifizieren, wenn eine AWS Lambda-Funktion in Ihrer AWS-Umgebung aufgerufen wird.
   a. Amazon GuardDuty
6. Ziehen Sie AWS-Partnerlösungen in Betracht. AWS -Partner bieten branchenführende Produkte an, die mit vorhandenen Kontrollen in Ihren On-Premises-Umgebungen gleichwertig oder identisch sind oder sich in diese integrieren lassen. Diese Produkte ergänzen die vorhandenen AWS-Services, sodass Sie eine umfassende Sicherheitsarchitektur bereitstellen und eine nahtlosere Erfahrung in Ihren Cloud- und On-Premises-Umgebungen ermöglichen können.
   a. Sicherheit der Infrastruktur

Ressourcen

Zugehörige bewährte Methoden:

- SEC01-BP06 Automatisieren der Bereitstellung von Standard-Sicherheitskontrollen

Zugehörige Dokumente:

- Get the full benefits of IMDSv2 and disable IMDSv1 across your AWS infrastructure

Zugehörige Videos:

- Security best practices for the Amazon EC2 instance metadata service

Datenschutz

Vor der Strukturierung von Workloads sollten grundlegende Sicherheitspraktiken implementiert werden. Mittels Datenklassifizierung lassen sich beispielsweise Daten nach Sensitivität kategorisieren. Die Verschlüsselung macht sie zudem für unbefugte Benutzer unleserlich. Derartige Methoden sind wichtig, um den Missbrauch von Daten zu verhindern oder die gesetzlichen Vorgaben zu erfüllen.

In AWS sind hinsichtlich des Datenschutzes eine Reihe unterschiedlicher Ansätze zu erwägen. Im nächsten Abschnitt werden folgende Ansätze erläutert.

Themen

Datenklassifizierung

Die Datenklassifizierung bietet eine Möglichkeit, Organisationsdaten basierend auf Wichtigkeit und Sensibilität zu kategorisieren, um Ihnen dabei zu helfen, angemessene Schutz- und Aufbewahrungskontrollen zu bestimmen.

Bewährte Methoden

SEC07-BP01 Verstehen Ihres Schemas zur Datenklassifizierung

Machen Sie sich ein Bild von der Klassifizierung der Daten, die Ihr Workload verarbeitet, den Anforderungen an die Verarbeitung, den damit verbundenen Geschäftsprozessen, dem Ort, an dem die Daten gespeichert sind, sowie dem Eigentümer der Daten. Ihr Schema für die Klassifizierung und den Umgang mit Daten sollte die geltenden rechtlichen und Compliance-Anforderungen Ihres

Workloads und die erforderlichen Datenkontrollen berücksichtigen. Das Verständnis der Daten ist der erste Schritt zur Datenklassifizierung.

Gewünschtes Ergebnis: Die in Ihrem Workload vorhandenen Datentypen sind gut verstanden und dokumentiert. Es gibt angemessene Kontrollen zum Schutz sensibler Daten auf der Grundlage ihrer Klassifizierung. Diese Kontrollen regeln z. B., wer auf die Daten zugreifen darf und zu welchem Zweck, wo die Daten gespeichert werden, die Verschlüsselungsrichtlinie für diese Daten und wie Verschlüsselungsschlüssel verwaltet werden, den Lebenszyklus der Daten und die Anforderungen an die Aufbewahrung, angemessene Vernichtungsprozesse, welche Sicherungs- und Wiederherstellungsprozesse vorhanden sind und die Überprüfung des Zugriffs.

Typische Anti-Muster:

- Fehlen einer formalen Richtlinie zur Datenklassifizierung, um die Sensibilitätsebenen und die Anforderungen an die Handhabung von Daten zu definieren
- Mangel an Wissen über die Sensibilitätsebenen der Daten innerhalb Ihres Workloads und fehlende Erfassung dieser Informationen in der Architektur- und Betriebsdokumentation
- Versäumnis, angemessene Kontrollen für Ihre Daten anzuwenden, die auf deren Sensibilität und Anforderungen basieren, wie in Ihrer Richtlinie zur Datenklassifizierung und -verarbeitung festgelegt
- Unterlassen von Feedback über die Anforderungen an die Datenklassifizierung und -verarbeitung an die Eigentümer der Richtlinien

Vorteile der Nutzung dieser bewährten Methode: Diese Vorgehensweise beseitigt Unklarheiten über den angemessenen Umgang mit Daten innerhalb Ihres Workloads. Die Anwendung einer formellen Richtlinie, die die Sensibilitätsebenen der Daten in Ihrer Organisation und die erforderlichen Schutzmaßnahmen definiert, kann Ihnen helfen, gesetzliche Vorschriften und andere Bescheinigungen und Zertifizierungen im Bereich der Cybersicherheit einzuhalten. Besitzer von Workloads können sich darauf verlassen, dass sie wissen, wo sensible Daten gespeichert sind und welche Schutzkontrollen vorhanden sind. Wenn Sie diese in der Dokumentation festhalten, können neue Team-Mitglieder sie besser verstehen und schon früh in ihrer Amtszeit Kontrollen durchführen. Diese Praktiken können auch dazu beitragen, die Kosten zu senken, indem die Kontrollen für jede Art von Daten richtig dimensioniert werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Wenn Sie einen Workload entwerfen, überlegen Sie vielleicht intuitiv, wie Sie sensible Daten schützen können. Bei einer mandantenfähigen Anwendung ist es beispielsweise intuitiv, die Daten jedes Mandanten als sensibel zu betrachten und Schutzmaßnahmen zu ergreifen, damit ein Mandant nicht auf die Daten eines anderen Mandanten zugreifen kann. Ebenso können Sie intuitiv Zugriffskontrollen so gestalten, dass nur Administratoren Daten ändern können, während andere Benutzer nur Lesezugriff oder gar keinen Zugriff haben.

Indem Sie diese Datensensibilitätsebenen zusammen mit den entsprechenden Datenschutzanforderungen definieren und in Richtlinien festhalten, können Sie formell feststellen, welche Daten sich in Ihrem Workload befinden. Sie können dann feststellen, ob die richtigen Kontrollen vorhanden sind, ob die Kontrollen überprüft werden können und welche Reaktionen angemessen sind, wenn ein falscher Umgang mit Daten festgestellt wird.

Um die Stellen in Ihrem Workload zu identifizieren, an denen sich sensible Daten befinden, sollten Sie die Verwendung eines Datenkatalogs in Betracht ziehen. Ein Datenkatalog ist eine Datenbank, die Daten in Ihrer Organisation, ihren Standort, ihre Vertraulichkeitsstufe und die zum Schutz dieser Daten eingeführten Kontrollen abbildet. Sie sollten außerdem die Verwendung von Ressourcen-Tags in Betracht ziehen, wenn verfügbar. Sie können zum Beispiel ein Tag mit dem Tag-Schlüssel `Classification` und dem Tag-Wert `PHI` für geschützte Gesundheitsinformationen (Protected Health Information, PHI) und ein weiteres Tag mit dem Tag-Schlüssel `Sensitivity` und dem Tag-Wert `High` verwenden. Mit Services wie AWS Config können Sie diese Ressourcen auf Änderungen überwachen und eine Warnung ausgeben, wenn sie so verändert werden, dass sie Ihren Schutzanforderungen nicht mehr genügen (z. B. durch Änderung der Verschlüsselungseinstellungen). Sie können die Standarddefinition Ihrer Tag-Schlüssel und zulässigen Werte mit Tag-Richtlinien, einem Feature von AWS Organizations, erfassen. Es wird nicht empfohlen, dass der Tag-Schlüssel oder -Wert private oder sensible Daten enthält.

Implementierungsschritte

1. Verstehen Sie das Datenklassifizierungsschema und die Schutzanforderungen Ihrer Organisation.
2. Identifizieren Sie die Arten von sensiblen Daten, die von Ihren Workloads verarbeitet werden.
3. Erfassen Sie die Daten in einem Datenkatalog, der einen zentralen Überblick über die Stellen, an denen sich Daten in der Organisation befinden, und ihre Vertraulichkeit bietet.
4. Erwägen Sie die Verwendung von Markierungen auf Ressourcen- und Datenebene, sofern verfügbar, um Daten mit ihrer Sensibilitätsstufe und anderen operativen Metadaten zu versehen, die bei der Überwachung und der Reaktion auf Vorfälle helfen können.

a. AWS Organizations-Tag-Richtlinien können verwendet werden, um Tagging-Standards durchzusetzen.

Ressourcen

Zugehörige bewährte Methoden:

- SUS04-BP01 Implementieren einer Richtlinie für die Klassifizierung von Daten

Zugehörige Dokumente:

- Data Classification Whitepaper
- Best Practices for Tagging AWS Resources

Zugehörige Beispiele:

- AWS Organizations Tag Policy Syntax and Examples

Zugehörige Tools:

- AWS Tag-Editor

SEC07-BP02 Anwenden von Datenschutzkontrollen basierend auf der Sensibilität der Daten

Wenden Sie Datenschutzkontrollen an, die ein angemessenes Maß an Kontrolle für jede in Ihrer Klassifizierungsrichtlinie definierte Datenklasse bieten. Auf diese Weise können Sie sensible Daten vor unbefugtem Zugriff und unbefugter Nutzung schützen und gleichzeitig die Verfügbarkeit und Nutzung der Daten aufrechterhalten.

Gewünschtes Ergebnis: Sie verfügen über eine Klassifizierungsrichtlinie, die die verschiedenen Sensibilitätsstufen für Daten in Ihrer Organisation definiert. Für jede dieser Sensibilitätsebenen haben Sie klare Richtlinien für zugelassene Speicher- und Bearbeitungsservices und -orte sowie deren erforderliche Konfiguration veröffentlicht. Sie implementieren die Kontrollen für jede Ebene entsprechend dem erforderlichen Schutzniveau und den damit verbundenen Kosten. Sie verfügen über Überwachungs- und Warnsysteme, um zu erkennen, wenn sich Daten an nicht autorisierten

Orten befinden, in nicht autorisierten Umgebungen verarbeitet werden, nicht autorisierte Akteure darauf zugreifen oder die Konfiguration der zugehörigen Services nicht mehr konform ist.

Typische Anti-Muster:

- Anwenden des gleichen Maßes an Schutzkontrollen für alle Daten: Dies kann dazu führen, dass zu viele Sicherheitskontrollen für wenig sensible Daten bereitgestellt werden oder hochsensible Daten nicht ausreichend geschützt werden.
- Unterlassen, die relevanten Stakeholder aus Sicherheits-, Compliance- und Geschäftsteams bei der Definition von Datenschutzkontrollen einzubeziehen
- Vernachlässigen des betrieblichen Aufwands und der Kosten, die mit der Implementierung und Pflege von Datenschutzkontrollen verbunden sind
- Fehlen von regelmäßigen Überprüfungen der Datenschutzkontrollen, um die Übereinstimmung mit den Klassifizierungsrichtlinien zu gewährleisten
- Fehlen einer vollständigen Übersicht über die Speicherorte von Daten im Ruhezustand und während der Übertragung.

Vorteile der Nutzung dieser bewährten Methode: Indem Sie Ihre Kontrollen auf die Klassifizierungsstufe Ihrer Daten abstimmen, kann Ihre Organisation bei Bedarf in höhere Kontrollstufen investieren. Dies kann eine Aufstockung der Ressourcen für die Sicherung, Überwachung, Messung, Behebung und Berichterstattung beinhalten. Wo weniger Kontrollen angebracht sind, können Sie die Zugänglichkeit und Vollständigkeit der Daten für Ihre Mitarbeiter, Kunden oder Wähler verbessern. Dieser Ansatz bietet Ihrer Organisation die größtmögliche Flexibilität bei der Datennutzung, während gleichzeitig die Datenschutzanforderungen eingehalten werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Die Implementierung von Datenschutzkontrollen auf der Grundlage von Datensensibilitätsebenen umfasst mehrere wichtige Schritte. Ermitteln Sie zunächst die verschiedenen Datensensibilitätsebenen innerhalb Ihrer Workload-Architektur (z. B. öffentlich, intern, vertraulich und eingeschränkt) und bewerten Sie, wo Sie diese Daten speichern und verarbeiten. Als Nächstes definieren Sie Isolationsgrenzen um die Daten herum, basierend auf ihrer Sensibilitätsebene. Wir empfehlen Ihnen, Daten in verschiedene AWS-Konten-Konten zu unterteilen und Service-Kontrollrichtlinien (SCPs) zu verwenden, um die für die einzelnen Sensibilitätsebenen zulässigen

Services und Aktionen einzuschränken. Auf diese Weise können Sie starke Isolationsgrenzen schaffen und das Prinzip der geringsten Berechtigung durchsetzen.

Nachdem Sie die Isolationsgrenzen definiert haben, implementieren Sie geeignete Schutzkontrollen auf der Grundlage der Sensibilitätsebenen der Daten. Beachten Sie die bewährten Methoden zum Schutz von Daten im Ruhezustand und zum Schutz von Daten während der Übertragung, um entsprechende Kontrollen wie Verschlüsselung, Zugriffskontrollen und Audits zu implementieren. Ziehen Sie Techniken wie Tokenisierung oder Anonymisierung in Betracht, um die Sensibilität Ihrer Daten zu verringern. Vereinfachen Sie die Anwendung konsistenter Datenrichtlinien in Ihrem Unternehmen mit einem zentralisierten System für Tokenisierung und De-Tokenisierung.

Überwachen und testen Sie fortlaufend die Wirksamkeit der implementierten Kontrollen. Überprüfen und aktualisieren Sie das Datenklassifizierungsschema, die Risikobewertungen und die Schutzkontrollen regelmäßig, wenn sich die Datenlandschaft und die Bedrohungen in Ihrer Organisation weiterentwickeln. Richten Sie die implementierten Datenschutzkontrollen an den einschlägigen Branchenvorschriften, Standards und gesetzlichen Anforderungen aus. Sorgen Sie außerdem für ein Sicherheitsbewusstsein und bieten Sie Schulungen an, damit die Mitarbeiter das Datenklassifizierungsschema und ihre Verantwortung im Umgang mit sensiblen Daten und deren Schutz verstehen.

Implementierungsschritte

1. Identifizieren Sie die Klassifizierungs- und Sensibilitätsstufen der Daten innerhalb Ihres Workloads.
2. Definieren Sie Isolationsgrenzen für jede Ebene und legen Sie eine Durchsetzungsstrategie fest.
3. Bewerten Sie die von Ihnen definierten Kontrollen, die den Zugriff, die Verschlüsselung, die Prüfung, die Aufbewahrung und andere von Ihrer Datenklassifizierungsrichtlinie geforderte Punkte regeln.
4. Prüfen Sie gegebenenfalls Optionen zur Verringerung der Sensibilität der Daten, z. B. durch Tokenisierung oder Anonymisierung.
5. Überprüfen Sie Ihre Kontrollen durch automatische Tests und die Überwachung Ihrer konfigurierten Ressourcen.

Ressourcen

Zugehörige bewährte Methoden:

- PERF03-BP01 Verwenden eines speziell entwickelten Datenspeichers, der die Datenzugriffs- und Speicheranforderungen am besten unterstützt

- COST04-BP05 Durchsetzen von Richtlinien zur Datenaufbewahrung

Zugehörige Dokumente:

- Data Classification Whitepaper
- Bewährte Methoden für Sicherheit, Identität und Compliance
- AWS KMS Best Practices
- Encryption best practices and features for AWS services

Zugehörige Beispiele:

- Building a serverless tokenization solution to mask sensitive data
- How to use tokenization to improve data security and reduce audit scope

Zugehörige Tools:

- AWS Key Management Service (AWS KMS)
- AWS CloudHSM
- AWS Organizations

SEC07-BP03 Automatisieren der Identifizierung und Klassifizierung

Durch die Automatisierung der Identifizierung und Klassifizierung von Daten können Sie die richtigen Kontrollen implementieren. Der Einsatz von Automatisierung als Ergänzung zur manuellen Ermittlung verringert das Risiko menschlicher Fehler und das Risiko einer Gefährdung.

Gewünschtes Ergebnis: Sie sind in der Lage zu überprüfen, ob die richtigen Kontrollen auf der Grundlage Ihrer Klassifizierungs- und Bearbeitungsrichtlinien vorhanden sind. Automatisierte Tools und Services helfen Ihnen bei der Identifizierung und Klassifizierung der Sensibilitätsebene Ihrer Daten. Die Automatisierung hilft Ihnen auch bei der kontinuierlichen Überwachung Ihrer Umgebungen, um zu erkennen und zu melden, wenn Daten auf unzulässige Weise gespeichert oder verarbeitet werden, sodass schnell Abhilfemaßnahmen ergriffen werden können.

Typische Anti-Muster:

- Vertrauen auf ausschließlich manuelle Prozesse, die fehleranfällig und zeitaufwendig sein können, um Daten zu identifizieren und zu klassifizieren Dies kann zu einer ineffizienten und inkonsistenten Datenklassifizierung führen, insbesondere wenn das Datenvolumen wächst.
- Fehlen von Mechanismen zur Verfolgung und Verwaltung von Datenbeständen in der gesamten Organisation
- Vernachlässigen der Notwendigkeit einer kontinuierlichen Überwachung und Klassifizierung von Daten, während sie sich innerhalb der Organisation bewegen und weiterentwickeln

Vorteile der Nutzung dieser bewährten Methode: Die Automatisierung der Identifizierung und Klassifizierung von Daten kann zu einer konsistenteren und präziseren Anwendung von Datenschutzkontrollen führen und das Risiko menschlicher Fehler verringern. Die Automatisierung kann auch den Zugriff auf und die Bewegung von sensiblen Daten transparent machen, sodass Sie unautorisierten Umgang mit diesen Daten erkennen und Korrekturmaßnahmen ergreifen können.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Auch wenn die Klassifizierung von Daten in den ersten Entwurfsphasen eines Workloads häufig nach menschlichem Ermessen erfolgt, sollten Sie zur Vorbeugung Systeme einsetzen, die die Identifizierung und Klassifizierung von Testdaten automatisieren. Beispielsweise können Entwickler ein Tool oder einen Dienst erhalten, um repräsentative Daten zu scannen und ihre Sensibilität zu bestimmen. Innerhalb von AWS können Sie Datensätze in Amazon S3 hochladen und sie unter Verwendung von Amazon Macie, Amazon Comprehend oder Amazon Comprehend Medical scannen. Ziehen Sie auch in Betracht, Daten im Rahmen von Modultests und Integrationstests zu scannen, um festzustellen, wo sensible Daten nicht erwartet werden. Eine Warnung vor sensiblen Daten in dieser Phase kann vor der Bereitstellung in der Produktion auf Schutzlücken hinweisen. Andere Funktionen wie die Erkennung sensibler Daten in AWS Glue, Amazon SNS und Amazon CloudWatch können ebenfalls verwendet werden, um PII zu erkennen und geeignete Abhilfemaßnahmen zu ergreifen. Verstehen Sie bei jedem automatisierten Tool oder Dienst, wie es sensible Daten definiert, und ergänzen Sie es mit anderen menschlichen oder automatisierten Lösungen, um eventuelle Lücken zu schließen.

Nutzen Sie die kontinuierliche Überwachung Ihrer Umgebungen als detektivische Kontrolle, um festzustellen, ob sensible Daten auf nicht konforme Weise gespeichert werden. Dies kann dazu beitragen, Situationen zu erkennen, in denen sensible Daten ohne ordnungsgemäße De-Identifizierung oder Schwärzung in Protokolldateien ausgegeben oder in eine

Datenanalyseumgebung kopiert werden. Daten, die in Amazon S3 gespeichert sind, können mit Amazon Macie kontinuierlich auf sensible Daten überwacht werden.

Implementierungsschritte

1. Überprüfen Sie das in SEC07-BP01 beschriebene Datenklassifizierungsschema in Ihrem Unternehmen.
   a. Wenn Sie das Datenklassifizierungsschema Ihrer Organisation kennen, können Sie präzise Prozesse für die automatisierte Identifizierung und Klassifizierung einrichten, die den Richtlinien Ihres Unternehmens entsprechen.
2. Führen Sie einen ersten Scan Ihrer Umgebungen zur automatischen Identifizierung und Klassifizierung durch.
   a. Ein erster vollständiger Scan Ihrer Daten kann dazu beitragen, ein umfassendes Verständnis darüber zu erlangen, wo sich sensible Daten in Ihren Umgebungen befinden. Wenn ein vollständiger Scan nicht erforderlich ist oder aus Kostengründen nicht im Voraus durchgeführt werden kann, sollten Sie prüfen, ob Stichprobenverfahren geeignet sind, um Ihre Ziele zu erreichen. Zum Beispiel kann Amazon Macie so konfiguriert werden, dass eine umfassende automatische Erkennung sensibler Daten in Ihren S3 Buckets durchgeführt wird. Diese Funktion nutzt Stichprobenverfahren, um kosteneffizient eine Vorabanalyse darüber durchzuführen, wo sensible Daten gespeichert sind. Eine tiefergehende Analyse von S3 Buckets kann dann mit einem Auftrag zur Erkennung sensibler Daten durchgeführt werden. Auch andere Datenspeicher können in S3 exportiert werden, um von Amazon Macie durchsucht zu werden.
   b. Richten Sie die in SEC07-BP02 definierte Zugriffskontrolle für Ihre beim Scan identifizierten Datenspeicherressourcen ein.
3. Konfigurieren Sie laufende Scans Ihrer Umgebungen.
   a. Die automatische Erkennungsfunktion für sensible Daten von Amazon Macie kann für laufende Scans Ihrer Umgebungen verwendet werden. Bekannte S3 Buckets, die für die Speicherung sensibler Daten autorisiert sind, können mit einer Zulassen-Liste in Amazon Macie ausgeschlossen werden.
4. Integrieren Sie die Identifizierung und Klassifizierung in Ihre Build- und Testprozesse.
   a. Identifizieren Sie Tools, mit denen Entwickler Daten auf Sensibilität prüfen können, während Workloads entwickelt werden. Verwenden Sie diese Tools als Teil der Integrationstests, um bei unerwarteten sensiblen Daten Alarm zu schlagen und eine weitere Bereitstellung zu verhindern.

5. Implementieren Sie ein System oder Runbook, um Maßnahmen zu ergreifen, wenn sensible Daten an nicht autorisierten Orten gefunden werden.
   a. Schränken Sie den Zugriff auf Daten mithilfe der automatischen Korrektur ein. Sie können diese Daten beispielsweise in einen S3-Bucket mit eingeschränktem Zugriff verschieben oder das Objekt markieren, wenn Sie die attributbasierte Zugriffskontrolle (ABAC) verwenden. Sie sollten außerdem eine Maskierung der Daten bei Entdeckung in Betracht ziehen.
   b. Bitten Sie die für Datenschutz und Vorfallreaktion zuständigen Teams, die Ursache des Vorfalls zu untersuchen. Die identifizierten Erkenntnisse können dazu beitragen, zukünftige Vorfälle zu verhindern.

Ressourcen

Zugehörige Dokumente:

- AWS Glue: Detect and process sensitive data
- Using managed data identifiers in Amazon SNS
- Amazon CloudWatch Logs: Help protect sensitive log data with masking

Zugehörige Beispiele:

- Enabling data classification for Amazon RDS database with Macie
- Detecting sensitive data in DynamoDB with Macie

Zugehörige Tools:

- Amazon Macie
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Glue

SEC07-BP04 Definieren eines skalierbaren Datenlebenszyklusmanagements

Machen Sie sich mit den Anforderungen an den Lebenszyklus Ihrer Daten in Bezug auf die verschiedenen Ebenen der Datenklassifizierung und -verarbeitung vertraut. Dazu kann gehören,

wie Daten behandelt werden, wenn sie zum ersten Mal in Ihre Umgebung gelangen, wie Daten umgewandelt werden und welche Regeln für ihre Vernichtung gelten. Berücksichtigen Sie Faktoren wie Aufbewahrungsfristen, Zugriff, Prüfung und Nachvollziehbarkeit der Herkunft.

Gewünschtes Ergebnis: Sie klassifizieren die Daten so nah wie möglich an dem Punkt und dem Zeitpunkt der Datenerfassung. Wenn die Klassifizierung von Daten eine Maskierung, Tokenisierung oder andere Prozesse zur Verringerung der Sensibilitätsebene erfordert, führen Sie diese Aktionen so nah wie möglich am Zeitpunkt der Datenerfassung durch.

Sie löschen Daten in Übereinstimmung mit Ihrer Richtlinie, wenn sie aufgrund ihrer Klassifizierung nicht mehr aufbewahrt werden sollten.

Typische Anti-Muster:

- Implementieren eines Einheitsansatzes für die Verwaltung des Lebenszyklus von Daten, ohne Berücksichtigung unterschiedlicher Sensibilitätsebenen und Zugriffsanforderungen
- Beschränken der Betrachtung des Lebenszyklusmanagements auf entweder nutzbare Daten oder gesicherte Daten, statt auf beide
- Annehmen, dass Daten, die in Ihren Workload eingegeben wurden, gültig sind, ohne ihren Wert oder ihre Herkunft zu ermitteln
- Vertrauen auf die Haltbarkeit von Daten als Ersatz für Datensicherungen und -schutz
- Beibehalten von Daten über ihre Nützlichkeit und die erforderliche Aufbewahrungsfrist hinaus

Vorteile der Nutzung dieser bewährten Methode: Eine gut definierte und skalierbare Strategie für die Verwaltung des Lebenszyklus von Daten hilft bei der Einhaltung gesetzlicher Vorschriften, verbessert die Datensicherheit, optimiert die Speicherkosten und ermöglicht einen effizienten Datenzugriff und -austausch unter Beibehaltung angemessener Kontrollen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Daten innerhalb eines Workloads sind oft dynamisch. Die Form, in der die Daten in Ihre Workload-Umgebung gelangen, kann sich von der Form unterscheiden, in der sie gespeichert oder in der Geschäftslogik, der Berichterstattung, der Analyse oder dem Machine Learning verwendet werden. Außerdem kann sich der Wert der Daten im Laufe der Zeit ändern. Einige Daten sind zeitlich begrenzt und verlieren an Wert, wenn sie älter werden. Überlegen Sie, wie sich diese

Änderungen an Ihren Daten auf die Bewertung nach Ihrem Datenklassifizierungsschema und die damit verbundenen Kontrollen auswirken. Verwenden Sie nach Möglichkeit einen automatisierten Lebenszyklus-Mechanismus wie Amazon S3-Lebenszyklus-Richtlinien und Amazon Data Lifecycle Manager, um Ihre Datenaufbewahrung, Archivierung und Ablaufprozesse zu konfigurieren. Für Daten, die in DynamoDB gespeichert sind, können Sie das Feature Time To Live (TTL) verwenden, um einen Ablaufzeitstempel pro Element zu definieren.

Unterscheiden Sie zwischen Daten, die zur Verwendung zur Verfügung stehen, und Daten, die als Backup gespeichert sind. Ziehen Sie die Verwendung von AWS Backup in Betracht, um die Sicherung von Daten über AWS-Services hinweg zu automatisieren. Amazon EBS-Snapshots bieten eine Möglichkeit, ein EBS-Volume zu kopieren und es unter Verwendung von S3-Features zu speichern, einschließlich Lebenszyklus, Datenschutz und Zugriff auf Schutzmechanismen. Zwei dieser Mechanismen sind S3 Object Lock und AWS Backup Vault Lock, die Ihnen zusätzliche Sicherheit und Kontrolle über Ihre Backups bieten können. Verwalten Sie eine klare Aufgabentrennung und Zugriffsrechte für Backups. Isolieren Sie Backups auf Kontoebene, um während eines Ereignisses eine Trennung von der betroffenen Umgebung zu gewährleisten.

Ein weiterer Aspekt des Lifecycle-Managements ist die Aufzeichnung des Datenverlaufs, während diese Ihren Workload durchlaufen. Dies wird als Nachverfolgung der Datenherkunft bezeichnet. Dadurch können Sie sicher sein, dass Sie wissen, woher die Daten stammen, welche Transformationen durchgeführt wurden, welcher Eigentümer oder Prozess diese Änderungen vorgenommen hat und wann. Dieser Verlauf hilft bei der Fehlersuche und bei der Untersuchung möglicher Sicherheitsvorfälle. Sie können zum Beispiel Metadaten über Transformationen in einer Amazon DynamoDB-Tabelle protokollieren. Innerhalb eines Data Lake können Sie Kopien der transformierten Daten in verschiedenen S3-Buckets für jede Stufe der Datenpipeline aufbewahren. Speichern Sie Schema- und Zeitstempelinformationen in einem AWS Glue Data Catalog. Unabhängig von Ihrer Lösung sollten Sie die Anforderungen Ihrer Endbenutzer berücksichtigen, um die geeigneten Tools für die Berichterstattung über die Herkunft Ihrer Daten zu bestimmen. So können Sie feststellen, wie Sie Ihre Herkunft am besten verfolgen können.

Implementierungsschritte

1. Analysieren Sie die Datentypen, Sensibilitätsebenen und Zugriffsanforderungen des Workloads, um die Daten zu klassifizieren und geeignete Strategien für das Lebenszyklusmanagement zu definieren.
2. Entwerfen und implementieren Sie Richtlinien für die Datenaufbewahrung und automatisierte Vernichtungsprozesse, die mit den rechtlichen, regulatorischen und organisatorischen Anforderungen übereinstimmen.

3. Etablieren Sie Prozesse und Automatisierungen für die kontinuierliche Überwachung, Prüfung und Anpassung von Strategien, Kontrollen und Richtlinien für die Verwaltung des Datenlebenszyklus, wenn sich die Anforderungen an den Workload und die Vorschriften weiterentwickeln.
   a. Ermitteln von Ressourcen, für die das automatische Lebenszyklusmanagement nicht aktiviert ist, mit AWS Config

Ressourcen

Zugehörige bewährte Methoden:

- COST04-BP05 Durchsetzen von Richtlinien zur Datenaufbewahrung
- SUS04-BP03 Verwalten des Lebenszyklus von Datensätzen mithilfe von Richtlinien

Zugehörige Dokumente:

- Data Classification Whitepaper
- AWS Blueprint for Ransomware Defense
- DevOps Guidance: Improve traceability with data provenance tracking

Zugehörige Beispiele:

- How to protect sensitive data for its entire lifecycle in AWS
- Build data lineage for data lakes using AWS Glue, Amazon Neptune, and Spline

Zugehörige Tools:

- AWS Backup
- Amazon Data Lifecycle Manager
- AWS Identity and Access Management Access Analyzer

Schutz von Daten im Ruhezustand

Daten im Ruhezustand stellen alle Daten dar, die Sie für einen beliebigen Zeitraum in Ihrer Workload im nichtflüchtigen Speicher speichern. Die Daten können sich in Blockspeichern, Objektspeichern, Datenbanken, Archiven, IoT-Geräten und sonstigen Speichermedien befinden. Durch den Schutz

Ihrer ruhenden Daten verringert sich das Risiko eines nicht autorisierten Zugriffs, wenn die Verschlüsselung und entsprechende Zugriffskontrollen implementiert werden.

Die Verschlüsselung und die Tokenisierung sind zwei wichtige, eigenständige Datenschutzschemata.

Mit Tokenisierung können Sie ein Token definieren, das eine vertrauliche Information repräsentiert (beispielsweise die Kreditkartennummer eines Kunden). Ein Token muss selbst bedeutungslos sein und darf nicht von den Daten abgeleitet werden, für die es die Tokenisierung durchführt. Daher kann ein kryptografischer Digest nicht als Token verwendet werden. Durch eine sorgfältige Tokenisierung können Sie den Schutz Ihrer Inhalte erhöhen und Ihre Compliance-Anforderungen erfüllen. Sie können beispielsweise den Umfang der Compliance eines Kreditkarten-Verarbeitungssystems eingrenzen, indem Sie anstelle von Kreditkartennummern Token verwenden.

Verschlüsselung dient dazu, Inhalte so umzuwandeln, dass sie ohne einen geheimen Schlüssel, mit dem der Inhalt wieder in normalen Text entschlüsselt wird, nicht lesbar sind. Sie haben die Möglichkeit, Informationen entsprechend Ihren Anforderungen sowohl durch die Tokenisierung als auch mittels Verschlüsselung sicher zu schützen. Darüber hinaus ist Maskierung eine Technik, die es ermöglicht, einen Teil eines Datenstammes bis zu einem Punkt zu verändern, an dem die verbleibenden Daten nicht mehr als sensibel betrachtet werden. Beispielsweise ermöglicht PCI-DSS, dass die letzten vier Ziffern einer Kartennummer außerhalb der Compliance-Rahmengrenze für die Indizierung beibehalten werden.

Überprüfen der Verwendung von Verschlüsselungsschlüsseln: Vergewissern Sie sich, dass Sie die Verwendung von Verschlüsselungsschlüsseln verstehen und prüfen, um zu überprüfen, ob die Zugriffskontrollmechanismen für die Schlüssel angemessen implementiert sind. Beispielsweise protokolliert jeder AWS-Service, der einen AWS KMS-Schlüssel verwendet, jede Nutzung in AWS CloudTrail. Anschließend können Sie AWS CloudTrail mit einem Tool wie Amazon CloudWatch Logs Insights abfragen, um sicherzustellen, dass alle Nutzungen Ihrer Schlüssel gültig sind.

Bewährte Methoden

- SEC08-BP01 Implementieren einer sicheren Schlüsselverwaltung
- SEC08-BP02 Erzwingen der Verschlüsselung im Ruhezustand
- SEC08-BP03 Automatisieren des Schutzes von Daten im Ruhezustand
- SEC08-BP04 Erzwingen der Zugriffskontrolle

SEC08-BP01 Implementieren einer sicheren Schlüsselverwaltung

Eine sichere Schlüsselverwaltung umfasst die Speicherung, Rotation, Zugriffskontrolle und Überwachung von Schlüsseldaten, die zum Schutz von Daten im Ruhezustand für Ihre Workloads erforderlich sind.

Gewünschtes Ergebnis: Ein skalierbarer, wiederholbarer und automatisierter Schlüsselverwaltungsmechanismus. Der Mechanismus setzt den Zugriff mit geringster Berechtigung auf Schlüsseldaten durch und stellt das richtige Gleichgewicht zwischen Schlüsselverfügbarkeit, Vertraulichkeit und Integrität her. Sie überwachen den Zugriff auf die Schlüssel. Wenn eine Rotation von Schlüsseldaten erforderlich ist, rotieren Sie diese mithilfe eines automatisierten Prozesses. Sie lassen keinen Zugriff auf Schlüsseldaten durch menschliche Bediener zu.

Typische Anti-Muster:

- Personen haben Zugriff auf unverschlüsselte Schlüsseldaten.
- Es werden benutzerdefinierte kryptografische Algorithmen erstellt.
- Die Berechtigungen für den Zugriff auf Schlüsseldaten sind zu weit gefasst.

Vorteile der Nutzung dieser bewährten Methode: Indem Sie einen sicheren Mechanismus für die Schlüsselverwaltung für Ihre Workload einrichten, können Sie dazu beitragen, Ihre Inhalte vor unbefugtem Zugriff zu schützen. Darüber hinaus müssen möglicherweise regulatorische Anforderungen hinsichtlich der Verschlüsselung Ihrer Daten erfüllt werden. Eine effektive Schlüsselverwaltungslösung kann technische Mechanismen bereitstellen, die diesen Vorschriften zum Schutz von Schlüsseldaten entsprechen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Die Verschlüsselung von Daten im Ruhezustand ist eine Basis-Sicherheitskontrolle. Um diese Kontrolle zu implementieren, benötigt Ihr Workload einen Mechanismus, um die Schlüsseldaten sicher zu speichern und zu verwalten, die für die Verschlüsselung Ihrer Daten im Ruhezustand verwendet werden.

AWS bietet den AWS Key Management Service (AWS KMS), um eine dauerhafte, sichere und redundante Speicherung von AWS KMS-Schlüsseln bereitzustellen. Viele AWS-Services lassen sich in AWS KMS integrieren, um die Verschlüsselung Ihrer Daten zu unterstützen. AWS KMS verwendet

FIPS 140-3 Level 3-validierte Hardware-Sicherheitsmodule zum Schutz Ihrer Schlüssel. Es gibt keinen Mechanismus zum Exportieren von AWS KMS-Schlüsseln als Klartext.

Bei der Bereitstellung von Workloads mit einer Multi-Konten-Strategie sollten Sie AWS KMS-Schlüssel in dem Konto aufbewahren, in dem sich auch der Workload befindet, der sie verwendet. Bei diesem verteilten Modell liegt die Verantwortung für die Verwaltung der AWS KMS-Schlüssel bei Ihrem Team. In anderen Anwendungsfällen kann sich Ihre Organisation dafür entscheiden, AWS KMS-Schlüssel in einem zentralen Konto zu speichern. Diese zentralisierte Struktur erfordert zusätzliche Richtlinien, um den kontoübergreifenden Zugriff zu ermöglichen, der benötigt wird, damit das Workload-Konto auf Schlüssel zugreifen kann, die im zentralen Konto gespeichert sind. Dieses Verfahren kann jedoch in Anwendungsfällen, in denen ein einzelner Schlüssel von mehreren AWS-Konten gemeinsam genutzt wird, besser geeignet sein.

Unabhängig davon, wo die Schlüsseldaten gespeichert werden, sollte der Zugriff auf den Schlüssel durch Schlüsselrichtlinien und IAM-Richtlinien eng kontrolliert werden. Schlüsselrichtlinien sind die primäre Methode für die Kontrolle des Zugriffs auf einen AWS KMS-Schlüssel. Darüber hinaus können AWS KMS-Schlüsselzuweisungen den Zugriff auf AWS-Services ermöglichen, um Daten in Ihrem Namen zu verschlüsseln und zu entschlüsseln. Machen Sie sich mit dem Leitfaden für die Steuerung des Zugriffs auf Ihre AWS KMS-Schlüssel vertraut.

Sie sollten die Verwendung von Verschlüsselungsschlüsseln auf ungewöhnliche Zugriffsmuster überwachen. Vorgänge, die mit von AWS verwalteten Schlüsseln und kundenseitig verwalteten Schlüsseln ausgeführt werden, die in AWS KMS gespeichert sind, können in AWS CloudTrail protokolliert werden. Sie sollten regelmäßig überprüft werden. Achten Sie besonders auf die Überwachung von Schlüsselzerstörungsereignissen. Um die versehentliche oder böswillige Zerstörung von Schlüsseldaten zu verhindern, werden Schlüsseldaten bei Schlüsselzerstörungsereignissen nicht sofort gelöscht. Versuche, Schlüssel in AWS KMS zu löschen, unterliegen einer Wartezeit, die standardmäßig 30 Tage beträgt. So haben Administratoren Zeit, diese Aktionen zu überprüfen und die Anforderung rückgängig zu machen, wenn notwendig.

Die meisten AWS-Services verwenden AWS KMS auf eine Weise, die für Sie transparent ist. Sie müssen lediglich entscheiden, ob Sie einen in AWS verwalteten oder einen kundenseitig verwalteten Schlüssel verwenden möchten. Wenn Ihr Workload die direkte Verwendung von AWS KMS zum Verschlüsseln oder Entschlüsseln von Daten erfordert, sollten Sie eine Umschlagverschlüsselung verwenden, um Ihre Daten zu schützen. Das AWS-Verschlüsselungs-SDK kann clientseitige Verschlüsselungsprimitive für Ihre Anwendungen bereitstellen, um die Umschlagverschlüsselung zu implementieren und eine Integration in AWS KMS zu ermöglichen.

Implementierungsschritte

1. Ermitteln Sie die geeigneten Schlüsselverwaltungsoptionen (von AWS verwaltet oder kundenseitig verwaltet) für den Schlüssel.
   a. Aus Gründen der Benutzerfreundlichkeit bietet AWS für die meisten Services AWS-eigene und von AWS verwaltete Schlüssel. Diese stellen eine Funktion für die Verschlüsselung von Daten im Ruhezustand bereit, ohne dass Schlüsseldaten oder -richtlinien verwaltet werden müssen.
   b. Wenn Sie kundenseitig verwaltete Schlüssel verwenden, sollten Sie den Standard-Schlüsselspeicher in Betracht ziehen, um das beste Gleichgewicht zwischen Agilität, Sicherheit, Datenhoheit und Verfügbarkeit zu erzielen. Andere Anwendungsfälle erfordern möglicherweise die Verwendung von benutzerdefinierten Schlüsselspeichern mit AWS CloudHSM oder mit dem externen Schlüsselspeicher.
2. Gehen Sie die Liste der Services durch, die Sie für Ihre Workload verwenden, um zu verstehen, wie AWS KMS in den Service integriert wird. EC2-Instances können beispielsweise verschlüsselte EBS-Volumes verwenden, um zu überprüfen, dass die von diesen Volumes erstellten Amazon-EBS-Snapshots auch mit einem kundenseitig verwalteten Schlüssel verschlüsselt werden. So wird die versehentliche Offenlegung unverschlüsselter Snapshot-Daten verhindert.
   a. Verwendung von AWS KMS durch AWS-Services
   b. Ausführliche Informationen zu den Verschlüsselungsoptionen, die ein AWS-Service bietet, finden Sie im Benutzerhandbuch oder im Entwicklerhandbuch für den Service unter dem Thema „Verschlüsselung im Ruhezustand“.
3. Implementieren Sie AWS KMS: AWS KMS erleichtert Ihnen das Erstellen und Verwalten von Schlüsseln sowie die Steuerung der Verschlüsselung in einer Vielzahl von AWS-Services und in Ihren Anwendungen.
   a. Erste Schritte: AWS Key Management Service (AWS KMS)
   b. Machen Sie sich mit den bewährten Methoden für die Steuerung des Zugriffs auf Ihre AWS KMS-Schlüssel vertraut.
4. Ziehen Sie das AWS Encryption SDK in Betracht: Verwenden Sie das AWS Encryption SDK mit AWS KMS-Integration, wenn Ihre Anwendung Daten clientseitig verschlüsseln muss.
   a. AWS Encryption SDK
5. Aktivieren Sie IAM Access Analyzer, um automatisch zu überprüfen und benachrichtigt zu werden, wenn zu weit gefasste AWS KMS-Schlüsselrichtlinien vorhanden sind.

   a. Ziehen Sie die Verwendung benutzerdefinierter Richtlinienprüfungen in Betracht, um sicherzustellen, dass die Aktualisierung der Ressourcenrichtlinie keinen öffentlichen Zugriff auf KMS-Schlüssel gewährt.

6. Aktivieren Sie Security Hub CSPM, um Benachrichtigungen zu erhalten, wenn falsch konfigurierte Schlüsselrichtlinien, Schlüssel mit geplanter Löschung oder Schlüssel ohne aktivierte automatische Rotation vorhanden sind.
7. Ermitteln Sie die für Ihre AWS KMS-Schlüssel geeignete Protokollierungsstufe. Da Aufrufe von AWS KMS, einschließlich schreibgeschützter Ereignisse, protokolliert werden, können die CloudTrail-Protokolle für AWS KMS sehr umfangreich werden.
   a. Einige Organisationen ziehen es vor, die AWS KMS-Protokollierungsaktivitäten in einem eigenen Pfad zu separieren. Weitere Informationen finden Sie im AWS KMS-Entwicklerhandbuch im Abschnitt Protokollieren von AWS KMS-API-Aufrufen mit CloudTrail.

Ressourcen

Zugehörige Dokumente:

- AWS Key Management Service
- AWS Kryptografische -Services und -Tools
- Schützen von Amazon-S3-Daten durch Verschlüsselung
- Umschlagverschlüsselung
- Das Versprechen zu digitaler Souveränität
- Das Geheimnis von AWS KMS-Schlüsselvorgängen, Bring Your Own Key, benutzerdefiniertem Schlüsselspeicher und Portabilität von Geheimtext
- AWS Key Management Service Kryptografische Details von

Zugehörige Videos:

- So funktioniert die Verschlüsselung in AWS
- Schützen Ihres Blockspeichers in AWS
- AWS Datenschutz in : Verwenden von Schlössern, Schlüsseln, Signaturen und Zertifikaten

Zugehörige Beispiele:

- Implementieren erweiterter Zugriffskontrollsmechanismen mit AWS KMS

SEC08-BP02 Erzwingen der Verschlüsselung im Ruhezustand

Verschlüsseln Sie private Daten im Ruhezustand, um die Vertraulichkeit zu wahren und eine zusätzliche Schutzebene hinsichtlich der unbeabsichtigten Offenlegung oder Exfiltration der Daten bereitzustellen. Die Verschlüsselung schützt die Daten, sodass sie ohne vorherige Entschlüsselung weder gelesen noch verwendet werden können. Inventarisieren und kontrollieren Sie unverschlüsselte Daten, um die mit einer Offenlegung der Daten verbundenen Risiken zu minimieren.

Gewünschtes Ergebnis: Sie verfügen über Mechanismen, die private Daten im Ruhezustand standardmäßig verschlüsseln. Diese Mechanismen helfen, die Vertraulichkeit der Daten zu wahren und bieten eine zusätzliche Schutzebene hinsichtlich der unbeabsichtigten Offenlegung oder Exfiltration der Daten. Sie führen ein Inventar unverschlüsselter Daten und kennen die Kontrollmechanismen, die zum Schutz dieser Daten eingerichtet wurden.

Typische Anti-Muster:

- keine Verwendung von Konfigurationen mit standardmäßiger Verschlüsselung
- Bereitstellung von Zugriffsmöglichkeiten mit zu vielen Berechtigungen für Entschlüsselungsschlüssel
- fehlende Überwachung der Ver- und Entschlüsselungsschlüssel
- Speichern von Daten ohne Verschlüsselung
- Verwendung desselben Verschlüsselungsschlüssels für alle Daten, ohne Berücksichtigung von Datennutzung, Typen und Klassifizierung

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Ordnen Sie Datenklassifizierungen in Ihren Workloads Verschlüsselungsschlüssel zu. Dieser Ansatz schützt vor Zugriff mit zu vielen Berechtigungen, wenn Sie entweder einen einzelnen Zugriffsschlüssel oder eine sehr kleine Anzahl von Verschlüsselungsschlüsseln für Ihre Daten verwenden (siehe SEC07-BP01 Verstehen Ihres Schemas zur Datenklassifizierung).

AWS Key Management Service (AWS KMS) kann in viele AWS-Services integriert werden, um die Verschlüsselung Ihrer Daten im Ruhezustand zu vereinfachen. In Amazon Elastic Compute

Cloud (Amazon EC2) können Sie beispielsweise die Standardverschlüsselung von Konten festlegen, sodass neue EBS-Volumes automatisch verschlüsselt werden. Überlegen Sie sich bei Verwendung von AWS KMS, wie stark die Daten eingeschränkt werden müssen. Standardmäßige und servicegesteuerte AWS KMS-Schlüssel werden von AWS für Sie verwaltet und verwendet. Ziehen Sie für sensible Daten, die einen differenzierten Zugriff auf den zugrunde liegenden Verschlüsselungsschlüssel erfordern, kundenseitig verwaltete Schlüssel (CMKs) in Betracht. Sie haben die vollständige Kontrolle über CMKs, einschließlich Rotation und Zugriffsverwaltung mithilfe von Schlüsselrichtlinien.

Darüber hinaus verschlüsseln Dienste wie Amazon Simple Storage Service (Amazon S3) jetzt standardmäßig alle neuen Objekte. Diese Implementierung bietet eine höhere Sicherheit, ohne die Leistung zu beeinträchtigen.

Andere Services, wie Amazon Elastic Compute Cloud (Amazon EC2) oder Amazon Elastic File System (Amazon EFS), unterstützen Einstellungen für die Standardverschlüsselung. Mit AWS-Config-Regeln können Sie automatisch überprüfen, ob Sie eine Verschlüsselung für Volumes in Amazon Elastic Block Store (Amazon EBS), Instances in Amazon Relational Database Service (Amazon RDS), Amazon-S3-Buckets und andere Services in Ihrer Organisation verwenden.

AWS bietet auch Optionen für die clientseitige Verschlüsselung, mit der Sie Daten vor dem Laden in die Cloud verschlüsseln können. Das AWS Encryption SDK ermöglicht die Verschlüsselung Ihrer Daten per Umschlagverschlüsselung. Sie stellen den Wrapping-Schlüssel bereit und das AWS Encryption SDK generiert einen eindeutigen Datenschlüssel für jedes verschlüsselte Datenobjekt. Ziehen Sie die Verwendung von AWS CloudHSM in Betracht, wenn Sie ein verwaltetes Single-Tenant-Hardware-Sicherheitsmodul (HSM) benötigen. Mit AWS CloudHSM können Sie kryptographische Schlüssel auf einem nach FIPS 140-2 Level 3 validierten HSM generieren, importieren und verwalten. Einige Anwendungsfälle von AWS CloudHSM umfassen den Schutz privater Schlüssel für die Ausgabe einer Zertifizierungsstelle (Certificate Authority, CA) und die Aktivierung der transparenten Datenverschlüsselung (Transparent Data Encryption, TDE) für Oracle-Datenbanken. Das AWS CloudHSM-Client-SDK bietet Software, die die clientseitige Verschlüsselung von Daten mit innerhalb von AWS CloudHSM gespeicherten Schlüsseln ermöglicht, bevor die Daten in AWS geladen werden. Der Amazon DynamoDB Encryption Client ermöglicht darüber hinaus das Verschlüsseln und Signieren von Elementen vor dem Laden in eine DynamoDB-Tabelle.

Implementierungsschritte

- Konfigurieren der Standardverschlüsselung für neue Amazon-EBS-Volumes: Geben Sie an, dass alle neu erstellten Amazon-EBS-Volumes verschlüsselt erstellt werden sollen. Dabei können

Sie den von AWS bereitgestellten Standardschlüssel oder einen von Ihnen erstellten Schlüssel verwenden.

- Konfigurieren von verschlüsselten Amazon Machine Images (AMIs): Beim Kopieren eines vorhandenen AMI mit konfigurierter Verschlüsselung werden Stamm-Volumes und Snapshots automatisch verschlüsselt.
- Konfigurieren der Amazon-RDS-Verschlüsselung: Konfigurieren Sie die Verschlüsselung für Ihre Amazon-RDS-Datenbank-Cluster DB-Cluster und Snapshots mithilfe der Verschlüsselungsoption.
- Erstellen und Konfigurieren von AWS KMS-Schlüsseln mit Richtlinien, die den Zugriff auf die entsprechenden Prinzipale für die jeweilige Datenklassifizierung einschränken: Erstellen Sie beispielsweise einen AWS KMS-Schlüssel für die Verschlüsselung von Produktionsdaten und einen anderen Schlüssel für die Verschlüsselung von Entwicklungs- oder Testdaten. Sie können auch anderen AWS-Konten Schlüsselzugriff gewähren. Ziehen Sie die Nutzung verschiedener Konten für Ihre Entwicklungs- und Produktionsumgebungen in Betracht. Wenn Ihre Produktionsumgebung Artefakte im Entwicklungskonto entschlüsseln muss, können Sie die zur Verschlüsselung der Entwicklungsartefakte verwendete CMK-Richtlinie so bearbeiten, dass das Produktionskonto diese Artefakte entschlüsseln kann. Die Produktionsumgebung kann dann die entschlüsselten Daten zur Verwendung in der Produktion einlesen.
- Konfigurieren der Verschlüsselung in zusätzlichen AWS-Services: Für andere von Ihnen verwendete AWS-Services können Sie in der zugehörigen Sicherheitsdokumentation die Verschlüsselungsoptionen des jeweiligen Service ermitteln.

Ressourcen

Zugehörige Dokumente:

- AWS Crypto Tools
- AWS Encryption SDK
- AWS KMS Cryptographic Details (Whitepaper)
- AWS Key Management Service
- Kryptografische AWS-Services und -Tools
- Amazon-EBS-Verschlüsselung
- Standardverschlüsselung für Amazon-EBS-Volumes
- Verschlüsseln von Amazon-RDS-Ressourcen
- Wie aktiviere ich die Standardverschlüsselung für einen Amazon-S3-Bucket?

- Schützen von Amazon-S3-Daten durch Verschlüsselung

Zugehörige Videos:

- So funktioniert die Verschlüsselung in AWS
- Schützen Ihres Blockspeichers in AWS

SEC08-BP03 Automatisieren des Schutzes von Daten im Ruhezustand

Nutzen Sie Automatisierung, um Daten im Ruhezustand zu validieren und zu kontrollieren. Nutzen Sie automatisierte Scans, um Fehlkonfigurationen Ihrer Datenspeicherlösungen zu erkennen, und führen Sie, wenn möglich, Abhilfemaßnahmen durch automatisierte programmatische Reaktionen durch. Integrieren Sie Automatisierung in Ihre CI/CD-Prozesse, um Fehlkonfigurationen des Datenspeichers zu erkennen, bevor sie in der Produktion bereitgestellt werden.

Gewünschtes Ergebnis: Automatisierte Systeme scannen und überwachen Datenspeicherorte auf falsch konfigurierte Steuerungen, unbefugten Zugriff und unerwartete Nutzung. Bei Erkennung falsch konfigurierter Speicherorte werden automatische Abhilfemaßnahmen initiiert. Automatisierte Prozesse erstellen Daten-Backups und speichern unveränderliche Kopien außerhalb der ursprünglichen Umgebung.

Typische Anti-Muster:

- Keine Berücksichtigung von Optionen zur Aktivierung der Verschlüsselung in den Standardeinstellungen, sofern unterstützt.
- Keine Berücksichtigung von Sicherheitsereignissen neben den betrieblichen Ereignissen bei der Formulierung einer automatisierten Backup- und Wiederherstellungsstrategie.
- Keine Erzwingung der Einstellungen für den öffentlichen Zugriff auf Speicher-Services.
- Keine Überwachung und Prüfung Ihrer Kontrollen zum Schutz von Daten im Ruhezustand.

Vorteile der Nutzung dieser bewährten Methode: Die Automatisierung trägt dazu bei, das Risiko falsch konfigurierter Datenspeicherorte zu vermeiden. Dadurch wird verhindert, dass Fehlkonfigurationen in Ihre Produktionsumgebungen gelangen. Diese bewährte Methode trägt außerdem dazu bei, gegebenenfalls vorhandene Fehlkonfigurationen zu erkennen und zu beheben.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Die Automatisierung zieht sich wie ein roter Faden durch die Praktiken zum Schutz Ihrer Daten im Ruhezustand. In SEC01-BP06 Automatisieren der Bereitstellung von Standard-Sicherheitskontrollen wird beschrieben, wie Sie die Konfiguration Ihrer Ressourcen mithilfe von IaC-Vorlagen (Infrastructure as Code) erfassen können – etwa mit AWS CloudFormation. Diese Vorlagen werden in ein Versionskontrollsystem übertragen und zur Bereitstellung von Ressourcen in AWS über eine CI/CD-Pipeline verwendet. Diese Techniken gelten auch für die Automatisierung der Konfiguration Ihrer Datenspeicherlösungen (zum Beispiel für Verschlüsselungseinstellungen für Amazon-S3-Buckets).

Sie können die Einstellungen, die Sie in Ihren IaC-Vorlagen definieren, mithilfe von Regeln in AWS CloudFormation Guard auf Fehlkonfigurationen in Ihren CI/CD-Pipelines überprüfen. Mit AWS Config können Sie Einstellungen, die in CloudFormation oder anderen IaC-Tools noch nicht verfügbar sind, auf Fehlkonfigurationen überwachen. Für Fehlkonfigurationen generierte Warnungen können automatisch behandelt werden, wie in SEC04-BP04 Initiieren von Abhilfemaßnahmen für nicht konforme Ressourcen beschrieben.

Der Einsatz von Automatisierung als Teil Ihrer Strategie zur Verwaltung von Berechtigungen ist ebenfalls ein wesentlicher Bestandteil des automatisierten Datenschutzes. Unter SEC03-BP02 Gewähren des Zugriffs mit den geringsten Berechtigungen und SEC03-BP04 Kontinuierliche Reduzierung der Berechtigungen erfahren Sie, wie Sie Richtlinien für Zugriff mit den geringsten Rechten konfigurieren, die kontinuierlich von AWS Identity and Access Management Access Analyzer überwacht werden, um Erkenntnisse zu generieren, wenn die Berechtigung reduziert werden kann. Neben der Automatisierung zur Überwachung von Berechtigungen können Sie Amazon GuardDuty für die Überwachung auf anomales Datenzugriffsverhalten für Ihre EBS-Volumes (über eine EC2-Instance) sowie für Ihre S3-Buckets und für unterstützte Amazon-Relational-Database-Service-Datenbanken konfigurieren.

Automatisierung spielt auch eine Rolle bei der Erkennung, ob sensible Daten an nicht autorisierten Orten gespeichert sind. Unter SEC07-BP03 Automatisieren der Identifizierung und Klassifizierung wird beschrieben, wie Amazon Macie Ihre S3-Buckets auf unerwartete sensible Daten überwachen und Warnungen generieren kann, die eine automatisierte Reaktion initiieren können.

Orientieren Sie sich an den Vorgehensweisen unter REL09 Sichern von Daten, um eine Strategie für eine automatisierte Datensicherung und -wiederherstellung zu entwickeln. Datensicherung und -wiederherstellung sind für die Wiederherstellung nach Sicherheitsereignissen ebenso wichtig wie für betriebliche Ereignisse.

Implementierungsschritte

1. Erfassen Sie die Datenspeicherkonfiguration in IaC-Vorlagen. Verwenden Sie automatische Prüfungen in Ihren CI/CD-Pipelines, um Fehlkonfigurationen zu erkennen.
   a. Sie können für CloudFormation Ihre IaC-Vorlagen verwenden und mithilfe von CloudFormation Guard Vorlagen auf Fehlkonfigurationen überprüfen.
   b. Verwenden Sie AWS Config, um Regeln in einem proaktiven Auswertungsmodus auszuführen. Verwenden Sie diese Einstellung, um die Konformität einer Ressource vor der Erstellung als Schritt in Ihrer CI/CD-Pipeline zu prüfen.
2. Überwachen Sie Ressourcen auf Fehlkonfigurationen des Datenspeichers.
   a. Konfigurieren Sie AWS Config so, dass Datenspeicherressourcen auf Änderungen der Kontrollkonfigurationen überwacht und Warnungen generiert werden, um Abhilfemaßnahmen aufzurufen, wenn eine Fehlkonfiguration erkannt wird.
   b. Weitere Hinweise zu automatischen Abhilfemaßnahmen finden Sie unter SEC04-BP04 Initiieren von Abhilfemaßnahmen für nicht konforme Ressourcen.
3. Überwachen und reduzieren Sie die Datenzugriffsberechtigungen kontinuierlich durch Automatisierung.
   a. IAM Access Analyzer kann kontinuierlich ausgeführt werden, um Warnungen zu generieren, wenn gegebenenfalls eine Reduzierung der Berechtigungen möglich ist.
4. Überwachen Sie anomales Datenzugriffsverhalten und geben Sie entsprechende Warnungen aus.
   a. GuardDuty überwacht sowohl bekannte Bedrohungssignaturen als auch Abweichungen vom Baseline-Verhalten beim Zugriff auf Datenspeicherressourcen wie EBS-Volumes, S3-Buckets und RDS-Datenbanken.
5. Überwachen Sie sensible Daten, die an unerwarteten Orten gespeichert sind, und geben Sie entsprechende Warnungen aus.
   a. Verwenden Sie Amazon Macie, um Ihre S3-Buckets kontinuierlich auf sensible Daten zu überprüfen.
6. Automatisieren Sie sichere und verschlüsselte Backups Ihrer Daten.
   a. AWS Backup ist ein verwalteter Service, der verschlüsselte und sichere Backups verschiedener Datenquellen in AWS erstellt. Mit Elastic Disaster Recovery können Sie vollständige Server-Workloads kopieren und einen kontinuierlichen Datenschutz mit einem in Sekunden gemessenen Recovery Point Objective (RPO) gewährleisten. Sie können beide Services so konfigurieren, dass sie zusammenarbeiten, um die Erstellung von Daten-Backups und das Kopieren der Daten an Failover-Standorte zu automatisieren. Dies kann dazu beitragen, dass

Ihre Daten auch dann verfügbar bleiben, wenn sie durch betriebliche oder sicherheitsrelevante Ereignisse beeinträchtigt werden.

Ressourcen

Zugehörige bewährte Methoden:

- SEC01-BP06 Automatisieren der Bereitstellung von Standard-Sicherheitskontrollen
- SEC03-BP02 Gewähren des Zugriffs mit den geringsten Berechtigungen
- SEC03-BP04 Kontinuierliche Reduzierung der Berechtigungen
- SEC04-BP04 Initiieren von Abhilfemaßnahmen für nicht konforme Ressourcen
- SEC07-BP03 Automatisieren der Identifizierung und Klassifizierung
- REL09-BP02 Schützen und Verschlüsseln von Backups
- REL09-BP03 Automatische Daten-Backups

Zugehörige Dokumente:

- AWS Prescriptive Guidance: Automatisches Verschlüsseln vorhandener und neuer Amazon-EBS-Volumes
- Ransomware-Risikomanagement in AWS unter Verwendung des NIST Cyber Security Framework (CSF)

Zugehörige Beispiele:

- Verwenden von proaktiven AWS Config-Regeln sowie von AWS CloudFormation-Hooks, um die Erstellung nicht richtlinienkonformer Cloud-Ressourcen zu verhindern
- Automatisieren und zentrales Verwalten des Datenschutzes für Amazon S3 mit AWS Backup
- AWS re:Invent 2023 – Implementieren von proaktivem Datenschutz mithilfe von Amazon-EBS-Snapshots
- AWS re:Invent 2022 – Entwickeln und Automatisieren für Ausfallsicherheit mit modernem Datenschutz

Zugehörige Tools:

- AWS CloudFormation Guard

- AWS CloudFormation Guard Rules Registry
- IAM Access Analyzer
- Amazon Macie
- AWS Backup
- Elastic Disaster Recovery

SEC08-BP04 Erzwingen der Zugriffskontrolle

Um Ihre Daten im Ruhezustand zu schützen, sollten Sie Zugriffskontrollen über Mechanismen wie Isolierung und Versionsverwaltung durchsetzen. Wenden Sie das Prinzip der geringsten Berechtigung und bedingte Zugriffskontrollen an. Verhindern Sie das Erteilen von öffentlichem Zugriff auf Ihre Daten.

Gewünschtes Ergebnis: Sie stellen sicher, dass nur autorisierte Benutzer auf Daten zugreifen können, und nur insoweit sie diese für ihre Arbeit benötigen. Sie schützen Ihre Daten mit regelmäßigen Backups und Versionsverwaltung vor beabsichtigten oder unbeabsichtigten Änderungen oder Löschungen. Sie isolieren kritische Daten von anderen Daten, um ihre Vertraulichkeit und Integrität zu schützen.

Typische Anti-Muster:

- gemeinsame Speicherung von Daten mit unterschiedlichen Anforderungen hinsichtlich Vertraulichkeit oder verschiedenen Klassifizierungen
- Verwendung von übermäßigen Berechtigungen für Entschlüsselungsschlüssel
- nicht ordnungsgemäße Klassifizierung von Daten
- keine Aufbewahrung von Backups wichtiger Daten
- Gewährung von dauerhaftem Zugriff auf Produktionsdaten
- keine Prüfung des Datenzugriffs bzw. keine regelmäßige Prüfung der Berechtigungen

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Der Schutz von Daten im Ruhezustand ist wichtig, um die Integrität und Vertraulichkeit der Daten zu wahren und die Einhaltung gesetzlicher Anforderungen sicherzustellen. Um dies zu erreichen,

können Sie mehrere Kontrollen implementieren, darunter Zugriffskontrolle, Isolierung, bedingter Zugriff und Versionsverwaltung.

Sie können eine Zugriffskontrolle auf der Basis der geringsten Berechtigung durchsetzen, die Benutzern und Services nur die zur Ausführung ihrer Aufgaben notwendigen Berechtigungen erteilt. Hierzu gehört auch der Zugriff auf Verschlüsselungsschlüssel. Überprüfen Sie Ihre AWS Key Management Service (AWS KMS)-Richtlinien, um sicherzustellen, dass die von Ihnen erteilte Zugriffsebene angemessen ist und entsprechende Bedingungen gelten.

Sie können Daten auf der Grundlage verschiedener Klassifizierungsebenen trennen, indem Sie unterschiedliche AWS-Konten für jede Ebene verwenden und diese Konten mithilfe von AWS Organizations verwalten. Diese Isolierung kann helfen, einen nicht autorisierten Zugriff zu verhindern, und minimiert das Risiko einer Offenlegung von Daten.

Überprüfen Sie regelmäßig die in Amazon-S3-Bucket-Richtlinien gewährte Zugriffsebene. Vermeiden Sie die Verwendung von öffentlich lesbaren oder beschreibbaren Buckets, wenn dies nicht unbedingt erforderlich ist. Ziehen Sie die Verwendung von AWS Config in Betracht, um öffentlich verfügbare Buckets zu erkennen, und von Amazon CloudFront, um Inhalten aus Amazon S3 bereitzustellen. Vergewissern Sie sich, dass die Buckets, die keinen öffentlichen Zugriff erteilen sollen, entsprechend konfiguriert sind, um dies zu verhindern.

Implementieren Sie Mechanismen für Versionsverwaltung und Objektsperre für kritische Daten, die in Amazon S3 gespeichert sind. Die Amazon-S3-Versionsverwaltung behält frühere Versionen von Objekten bei, um nach versehentlichem Löschen oder Überschreiben Daten wiederherstellen zu können. Amazon S3 Object Lock stellt eine obligatorische Zugriffskontrolle für Objekte bereit, die das Löschen oder Überschreiben von Objekten auch durch Root-Benutzer verhindert, bis die Sperre abläuft. Darüber hinaus bietet Amazon Glacier Vault Lock ein ähnliches Feature für in Amazon Glacier gespeicherte Archive.

Implementierungsschritte

1. Durchsetzen der Zugriffskontrolle nach dem Prinzip der geringsten Berechtigung:
    - Überprüfen Sie die den Benutzern und Services erteilten Zugriffsberechtigungen und stellen Sie sicher, dass diese nur über die Berechtigungen verfügen, die sie für ihre Aufgaben benötigen.
    - Überprüfen Sie den Zugriff auf Verschlüsselungsschlüssel durch die Prüfung der AWS Key Management Service (AWS KMS)-Richtlinien.
2. Trennen von Daten anhand verschiedener Klassifizierungsebenen:
    - Verwenden Sie unterschiedliche AWS-Konten für jede Datenklassifizierungsebene.

- Verwalten Sie diese Konten mit AWS Organizations.

3. Überprüfen der Berechtigungen für Amazon-S3-Buckets und -Objekte:
   - Überprüfen Sie regelmäßig die in Amazon-S3-Bucket-Richtlinien erteilte Zugriffsebene.
   - Vermeiden Sie die Verwendung von öffentlich lesbaren oder beschreibbaren Buckets, wenn dies nicht unbedingt erforderlich ist.
   - Ziehen Sie die Verwendung von AWS Config für die Erkennung öffentlich verfügbarer Buckets in Betracht.
   - Verwenden Sie Amazon CloudFront, um Inhalte aus Amazon S3 bereitzustellen.
   - Vergewissern Sie sich, dass die Buckets, die keinen öffentlichen Zugriff gewähren sollen, entsprechend konfiguriert sind, um dies zu verhindern.
   - Sie können dasselbe Überprüfungsverfahren für Datenbanken und andere Datenquellen anwenden, die die IAM-Authentifizierung verwenden, z. B. SQS oder Datenspeicher von Drittanbietern.
4. Verwenden von AWS IAM Access Analyzer:
   - Sie können AWS IAM Access Analyzer nutzen, um Amazon-S3-Buckets zu analysieren und Erkenntnisse zu generieren, wenn eine S3-Richtlinie Zugriff auf eine externe Entität gewährt.
5. Implementieren von Mechanismen für Versionsverwaltung und Objektsperre:
   - Verwenden Sie die Amazon-S3-Versionsverwaltung, um frühere Versionen von Objekten beizubehalten, sodass Daten nach versehentlichem Löschen oder Überschreiben wiederhergestellt werden können.
   - Verwenden Sie Amazon S3 Object Lock, um eine obligatorische Zugriffskontrolle für Objekte bereitzustellen, die das Löschen oder Überschreiben von Objekten auch durch Root-Benutzer verhindert, bis die Sperre abläuft.
   - Verwenden Sie Amazon Glacier Vault Lock für Archive, die in Amazon Glacier gespeichert sind.
6. Verwenden von Amazon S3 Inventory:
   - Sie können Amazon S3 Inventory verwenden, um den Replikations- und Verschlüsselungsstatus Ihrer S3-Objekte zu prüfen und zu melden.
7. Überprüfen von Berechtigungen für die Amazon-EBS und AMI-Freigabe:
   - Überprüfen Sie die Freigabeberechtigungen für Amazon EBS und AMI-Freigabe, um sicherzustellen, dass Ihre Images und Volumes nicht für AWS-Konten außerhalb Ihres Workloads freigegeben werden.
8. Regelmäßiges Überprüfen der Freigaben über AWS Resource Access Manager:

- Sie können AWS Resource Access Manager für die Freigabe von Ressourcen innerhalb Ihrer Amazon-VPCs verwenden, z. B. Richtlinien für AWS Network Firewall, Regeln für Amazon Route 53 Resolver und Subnetze.
- Überprüfen Sie die freigegebenen Ressourcen regelmäßig und beenden Sie die Freigabe von Ressourcen, die keine Freigabe mehr erfordern.

Ressourcen

Zugehörige bewährte Methoden:

- SEC03-BP01 Definieren von Zugriffsanforderungen
- SEC03-BP02 Gewähren des Zugriffs mit den geringsten Berechtigungen

Zugehörige Dokumente:

- AWS KMS Cryptographic Details (Whitepaper
- Einführung in die Verwaltung von Zugriffsberechtigungen für Ihre Amazon-S3-Ressourcen
- Übersicht über die Verwaltung des Zugriffs auf Ihre AWS KMS-Ressourcen
- AWS-Config-Regeln
- Amazon S3 + Amazon CloudFront: Die perfekte Kombination in der Cloud
- Verwenden der Versionsverwaltung
- Sperren von Objekten mithilfe von Amazon S3 Object Lock
- Freigeben eines Amazon-EBS-Snapshots
- Gemeinsame AMIs
- Hosten einer Single-Page-Anwendung auf Amazon S3
- AWS Globale -Bedingungsschlüssel
- Erstellen eines Datenperimeters in AWS

Zugehörige Videos:

- Schützen Ihres Blockspeichers in AWS

Schützen von Daten während der Übertragung

Unter Daten während der Übertragung verstehen wir alle Daten, die von einem System an ein anderes gesendet werden. Hierzu zählt auch die Kommunikation zwischen Ressourcen innerhalb Ihrer Workload sowie zwischen anderen Services und Ihren Endbenutzern. Durch geeigneten Schutz Ihrer Daten während der Übertragung stellen Sie die Integrität und Vertraulichkeit der Daten Ihrer Anwendungen sicher.

Sichern von Daten zwischen VPC oder On-Premises-Standorten: Sie können AWS PrivateLink verwenden, um eine sichere und private Netzwerkverbindung zwischen Amazon Virtual Private Cloud (Amazon VPC) oder einer On-Premises-Verbindung zu Services zu schaffen, die in AWS gehostet werden. Sie können auf AWS-Services, Services von Drittanbietern und Services in anderen AWS-Konten so zugreifen, als befänden sie sich in Ihrem privaten Netzwerk. Mit AWS PrivateLink können Sie auf Services über Konten mit sich überschneidenden IP-CIDRs zugreifen, ohne ein Internet-Gateway oder NAT zu benötigen. Sie müssen auch keine Firewall-Regeln, Pfaddefinitionen oder Routing-Tabellen konfigurieren. Der Datenverkehr verbleibt auf dem Amazon-Backbone und wird nicht über das Internet geleitet, so dass Ihre Daten geschützt sind. Sie können branchenspezifische Compliance-Vorschriften wie HIPAA und EU/US Privacy Shield einhalten. AWS PrivateLink arbeitet nahtlos mit Lösungen von Drittanbietern zusammen, um ein vereinfachtes globales Netzwerk zu schaffen, das es Ihnen ermöglicht, Ihre Migration in die Cloud zu beschleunigen und die verfügbaren AWS-Services zu nutzen.

Bewährte Methoden

- SEC09-BP01 Implementieren einer sicheren Schlüssel- und Zertifikatverwaltung
- SEC09-BP02 Erzwingen von Verschlüsselung bei der Übertragung
- SEC09-BP03 Authentifizieren der Netzwerkkommunikation

SEC09-BP01 Implementieren einer sicheren Schlüssel- und Zertifikatverwaltung

Transport Layer Security (TLS)-Zertifikate werden verwendet, um die Netzwerkkommunikation zu schützen und die Identität von Websites, Ressourcen und Workloads über das Internet sowie in privaten Netzwerken zu bestimmen.

Gewünschtes Ergebnis: Ein sicheres Zertifikatverwaltungssystem, das Zertifikate in einer Public-Key-Infrastruktur (PKI) bereitstellen, speichern und verlängern kann. Ein sicherer Schlüssel- und

Zertifikatverwaltungsmechanismus verhindert die Offenlegung von Zertifikatdaten mit privaten Schlüsseln und erneuert das Zertifikat automatisch in regelmäßigen Abständen. Er lässt sich auch in andere Services integrieren, um eine sichere Netzwerkkommunikation und Identität für Computerressourcen innerhalb Ihrer Workload zu gewährleisten. Schlüsseldaten sollten niemals für menschliche Identitäten zugänglich sein.

Typische Anti-Muster:

- Während der Bereitstellung oder Verlängerung von Zertifikaten werden manuelle Schritte ausgeführt.
- Beim Entwerfen einer privaten Zertifizierungsstelle (Certificate Authority, CA) wird die Hierarchie der Zertifizierungsstelle nicht ausreichend beachtet.
- Für öffentliche Ressourcen werden selbstsignierte Zertifikate verwendet.

Vorteile der Nutzung dieser bewährten Methode:

- Die Zertifikatverwaltung wird durch automatisierte Bereitstellung und Verlängerung vereinfacht.
- Die Verschlüsselung von Daten während der Übertragung mit TLS-Zertifikaten wird gefördert.
- Sicherheit und Überprüfbarkeit der von der Zertifizierungsstelle ausgeführten Zertifikataktionen werden gesteigert.
- Verwaltungsaufgaben werden auf verschiedenen Ebenen der CA-Hierarchie strukturiert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Moderne Workloads nutzen verschlüsselte Netzwerkkommunikation mithilfe von PKI-Protokollen wie TLS in großem Umfang. Die Verwaltung von PKI-Zertifikaten kann komplex sein. Eine automatisierte Bereitstellung und Verlängerung von Zertifikaten kann jedoch zu einer reibungsloseren Zertifikatverwaltung beitragen.

AWS bietet zwei Services zur Verwaltung universeller PKI-Zertifikate: AWS Certificate Manager und AWS Private Certificate Authority (AWS Private CA). ACM ist der primäre Service, den Kunden für die Bereitstellung und Verwaltung von Zertifikaten sowohl für öffentliche als auch für private AWS-Workloads verwenden. ACM stellt mithilfe von AWS Private CA private Zertifikate aus und kann in viele andere verwaltete AWS-Services integriert werden, um sichere TLS-Zertifikate für Workloads bereitzustellen. ACM kann auch über Amazon Trust Services öffentlich vertrauenswürdige Zertifikate

ausstellen. Öffentliche AVM-Zertifikate können für öffentlich zugängliche Workloads verwendet werden, da moderne Browser und Betriebssysteme diesen Zertifikaten standardmäßig vertrauen.

AWS Private CA ermöglicht es Ihnen, Ihre eigene Stamm- oder untergeordnete Zertifizierungsstelle einzurichten und TLS-Zertifikate über eine API auszustellen. Sie können diese Art von Zertifikaten in Szenarien verwenden, in denen Sie die Vertrauenskette auf der Clientseite der TLS-Verbindung steuern und verwalten. Zusätzlich zu TLS-Anwendungsfällen kann AWS Private CA für die Ausstellung von Zertifikaten für Kubernetes-Pods, Matter-Geräteproduktbescheinigungen, Codesignaturen und andere Anwendungsfälle verwendet werden, und zwar mit einer benutzerdefinierten Vorlage. Sie können auch IAM Roles Anywhere verwenden, um temporäre IAM-Anmeldeinformationen für On-Premises-Workloads bereitzustellen, für die von Ihrer privaten CA signierte X.509-Zertifikate ausgestellt wurden.

Zusätzlich zu ACM und AWS Private CA bietet AWS IoT Core spezielle Unterstützung für die Bereitstellung und Verwaltung von PKI-Zertifikaten für IoT-Geräte. AWS IoT Core bietet spezielle Mechanismen für das Onboarding von IoT-Geräten in Ihre Public-Key-Infrastruktur in großem Umfang.

Einige AWS-Services, wie Amazon API Gateway und Elastic Load Balancing, bieten eigene Funktionen für die Verwendung von Zertifikaten zum Schutz von Anwendungsverbindungen. Sowohl API Gateway als auch Application Load Balancer (ALB) unterstützen beispielsweise Mutual TLS (mTLS) über Client-Zertifikate, die Sie über die AWS-Managementkonsole, die CLI oder APIs erstellen und exportieren.

Überlegungen zur Einrichtung einer privaten CA-Hierarchie

Wenn Sie eine private Zertifizierungsstelle einrichten müssen, ist es wichtig, dass Sie besonders darauf achten, die CA-Hierarchie im Voraus richtig zu entwerfen. Es hat sich bewährt, beim Erstellen einer privaten CA-Hierarchie jede Ebene der Hierarchie in separaten AWS-Konten bereitzustellen. Dieser gezielte Schritt reduziert die Oberfläche für jede Ebene in der CA-Hierarchie, wodurch es einfacher wird, Anomalien in CloudTrail-Protokolldaten zu erkennen und den Umfang des Zugriffs oder die Auswirkungen eines unbefugten Zugriffs auf eines der Konten zu reduzieren. Die Stammzertifizierungsstelle sollte sich in einem eigenen separaten Konto befinden und nur zur Ausstellung eines oder mehrerer Zertifikate für eine Zwischenzertifizierungsstelle verwendet werden.

Erstellen Sie dann eine oder mehrere Zwischenzertifizierungsstellen in Konten, die vom Konto der Stammzertifizierungsstelle getrennt sind, um Zertifikate für Endbenutzer, Geräte oder andere Workloads auszustellen. Stellen Sie abschließend Zertifikate von Ihrer Stammzertifizierungsstelle an die Zwischenzertifizierungsstellen aus, die wiederum Zertifikate für die Endbenutzer oder Geräte

ausstellen. Weitere Informationen zur Planung Ihrer CA-Bereitstellung und zum Entwerfen einer CA-Hierarchie, einschließlich Planung von Ausfallsicherheit, regionsübergreifender Replikation, gemeinsamer Nutzung von Zertifizierungsstellen in Ihrer Organisation und mehr, finden Sie unter Planen Ihrer AWS Private CA-Bereitstellung.

Implementierungsschritte

1. Ermitteln Sie die relevanten AWS-Services, die für Ihren Anwendungsfall erforderlich sind:
   - In vielen Anwendungsfällen kann die bestehende Public-Key-Infrastruktur von AWS mithilfe von AWS Certificate Manager genutzt werden. ACM kann zur Bereitstellung von TLS-Zertifikaten für Webserver, Load Balancer oder für andere Zwecke für öffentlich vertrauenswürdige Zertifikate verwendet werden.
   - Ziehen Sie die Verwendung von AWS Private CA in Betracht, wenn Sie Ihre eigene private Zertifizierungsstellenhierarchie einrichten müssen oder Zugriff auf exportierbare Zertifikate benötigen. Mit ACM können dann viele Arten von Endentitätszertifikaten unter Verwendung der AWS Private CA ausgegeben werden.
   - Für Anwendungsfälle, in denen in großem Umfang Zertifikate für eingebettete IoT-Geräte (Internet of Things, Internet der Dinge) bereitgestellt werden müssen, empfiehlt sich gegebenenfalls die Verwendung von AWS IoT Core.
   - Ziehen Sie die Verwendung nativer mTLS-Funktionen in Services wie Amazon API Gateway oder Application Load Balancer in Betracht.
2. Implementieren Sie nach Möglichkeit eine automatisierte Zertifikatverlängerung:
   - Verwenden Sie die von ACM verwaltete Verlängerung für von ACM ausgestellte Zertifikate zusammen mit integrierten verwalteten AWS-Services.
3. Richten Sie Protokollierung und Audit Trails ein:
   - Aktivieren Sie CloudTrail-Protokolle, um Zugriffe auf die Konten zu verfolgen, die Zertifizierungsstellen enthalten. Erwägen Sie, die Integritätsprüfung der Protokolldatei in CloudTrail zu konfigurieren, um die Authentizität der Protokolldaten zu überprüfen.
   - Generieren und überprüfen Sie regelmäßig Auditberichte, in denen die Zertifikate aufgeführt werden, die Ihre private CA ausgestellt oder widerrufen hat. Diese Berichte können in einen S3-Bucket exportiert werden.
   - Wenn Sie eine private CA bereitstellen, müssen Sie auch einen S3-Bucket einrichten, um die CRL (Certificate Revocation List, Zertifikatsperrliste) zu speichern. Anleitungen zur Konfiguration dieses S3-Buckets basierend auf den Anforderungen Ihrer Workload finden Sie unter Planung einer Zertifikatsperrliste (CRL).

Ressourcen

Zugehörige bewährte Methoden:

- SEC02-BP02 Verwenden von temporären Anmeldeinformationen
- SEC08-BP01 Implementieren einer sicheren Schlüsselverwaltung
- SEC09-BP03 Authentifizieren der Netzwerkkommunikation

Zugehörige Dokumente:

- Hosten und Verwalten einer ganzen privaten Zertifikatinfrastruktur in AWS
- Sichern einer ACM Private CA-Hierarchie auf Unternehmensebene für die Automobil- und Produktionsbranche
- Bewährte Private-CA-Methoden
- So verwenden Sie AWS RAM, um Ihre ACM Private CA kontoübergreifend zu teilen

Zugehörige Videos:

- Aktivieren von AWS Certificate Manager Private CA (Workshop)

Zugehörige Beispiele:

- Private-CA-Workshop
- Workshop zur IoT-Geräteverwaltung (einschließlich Gerätebereitstellung)

Zugehörige Tools:

- Plugin für Kubernetes-Zertifikatmanager für die Verwendung von AWS Private CA

SEC09-BP02 Erzwingen von Verschlüsselung bei der Übertragung

Erzwingen Sie Ihre definierten Verschlüsselungsanforderungen basierend auf den Richtlinien, regulatorischen Verpflichtungen und Standards Ihrer Organisation, damit Sie Ihre Organisations-, Rechts- und Compliance-Anforderungen erfüllen können. Verwenden Sie nur Protokolle mit Verschlüsselung, wenn Sie vertrauliche Daten außerhalb Ihrer Virtual Private Cloud (VPC)

übertragen. Verschlüsselung trägt auch dann zur Wahrung der Datenvertraulichkeit bei, wenn die Daten nicht vertrauenswürdige Netzwerke durchqueren.

Gewünschtes Ergebnis: Sie verschlüsseln den Netzwerkdatenverkehr zwischen Ihren Ressourcen und dem Internet, um nicht autorisierten Zugriff auf die Daten zu verhindern. Sie verschlüsseln den Netzwerkverkehr in Ihrer internen AWS-Umgebung entsprechend Ihren Sicherheitsanforderungen. Sie verschlüsseln Daten während der Übertragung mit sicheren TLS-Protokollen und Cipher Suites.

Typische Anti-Muster:

- Verwendung veralteter Versionen von SSL, TLS und Komponenten von Verschlüsselungssammlungen (zum Beispiel SSL v3.0, RSA-Schlüssel mit 1024 Bit und RC4-Verschlüsselung)
- Zulassen von unverschlüsseltem (HTTP-)Datenverkehr zu oder von öffentlich zugänglichen Ressourcen
- keine Überwachung und kein Ersatz von X.509-Zertifikaten, bevor sie ablaufen
- Verwendung selbstsignierter X.509-Zertifikate für TLS

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

AWS-Services bieten HTTPS-Endpunkte, die für die Kommunikation TLS nutzen. Dadurch werden die Daten bei der Kommunikation mit den AWS-APIs während der Übertragung verschlüsselt. Unsichere HTTP-Protokolle können in einer Virtual Private Cloud (VPC) durch die Verwendung von Sicherheitsgruppen überprüft und blockiert werden. HTTP-Anforderungen können auch automatisch an HTTPS umgeleitet werden (in Amazon CloudFront oder in einem Application Load Balancer). Sie können eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) verwenden, um die Fähigkeit zum Hochladen von Objekten über HTTP einzuschränken und so die Verwendung von HTTPS für Objekt-Uploads in Ihren Buckets durchzusetzen. Sie haben uneingeschränkte Kontrolle über Ihre Datenverarbeitungsressourcen und können die Verschlüsselung während der Übertragung in allen Ihren Services implementieren. Darüber hinaus können Sie die VPN-Konnektivität mit Ihrer VPC von einem externen Netzwerk oder von AWS Direct Connect aus verwenden, um die Verschlüsselung des Datenverkehrs zu erleichtern. Vergewissern Sie sich, dass Ihre Clients bei Aufruffen von AWS-APIs mindestens TLS 1.2 verwenden, da AWS die Verwendung älterer TLS-Versionen im Februar 2024 eingestellt hat. Wir empfehlen Ihnen, TLS 1.3 zu verwenden. Wenn Sie besondere Anforderungen an die Verschlüsselung während der Übertragung stellen, finden Sie im AWS Marketplace Informationen zu verfügbaren Lösungen von Drittanbietern.

Implementierungsschritte

- Erzwingen der Verschlüsselung bei der Übertragung: Die definierten Verschlüsselungsanforderungen sollten sich nach den neuesten Standards und bewährten Methoden richten und nur sichere Protokolle zulassen. Konfigurieren Sie beispielsweise eine Sicherheitsgruppe, die nur das HTTPS-Protokoll für einen Application Load Balancer oder eine Amazon–EC2-Instance zulässt.
- Konfigurieren von sicheren Protokollen in Edge-Services: Konfigurieren Sie HTTPS mit Amazon CloudFront und verwenden Sie ein für Ihren Sicherheitsstatus und Ihren Anwendungsfall geeignetes Sicherheitsprofil.
- Verwenden eines VPN für externe Konnektivität: Verwenden Sie gegebenenfalls ein IPsec-VPN, um Punkt-zu-Punkt- oder Netzwerk-zu-Netzwerk-Verbindungen zu schützen und so Datenschutz und Datenintegrität zu gewährleisten.
- Konfigurieren von sicheren Protokollen bei Load Balancern: Wählen Sie eine Sicherheitsrichtlinie aus, die die stärksten Verschlüsselungssammlungen bereitstellt, die von den Clients unterstützt werden, die eine Verbindung mit dem Listener herstellen. Erstellen Sie einen HTTPS-Listener für Ihren Application Load Balancer.
- Konfigurieren von sicheren Protokollen bei Amazon Redshift: Konfigurieren Sie Ihren Cluster so, dass eine Verbindung über Secure Socket Layer (SSL) oder Transport Layer Security (TLS) verwendet werden muss.
- Konfigurieren von sicheren Protokollen: Sehen Sie sich die AWS-Servicedokumentation an, um die Funktionen zur Verschlüsselung während der Übertragung zu bestimmen.
- Konfigurieren von sicherem Zugriff beim Hochladen in Amazon-S3-Buckets: Verwenden Sie die Richtliniensteuerung für Amazon-S3-Buckets, um sicheren Zugriff auf Daten zu erzwingen.
- Erwägen der Verwendung von AWS Certificate Manager: ACM ermöglicht die Bereitstellung und Verwaltung öffentlicher TLS-Zertifikate für die Verwendung mit AWS-Services.
- Erwägen der Verwendung von AWS Private Certificate Authority für private PKI-Anforderungen: AWS Private CA ermöglicht die Erstellung privater Zertifizierungsstellenhierarchien, um X.509-Endentitätszertifikate auszustellen, die zum Erstellen verschlüsselter TLS-Kanäle verwendet werden können.

Ressourcen

Zugehörige Dokumente:

- Verwenden von HTTPS mit CloudFront

- Verbinden Ihrer VPC mit Remote-Netzwerken über AWS Virtual Private Network
- Erstellen eines HTTPS-Listeners für Ihren Application Load Balancer
- Tutorial: SSL/TLS unter Amazon Linux 2 konfigurieren
- Verwenden von SSL/TLS für die Verschlüsselung einer Verbindung zu einer DB-Instance
- Konfigurieren von Sicherheitsoptionen für Verbindungen

SEC09-BP03 Authentifizieren der Netzwerkkommunikation

Überprüfen Sie die Kommunikationsidentität mithilfe von Protokollen mit Authentifizierungsunterstützung – beispielsweise Transport Layer Security (TLS) oder IPsec.

Gestalten Sie Ihre Workload so, dass bei der Kommunikation zwischen Services, Anwendungen oder Benutzern sichere, authentifizierte Netzwerkprotokolle verwendet werden. Die Verwendung von Netzwerkprotokollen, die Authentifizierung und Autorisierung unterstützen, ermöglicht eine bessere Kontrolle des Netzwerkflusses und reduziert die Auswirkungen von nicht autorisiertem Zugriff.

Gewünschtes Ergebnis: Eine Workload mit klar definierten Datenflüssen auf Daten- und Steuerebene zwischen Services. Die Datenflüsse verwenden authentifizierte und verschlüsselte Netzwerkprotokolle, sofern dies technisch möglich ist.

Typische Anti-Muster:

- unverschlüsselte oder unauthentifizierte Datenflüsse innerhalb Ihrer Workload
- Wiederverwendung von Authentifizierungsdaten für mehrere Benutzer oder Entitäten
- alleinige Verwendung von Netzwerkkontrollen als Zugriffskontrolle
- Erstellung eines benutzerdefinierten Authentifizierungsmechanismus, anstatt sich auf branchenübliche Standard-Authentifizierungsmechanismen zu verlassen
- Übermäßig freizügige Datenflüsse zwischen Service-Komponenten oder anderen Ressourcen in der VPC

Vorteile der Nutzung dieser bewährten Methode:

- Schränkt den Umfang der Auswirkungen eines unberechtigten Zugriffs auf einen Teil des Workloads ein.
- Bietet ein höheres Maß an Sicherheit, dass Aktionen nur von authentifizierten Personen durchgeführt werden können.

- Verbessert die Entkopplung von Services, indem die vorgesehenen Schnittstellen für die Datenübertragung klar definiert und erzwungen werden.
- Verbessert die Überwachung und Protokollierung sowie die Reaktion auf Vorfälle durch Zuordnung von Anforderungen sowie durch klar definierte Kommunikationsschnittstellen.
- Bietet durch die Kombination von Netzwerkkontrollen mit Authentifizierungs- und Autorisierungskontrollen einen umfassenden Schutz für Ihre Workloads.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

Implementierungsleitfaden

Die Netzwerkdatenverkehrsmuster Ihrer Workload lassen sich in zwei Kategorien einteilen:

- Der Ost-West-Verkehr steht für Datenflüsse zwischen Services, die eine Workload ausmachen.
- Der Nord-Süd-Verkehr stellt die Datenflüsse zwischen Ihrer Workload und den Consumern dar.

Während es üblich ist, den Nord-Süd-Verkehr zu verschlüsseln, ist der Schutz des Ost-West-Verkehrs mit authentifizierten Protokollen weniger verbreitet. In modernen Sicherheitspraktiken wird darauf hingewiesen, dass das Netzwerkdesign allein noch keine vertrauenswürdige Beziehung zwischen zwei Entitäten gewährleistet. Auch wenn sich zwei Services innerhalb einer gemeinsamen Netzwerkgrenze befinden, ist es immer noch die beste Methode, die Kommunikation zwischen diesen Services zu verschlüsseln, zu authentifizieren und zu autorisieren.

Beispielsweise verwenden AWS-Service-APIs das Signaturprotokoll AWS Signature Version 4 (SigV4), um den Anforderer zu authentifizieren, unabhängig davon, aus welchem Netzwerk die Anforderung stammt. Diese Authentifizierung stellt sicher, dass AWS-APIs die Identität des Anforderers der Aktion überprüfen können. Diese Identität kann dann mit Richtlinien kombiniert werden, um eine Autorisierungsentscheidung zu treffen und zu bestimmen, ob die Aktion zugelassen werden soll.

Mit Services wie Amazon VPC Lattice und Amazon API Gateway können Sie das gleiche SigV4-Signaturprotokoll verwenden, um den Ost-West-Verkehr in Ihren eigenen Workloads zu authentifizieren und zu autorisieren. Wenn Ressourcen außerhalb Ihrer AWS-Umgebung mit Services kommunizieren müssen, die eine SigV4-basierte Authentifizierung und Autorisierung erfordern, können Sie AWS Identity and Access Management (IAM) Roles Anywhere für die AWS-fremde Ressource verwenden, um temporäre AWS-Anmeldeinformationen zu erhalten. Diese

Anmeldeinformationen können verwendet werden, um Anforderungen für Services zu signieren, die Zugriff mithilfe von SigV4 autorisieren.

Ein weiterer gängiger Mechanismus zur Authentifizierung des Ost-West-Verkehrs ist die gegenseitige TLS-Authentifizierung (mTLS). Viele IoT-Anwendungen (Internet of Things, Internet der Dinge) und Business-to-Business-Anwendungen sowie Microservices verwenden mTLS, um die Identität beider Seiten einer TLS-Kommunikation durch die Verwendung von X.509-Zertifikaten auf Client- und Server-Seite zu validieren. Diese Zertifikate können von AWS Private Certificate Authority (AWS Private CA) ausgestellt werden. Sie können Services wie Amazon API Gateway verwenden, um die mTLS-Authentifizierung für die Kommunikation zwischen oder innerhalb eines Workloads bereitzustellen. Application Load Balancer unterstützt mTLS auch für interne oder externe Workloads. mTLS stellt zwar Authentifizierungsinformationen für beide Seiten einer TLS-Kommunikation bereit, bietet aber keinen Mechanismus zur Autorisierung.

Und zu guter Letzt: OAuth 2.0 und OpenID Connect (OIDC) sind zwei Protokolle, die in der Regel für die Steuerung des Zugriffs von Benutzern auf Services verwendet werden. Inzwischen werden sie jedoch auch für Datenverkehr zwischen Services immer beliebter. API Gateway bietet einen JSON Web Token (JWT) Authorizer, der es Workloads ermöglicht, den Zugriff auf API-Routen mithilfe von JWTs zu beschränken, die von OIDC- oder OAuth-2.0-Identitätsanbietern ausgestellt wurden. OAuth2-Bereiche können als Quelle für grundlegende Autorisierungsentscheidungen verwendet werden, aber die Autorisierungsprüfungen müssen immer noch in der Anwendungsschicht implementiert werden. Und OAuth2-Bereiche allein können komplexere Autorisierungsanforderungen nicht unterstützen.

Implementierungsschritte

- Definieren und Dokumentieren der Netzwerkflüsse Ihrer Workload: Der erste Schritt bei der Implementierung einer umfassenden Verteidigungsstrategie ist die Definition der Datenflüsse Ihrer Workload.
  - Erstellen Sie ein Datenflussdiagramm, das klar definiert, wie Daten zwischen den verschiedenen Services, aus denen sich Ihre Workload zusammensetzt, übertragen werden. Dieses Diagramm ist der erste Schritt zur Erzwingung dieser Datenflüsse über authentifizierte Netzwerkkanäle.
  - Nutzen Sie Ihre Workloads in der Entwicklungs- und Testphase, um zu überprüfen, ob das Datenflussdiagramm das Verhalten der Workloads zur Laufzeit korrekt wiedergibt.
  - Ein Datenflussdiagramm kann auch bei der Durchführung einer Bedrohungsmodellierung nützlich sein, wie unter SEC01-BP07 Identifizieren von Bedrohungen und Priorisieren von Abhilfemaßnahmen unter Verwendung eines Bedrohungsmodells beschrieben.

- Einrichten von Netzwerkkontrollen: Erwägen Sie die Verwendung von AWS-Funktionen, um Netzwerkkontrollen einzurichten, die auf Ihre Datenflüsse abgestimmt sind. Netzwerkgrenzen sollten zwar nicht die einzige Sicherheitskontrolle sein, aber sie stellen eine Schicht der umfassenden Verteidigungsstrategie zum Schutz Ihrer Workload dar.
  - Verwenden Sie Sicherheitsgruppen, um den Datenfluss zwischen Ressourcen zu definieren und einzuschränken.
  - Erwägen Sie die Verwendung von AWS PrivateLink, um sowohl mit AWS als auch mit Drittanbieter-Services zu kommunizieren, die AWS PrivateLink unterstützen. Daten, die über einen AWS PrivateLink-Schnittstellen-Endpunkt gesendet werden, bleiben innerhalb des AWS-Netzwerk-Backbones und durchlaufen nicht das öffentliche Internet.
- Implementieren von Authentifizierung und Autorisierung für alle Services in Ihrer Workload: Wählen Sie die AWS-Services aus, die am besten geeignet sind, um authentifizierte, verschlüsselte Datenflüsse in Ihrer Workload bereitzustellen.
  - Ziehen Sie die Verwendung von Amazon VPC Lattice in Betracht, um die Kommunikation zwischen Services zu schützen. VPC Lattice kann SigV4-Authentifizierung in Kombination mit Authentifizierungsrichtlinien verwenden, um den Zugriff zwischen Services zu steuern.
  - Ziehen Sie für die Kommunikation zwischen Services mit mTLS API Gateway oder Application Load Balancer in Betracht. AWS Private CA kann verwendet werden, um eine private CA-Hierarchie einzurichten, die Zertifikate für die Verwendung mit mTLS ausstellen kann.
  - Im Falle einer Integration in Services, die OAuth 2.0 oder OIDC verwenden, sollten Sie die Verwendung von API Gateway mit dem JWT-Genehmiger in Betracht ziehen.
  - Für die Kommunikation zwischen Ihrer Workload und IoT-Geräten sollten Sie die Verwendung von AWS IoT Core in Betracht ziehen. Dadurch stehen Ihnen mehrere Optionen für die Verschlüsselung und Authentifizierung des Netzwerkverkehrs zur Verfügung.
- Überwachung auf nicht autorisierten Zugriff: Überwachen Sie kontinuierlich unbeabsichtigte Kommunikationskanäle, nicht autorisierte Prinzipale, die versuchen, auf geschützte Ressourcen zuzugreifen, und andere unzulässige Zugriffsmuster.
  - Wenn Sie VPC Lattice zur Verwaltung des Zugriffs auf Ihre Services verwenden, empfiehlt es sich gegebenenfalls, die Zugriffsprotokolle von VPC Lattice zu aktivieren und zu überwachen. Diese Zugriffsprotokolle enthalten Informationen über die anfordernde Entität, Netzwerkinformationen einschließlich Quell- und Ziel-VPC sowie Metadaten der Anforderung.
  - Erwägen Sie die Aktivierung von VPC-Flow-Protokollen, um Metadaten zu Netzwerkflüssen zu erfassen und regelmäßig auf Anomalien zu überprüfen.

- Weitere Hinweise zum Planen, Simulieren und Reagieren auf Sicherheitsvorfälle finden Sie im AWS Security Incident Response Guide und im Abschnitt Vorfallreaktion der Säule „Sicherheit“ des AWS-Well-Architected-Framework.

Ressourcen

Zugehörige bewährte Methoden:

- SEC03-BP07 Analysieren des öffentlichen und kontoübergreifenden Zugriffs
- SEC02-BP02 Verwenden von temporären Anmeldeinformationen
- SEC01-BP07 Identifizieren von Bedrohungen und Priorisieren von Abhilfemaßnahmen unter Verwendung eines Bedrohungsmodells

Zugehörige Dokumente:

- Auswerten von Zugriffskontrollmethoden zum Schutz von Amazon-API-Gateway-APIs
- Konfigurieren der gegenseitigen TLS-Authentifizierung für eine REST-API
- Schützen von API-Gateway-HTTP-Endpunkten mit JWT-Genehmiger
- Autorisieren von direkten Aufrufen von AWS-Services mithilfe des AWS IoT Core-Anmeldeinformationsanbieters
- Leitfaden zur Reaktion auf Sicherheitsvorfälle in AWS

Zugehörige Videos:

- AWS re:invent 2022 – Vorstellung von VPC Lattice
- AWS re:invent 2020 – Serverlose API-Authentifizierung für HTTP-APIs in AWS

Zugehörige Beispiele:

- Workshop zu Amazon VPC Lattice
- Zero-Trust, Episode 1: Der Phantom-Service-Perimeter-Workshop

Vorfallreaktion

Auch bei ausgereiften präventiven und Erkennungskontrollen, sollte Ihr Unternehmen Verfahren etablieren, um auf Sicherheitsvorfälle reagieren und mögliche Auswirkungen mindern zu können. Ihre Vorbereitung wirkt sich stark auf die Fähigkeit Ihrer Teams aus, während eines Vorfalls effektiv zu arbeiten, Probleme zu isolieren, einzudämmen und forensisch zu untersuchen sowie den Betrieb in einem bekannten guten Zustand wiederherzustellen. Durch die Bereitstellung von Tools und Zugriff vor einem Sicherheitsvorfall und die routinemäßige Reaktion auf Vorfälle im Alltag können Sie sicherstellen, dass Sie eine Wiederherstellung durchführen und die Betriebsunterbrechung minimieren können.

Themen

Aspekte der Reaktion auf AWS-Vorfälle

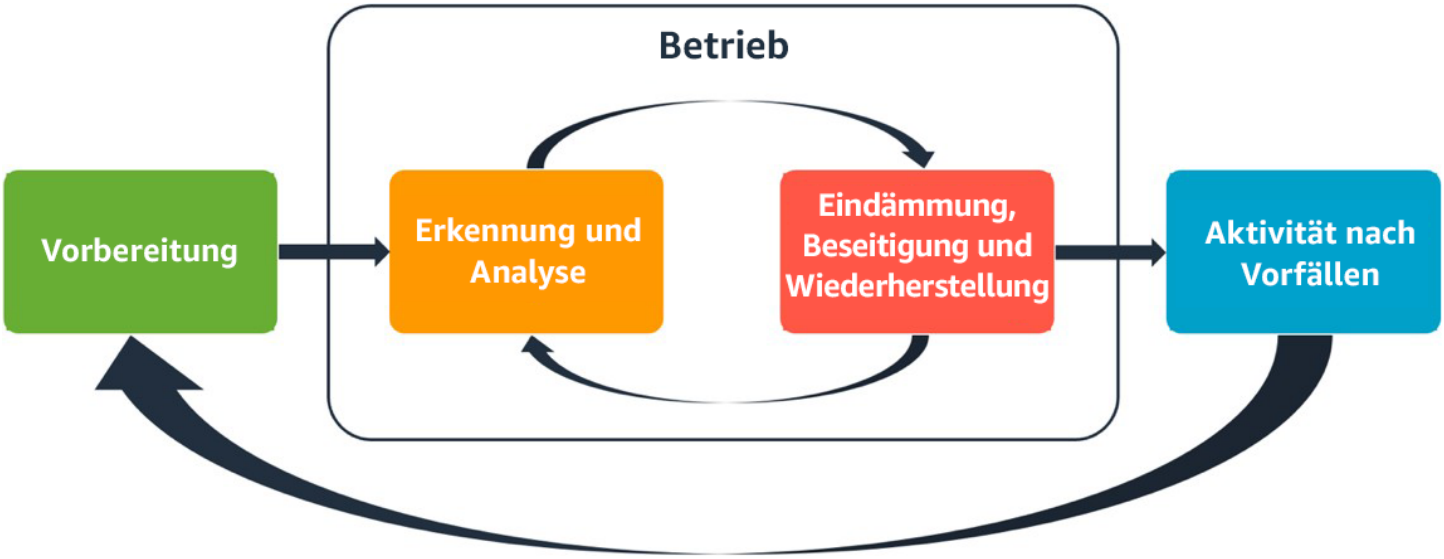
Alle AWS-Benutzer innerhalb einer Organisation sollten ein grundlegendes Verständnis der Prozesse zur Reaktion auf Sicherheitsvorfälle haben und das Sicherheitspersonal sollte wissen, wie auf Sicherheitsprobleme zu reagieren ist. Ausbildung, Schulung und Erfahrung sind für ein erfolgreiches Programm zur Reaktion auf Cloud-Vorfälle von entscheidender Bedeutung und werden idealerweise schon lange vor einem möglichen Sicherheitsvorfall implementiert. Die Grundlage für ein erfolgreiches Reaktionsprogramm für Cloud-Vorfälle bilden Vorbereitung, Betrieb und Aktivität nach Vorfällen.

Im Folgenden werden diese Aspekte genauer beschrieben:

- Vorbereitung: Bereiten Sie Ihr Vorfallreaktionsteam darauf vor, Vorfälle in AWS zu erkennen und darauf zu reagieren, indem Sie Erkennungsfunktionen aktivieren und einen angemessenen Zugriff auf die erforderlichen Tools und Cloud-Services gewährleisten. Bereiten Sie außerdem die erforderlichen Playbooks vor, sowohl manuell als auch automatisiert, um zuverlässige und konsistente Reaktionen auf Vorfälle zu gewährleisten.

- Betrieb: Reagieren Sie auf Sicherheitsereignisse und potenzielle Vorfälle gemäß den NIST-Reaktionsphasen: Erkennung, Analyse, Eindämmung, Beseitigung und Wiederherstellung.
- Aktivität nach Vorfällen: Analysieren Sie die Ergebnisse Ihrer Sicherheitsereignisse und Simulationen, um die Wirksamkeit Ihrer Maßnahmen zu verbessern, den Nutzen der Maßnahmen und Untersuchungen zu steigern und das Risiko weiter zu reduzieren. Sie müssen aus Vorfällen lernen und die Verantwortung für Verbesserungsmaßnahmen für klar definiert sein.

Das folgende Diagramm zeigt den Ablauf der Phasen gemäß dem zuvor erwähnten NIST-Lebenszyklus für die Reaktion auf Vorfälle. Hierbei umfasst der Betrieb Erkennung und Analyse sowie Eindämmung, Beseitigung und Wiederherstellung.



Aspekte der Reaktion auf AWS-Vorfälle

Designziele für die Reaktion auf Cloud-Vorfälle

Obwohl die allgemeinen Prozesse und Mechanismen der Reaktion auf Vorfälle, wie sie in NIST SP 800-61: Computer Security Incident Handling Guide definiert sind, bestehen bleiben, empfehlen wir Ihnen, diese spezifischen Designziele zu bewerten, die für die Reaktion auf Sicherheitsvorfälle in einer Cloud-Umgebung relevant sind:

- Festlegen von Reaktionszielen: Arbeiten Sie mit Interessenvertretern, dem Rechtsbeistand und der Leitung der Organisation zusammen, um das Ziel der Reaktion auf einen Vorfall zu ermitteln. Zu den gemeinsamen Zielen gehören die Eindämmung und Entschärfung des Problems, die Wiederherstellung der beschädigten Ressourcen, die Sicherung der Daten für die Forensik, die Wiederherstellung eines sicheren Betriebs und schließlich das Lernen aus Vorfällen.

- Reagieren mit der Cloud: Implementieren Sie Reaktionsmuster in der Cloud dort, wo das Ereignis und die Daten auftreten.
- Vorhandene und benötigte Informationen: Bewahren Sie Protokolle, Ressourcen, Snapshots und andere Beweise auf, indem Sie sie kopieren und in einem zentralen Cloud-Konto für die Vorfallreaktion speichern. Verwenden Sie Tags, Metadaten und Mechanismen, die Aufbewahrungsrichtlinien erzwingen. Sie müssen wissen, welche Services Sie verwenden, und dann die Anforderungen für die Untersuchung dieser Services ermitteln. Um Ihnen zu helfen, Ihre Umgebung zu verstehen, können Sie auch Tagging verwenden.
- Verwenden von Wiederbereitstellungsmechanismen: Wenn eine Sicherheitsanomalie auf eine falsche Konfiguration zurückzuführen ist, kann die Behebung so einfach sein wie das Entfernen der Abweichung durch die erneute Bereitstellung der Ressourcen mit der richtigen Konfiguration. Wenn eine mögliche Gefährdung festgestellt wird, muss sichergestellt werden, dass die erneute Bereitstellung eine erfolgreiche und überprüfte Beseitigung der Ursachen beinhaltet.
- Automatisieren wo möglich: Wenn Probleme auftreten oder Vorfälle sich wiederholen, erstellen Sie Mechanismen, die programmgesteuert Tests durchführen und auf gängige Ereignisse reagieren. Setzen Sie Mitarbeiter ein, wenn auf einzigartige, komplexe oder sensible Vorfälle reagiert werden muss, bei denen Automatisierungen unzureichend sind.
- Auswahl skalierbarer Lösungen: Streben Sie an, die Skalierbarkeit des Cloud-Computing-Ansatzes Ihrer Organisation zu erreichen. Implementieren Sie Erkennungs- und Reaktionsmechanismen, die sich in Ihren Umgebungen skalieren lassen, um die Zeit zwischen Erkennung und Reaktion effektiv zu reduzieren.
- Analyse und Verbessern des Prozesses: Identifizieren Sie proaktiv Sicherheitslücken bei Ihren Prozessen, Tools oder Mitarbeitern und implementieren Sie einen Plan, um diese zu beheben. Simulationen sind eine sichere Methode, um Lücken aufzudecken und Prozesse zu verbessern.

Diese Entwurfsziele sollen als Erinnerung daran dienen, Ihre Architekturimplementierung daraufhin zu überprüfen, ob sie sowohl zur Reaktion auf Vorfälle als auch zur Bedrohungserkennung in der Lage ist. Denken Sie bei der Planung Ihrer Cloud-Implementierungen daran, wie auf einen Vorfall reagiert werden soll, idealerweise mit einer forensisch fundierten Reaktionsmethodik. In einigen Fällen bedeutet dies, dass Sie möglicherweise mehrere Organisationen, Konten und Tools verwenden, die speziell für diese Reaktionsaufgaben eingerichtet wurden. Diese Tools und Funktionen sollten der für Vorfälle verantwortlichen Person über die Bereitstellungspipeline zur Verfügung gestellt werden. Sie sollten nicht statisch sein, da dies zu einem größeren Risiko führen kann.

Vorbereitung

Die Vorbereitung auf einen Vorfall ist entscheidend für eine zeitnahe und effektive Reaktion im Ernstfall. Die Vorbereitung erfolgt in drei Bereichen:

- Personen: Um Ihre Mitarbeiter auf einen Sicherheitsvorfall vorzubereiten, müssen Sie die für die Reaktion auf Vorfälle relevanten Personen identifizieren und sie in den Bereichen Vorfallreaktion und Cloud-Technologien schulen.
- Prozess: Zur Vorbereitung Ihrer Prozesse auf einen Sicherheitsvorfall müssen Sie Architekturen dokumentieren, detaillierte Pläne zur Reaktion auf Vorfälle entwickeln und Playbooks für eine einheitliche Reaktion auf Sicherheitsereignisse erstellen.
- Technologie: Um Ihre Technologie auf einen Sicherheitsvorfall vorzubereiten, müssen Sie den Zugriff einrichten, die erforderlichen Protokolle erfassen und überwachen, effektive Warnmechanismen implementieren und Reaktions- und Ermittlungsfunktionen entwickeln.

Jeder dieser Bereiche ist für eine effektive Reaktion auf Vorfälle gleichermaßen wichtig. Ohne alle drei ist kein Vorfallreaktionsprogramm vollständig oder wirksam. Die Vorbereitung von Mitarbeitern, Prozessen und Technologien muss eng ineinandergreifen, um auf einen Vorfall vorbereitet zu sein.

Bewährte Methoden

- SEC10-BP01 Identifizieren wichtiger Mitarbeiter und externer Ressourcen
- SEC10-BP02 Entwickeln von Vorfallmanagementplänen
- SEC10-BP03 Vorbereiten forensischer Funktionen
- SEC10-BP04 Entwickeln und Testen von Playbooks für die Reaktion auf Sicherheitsvorfälle
- SEC10-BP05 Vorab bereitgestellter Zugriff
- SEC10-BP06 Vorabbereitstellen von Tools
- SEC10-BP07 Durchführen von Simulationen

SEC10-BP01 Identifizieren wichtiger Mitarbeiter und externer Ressourcen

Identifizieren Sie internes und externes Personal, Ressourcen und rechtliche Anforderungen, um Ihre Organisation bei der Reaktion auf einen Vorfall zu unterstützen.

Gewünschtes Ergebnis: Sie verfügen über eine Liste mit den wichtigsten Mitarbeitern, ihren Kontaktinformationen und ihrer Rolle bei der Reaktion auf ein Sicherheitsereignis. Sie überprüfen

diese Informationen regelmäßig und aktualisieren sie, um personelle Veränderungen aus Sicht der internen und externen Tools zu berücksichtigen. Bei der Dokumentation dieser Informationen berücksichtigen Sie alle Drittanbieter und Dienstleister, einschließlich Sicherheitspartnern, Cloud-Anbietern und Software as a Service (SaaS)-Anwendungen. Während eines Sicherheitsereignisses stehen Mitarbeiter mit dem entsprechenden Maß an Verantwortung, Kontext und Zugriff zur Verfügung, um zu reagieren und das Ereignis zu bewältigen.

Typische Anti-Muster:

- Fehlen einer aktualisierten Liste der wichtigsten Mitarbeiter mit Kontaktinformationen, ihren Aufgaben und ihren Verantwortlichkeiten bei der Reaktion auf Sicherheitsvorfälle
- Voraussetzen, dass jeder die Personen, die Abhängigkeiten, die Infrastruktur und die Lösungen bei der Reaktion auf ein Ereignis und bei der Bewältigung eines Ereignisses versteht
- Fehlen eines Dokuments oder eines Wissens-Repositorys, das die wichtigsten Infrastruktur- oder Anwendungsdesigns darstellt
- Fehlen von angemessenen Einarbeitungsprozessen für neue Mitarbeiter, um effektiv zur Reaktion auf ein Sicherheitsereignis beizutragen (etwa die Durchführung von Ereignissimulationen)
- Fehlen eines Eskalationspfads für den Fall, dass wichtige Mitarbeiter vorübergehend nicht verfügbar sind oder bei Sicherheitsereignissen nicht reagieren

Vorteile der Nutzung dieser bewährten Methode Diese Praxis reduziert die Triage- und Reaktionszeit, die für die Identifizierung der richtigen Mitarbeiter und ihrer Rollen während eines Ereignisses aufgewendet wird. Minimieren Sie Zeitverluste während eines Ereignisses, indem Sie eine aktualisierte Liste der wichtigsten Mitarbeiter und ihrer Rollen führen, damit Sie die richtigen Personen für die Triage und die Bewältigung eines Ereignisses einsetzen können.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Identifizieren Sie wichtige Personen in Ihrer Organisation: Führen Sie eine Kontaktliste der Personen in Ihrer Organisation, die Sie einbeziehen müssen. Überprüfen und aktualisieren Sie diese Informationen regelmäßig bei personellen Veränderungen wie organisatorischen Änderungen, Beförderungen und Teamwechseln. Dies ist besonders wichtig für Schlüsselpositionen wie Incident Manager, Incident Responder und Communications Lead.

- Incident Manager: Incident Managers haben die Gesamtverantwortung für die Reaktion auf das Ereignis.

- Incident Responder: Incident Responders sind für Untersuchungen und Abhilfemaßnahmen zuständig. Diese Personen können sich je nach Art des Ereignisses unterscheiden, sind aber in der Regel Entwickler und Betriebs-Teams, die für die betroffene Anwendung verantwortlich sind.
- Communications Lead: Communications Leads sind für die interne und externe Kommunikation verantwortlich, insbesondere mit Behörden, Regulierungsbehörden und Kunden.
- Onboarding-Prozess: Führen Sie regelmäßige Schulungen und ein Onboarding für neue Mitarbeiter durch, um ihnen die notwendigen Fähigkeiten und Kenntnisse zu vermitteln, damit sie effektiv bei der Reaktion auf Vorfälle mitwirken können. Integrieren Sie Simulationen und praktische Übungen in den Onboarding-Prozess, damit sie besser vorbereitet sind.
- Fachexperten (Subject Matter Experts, SMEs): Im Falle von verteilten und autonomen Teams empfehlen wir Ihnen, für geschäftskritische Workloads SMEs zu bestimmen. Sie bieten Einblicke in den Betrieb und die Datenklassifizierung von kritischen Workloads, die an dem Ereignis beteiligt sind.

Beispieltabellenformat:

```
  | Role | Name | Contact Information | Responsibilities |
1 | ——- | ——- | ——- | ——- |
2 | Incident Manager | Jane Doe| jane.doe@example.com | Overall authority during
 response |
3 | Incident Responder | John Smith | john.smith@example.com | Investigation and
 remediation |
4 | Communications Lead | Emily Johnson | emily.johnson@example.com | Internal and
 external communications |
5 | Communications Lead | Michael Brown | michael.brown@example.com | Insights on
 critical workloads |
```

Erwägen Sie die Verwendung des Features AWS Systems Manager Incident Manager, um wichtige Kontakte zu erfassen, einen Reaktionsplan zu definieren, Bereitschaftspläne zu automatisieren und Eskalationspläne zu erstellen. Automatisieren und rotieren Sie alle Mitarbeiter durch einen Bereitschaftsdienstplan, sodass die Verantwortung für die Workload auf alle zuständigen Personen verteilt wird. Dies fördert gute Praktiken wie die Ausgabe relevanter Metriken und Protokolle sowie die Definition von Alarmschwellen, die für die Workload von Bedeutung sind.

Identifizieren Sie externe Partner: Unternehmen nutzen Tools, die von unabhängigen Softwareanbietern (ISVs), Partnern und Subunternehmern entwickelt wurden, um differenzierte Lösungen für ihre Kunden zu erstellen. Binden Sie wichtige Mitarbeiter dieser Parteien ein, die Ihnen bei der Reaktion auf einen Vorfall und bei dessen Bewältigung helfen können. Wir empfehlen Ihnen,

sich für die entsprechende Stufe von Support anzumelden, um über einen Supportfall sofortigen Zugang zu AWS -Fachexperten zu erhalten. Erwägen Sie, ähnliche Vereinbarungen mit allen Anbietern kritischer Lösungen für die Workloads zu schließen. Einige Sicherheitsereignisse machen es erforderlich, dass börsennotierte Unternehmen die zuständigen Behörden und Aufsichtsbehörden über das Ereignis und dessen Auswirkungen informieren. Pflegen und aktualisieren Sie die Kontaktinformationen der relevanten Abteilungen und der zuständigen Personen.

Implementierungsschritte

1. Richten Sie eine Lösung für das Vorfallmanagement ein.
   a. Erwägen Sie die Bereitstellung von Incident Manager in Ihrem Security-Tooling-Konto.
2. Definieren Sie Kontakte in Ihrer Lösung für das Vorfallmanagement.
   a. Definieren Sie für jeden Kontakt mindestens zwei Arten von Kontaktkanälen (z. B. SMS, Telefon oder E-Mail), um die Erreichbarkeit während eines Vorfalls sicherzustellen.
3. Definieren Sie einen Reaktionsplan.
   a. Ermitteln Sie die am besten geeigneten Ansprechpartner für einen Vorfall. Definieren Sie Eskalationspläne, die sich an den Rollen der einzuschaltenden Mitarbeiter orientieren (und nicht an einzelnen Ansprechpartnern). Erwägen Sie die Aufnahme von Kontakten, die gegebenenfalls für die Benachrichtigung externer Stellen zuständig sind, auch wenn diese nicht direkt an der Lösung des Vorfalls beteiligt sind.

Ressourcen

Zugehörige bewährte Methoden:

- OPS02-BP03 Betriebsaktivitäten haben feste Besitzer, die für ihre Leistung verantwortlich sind

Zugehörige Dokumente:

- AWS Security Incident Response Guide

Zugehörige Beispiele:

- AWS Customer Playbook Framework
- Vorbereiten und Reagieren auf Sicherheitsvorfälle in Ihrer AWS-Umgebung

Zugehörige Tools:

- AWS Systems Manager Incident Manager

Zugehörige Videos:

- Der Sicherheitsansatz von Amazon bei der Entwicklung

SEC10-BP02 Entwickeln von Vorfallmanagementplänen

Das erste Dokument, das für die Vorfallreaktion entwickelt werden muss, ist der Vorfallreaktionsplan. Der Vorfallreaktionsplan ist als Grundlage für Ihr Vorfallreaktionsprogramm und Ihre Vorfallreaktionsstrategie konzipiert.

Vorteile der Nutzung dieser bewährten Methode: Die Entwicklung durchdachter und klar definierter Prozesse zur Vorfallreaktion ist der Schlüssel zu einem erfolgreichen und skalierbaren Vorfallreaktionsprogramm. Wenn ein Sicherheitsereignis eintritt, können Ihnen klare Schritte und Workflows dabei helfen, rechtzeitig zu reagieren. Möglicherweise verfügen Sie bereits über Prozesse zur Vorfallreaktion. Unabhängig von Ihrem aktuellen Status ist es wichtig, Ihre Prozesse zur Vorfallreaktion regelmäßig zu aktualisieren, zu wiederholen und zu testen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Ein Vorfallmanagementplan ist von entscheidender Bedeutung, um auf Sicherheitsvorfälle zu reagieren, sie einzudämmen und ihre potenziellen Folgen zu beheben. Ein Vorfallmanagementplan ist ein strukturierter Prozess für die Identifizierung und Behebung von Sicherheitsvorfällen sowie die zeitnahe Reaktion darauf.

In der Cloud gibt es viele der betrieblichen Rollen und Anforderungen, die auch für eine On-Premises-Umgebung typisch sind. Beim Erstellen eines Plans für das Vorfallmanagement ist es wichtig, Reaktions- und Wiederherstellungsstrategien zu entwickeln, die Ihren Anforderungen an geschäftliche Ergebnisse und Compliance optimal entsprechen. Wenn Sie beispielsweise Workloads in AWS ausführen, die in den USA FedRAMP-konform sind, sollten Sie die Empfehlungen im NIST SP 800-61 Computer Security Handling Guide befolgen. Ähnlich gilt bei der Ausführung von Workloads, die persönlich identifizierbare Informationen (PII) speichern, dass Sie diese schützen und auf Probleme im Zusammenhang mit Datenresidenz und Verwendung von Daten reagierren müssen.

Wenn Sie einen Vorfallmanagementplan für Ihre Workloads in AWS erstellen, beginnen Sie mit dem AWS-Modell der geteilten Verantwortung zum Aufbau eines durchdachten Verteidigungskonzepts für die Vorfallreaktion. In diesem Modell kümmert sich AWS um die Sicherheit der Cloud und Sie sind für die Sicherheit in der Cloud verantwortlich. Das bedeutet, dass Sie die Kontrolle behalten und für die Sicherheitskontrollen verantwortlich sind, für deren Implementierung Sie sich entscheiden. Der Leitfaden für AWS Security Incident Response enthält zentrale Konzepte und grundlegende Anleitungen für den Aufbau eines Cloud-basierten Vorfallmanagementplans.

Ein effektiver Vorfallmanagementplan muss kontinuierlich durchlaufen und stets an die Ziele Ihrer Cloud-Operationen angepasst werden. Erwägen Sie die Verwendung der nachfolgend erläuterten Implementierungspläne für die Erstellung und Weiterentwicklung Ihres Vorfallmanagementplans.

Implementierungsschritte

1. Definieren Sie Rollen und Verantwortlichkeiten innerhalb Ihrer Organisation für den Umgang mit Sicherheitsereignissen. Daran sollten Vertreter verschiedener Bereiche beteiligt sein, darunter:
   - Personalabteilung (HR)
   - Führungsteam
   - Rechtsabteilung
   - Besitzer und Entwickler von Anwendungen (fachliche Experten)
2. Beschreiben Sie klar, welche Personen bei einem Vorfall verantwortlich sind, Rechenschaft geben müssen, konsultiert werden müssen und informiert werden müssen (Responsibile, Accountable, Consulted, Informed, RACI). Erstellen Sie ein RACI-Diagramm, um eine schnelle und direkte Kommunikation zu unterstützen, und beschreiben Sie klar die Personen, die während der verschiedenen Phasen eines Ereignisses die Leitung haben.
3. Binden Sie während eines Vorfalls Anwendungsbesitzer und Entwickler (fachliche Experten) ein, da sie wertvolle Informationen und Kontext bereitstellen können, um die Auswirkungen messen zu können. Entwickeln Sie Beziehungen zu diesen fachlichen Experten und üben Sie mit ihnen Szenarien für die Vorfallreaktion, bevor es zu einem tatsächlichen Vorfall kommt.
4. Binden Sie vertrauenswürdige Partner oder externe Experten in das Untersuchungs- oder Reaktionsverfahren ein, da sie zusätzliche Kenntnisse und Perspektiven bereitstellen können.
5. Passen Sie Ihre Pläne und Rollen für das Vorfallmanagement an lokale Vorschriften oder Compliance-Anforderungen an, denen Ihre Organisation unterliegt.
6. Üben und testen Sie Ihre Pläne für die Vorfallreaktion regelmäßig und beziehen Sie alle definierten Rollen und Verantwortlichkeiten ein. Auf diese Weise können Sie den Prozess rationalisieren und sicherstellen, dass Sie koordiniert und effizient auf Sicherheitsvorfälle reagieren.

7. Überprüfen und aktualisieren Sie Rollen, Verantwortlichkeiten und RACI-Diagramm regelmäßig oder bei Änderungen von Organisationsstruktur oder Anforderungen.

Die AWS-Reaktionsteams und der Support

- AWS Support
  - Support bietet eine Reihe an Plänen, die den Zugriff auf Tools und das Know-how für den Erfolg und den betriebsbereiten Zustand der AWS-Lösungen ermöglichen. Wenn Sie technischen Support und weitere Ressourcen benötigen, um Ihre AWS-Umgebung zu planen, bereitzustellen und zu optimieren, können Sie einen Supportplan auswählen, der am besten zu Ihrem AWS-Anwendungsfall passt.
  - Das Support-Center in der AWS-Managementkonsole (Anmeldung erforderlich) ist Ihre zentrale Anlaufstelle, um Unterstützung bei Problemen zu erhalten, die sich auf Ihre AWS-Ressourcen auswirken. Der Zugriff auf den Support wird über AWS Identity and Access Management gesteuert. Weitere Informationen zum Zugriff auf Support-Funktionen finden Sie unter Erste Schritte mit Support.
- AWS Kundenvorfallreaktionsteam (CIRT)
  - Das AWS-Kundenvorfallreaktionsteam (CIRT) ist ein spezialisiertes globales, rund um die Uhr verfügbares AWS-Team, das Kunden bei aktiven Sicherheitsereignissen auf Kundenseite des AWS-Modells der geteilten Verantwortung unterstützt.
  - Wenn das AWS-CIRT Sie unterstützt, bietet es Hilfe bei der Fehlererkennung und Wiederherstellung eines aktiven Sicherheitsereignisses in AWS an. Sie können mithilfe von AWS-Service-Protokollen bei der Ursachenanalyse helfen und Ihnen Empfehlungen für die Wiederherstellung geben. Sie können Ihnen auch Sicherheitsempfehlungen und bewährte Methoden an die Hand geben, mit denen Sie Sicherheitsereignisse in Zukunft vermeiden können.
  - AWS-Kunden können das AWS-CIRT über einen Support-Fall einbinden.
- AWS Security Incident Response
  - AWS Security Incident Response wurde auf der re:Invent 2024 angekündigt, ein verwalteter Service zur Reaktion auf Sicherheitsvorfälle, der sowohl moderne Triage-Technologie als auch HITL nutzt. Der Service nimmt alle Ergebnisse von GuardDuty und alle Ergebnisse Dritter auf, die an AWS Security Hub CSPM zur Triage gesendet wurden, um den Kunden nur über Ergebnisse zu informieren, die einer Untersuchung bedürfen. Der Service bietet auch ein Portal, über das reaktive Fälle eingereicht werden können, falls der Kunde ein Sicherheitsereignis

bemerkt, und Unterstützung durch das Advanced Incident Response Team von AWS angefordert werden kann.

- Unterstützung für DDoS-Reaktion
  - AWS bietet AWS Shield, das einen verwalteten Distributed Denial of Service (DDoS)-Schutz-Service bereitstellt, der in AWS ausgeführte Web-Anwendungen schützt. Shield bietet eine ständig aktive Erkennung und automatische Inline-Schutzmaßnahmen, mit denen Ausfallzeiten und Latenz von Anwendungen minimiert werden können. Sie müssen also nicht Support kontaktieren, um vom DDoS-Schutz zu profitieren. Shield umfasst zwei Stufen: AWS Shield Standard und AWS Shield Advanced. Weitere Informationen zu den Unterschieden zwischen diesen beiden Stufen finden Sie in der Shield-Funktionsdokumentation.
- AWS Managed Services (AMS)
  - AWS Managed Services (AMS) stellt eine fortlaufende Verwaltung Ihrer AWS-Infrastruktur bereit, damit Sie sich auf Ihre Anwendungen konzentrieren können. AMS trägt durch eine Implementierung bewährter Methoden zur Verwaltung Ihrer Infrastruktur dazu bei, den Betriebsaufwand zu reduzieren und das Risiko zu senken. Außerdem automatisiert AMS häufige Aktivitäten wie Änderungsanforderungen, Überwachung, Patch-Verwaltung, Sicherheit sowie Backup-Services und bietet während der gesamten Lebensdauer Services zum Bereitstellen, Ausführen und Unterstützen Ihrer Infrastruktur.
  - AMS übernimmt die Verantwortung für die Bereitstellung einer Reihe von Sicherheitskontrollen und bietet rund um die Uhr Erstreaktion auf Warnungen an. Wenn eine Warnung ausgelöst wird, folgt AMS einer Reihe automatisierter und manueller Standard-Playbooks, um eine konsistente Reaktion zu gewährleisten. Diese Playbooks werden den AMS-Kunden während des Onboardings zur Verfügung gestellt, damit sie eine Reaktion entwickeln und mit AMS abstimmen können.

Erstellen des Vorfallreaktionsplans

Der Vorfallreaktionsplan ist als Grundlage für Ihr Vorfallreaktionsprogramm und Ihre Vorfallreaktionsstrategie konzipiert. Er sollte immer formell schriftlich festgehalten werden. Ein Vorfallreaktionsplan enthält in der Regel folgende Abschnitte:

- Überblick über das Vorfallreaktionsteam: Enthält die Ziele und Funktionen des Vorfallreaktionsteams.
- Rollen und Zuständigkeiten: Hier werden die für die Vorfallreaktion zuständigen Stakeholder aufgeführt und ihre Rollen im Falle eines Vorfalls beschrieben.

- Kommunikationsplan: Enthält Kontaktinformationen und gibt an, wie Sie während eines Vorfalls kommunizieren.
- Alternative Kommunikationsmethoden: Es hat sich bewährt, Out-of-Band-Kommunikation als Alternative für die Kommunikation bei Vorfällen zu verwenden. Ein Beispiel für eine Anwendung, die einen sicheren Out-of-Band-Kommunikationskanal bereitstellt, ist AWS Wickr.
- Phasen der Vorfallreaktion und zu ergreifende Maßnahmen: Hier sind die Phasen der Vorfallreaktion aufgeführt (beispielsweise Erkennung, Analyse, Beseitigung, Eindämmung und Wiederherstellung) – einschließlich der in diesen Phasen zu ergreifenden allgemeinen Maßnahmen.
- Definitionen des Schweregrads und der Priorisierung des Vorfalls: Hier wird erläutert, wie der Schweregrad eines Vorfalls klassifiziert wird, wie der Vorfall priorisiert wird und wie sich die Schweregraddefinitionen dann auf die Eskalationsverfahren auswirken.

Diese Abschnitte sind zwar in Unternehmen verschiedener Größen und Branchen üblich, der Vorfallreaktionsplan ist jedoch für jede Organisation individuell. Erstellen Sie einen Vorfallreaktionsplan, der für Ihre Organisation am besten geeignet ist.

Ressourcen

Zugehörige bewährte Methoden:

- SEC04 Erkennung

Zugehörige Dokumente:

- Leitfaden zur Reaktion auf Sicherheitsvorfälle in AWS
- NIST: Computer Security Incident Handling Guide

SEC10-BP03 Vorbereiten forensischer Funktionen

Bevor es zu einem Sicherheitsvorfall kommt, empfiehlt es sich gegebenenfalls, forensische Funktionen zur Unterstützung der Untersuchung von Sicherheitsereignissen zu entwickeln.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Konzepte aus der traditionellen On-Premises-Forensik gelten auch für AWS. Wichtige Informationen für den Einstieg in den Aufbau forensischer Funktionen in der AWS Cloud finden Sie in den Strategien für forensische Untersuchungsumgebungen in der AWS Cloud.

Nachdem Sie Ihre Umgebung und AWS-Konto-Struktur für die Forensik eingerichtet haben, können Sie die Technologien definieren, die für eine effektive Anwendung forensisch fundierter Methoden in den vier Phasen erforderlich sind:

- Sammlung: Erfassen Sie relevante AWS-Protokolle wie AWS CloudTrail, AWS Config, VPC Flow Logs und Protokolle auf Host-Ebene. Erfassen Sie Snapshots, Backups und Speicherabbilder der betroffenen AWS-Ressourcen, sofern verfügbar.
- Prüfung: Prüfen Sie die erfassten Daten, indem Sie die relevanten Informationen extrahieren und bewerten.
- Analyse: Analysieren Sie die erfassten Daten, um den Vorfall zu verstehen und Schlüsse daraus zu ziehen.
- Berichterstellung: Präsentieren Sie die Informationen, die sich aus der Analysephase ergeben.

Implementierungsschritte

Vorbereiten Ihrer forensischen Umgebung

AWS Organizations hilft Ihnen bei der zentralen Verwaltung und Steuerung einer AWS-Umgebung, während Sie AWS-Ressourcen erweitern und skalieren. Eine AWS-Organisation konsolidiert Ihre AWS-Konten, sodass Sie sie als eine einzige Einheit verwalten können. Mithilfe von Organisationseinheiten können Sie Konten gruppieren und als eine Einheit verwalten.

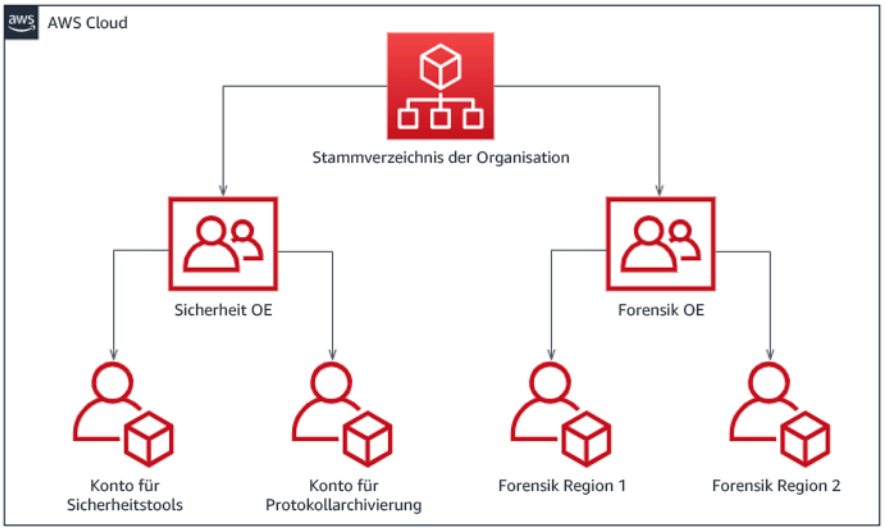
Für die Reaktion auf Vorfälle ist es hilfreich, über eine AWS-Konto-Struktur zu verfügen, die die Funktionen der Vorfallreaktion unterstützt. Dazu gehören eine sicherheitsbezogene Organisationseinheit und eine forensische Organisationseinheit. Innerhalb der sicherheitsbezogenen Organisationseinheit sollten Sie über Konten für Folgendes verfügen:

- Protokollarchivierung: Aggregieren Sie Protokolle in einem für die Protokollarchivierung vorgesehenen AWS-Konto mit eingeschränkten Berechtigungen.
- Sicherheits-Tools: Zentralisieren Sie Sicherheits-Services in einem AWS-Konto für Sicherheitstools. Dieses Konto fungiert als delegierter Administrator für Sicherheits-Services.

Innerhalb der forensischen Organisationseinheit haben Sie die Möglichkeit, für jede Region, in der Sie tätig sind, eines oder mehrere forensische Konten zu implementieren, je nachdem, was für Ihr Geschäfts- und Betriebsmodell am besten geeignet ist. Wenn Sie ein forensisches Konto pro Region erstellen, können Sie die Erstellung von AWS-Ressourcen außerhalb dieser Region blockieren und so das Risiko verringern, dass Ressourcen in eine unbeabsichtigte Region kopiert werden. Wenn Sie beispielsweise nur in den Regionen „USA Ost (Nord-Virginia)“ (`us-east-1`) und „USA West (Oregon)“ (`us-west-2`) aktiv sind, würde die forensische Organisationseinheit zwei Konten umfassen: eins für `us-east-1` und eins für `us-west-2`.

Sie können ein forensisches AWS-Konto für mehrere Regionen erstellen. Achten Sie darauf, dass Sie Ihre Anforderungen an die Datensouveränität einhalten, wenn Sie AWS-Ressourcen in dieses Konto kopieren. Da die Bereitstellung neuer Konten etwas dauert, ist es unerlässlich, die forensischen Konten rechtzeitig vor einem Vorfall einzurichten und zu instrumentieren, damit die Notfallteams vorbereitet sind und sie effektiv nutzen können.

Das folgende Diagramm zeigt eine Beispiel-Kontenstruktur mit einer forensischen Organisationseinheit mit regionsspezifischen forensischen Konten:



Regionsspezifische Kontenstruktur für die Reaktion auf Vorfälle

Erfassen von Backups und Snapshots

Die Einrichtung von Backups wichtiger Systeme und Datenbanken ist für die Wiederherstellung nach einem Sicherheitsvorfall und für forensische Zwecke von entscheidender Bedeutung. Mit vorhandenen Backups können Sie Ihre Systeme wieder in einen vorherigen sicheren Zustand versetzen. In AWS können Sie Snapshots von verschiedenen Ressourcen erstellen. Snapshots bieten Ihnen zeitpunktbezogene Backups dieser Ressourcen. Es gibt viele AWS-Services, die Sie

beim Backup und der Wiederherstellung unterstützen können. Einzelheiten zu diesen Services und Ansätzen für Backup und Wiederherstellung finden Sie unter Präskriptive Leitlinien für Backup und Wiederherstellung sowie unter Verwendung von Backups zur Wiederherstellung nach Sicherheitsvorfällen.

Vor allem, wenn es um Situationen wie Ransomware geht, ist es wichtig, dass Ihre Backups gut geschützt sind. Hinweise zum Schutz Ihrer Backups finden Sie in den 10 besten Sicherheitsmethoden zum Schutz von Backups in AWS. Zusätzlich zum Schutz Ihrer Backups sollten Sie Ihre Backup- und Wiederherstellungsprozesse regelmäßig testen, um sicherzustellen, dass die vorhandenen Technologien und Prozesse wie erwartet funktionieren.

Automatisieren der Forensik

Während eines Sicherheitsereignisses muss Ihr Vorfallreaktionsteam in der Lage sein, schnell Nachweise zu sammeln und zu analysieren und gleichzeitig die Genauigkeit für den Zeitraum rund um das Ereignis aufrechtzuerhalten (beispielsweise durch Erfassen von Protokollen zu einem bestimmten Ereignis oder einer bestimmten Ressource oder durch Erfassen von Speicherabbildern einer Amazon-EC2-Instance). Für das Vorfallreaktionsteam ist es sowohl schwierig als auch zeitaufwändig, die relevanten Nachweise manuell zu erfassen, insbesondere bei einer großen Anzahl von Instances und Konten. Darüber hinaus kann die manuelle Erfassung anfällig für menschliche Fehler sein. Daher sollten Sie die Automatisierung für die Forensik so weit wie möglich entwickeln und implementieren.

AWS bietet eine Reihe von Automatisierungsressourcen für die Forensik, die weiter unten im Abschnitt „Ressourcen“ aufgeführt sind. Diese Ressourcen sind Beispiele für forensische Muster, die von entwickelt und von Kunden implementiert wurden. Obwohl sie für den Anfang eine nützliche Referenzarchitektur sein können, sollten Sie erwägen, sie zu ändern oder neue forensische Automatisierungsmuster zu erstellen, die auf Ihrer Umgebung, Ihren Anforderungen, Tools und forensischen Prozessen basieren.

Ressourcen

Zugehörige Dokumente:

- Leitfaden zur Reaktion auf Sicherheitsvorfälle in AWS: Entwickeln forensischer Funktionen
- Leitfaden zur Reaktion auf Sicherheitsvorfälle in AWS: Forensische Ressourcen
- Strategien für forensische Untersuchungsumgebungen in der AWS Cloud
- Automatisieren der forensischen Datenträgererfassung in AWS
- Präskriptive AWS-Anleitung: Automatisieren der Vorfallreaktion und Forensik

Zugehörige Videos:

- Automatisieren der Vorfallreaktion und Forensik

Zugehörige Beispiele:

- Framework für die automatisierte Reaktion auf Vorfälle und für die Forensik
- Automatisierter forensischer Orchestrator für Amazon EC2

SEC10-BP04 Entwickeln und Testen von Playbooks für die Reaktion auf Sicherheitsvorfälle

Ein wichtiger Teil der Vorbereitung Ihrer Prozesse zur Vorfallreaktion ist die Entwicklung von Playbooks. Playbooks für die Vorfallreaktion enthalten präskriptive Anleitungen und Schritte, die Sie ausführen sollten, wenn ein Sicherheitsereignis eintritt. Eine klare Struktur und klare Schritte vereinfachen die Reaktion und verringern die Wahrscheinlichkeit menschlicher Fehler.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Playbooks sollten für Vorfallszenarien wie die folgenden erstellt werden:

- Erwartete Vorfälle: Sie sollten Playbooks für zu erwartende Vorfälle erstellen. Dazu gehören Bedrohungen wie Denial of Service (DoS), Ransomware und die Kompromittierung von Anmeldeinformationen.
- Bekannte Sicherheitserkenntnisse oder Warnungen: Sie sollten Playbooks für bekannte Sicherheitserkenntnisse und Warnungen erstellen, z. B. aus Amazon GuardDuty. Wenn Sie eine GuardDuty-Erkenntnis erhalten, sollte das Playbook klare Schritte beschreiben, um zu verhindern, dass die Warnung falsch behandelt oder ignoriert wird. Weitere Informationen und Anleitungen zur Behebung finden Sie unter Beheben von Sicherheitsproblemen, die von GuardDuty entdeckt wurden.

Playbooks sollten technische Schritte enthalten, die ein Sicherheitsanalyst ausführen muss, um einen potenziellen Sicherheitsvorfall angemessen zu untersuchen und darauf zu reagieren.

Das Customer Incident Response Team (CIRT) von AWS hat ein GitHub-Repository mit Playbooks zur Reaktion auf Vorfälle veröffentlicht, die nach Bedrohungsszenario, Typ und Ressource geordnet

sind. Diese Playbooks können an Ihre bestehenden Verfahren zur Reaktion auf Vorfälle angepasst werden oder als Grundlage für die Entwicklung neuer Verfahren dienen.

Implementierungsschritte

Zu den Elementen, die in ein Playbook aufgenommen werden sollten, gehören:

- Playbook-Übersicht: Welches Risiko- oder Vorfallszenario behandelt dieses Playbook? Was ist das Ziel des Playbooks?
- Voraussetzungen: Welche Protokolle, Erkennungsmechanismen und automatisierten Tools sind für dieses Vorfallszenario erforderlich? Wie lautet die erwartete Benachrichtigung?
- Kommunikations- und Eskalationsinformationen: Wer ist beteiligt und wie lauten die Kontaktinformationen? Welche Aufgaben haben die einzelnen Stakeholder?
- Reaktionsschritte: Welche taktischen Maßnahmen sollten in den einzelnen Phasen der Vorfallreaktion ergriffen werden? Welche Abfragen sollte ein Analyst ausführen? Welcher Code sollte ausgeführt werden, um das gewünschte Ergebnis zu erzielen?
  - Erkennen: Wie wird der Vorfall erkannt?
  - Analysieren: Wie wird der Umfang der Auswirkungen bestimmt?
  - Eindämmen: Wie wird der Vorfall isoliert, um den Umfang zu begrenzen?
  - Beseitigen: Wie wird die Bedrohung aus der Umgebung entfernt?
  - Wiederherstellen: Wie wird das betroffene System oder die betroffene Ressource wieder in der Produktion bereitgestellt?
- Erwartete Ergebnisse: Was ist das erwartete Ergebnis des Playbooks, nachdem Abfragen und Code ausgeführt wurden?

Ressourcen

Zugehörige bewährte Methoden für Well-Architected:

- SEC10-BP02 Entwickeln von Vorfallmanagementplänen

Zugehörige Dokumente:

- Framework für Playbooks für die Vorfallreaktion
- Entwickeln eigener Playbooks für die Vorfallreaktion
- Exemplarische Playbooks für die Vorfallreaktion

- Entwicklung eines Runbooks für die Vorfallreaktion in AWS mit Jupyter Playbooks und CloudTrail Lake

SEC10-BP05 Vorab bereitgestellter Zugriff

Stellen Sie sicher, dass Notfallteams über den richtigen vorab bereitgestellten Zugriff in AWS verfügen, um die Zeit von der Untersuchung bis zur Wiederherstellung zu verkürzen.

Typische Anti-Muster:

- Verwendung des Root-Kontos für die Reaktion auf Vorfälle
- Veränderung bestehender Benutzerkonten
- Direkte Anpassung von IAM-Berechtigungen bei Just-In-Time-Berechtigungserhöhungen

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

AWS empfiehlt, nach Möglichkeit die Abhängigkeit von langlebigen Anmeldeinformationen zu reduzieren oder ganz zu beseitigen und stattdessen Just-In-Time-Berechtigungseskalationsmechanismen zu verwenden. Langlebige Anmeldeinformationen sind ein potenzielles Sicherheitsrisiko und erhöhen den Verwaltungsaufwand. Für die meisten Verwaltungsaufgaben und für die Reaktion auf Vorfälle empfehlen wir die Implementierung eines Identitätsverbunds zusammen mit einer temporären Eskalierung für Administratorzugriff. In diesem Modell beantragt ein Benutzer eine höhere Berechtigungsstufe (etwa für eine Vorfallreaktionsrolle). Anschließend wird, sofern der Benutzer grundsätzlich dafür infrage kommt, eine entsprechende Anforderung an einen Genehmiger gesendet. Wenn die Anforderung genehmigt wurde, erhält der Benutzer temporäre AWS-Anmeldeinformationen für die Durchführung seiner Aufgaben. Nach Ablauf dieser Anmeldeinformationen muss der Benutzer eine neue Erhöhungsanforderung übermitteln.

Wir empfehlen für die meisten Vorfallreaktionsszenarien die Verwendung temporärer Berechtigungseskalierungen. Die korrekte Vorgehensweise ist die Verwendung von AWS -Security-Token-Service und Sitzungsrichtlinien zur Festlegung der Zugriffsbereiche.

Es gibt Szenarien, in denen Verbundidentitäten nicht verfügbar sind. Hier ein paar Beispiele:

- Ausfall im Zusammenhang mit einem kompromittierten Identitätsanbieter (IdP)

- Durch fehlerhafte Konfiguration oder menschlichen Fehler beeinträchtigtes Managementsystem für den Verbundzugriff
- Böswillige Aktivität wie etwa ein DDoS-Angriff (Distributed Denial of Service) oder anderweitig verursachte Nichtverfügbarkeit des Systems

Für diese Fälle sollte Notfallzugriff (Break-Glass-Zugriff) konfiguriert werden, um eine Untersuchung und schnelle Behandlung des Vorfalls zu ermöglichen. Wir empfehlen die Verwendung eines Benutzers, einer Gruppe oder einer Rolle mit ausreichenden Berechtigungen für die Durchführung von Aufgaben und den Zugriff auf AWS-Ressourcen. Verwenden Sie den Root-Benutzer nur für Aufgaben, die Root-Benutzeranmeldeinformationen erfordern. Um zu prüfen, ob die Notfallteams über die korrekte Zugriffsstufe für AWS und andere relevante Systeme verfügen, empfehlen wir die Bereitstellung dedizierter Konten. Die Konten benötigen privilegierten Zugriff und müssen streng kontrolliert und überwacht werden. Die Konten müssen mit den geringstmöglichen Berechtigungen versehen sein, die für die erforderlichen Aufgaben benötigt werden, und die Zugriffsstufe muss auf den Playbooks basieren, die im Rahmen des Vorfallmanagementplans erstellt werden.

Verwenden Sie als bewährte Methode zweckgerichtet erstellte und dedizierte Benutzer und Rollen. Die vorübergehende Eskalierung des Zugriffs eines Benutzers oder einer Rolle über IAM-Richtlinien macht unklar, welchen Zugriff Benutzer während eines Vorfalls hatten, und birgt die Gefahr, dass die eskalierten Berechtigungen später nicht widerrufen werden.

Es ist wichtig, möglichst viele Abhängigkeiten zu entfernen, um sicherzustellen, dass in einem möglichst großen Spektrum von Ausfallszenarien zugegriffen werden kann. Erstellen Sie deshalb ein Playbook, um sicherzustellen, dass Vorfallreaktionsbenutzer als Benutzer in einem dedizierten Sicherheitskonto erstellt und nicht durch einen vorhandenen Verbund oder eine Single Sign-On (SSO)-Lösung verwaltet werden. Alle einzelnen Mitglieder von Notfallteams müssen über ein eigenes benanntes Konto verfügen. Die Kontokonfiguration muss eine Richtlinie für sichere Passwörter sowie die Multi-Faktor-Authentifizierung (MFA) erzwingen. Wenn die Playbooks zur Vorfallreaktion nur Zugriff auf die AWS-Managementkonsole benötigen, sollten für den Benutzer keine Zugriffsschlüssel konfiguriert werden und er sollte explizit auch keine Zugriffsschlüssel erstellen dürfen. Dies kann mit AWS-Richtlinien oder Service-Kontrollrichtlinien (SCPs) konfiguriert werden, wie in den bewährten -Sicherheitsmethoden für AWS Organizations SCPs erläutert. Mit Ausnahme der Möglichkeit zur Übernahme von Vorfallreaktionsrollen in anderen Konten sollten die Benutzer über keinerlei Berechtigungen verfügen.

Während eines Vorfalls kann es erforderlich sein, anderen internen oder externen Personen Zugriff zu gewähren, um Untersuchungs-, Korrektur- oder Wiederherstellungsaktivitäten zu unterstützen.

Verwenden Sie in diesem Fall den vorher erwähnten Playbook-Mechanismus. Darüber hinaus muss ein Prozess vorhanden sein, um sicherzustellen, dass jeglicher zusätzliche Zugriff sofort nach Abschluss des Vorfalls widerrufen wird.

Um sicherzustellen, dass die Verwendung von Vorfallreaktionsrollen ordnungsgemäß überwacht und geprüft werden kann, ist es wichtig, dass die für diesen Zweck erstellten IAM-Konten nicht von mehreren Personen verwendet werden und dass der Root-Benutzer des AWS-Kontos nur verwendet wird, wenn dies für eine bestimmte Aufgabe erforderlich ist. Wenn der Root-Benutzer erforderlich ist (zum Beispiel, wenn kein IAM-Zugriff auf ein bestimmtes Konto verfügbar ist), verwenden Sie einen separaten Prozess mit einem verfügbaren Playbook, um die Verfügbarkeit der Anmeldeinformationen und des MFA-Tokens des Root-Benutzers zu prüfen.

Erwägen Sie zur Konfiguration der IAM-Richtlinien für die Vorfallreaktionsrollen die Verwendung von IAM Access Analyzer, um Richtlinien auf der Grundlage von AWS CloudTrail-Protokollen zu erstellen. Gewähren Sie dazu der Vorfallreaktionsrolle in einem Nicht-Produktionskonto Administratorzugriff und durchlaufen Sie Ihre Playbooks. Anschließend kann eine Richtlinie erstellt werden, die nur die ausgeführten Aktionen zulässt. Diese Richtlinie kann dann auf alle Vorfallreaktionsrollen über alle Konten hinweg angewendet werden. Möglicherweise möchten Sie eine separate IAM-Richtlinie für jedes Playbook erstellen, um Management und Auditing zu vereinfachen. Beispiel-Playbooks können Reaktionspläne für Ransomware-Angriffe, Datenschutzverletzungen, Verlust von produktionsrelevantem Zugriff oder andere Szenarien enthalten.

Verwenden Sie die Vorfallreaktionskonten, um dedizierte IAM-Rollen in anderen AWS-Konten-Konten für die Vorfallreaktion anzunehmen. Diese Rollen müssen so konfiguriert sein, dass sie nur von Benutzern im Sicherheitskonto angenommen werden können, und das Vertrauensverhältnis muss erfordern, dass der aufrufende Prinzipal per MFA authentifiziert wurde. Die Rollen müssen eng gefasste IAM-Richtlinien verwenden, um den Zugriff zu steuern. Stellen Sie sicher, dass alle `AssumeRole`-Anforderungen für diese Rollen in CloudTrail protokolliert und gemeldet werden und dass alle mit diesen Rollen durchgeführten Aktivitäten protokolliert werden.

Es wird nachdrücklich empfohlen, die IAM–Konten und die IAM-Rollen deutlich zu benennen, damit sie in CloudTrail-Protokollen leicht zu finden sind. Geben Sie also beispielsweise den IAM-Konten den Namen *<USER_ID>*`-BREAK-GLASS` und den IAM-Rollen den Namen `BREAK-GLASS-ROLE`.

CloudTrail wird verwendet, um API-Aktivitäten in Ihren AWS-Konten zu protokollieren, und sollte zum Konfigurieren von Warnungen zur Nutzung der Vorfallreaktionsrollen eingesetzt werden. Weitere Informationen finden Sie im Blog-Beitrag zur Konfiguration von Warnungen bei Verwendung von Root-Schlüsseln. Die Anweisungen können geändert werden, um den Amazon CloudWatch-

Metrikfilter so zu konfigurieren, dass nach `AssumeRole`-Ereignissen gefiltert wird, die mit der IAM-Rolle für die Vorfallreaktion zusammenhängen:

```
{ $.eventName = "AssumeRole" && $.requestParameters.roleArn =
 "<INCIDENT_RESPONSE_ROLE_ARN>" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !
= "AwsServiceEvent" }
```

Da die Vorfallreaktionsrollen sehr wahrscheinlich eine hohe Zugriffsstufe haben, ist es wichtig, dass diese Warnungen an eine weit gefasste Gruppe gesendet werden und dass umgehend auf sie reagiert wird.

Während eines Vorfalls kann es vorkommen, dass ein Mitglied eines Notfallteams Zugriff auf Systeme benötigt, die nicht direkt durch IAM geschützt sind. Dazu können Amazon-Elastic-Compute-Cloud-Instances, Amazon-Relational-Database-Service-Datenbanken oder Software as a Service (SaaS)-Plattformen gehören. Es wird nachdrücklich empfohlen, anstelle nativer Protokolle wie SSH oder RDP AWS Systems Manager Session Manager für alle administrativen Zugriffe auf Amazon-EC2-Instances zu verwenden. Dieser Zugriff kann mit IAM (sicher und geprüft) gesteuert werden. Gegebenenfalls ist es auch möglich, Teile Ihrer Playbooks mithilfe von Run-Command-Dokumenten von AWS Systems Manager zu automatisieren, um Benutzerfehler zu reduzieren und die Wiederherstellung zu beschleunigen. Für den Zugriff auf Datenbanken und Tools von Drittanbietern empfehlen wir die Speicherung von Anmeldeinformationen in AWS Secrets Manager und die Gewährung des Zugriffs für die Vorfallreaktionsrollen.

Außerdem sollte die Verwaltung der IAM-Konten für die Vorfallreaktion Ihren Joiners-, Movers- und Leavers-Prozessen hinzugefügt sowie regelmäßig geprüft und getestet werden, um sicherzustellen, dass nur die beabsichtigten Zugriffsrechte gewährt werden.

Ressourcen

Zugehörige Dokumente:

- Verwaltung des vorübergehend erhöhten Zugriffs auf Ihre AWS-Umgebung
- Leitfaden zur Reaktion auf Sicherheitsvorfälle in AWS
- AWS Elastic Disaster Recovery
- AWS Systems Manager Incident Manager
- Einrichten einer Kontopasswortrichtlinie für IAM-Benutzer
- Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS
- Konfigurieren des kontoübergreifenden Zugriffs mit MFA

- Verwenden von IAM Access Analyzer zum Erstellen von IAM-Richtlinien
- Bewährte Methoden für AWS Organizations-Service-Kontrollrichtlinien in einer Mehrkontenumgebung
- Empfang von Benachrichtigungen, wenn die Root-Zugriffsschlüssel Ihres AWS-Kontos verwendet werden
- Erstellen detaillierter Sitzungsberechtigungen mithilfe von IAM-verwalteten Richtlinien
- „Break Glass“-Zugriff

Zugehörige Videos:

- Automatisieren der Vorfallreaktion und Forensik in AWS
- DIY-Leitfaden für Runbooks, Vorfallberichte und Vorfallreaktion
- Vorbereiten und Reagieren auf Sicherheitsvorfälle in Ihrer AWS-Umgebung

SEC10-BP06 Vorabbereitstellen von Tools

Stellen Sie sicher, dass Sicherheitspersonal über die richtigen Tools verfügt, um die Zeit von der Untersuchung bis zur Wiederherstellung zu verkürzen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Zur Automatisierung von Sicherheitsreaktionen und Betriebsfunktionen können Sie eine umfassende Palette von APIs und Tools von AWS verwenden. Sie können die Identitätsverwaltung, die Netzwerksicherheit, den Datenschutz und Überwachungsfunktionen vollständig automatisieren und mithilfe gängiger Softwareentwicklungsmethoden bereitstellen, die Sie bereits eingerichtet haben. Durch die Sicherheitsautomatisierung kann Ihr System Überwachungs- und Überprüfungsaufgaben übernehmen und eine Reaktion initiieren (im Gegensatz zur manuellen Überwachung der Sicherheitslage und manuellen Reaktion auf Ereignisse).

Wenn Ihre Vorfallreaktionsteams weiterhin auf die gleiche Weise auf Warnungen reagieren, werden Warnungen möglicherweise nicht mehr ernst genommen. Im Laufe der Zeit kann das Team für Warnungen desensibilisiert werden und entweder Fehler bei der Verarbeitung normaler Situationen machen oder außergewöhnliche Warnungen übersehen. Automatisierung hilft, eine Abstumpfung gegenüber Warnungen zu vermeiden, indem Funktionen verwendet werden, die repetitive und gewöhnliche Warnungen verarbeiten, sodass Mitarbeiter die nötigen freien Kapazitäten haben, um

sich um sensible und besondere Vorfälle zu kümmern. Die Integration von Systemen zur Erkennung von Anomalien wie Amazon GuardDuty, AWS CloudTrail Insights und Amazon CloudWatch Anomaly Detection kann den durch allgemeine schwellenwertbasierte Warnungen verursachten Aufwand reduzieren.

Sie können manuelle Prozesse verbessern, indem Sie die Schritte im Prozess programmatisch automatisieren. Nachdem Sie das Korrekturmuster für ein Ereignis definiert haben, können Sie dieses Muster in umsetzbare Logik zerlegen und den Code schreiben, um diese Logik auszuführen. Notfallteams können anschließend diesen Code ausführen, um das Problem zu beheben. Mit der Zeit können Sie immer mehr Schritte automatisieren und schließlich häufige Vorfälle automatisch behandeln.

Bei einer Sicherheitsuntersuchung müssen Sie relevante Protokolle heranziehen können, um alle Aspekte und den Zeitrahmen des Vorfalls zu verstehen. Protokolle werden auch für die Generierung von Warnungen benötigt, die auf bestimmte Ereignisse aufmerksam machen. Es ist sehr wichtig, Abfrage- und Abrufmechanismen auszuwählen, zu aktivieren, zu speichern und einzurichten sowie die Alarmierung einzurichten. Darüber hinaus stellt Amazon Detective eine effektive Möglichkeit zur Bereitstellung von Tools zum Durchsuchen von Protokolldaten dar.

AWS bietet über 200 Cloud-Services und Tausende von Funktionen. Wir empfehlen Ihnen, die Services zu überprüfen, die Ihre Strategie zur Vorfallreaktion unterstützen und vereinfachen können.

Zusätzlich zur Protokollierung sollten Sie eine Markierungsstrategie entwickeln und implementieren. Die Markierung kann dabei helfen, einen Kontext im Zusammenhang mit dem Zweck einer AWS-Ressource bereitzustellen. Die Markierung kann auch für die Automatisierung verwendet werden.

Implementierungsschritte

Auswählen und Einrichten von Protokollen für die Analyse und Alarmierung

In der folgenden Dokumentation finden Sie Informationen zur Konfiguration der Protokollierung für die Vorfallreaktion:

- Protokollierungsstrategien für die Reaktion auf Sicherheitsvorfälle
- SEC04-BP01 Konfigurieren der Service- und Anwendungsprotokollierung

Aktivieren von Sicherheits-Services zur Unterstützung von Erkennung und Reaktion

AWS bietet native Erkennungs-, Präventions- und Reaktionsfunktionen und andere Services, die für den Aufbau benutzerdefinierter Sicherheitslösungen verwendet werden können. Eine Liste der

wichtigsten Services für die Reaktion auf Sicherheitsvorfälle finden Sie unter Definitionen der Cloud-Funktionen und auf der Homepage für Reaktionen auf Sicherheitsvorfälle.

Entwickeln und Implementieren einer Markierungsstrategie

Es kann schwierig sein, kontextbezogene Informationen zum geschäftlichen Anwendungsfall und zu relevanten internen Stakeholdern rund um eine AWS-Ressource zu erhalten. Eine Möglichkeit sind Tags, die Ihren AWS-Ressourcen Metadaten zuweisen und aus einem benutzerdefinierten Schlüssel und Wert bestehen. Sie können Tags erstellen, um Ressourcen nach Zweck, Besitzer, Umgebung, Art der verarbeiteten Daten und anderen Kriterien Ihrer Wahl zu kategorisieren.

Eine konsistente Markierungsstrategie kann Reaktionen beschleunigen und den Zeitaufwand für den organisatorischen Kontext minimieren, da Sie Kontextinformationen zu einer AWS-Ressource schnell identifizieren und erkennen können. Tags können auch als Mechanismus zur Initiierung von Reaktionsautomatisierungen dienen. Weitere Informationen über zu markierende Elemente finden Sie unter Markieren Ihrer AWS-Ressourcen. Sie sollten zunächst die Tags definieren, die Sie in Ihrer Organisation implementieren möchten. Anschließend können Sie diese Markierungsstrategie implementieren und erzwingen. Weitere Einzelheiten zur Implementierung und Erzwingung finden Sie unter Implementieren einer Markierungsstrategie für AWS-Ressourcen mithilfe von AWS-Markierungsrichtlinien und Service-Kontrollrichtlinien (SCPs).

Ressourcen

Zugehörige bewährte Methoden für Well-Architected:

- SEC04-BP01 Konfigurieren der Service- und Anwendungsprotokollierung
- SEC04-BP02 Erfassen von Protokollen, Erkenntnissen und Metriken an standardisierten Orten

Zugehörige Dokumente:

- Protokollierungsstrategien für die Reaktion auf Sicherheitsvorfälle
- Definitionen der Cloud-Funktionen für die Vorfallreaktion

Zugehörige Beispiele:

- Bedrohungserkennung und -reaktion mit Amazon GuardDuty und Amazon Detective
- Security-Hub-Workshop
- Management von Schwachstellen mit Amazon Inspector

SEC10-BP07 Durchführen von Simulationen

Organisationen wachsen und entwickeln sich weiter. Gleiches gilt auch für die Bedrohungslandschaft. Daher ist es wichtig, Ihre Fähigkeiten zur Vorfallreaktion kontinuierlich zu überprüfen. Die Durchführung von Simulationen (auch bekannt als Gamedays) ist eine Methode, mit der diese Bewertung durchgeführt werden kann. Bei Simulationen werden reale Sicherheitsereignisse als Szenarien verwendet, die die Taktiken, Techniken und Verfahren (Tactics, Techniques and Procedures, TTPs) eines Bedrohungsakteurs nachahmen und es einer Organisation ermöglichen, ihre Fähigkeiten zur Vorfallreaktion einzusetzen und zu bewerten, indem sie auf diese simulierten Cyberereignisse so reagieren, wie sie es im Ernstfall tun würden.

Vorteile der Nutzung dieser bewährten Methode: Simulationen haben eine Vielzahl von Vorteilen:

- Validierung der Cybersicherheit und Stärkung des Vertrauens Ihres Vorfallreaktionsteams
- Testen der Genauigkeit und Effizienz von Tools und Workflows
- Optimierung der Kommunikations- und Eskalationsmethoden Ihres Vorfallreaktionsplans
- Möglichkeit, auf weniger verbreitete Vektoren zu reagieren

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Es gibt drei Hauptarten von Simulationen:

- Tabletop-Übungen: Beim Tabletop-Ansatz für Simulationen handelt es sich um eine Diskussionsrunde, an der die verschiedenen, mit der Vorfallreaktion betrauten Stakeholder teilnehmen, um Rollen und Verantwortlichkeiten zu üben und etablierte Kommunikationstools und Playbooks zu verwenden. Die Übung kann in der Regel an einem ganzen Tag sowie an einem virtuellen und/oder physischen Ort durchgeführt werden. Da sie auf Diskussionen basiert, konzentriert sich die Tabletop-Übung auf Prozesse, Menschen und Zusammenarbeit. Technologie ist ein integraler Bestandteil der Diskussion, aber der tatsächliche Einsatz von Tools oder Skripten für die Vorfallreaktion ist in der Regel kein Teil der Tabletop-Übung.
- Übungen des lila Teams: Übungen des lila Teams verbessern die Zusammenarbeit zwischen dem Vorfallreaktionsteam (blaues Team) und den simulierten Bedrohungsakteuren (rotes Team). Das blaue Team besteht aus Mitgliedern des Security Operations Center (SOC), kann aber auch andere Stakeholder enthalten, die an einem tatsächlichen Cyberereignis beteiligt wären. Das rote Team besteht aus einem Penetrationstest-Team oder wichtigen Stakeholdern, die in

offensiver Sicherheit geschult sind. Das rote Team arbeitet bei der Planung eines Szenarios mit den Übungsleitern zusammen, damit das Szenario korrekt und durchführbar ist. Bei Übungen des lila Teams liegt das Hauptaugenmerk auf den Erkennungsmechanismen, den Tools und den Standard-Betriebsabläufen (Standard Operating Procedures, SOPs), mit denen die Maßnahmen zur Vorfallreaktion unterstützt werden.

- Übungen des roten Teams: Bei einer Übung des roten Teams führt das Offensivteam (rotes Team) eine Simulation durch, um ein bestimmtes Ziel oder eine Reihe von Zielen aus einem vorher festgelegten Bereich zu erreichen. Die Verteidiger (blaues Team) kennen nicht unbedingt den Umfang und die Dauer der Übung, was eine realistischere Einschätzung darüber ermöglicht, wie sie auf einen tatsächlichen Vorfall reagieren würden. Da es sich bei den Übungen des roten Teams um invasive Tests handeln kann, sollten Sie vorsichtig sein und Kontrollen implementieren, um sicherzustellen, dass die Übung Ihrer Umgebung nicht tatsächlich schadet.

Erwägen Sie, in regelmäßigen Abständen Cybersimulationen durchzuführen. Jeder Übungstyp kann den Teilnehmern und der gesamten Organisation einzigartige Vorteile bieten. Sie können also etwa mit weniger komplexen Simulationstypen beginnen (beispielsweise mit Tabletop-Übungen) und dann zu komplexeren Simulationstypen übergehen (Übungen des roten Teams). Wählen Sie auf der Grundlage Ihres Sicherheitsreifegrads, Ihrer Ressourcen und der gewünschten Ergebnisse einen Simulationstyp aus. Einige Kunden entscheiden sich aufgrund der Komplexität und der Kosten möglicherweise gegen Übungen des roten Teams.

Implementierungsschritte

Unabhängig von der Art der gewählten Simulation folgen diese im Allgemeinen den folgenden Implementierungsschritten:

1. Definieren Sie die wichtigsten Übungselemente: Definieren Sie das Simulationsszenario und die Ziele der Simulation. Beide sollten von der Führungsebene akzeptiert werden.
2. Identifizieren Sie die wichtigsten Stakeholder: Für eine Übung sind mindestens Übungsleiter und Teilnehmer erforderlich. Je nach Szenario können gegebenenfalls weitere Stakeholder einbezogen werden – etwa aus der Rechts- oder Kommunikationsabteilung oder aus der Geschäftsleitung.
3. Erstellen und testen Sie das Szenario: Das Szenario muss möglicherweise während der Erstellung neu definiert werden, falls bestimmte Elemente nicht realisierbar sind. Als Ergebnis dieser Phase wird ein fertiges Szenario erwartet.
4. Führen Sie die Simulation durch: Die Art der Simulation bestimmt die Durchführung (ein Szenario auf Papier im Vergleich zu einem hochtechnischen, simulierten Szenario). Die Übungsleiter sollten

ihre Taktiken an den Übungsobjekten ausrichten und alle Übungsteilnehmer nach Möglichkeit einbeziehen, um den größtmöglichen Nutzen zu erzielen.

5. Arbeiten Sie den After-Action Report (AAR, Abschlussbericht) aus: Identifizieren Sie Bereiche mit guten Ergebnissen sowie verbesserungswürdige Bereiche und potenzielle Lücken. Der AAR sollte die Effektivität der Simulation sowie die Reaktion des Teams auf das simulierte Ereignis messen, damit der Fortschritt im Laufe der Zeit mit zukünftigen Simulationen verfolgt werden kann.

Ressourcen

Zugehörige Dokumente:

- Leitfaden zur Reaktion auf Sicherheitsvorfälle in AWS

Zugehörige Videos:

- AWS GameDay – Sicherheitsausgabe
- Ausführen effektiver Simulationen von Reaktionen auf Sicherheitsvorfälle

Operationen

Der Betrieb ist der Kern der Reaktion auf Vorfälle. Hier finden die Maßnahmen zur Reaktion und Behebung von Sicherheitsvorfällen statt. Der Betrieb umfasst die folgenden fünf Phasen: Erkennung, Analyse, Eindämmung, Beseitigung und Wiederherstellung. Beschreibungen dieser Phasen und der jeweiligen Ziele finden Sie in der folgenden Tabelle.

Phase	Ziel
Erkennung	Identifizieren eines potenziellen Sicherhei tsereignisses.
Analyse	Feststellen, ob es sich bei einem Sicherhei tsereignis um einen Vorfall handelt, und Bewerten des Umfangs des Vorfalls.
Eindämmung	Minimieren und Beschränken des Umfangs des Sicherheitsereignisses.

Phase	Ziel
Beseitigung	Entfernen nicht autorisierter Ressourcen oder Artefakte im Zusammenhang mit dem Sicherheitsereignis. Implementieren von Abhilfemaßnahmen zur Behebung der Ursache des Sicherheitsvorfalls.
Wiederherstellung	Wiederherstellen der Systeme in einem bekannten sicheren Zustand und Überwachen dieser Systeme, um sicherzustellen, dass die Bedrohung nicht erneut auftritt.

Die Phasen sollen als Leitfaden für die Reaktion auf Sicherheitsvorfälle und deren Behandlung dienen, damit Sie effektiv und nachhaltig reagieren können. Die tatsächlichen Maßnahmen, die Sie ergreifen, sind abhängig vom jeweiligen Vorfall. Bei einem Vorfall mit Ransomware müssen beispielsweise andere Schritte ausgeführt werden als bei einem Vorfall, an dem ein öffentlicher Amazon-S3-Bucket beteiligt ist. Darüber hinaus folgen diese Phasen nicht unbedingt aufeinander. Nach der Eindämmung und Beseitigung müssen Sie möglicherweise zur Analyse zurückkehren, um zu ermitteln, ob Ihre Maßnahmen wirksam waren.

Eine gründliche Vorbereitung Ihrer Mitarbeiter, Prozesse und Technologien ist der Schlüssel zu einem effektiven Betrieb. Folgen Sie daher den bewährten Methoden aus dem Abschnitt Vorbereitung, um effektiv auf ein aktives Sicherheitsereignis reagieren zu können.

Weitere Informationen finden Sie im Abschnitt Betrieb des AWS-Leitfadens zur Reaktion auf Sicherheitsvorfälle.

Aktivität nach Vorfällen

Die Bedrohungslage ändert sich ständig, und es ist wichtig, dass Ihre Organisation ebenso dynamisch in der Lage ist, Ihre Umgebungen wirksam zu schützen. Der Schlüssel zur kontinuierlichen Verbesserung liegt darin, die Ergebnisse Ihrer Vorfälle und Simulationen ständig zu analysieren, um Ihre Fähigkeiten zu verbessern, mögliche Sicherheitsvorfälle effektiv zu erkennen, darauf zu reagieren und zu untersuchen. So können Sie potenzielle Schwachstellen reduzieren, die Reaktionszeit verkürzen und den sicheren Betrieb wieder aufnehmen. Mithilfe der folgenden

Mechanismen können Sie überprüfen, ob Ihre Organisation über die neuesten Funktionen und Kenntnisse verfügt, um unabhängig von der Situation effektiv reagieren zu können.

Bewährte Methoden

- SEC10-BP08 Entwickeln eines Frameworks, um aus Vorfällen zu lernen

SEC10-BP08 Entwickeln eines Frameworks, um aus Vorfällen zu lernen

Die Implementierung eines Erkenntnis-Frameworks und einer Ursachenanalyse kann nicht nur zur Verbesserung der Reaktion auf Vorfälle, sondern auch zur Verhinderung einer Wiederholung des Vorfalls beitragen. Durch das Lernen aus Vorfällen können Sie verhindern, dass sich die gleichen Fehler, Risiken oder Fehlkonfigurationen wiederholen. Dies verbessert nicht nur Ihre Sicherheitslage, sondern minimiert auch den Zeitverlust durch vermeidbare Situationen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Es ist wichtig, ein Erkenntnis-Framework zu implementieren, das ganz allgemein Folgendes ermittelt und erreicht:

- Wann kommt es zu Erkenntnissen?
- Was beinhaltet der Erkenntnisprozess?
- Wie werden Erkenntnisse gewonnen?
- Wer ist auf welche Weise an dem Prozess beteiligt?
- Wie werden verbesserungswürdige Bereiche identifiziert?
- Wie stellen Sie sicher, dass Verbesserungen effektiv verfolgt und implementiert werden?

Das Framework sollte sich nicht auf Einzelpersonen konzentrieren oder ihnen die Schuld geben, sondern stattdessen den Fokus auf die Verbesserung der Tools und Prozesse legen.

Implementierungsschritte

Abgesehen von den zuvor aufgeführten Ergebnissen auf hoher Ebene ist es wichtig, sicherzustellen, dass Sie die richtigen Fragen stellen, um den größtmöglichen Nutzen (Informationen, die zu umsetzbaren Verbesserungen führen) aus dem Prozess zu ziehen. Berücksichtigen Sie die folgenden Fragen, um Ihre Diskussionen über Erkenntnisse zu fördern:

- Was ist vorgefallen?
- Wann wurde der Vorfall zum ersten Mal identifiziert?
- Wie wurde er identifiziert?
- Von welchen Systemen wurde eine Warnung im Zusammenhang mit der Aktivität ausgegeben?
- Welche Systeme, Services und Daten waren beteiligt?
- Was ist konkret passiert?
- Was hat gut funktioniert?
- Was hat nicht gut funktioniert?
- Welcher Prozess oder welche Verfahren haben versagt oder konnten nicht skaliert werden, um auf den Vorfall zu reagieren?
- Was kann in den folgenden Bereichen verbessert werden:
  - Personen
    - Waren die Mitarbeiter, die kontaktiert werden mussten, tatsächlich verfügbar und war die Kontaktliste auf dem neuesten Stand?
    - Fehlten den Mitarbeitern Schulungen oder Fähigkeiten, die erforderlich waren, um effektiv auf den Vorfall reagieren und ihn untersuchen zu können?
    - Waren die erforderlichen Ressourcen bereit und verfügbar?
  - Prozess
    - Wurden Prozesse und Verfahren eingehalten?
    - Waren Prozesse und Verfahren für diesen Vorfall bzw. für diese Art von Vorfall dokumentiert und verfügbar?
    - Fehlten erforderliche Prozesse und Verfahren?
    - Konnten die Notfallteams rechtzeitig auf die erforderlichen Informationen zugreifen, um auf das Problem zu reagieren?
  - Technologie
    - Haben die bestehenden Warnsysteme die Aktivität effektiv identifiziert und gemeldet?
    - Wie hätten wir die Zeit bis zur Erkennung um 50 % reduzieren können?
    - Müssen bestehende Warnungen verbessert oder neue Warnungen für diesen Vorfall bzw. für diese Art von Vorfall erstellt werden?
    - War mit den vorhandenen Tools eine effektive Untersuchung (Suche/Analyse) des Vorfalls möglich?
    - Was kann getan werden, um diesen Vorfall bzw. diese Art von Vorfall früher zu erkennen?

- Was kann getan werden, um zu verhindern, dass sich dieser Vorfall bzw. diese Art von Vorfall wiederholt?
- Wer ist für den Verbesserungsplan zuständig und wie testen Sie, ob er implementiert wurde?
- Wie sieht der Zeitplan für die Implementierung und das Testen zusätzlicher Überwachungen oder präventiver Kontrollen und Prozesse aus?

Diese Liste ist nicht vollständig. Sie soll jedoch als Ausgangspunkt dienen, um zu ermitteln, was die Organisations- und Geschäftsanforderungen sind und wie Sie diese analysieren können, um am effektivsten aus Vorfällen zu lernen und Ihre Sicherheitslage kontinuierlich zu verbessern. Am wichtigsten ist, damit zu beginnen und Erkenntnisse standardmäßig in Ihren Prozess zur Vorfallreaktion, in die Dokumentation und in die Erwartungen der Stakeholder zu integrieren.

Ressourcen

Zugehörige Dokumente:

- AWS-Leitfaden für die Reaktion auf Sicherheitsvorfälle – Entwickeln eines Frameworks, um aus Vorfällen zu lernen
- NCSC-CAF-Leitfaden – Erkenntnisse

Anwendungssicherheit

Anwendungssicherheit (Application Security, AppSec) beschreibt den gesamten Prozess des Entwurfs, der Erstellung und Tests der Sicherheitseigenschaften von Workloads, die Sie entwickeln. Sie sollten die Personen in Ihrer Organisation entsprechend geschult haben und die Sicherheitseigenschaften Ihrer Entwicklung und der Infrastruktur Ihrer Softwareveröffentlichung verstehen. Sie sollten auch Automatisierung zum Identifizieren von Sicherheitsproblemen einsetzen.

Das Einführen von Anwendungssicherheitstests als Teil Ihres Softwareentwicklungs-Lebenszyklus (SDLC) sowie des Prozesses nach der Veröffentlichung hilft Ihnen dabei, sicherzustellen, dass Sie über einen strukturierten Mechanismus zum Identifizieren, Lösen und Verhindern von Anwendungssicherheitsproblemen verfügen, die sich in Ihre Produktionsumgebung einschleichen könnten.

Ihre Methodologie zur Anwendungsentwicklung sollte Sicherheitskontrollen enthalten, während Sie Ihre Workloads entwerfen, entwickeln, bereitstellen und ausführen. Während Sie das machen, passen Sie den Prozess für kontinuierliche Fehlerverringerung und Minimierung von technischen Schulden an. Das Verwenden von Bedrohungsmodellierung in der Designphase hilft Ihnen beispielsweise dabei, Designfehler früh aufzudecken, wodurch sie einfacher und günstiger behoben werden können – im Gegensatz dazu, wenn Sie warten und die Fehler später beseitigen.

Je früher Fehler im Softwareentwicklungs-Lebenszyklus behoben werden, desto geringer sind die Kosten und die Komplexität. Die einfachste Weise, Probleme zu lösen, ist keine zu haben. Daher hilft Ihnen ein Bedrohungsmodell, sich bereits in der Designphase auf die richtigen Ergebnisse zu konzentrieren. Während Ihr AppSec-Programm reift, können Sie mithilfe von Automatisierung die Anzahl an durchgeführten Tests erhöhen, die Genauigkeit des Feedbacks für Entwickler verbessern und die für Sicherheitsüberprüfungen aufgewendete Zeit verringern. All diese Aktionen erhöhen die Qualität der Software, die Sie entwickeln, und beschleunigen das Ausliefern von Funktionen in die Produktion.

Bei diesen Implementierungsrichtlinien gibt es vier Schwerpunktbereiche: Organisation und Kultur, Sicherheit der Pipeline, Sicherheit in der Pipeline und Verwaltung von Abhängigkeiten. Jeder Bereich bietet einen Satz an Prinzipien, die Sie implementieren können, und bietet eine umfassende Sicht darauf, wie Sie Ihre Workloads entwerfen, entwickeln, aufbauen, bereitstellen und ausführen.

In AWS gibt es eine Reihe von Ansätzen, die Sie in Zusammenhang mit Ihrem Anwendungssicherheitsprogramm verwenden können. Einige dieser Ansätze basieren auf

Technologie, während sich andere auf die menschlichen und betrieblichen Aspekte Ihres Anwendungssicherheitsprogramms konzentrieren.

Best Practices

- SEC11-BP01 Für Anwendungssicherheit schulen
- SEC11-BP02 Automatisieren des Testens während des Entwicklungs- und Veröffentlichungslebenszyklus
- SEC11-BP03 Durchführen regelmäßiger Penetrationstests
- SEC11-BP04 Durchführen von Codeüberprüfungen
- SEC11-BP05 Services für Pakete und Abhängigkeiten zentralisieren
- SEC11-BP06 Programmatisches Bereitstellen von Software
- SEC11-BP07 Die Sicherheitseigenschaften der Pipelines regelmäßig bewerten
- SEC11-BP08 Ein Programm entwickeln, das den Workload-Teams die Verantwortung für die Sicherheit überträgt

SEC11-BP01 Für Anwendungssicherheit schulen

Schulen Sie Ihr Team in Bezug auf Praktiken für die sichere Entwicklung und Ausführung, um die Entwicklung sicherer und qualitativ hochwertiger Software zu fördern. Diese Vorgehensweise hilft Ihrem Team, Sicherheitsprobleme früher im Entwicklungszyklus zu verhindern, zu erkennen und zu beheben. Ziehen Sie Schulungen zu den Themen Bedrohungsmodellierung, sichere Programmierpraktiken und Nutzung von Services für sichere Konfigurationen und Abläufe in Betracht. Bieten Sie Ihrem Team Zugang zu Schulungen über Self-Service-Ressourcen und holen Sie regelmäßig Feedback ein, um kontinuierlich Verbesserungen vorzunehmen.

Gewünschtes Ergebnis: Sie vermitteln Ihrem Team die erforderlichen Kenntnisse und Fähigkeiten, um Software von Anfang an unter dem Aspekt der Sicherheit zu entwerfen und zu entwickeln. Durch Schulungen zu Bedrohungsmodellierung und sicheren Entwicklungspraktiken verfügt Ihr Team über fundierte Kenntnisse potenzieller Sicherheitsrisiken und weiß, wie diese Risiken während des Softwareentwicklungszyklus gemindert werden können. Dieser proaktive Sicherheitsansatz ist Teil Ihrer Teamkultur und versetzt Sie in die Lage, potenzielle Sicherheitsprobleme frühzeitig zu erkennen und zu beheben. Ihr Team kann somit qualitativ hochwertige, sichere Software und Features effizienter bereitstellen, wodurch die Bereitstellung insgesamt beschleunigt werden kann. In Ihrer Organisation besteht eine auf Zusammenarbeit und Einbeziehung beruhende Sicherheitskultur, wobei alle Entwickler gemeinsam für die Sicherheit verantwortlich sind.

Typische Anti-Muster:

- Sie warten bis zu einer Sicherheitsüberprüfung und berücksichtigen erst dann die Sicherheitseigenschaften eines Systems.
- Sie überlassen alle sicherheitsbezogenen Entscheidungen einem zentralen Sicherheitsteam.
- Sie kommunizieren nicht, wie die im Softwareentwicklungszyklus getroffenen Entscheidungen mit den allgemeinen Sicherheitserwartungen- oder -richtlinien der Organisation im Zusammenhang stehen.
- Sie führen die Sicherheitsüberprüfung zu spät durch.

Vorteile der Nutzung dieser bewährten Methode:

- Bessere Kenntnis der Unternehmensanforderungen hinsichtlich der Sicherheit frühzeitig im Entwicklungszyklus
- Schnellere Auslieferung von Funktionen durch schnelles Identifizieren und Lösen potenzieller Sicherheitsprobleme
- Verbesserte Qualität von Software und Systemen

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Um sichere und qualitativ hochwertige Software zu entwickeln, sollten Sie Ihr Team in Bezug auf gängige Praktiken für die sichere Entwicklung und Ausführung von Anwendungen schulen. Diese Vorgehensweise hilft Ihrem Team, Sicherheitsprobleme früher im Entwicklungszyklus zu verhindern, zu erkennen und zu beheben. So kann eine schnellere Bereitstellung erfolgen.

Um dieses Ziel zu erreichen, sollten Sie Ihr Team mithilfe von AWS-Ressourcen wie dem Workshop zur Bedrohungsmodellierung in der Bedrohungsmodellierung schulen. Die Bedrohungsmodellierung kann Ihrem Team helfen, potenzielle Sicherheitsrisiken zu verstehen und Systeme von Anfang an mit Blick auf die Sicherheit zu entwerfen. Darüber hinaus können Sie Zugang zu Schulungen von AWS Training and Certification, Branchenschulungen oder Schulungen von AWS-Partnern zum Thema „Sichere Entwicklungspraktiken“ bieten. Weitere Informationen zu einem umfassenden Ansatz für Design, Entwicklung, Sicherung und effizienten Betrieb in großem Maßstab finden Sie in der AWS-DevOps-Anleitung.

Definieren und kommunizieren Sie den Prozess der Sicherheitsüberprüfung in Ihrer Organisation klar und deutlich und legen Sie die Verantwortlichkeiten Ihres Teams, des Sicherheitsteams und anderer Stakeholder fest. Veröffentlichen Sie Self-Service-Anleitungen, Codebeispiele und Vorlagen zur Erfüllung Ihrer Sicherheitsanforderungen. Sie können AWS-Services wie AWS CloudFormation, AWS Cloud Development Kit (AWS CDK) (AWS CDK)-Konstrukten und Service Catalog verwenden, um vorab genehmigte, sichere Konfigurationen bereitzustellen und die Notwendigkeit benutzerdefinierter Einrichtungen zu verringern.

Holen Sie regelmäßig Feedback von Ihrem Team zu seiner Erfahrung mit dem Prozess zur Sicherheitsüberprüfung und den Schulungen ein und verwenden Sie dieses Feedback, um kontinuierlich Verbesserungen zu implementieren. Führen Sie Gamedays oder Bug-Bash-Kampagnen durch, um Sicherheitsprobleme zu identifizieren und zu beheben und gleichzeitig die Fähigkeiten Ihres Teams zu verbessern.

Implementierungsschritte

1. Ermittlung des Schulungsbedarfs: Beurteilen Sie anhand von Umfragen, Codeüberprüfungen oder Diskussionen mit Teammitgliedern den aktuellen Kenntnisstand und die Wissenslücken in Ihrem Team in Bezug auf sichere Entwicklungspraktiken.
2. Planung der Schulung: Erstellen Sie auf der Grundlage des ermittelten Bedarfs einen Schulungsplan, der relevante Themen wie Bedrohungsmodellierung, sichere Programmierungspraktiken, Sicherheitstests und sichere Bereitstellungspraktiken umfasst. Nutzen Sie Ressourcen wie den Workshop zur Bedrohungsmodellierung, Schulungen von AWS Training and Certification, Branchenschulungen oder Schulungsprogramme von AWS-Partnern.
3. Planung und Durchführung von Schulungen: Planen Sie regelmäßige Schulungen oder Workshops für Ihr Team. Hierbei kann es sich je nach Vorlieben des Teams und Verfügbarkeit um Schulungen mit Kursleiter oder um Schulungen zum Selbststudium handeln. Ermutigen Sie zu praktischen Übungen und zur Nutzung von praktischen Beispielen, um das Lernen zu vertiefen.
4. Definition eines Prozesses zur Sicherheitsüberprüfung: Legen Sie in Zusammenarbeit mit Ihrem Sicherheitsteam und anderen Stakeholdern den Prozess zur Sicherheitsüberprüfung für Ihre Anwendungen klar fest. Dokumentieren Sie die Verantwortlichkeiten aller am Prozess beteiligten Teams oder Einzelpersonen, einschließlich Ihres Entwicklungsteams, Ihres Sicherheitsteams und anderer relevanter Stakeholder.
5. Erstellen von Self-Service-Ressourcen: Entwickeln Sie Self-Service-Anleitungen, Codebeispiele und Vorlagen, die zeigen, wie die Sicherheitsanforderungen Ihrer Organisation erfüllt werden können. Ziehen Sie die Verwendung von AWS-Services wie CloudFormation, AWS CDK-

Konstrukts und Service Catalog in Betracht, um vorab genehmigte, sichere Konfigurationen bereitzustellen und die Notwendigkeit benutzerdefinierter Einrichtungen zu verringern.

6. Kommunikation und Kontaktpflege: Informieren Sie Ihr Team auf effektive Weise über den Prozess zur Sicherheitsüberprüfung und die verfügbaren Self-Service-Ressourcen. Führen Sie Schulungen oder Workshops durch, um die Teammitglieder mit diesen Ressourcen vertraut zu machen, und vergewissern Sie sich, dass sie über die richtige Handhabung der Ressourcen Bescheid wissen.
7. Einholung von Feedback und Verbesserungen Holen Sie regelmäßig Feedback von Ihrem Team zu seiner Erfahrung mit dem Prozess zur Sicherheitsüberprüfung und den Schulungen ein. Nutzen Sie dieses Feedback, um Bereiche mit Verbesserungspotenzial zu identifizieren und die Schulungsmaterialien, Self-Service-Ressourcen sowie den Prozess zur Sicherheitsüberprüfung kontinuierlich zu verbessern.
8. Durchführung von Sicherheitsübungen: Organisieren Sie Gamedays oder Bug-Bash-Kampagnen, um Sicherheitsprobleme in Ihren Anwendungen zu identifizieren und zu beheben. Diese Übungen helfen nicht nur dabei, potenzielle Schwachstellen aufzudecken, sondern bieten Ihrem Team auch die Möglichkeit, praktische Erfahrungen zu sammeln und so seine Fähigkeiten in Bezug auf die sichere Entwicklung und Ausführung zu verbessern.
9. Weiteres Lernen und weitere Verbesserungen: Ermutigen Sie Ihr Team, sich über die neuesten Methoden, Tools und Techniken für die sichere Entwicklung auf dem Laufenden zu halten. Überprüfen und aktualisieren Sie Ihre Schulungsmaterialien und Ressourcen regelmäßig, um der sich weiterentwickelnden Sicherheitslandschaft und Änderungen in Bezug auf bewährte Methoden Rechnung zu tragen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC11-BP08 Ein Programm entwickeln, das den Workload-Teams die Verantwortung für die Sicherheit überträgt

Zugehörige Dokumente:

- AWS Training and Certification
- Betrachtung der Cloud-Sicherheits-Governance
- Konzepte für Bedrohungsmodellierung
- Schulungen beschleunigen – AWS Skills Guild

- AWS DevOps Sagas

Zugehörige Videos:

- Proaktive Sicherheit: Überlegungen und Ansätze

Zugehörige Beispiele:

- Workshop zur Bedrohungsmodellierung
- Branchenbewusstsein für Entwickler

Zugehörige Services:

- AWS CloudFormation
- AWS Cloud Development Kit (AWS CDK) (AWS CDK) Konstrukte
- Servicekatalog

SEC11-BP02 Automatisieren des Testens während des Entwicklungs- und Veröffentlichungslebenszyklus

Automatisieren Sie das Testen der Sicherheitseigenschaften während des Entwicklungs- und Veröffentlichungslebenszyklus. Automatisierung vereinfacht die kontinuierliche und wiederholbare Identifizierung potenzieller Probleme. Dadurch wird das Risiko von Sicherheitsproblemen in der bereitgestellten Software verringert.

Gewünschtes Ergebnis: Das Ziel von automatisiertem Testen ist, eine programmatische Möglichkeit zur frühen Erkennung von potenziellen Problemen – häufig im Laufe des Entwicklungslebenszyklus – zu bieten. Wenn Sie Regressionstests automatisieren, können Sie funktionale und nicht funktionale Tests erneut durchführen, um zu überprüfen, ob zuvor getestete Software nach einer Änderung weiterhin wie erwartet funktioniert. Wenn Sie Sicherheitstests für Komponenten definieren, um nach häufigen Fehlkonfigurationen zu suchen, wie einer fehlerhaften oder fehlenden Authentifizierung, können Sie diese Fehler früh im Entwicklungsprozess identifizieren und beheben.

Testautomatisierung verwendet speziell entwickelte Testfälle zur Anwendungsvalidierung auf Basis der Anforderungen und der gewünschten Funktionalität der Anwendung. Das Ergebnis von automatisiertem Testen basiert auf dem Vergleich zwischen der erstellten Testausgabe

und der erwarteten Ausgabe, wodurch der gesamte Lebenszyklus des Testens beschleunigt wird. Testmethoden wie Regressionstests und Modultest-Suites eignen sich am besten zur Automatisierung. Durch die Automatisierung des Testens von Sicherheitseigenschaften können Entwickler automatisiertes Feedback erhalten, ohne auf eine Sicherheitsüberprüfung warten zu müssen. Automatisierte Tests in Form von statischer oder dynamischer Codeanalyse können die Qualität von Code erhöhen und dabei helfen, potenzielle Softwareprobleme früh im Entwicklungslebenszyklus zu erkennen.

Typische Anti-Muster:

- Testfälle und Testergebnisse des automatisierten Testens werden nicht kommuniziert.
- Automatisiertes Testen wird erst unmittelbar vor einer Veröffentlichung durchgeführt.
- Testfälle werden mit sich häufig ändernden Anforderungen automatisiert.
- Es wird keine Anleitung für den Umgang mit den Ergebnissen von Sicherheitstests bereitgestellt.

Vorteile der Nutzung dieser bewährten Methode:

- Verringerte Abhängigkeit von Menschen, die die Sicherheitseigenschaften eines Systems evaluieren
- Konsistente Erkenntnisse bei mehreren Arbeitsabläufen für mehr Konsistenz
- Geringere Wahrscheinlichkeit, dass Sicherheitsprobleme in Produktionssoftware gelangen
- Kürzeres Zeitfenster zwischen der Erkennung und Behebung von Softwareproblemen, da sie früher entdeckt werden
- Erhöhte Sichtbarkeit von systemischem oder wiederholtem Verhalten bei mehreren Arbeitsabläufen, dank derer organisationsweite Verbesserungen vorangetrieben werden können

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Setzen Sie während der Entwicklung Ihrer Software unterschiedliche Mechanismen für das Testen von Software ein, um sicherzustellen, dass Sie Ihre Anwendung sowohl auf funktionale Anforderungen (basierend auf Ihrer Geschäftslogik) als auch auf nicht funktionale Anforderungen testen, die sich auf die Zuverlässigkeit, Leistung und Sicherheit der Anwendung konzentrieren.

Bei statischen Anwendungssicherheitstests (SAST) wird Ihr Quellcode auf ungewöhnliche Sicherheitsmuster untersucht und es werden Hinweise auf fehleranfälligen Code bereitgestellt.

SAST nutzt statische Eingaben wie etwa die Dokumentation (Anforderungsspezifikationen, Designdokumentation und Designspezifikationen) und den Anwendungscode, um Tests in Bezug auf eine Reihe von bekannten Sicherheitsproblemen durchzuführen. Statische Code-Analyzer helfen dabei, die Analyse großer Codemengen zu beschleunigen. Die NIST Quality Group bietet einen Vergleich von Quellcode-Sicherheitsanalysen, der Open-Source-Tools für Bytecode-Scanner und Binärcode-Scanner umfasst.

Ergänzen Sie Ihr statisches Testen mit Methoden für dynamische Anwendungssicherheitstests (DAST). Hierbei wird die Anwendung bei ihrer Ausführung getestet, um potenzielles unerwartetes Verhalten zu identifizieren. Dynamisches Testen kann verwendet werden, um potenzielle Probleme zu erkennen, die über die statische Analyse nicht gefunden werden können. Das Testen in der Code-Repository-, Build- und Pipeline-Phase ermöglicht es Ihnen, nach unterschiedlichen Arten potenzieller Fehler in Ihrem Code zu suchen. Amazon Q Developer bietet Codeempfehlungen, einschließlich Sicherheitsscans, in der IDE des Entwicklers. Amazon CodeGuru Security kann kritische Fehler, Sicherheitsprobleme und schwer zu findende Bugs während der Anwendungsentwicklung identifizieren und bietet Empfehlungen zur Verbesserung der Codequalität. Auch die Extraktion von Software-Stücklisten (SBOM, Software Bill of Materials) ermöglicht es Ihnen, einen formalen Datensatz zu extrahieren, der die Details und die Beziehungen der verschiedenen Komponenten enthält, die bei der Erstellung Ihrer Software verwendet wurden. Dies ermöglicht Ihnen ein fundiertes Schwachstellenmanagement und die schnelle Identifizierung von Software- oder Komponentenabhängigkeiten sowie Lieferkettenrisiken.

Der Workshop Security for Developers verwendet AWS-Entwickler-Tools wie AWS CodeBuild, AWS CodeCommit und AWS CodePipeline für die Automatisierung der Veröffentlichungs-Pipeline, die SAST- und DAST-Testmethoden umfasst.

Richten Sie beim Durchlaufen Ihres Softwareentwicklungs-Lebenszyklus einen iterativen Prozess ein, der regelmäßige Anwendungsüberprüfungen mit Ihrem Sicherheitsteam enthält. Aus diesen Sicherheitsüberprüfungen gewonnenes Feedback sollte behandelt und im Rahmen der Bereitschaftsüberprüfung Ihrer Softwareversion validiert werden. Diese Überprüfungen schaffen einen robusten Sicherheitsstatus der Anwendungen und bieten Entwicklern umsetzbares Feedback, um Maßnahmen zum Beheben von Problemen zu ergreifen.

Implementierungsschritte

- Implementieren Sie eine konsistente IDE, eine Codeüberprüfung und CI/CD-Tools mit Sicherheitstests.

- Überlegen Sie, wo im Softwareentwicklungs-Lebenszyklus Pipelines blockiert werden können, anstatt Entwickler darüber zu informieren, dass Probleme behoben werden müssen.
- Automated Security Helper (ASH) ist ein Beispiel für ein Open-Source-Tool für Codesicherheits-Scans.
- Die Durchführung von Tests oder Codeanalysen mithilfe von automatisierten Tools wie Amazon Q Developer, das in Entwickler-IDEs integriert ist, und Amazon CodeGuru Security für das Scannen von Code beim Commit ermöglicht es Entwicklern, Feedback zur richtigen Zeit zu erhalten.
- Beim Entwickeln mithilfe von AWS Lambda können Sie Amazon Inspector verwenden, um den Anwendungscode in Ihren Funktionen zu scannen.
- Wenn automatisiertes Testen in CI/CD-Pipelines enthalten ist, sollten Sie ein Ticket-System verwenden, um die Meldung und Behebung von Softwareproblemen nachzuverfolgen.
- Bei Sicherheitstests, die möglicherweise Erkenntnisse liefern, sollten Sie Lösungsanweisungen bereitstellen, damit Entwickler die Codequalität verbessern können.
- Analysieren Sie regelmäßig die Erkenntnisse automatisierter Tools, um die nächste Automatisierung, Entwicklerschulung oder Sensibilisierungskampagne zu planen.
- Für eine SBOM-Extraktion im Rahmen Ihrer CI/CD-Pipelines verwenden Sie Amazon Inspector SBOM Generator, um Software-Stücklisten für Archive, Container-Images, Verzeichnisse, lokale Systeme und kompilierte Go- und Rust-Binärdateien im CycloneDX-SBOM-Format zu erstellen.

Ressourcen

Zugehörige bewährte Methoden:

- DevOps-Leitfaden: DL.CR.3 Festlegen klarer Abschlusskriterien für Codeaufgaben

Zugehörige Dokumente:

- Continuous Delivery und Continuous Deployment

- AWS Kompetenzpartner für DevOps
- AWS Kompetenzpartner für Sicherheit für Anwendungssicherheit
- Auswählen eines Well-Architected-CI/CD-Ansatzes
- Secrets-Erkennung in Amazon CodeGuru Security
- Erkennungsbibliothek von Amazon CodeGuru Security

- Beschleunigen von Bereitstellungen in AWS mit effektiver Governance
- Umgang von AWS mit der Automatisierung sicherer, vollautomatischer Bereitstellungen
- Erreichen eines effektiven Gleichgewichts zwischen Sicherheit und Geschwindigkeit mithilfe von Amazon CodeGuru Security

Zugehörige Videos:

- Vollständige Automatisierung: Automatisieren der Pipelines für kontinuierliche Bereitstellung bei Amazon
- Automatisieren von kontoübergreifenden CI/CD-Pipelines
- Der Softwareentwicklungsprozess bei Amazon
- Testen von Software und Systemen bei Amazon

Zugehörige Beispiele:

- Branchenbewusstsein für Entwickler
- Automated Security Helper (ASH)
- AWS CodePipeline Governance – Github

SEC11-BP03 Durchführen regelmäßiger Penetrationstests

Führen Sie regelmäßige Penetrationstests für Ihre Software durch. Dieser Mechanismus hilft bei der Identifizierung potenzieller Softwareprobleme, die bei automatisierten Tests oder einer manuellen Überprüfung des Codes nicht erkannt werden können. Er kann Ihnen außerdem dabei helfen, die Wirksamkeit Ihrer Erkennungskontrollen zu verstehen. Penetrationstests sollen ermitteln, ob es möglich ist, die Software so zu beeinflussen, dass sie sich unerwartet verhält – etwa, indem sie Daten verfügbar macht, die geschützt sein sollten, oder umfassendere Berechtigungen gewährt als erwartet.

Gewünschtes Ergebnis: Penetrationstests werden zur Erkennung und Behandlung sowie zur Validierung der Sicherheitseigenschaften Ihrer Anwendung verwendet. Regelmäßige und geplante Penetrationstests sollten als Teil des Softwareentwicklungs-Lebenszyklus durchgeführt werden. Die aus Penetrationstests gewonnenen Erkenntnisse sollten vor der Veröffentlichung der Software behandelt werden. Analysieren Sie die Erkenntnisse von Penetrationstests, um zu ermitteln, ob es sich um Probleme handelt, die mithilfe von Automatisierung gefunden werden können. Ein

regelmäßiger und wiederholbarer Prozess für Penetrationstests mit einem aktiven Feedback-Mechanismus fließt in die Anweisungen für Entwickler ein und verbessert die Softwarequalität.

Typische Anti-Muster:

- Penetrationstests werden nur für bekannte oder weit verbreitete Sicherheitsprobleme verwendet.
- Penetrationstests werden für Anwendungen ohne abhängige Drittanbieter-Tools und -Bibliotheken durchgeführt.
- Penetrationstests werden nur für Paketsicherheitsprobleme durchgeführt und die implementierte Geschäftslogik wird nicht evaluiert.

Vorteile der Nutzung dieser bewährten Methode:

- Gesteigertes Vertrauen in die Sicherheitseigenschaften der Software vor der Veröffentlichung
- Möglichkeit, bevorzugte Anwendungsmuster zu identifizieren, wodurch die Softwarequalität erhöht wird
- Verbesserte Sicherheitseigenschaften von Software durch eine Feedbackschleife, die früher im Entwicklungszyklus ermittelt, wo Automatisierungen oder zusätzliche Schulungen hilfreich sind

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Penetrationstests sind eine strukturierte Sicherheitstestübung, bei der Szenarien mit geplanten Sicherheitsverstößen zur Erkennung und Behandlung sowie zur Validierung von Sicherheitskontrollen durchgespielt werden. Penetrationstests starten mit einer Erkundung, bei der Daten basierend auf dem aktuellen Design der Anwendung und ihrer Abhängigkeiten gesammelt werden. Eine kuratierte Liste mit sicherheitsspezifischen Testszenarien wird entwickelt und durchlaufen. Der wesentliche Zweck dieser Tests besteht darin, Sicherheitsprobleme in Ihrer Anwendung aufzudecken, die dazu genutzt werden können, unbeabsichtigten Zugriff auf Ihre Umgebung oder unautorisierten Zugriff auf Daten zu erhalten. Sie sollten Penetrationstests durchführen, wenn Sie neue Funktionen einführen oder wenn sich die Funktion oder technische Implementierung Ihrer Anwendung erheblich geändert hat.

Sie sollten in Ihrem Entwicklungslebenszyklus die am besten geeignete Phase bestimmen, um Penetrationstests durchzuführen. Diese Tests sollten so spät stattfinden, dass sich das System nahe

am vorgesehenen Veröffentlichungszustand befindet, aber es sollte noch genügend Zeit vorhanden sein, damit Probleme behoben werden können.

Implementierungsschritte

- Implementieren Sie einen strukturierten Prozess für den Umfang der Penetrationstests. Dieser Prozess sollte auf dem Bedrohungsmodell basieren, um den Kontext zu wahren.
- Bestimmen Sie den geeigneten Zeitpunkt im Entwicklungszyklus zum Durchführen von Penetrationstests. Penetrationstests sollten dann erfolgen, wenn nur noch minimale Anwendungsänderungen zu erwarten sind, aber noch ausreichend Zeit für die Fehlerbehebung übrig ist.
- Schulen Sie Ihre Entwickler hinsichtlich der zu erwartenden Erkenntnisse aus Penetrationstests sowie dahingehend, wie sie Informationen zu deren Behandlung erhalten können.
- Verwenden Sie Tools zur Beschleunigung von Penetrationstests durch Automatisierung gängiger oder wiederholbarer Tests.
- Analysieren Sie Erkenntnisse aus Penetrationstests, um systemische Sicherheitsprobleme zu identifizieren, und verwenden Sie diese Daten, um sie in zusätzliche automatisierte Tests und fortlaufende Entwicklerschulungen einfließen zu lassen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC11-BP01 Für Anwendungssicherheit schulen
- SEC11-BP02 Automatisieren des Testens während des Entwicklungs- und Veröffentlichungslebenszyklus

Zugehörige Dokumente:

- AWS-Penetrationstests enthält ausführliche Informationen zu Penetrationstests in AWS.
- Beschleunigen von Bereitstellungen in AWS mit effektiver Governance
- AWS Kompetenzpartner für Sicherheit
- Modernisieren Ihrer Penetrationstestarchitektur in AWS Fargate
- AWS Fehlerinjektionsservice

Zugehörige Beispiele:

- Automatisieren von API-Tests mit AWS CodePipeline (GitHub)
- Automated Security Helper (GitHub)

SEC11-BP04 Durchführen von Codeüberprüfungen

Führen Sie Codeüberprüfungen durch, um die Qualität und Sicherheit der Software während der Entwicklung zu überprüfen. Bei Codeüberprüfungen müssen andere Teammitglieder als der ursprüngliche Verfasser des Codes den Code auf mögliche Probleme und Schwachstellen sowie auf die Einhaltung von Programmierstandards und bewährten Methoden überprüfen. Dieser Prozess hilft, Fehler, Inkonsistenzen und Sicherheitslücken zu erkennen, die der ursprüngliche Entwickler möglicherweise übersehen hat. Verwenden Sie automatisierte Tools zur Unterstützung bei Codeüberprüfungen.

Gewünschtes Ergebnis: Sie beziehen Codeüberprüfungen während der Entwicklung ein, um die Qualität der Software, die gerade geschrieben wird, zu verbessern. Sie nutzen die bei der Codeüberprüfung gewonnenen Erkenntnisse für die Weiterbildung weniger erfahrener Mitglieder des Teams. Sie identifizieren Möglichkeiten zur Automatisierung und unterstützen den Prozess zur Codeüberprüfung mithilfe von automatisierten Tools und Tests.

Typische Anti-Muster:

- Sie überprüfen den Code vor der Bereitstellung nicht.
- Die Person, die den Code geschrieben hat, überprüft den Code selbst.
- Sie verwenden keine Automatisierung und keine Tools zur Unterstützung und Orchestrierung von Codeüberprüfungen.
- Sie schulen die Entwickler vor der Codeüberprüfung nicht in Bezug auf Anwendungssicherheit.

Vorteile der Nutzung dieser bewährten Methode:

- Verbesserte Codequalität
- Erhöhte Konsistenz bei der Codeentwicklung durch erneute Verwendung gängiger Ansätze
- Verringerte Anzahl von Schwierigkeiten, die bei Penetrationstests und in späteren Phasen entdeckt werden
- Verbesserter Wissenstransfer innerhalb des Teams

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Codeüberprüfungen helfen, die Qualität und Sicherheit der Software während der Entwicklung zu überprüfen. Bei manuellen Prüfungen wird der Code von einem anderen Teammitglieder als dem ursprünglichen Verfasser des Codes auf mögliche Probleme und Schwachstellen sowie auf die Einhaltung von Programmierstandards und bewährten Methoden überprüft. Dieser Prozess hilft, Fehler, Inkonsistenzen und Sicherheitslücken zu erkennen, die der ursprüngliche Entwickler möglicherweise übersehen hat.

Ziehen Sie die Verwendung von Amazon CodeGuru Security für automatisierte Codeüberprüfungen in Betracht. CodeGuru Security verwendet Machine Learning und Automated Reasoning, um Ihren Code zu analysieren und potenzielle Sicherheitsschwachstellen und Codierungsprobleme zu identifizieren. Integrieren Sie automatisierte Codeüberprüfungen in Ihre bestehenden Code-Repositorys und CI/CD-Pipelines (Continuous Integration/Continuous Deployment).

Implementierungsschritte

1. Richten Sie einen Prozess zur Codeüberprüfung ein:
   - Legen Sie fest, wann Codeüberprüfungen durchgeführt werden sollen, beispielsweise vor der Zusammenführung von Code in den Hauptzweig oder vor der Bereitstellung in der Produktion.
   - Legen Sie fest, wer am Prozess zur Codeüberprüfung beteiligt sein sollte, beispielsweise Teammitglieder, erfahrene Entwickler und Sicherheitsexperten.
   - Entscheiden Sie sich für die Methode zur Codeüberprüfung, einschließlich des Prozesses und der zu verwendenden Tools.
2. Richten Sie Tools zur Codeüberprüfung ein:
   - Evaluieren Sie Tools zur Codeüberprüfung, die den Anforderungen Ihres Teams entsprechen, wie z. B. GitHub Pull Requests oder CodeGuru Security, und wählen Sie geeignete Tools aus.
   - Integrieren Sie die ausgewählten Tools in Ihre bestehenden Code-Repositorys und CI/CD-Pipelines.
   - Konfigurieren Sie die Tools so, dass die Anforderungen an die Codeüberprüfung (z. B. Mindestanzahl von Prüfern und Genehmigungsregeln) durchgesetzt werden.
3. Definieren Sie eine Checkliste und Richtlinien für die Codeüberprüfung:

- Erstellen Sie eine Checkliste oder Richtlinien für die Codeüberprüfung, aus der/denen hervorgeht, was überprüft werden sollte. Berücksichtigen Sie Faktoren wie die Codequalität, Sicherheitsschwachstellen, die Einhaltung von Programmierstandards und die Leistung.
- Kommunizieren Sie die Checkliste oder die Richtlinien dem Entwicklungsteam und stellen Sie sicher, dass jeder die Erwartungen versteht.

4. Schulen Sie die Entwickler in Bezug auf bewährte Methoden zur Codeüberprüfung:
   - Bieten Sie Ihrem Team Schulungen zur Durchführung effektiver Codeüberprüfungen an.
   - Informieren Sie Ihr Team über die Prinzipien der Anwendungssicherheit und allgemeine Schwachstellen, auf die bei Überprüfungen geachtet werden sollte.
   - Fördern Sie den Wissensaustausch und Pair-Programming-Sitzungen zur Weiterbildung von weniger erfahrenen Teammitgliedern.
5. Implementieren Sie den Prozess zur Codeüberprüfung:
   - Integrieren Sie den Schritt zur Codeüberprüfung in Ihren Entwicklungsworkflow, beispielsweise das Erstellen einer Pull-Anforderung und das Zuweisen von Prüfern.
   - Verlangen Sie die Überprüfung von Codeänderungen vor der Zusammenführung oder Bereitstellung.
   - Fördern Sie während des Überprüfungsprozesses eine offene Kommunikation und konstruktives Feedback.
6. Überwachen Sie den Prozess und nehmen Sie Verbesserungen vor:
   - Überprüfen Sie regelmäßig die Effektivität Ihres Prozesses zur Codeüberprüfung und holen Sie Feedback vom Team ein.
   - Identifizieren Sie Möglichkeiten zur Automatisierung oder zur Verbesserung der Tools, um den Prozess zur Codeüberprüfung zu optimieren.
   - Aktualisieren und optimieren Sie die Checkliste oder die Richtlinien für die Codeüberprüfung kontinuierlich auf der Grundlage von Erkenntnissen und bewährten Methoden der Branche.
7. Fördern Sie eine Kultur der Codeüberprüfung:
   - Machen Sie deutlich, wie wichtig Codeüberprüfungen für die Wahrung der Codequalität und -sicherheit sind.
   - Feiern Sie Erfolge und Erkenntnisse aus dem Prozess zur Codeüberprüfung.
   - Fördern Sie ein auf Zusammenarbeit und Unterstützung beruhendes Umfeld, in dem Entwickler ein gutes Gefühl dabei haben, Feedback zu geben und zu empfangen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC11-BP02 Automatisieren des Testens während des Entwicklungs- und Veröffentlichungslebenszyklus

Zugehörige Dokumente:

- DevOps-Leitfaden: DL.CR.2 Durchführen von Peer-Reviews bei Codeänderungen
- Informationen zu Pull-Anforderungen in GitHub

Zugehörige Beispiele:

- Automatisieren von Codeüberprüfungen mit Amazon CodeGuru Security
- Automatisieren der Erkennung von Sicherheitsschwachstellen und Bugs in CI/CD-Pipelines mithilfe der CLI von Amazon CodeGuru Security

Zugehörige Videos:

- Kontinuierliche Verbesserung der Codequalität mit Amazon CodeGuru Security

SEC11-BP05 Services für Pakete und Abhängigkeiten zentralisieren

Stellen Sie zentralisierte Services für den Erhalt von Softwarepaketen und anderen Abhängigkeiten für Ihre Teams bereit. Auf diese Weise können Pakete validiert werden, bevor sie in die von Ihnen geschriebene Software integriert werden, und es wird eine Datenquelle für die Analyse der Software bereitgestellt, die in Ihrer Organisation verwendet wird.

Gewünschtes Ergebnis: Sie erstellen Ihren Workload aus externen Softwarepaketen neben dem von Ihnen geschriebenen Code. Dies macht die Implementierung von häufig verwendeten Funktionen wie einem JSON-Parser oder einer Verschlüsselungsbibliothek einfacher. Sie stellen die Quellen für diese Pakete und Abhängigkeiten zentral bereit, sodass Ihr Sicherheitsteam sie vor der Verwendung validieren kann. Sie verwenden diesen Ansatz zusammen mit manuellen und automatisierten Tests, um das Vertrauen in die Qualität der entwickelten Software zu steigern.

Typische Anti-Muster:

- Sie rufen Pakete willkürlich aus Repositorys im Internet ab.
- Sie testen neue Pakete nicht, bevor Sie sie für Entwickler verfügbar machen.

Vorteile der Nutzung dieser bewährten Methode:

- Besseres Verständnis, welche Pakete in der entwickelten Software verwendet werden
- Benachrichtigung von Workload-Teams, wenn ein Paket aktualisiert werden muss (basierend auf dem Verständnis davon, wer was verwendet)
- Geringeres Risiko, dass ein Paket mit Problemen in Ihre Software eingeschlossen wird

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Stellen Sie zentralisierte Services für Pakete und Abhängigkeiten so bereit, dass sie von Entwicklern einfach verwendet werden können. Zentralisierte Services können logisch zentral sein, anstatt als monolithisches System implementiert zu werden. Mit diesem Ansatz können Sie Services anbieten, die die Anforderungen Ihrer Entwickler erfüllen. Sie sollten eine effiziente Methode implementieren, mit der dem Repository im Falle von Updates oder neuen Anforderungen Pakete hinzugefügt werden können. Mithilfe von AWS-Services wie AWS CodeArtifact oder ähnlichen AWS-Partnerlösungen kann diese Funktion bereitgestellt werden.

Implementierungsschritte

- Implementieren Sie einen logisch zentralisierten Repository-Service, der in allen Umgebungen, in denen die Software entwickelt wird, verfügbar ist.
- Schließen Sie Zugriff auf das Repository als Komponente des AWS-Konto-Vergabeprozesses ein.
- Entwickeln Sie eine Automatisierung zum Testen von Paketen, bevor diese in einem Repository veröffentlicht werden.
- Pflegen Sie Metriken der am häufigsten verwendeten Pakete, Sprachen und Teams mit den häufigsten Änderungen.
- Stellen Sie einen automatisierten Mechanismus für Entwicklerteams bereit, damit sie neue Pakete anfordern und Feedback geben können.

- Scannen Sie regelmäßig Pakete in Ihrem Repository, um die Auswirkungen kürzlich entdeckter Probleme zu identifizieren.

Ressourcen

Zugehörige bewährte Methoden:

- SEC11-BP02 Automatisieren des Testens während des Entwicklungs- und Veröffentlichungslebenszyklus

Zugehörige Dokumente:

- DevOps-Anleitung: DL.CS.2 Signieren von Codeartefakten nach jedem Build
- Ebenen der Lieferkette für Softwareartefakte (SLSA)

Zugehörige Beispiele:

- Beschleunigen von Bereitstellungen in AWS mit effektiver Governance
- Erhöhen Ihrer Paketsicherheit mit dem Toolkit von CodeArtifact Package Origin Control
- Pipeline zur Veröffentlichung von Paketen in mehreren Regionen (GitHub)
- Veröffentlichen von Node.js-Modulen in AWS CodeArtifact mithilfe von AWS CodePipeline (GitHub)
- Beispiel für eine AWS CDK-Java-CodeArtifact-Pipeline (GitHub)
- Verteilen privater .NET-NuGet-Pakete mit AWS CodeArtifact (GitHub)

Zugehörige Videos:

- Proaktive Sicherheit: Überlegungen und Ansätze
- Die AWS-Philosophie zu Sicherheit (re:Invent 2017)
- Wenn Sicherheit und Dringlichkeit von Bedeutung sind: Umgang mit Log4Shell

SEC11-BP06 Programmatisches Bereitstellen von Software

Führen Sie Bereitstellungen von Software nach Möglichkeit programmatisch durch. Dieser Ansatz verringert die Wahrscheinlichkeit eines Bereitstellungsfehlers oder der Einführung eines unerwarteten Problems aufgrund eines menschlichen Fehlers.

Gewünschtes Ergebnis: Sie testen die Version Ihres Workloads, die Sie auch bereitstellen, und die Bereitstellung erfolgt stets konsistent. Sie externalisieren die Konfiguration Ihres Workloads, wodurch die Bereitstellung in verschiedenen Umgebungen ohne Änderungen leichter möglich wird. Sie nutzen das kryptografische Signieren Ihrer Softwarepakete, um sicherzustellen, dass sich zwischen den Umgebungen nichts ändert.

Typische Anti-Muster:

- Software wird manuell in der Produktion bereitgestellt.
- An Software werden manuell Änderungen vorgenommen, um unterschiedlichen Umgebungen gerecht zu werden.

Vorteile der Nutzung dieser bewährten Methode:

- Gesteigertes Vertrauen in den Prozess der Softwareveröffentlichung
- Verringertes Risiko, dass eine fehlgeschlagene Änderung die Geschäftsfunktionen beeinträchtigt
- Erhöhte Veröffentlichungsfrequenz aufgrund eines geringeren Änderungsrisikos
- Automatische Rollback-Funktion für unerwartete Ereignisse während der Bereitstellung
- Möglichkeit, kryptografisch nachzuweisen, dass es sich bei der getesteten Software um die bereitgestellte Software handelt

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Um eine robuste und zuverlässige Anwendungsinfrastruktur aufrechtzuerhalten, sollten Sie sichere und automatisierte Bereitstellungsverfahren einführen. Dies beinhaltet das Entfernen von permanentem menschlichem Zugriff aus Produktionsumgebungen, die Verwendung von CI/CD-Tools für Bereitstellungen und die Externalisierung von umgebungsspezifischen Konfigurationsdaten. Mit diesem Ansatz können Sie die Sicherheit erhöhen, das Risiko menschlicher Fehler verringern und den Bereitstellungsprozess optimieren.

Sie können die Struktur Ihres AWS-Kontos so aufbauen, dass ein permanenter menschlicher Zugriff auf Produktionsumgebungen nicht mehr möglich ist. Durch diese Vorgehensweise wird das Risiko unbefugter oder versehentlicher Änderungen minimiert und so die Integrität Ihrer Produktionssysteme verbessert. Anstatt direkten menschlichen Zugriff zu gewähren, können Sie CI/CD-Tools wie AWS CodeBuildund AWS CodePipeline für Bereitstellungen verwenden. Mit diesen Services können Sie

die Erstellungs-, Test- und Bereitstellungsprozesse automatisieren. Es sind dann weniger manuelle Eingriffe notwendig und es kann eine größere Konsistenz erzielt werden.

Um die Sicherheit und Rückverfolgbarkeit weiter zu verbessern, können Sie Ihre Anwendungspakete nach dem Testen signieren und diese Signaturen während der Bereitstellung validieren. Verwenden Sie hierfür kryptografische Tools wie AWS Signer oder AWS Key Management Service (AWS KMS). Durch das Signieren und Überprüfen von Paketen können Sie sicherstellen, dass Sie nur autorisierten und validierten Code in Ihren Umgebungen bereitstellen.

Darüber hinaus kann Ihr Team Ihren Workload so gestalten, dass umgebungsspezifische Konfigurationsdaten aus einer externen Quelle wie AWS Systems Manager Parameter Store abgerufen werden. Bei dieser Vorgehensweise wird der Anwendungscode von den Konfigurationsdaten getrennt, sodass Sie Konfigurationen unabhängig verwalten und aktualisieren können, ohne den Anwendungscode selbst ändern zu müssen.

Um die Bereitstellung und Verwaltung der Infrastruktur zu optimieren, sollten Sie die Verwendung von Infrastructure as Code (IaC)-Tools wie AWS CloudFormation oder AWS CDK in Betracht ziehen. Sie können diese Tools verwenden, um Ihre Infrastruktur als Code zu definieren und so eine bessere Konsistenz und Wiederholbarkeit von Bereitstellungen in verschiedenen Umgebungen zu erreichen.

Erwägen Sie Canary-Bereitstellungen, um die erfolgreiche Bereitstellung Ihrer Software zu validieren. Bei Canary-Bereitstellungen werden Änderungen an einer Teilmenge der Instances oder Benutzer vorgenommen, bevor sie in der gesamten Produktionsumgebung bereitgestellt werden. Sie können dann die Auswirkungen der Änderungen überwachen und bei Bedarf ein Rollback durchführen, wodurch das Risiko weit verbreiteter Probleme minimiert wird.

Folgen Sie den Empfehlungen im Whitepaper Ihre AWS-Umgebung mit mehreren Konten organisieren. Dieses Whitepaper enthält Anleitungen zum Aufteilen von Umgebungen (z. B. Entwicklung, Staging und Produktion) auf verschiedene AWS-Konten, wodurch eine noch bessere Sicherheit und Isolierung erzielt werden kann.

Implementierungsschritte

1. Richten Sie die AWS-Kontostruktur ein:
   - Folgen Sie den Anweisungen im Whitepaper Ihre AWS-Umgebung mit mehreren Konten organisieren, um separate AWS-Konten für verschiedene Umgebungen zu erstellen (z. B. Entwicklung, Staging und Produktion).
   - Konfigurieren Sie die entsprechenden Zugriffskontrollen und Berechtigungen für jedes Konto, um den direkten menschlichen Zugriff auf Produktionsumgebungen einzuschränken.

2. Implementieren Sie eine CI/CD-Pipeline:
   - Richten Sie eine CI/CD-Pipeline mithilfe von Services wie AWS CodeBuild und AWS CodePipeline ein.
   - Konfigurieren Sie die Pipeline so, dass Ihr Anwendungscode automatisch erstellt, getestet und in den jeweiligen Umgebungen bereitgestellt wird.
   - Integrieren Sie Code-Repositorys in die CI/CD-Pipeline für die Versions- und Codeverwaltung.
3. Signieren und verifizieren Sie Anwendungspakete:
   - Verwenden Sie AWS Signer oder AWS Key Management Service (AWS KMS), um Ihre Anwendungspakete zu signieren, nachdem sie getestet und validiert wurden.
   - Konfigurieren Sie den Bereitstellungsprozess so, dass die Signaturen der Anwendungspakete überprüft werden, bevor Sie diese in den Zielumgebungen bereitstellen.
4. Externalisieren Sie Konfigurationsdaten:
   - Speichern Sie umgebungsspezifische Konfigurationsdaten in AWS Systems Manager Parameter Store.
   - Ändern Sie Ihren Anwendungscode, um während der Bereitstellung oder Laufzeit Konfigurationsdaten aus dem Parameter Store abzurufen.
5. Implementieren Sie Infrastructure as Code (IaC):
   - Verwenden Sie IaC-Tools wie AWS CloudFormation oder AWS CDK, um Ihre Infrastruktur als Code zu definieren und zu verwalten.
   - Erstellen Sie CloudFormation-Vorlagen oder CDK-Skripts, um die erforderlichen AWS-Ressourcen für Ihre Anwendung bereitzustellen und zu konfigurieren.
   - Integrieren Sie IaC in Ihre CI/CD-Pipeline, um Infrastrukturänderungen zusammen mit Änderungen des Anwendungscodes automatisch bereitzustellen.
6. Implementieren Sie Canary-Bereitstellungen:
   - Konfigurieren Sie Ihren Bereitstellungsprozess so, dass er Canary-Bereitstellungen unterstützt, bei denen Änderungen auf eine Teilmenge der Instances oder Benutzer angewendet werden, bevor Sie sie in der gesamten Produktionsumgebung bereitstellen.
   - Verwenden Sie Services wie AWS CodeDeploy oder AWS ECS, um Canary-Bereitstellungen zu verwalten und die Auswirkungen von Änderungen zu überwachen.
   - Implementieren Sie Rollback-Mechanismen, um zur vorherigen stabilen Version zurückzukehren, falls während der Canary-Bereitstellung Probleme festgestellt werden.
7. Überwachen und prüfen Sie den Prozess:

- Richten Sie Überwachungs- und Protokollierungsmechanismen ein, um Bereitstellungen, die Anwendungsleistung und Infrastrukturänderungen zu verfolgen.
- Verwenden Sie Services wie Amazon CloudWatch und AWS CloudTrail, um Protokolle und Metriken zu sammeln und zu analysieren.
- Führen Sie Audits und Compliance-Prüfungen ein, um die Einhaltung bewährter Methoden für die Sicherheit und regulatorischer Anforderungen zu überprüfen.

8. Führen Sie kontinuierliche Verbesserungen ein:
   - Überprüfen und aktualisieren Sie Ihre Bereitstellungspraktiken regelmäßig und berücksichtigen Sie dabei Feedback und Erfahrungen aus früheren Bereitstellungen.
   - Automatisieren Sie den Bereitstellungsprozess so weit wie möglich, um manuelle Eingriffe und potenzielle menschliche Fehler zu reduzieren.
   - Arbeiten Sie mit funktionsübergreifenden Teams (beispielsweise den Betriebs- oder Sicherheitsteams) zusammen, um die Bereitstellungspraktiken abzustimmen und kontinuierlich zu verbessern.

Wenn Sie diese Schritte befolgen, können Sie sichere und automatisierte Bereitstellungspraktiken in Ihrer AWS-Umgebung implementieren und so die Sicherheit erhöhen, das Risiko menschlicher Fehler verringern und den Bereitstellungsprozess optimieren.

Ressourcen

Zugehörige bewährte Methoden:

- SEC11-BP02 Automatisieren des Testens während des Entwicklungs- und Veröffentlichungslebenszyklus
- DL.CI.2 Automatisches Auslösen von Builds bei Änderungen am Quellcode

Zugehörige Dokumente:

- Beschleunigen von Bereitstellungen in AWS mit effektiver Governance
- Automatisierung sicherer, vollautomatischer Bereitstellungen
- Signieren von Code mithilfe von AWS Certificate Manager Private CA und asymmetrischen Schlüsseln von AWS Key Management Service
- Signieren von Code: eine Vertrauens- und Integritätskontrolle für AWS Lambda

Zugehörige Videos:

- Vollständige Automatisierung: Automatisieren der Pipelines für kontinuierliche Bereitstellung bei Amazon

Zugehörige Beispiele:

- Blau/Grün-Bereitstellungen mit AWS Fargate

SEC11-BP07 Die Sicherheitseigenschaften der Pipelines regelmäßig bewerten

Wenden Sie die Prinzipien der Well-Architected-Säule „Sicherheit“ bei Ihren Pipelines an und achten Sie dabei besonders auf die Trennung von Berechtigungen. Bewerten Sie die Sicherheitseigenschaften Ihrer Pipeline-Infrastruktur regelmäßig. Durch eine effektive Verwaltung der Pipeline-Sicherheit können Sie die Sicherheit der Software sicherstellen, die diese Pipelines durchläuft.

Gewünschtes Ergebnis: Für die Pipelines, die Sie zum Entwickeln und Bereitstellen Ihrer Software verwenden, sollten dieselben empfohlenen Praktiken verwendet werden wie für jeden anderen Workload in Ihrer Umgebung. Die Tests, die Sie in Ihren Pipelines implementieren, können von den Teams, die diese verwenden, nicht bearbeitet werden. Mithilfe temporärer Anmeldeinformationen geben Sie den Pipelines nur die erforderlichen Berechtigungen für die Bereitstellungen, die diese durchführen. Sie implementieren Sicherheitsvorkehrungen, um zu verhindern, dass über die Pipelines Bereitstellungen in den falschen Umgebungen erfolgen. Sie konfigurieren Ihre Pipelines so, dass sie einen Status ausgeben, damit die Integrität Ihrer Build-Umgebungen validiert werden kann.

Typische Anti-Muster:

- Sicherheitstests können von Entwicklern umgangen werden.
- Berechtigungen für Bereitstellungs-Pipelines sind übermäßig weit gefasst.
- Pipelines sind nicht für die Validierung von Eingaben konfiguriert.
- Berechtigungen im Zusammenhang mit Ihrer CI/CD-Infrastruktur werden nicht regelmäßig überprüft.
- Langfristige oder fest codierte Anmeldeinformationen werden verwendet.

Vorteile der Nutzung dieser bewährten Methode:

- Größeres Vertrauen in die Integrität der Software, die über die Pipelines entwickelt und bereitgestellt wird.
- Eine Bereitstellung kann angehalten werden, wenn es verdächtige Aktivitäten gibt.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Ihre Bereitstellungs-Pipelines sind eine wichtige Komponente Ihres Softwareentwicklungszyklus und sollten denselben Sicherheitsprinzipien und -praktiken folgen wie jeder andere Workload in Ihrer Umgebung. Hierzu gehören die Implementierung geeigneter Zugriffskontrollen, die Validierung von Eingaben und die regelmäßige Überprüfung der Berechtigungen im Zusammenhang mit Ihrer CI/CD-Infrastruktur.

Stellen Sie sicher, dass die für die Entwicklung und Bereitstellung von Anwendungen verantwortlichen Teams die Sicherheitstests und -prüfungen, die in Ihren Pipelines implementiert sind, nicht bearbeiten oder umgehen können. Diese Trennung von Bereichen trägt dazu bei, die Integrität Ihrer Entwicklungs- und Bereitstellungsprozesse zu wahren.

Ziehen Sie als Ausgangspunkt die Verwendung der Referenzarchitektur für AWS-Bereitstellungs-Pipelines in Betracht. Diese Referenzarchitektur bietet eine sichere und skalierbare Grundlage für das Erstellen Ihrer CI/CD-Pipelines in AWS.

Darüber hinaus können Sie Services wie AWS Identity and Access Management Access Analyzer verwenden, um IAM-Richtlinien mit den geringsten Berechtigungen sowohl für Ihre Pipeline-Berechtigungen als auch als Schritt in Ihrer Pipeline zur Überprüfung von Workload-Berechtigungen zu erstellen. Auf diese Weise können Sie überprüfen, ob Ihre Pipelines und Workloads nur über die erforderlichen Berechtigungen für ihre spezifischen Funktionen verfügen, und so das Risiko unbefugter Zugriffe oder Aktionen verringern.

Implementierungsschritte

- Beginnen Sie mit der Referenzarchitektur für AWS-Bereitstellungs-Pipelines.
- Erwägen Sie, AWS IAM Access Analyzer zu verwenden, um für die Pipelines programmatisch IAM-Richtlinien mit der geringsten Berechtigung zu erstellen.
- Integrieren Sie Ihre Pipelines mit Überwachung und Benachrichtigung, so dass Sie über unerwartete oder ungewöhnliche Aktivitäten benachrichtigt werden. Bei von AWS verwalteten

Services können Sie mithilfe von Amazon EventBridge Daten an Ziele wie AWS Lambda oder Amazon Simple Notification Service (Amazon SNS) umleiten.

Ressourcen

Zugehörige Dokumente:

- AWS Referenzarchitektur für -Bereitstellungs-Pipelines
- Überwachung von AWS CodePipeline
- Bewährte Methoden für die Sicherheit für AWS CodePipeline

Zugehörige Beispiele:

- DevOps-Überwachungs-Dashboard (GitHub)

SEC11-BP08 Ein Programm entwickeln, das den Workload-Teams die Verantwortung für die Sicherheit überträgt

Entwickeln Sie ein Programm oder einen Mechanismus, das bzw. der es Entwicklerteams ermöglicht, Entscheidungen bezüglich der Sicherheit der von ihnen erstellten Software zu treffen. Zwar muss Ihr Sicherheitsteam diese Entscheidungen immer noch während einer Überprüfung validieren, die Übertragung der Sicherheitsverantwortlichkeit auf Entwicklerteams ermöglicht jedoch eine schnellere und sicherere Workload-Entwicklung. Zudem fördert dieser Mechanismus eine Kultur der Verantwortlichkeit, die einen positiven Einfluss auf den Betrieb der von Ihnen entwickelten Systeme hat.

Gewünschtes Ergebnis: Sie haben die Verantwortung für Sicherheit und die Entscheidungsfindung in Ihren Teams verankert. Sie haben Ihre Teams entweder in Bezug auf die richtige Einstellung zur Sicherheit geschult oder die Teams um integrierte oder dem Team zugewiesene Sicherheitsmitarbeiter erweitert. So können Ihre Teams früher im Entwicklungszyklus bessere Sicherheitsentscheidungen treffen.

Typische Anti-Muster:

- Einem Sicherheitsteam werden alle Entscheidungen bezüglich des Sicherheitsdesigns überlassen.
- Sicherheitsanforderungen werden nicht früh genug im Entwicklungsprozess behandelt.

- Es wird kein Feedback von Entwicklern und Sicherheitsexperten zum Betrieb des Programms eingeholt.

Vorteile der Nutzung dieser bewährten Methode:

- Beschleunigung von Sicherheitsüberprüfungen.
- Verringerung von Sicherheitsproblemen, die erst in der Phase der Sicherheitsüberprüfung erkannt werden.
- Verbesserung der gesamten Qualität der Software, die geschrieben wird.
- Möglichkeit, systemische Probleme oder Bereiche mit hoher Wertverbesserung zu identifizieren und zu verstehen.
- Verringerung der erforderlichen Überarbeitung aufgrund von Erkenntnissen aus der Sicherheitsüberprüfung.
- Verbesserung bei der Wahrnehmung der Sicherheitsfunktion.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

Implementierungsleitfaden

Beginnen Sie mit der Anleitung unter SEC11-BP01 Für Anwendungssicherheit schulen. Bestimmen Sie danach das Betriebsmodell für das Programm, von dem Sie denken, dass es am besten für Ihre Organisation geeignet ist. Die zwei Hauptmuster sind, Entwickler zu schulen oder Sicherheitsexperten in Entwicklungsteams einzubetten. Nachdem Sie sich für eine anfängliche Verfahrensweise entschieden haben, sollten Sie eine Pilotphase mit einem einzelnen Team oder einer kleinen Gruppe von Workload-Teams durchführen, um sich zu vergewissern, dass das Modell für Ihre Organisation funktioniert. Unterstützung der Führungskräfte aus dem Entwicklungs- und Sicherheitsbereich der Organisation hilft bei der Durchführung und trägt zum Erfolg des Programms bei. Bei der Entwicklung dieses Programms ist es wichtig, Metriken auszuwählen, die Aufschluss über den Wert des Programms geben. Zu erfahren, wie AWS mit diesem Problem umgegangen ist, ist eine gute Lernerfahrung. Diese bewährte Methode konzentriert sich auf die Veränderung und Kultur der Organisation. Die von Ihnen eingesetzten Tools sollten die Zusammenarbeit zwischen der Entwickler- und Sicherheits-Community unterstützen.

Implementierungsschritte

- Beginnen Sie damit, Ihre Entwickler im Bereich der Anwendungssicherheit zu schulen.

- Schaffen Sie eine Community und ein Onboarding-Programm zur Schulung von Entwicklern.
- Geben Sie dem Programm einen Namen. Häufig wird etwas wie Guardians, Champions oder Advocates verwendet.
- Bestimmen Sie das Modell, das verwendet werden soll: Schulen Sie Entwickler, betten Sie Sicherheitstechniker ein oder verwenden Sie andere verwandte Sicherheitsrollen.
- Identifizieren Sie Projektsponsoren aus dem Sicherheits- und Entwicklungsbereich sowie gegebenenfalls aus anderen relevanten Gruppen.
- Verfolgen Sie Metriken für die Anzahl der am Programm beteiligten Personen, die für Überprüfungen erforderliche Zeit und das Feedback von Entwicklern und Sicherheitsexperten. Nutzen Sie diese Metriken für Verbesserungen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC11-BP01 Für Anwendungssicherheit schulen
- SEC11-BP02 Automatisieren des Testens während des Entwicklungs- und Veröffentlichungslebenszyklus

Zugehörige Dokumente:

- Konzepte für Bedrohungsmodellierung
- Betrachtung der Cloud-Sicherheits-Governance
- Wie AWS das Security-Guardians-Programm erstellt hat, einen Mechanismus zur Verteilung der Verantwortung in Bezug auf Sicherheit
- Erstellen eines Security-Guardians-Programms zur Verteilung der Verantwortung in Bezug auf Sicherheit

Zugehörige Videos:

- Proaktive Sicherheit: Überlegungen und Ansätze
- Tipps zu AppSec-Tools und Sicherheitskultur von AWS und Toyota Motor North America

Schlussfolgerung

Sicherheit ist immer ein wichtiges Thema. Vorfälle sollten als Chancen zur Verbesserung der Sicherheit einer Architektur betrachtet werden. Jede Organisation sollte tiefgreifende Verteidigungsmechanismen haben, wie etwa starke Identitätskontrollen, automatisierte Reaktionen auf Sicherheitsvorfälle, Schutzmechanismen auf mehreren Ebenen der Infrastruktur sowie die Verschlüsselung gut klassifizierter Daten. Dieser Aufwand ist dank der in diesem paper erörterten programmatischen Funktionen, AWS Merkmale und Dienste einfacher.

AWS ist bestrebt, Sie beim Aufbau und Betrieb von Architekturen zu unterstützen, die Informationen, Systeme und Ressourcen schützen und gleichzeitig einen geschäftlichen Nutzen bieten.

Mitwirkende

Folgende Personen und Organisationen haben zu diesem Dokument beigetragen:

- Jay Michael, Principal Security Lead Solutions Architect, Amazon Web Services
- Kiaan Sumeet, Principal Security Consultant, Amazon Web Services
- Michael Fischer, Principal Solutions Architect, Amazon Web Services
- Conor Colgan, Principal Solutions Architect, Amazon Web Services
- Dave Walker, Principal Solutions Architect, Security & Compliance, Amazon Web Services
- Patrick Palmer, Principal Solutions Architect, Security & Compliance, Amazon Web Services
- Monka Vu Minh, Security Consultant, Amazon Web Services
- Kurt Kumar, Security Consultant, Amazon Web Services
- Fahima Khan, Security Solutions Architect, Amazon Web Services
- Mutaz Hajeer, Senior Security Solutions Architect, Amazon Web Services
- Luis Pastor, Senior Security Solutions Architect, Amazon Web Services
- Colin Igbokwe, Senior Security Solutions Architect, Amazon Web Services
- Geoff Sweet, Senior Security Solutions Architect, Amazon Web Services
- Anthony Harvey, Senior Security Solutions Architect, Amazon Web Services
- Sowjanya Rajavaram, Senior Security Solutions Architect, Amazon Web Services
- Krishna Prasad, Senior Solutions Architect, Amazon Web Services
- Faisal Farooq, Senior Solutions Architect, Amazon Web Services
- Arun Krishnaswamy, Senior Solutions Architect, Amazon Web Services
- Dan Girard, Senior Solutions Architect, Amazon Web Services
- Marc Luescher, Senior Solutions Architect, Amazon Web Services
- Kyle Nicodemus, Senior Technical Account Manager, Amazon Web Services
- Irina Szabo, Senior Technical Account Manager, Amazon Web Services
- Arun Sivaraman, Solutions Architect, Amazon Web Services
- Stephen Novak, Technical Account Manager, Amazon Web Services
- Jonathan Risbrook, Technical Account Manager, Amazon Web Services
- Freddy Kasprzykowski, Practice Manager - Global Financial Services, Amazon Web Services
- Pat Gaw, Principal Security Consultant, Amazon Web Services

- Jason Garman, Principal Security Solutions Architect, Amazon Web Services
- Mark Keating, Principal Security Solutions Architect, Amazon Web Services
- Zach Miller, Principal Security Solutions Architect, Amazon Web Services
- Maitreya Ranganath, Principal Security Solutions Architect, Amazon Web Services
- Reef Dsouza, Principal Solutions Architect, Amazon Web Services
- Brad Burnett, Security Solutions Architect, Amazon Web Services
- Matt Saner, Senior Manager, Security Solutions Architecture, Amazon Web Services
- Priyank Ghedia, Senior Security Solutions Architect, Amazon Web Services
- Arthur Mnev, Senior Security Solutions Architect, Amazon Web Services
- Kyle Dickinson, Senior Security Solutions Architect, Amazon Web Services
- Kevin Boland, Senior Security Solutions Architect, Amazon Web Services
- Anna McAbee, Senior Security Solutions Architect, Amazon Web Services
- Recep Meric Degirmenci, Senior Security Solutions Architect, Amazon Web Services
- Daniel Salzedo, Senior Security Technical Product Manager, Amazon Web Services
- Jake Izumi, Senior Solutions Architect, Amazon Web Services
- Bert Bullough, Senior Solutions Architect, Amazon Web Services
- Robert McCall, Solutions Architect, Amazon Web Services
- Angela Chao, ESL TAM, AWS Enterprise Support, Amazon Web Services
- Pratima Singh, Senior ANZ Security Spec. Solutions Architect, Amazon Web Services
- Darran Boyd, Principal, Office of the CISO, AWS Security, Amazon Web Services
- Byron Pogson, Senior Security Solutions Architect, Amazon Web Services

Weitere Informationen

Weitere Informationen erhalten Sie in den folgenden Quellen:

- Whitepaper zum AWS Well-Architected Framework
- AWS -Architekturzentrum

Dokumentversionen

Abonnieren Sie den RSS-Feed, um über Aktualisierungen des Whitepapers benachrichtigt zu werden.

Änderung	Beschreibung	Datum
Leitfäden zu bewährten Methoden aktualisiert	Aktualisierung von bewährten Methoden, mit neuen Leitlinien in den folgenden Bereichen: SEC 2, SEC 3, SEC 4, SEC 6, SEC 7, SEC 8, SEC 9, SEC 10 und SEC 11. Die Leitlinien wurden in allen Bereichen aktualisiert und präzisiert.	6. November 2024
Leitfäden zu bewährten Methoden aktualisiert	In der gesamten Säule wurden umfangreiche Aktualisierungen der bewährten Methoden vorgenommen. Zahlreiche bewährte Methoden wurden neu angeordnet und konsolidiert. Signifikante Änderungen in SEC 1, 4, 5, 6, 7, 8 und 9	27. Juni 2024
Leitfäden zu bewährten Methoden aktualisiert	Bewährte Methoden wurden mit neuen Leitfäden in den folgenden Bereichen aktualisiert: Sicheres Betreiben Ihrer Workloads und Schutz von Daten während der Übertragung.	6. Dezember 2023
Leitfäden zu bewährten Methoden aktualisiert	Wichtige Aktualisierungen der Leitfäden und bewährten Methoden in Vorfallreaktion.	3. Oktober 2023

	Mehrere bewährte Methoden in Vorbereitung aktualisiert. Zwei neue Bereiche zu „Vorfallreaktion“ hinzugefügt: Betrieb und Aktivität nach Vorfällen. Neue bewährte Methode SEC10-BP08 Entwickeln eines Frameworks, um aus Vorfällen zu lernen hinzugefügt.	
Leitfäden zu bewährten Methoden aktualisiert	Bewährte Methoden wurden mit neuen Leitfäden in den folgenden Bereichen aktualisiert: Vorbereiten und Simulieren.	13. Juli 2023
Aktualisierungen für das neue Framework.	Bewährte Methoden mit verbindlichen Anleitungen aktualisiert und neue bewährte Methoden hinzugefügt. Abschnitt für bewährte Methoden für die Anwendungssicherheit (AppSec) hinzugefügt.	10. April 2023
Whitepaper aktualisiert	Bewährte Methoden mit neuen Implementierungsanleitungen aktualisiert.	15. Dezember 2022
Whitepaper aktualisiert	Weitere bewährte Methoden und Verbesserungspläne hinzugefügt.	20. Oktober 2022
Kleines Update	IAM-Information aktualisiert, um die aktuellen bewährten Methoden widerzuspiegeln.	28. Juni 2022

Kleines Update	Zusätzliche AWS PrivateLink-Informationen hinzugefügt und fehlerhafte Links korrigiert.	19. Mai 2022
Kleines Update	AWS PrivateLink hinzugefügt.	6. Mai 2022
Kleines Update	Nicht inklusive Sprache entfernt.	22. April 2022
Kleines Update	Informationen über VPC Network Access Analyzer hinzugefügt.	2. Februar 2022
Kleines Update	Fehlerhafter Link behoben.	27. Mai 2021
Kleines Update	Redaktionelle Änderungen im gesamten Dokument.	17. Mai 2021
Größere Aktualisierung	Abschnitt über Governance hinzugefügt, verschiedene Abschnitte detaillierter gestaltet, neue Features und Services hinzugefügt.	7. Mai 2021
Kleines Update	Links aktualisiert.	10. März 2021
Kleines Update	Fehlerhafter Link behoben.	15. Juli 2020
Aktualisierungen für das neue Framework	Anleitung zur Konto-, Identitäts- und Berechtigungsverwaltung aktualisiert.	8. Juli 2020
Aktualisierungen für das neue Framework	Aktualisiert mit zusätzlichen Ratschlägen in allen Bereichen sowie neuen bewährten Methoden, Services und Features.	30. April 2020

Whitepaper aktualisiert	Aktualisierungen bezüglich neuer AWS-Services und -Features sowie aktualisierte Verweise.	1. Juli 2018
Whitepaper aktualisiert	Aktualisierung des Abschnitts „Konfiguration und Wartung der Systemsicherheit“ mit neuen AWS-Services und -Features.	1. Mai 2017
Erste Veröffentlichung	Säule „Sicherheit“ des AWS Well-Architected-Framework veröffentlicht.	1. November 2016

Hinweise

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS Produktangebote und Praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWS Produkte oder Dienstleistungen werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. Die Verantwortlichkeiten und Verbindlichkeiten AWS gegenüber seinen Kunden werden durch AWS Vereinbarungen geregelt, und dieses Dokument ist weder Teil einer Vereinbarung zwischen AWS und seinen Kunden noch ändert es diese.

AWS Glossar

Die neueste AWS Terminologie finden Sie im AWS Glossar in der AWS-Glossar Referenz.