AWS Well-Architected Framework

Säule „Sicherheit“

Säule „Sicherheit“ : AWS Well-Architected Framework

Table of Contents

Säule „Sicherheit“ – AWS Well-Architected Framework

Veröffentlichungsdatum: 27. Juni 2024 (Dokumentversionen)

Der Schwerpunkt dieses Dokuments liegt auf 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 Systemen 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, Ihren 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:

- Operative Exzellenz
- Sicherheit
- Zuverlässigkeit
- Leistungseffizienz
- Kostenoptimierung
- Nachhaltigkeit

Dieses Whitepaper konzentriert sich auf die 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 Praktiken in diesem Whitepaper können Sie Architekturen erstellen, die Ihre Daten und Systeme schützen, den Zugriff steuern und bei Sicherheitsereignissen automatisch reagieren.

Sicherheitsgrundlagen

In der Säule der Sicherheit wird beschrieben, wie Sie Cloud-Technologien nutzen, um Daten, Systeme und Komponenten so zu schützen, dass sich Ihre Sicherheitslage verbessert. 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: Implementieren Sie das Prinzip der geringsten Rechte 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: Wenden Sie einen umfassenden Verteidigungsansatz mit mehreren Sicherheitskontrollen an. 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 Daten nach Sensibilität und Nutzungsmechanismen wie Verschlüsselung, Tokenisierung und Zugriff, sofern zutreffend.
- Trennen von Benutzern und Daten: Verwenden Sie Mechanismen und Tools, um den direkten Zugriff oder die manuelle Verarbeitung von Daten zu reduzieren oder gänzlich zu eliminieren. 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 zur Vorfallverwaltung

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
- Vorfallsreaktion
- Anwendungssicherheit

Geteilte Verantwortung

Sicherheit und Compliance sind eine geteilte Verantwortung zwischen AWS und dem Kunden. 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.

Verantwortung von AWS für die Sicherheit der Cloud – AWS ist für den Schutz der Infrastruktur verantwortlich, auf der alle in AWS Cloud angebotenen Services betrieben werden. Diese Infrastruktur umfasst die Hardware, Software, Netzwerke und Einrichtungen, in bzw. auf denen AWS-Cloud-Services ausgeführt werden.

Verantwortung des Kunden für die Sicherheit in der Cloud – Die Verantwortung des Kunden wird durch die von ihm gewählten AWS-Cloud-Services bestimmt. 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.

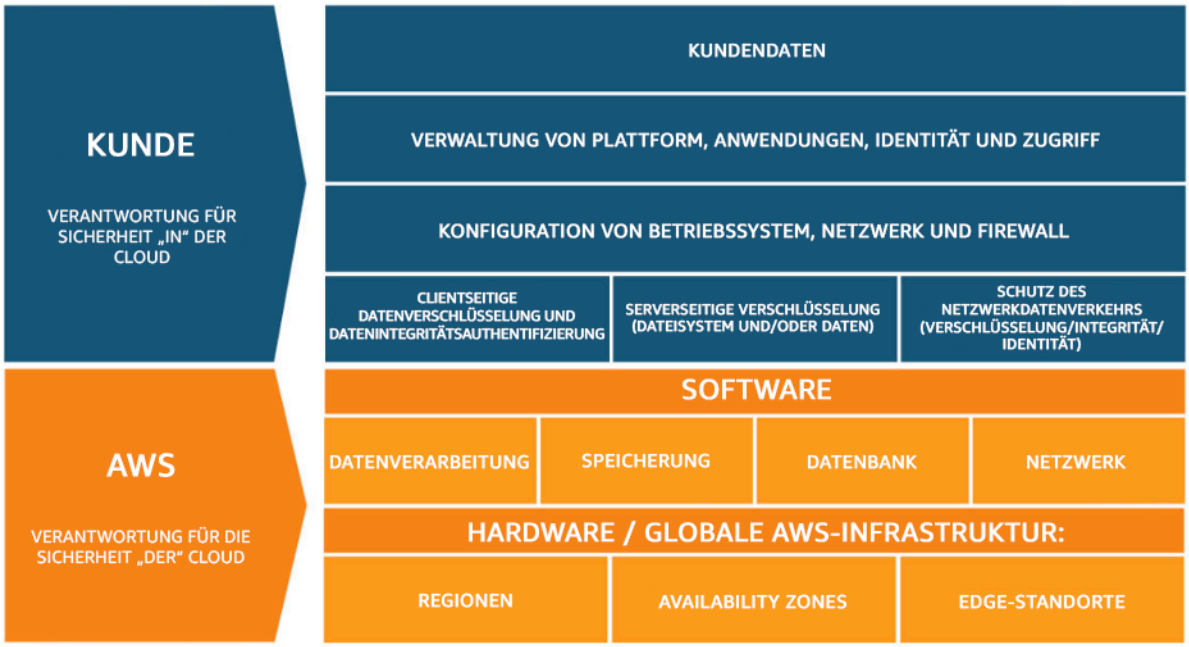


Abbildung 1: Das AWS-Modell der geteilten Verantwortung.

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 ein Kunde vollständig von AWS erbt.

- Physische Kontrollen und Umgebungskontrollen

Verteilte Kontrollen – Kontrollen, die sowohl für die Infrastrukturebene als auch für die Kundenebene gelten, jedoch in unterschiedlichen Zusammenhängen oder aus unterschiedlichen 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. Einige Beispiele sind:

- Patch Management – AWS ist für das Patchen und Beheben von Fehlern innerhalb der Infrastruktur zuständig, aber die Kunden sind für das Patchen ihres Gastbetriebssystems und ihrer Anwendungen verantwortlich.
- Konfigurationsmanagement – AWS verwaltet die Konfiguration seiner Infrastrukturgeräte, aber die Kunden sind für die Konfiguration ihrer eigenen Gastbetriebssysteme, Datenbanken und Anwendungen verantwortlich.
- Sensibilisierung und Schulung – AWS schult AWS-Mitarbeiter, aber die Kunden müssen ihre eigenen Mitarbeiter schulen.

Kundenspezifisch – Kontrollen, die allein in der Verantwortung der Kunden liegen, basierend auf den Anwendungen, die sie innerhalb der AWS-Services einsetzen. Einige Beispiele sind:

- 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 erben. Eine nützliche Ressource ist AWS Artifact,das 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. Das 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. Das ist das

Restrisiko. Kontrollziele können sich auf einen 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.

Wahrschein-lichkeit	Risikostufe				
Sehr wahrscheinlich	Niedrig	Mittel	Hoch	Kritisch	Kritisch
Wahrscheinlich	Niedrig	Mittel	Mittel	Hoch	Kritisch
Möglich	Niedrig	Niedrig	Mittel	Mittel	Hoch
Unwahrscheinlich	Niedrig	Niedrig	Mittel	Mittel	Hoch
Sehr unwahrscheinlich	Niedrig	Niedrig		Mittel	Hoch
Folge	Geringfügig	Niedrig	Mittel	Hoch	Schwerwiegend

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-Kontenund 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 Stammbenutzer ist, der das Zurücksetzen des Passworts ermöglicht. Mit Organizations können Sie Konten in Organisationseinheiten (OEs) gruppieren, die je nach Anforderungen und Zweck des Workloads 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 Leitlinien 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 Ihrem Unternehmen durchgeführten Aktionen mithilfe von AWS CloudTrailkonfigurieren und verhindern, dass Mitgliedskonten die Protokollierung deaktivieren. Sie können auch Daten für Regeln, die Sie mit AWS Configdefiniert haben, zentral aggregieren, sodass Sie Ihre Workloads auf Compliance prüfen und schnell auf Änderungen reagieren können. AWS CloudFormation Mit StackSets können Sie AWS CloudFormation-Stacks in Ihrem Unternehmen über Konten und Organisationseinheiten hinweg zentral verwalten. Auf diese Weise können Sie automatisch ein neues Konto bereitstellen, um Ihre Sicherheitsanforderungen zu erfüllen.

Verwenden Sie die Funktion „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.

Bewährte Methoden

- 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-Operationen, 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 einen 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, wenn diese bewährte Methode nicht eingeführt wird: 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. Für Erläuterungen der Konzepte, Muster und der Implementierung einer Mehrkonten-Strategie auf AWS siehe Organisation Ihrer AWS-Umgebung mit mehreren Konten.

Wenn Sie mehrere AWS-Konten zentral verwalten, sollten Ihre Konten in einer gemäß den Ebenen der Organisationseinheiten (OUs) definierten Hierarchie organisiert sein. Dadurch können Sicherheitskontrollen anhand der OUs 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 OU-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 Ebenen von OUs definierten Hierarchie, wobei jede OU eine Anzahl 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.

Über AWS Organizations hinaus ermöglicht AWS Control Tower die Einrichtung bewährter Methoden mit einem Klick für eine Mehrkonten-AWS-Umgebung mit einer Landing Zone. Die Landing Zone ist der Einstiegspunkt für die Mehrkonten-Umgebung, eingerichtet von Control Tower. Control Tower bietet verschiedene 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 OUs 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 OU-Struktur: Eine korrekt gestaltete OU-Struktur reduziert den Verwaltungsaufwand für die Erstellung und Wahrung von Service-Kontrollrichtlinien und anderen Sicherheitskontrollen. Ihre OU-Struktur sollte an Ihre geschäftlichen Anforderungen, die Sensitivität der Daten und die Workload-Struktur angepasst sein.
2. Erstellen einer Landing Zone für Ihre Mehrkonten-Umgebung: Eine Landing Zone bietet eine konsistente Sicherheits- und Infrastrukturbasis, von der aus Ihre Organisation Workloads schnell entwickeln, starten und bereitstellen kann. Sie können eine individuell erstellte Landing Zone oder AWS Control Tower 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 AWSCloudFormation StackSets: StackSets helfen dabei, Ressourcen wie IAM-Richtlinien, -Rollen und -Gruppen aus einer genehmigten Vorlage in verschiedenen AWS-Konten und Regionen bereitzustellen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC02-BP04 Verlassen auf einen zentralen Identitätsanbieter

Zugehörige Dokumente:

- AWS Control Tower
- AWS Security Audit Guidelines (Richtlinien zur AWS-Sicherheitsprüfung)
- IAM Best Practices (Bewährte Methoden für IAM)
- Use CloudFormation StackSets to provision resources across multiple AWS-Konten and regions (Verwendung von CloudFormation StackSets zur Bereitstellung von Ressourcen für mehrere AWS-Konten und Regionen)
- Organizations FAQ (Häufig gestellte Fragen zu Organisationen)
- AWS Organizations terminology and concepts (AO-Terminologie und -Konzepte)
- Best Practices for Service Control Policies in an AWS Organizations Multi-Account Environment (Bewährte Methoden für Service-Kontrollrichtlinien in einer AO-Mehrkonten-Umgebung)
- AWS Account Management Reference Guide (Referenz zur Verwaltung von AWS-Konten)

- Organizing Your AWS Environment Using Multiple Accounts (Organisieren der AWS-Umgebung mithilfe mehrerer Konten)

Zugehörige Videos:

- Enable AWS adoption at scale with automation and governance(AWS-Übernahme in großem Umfang mit Automatisierung und Governance)
- Security Best Practices the Well-Architected Way (Bewährte Sicherheitsmethoden mit durchdachter Architektur)
- Building and Governing Multiple Accounts using AWS Control Tower (Aufbau und Verwaltung mehrerer Konten mit AWS Control Tower)
- Enable Control Tower for Existing Organizations (Aktivierung von Control Tower für bestehende Organisationen)

Zugehörige Workshops:

- Control Tower Immersion Day

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: Der Schutz 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, wenn diese bewährte Methode nicht eingeführt wird: 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 Prüfung 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 der Root-Benutzer des AWS-Konto bezeichnet. Sie können sich mit der E-Mail-Adresse und dem Passwort, die bei der Konto-Erstellung verwendet wurden, als Root-Benutzer anmelden. 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) aktiviert sein.

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 DNS (Domain Name Service)-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 korrekte 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. Aktivieren 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 Backup. Pro Konto sind bis zu 8 MFA-Geräte zulässig.
        - Beachten Sie, dass die Verwendung von mehr als einem 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 der Zugriff darauf erforderlich wäreAWS-Konto, 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.

Aufdeckende Kontrollen

- Erstellen Sie Alarme, um die Verwendung der Root-Anmeldeinformationen zu erkennen (CIS 1.7). Ist Amazon GuardDuty aktiviert, wird die Nutzung der API-Anmeldeinformationen des Root-Benutzers überwacht und Sie werden über das Ergebnis von RootCredentialUsage benachrichtigt.
- Evaluieren und implementieren Sie die AWSim Well-Architected Security Pillar Conformance Pack enthaltenen aufdeckenden Kontrollen für AWS Config oder, falls SieAWS Control Tower verwenden, die nachdrücklich empfohlenen Kontrollen, die in Control Tower verfügbar sind.

Operationale 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. Konsultieren Sie den AWS-Reaktionsleitfaden für Sicherheitsvorfälle und die bewährten Methoden im Abschnitt zu Notfallreaktionen im Whitepaper der Säule „Sicherheit“ für weitere Informationen zum Aufbau einer Sicherheitsstrategie für Ihr AWS-Konto.

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 Security Audit Guidelines (Richtlinien zur AWS-Sicherheitsprüfung)
- IAM Best Practices (Bewährte Methoden für IAM)
- Amazon GuardDuty – root credential usage alert (Amazon GuardDuty – Alarm bei Verwendung der Root-Anmeldeinformationen)
- Step-by-step guidance on monitoring for root credential use through CloudTrail (Schritt-für-Schritt-Anleitung zur Überwachung der Verwendung von Root-Anmeldeinformationen mit CloudTrail)
- MFA tokens approved for use with AWS (Zur Verwendung mit AWS genehmigte MFA-Tokens)
- Implementing break glass access on AWS (Implementieren des „Break Glass“-Zugriffs in AWS)

- Top 10 security items to improve in your AWS-Konto (Die 10 wichtigsten Sicherheitsverbesserungen für Ihr AWS-Konto)
- What do I do if I notice unauthorized activity in my AWS-Konto? (Was muss ich tun, wenn ich unbefugte Aktivitäten in meinem AWS-Konto erkenne?)

Zugehörige Videos:

- Enable AWS adoption at scale with automation and governance (AWS-Übernahme in großem Umfang mit Automatisierung und Governance)
- Security Best Practices the Well-Architected Way (Bewährte Sicherheitsmethoden mit durchdachter Architektur)
- Limiting use of AWS root credentials from AWS re:inforce 2022 – Security best practices with AWS IAM (Einschränkung der Verwendung der AWS-Root-Anmeldeinformationen von der AWS re:inforce 2022 – Bewährte Sicherheitsmethoden mit AWS IAM)

Zugehörige Beispiele und Workshops:

- Lab: AWS-Konto und Root-Benutzer

Sicheres Betreiben Ihrer Workloads

Das sichere Betreiben von Workloads deckt den gesamten Lebenszyklus eines Workloads 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 einen bestimmten Workload erfüllt werden und für diesen 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 auf jeden Sicherheitsbereich übergreifende bewährte Methoden anwenden. Nutzen Sie Anforderungen und Prozesse, die Sie in Operational Excellence definiert haben, auf Organisations- und Workload-Ebene, und wenden Sie sie auf alle Bereiche an. Bleiben Sie auf dem Laufenden mit AWS- und Branchenempfehlungen sowie

Bedrohungsinformationen, um Ihr Bedrohungsmodell und Ihre Kontrollziele weiterzuentwickeln. 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 Dienste, 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.

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-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 Ihren 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, wenn diese bewährte Methode nicht eingeführt wird: 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 in den 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 Ihrem 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 einsetzen möchten, die sich an Ihren Cybersicherheits-Rahmenbedingungen orientieren, sollten Sie die Verwendung von AWS Security Hub-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 nicht über die gewünschten Kontrollmeldungen verfügt, kann es durch AWS Config-Konformitätspakete ergänzt werden.

Verwenden Sie APN-Partner-Pakete, 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-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 Einführung 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, wenn diese bewährte Methode nicht eingeführt wird: 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 Sicherheitslücken 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-Funktionen verwendet. Sowohl AWS WAF als auch AWS Shield Advanced bieten verwaltete Regelgruppen, die automatisch aktualisiert werden, wenn neue Bedrohungen auftauchen.

Sehen Sie sich die Säule „Operative Exzellenz“ – AWS-Well-Architected-Framework an, um mehr über automatisiertes Flottenmanagement und Patching zu erfahren.

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 Best Practices der Säule „Operative Exzellenz“ – AWS-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 Backups.

Gewünschtes Ergebnis: Sie berücksichtigen den Umfang Ihrer Sicherheitsverwaltung bei der Auswahl von AWS-Services für Ihren 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 Einführung 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, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Es gibt mehrere Möglichkeiten, wie Sie die Komponenten Ihres Workloads 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 der 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 bei der Gestaltung 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 Dienst 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 Ihres Workloads, die durch einen verwalteten Service ersetzt werden können.
   a. Wenn Sie einen 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, Rebuild 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 Ihren 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 den 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 2023 – 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 IaC-Vorlagen (Infrastructure as Code), 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 Self-Service-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 Einführung 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 Self-Service-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, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Wenn Sie die in SEC01-BP01 Trennen von Workloads mithilfe von Konten beschriebenen Verfahrensweisen befolgen, erhalten Sie am Ende mehrere AWS-Konten für verschiedene Umgebungen, die Sie unter Verwendung von 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-Praktiken, 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 Self-Service-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 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 einer Versionskontrolle
- OPS05-BP04 Einsatz von Systemen zur Bild- und Bereitstellungsverwaltung
- REL08-BP05 Automatisieren von Änderungen
- SUS06-BP01 Einführen von Methoden, die schnelle Verbesserungen für die Nachhaltigkeit ermöglichen

Zugehörige Dokumente:

- Organizing Your AWS Environment Using Multiple Accounts

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 Ihren 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 Ihres Workloads und der sich entwickelnden Sicherheitslandschaft aktuell.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: 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) Application Threat Modeling

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 Ihres Workloads. 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 Funktionen 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 gemeinsamen 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 Post zum Thema Bedrohungsmodellierungskonzepte im AWS Security Blog.

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:

- Schreiben Sie nützliche, an der Bedrohungsgrammatik ausgerichtete Bedrohungserklärungen, 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 Security Blog)
- NIST: Guide to Data-Centric System Threat Modelling

Zugehörige Videos:

- AWS Summit ANZ 2021 - How to approach threat modelling
- AWS Summit ANZ 2022 - Scaling security – Optimise for fast and secure delivery

Zugehöriges Training:

- Threat modeling the right way for builders – AWS Skill Builder virtual self-paced training
- 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 Ihren 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 Einführung 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, wenn diese bewährte Methode nicht eingeführt wird: niedrig

Implementierungsleitfaden

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

- Neuigkeiten zu AWS
- AWS News Blog
- AWS Security Blog
- AWS-Sicherheitsberichte
- Überblick über die AWS-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 bieten ihre eigenen SNS-Themen an, um über neue Standards, Erkenntnisse und andere Aktualisierungen für diese speziellen Services informiert zu bleiben.

Neue Services und Funktionen 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-Sitzungen online auf dem AWS-Events-Kanal auf YouTube 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 den 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 -Funktionen
- 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

Identitätsmanagement

Es gibt zwei Arten von Identitäten, die Sie beim Betrieb sicherer AWS-Workloads verwalten müssen.

- Menschliche Identitäten: Die Administratoren, Entwickler, Bediener und Benutzer Ihrer Anwendungen benötigen eine Identität für den Zugriff auf Ihre AWS-Umgebungen und -Anwendungen. Es kann sich hierbei um Mitglieder Ihrer Organisation oder um externe Benutzer handeln, mit denen Sie zusammenarbeiten und die mit Ihren AWS-Ressourcen über einen Webbrowser, eine Client-Anwendung, mobile Anwendung oder interaktive Befehlszeilen-Tools interagieren.
- 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 Maschinen, die in Ihrer AWS-Umgebung ausgeführt werden, z. B. Amazon EC2-Instances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus verfügen Sie möglicherweise auch über Maschinen außerhalb von AWS, die Zugriff auf Ihre AWS-Umgebung benötigen.

Bewährte Methoden

- 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 (die Authentifizierung unter Verwendung von Anmeldeinformationen) kann 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: Senkung des Risikos unbeabsichtigter Zugriffe auf Anmeldeinformationen in AWS durch die Verwendung starker Anmeldemechanismen für AWS Identity and Access Management (IAM)-Benutzer, den Root-Benutzer des AWS-Konto, AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) und externe Identitätsanbieter. 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 Kontrollmechanismen für verdächtige Anmeldevorgänge.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Es gibt viele Möglichkeiten zur Anmeldung für menschliche Identitäten bei AWS. Eine bewährte AWS-Methode besteht darin, einen zentralisierten Identitätsanbieter mit Verbundverfahren (direkter Verbund oder unter Verwendung von AWS IAM Identity Center) für die Authentifizierung bei AWS zu verwenden. In diesem Fall sollten Sie einen sicheren Anmeldeprozess mit Ihrem Identitätsanbieter oder Microsoft Active Directory einrichten.

Wenn Sie ein AWS-Konto zum ersten Mal einrichten, beginnen Sie mit einem Root-Benutzer für das AWS-Konto. Sie sollten den Root-Benutzer des Kontos nur zur Einrichtung des Zugriffs für Ihre

Benutzer (und für Aufgaben, die den Root-Benutzer erfordern) verwenden. Es ist wichtig, MFA für den Root-Benutzer des Kontos sofort nach der Einrichtung Ihres AWS-Konto zu aktivieren, und den Root-Benutzer anhand der Anleitung zu bewährten Methoden von AWS zu schützen.

Wenn Sie in AWS IAM Identity Center Benutzer erstellen, dann sollten Sie auch den Anmeldeprozess in diesem Service schützen. Für Verbraucheridentitäten können Sie Amazon Cognito user pools verwenden und den Anmeldeprozess in diesem Service schützen oder indem Sie einen der von Amazon Cognito user pools unterstützten Identitätsanbieter verwenden.

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

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

Implementierungsschritte

Es folgen allgemeine Empfehlungen für starke Anmeldeverfahren. Die tatsächlich konfigurierten Einstellungen sollten von Ihrer Unternehmensrichtlinie oder von einem Standard wie NIST 800-63 vorgegeben werden.

- Setzen Sie MFA voraus. Ein bewährtes IAM-Verfahren besteht darin, MFA für menschliche Identitäten und Workloads vorauszusetzen. 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.
- Erlauben Sie Benutzern, Ihr eigenes Passwort zu ändern.
- Erstellen Sie individuelle Identitäten anstelle gemeinsam genutzter Anmeldeinformationen. Durch das Erstellen individueller Identitäten können Sie jedem Benutzer einen einmaligen Satz mit Sicherheitsanmeldeinformationen zuweisen. Individuelle Benutzer bieten die Möglichkeit, die Aktivität der einzelnen Benutzer zu prüfen.

Empfehlungen für IAM Identity Center:

- Bei Verwendung des Standardverzeichnisses bietet IAM Identity Center eine vordefinierte Passwortrichtlinie, die die Passwortlänge, -komplexität und die Anforderungen im Zusammenhang mit der erneuten Verwendung festlegt.

- Aktivieren Sie MFA und konfigurieren Sie die kontextsensitive oder ständig aktive Einstellung für MFA, wenn die Identitätsquelle das Standardverzeichnis, AWS Managed Microsoft AD oder AD Connector ist.
- Erlauben Sie Benutzern die Registrierung ihrer eigenen MFA-Geräte.

Verzeichnisempfehlungen für Amazon Cognito user pools:

- Konfigurieren Sie die Einstellungen für die Passwortstärke.
- Verlangen Sie MFA für Benutzer.
- Verwenden Sie die erweiterten Sicherheitseinstellungen von Amazon Cognito user pools für Funktionen wie die adaptive Authentifizierung, die verdächtige Anmeldeversuche blockieren können.

IAM-Benutzerempfehlungen:

- Idealerweise verwenden Sie IAM Identity Center oder den direkten Verbund. Möglicherweise benötigen Sie aber auch IAM-Benutzer. Richten Sie in diesem Fall eine Passwortrichtlinie für IAM-Benutzer ein. Sie können die Passwortrichtlinie verwenden, um Anforderungen wie Mindestlänge zu definieren oder ob das Passwort nicht-alphanumerische Zeichen beinhalten sollte.
- Erstellen Sie eine IAM-Richtlinie, um die MFA-Anmeldung zu erzwingen, damit 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:

- AWS IAM Identity Center (successor to AWS Single Sign-On) Password Policy (Passwortrichtlinie von AWS IAM Identity Center (Nachfolger von AWS Singe Sign-On))
- IAM-Benutzer-Passwortrichtlinie

- Setting the AWS-Konto root user password (Einrichten des Root-Benutzerpassworts für das AWS-Konto)
- Amazon Cognito-Passwortrichtlinie
- AWS-Anmeldeinformationen
- Bewährte Methoden für die Sicherheit in IAM

Zugehörige Videos:

- Managing user permissions at scale with AWS IAM Identity Center (Verwalten von Benutzerberechtigungen in großem Umfang mit AWS IAM Identity Center)
- Mastering identity at every layer of the cake (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: Senkung des Risikos im Zusammenhang mit langfristigen Anmeldeinformationen durch die Verwendung temporärer Anmeldeinformationen, wo immer dies für menschliche und maschinelle Identitäten möglich ist. Langfristige Anmeldeinformationen sind mit vielen Risiken verbunden, so kann es beispielsweise vorkommen, dass sie in Code in öffentliche GitHub-Repositorys hochgeladen werden. Durch die Verwendung temporärer Anmeldeinformationen können Sie die Gefahr der Kompromittierung von Anmeldeinformationen deutlich senken.

Typische Anti-Muster:

- Entwickler verwenden langfristige Zugriffsschlüssel von IAM users, 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.

- Verwendung langfristiger Zugriffsschlüssel für Maschinenidentitäten, 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 müssen in fast jedem Fall mit AWS-Zugriffsschlüsseln signiert werden. Diese Anfragen können mit temporären oder langfristigen Anmeldeinformationen signiert werden. Sie sollten langfristige Anmeldeinformationen (bzw. Zugriffsschlüssel) nur nutzen, wenn Sie einen IAM-Benutzer oder den Root-Benutzer des AWS-Konto verwenden. Wenn Sie einen Verbund mit AWS nutzen oder eine IAM-Rolle über andere Methoden annehmen, werden temporäre Anmeldeinformationen generiert. Selbst wenn Sie mit Anmeldeinformationen auf die AWS Management Console 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 auszuschalten.

Implementierungsschritte

Für menschliche Identitäten wie Mitarbeiter, Administratoren, Entwickler, Bediener und Kunden:

- Sie sollten einen zentralisierten Identitätsanbieter nutzen und von menschlichen Benutzern die Verwendung von Verbundverfahren mit einem Identitätsanbieter verlangen, damit mit temporären Anmeldeinformationen auf AWS zugegriffen wird. Ein Verbund für Ihre Benutzer kann per direktem Verbund zu jedem AWS-Konto oder mit AWSIAM Identity Center (Nachfolger von AWS IAM Identity Center) und dem Identitätsanbieter Ihrer Wahl erreicht werden. Ein Verbund bietet eine Reihe von Vorteilen gegenüber der Verwendung von IAM-Benutzern und eliminiert langfristige Anmeldeinformationen. Ihre Benutzer können auch temporäre Anmeldeinformationen aus der Befehlszeile für einen direkten Verbund oder mit IAM Identity Center anfordern. Dies bedeutet, dass es nur wenige Anwendungsfälle gibt, für die IAM-Benutzer oder langfristige Anmeldeinformationen für Ihre Benutzer erforderlich sind.

- Wenn Dritten, wie beispielsweise Anbietern von Software as a Service (SaaS), der Zugriff auf Ressourcen in Ihrem AWS-Konto gewährt wird, können Sie kontoübergreifende Rollen und ressourcenbasierende Richtlinien verwenden.
- Wenn Sie Verbraucheranwendungen oder Kunden Zugriff auf Ihre AWS-Ressourcen gewähren müssen, können Sie Amazon Cognito-Identitätspools oder Amazon Cognito user pools verwenden, um temporäre Anmeldeinformationen bereitzustellen. Die Berechtigungen für die Anmeldeinformationen werden über IAM-Rollen konfiguriert. Sie können auch eine separate IAM-Rolle mit eingeschränkten Berechtigungen für Gastbenutzer definieren, die nicht authentifiziert sind.

Für Maschinenidentitäten müssen Sie möglicherweise langfristige Anmeldeinformationen verwenden. In solchen Fällen sollten Sie verlangen, dass Workloads temporäre Anmeldeinformationen mit IAM-Rollen zum Zugriff auf AWS verwenden.

- Für Amazon Elastic Compute Cloud (Amazon EC2) können Sie Rollen für Amazon EC2 verwenden.
- AWS Lambda ermöglicht die Konfiguration einer Lambda-Ausführungsrolle, um dem Service Berechtigungen zum Ausführen von AWS-Aktionen unter Verwendung temporärer Anmeldeinformationen zu erteilen. Es gibt zahlreiche ähnliche Modelle für AWS-Services zum Gewähren temporärer Anmeldeinformationen mit IAM-Rollen.
- Für IoT-Geräte können Sie den Anmeldeinformationenanbieter von AWS IoT Core zur Anfrage nach temporären Anmeldeinformationen verwenden.
- Für On-Premises-Systeme oder außerhalb von AWS ausgeführte Systeme, die Zugriff auf AWS-Ressourcen benötigen, können Sie IAM Roles Anywhere verwenden.

Es gibt Szenarien, in denen temporäre Anmeldeinformationen nicht in Frage kommen und stattdessen langfristige Anmeldeinformationen verwendet werden müssen. In solchen Fällen sollten Sie die Anmeldeinformationen regelmäßig prüfen und rotieren sowie die Zugriffsschlüssel für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern, regelmäßig wechseln. Beispiele, bei denen langfristige Anmeldeinformationen erforderlich sind, sind etwa WordPress-Plugins und AWS-Clients von Drittanbietern. In Situationen, die langfristige Anmeldeinformationen erfordern, oder für andere Anmeldeinformationen als AWS-Zugriffsschlüssel, wie z. B. Datenbankanmeldungen, können Sie einen Service verwenden, der für die Verwaltung von Secrets gedacht ist, wie etwa AWS Secrets Manager. Secrets Manager erleichtert die Verwaltung, das Rotieren und die Speicherung

verschlüsselter Secrets unter Verwendung unterstützter Services. Weitere Informationen zur Rotation langfristiger Anmeldeinformationen finden Sie unter Rotation von Zugriffsschlüsseln.

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 Sicherheits-Anmeldeinformationen
- AWS-Anmeldeinformationen
- Bewährte Methoden für die Sicherheit in IAM
- IAM-Rollen
- IAM Identity Center
- Identitätsanbieter und Verbund
- Rotieren der Zugriffsschlüssel
- Partnerlösungen im Bereich Sicherheit: Zugriff und Zugriffssteuerung
- Der Root-Benutzer des AWS-Kontos

Zugehörige Videos:

- Managing user permissions at scale with AWS IAM Identity Center (successor to AWS IAM Identity Center) (Verwalten von Benutzerberechtigungen in großem Umfang mit AWS IAM Identity Center (Nachfolger von AWS IAM Identity Center))
- Mastering identity at every layer of the cake (Beherrschen der Identität auf jeder Ebene)

SEC02-BP03 Sicheres Speichern und Verwenden von Secrets

Ein Workload muss seine 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 für die sichere Verwaltung von Anwendungsanmeldeinformationen, der die folgenden Ziele erreicht:

- Identifikation der für den 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 dem Workload vorhandene Secrets
- Kontinuierliche Überwachung, 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 rotierenden 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 in Übertragung verschlüsselt gespeichert.
- Organisation des Zugriffs auf Anmeldeinformationen über eine API (vorstellbar als Automat für Anmeldeinformationen)
- Prüfung und Protokollierung des Zugriffs (Lese- und Schreibzugriff) auf Anmeldeinformationen
- 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 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 des Workloads nicht mehr benötigt werden und sicher entfernt werden können.

Bei Anmeldeinformationen, die für die korrekte Funktion des Workloads 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 langfristige Anmeldeinformation durch eine 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 aufbewahrt, verwaltet und regelmäßig rotiert werden.

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

Credential type	Description	Suggested strategy
IAM access keys	AWS IAM access and secret keys used to assume IAM roles inside of a workload	Replace: Use IAM-Rollen assigned to the compute instances (such as Amazon EC2 or AWS Lambda) instead. For interoperability with third parties that require access to resources in your AWS-Konto , ask if they support Kontoüber greifender AWS-Zugriff. For

Credential type	Description	Suggested strategy
		mobile apps, consider using temporary credentials through Amazon Cognito-Identitäts pools (Verbundidentitäten). For workloads running outside of AWS, consider IAM Roles Anywhere or AWS Systems Manager Hybride Aktivierungen.
SSH keys	Secure Shell private keys used to log into Linux EC2 instances, manually or as part of an automated process	Replace: Use AWS Systems Manager or EC2 Instance Connect to provide programmatic and human access to EC2 instances using IAM roles.
Application and database credentials	Passwords – plain text string	Rotate: Store credentials in AWS Secrets Manager and establish automated rotation if possible.
Amazon RDS and Aurora Admin Database credentials	Passwords – plain text string	Replace: Use the Secrets Manager-Integration mit Amazon RDS or Amazon Aurora. In addition, some RDS database types can use IAM roles instead of passwords for some use cases (for more detail, see IAM-Datenbankauthentifizierung).
OAuth tokens	Secret tokens – plain text string	Rotate: Store tokens in AWS Secrets Manager and configure automated rotation.

Credential type	Description	Suggested strategy
API tokens and keys	Secret tokens – plain text string	Rotate: Store in AWS Secrets Manager and establish automated rotation if possible.

Ein typisches Anti-Muster ist die Einbettung von IAM-Zugriffsschlüsseln in Quellcode, Konfigurationsdateien oder Mobil-Apps. Wenn ein IAM-Zugriffsschlüssel für die Kommunikation mit einem AWS-Service 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. Bei Verbindungen mit Drittparteien sollten Sie den Zugriff lieber über eine IAM-Rolle mit dem erforderlichen Zugriff auf die Ressourcen Ihres Kontos delegieren, anstatt einen IAM-Benutzer zu konfigurieren und der Drittpartei den geheimen Zugriffsschlüssel für diesen Benutzer zuzusenden.

Es gibt viele Fälle, in denen der Workload die Speicherung von Secrets erfordert, um mit anderen Services und Ressourcen zusammenwirken zu können. AWS Secrets Manager wurde speziell entwickelt, um solche Anmeldeinformationen sowie die Speicherung, Verwendung und Rotation von API-Tokens, Passwörtern und anderer Anmeldeinformationen sicher zu handhaben.

AWS Secrets Manager bietet fünf entscheidende Funktionen, die für die sichere Speicherung und Handhabung sensitiver Anmeldeinformationen sorgen: Verschlüsselung im Ruhezustand, Verschlüsselung in Übertragung, Umfassende Prüfungen, detaillierte Zugriffssteuerung und erweiterbare Rotation von Anmeldeinformationen. Andere Secret-Managementservices von AWS-Partnern oder lokal entwickelte Lösungen mit ähnlichen Funktionen und Sicherungen sind ebenfalls akzeptabel.

Implementierungsschritte

1. Identifizieren Sie Code-Pfade mit hartkodierten Anmeldeinformationen mithilfe automatisierter Tools wie etwa Amazon CodeGuru.
   - Scannen Sie Ihre Code-Repositorys mit Amazon CodeGuru. Sobald die Prüfung abgeschlossen ist, filtern sie nach `Type=Secrets` in CodeGuru, 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, er jedoch IAM-Anmeldeinformationen für den Zugriff auf AWS-Ressourcen benötigt, können Sie IAM Roles Anywhere oder AWS Systems Manager Hybride Aktivierungen verwenden.

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 automatisch ein Secret in Secrets Manager unter Verwendung der erkannten Anmeldeinformationen erstellen.
   b. Integrieren Sie den Secret-Abruf von Secrets Manager in Ihren Anwendungscode.
      - Serverless-Lambda-Funktionen können eine sprachneutrale Lambda-Erweiterung verwenden.
      - Für EC2-Instances oder Container bietet AWS clientseitigen Beispielcode für den Abruf von Secrets von Secrets Manager in verschiedenen verbreiteten Programmiersprachen.
4. Prüfen Sie Ihre Codebasis regelmäßig und wiederholen Sie dies, um sicherzustellen, dass dem Code keine neuen Secrets hinzugefügt wurden.
   - Erwägen Sie die Verwendung eines Tools wie etwa git-secrets, um zu vermeiden, dass neue Secrets in Ihr Quellcode-Repository eingebracht werden.
5. Überwachen Sie die Secrets Manager-Aktivität auf Anzeichen für unerwartete Nutzungen, den unautorisierten Zugriff auf Secrets 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 Introduces Secrets Detector (Amazon CodeGuru stellt Secrets Detector vor)
- How AWS Secrets Manager uses AWS Key Management Service (Wie AWS Secrets Manager AWS Key Management Service verwendet)
- Secret encryption and decryption in Secrets Manager (Secret-Ver- und Entschlüsselung in Secrets Manager)
- Blog-Einträge zu Secrets Manager
- Amazon RDS announces integration with AWS Secrets Manager (Amazon RDS kündigt Integration mit AWS Secrets Manager an)

Zugehörige Videos:

- Best Practices for Managing, Retrieving, and Rotating Secrets at Scale (Bewährte Methoden zum Verwalten, Abrufen und Rotieren von Secrets in großem Umfang)
- Find Hard-Coded Secrets Using Amazon CodeGuru Secrets Detector (Finden hartkodierter Secrets mit CodeGuru Secrets Detector)
- Securing Secrets for Hybrid Workloads Using AWS Secrets Manager (Sichern von Secrets für hybride Workloads mit AWS Secrets Manager)

Zugehörige Workshops:

- Store, retrieve, and manage sensitive credentials in AWS Secrets Manager (Speichern, Abrufen und verwalten sensitiver Anmeldeinformationen in AWS Secrets Manager)
- AWS Systems Manager Hybride Aktivierungen

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 bei fehlender Befolgung dieser Best Practice:: Hoch

Implementierungsleitfaden

Leitfaden für Benutzer im Unternehmen, die auf AWS zugreifen

Benutzer in Ihrer Belegschaft, z. B. Mitarbeiter und Auftragnehmer in Ihrer Organisation, benötigen möglicherweise Zugriff auf AWS über die AWS Management Console oder 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 Ihrem AWS Unternehmen.

- 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. Die Flexibilität von IAM ermöglicht es Ihnen, einen separaten SAML 2.0- oder Open ID Connect (OIDC)- Identitätsanbieter für jedes AWS-Konto zu aktivieren und Verbundbenutzerattribute für die Zugriffskontrolle zu 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 Management Console gesendet wird. Dies ermöglicht den Benutzern das Single Sign-On (SSO) bei der AWS Management Console, indem sie eine IAM-Rolle annehmen. Ihre Benutzer können außerdem temporäre AWS-API-Anmeldeinformationen für die Verwendung in der AWS CLI oder AWS SDKs von AWS STS erhalten, indem sie die IAM-Rolle mit einer SAML-Zusicherung des Identitätsanbieters annehmen.
- Für den Verbund der Benutzer in Ihrer Belegschaft mit mehreren Konten in Ihrer AWS-Organisation können Sie AWS IAM Identity Center verwenden und damit den Zugriff für Ihre Belegschaftsbenutzer 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 eine Verbindung mit Ihrem externen Identitätsanbieter über SAML 2.0 herstellen und automatisch Benutzer und Gruppen mit SCIM bereitstellen oder eine Verbindung zu Ihrem Microsoft AD-Verzeichnis mit AWS Directory Serviceherstellen. Sobald eine Identitätsquelle konfiguriert wurde, können Sie Benutzern und Gruppen Zugriff auf AWS-Konten zuweisen, indem Sie Richtlinien nach dem Prinzip der geringsten Berechtigungen in Ihrem Berechtigungssatzdefinieren. Die Benutzer in Ihrer Belegschaft können sich über Ihren zentralen Identitätsanbieter authentifizieren, um sich beim AWS-Zugangsportal anzumelden. Außerdem können sie sich so per Single-Sign-On bei den AWS-Konten und Cloud-Anwendungen anmelden, die ihnen zugewiesen sind. 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 außerdem den Single-Sign-On-Zugriff auf AWS-Anwendungen wie Amazon SageMaker Studio und AWS IoT Sitewise Monitor-Portale.

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 users und -Gruppen mehr verwenden. Stattdessen werden Ihre Benutzer und Gruppen außerhalb von AWS verwaltet und Benutzer können auf AWS-Ressourcen als Identitätsverbundzugreifen. Bei einem Identitätsverbund werden die Gruppen verwendet, die von Ihrem zentralen Identitätsanbieter definiert wurden. Sie sollten IAM-Gruppen, IAM users und langlebige Benutzeranmeldeinformationen (Passwörter und Zugriffsschlüssel) identifizieren und entfernen, die in Ihren AWS-Konten nicht mehr benötigt werden. Sie können ungenutzte Anmeldeinformationen mit IAM-Berichten zu Anmeldeinformationen suchen, die entsprechenden IAM users löschen und IAM-Gruppen entfernen. Sie können eine Service-Kontrollrichtlinie (SCP) auf Ihre Organisation anwenden, mit der das Erstellen neuer IAM users und -Gruppen verhindert und erzwungen wird, dass der Zugriff auf AWS über Verbundidentitäten erfolgt.

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 mobilen 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 Sicherheitsfunktionen 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 users 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 für Well-Architected:

- 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:

- AWS-Identitätsverbund
- Bewährte Sicherheitsmethoden in IAM
- Bewährte Methoden für AWS Identity and Access Management
- Getting started with IAM Identity Center delegated administration (Erste Schritte mit der delegierten IAM Identity Center-Verwaltung)
- How to use customer managed policies in IAM Identity Center for advanced use cases (Verwenden von vom Kunden verwalteten Richtlinien in IAM Identity Center für fortgeschrittene Anwendungsfälle)
- AWS CLI v2: IAM Identity Center-Anbieter für Anmeldeinformationen

Zugehörige Videos:

- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive (AWS re:inforce 2022 – AWS Identity and Access Management (IAM) zur Vertiefung)
- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center (AWS re:Invent 2022 – Vereinfachen des vorhandenen Mitarbeiterzugriffs mit IAM Identity Center)
- AWS re:Invent 2018: Mastering identity at every layer of the cake (AWS re:Invent 2018: Beherrschen der Identität auf jeder Ebene)

Zugehörige Beispiele:

- Workshop: Using AWS IAM Identity Center to achieve strong identity management (Verwenden von IAM Identity Center für eine robuste Identitätsverwaltung)
- Workshop: Serverless identity (Serverless-Identität)

Zugehörige Tools:

- AWS Security Competency Partners: Identity and Access Management
- 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: Implementierung der Rotation von Anmeldeinformationen zur Reduzierung der mit der Nutzung langfristiger Anmeldeinformationen verbundenen Risiken. 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: mittel

Implementierungsleitfaden

Wenn Sie sich nicht auf temporäre Anmeldeinformationen verlassen können und langfristige Anmeldeinformationen benötigen, prüfen Sie die definierten Anmeldeinformationen, um sicherzustellen, dass die definierten Kontrollen (z. B. 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 zentralisierten Identitäten übergehen, können Sie einen Anmeldeinformationenbericht für die Prüfung Ihrer Benutzer generieren.

Wir empfehlen außerdem, dass Sie MFA in Ihrem Identitätsanbieter erzwingen. Sie können AWS-Config-Regeln einrichten oder Sicherheitsstandards von AWS Security Hub verwenden, um festzustellen, ob Benutzer MFA aktiviert 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

- Prüfen Sie die Anmeldeinformationen regelmäßig: Durch die Prüfung der Identitäten, die in Ihrem Identitätsanbieter und IAM konfiguriert sind, können Sie sicherstellen, 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 Dienste, 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 mit Amazon CloudWatch Alarme für bestimmte API-Aufrufe innerhalb Ihrer AWS-Umgebung einrichten. Amazon GuardDuty kann Sie auch bei unerwarteten Aktivitäten benachrichtigen, die auf zu großzügige Zugriffsrechte hindeuten können, sowie auf nicht beabsichtigte Zugriffe auf IAM-Anmeldeinformationen.

- Regelmäßige Rotation von Anmeldeinformationen: Wenn Sie keine temporären Anmeldeinformationen verwenden können, rotieren Sie IAM-Zugriffsschlüssel regelmäßig (maximal alle 90 Tage). Wenn ein Zugriffsschlüssel ohne Ihr Wissen kompromittiert wurde, wird dadurch begrenzt, für wie lange die Anmeldeinformationen zum Zugriff auf Ihre Ressourcen genutzt werden können. Weitere Informationen zum Rotieren von Zugriffsschlüsseln für IAM-Benutzer finden Sie unter Rotieren der Zugriffsschlüssel.
- Prüfen Sie die IAM-Berechtigungen: Um die Sicherheit Ihres AWS-Konto zu erhöhen, sollten Sie alle Ihre IAM-Richtlinien regelmäßig überprüfen und überwachen. Stellen Sie sicher, dass die Richtlinien dem Prinzip der geringsten Berechtigung entsprechen.
- Erwägen Sie die Automatisierung der Erstellung und Aktualisierung von IAM-Ressourcen: IAM Identity Center automatisiert viele IAM-Aufgaben wie etwa das Rollen- und Richtlinienmanagement. 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.
- Verwenden Sie IAM Roles Anywhere, um IAM-Benutzer durch Maschinenidentitäten zu ersetzen: IAM Roles Anywhere ermöglicht die Verwendung von Rollen in Bereichen, in denen dies herkömmlicherweise nicht möglich war, etwa 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 (Bewährte Methoden für IAM)
- Identitätsanbieter und Verbund

- Partnerlösungen im Bereich Sicherheit: Zugriff und Zugriffssteuerung
- Temporäre Sicherheits-Anmeldeinformationen
- Getting credential reports for your AWS-Konto (Abrufen von Berichten zu Anmeldeinformationen für Ihr AWS-Konto)

Zugehörige Videos:

- Best Practices for Managing, Retrieving, and Rotating Secrets at Scale (Bewährte Methoden zum Verwalten, Abrufen und Rotieren von Secrets in großem Umfang)
- Managing user permissions at scale with AWS IAM Identity Center (Verwalten von Benutzerberechtigungen in großem Umfang mit AWS IAM Identity Center)
- Mastering identity at every layer of the cake (Beherrschen der Identität auf jeder Ebene)

Zugehörige Beispiele:

- Well-Architected Lab - Automated IAM User Cleanup (Well-Architected Lab – Automatisierte IAM-Benutzerbereinigung)
- Well-Architected Lab - Automated Deployment of IAM Groups and Roles (Well-Architected Lab – Automatisierte Bereitstellung von IAM-Gruppen und -Rollen)

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 oder Standort, können eine zusätzliche Ebene des Berechtigungsumfangs bieten, wenn Personen eine ähnliche Funktion ausüben, aber für unterschiedliche Teilmengen von Ressourcen.

Gewünschtes Ergebnis: Sie können Änderungen der Berechtigungen auf der Grundlage der Funktion auf alle Benutzer anwenden, die diese 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.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

AWS-Berechtigungen werden in Dokumenten definiert, die Richtlinien genannt werden und einem Prinzipal zugeordnet sind, z. B. einem Benutzer, einer Gruppe, einer Rolle oder einer Ressource. 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. Eine `WebAppDeveloper`-Gruppe kann zum Beispiel eine Richtlinie für die Konfiguration eines Services wie Amazon CloudFront innerhalb eines Entwicklungskontos enthalten. Eine `AutomationDeveloper` -Gruppe kann einige CloudFront-Berechtigungen mit der `WebAppDeveloper`-Gruppe gemeinsam haben. Diese Berechtigungen können in einer separaten Richtlinie erfasst und mit beiden Gruppen verknüpft werden, anstatt dass Benutzer aus beiden Funktionen zu `CloudFront-Zugriffs`gruppe gehören.

Zusätzlich zu Gruppen können Sie auch Attribute verwenden, um den Zugriff weiter einzuschränken. Sie können z. B. ein `Projekt`-Attribut für Benutzer in Ihrer `WebAppDeveloper`-Gruppe haben, um den Zugriff auf projektspezifische Ressourcen einzuschränken. 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 feststellen, ob Sie Gruppen und Attribute innerhalb Ihres Identitätsanbieters, innerhalb von IAM Identity Center oder mit IAM user-Gruppen in einem bestimmten Konto definieren müssen.
2. Definieren Sie Gruppen.
   a. Legen Sie Ihre Gruppen je nach Funktion und Umfang des erforderlichen Zugriffs fest.
   b. Wenn Sie innerhalb von IAM Identity Center definieren, erstellen Sie Gruppen und ordnen 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 Sie Attribute.
   a. Wenn Sie einen externen Identitätsanbieter verwenden, bieten sowohl das SCIM- als auch das SAML 2.0-Protokoll standardmäßig bestimmte Attribute. Zusätzliche Attribute können über SAML-Assertions unter Verwendung des Attributnamens `https://aws.amazon.com/SAML/Attributes/PrincipalTag` definiert und übergeben werden.
   b. Wenn Sie innerhalb von IAM Identity Center definieren, aktivieren Sie das Feature der attributbasierten Zugriffskontrolle (Attribute-based Access Control, ABAC) und definieren Sie Attribute wie gewünscht.
4. Umfangsberechtigungen basierend auf Gruppen und Attributen.
   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 zum Beispiel eine Bedingung definieren, die den Zugriff auf eine Ressource nur dann erlaubt, wenn der Wert eines `PrincipalTag`-Bedingungsschlüssels mit dem Wert eines gleichnamigen `ResourceTag`-Schlüssels übereinstimmt.

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:

- Bewährte Methoden in IAM
- Identitäten verwalten in IAM Identity Center
- What Is ABAC for AWS?
- ABAC in IAM Identity Center

Zugehörige Videos:

- Managing user permissions at scale with AWS IAM Identity Center
- Mastering identity at every layer of the cake

Berechtigungsverwaltung

Verwalten Sie Berechtigungen zum Steuern des Zugriffs für menschliche Identitäten und Maschinenidentitäten, die Zugriff auf AWS und Ihre Workloads benötigen. Berechtigungen steuern, wer worauf und unter welchen Bedingungen zugreifen kann. Legen Sie Berechtigungen für bestimmte Personen- oder Maschinenidentitäten fest, um Zugriff auf bestimmte Service-Aktionen für bestimmte Ressourcen zu gewähren. Geben Sie außerdem Bedingungen an, die erfüllt sein müssen, damit der Zugriff gewährt wird. Sie können beispielsweise Entwicklern erlauben, neue Lambda-Funktionen zu erstellen, aber nur in einer bestimmten Region. Befolgen Sie bei der skalierbaren Verwaltung Ihrer AWS-Umgebungen die folgenden bewährten Methoden, um sicherzustellen, dass Identitäten nur den benötigten Zugriff haben und nicht mehr.

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, was die betreffende Identität tun darf (ihre Berechtigungen). Identitätsbasierte Richtlinien können weiter unterteilt werden.

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

- Von AWS verwaltete Richtlinien – Verwaltete Richtlinien, die von AWS erstellt und verwaltet werden.
- Vom Kunden verwaltete Richtlinien – 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.

Ressourcenbasierte Richtlinien werden einer 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.

Mit der attributbasierten Zugriffskontrolle (ABAC) können Sie Berechtigungen basierend auf Attributen erteilen. In AWS werden diese Tags genannt. Tags können an IAM-Prinzipale (Benutzer oder Rollen) und an AWS-Ressourcen angefügt werden. Mithilfe von IAM-Richtlinien können Administratoren eine wiederverwendbare Richtlinie erstellen, die Berechtigungen basierend auf den Attributen des IAM-Prinzipals anwendet. Als Administrator können Sie beispielsweise eine einzelne IAM-Richtlinie verwenden, die Entwicklern in Ihrer Organisation Zugriff auf AWS-Ressourcen gewährt, die mit den Projekt-Tags der Entwickler übereinstimmen. Wenn das Entwicklerteam Ressourcen zu Projekten

hinzufügt, werden Berechtigungen automatisch basierend auf Attributen angewendet. Daher ist nicht für jede neue Ressource eine Richtlinienaktualisierung erforderlich.

Organizations Service Control Policies (SCP) definieren die maximalen Berechtigungen für Kontomitglieder einer Organisation oder Organisationseinheit (OU). SCPs beschränken die Berechtigungen, die identitätsbasierte Richtlinien oder ressourcenbasierte Richtlinien Entitäten (Benutzern oder Rollen) innerhalb des Kontos gewähren, erteilen aber keine Berechtigungen.

Sitzungsrichtlinien übernehmen eine Rolle oder einen Verbundbenutzer. 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. Diese Richtlinien beschränken die Berechtigungen für eine erstellte Sitzung, gewähren aber 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

Administratoren, Endbenutzer oder andere Komponenten müssen auf jede Komponente oder Ressource Ihres Workloads zugreifen. Sie müssen eine klare Definition davon haben, wer oder was Zugriff auf die einzelnen Komponenten haben soll. Anschließend wählen Sie den entsprechenden Identitätstyp und die entsprechende Authentifizierungs- und Autorisierungsmethode aus.

Typische Anti-Muster:

- Hartkodierung oder Speicherung von geheimen Daten in Ihrer Anwendung

- Gewähren individueller Berechtigungen für alle Nutzer
- Verwendung langlebiger Anmeldeinformationen

Risikostufe, wenn diese bewährte Methode nicht genutzt wird: Hoch

Implementierungsleitfaden

Administratoren, Endbenutzer oder andere Komponenten müssen auf jede Komponente oder Ressource Ihres Workloads zugreifen. Sie müssen eine klare Definition davon haben, wer oder was Zugriff auf die einzelnen Komponenten haben soll. Anschließend wählen Sie den entsprechenden Identitätstyp und die entsprechende Authentifizierungs- und Autorisierungsmethode aus.

Regulärer Zugriff auf AWS-Konten in der Organisation sollte per 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 beispielsweise AWS Secrets Manager und AWS Systems Manager Parameter Storekönnen dabei helfen, Secrets in sicherer Weise von Anwendungen oder Workloads zu trennen, wenn es nicht möglich ist, IAM-Rollen zu verwenden. 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 Identity and Access Management Roles Anywhere verwenden, um temporäre Sicherheitsanmeldeinformationen in IAM für Workloads zu erhalten, die außerhalb von AWS ausgeführt werden. Ihre Workloads können dieselben IAM-Richtlinien und IAM-Rollen verwenden, die Sie für AWS-Anwendungen zum Zugriff auf AWS-Ressourcen nutzen.

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

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 von nicht benötigten 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:

- Become an IAM Policy Master in 60 Minutes or Less (Experte für IAM-Richtlinien in unter 60 Minuten)
- Separation of Duties, Least Privilege, Delegation, and CI/CD (Trennung von Pflichten, geringste Berechtigung, Delegierung und CI/CD)
- Streamlining identity and access management for innovation (Optimieren des Identitäts- und Zugriffsmanagements für Innovation)

SEC03-BP02 Gewähren des Zugriffs mit den geringsten Berechtigungen

Es hat sich bewährt, nur den Zugriff zu gewähren, den Identitäten 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: Die Benutzer sollten nur über die erforderlichen Berechtigungen für ihre Aufgabe verfügen. Die Benutzer sollten nur Zugriff auf Produktionsumgebungen erhalten, um eine bestimmte Aufgabe in einem begrenzten Zeitraum auszuführen. Nach Abschluss der Aufgabe sollte der Zugriff widerrufen werden. Nicht mehr benötigte Berechtigungen sollten widerrufen werden. Dies gilt auch, wenn ein Benutzer zu einem anderen Projekt wechselt oder eine andere Tätigkeit übernimmt. Administratorberechtigungen sollten nur einer kleinen Gruppe von vertrauenswürdigen Administratoren erteilt werden. Die Berechtigungen sollten regelmäßig geprüft werden, um eine schleichende Ausweitung der Berechtigungen zu vermeiden. Maschinen- oder Systemkonten sollten die geringsten Berechtigungen erhalten, die zur Ausführung ihrer Aufgaben benötigt werden.

Typische Anti-Muster:

- Standardmäßige Gewährung von Administratorberechtigungen für Benutzer
- Verwendung des Root-Benutzers für alltägliche Aktivitäten
- Erstellung übermäßig großzügiger Richtlinien, jedoch ohne vollständige Administratorberechtigungen
- Keine Überprüfung der Berechtigungen, um festzustellen, ob sie einen Zugriff mit den geringsten Berechtigungen gewähren

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Das Prinzip der geringsten Berechtigung besagt, dass nur die Berechtigungen für die kleinste Gruppe von Aktionen erteilt werden sollte, die für die Durchführung einer bestimmten Aufgabe notwendig 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 verfügt standardmäßig über vollen Zugriff und sollte strikt 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. Mit dem Bedingungsschlüssel `PrincipalOrgID` können Sie beispielsweise Aktionen verweigern, wenn der Anforderer nicht Ihrer AWS-Organisation angehört.

Sie können auch Anforderungen kontrollieren, die AWS-Services in Ihrem Namen stellen, wie das Erstellen einer AWS Lambda-Funktion durch AWS CloudFormation. Hierfür verwenden Sie den Bedingungsschlüssel `CalledVia`. Sie sollten unterschiedliche Richtlinientypen in Ebenen organisieren, um einen umfassenden Verteidigungsansatz 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. So können Sie beispielsweise Ihren Anwendungsteams gestatten, eigene IAM-Richtlinien für die von ihnen erstellten Systeme zu erstellen, müssen aber auch eine Berechtigungsgrenze anwenden, um die maximalen Berechtigungen zu begrenzen, die das System erhalten kann.

Implementierungsschritte

- Implementieren Sie Richtlinien für geringste Berechtigungen: Weisen Sie IAM-Gruppen und -Rollen Zugriffsrichtlinien zu, die in ihrem Umfang möglichst gering und an die von Ihnen definierte Rolle oder Funktion der Benutzer angepasst sind.
  - Basisrichtlinien zur API-Nutzung: Eine Möglichkeit, herauszufinden, welche Berechtigungen benötigt werden, besteht in der Prüfung der AWS CloudTrail-Protokolle. 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 eine IAM-Richtlinie auf der Grundlage einer Aktivität generieren. Sie können IAM Access Advisor auf Organisations- oder Kontoebene verwenden, um zu verfolgen, auf welche Informationen für eine bestimmte Richtlinie zuletzt zugegriffen wurde.
- Erwägen Sie, von AWS verwaltete Richtlinien für berufliche Funktionen zu verwenden. Beim Erstellen von differenzierten Berechtigungsrichtlinien haben Sie zunächst möglicherweise Schwierigkeiten, herauszufinden, wo Sie beginnen sollten. AWS verfügt über verwaltete Richtlinien für allgemeine Job-Rollen, wie z. B. Fakturierungsmitarbeiter, Datenbankadministratoren und Datenwissenschaftler. Diese Richtlinien können helfen, den Zugriff der Benutzer einzuschränken

und gleichzeitig festzulegen, wie die Richtlinien für die geringste Berechtigung implementiert werden sollen.

- Entfernen von unnötigen Berechtigungen: Entfernen Sie nicht benötigte Berechtigungen und schränken Sie zu großzügige Richtlinien ein. Die Richtliniengenerierung von IAM Access Analyzer kann bei der Feinabstimmung von Berechtigungsrichtlinien hilfreich sein.
- Stellen Sie sicher, dass Benutzer nur beschränkten Zugriff auf Produktionsumgebungen haben: Benutzer sollten nur Zugriff auf Produktionsumgebungen haben, wenn ein gültiger Anwendungsfall vorliegt. 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.
- Ziehen Sie Berechtigungsgrenzen in Betracht: Eine Berechtigungsgrenze ist eine Funktion für eine verwaltete Richtlinie. Sie legt die maximalen Berechtigungen fest, die mit einer identitätsbasierten Richtlinie einer IAM-Entität erteilt werden können. Eine Berechtigungsgrenze erlaubt einer Entität nur die Ausführung jener Aktionen, die sowohl nach ihren identitätsbasierten Richtlinien als auch nach ihren Berechtigungsgrenzen zulässig sind.
- Ziehen Sie Ressourcen-Tags für Berechtigungen in Betracht: Ein attributbasiertes Zugriffskontrollmodell, das Ressourcen-Tags verwendet, bietet Ihnen die Möglichkeit, den Zugriff basierend auf dem Zweck der Ressource, dem Besitzer, der Umgebung oder anderen Kriterien zu gewähren. Mithilfe von Ressourcen-Tags können Sie beispielsweise zwischen Entwicklungs- und Produktionsumgebungen unterscheiden. Mit diesen Tags können Sie den Zugriff der Entwickler auf die Entwicklungsumgebung beschränken. Durch die Kombination von Tagging und Berechtigungsrichtlinien können Sie einen differenzierten Ressourcenzugriff erzielen, ohne komplizierte, benutzerdefinierte Richtlinien für jeden Tätigkeitsbereich definieren zu müssen.
- Verwenden Sie Service-Kontrollrichtlinien für AWS Organizations. 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.
- Erstellen Sie eine Benutzerlebenszyklus-Richtlinie für Ihre Organisation: Benutzerlebenszyklus-Richtlinien definieren Aufgaben, die ausgeführt werden müssen, wenn Benutzer neu in AWS eingebunden werden, ihre Rolle oder ihren Aufgabenbereich ändern oder keinen Zugriff mehr auf AWS benötigen. Bei jedem Schritt im Lebenszyklus eines Benutzers sollten

Berechtigungsprüfungen erfolgen, um sicherzustellen, dass die Berechtigungen angemessen restriktiv sind und keine schleichenden Berechtigungserweiterungen stattfinden.

- Legen Sie einen regelmäßigen Zeitplan für die Prüfung von Berechtigungen und das Entfernen nicht benötigter Berechtigungen fest: Sie sollten den Benutzerzugriff regelmäßig prüfen, um sicherzustellen, dass die Benutzer nicht zu viele Zugriffsrechte haben. AWS Config und IAM Access Analyzer können bei der Prüfung der Benutzerberechtigungen hilfreich sein.
- Erstellen Sie eine Job-Rollen-Matrix: In einer Job-Rollen-Matrix sind die verschiedenen Rollen und erforderlichen Zugriffsebenen innerhalb Ihrer AWS-Präsenz visuell dargestellt. 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 für geringste Berechtigungen
- IAM Access Analyzer erleichtert die Implementierung geringster Berechtigungen durch die Generierung von IAM-Richtlinien auf der Grundlage der Zugriffsaktivitäten
- Delegieren Sie die Berechtigungsverwaltung an Entwickler und verwenden Sie hierfür IAM-Berechtigungsgrenzen
- Verfeinern der Berechtigungen mithilfe der zuletzt genutzten Informationen
- 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
- Tagging zum Organisieren Ihrer Umgebung und Stärkung der Rechenschaftspflicht

- AWS-Markierungsstrategien
- Markieren von AWS-Ressourcen

Zugehörige Videos:

- Next-generation permissions management (Berechtigungsmanagement der nächsten Generation)
- Zero Trust: An AWS perspective (Zero Trust: Eine AWS-Perspektive)
- How can I use permissions boundaries to limit users and roles to prevent privilege escalation? (Wie kann ich mit Berechtigungsgrenzen Benutzer und Rollen einschränken, um die Eskalation von Berechtigungen zu vermeiden?)

Zugehörige Beispiele:

- Lab: IAM-Berechtigungsgrenzen – Übertragung der Rollenerstellung
- Lab: IAM-Tag-basierte Zugriffskontrolle für EC2

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 mit der Cloud (SEC02-BP04), 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. Die Fragen und bewährten Methoden in der Säule „Zuverlässigkeit“ können Sie dabei unterstützen, Ausfallmodi zu identifizieren und widerstandsfähigere Systeme zu entwickeln, um die Wahrscheinlichkeit von Ausfällen zu minimieren.

- 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 bei fehlender Befolgung dieser Best Practice:: 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 (IAM users und -Rollen) und die kontoübergreifenden IAM-Rollen in allen Workload-Konten. So wird sichergestellt, dass diese Ressourcen bereit und verfügbar sind, wenn ein Notfallereignis eintritt. Durch das Erstellen von Ressourcen im Voraus sind Sie nicht abhängig von den APIs der AWS- Steuerebene (zum Erstellen und Ändern von AWS-Ressourcen), die im Notfall möglicherweise nicht verfügbar sind. Wenn Sie IAM-Ressourcen vorab erstellen, müssen Sie außerdem keine möglichen Verzögerungen aufgrund einer letztendlichen Konsistenz 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. Das Genehmigungsverfahren 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.
- Stellen Sie sicher, dass der Prozess detaillierte Auditprotokolle und Ereignisse sowohl für erfolgreiche als auch für fehlgeschlagene Versuche generiert, Notfallzugriff zu erhalten. Überwachen Sie sowohl den Anforderungsprozess als auch den Notfallzugriffsmechanismus, um Missbrauch oder nicht autorisierte Zugriffe zu erkennen. Korrelieren Sie Aktivitäten mit laufenden Notfallereignissen aus Ihrem Vorfallsmanagement-System und senden Sie Benachrichtigungen, wenn Aktionen außerhalb der erwarteten Zeiträume erfolgen. Sie sollten beispielsweise die Aktivitäten im AWS-Konto für den Notfallzugriff überwachen und entsprechende Benachrichtigungen senden, da es im normalen Betrieb nie verwendet werden sollte.
- 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 der Simulation von Vorfallsreaktionen (SEC10-BP07) und Tests der Notfallwiederherstellung (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 Kundenverkehrs 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 users) 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.

Das Notfallzugriffsverfahren kann einen der folgenden Ansätze verwenden:

- Sie können vorab IAM users für Ihre Notfalladministratoren im Notfallzugriffskonto erstellen, denen sichere Passwörtern und MFA-Token zugeordnet sind. Diese IAM users verfügen über Berechtigungen, um 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 user einem Notfalladministrator zugewiesen ist und Sie anhand der CloudTrail-Ereignisse feststellen können, welcher Benutzer sich angemeldet hat. Der Nachteil

ist, dass Sie mehrere IAM users mit den zugehörigen langlebigen Passwörtern und MFA-Token verwalten müssen.

- Sie können den Root-Benutzer für das Notfallzugriff-AWS-Konto 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 Rechte 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 Management Console 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 Management Console.

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 users und optional IAM-Identitätsanbieter. Erstellen Sie außerdem vorab kontoübergreifende IAM-Rollen in den AWS-Konten für den Workload mit Vertrauensbeziehungen zu den entsprechenden IAM-Rollen im Notfallzugriffskonto. Nutzen Sie Instrumentierungsservices wie AWS CloudFormation StackSets mit AWS Organizations, um solche Ressourcen in den Mitgliedskonten Ihrer Organisation zu erstellen.

- Erstellen Sie in AWS Organizations Service-Kontrollrichtlinien (Service Control Policies, SCPs), 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:
  - Unter Verwendung der IAM users: Erstellen Sie vorab die IAM users mit sicheren Passwörtern und den zugehörigen MFA-Geräten.
  - Unter Verwendung des Root-Benutzers des Notfallkontos: 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 Management Console 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:

- Set up emergency access to the AWS Management Console (Einrichten des Notfallzugriffs auf die AWS-Managementkonsole)
- Enabling SAML 2.0 federated users to access the AWS Management Console (Aktivieren des Zugriffs von SAML 2.0-Verbundbenutzern auf die AWS-Managementkonsole)
- Break glass access („Break Glass“-Zugriff)

Zugehörige Videos:

- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center (AWS re:Invent 2022 – Vereinfachen des vorhandenen Mitarbeiterzugriffs mit IAM Identity Center)
- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive (AWS re:inforce 2022 – AWS Identity and Access Management (IAM) zur Vertiefung)

Zugehörige Beispiele:

- AWS Break Glass Role (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: Berechtigungsrichtlinien sollten dem Prinzip der geringsten Berechtigung folgen. 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 offen gelegt werden oder wenn anderweitig ohne Genehmigung darauf zugegriffen wird.

Typische Anti-Muster:

- standardmäßige Gewährung von Administratorberechtigungen für Benutzer
- Erstellung übermäßig lockerer 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 sServices 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 Zugriffssteuerung (Attribute-based Access Control, ABAC) kann die Verwaltung von Berechtigungen vereinfachen, da Sie Benutzern Berechtigungen auf der Grundlage ihrer Attribute erteilen können, anstatt jedem Benutzer direkt Berechtigungsrichtlinien zuzuweisen.

Implementierungsschritte

- Verwendung von AWS Identity and Access Management Access Analyzer: IAM Access Analyzer hilft bei der Identifizierung von Ressourcen in Ihrer Organisation und in Konten, wie etwa Amazon Simple Storage Service (Amazon S3)-Buckets oder IAM-Rollen, diegemeinsam mit einer externen Entität genutzt werden.

- Verwendung der Richtliniengenerierung von IAM Access Analyzer: Die Richtliniengenerierung von IAM Access Analyzer hilft bei der Erstellung detaillierter Berechtigungsrichtlinien auf der Grundlage eines IAM-Benutzers oder der Zugriffsaktivität einer IAM-Rolle.
- Festlegen eines akzeptablen Zeitrahmens und einer Nutzungsrichtlinie für IAM-Benutzer und -Rollen: Verwenden Sie den Zeitstempel des letzten Zugriffs, um nicht verwendete Benutzer und Rollen zu identifizieren und diese zu entfernen. Prüfen Sie die Informationen zum letzten Zugriff auf Services und Aktionen, um Berechtigungen für bestimmte Benutzer und Rollen zu identifizieren und entsprechend zuzuteilen. 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. Funktionen für die zuletzt abgerufenen Informationen sind in der AWS Management Console und programmgesteuert verfügbar, damit Sie sie in Ihre Infrastruktur-Workflows und automatisierten Tools integrieren können.
- Erwägen Sie die Protokollierung von Datenereignissen in AWS CloudTrail: 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 Aktivierung 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 von geringsten Berechtigungen
- Entfernen von nicht benötigten Anmeldeinformationen
- Was ist AWS CloudTrail?
- Arbeiten mit Richtlinien
- Protokollierung und Überwachung von DynamoDB
- Enabling CloudTrail event logging for Amazon S3 buckets and objects (Aktivieren von CloudTrail-Ereignisprotokollierung für Amazon-S3-Buckets und -Objekte)
- Getting credential reports for your AWS-Konto (Abrufen von Berichten zu Anmeldeinformationen für Ihr AWS-Konto)

Zugehörige Videos:

- Become an IAM Policy Master in 60 Minutes or Less (Experte für IAM-Richtlinien in unter 60 Minuten werden)
- Separation of Duties, Least Privilege, Delegation, and CI/CD (Trennung von Pflichten, geringste Berechtigung, Delegierung und CI/CD)
- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive (AWS re:inforce 2022 – AWS Identity and Access Management (IAM) zur 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 Berechtigungsrichtlinien umfasst Ihren Integritätsschutz, um die effektiven Berechtigungen eines Prinzipals bei Autorisierungsentscheidungen 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: Sie haben eine klare Isolierung der Umgebungen durch separate AWS-Konten. Service-Kontrollrichtlinien (SCPs) 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:

- Erstellen eines AWS-Konten als Mitglied innerhalb einer AWS-Organisation, aber keine Verwendung von SCPs, um die Verwendung und die verfügbaren Berechtigungen für ihre Anmeldeinformationen einzuschränken
- Zuweisung von Berechtigungen auf der Grundlage der geringsten Berechtigung, aber kein Integritätsschutz für die maximale Anzahl von Berechtigungen, die gewährt werden können

- Vertrauen auf die implizite Verweigerungsgrundlage von AWS IAM, um Berechtigungen einzuschränken, in der Annahme, dass die Richtlinien keine unerwünschte explizite Erlaubnis erteilen werden
- mehrere Workload-Umgebungen im selben AWS-Konto ausführen und sich dann auf Mechanismen wie VPCs, Tags oder Ressourcenrichtlinien verlassen, um Berechtigungsgrenzen durchzusetzen

Vorteile der Einführung dieser bewährten Methode: Einrichtungen zum Integritätsschutz helfen dabei, Vertrauen zu schaffen, dass unerwünschte Berechtigungen nicht gewährt 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 Erlaubnis nicht auf die Ressourcen eines anderen Kontos zugreifen, selbst wenn sich beide Konten in derselben AWS-Organisation oder unter 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 (SCPs) verwenden, die Sie entweder auf eine OE oder ein Konto anwenden können. SCPs können allgemeine Zugriffskontrollen durchsetzen, wie z. B. 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.

Ein weiterer Schritt ist die Verwendung von IAM-Ressourcenrichtlinien, um die verfügbaren Aktionen, die Sie für die von ihnen geregelten Ressourcen durchführen können, zusammen mit den Bedingungen, die der handelnde Prinzipal erfüllen muss, zu definieren. Dies kann so weit gefasst sein, dass alle Aktionen erlaubt sind, solange das Prinzipal zu Ihrer Organisation gehört (unter Verwendung des Bedingungsschlüssels PrincipalOrgId), oder so granular, dass nur bestimmte Aktionen von einer bestimmten IAM-Rolle erlaubt sind. 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 seinen Workload erforderlichen Berechtigungen verwalten. Dazu muss es möglicherweise neue IAM-Rollen und Berechtigungsrichtlinien erstellen. Sie können den maximalen Umfang der Berechtigungen, die das Team gewähren darf, in einer IAM-Berechtigungsgrenze erfassen und dieses Dokument mit einer IAM-Rolle verknüpfen, die das Team dann zur Verwaltung seiner IAM-Rollen und Berechtigungen verwenden kann. Dieser Ansatz kann ihm die Freiheit geben, ihre Arbeit zu erledigen und gleichzeitig die Risiken eines administrativen IAM-Zugriffs verringern.

Ein detaillierterer Schritt ist die Implementierung von Techniken zur Verwaltung von privilegiertem Zugriff (Privileged Access Management, PAM) und temporärer erweiterter Zugriffsverwaltung (Temporary Elevated Access Management, TEAM). Ein Beispiel für PAM ist die Anforderung an Prinzipale, sich mehrfach zu authentifizieren, bevor sie privilegierte Aktionen durchführen. Weitere Informationen finden Sie unter Configuring MFA-protected API access. 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 Berechtigungen, die einem Prinzipal von einer IAM-Rolle gewährt werden, mit einer Sitzungsrichtlinie einzuschränken und diese Einschränkung dann während des genehmigten Zeitfensters vorübergehend aufzuheben. Weitere Informationen über Lösungen, die AWS und ausgewählte Partner validiert haben, finden Sie unter Temporär 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. Wir empfehlen Ihnen, Ihre SCPs nach dem Prinzip der Erlaubnisliste zu schreiben, die alle Aktionen verweigert, außer denen, die Sie erlauben, und den Bedingungen, unter denen sie erlaubt sind. Beginnen Sie damit, die Ressourcen zu definieren, die Sie kontrollieren möchten, und setzen Sie den Effekt auf Verweigern. Verwenden Sie das NotAction-Element, um alle Aktionen zu verweigern, außer denen, die Sie angeben. Kombinieren Sie dies mit einer NotLike-Bedingung, um festzulegen, wann diese Aktionen erlaubt sind, falls zutreffend, wie z. B. StringNotLike und ArnNotLike.
   b. Siehe Service control policy examples.
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 Workloads IAM-Rollen und -Berechtigungen verwenden können.
5. Evaluieren Sie PAM- und TEAM-Lösungen auf der Grundlage Ihrer Bedürfnisse.

Ressourcen

Zugehörige Dokumente:

- Data perimeters on AWS
- Establish permissions guardrails using data perimeters
- Policy evaluation logic

Zugehörige Beispiele:

- Service control policy examples

Zugehörige Tools:

- AWS Solution: Temporary Elevated Access Management
- Validated security partner solutions for 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 von Prinzipalen innerhalb der Organisation an und verringern so das Risiko unnötiger Privilegien. 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 gewähren Identitäten im Voraus übermäßige oder weitreichende Zugriffsrechte, die über das ursprünglich erforderliche Maß hinausgehen.
- Sie unterlassen die Überprüfung der Zugriffsprivilegien und passen sie an, wenn sich die Rollen und Verantwortlichkeiten der Identitäten im Laufe der Zeit ändern.
- Sie verlassen inaktive oder beendete Identitäten mit aktiven Zugriffsrechten. Dies erhöht das Risiko eines unbefugten Zugriffs.
- Sie automatisieren die Verwaltung von Identitätslebenszyklen nicht.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: 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 das Risiko übermäßiger oder unnötiger Zugriffsberechtigungen zu verringern.

Sie können den Lebenszyklus von IAM users direkt innerhalb des AWS-Konto oder durch den Verbund von Ihrem Identitätsanbieter für die Belegschaft zu AWS-IAM Identity Center verwalten. Für IAM users 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 deren Lebenszyklus zu verwalten, indem Sie Benutzer- und Gruppeninformationen vom Identitätsanbieter Ihrer Organisation mit dem Protokoll System für domänenübergreifendes Identitätsmanagement (System for Cross-Domain Identity Management, SCIM) synchronisieren.

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. Integrieren Sie einen Anbieter von Verbundidentitäten (wie Microsoft Active Directory, Okta, Ping Identity) als maßgebliche Quelle für Benutzer- und Gruppeninformationen mit IAM Identity Center.
4. Verwenden Sie das SCIM-Protokoll, um Benutzer- und Gruppeninformationen vom 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:

- Manage your identity source
- Manage identities in IAM Identity Center
- Using AWS Identity and Access Management Access Analyzer
- IAM Access Analyzer policy generation

Zugehörige Videos:

- AWS re:Inforce 2023 – Manage temporary elevated access with AWS IAM Identity Center
- AWS re:Invent 2022 – Simplify your existing workforce access with IAM Identity Center
- AWS re:Invent 2022 – Harness power of IAM policies & rein in permissions w/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: Wissen, welche Ihrer AWS-Ressourcen für wen 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 mithilfe von Richtlinien gewähren, die an Ressourcen angefügt sind – (z. B. Amazon Simple Storage Service (Amazon S3)-Bucket-Richtlinien – oder indem Sie einem Prinzipal erlauben, eine IAM-Rolle in einem anderen Konto anzunehmen. Prüfen Sie bei der Verwendung von Ressourcenrichtlinien, dass der Zugriff nur autorisierten Prinzipalen gewährt ist. Definieren Sie einen Prozess für die Genehmigung aller Ressourcen, die öffentlich verfügbar sein müssen.

AWS Identity and Access Management Access Analyzer verwendet belegbare 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. Erwägen Sie die Konfiguration von IAM Access Analyzer mit AWS Organizations, um die Transparenz aller Ihrer Konten sicherzustellen. IAM Access Analyzer ermöglicht Ihnen auch die Voranzeige der Ergebnisse vor der Bereitstellung von Ressourcenberechtigungen. So können Sie sicherstellen, dass mit den Richtlinienänderungen nur der beabsichtigte öffentliche und kontoübergreifende Zugriff auf Ihre Ressourcen gewährt wird. Beim Entwurf des Mehrkonten-Zugriffs können Sie mit Vertrauensrichtlinien steuern, in welchen Fällen eine Rolle angenommen werden kann. So können Sie etwa den Bedingungsschlüssel `PrincipalOrgId` verwenden, um den Versuch, eine Rolle von außerhalb Ihrer AWS Organizations anzunehmen, abzulehnen.

AWS Config kann Ressourcen melden, die nicht korrekt konfiguriert sind, und über AWS Config-Richtlinienprüfungen Ressourcen erkennen, für die der öffentliche Zugriff konfiguriert ist. Services wie AWS Control Tower und AWS Security Hub vereinfachen die Bereitstellung von Prüfungen und Integritätsschutz über AWS Organizations hinweg, um öffentlich zugängliche Ressourcen zu identifizieren und zu korrigieren. Beispielsweise verfügt AWS Control Tower über verwalteten Integritätsschutz, der erkennen kann, ob Amazon EBS-Snapshots von AWS-Konten wiederhergestellt werden können.

Implementierungsschritte

- Erwägen Sie die Aktivierung von AWS Config für AWS Organizations: AWS Config ermöglicht die Aggregierung von Ergebnissen mehrerer Konten in einer AWS Organizations zu einem delegierten Administratorkonto. Dies sorgt für eine umfassende Sicht und ermöglicht die Bereitstellung von AWS-Config-Regeln über mehrere Konten hinweg, um öffentlich zugängliche Ressourcen zu erkennen.
- Konfiguration von AWS Identity and Access Management Access Analyzer: IAM Access Analyzer hilft Ihnen, die Ressourcen in Ihrer Organisation und Ihren Konten zu identifizieren, z. B. Amazon S3-Buckets oder IAM-Rollen, die mit einer externen Entität geteilt werden.
- Verwenden Sie die automatische Korrektur in AWS Config, um auf Änderungen in der Konfiguration des öffentlichen Zugriffs auf Amazon S3-Buckets reagieren zu können: Sie können die Einstellungen zur Blockierung des öffentlichen Zugriffs für Amazon S3-Buckets automatisch erneut aktivieren.
- Implementierung von Überwachung und Benachrichtigung, wenn Amazon S3-Buckets öffentlich zugänglich werden: Sie müssen über Überwachungs- und Benachrichtigungsmechanismen verfügen, um zu erkennen, wenn Amazon S3 Block Public Access deaktiviert ist, und wenn Amazon S3-Buckets öffentlich zugänglich werden. Dazu können Sie bei Verwendung von AWS Organizations eine Servicekontrollrichtlinie erstellen, die Änderungen an Amazon S3-Richtlinien für den öffentlichen Zugriff verhindern. AWS Trusted Advisor prüft auf Amazon S3-Buckets, die Open-Access-Berechtigungen haben. 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. Die Prüfung von Trusted Advisor untersucht explizite Bucket-Berechtigungen und zugeordnete Bucket-Richtlinien, die die Bucket-Berechtigungen möglicherweise überschreiben. Sie können auch mit AWS Config Ihre Amazon S3-Buckets für den öffentlichen Zugriff überwachen. Für weitere Informationen vgl. Verwendung von AWS Config zur Überwachung und Reaktion auf Amazon S3-Buckets mit öffentlicher Zugänglichkeit. Bei der Prüfung der Zugänglichkeit ist es wichtig, zu berücksichtigen, welche Art von Daten Amazon S3-Buckets enthalten. Amazon Macie hilft dabei, sensitive Daten wie etwa PII, PHI und Anmeldeinformationen wie private oder AWS-Schlüssel zu erkennen und zu schützen.

Ressourcen

Zugehörige Dokumente:

- Verwendung von AWS Identity and Access Management Access Analyzer

- AWS Control Tower Controls Library
- AWS Foundational Security Best Practices Standard
- AWS Config Managed Rules
- Prüfungsreferenz von AWS Trusted Advisor
- Monitoring AWS Trusted Advisor check results with Amazon EventBridge (Überwachen der Prüfergebnisse von AWS Trusted Advisor mit Amazon EventBridge)
- Managing AWS Config Rules Across All Accounts in Your Organization (Verwaltung von AWS Config-Regeln für alle Konten in Ihrer Organisation)
- AWS Config und AWS Organizations

Zugehörige Videos:

- Best Practices for securing your multi-account environment(Bewährte Methoden für den Schutz Ihrer Mehrkonten-Umgebung)
- Dive Deep into IAM Access Analyzer (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: Minimierung unbeabsichtigter Zugriffe durch Verwendung sicherer Verfahren für die Freigabe von Ressourcen innerhalb Ihrer Organisation und die Unterstützung Ihrer Initiative zur Verhinderung von Datenverlusten. 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. Anleitungen

zur Analyse extern freigegebener 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 öffentlicher und kontoübergreifender Zugriffe, um Richtlinien einzurichten, die externe Zugriffe auf die Ressourcen beschränken, für die dies erforderlich ist, und um einen Prozess zur kontinuierlichen Überwachung und Benachrichtigung einzurichten.

Die kontoübergreifende Freigabe innerhalb von AWS Organizations wird von einer Reihe von AWS-Services unterstützt, wie etwa AWS Security Hub, 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 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 verbreitete Ressourcen freigeben, wie etwa VPC-Subnetze und Transit Gateway-Anhänge, AWS Network Firewall oder Amazon SageMaker-Pipelines.

Um Ihr Konto darauf zu beschränken, Ressourcen nur innerhalb Ihrer Organisation freizugeben, verwenden Sie Service Control Policies (SCPs, Service-Kontrollrichtlinien), um den Zugriff auf externe Prinzipale zu verhindern. Kombinieren Sie bei der Freigabe von Ressourcen identitätsbasierte Kontrollen und Netzwerk-Kontrollen zur Erstellung eines Datenperimeters für

Ihre Organisation zum Schutz gegen unbeabsichtigte Zugriffe. 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. So können Sie Beispielsweise als Teil ihres Datenperimeters VPC-Endpunktrichtlinien und die Bedingung `AWS:0rincipal0rgID` verwenden, um sicherzustellen, dass die auf Ihre Amazon S3-Buckets zugreifenden Identitäten zu Ihrer Organisation gehören. Es ist wichtig zu wissen, dass SCPs nicht für serviceverknüpfte Rollen (LSR) oder AWS-Service-Prinzipale gelten.

Bei Verwendung von Amazon S3 sollten Sie ACLs für Ihren Amazon S3-Bucket deaktivieren und IAM-Richtlinien für die Einrichtung der Zugriffskontrollen verwenden. Für die Einschränkung des Zugriffs auf einen Amazon S3-Ursprung von Amazon CloudFront aus migrieren Sie von der Ursprungszugriffsidentität (OAI) zur Ursprungszugriffssteuerung (OAC), die zusätzliche Funktionen wie beispielsweise die serverseitige Verschlüsselung mit AWS Key Management Service unterstützt.

In manchen Fällen möchten Sie möglicherweise die Freigabe von Ressourcen außerhalb Ihrer Organisation zulassen oder einer Drittpartei den Zugriff auf Ihre Ressourcen gewähren. Präskriptive Anleitungen zur Verwaltung von Berechtigungen für die externe Freigabe von Ressourcen finden Sie unterBerechtigungsmanagement.

Implementierungsschritte

1. Nutzen Sie AWS Organizations.

   AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten zu einer zentral erstellten und 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. Integrieren Sie AWS Organizations mit AWS-Services.

   Wenn Sie einen AWS-Service zur Ausführung von Aufgaben in Ihrem Namen in den Mitgliedskonten Ihrer Organisation aktivieren, erstellt AWS Organizations eine serviceverknüpfte IAM-Rolle für den jeweiligen Service in jedem Mitgliedskonto. Sie sollten den vertrauenswürdigen Zugriff mit der AWS Management Console, den AWS-APIs oder der AWS CLI verwalten. Präskriptive Anleitungen zur Einrichtung vertrauenswürdigen Zugangs finden Sie unter

Verwendung von AWS Organizations mit anderen AWS-Services und unter AWS-Services, die Sie mit Organizations verwenden können.

3. Richten Sie einen Datenperimeter ein.

   Der AWS-Perimeter wird typischerweise als von AWS Organizations verwaltete Organisation repräsentiert. Zusammen mit On-Premises-Netzwerken und -Systemen ist der Zugriff auf AWS-Ressourcen das, was viele als den Perimeter von My AWS bezeichnen. Das Ziel des Perimeters 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.

   a. Definieren und implementieren Sie die Perimeter.

      Befolgen Sie die Schritte unter Perimeter-Implementierung im Whitepaper zum Thema „Aufbau eines Perimeters in AWS“ für jede Autorisierungsbedingung. Eine präskriptive Anleitung zum Schutz von Netzwerkebenen finden Sie unter Schutz von Netzwerken.

   b. Sorgen Sie für kontinuierliche Überwachung und Benachrichtigung.

      AWS Identity and Access Management Access Analyzer hilft bei der Identifizierung von Ressourcen in Ihrer Organisation und in Konten, die gemeinsam mit externen Entitäten genutzt werden. Sie können IAM Access Analyzer mit AWS Security Hub integrieren, um Ergebnisse für eine Ressource von IAM Access Analyzer zu Security Hub zu senden und zu aggregieren und so die Sicherheitssituation ihrer Umgebung zu analysieren. Aktivieren Sie für die Integration IAM Access Analyzer und Security Hub in jeder Region und in jedem Konto. Sie können auch mit AWS-Config-Regeln die Konfiguration prüfen und die jeweilige Partei mit AWS Chatbot mit AWS Security Hub benachrichtigen. Anschließend können Sie mit Automatisierungsdokumenten von AWS Systems Manager nicht-konforme Ressourcen reparieren.

   c. Präskriptive Anleitungen zur Überwachung und kontinuierlichen Beratung zu extern freigegebenen Ressourcen finden Sie unter Analyse des öffentlichen und kontoübergreifenden Zugriffs.

4. Verwenden Sie die Ressourcenfreigabe in AWS-Services, und sorgen Sie für entsprechende Einschränkungen.

   Viele AWS-Services erlauben die Freigabe von Ressourcen für ein anderes Konto oder die Ausrichtung auf eine Ressource in einem anderen Konto, wie etwa Amazon Machine Images (AMIs) und AWS Resource Access Manager (AWS RAM). Schränken Sie die `ModifyImageAttribute`-API auf die Angabe der vertrauenswürdigen Konten für die Freigabe des AMI ein. Geben Sie die Bedingung `ram:RequestedAllowsExternalPrincipals` bei Verwendung von AWS RAM an, um die Freigabe auf Ihre Organisation zu beschränken und

Zugriffe von nicht vertrauenswürdigen Entitäten zu verhindern. Präskriptive Anleitungen und Überlegungen dazu finden Sie unter Ressourcenfreigabe und externe Ziele.

5. Verwenden Sie AWS RAM für sichere Freigaben in einem Konto oder mit anderen AWS-Konten.

   AWS RAM hilft bei der sicheren Freigabe 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 Ressourcen bereits mit einer ressourcenbasierten Richtlinie freigegeben haben, können Sie mit der `PromoteResourceShareCreatedFromPolicy`-API oder einem Äquivalent die Ressourcenfreigabe zu einer vollständigen AWS RAM-Ressourcenfreigabe erhöhen.

   In manchen Fällen müssen Sie möglicherweise weitere Schritte unternehmen, um Ressourcen freizugeben. So müssen Sie etwa für die Freigabe eines verschlüsselten Snapshots 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 auf AWS
- Verwenden einer externen ID, um Dritten Zugriff auf Ihre AWS-Ressourcen zu gewähren
- AWS-Services, die Sie mit AWS Organizations verwenden können
- Einrichten eines Datenperimeters auf AWS: Zulassen ausschließlich vertrauenswürdiger Identitäten für den Zugriff auf Unternehmensdaten

Zugehörige Videos:

- Granular Access with AWS Resource Access Manager (Granulärer Zugriff mit AWS Resource Access Manager)
- Securing your data perimeter with VPC endpoints (Schutz Ihres Datenperimeters mit VPC-Endpunkten)
- Establishing a data perimeter onAWS(Einrichten eines Datenperimeters auf AWS)

Zugehörige Tools:

- Beispiele für eine Datenperimeterrichtlinie

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: Langfristige AWS Identity and Access Management (IAM)-Anmeldeinformationen, IAM-Zugriffsschlüssel und geheime Schlüssel, die einem Benutzer zugeordnet sind, können von allen verwendet werden, sofern sie gültig und aktiv sind. Die Verwendung einer IAM-Rolle und temporärer Anmeldeinformationen hilft bei der Verbesserung Ihrer allgemeinen Sicherheitsposition durch Reduzierung des Aufwands für die Verwaltung langfristiger Anmeldeinformationen und des operationalen Overheads dieser sensiblen Details. Durch die Verwendung einer universell eindeutigen Kennung (UUID) für die externe ID in der IAM-Vertrauensrichtlinie und die Anbindung der IAM-Richtlinien an die IAM-Rolle unter Ihrer Kontrolle können Sie prüfen und sicherstellen, dass der der Drittpartei gewährte Zugriff nicht zu umfangreich ist. Anleitungen zur 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 dazu eine Vertrauensrichtlinie mit 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 auch IAM Roles Anywhere 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. Achten Sie auf andere AWS-Services, die die Freigabe unterstützen. Beispielsweise erlaubt AWS Well-Architected Tool die Freigabe eines Workloads für andere AWS-Konten, und AWS Resource Access Manager hilft Ihnen bei der sicheren Freigabe einer AWS-Ressource, deren Eigentümer Sie sind, für andere Konten.

Implementierungsschritte

1. Verwenden Sie kontoübergreifende Rollen, um Zugriff auf externe Konten zu gewähren.

   Kontoübergreifende Rollen reduzieren den Umfang sensibler Informationen, die von externen Konten und Drittparteien für deren Kunden gespeichert werden. Kontoübergreifende Rollen ermöglichen die sichere Gewährung des Zugriffes auf AWS-Ressourcen in Ihrem Konto für Drittparteien wie etwa AWS Partners oder andere Konten in Ihrer Organisation, bei gleichzeitiger Wahrung der Möglichkeit, 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. IAM Roles Anywhere hilft Ihnen bei der

Aktivierung von Workloads Dritter zur sicheren Interaktion mit Ihren AWS-Workloads und zur weiteren Reduzierung der Erfordernis langfristiger Anmeldeinformationen.

Sie sollten keine langfristigen Anmeldeinformationen oder mit Benutzern verbundene Zugriffsschlüssel für die externe Gewährung des Zugriffs auf Konten verwenden. Verwenden Sie stattdessen kontoübergreifende Rollen, um kontoübergreifenden Zugriff zu gewähren.

2. Verwenden Sie eine externe ID mit Drittparteien.

   Die Verwendung einer externen ID ermöglicht Ihnen, in einer IAM-Vertrauensrichtlinie festzulegen, wer eine Rolle annehmen kann. Die Vertrauensrichtlinie kann verlangen, dass der Benutzer, der die Rolle annimmt, die Bedingung und das Ziel seiner Aktivität bestätigt. Sie bietet dem Kontoinhaber auch die Möglichkeit, die anzunehmende Rolle nur unter bestimmten Umständen zuzulassen. Die primäre Funktion der externen ID besteht darin, das Confused-Deputy-Problem anzugehen und zu verhindern.

   Verwenden Sie eine externe ID, wenn Sie AWS-Konto-Eigentümer sind und eine Rolle für eine Drittpartei konfiguriert haben, die neben Ihrem auf andere AWS-Konten zugreift, oder wenn Sie Rollen für verschiedene Kunden annehmen. Arbeiten Sie zusammen mit der Drittpartei oder AWS Partner an der Einrichtung einer externen ID-Bedingung für die IAM-Vertrauensrichtlinie.

3. Verwenden Sie universell eindeutige externe IDs.

   Implementieren Sie einen Prozess, der für externe IDs zufällige und eindeutige Werte generiert, etwa eine universell eindeutige Kennung (UUID). Eine Drittpartei, die externe IDs für verschiedene Kunden wiederverwendet, behebt das Confused-Deputy-Problem nicht, da Kunde A möglicherweise unter Verwendung des Rollen-ARN von Kunde B zusammen mit der duplizierten externen ID die Daten von Kunde B einsehen kann. In einer Multi-Tenant-Umgebung, in der eine Drittpartei mehrere Kunden mit verschiedenen AWS-Konten unterstützt, muss die Drittpartei eine andere eindeutige ID als die externe ID für jedes AWS-Konto verwenden. Die Drittpartei ist für das Erkennen doppelter externer IDs und die sichere Zuordnung jedes Kunden zur entsprechenden externen ID verantwortlich. Die Drittpartei muss durch Testen sicherstellen, dass sie die Rolle nur annehmen kann, wenn die externe ID angegeben wird. Die Drittpartei sollte den ARN der Kundenrolle und die externe ID nicht speichern, bis die externe ID benötigt wird.

   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.

Sie oder die Drittpartei können/kann die externe ID generieren. 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.

4. Nehmen Sie von Kunden bereitgestellte langfristige Anmeldeinformationen außer Betrieb.

   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 unterIdentitätsmanagement. Arbeiten Sie auch mit Ihrem AWS-Konto-Team und der Drittpartei daran, ein Runbook zur Risikodämpfung zu erstellen. Präskriptive Anleitungen zur Reaktion auf mögliche Auswirkungen von Sicherheitsvorfällen finden Sie unter Vorfallbehandlung.

5. Prüfen Sie, ob die Einrichtung über präskriptive Anleitungen verfügt oder automatisiert ist.

   Die für den kontoübergreifenden Zugriff in Ihren Konten erstellte Richtlinie muss dem Prinzip der geringsten Berechtigungen folgen. 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 für die Erstellung 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 mit der AWS CloudFormation-Vorlage oder einem Äquivalent Änderungen überwachen, mit besonderem Augenmerk auf „Drift Detection“.

6. 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.

Präskriptive Anleitungen zu Erkennungsverfahren finden Sie unter Bewährte Erkennungsmethoden.

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 Detection

Zugehörige Dokumente:

- Bucket-Besitzer gewährt kontoübergreifende Berechtigung für Objekte, die er nicht besitzt
- Verwendung von Vertrauensrichtlinien mit IAM-Rollen
- Delegieren des Zugriffs in allen AWS-Konten mithilfe von IAM-Rollen
- Wie greife ich mit IAM auf Ressourcen in einem anderen AWS-Konto zu?
- Bewährte Sicherheitsmethoden in IAM
- Logik für die kontenübergreifende Richtlinienauswertung
- Verwenden einer externen ID, um Dritten Zugriff auf Ihre AWS-Ressourcen zu gewähren
- Collecting Information from AWS CloudFormation Resources Created in External Accounts with Custom Resources (Erfassen von Informationen von in externen Konten mit benutzerdefinierten Ressourcen erstellten AWS-CloudFormation-Ressourcen)
- Securely Using External ID for Accessing AWS Accounts Owned by Others (Sichere Verwendung einer externen ID für den Zugriff auf AWS-Konten, die anderen gehören)
- Extend IAM roles to workloads outside of IAM with IAM Roles Anywhere (Erweitern von IAM-Rollen auf Workloads außerhalb von IAM mit IAM Roles Anywhere)

Zugehörige Videos:

- How do I allow users or roles in a separate AWS-Konto access to my AWS-Konto? (Wie gewähre ich Benutzern oder Rollen in einem separaten AWS-Konto Zugriff auf mein AWS-Konto?)
- AWS re:Invent 2018: Become an IAM Policy Master in 60 Minutes or Less (AWS re:Invent 2018: Werden Sie in höchstens 60 Minuten zum IAM-Richtlinienexperten)
- AWS Knowledge Center Live: IAM Best Practices and Design Decisions (AWS Knowledge Center Live: Bewährte IAM-Methoden und -Entwurfsentscheidungen)

Zugehörige Beispiele:

- Well-Architected Lab - Lambda cross account IAM role assumption (Level 300) (Well-Architected Lab – Lambda-kontoübergreifende IAM-Rollenannahme)
- Configure cross-account access to Amazon DynamoDB (Konfigurieren des kontoübergreifenden Zugriffs auf Amazon DynamoDB)
- 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. Die erste Teil kann an mehreren Stellen im Lebenszyklus einer Anwendung stattfinden. Durch die Verwendung von Infrastruktur als Code (z. B. eine CloudFormation-Vorlage) können Sie vor der Bereitstellung eines Workloads durch die Implementierung von Prüfungen in den CI/CD-Pipelines oder der Versionskontrolle auf unerwünschte Konfigurationen prüfen. Wenn Sie dann einen 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 Ihrem 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 Ihrem Workload können beispielsweise auf Exploits analysiert werden, die verwendet werden. Sie sollten regelmäßig die Erkennungsmechanismen im Zusammenhang mit Ihrem 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 Steuerelemente sind wichtige reaktive Faktoren, die es Ihrem Unternehmen 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. In den nächsten Abschnitten werden folgende Ansätze erläutert:

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.
- Nutzung ausschließlich manueller Prozesse für die Verwaltung und Verwendung von Protokollen
- Speichern aller Arten von Protokollen nur für den Fall, dass sie benötigt werden
- Prüfung der Protokollintegrität nur bei Bedarf

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 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 Management Console, 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-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-Ergebnisse, 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: Cloud Capability-Definitionen – 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-Protokolle sind, sollten Sie erwägen, weniger häufig benötigte Protokolle in Amazon S3 zu archivieren.
- Wählen Sie den Protokollspeicher: 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 jeden AWS-Service oder jede AWS-Anwendung in Ihrer Organisation nach den entsprechenden Anleitungen zur Protokollkonfiguration:
  - Konfigurieren eines AWS CloudTrail-Trails
  - Konfigurieren von VPC-Flow-Protokollen
  - Konfigurieren des Amazon GuardDuty-Ergebnisexports
  - Konfigurieren der AWS Config-Aufzeichnung
  - Konfigurieren des Web-ACL-Datenverkehrs von AWS WAF
  - Konfigurieren der Netzwerkdatenverkehrsprotokolle von AWS Network Firewall
  - Konfigurieren der Zugriffsprotokolle von Elastic Load Balancing
  - Konfigurieren von Resolver-Query-Protokollen 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 Ihr 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 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. Für Informationen zur Erstellung dieser Alarm- und Erkennungsmechanismen vgl. Erkennung in der AWS-Sicherheits- und Vorfallreaktionsanleitung.

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-Sicherheits- und Vorfallreaktionsanleitung
- Erste Schritte mit Amazon Security Lake

- Erste Schritte: Amazon CloudWatch Logs
- Security Partner Solutions: Logging and Monitoring (Partnerlösungen im Bereich Sicherheit: Protokollierung und Überwachung)

Zugehörige Videos:

- AWS re:Invent 2022 - Introducing Amazon Security Lake (AWS re:Invent 2022 – Vorstellung von Amazon Security Lake)

Zugehörige Beispiele:

- Assisted Log Enabler für AWS
- Historischer Export von Ergebnissen von AWS Security Hub

Zugehörige Tools:

- Snowflake for Cybersecurity

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 Einführung 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 meistern, sollten Sie alle relevanten Quellen von Sicherheitsprotokolldaten in einem Protokollarchiv-Konto zusammenfassen. Dies ist beschrieben in: Organizing Your AWS Environment Using Multiple Accounts. 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 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 Amazon 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 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 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, Amazon 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 geben.

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:

- Aggregating, searching, and visualizing log data from distributed sources with Amazon Athena and Amazon QuickSight
- How to visualize Amazon Security Lake findings with Amazon QuickSight
- Generate AI powered insights for Amazon Security Lake using Amazon SageMaker Studio and Amazon Bedrock
- Identify cybersecurity anomalies in your Amazon Security Lake data using Amazon SageMaker
- Ingest, transform, and deliver events published by Amazon Security Lake to Amazon OpenSearch Service
- How to use AWS Security Hub and Amazon OpenSearch Service for SIEM

Zugehörige Tools:

- Amazon Security Lake
- Amazon Security Lake-Partnerintegrationen
- Open Cybersecurity Schema Framework (OCSF)
- Amazon Athena
- Amazon QuickSight
- 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 Einführung 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, 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.

In ihrer grundlegendsten Form enthalten Warnmeldungen Informationen darüber, wer (Prinzipal oder Identität) was (Aktion, die ergriffen wird) im Hinblick auf (Ressourcen, die betroffen sind) macht. 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 eine 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 könnte GuardDuty diesen korrelierten Ereigniskontext als neue Sicherheitswarnung veröffentlichen und die Kritikalität auf hoch setzen, 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, EventBridge und CloudWatch in Betracht.

3. Identifizieren Sie Quellen für die Korrelation und Anreicherung von Daten. Beispiele für Quellen sind CloudTrail, VPC-Flow-Protokolle, Amazon Security Lake sowie Infrastruktur- und Anwendungsprotokolle.
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 Funktion AWS Lambda 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-Leitfaden für Security Incident Response

Zugehörige Beispiele:

- How to enrich AWS Security Hub findings with account metadata
- How to use AWS Security Hub and Amazon OpenSearch Service for SIEM

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 Einführung 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 Ihnen dabei helfen, die Konfiguration der Ressourcen in Ihren Konten auf die Einhaltung Ihrer Anforderungen hin zu überwachen. Wenn nicht konforme Ressourcen entdeckt werden, empfehlen wir Ihnen, den Versand von Warnmeldungen an eine Cloud Security Posture Management (CSPM)-Lösung wie AWS Security Hub zu konfigurieren, um bei der Abhilfe zu unterstützen. Diese Lösungen bieten einen zentralen Ort für Ihre Sicherheitsbeauftragten, um Probleme zu überwachen und Korrekturmaßnahmen zu ergreifen.

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 verwenden, können Sie dies über Angepasste Aktionen tun, wodurch die Suchinformationen in Amazon EventBridge veröffentlicht werden. Eine EventBridge-Regel kann dann Ihre Abhilfe einleiten. Sie können die benutzerdefinierte Aktion in Security Hub so konfigurieren, dass sie entweder automatisch oder manuell ausgeführt wird.

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 Erkenntnis in Security Hub.

Als Ausgangspunkt können 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 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 Erkenntnis in Security Hub.

Ressourcen

Zugehörige bewährte Methoden:

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

Zugehörige Dokumente:

- AWS Security Incident Response Guide – Detection

Zugehörige Beispiele:

- Automatische 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
- Automatische 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 Ihres Workloads 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 Richtlinien-Durchsetzungsmechanismen (z. B. Webanwendungs-Firewalls und/oder API-Gateways).

Regionen, Availability Zones, AWS Lokale Zonen und AWS Outposts

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

AWS hat das Konzept einer Region, d. h. eines physischen Standorts auf der ganzen Welt, an dem wir Rechenzentren 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 Residenz der Daten 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, in denen Ihre Daten sich physisch befinden; was hilfreich sein kann Ihre regionale Compliance- und Data-Residency-Anforderungen zu erfüllen. Jedes 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 (60 Meilen) 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-Die Regionen erfüllen die höchsten Anforderungen an Sicherheit, Compliance und Datenschutz.

AWS-Local Zones bringen Rechen-, 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 der 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 Dienste in der Region zugreifen.

AWS-Outposts bringen native AWS-Services, Infrastruktur und Betriebsmodelle in praktisch jedes Rechenzentrum, jede Colocation-Fläche 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

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

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

Die sorgfältige Verwaltung Ihres Netzwerkdesigns bildet die Grundlage, um Ressourcen innerhalb Ihrer Umgebung zu isolieren und einzugrenzen. Da viele Ressourcen in Ihrem 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. Siehe das AWS Well-Architected Serverless Applications Lens für spezifische Anleitungen zur Serverless-Sicherheit. .

Bewährte Methoden

- SEC05-BP01 Erstellen von Netzwerkebenen
- SEC05-BP02 Kontrollieren des Datenverkehrsflusses innerhalb Ihrer Netzwerkebenen
- SEC05-BP03 Implementieren eines prüfungsbasierten Schutzes
- SEC05-BP04 Automatisieren des Netzwerkschutzes

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 Einführung 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 2023 – AWS networking foundations

Zugehörige Beispiele:

- VPC-Beispiele
- Access container applications privately on Amazon ECS by using AWS Fargate, AWS PrivateLink, and a Network Load Balancer
- 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 Einführung 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 einer 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 Implement inspection-based protection.

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

Zugehörige Beispiele:

- Lab: CloudFront for Web Application

SEC05-BP03 Implementieren eines prüfungsbasierten Schutzes

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 Vorteile intelligenter Systeme außer Acht lassen
- Erstellen von Firewall-Regeln auf der Grundlage bestimmter aktueller Bedrohungsmuster, die sich ändern können
- Überprüfung des Datenverkehrs beschränkt auf den Übergang von privaten zu öffentlichen Subnetzen oder von öffentlichen Subnetzen zum Internet
- Sie verfügen nicht über eine Basisansicht Ihres Netzwerkdatenverkehrs, die Sie auf Verhaltensanomalien hin überprüfen können.

Vorteile der Einführung 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 Bedrohungsdaten basieren, da sich die Bedrohungslandschaft im Laufe der Zeit verändert. 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

Kontrollieren Sie Ihren zustandsbehafteten und zustandslosen Netzwerkverkehr im Detail mit AWS Network Firewall oder anderen Firewalls und Intrusion Prevention Systems (IPS) in AWS Marketplace, die Sie hinter einer (GWLB) bereitstellen können. AWS Network Firewall unterstützt Suricata-kompatible Open-Source-IPS-Spezifikationen zum Schutz Ihres Workloads.

Sowohl die Lösung AWS Network Firewall als auch die Lösungen der Anbieter, die eine GWLB verwenden, unterstützen verschiedene Modelle für die Bereitstellung von Inline-Prüfungen. Sie können zum Beispiel Prüfungen pro VPC durchführen, die Prüfungen in einer VPC zentralisieren oder in einem hybriden Modell bereitstellen, bei dem der Ost-West-Verkehr durch eine Prüfungs-VPC fließt und der Internet-Eingang pro VPC geprüft wird. Eine weitere Frage ist, ob die Lösung das Unwrapping von Transport Layer Security (TLS) unterstützt und damit eine Deep Packet Inspection für Datenverkehrsflüsse in beide Richtungen ermöglicht. Weitere Informationen und ausführliche Details zu diesen Konfigurationen finden Sie in den AWS Network Firewall Leitlinien für bewährte Methoden.

Wenn Sie Lösungen verwenden, die Out-of-Band-Prüfungen durchführen, wie z. B. die pcap-Analyse von Paketdaten von Netzwerkschnittstellen, die im Promiscuous-Modus arbeiten, können Sie die VPC traffic mirroring konfigurieren. 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 der AWS Marketplace verfügbar sind, die möglicherweise eine Inline-Bereitstellung hinter einer GWLB unterstützen.

Bei Komponenten, die über HTTP-basierte Protokolle abgewickelt werden, schützen Sie Ihre Anwendung mit einer Web Application Firewall (WAF) vor gängigen Bedrohungen. AWS WAF ist eine Web Application Firewall, mit der Sie HTTP(S)-Anfragen, die Ihren konfigurierbaren Regeln entsprechen, überwachen und blockieren können, bevor sie an Amazon API Gateway, Amazon CloudFront, AWS AppSync oder Application Load Balancer gesendet werden. Wenn Sie die Bereitstellung Ihrer Web Application Firewall prüfen, sollten Sie eine Deep Packet Inspection in Betracht ziehen, da einige Firewalls verlangen, dass Sie TLS vor der Überprüfung des Datenverkehrs beenden. Um mit AWS WAF zu beginnen, können Sie Von AWS verwaltete Regeln in Kombination mit Ihren eigenen oder mit bestehenden Partner-Integrationen verwenden.

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

Implementierungsschritte

1. Legen Sie fest, ob Sie die Inspektionsregeln weit fassen können, z. B. durch eine Inspektions-VPC, oder ob Sie einen granulareren Ansatz pro VPC benötigen.
2. Für Inline-Prüfungslösungen:
    a. Wenn Sie AWS Network Firewall verwenden, 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 Verfügbarkeitszonen bereit und konfigurieren sie. Dann erstellen Sie Ihre GWLB, den Endservice, den Endpunkt und konfigurieren das Routing für Ihren Datenverkehr.
3. Für Out-of-Band-Prüfungslösungen:
    1. Aktivieren Sie die VPC-Datenverkehrsspiegelung auf den Schnittstellen, auf denen der ein- und ausgehende Datenverkehr gespiegelt werden soll. Sie können Amazon EventBridge-Regeln verwenden, um eine AWS Lambda-Funktion aufzurufen, die die Datenverkehrsspiegelung auf Schnittstellen aktiviert, 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 AWS WAF zu konfigurieren, beginnen Sie mit der Konfiguration einer Internet-Zugriffssteuerungsliste (Web Access Control List, web ACL). Die web ACL ist eine Sammlung von Regeln mit einer seriell verarbeiteten Standardaktion (ALLOW oder DENY), die definiert, wie Ihre WAF den Datenverkehr behandelt. Sie können Ihre eigenen Regeln und Gruppen erstellen oder verwaltete Regelgruppen von AWS in Ihrer web ACL verwenden.
    b. Sobald Ihre web ACL konfiguriert ist, verknüpfen Sie die Web-ACL mit einer AWS-Ressource (z. B. einer Application Load Balancer, API Gateway-REST-API oder CloudFront-Distribution), um den Webverkehr zu schützen.

Ressourcen

Zugehörige Dokumente:

- What is Traffic Mirroring?
- Implementing inline traffic inspection using third-party security appliances

- AWS Network Firewall example architectures with routing
- Centralized inspection architecture with AWS Gateway Load Balancer and AWS Transit Gateway

Zugehörige Beispiele:

- Best practices for deploying Gateway Load Balancer
- TLS inspection configuration for encrypted egress traffic and AWS Network Firewall

Zugehörige Tools:

- AWS Marketplace IDS/IPS

SEC05-BP04 Automatisieren des Netzwerkschutzes

Automatisieren Sie die Bereitstellung Ihres Netzwerkschutzes mit DevOps-Verfahren 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 Einführung 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 Netzwerkschutzkontrollen, die in SEC05-BP02 Control traffic flows within your network layers und SEC05-BP03 Implement inspection-based protection beschrieben sind, verfügen über verwaltete Regelsysteme, die automatisch auf der Grundlage der neuesten Bedrohungsdaten aktualisiert werden können. Beispiele für den Schutz Ihrer Web-Endpunkte sind AWS WAF verwaltete Regeln und AWS Shield Advanced automatische DDoS-Abwehr auf Anwendungsebene. Verwenden Sie AWS Network Firewall-verwaltete Regelgruppen, um auch bei Domain-Listen mit geringer Reputation und Bedrohungssignaturen auf dem Laufenden zu bleiben.

Neben den verwalteten Regeln empfehlen wir Ihnen, DevOps-Praktiken einzusetzen, um die Bereitstellung Ihrer Netzwerkressourcen, Schutzmaßnahmen und der von Ihnen festgelegten Regeln zu automatisieren. 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 von DevOps für die Verwaltung Ihrer Netzwerkkontrollen zu nutzen, wie z. B. besser vorhersehbare Releases, automatisierte Tests mit Tools wie AWS CloudFormation Guard und die Erkennung von Abweichungen zwischen Ihrer bereitgestellten Umgebung und Ihrer gewünschten Konfiguration.

Basierend auf den Entscheidungen, die Sie im Rahmen von SEC05-BP01 Erstellen von Netzwerkebenen getroffen haben, verfügen Sie möglicherweise über einen zentralen Verwaltungsansatz für die Erstellung von VPCs, die für Ingress-, Egress- und Inspektionsflüsse bestimmt sind. Diese VPCs können Sie, wie in der AWS Security Reference Architecture (AWS

SRA) beschrieben, in einem speziellen Netzwerkinfrastrukturkonto definieren. Sie können ähnliche Techniken verwenden, um die von Ihren Workloads in anderen Konten verwendeten VPCs, deren Sicherheitsgruppen, AWS Network Firewall-Bereitstellungen, Route 53-Resolver-Regeln und DNS-Firewall-Konfigurationen sowie andere Netzwerkressourcen zentral zu definieren. Sie können diese Ressourcen mit Ihren anderen Konten mit der 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 der Bereitstellung von Standard-Sicherheitskontrollen

Zugehörige Dokumente:

- AWS Security Reference Architecture – Network account

Zugehörige Beispiele:

- AWS Deployment Pipeline Reference Architecture
- NetDevSecOps to modernize AWS networking deployments
- Integrating AWS CloudFormation security tests with AWS Security Hub and AWS CodeBuild reports

Zugehörige Tools:

- AWS CloudFormation
- AWS CloudFormation Guard
- cfn_nag

Schutz der Datenverarbeitung

Zu den Datenverarbeitungsressourcen zählen EC2-Instances, Container, AWS-Lambda-Funktionen, Datenbankservices, IoT-Geräte und mehr. Jede dieser Arten von Rechenressourcen erfordert unterschiedliche Ansätze zu ihrer Sicherung. 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 Rechenressourcen 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 Datenverarbeitung über gehärtete Images
- SEC06-BP03 Reduzieren der manuellen Verwaltung und des interaktiven Zugriffs
- SEC06-BP04 Validieren der Softwareintegrität
- 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: Erstellen und Verwalten eines Programms für das Schwachstellenmanagement. Überprüfen und Patchen Sie regelmäßig Ressourcen wie Amazon EC2-Instances, Amazon Elastic Container Service (Amazon ECS)-Container und Amazon Elastic Kubernetes Service (Amazon EKS)-Workloads. Konfigurieren Sie Wartungszeitfenster für AWS-verwaltete Ressourcen wie Amazon Relational Database Service (Amazon RDS)-Datenbanken. Verwenden Sie statisches Code-Scanning, um Anwendungsquellcode auf verbreitete Probleme zu überprüfen. Ziehen Sie Penetrationstests für Webanwendungen in Betracht, wenn Ihre Organisation über die entsprechenden Fähigkeiten verfügt oder externe Unterstützung erhalten kann.

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

Vorteile der Nutzung dieser bewährten Methode:

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Ein Programm für das Schwachstellenmanagement beinhaltet Sicherheitsbewertungen, die Identifizierung von Problemen sowie die Priorisierung und Durchführung von Patching-Vorgängen im Rahmen der Behebung der Probleme. Automatisierung ist der Schlüssel zur kontinuierlichen Prüfung von Workloads auf Probleme und unbeabsichtigte Offenlegung in Netzwerken sowie für die Durchführung von Abhilfemaßnahmen. Die Automatisierung der Erstellung und Aktualisierung von Ressourcen spart Zeit und senkt die Gefahr von Konfigurationsfehlern, die zu weiteren Problemen führen können. Ein gut gestaltetes Programm für das Schwachstellenmanagement sollte auch Schwachstellentests in den Entwicklungs- und Bereitstellungsphasen des Softwarelebenszyklus beinhalten. Die Implementierung des Schwachstellenmanagements während der Entwicklung und der Bereitstellung verringert die Gefahr, dass eine Schwachstelle in Ihre Produktionsumgebung gelangt.

Die Implementierung eines Programms für das Schwachstellenmanagement erfordert ein gutes Verständnis des AWS-Modells der geteilten Verantwortung und seiner Beziehung zu Ihren spezifischen Workloads. In diesem Modell der geteilten Verantwortung ist AWS für den Schutz der Infrastruktur der AWS Cloud verantwortlich. Diese Infrastruktur umfasst die Hardware, Software,

Netzwerke und Einrichtungen, in bzw. auf denen AWS Cloud-Services ausgeführt werden. Sie sind für die Sicherheit in der Cloud verantwortlich, zum Beispiel für die eigentlichen Daten, die Sicherheitskonfiguration und Verwaltungsaufgaben für Amazon EC2-Instances sowie für die Sicherstellung, dass Ihre Amazon S3-Objekte korrekt klassifiziert und konfiguriert sind. Ihr Konzept für das Schwachstellenmanagement kann auch je nach den von Ihnen genutzten Services variieren. So verwaltet beispielsweise AWS die Patches für unseren verwalteten relationalen Datenbankservice Amazon RDS, Sie sind jedoch selbst für das Patchen selbst gehosteter Datenbanken verantwortlich.

AWS bietet eine Reihe von Services zur Unterstützung Ihres Programms für das Schwachstellenmanagement. Amazon Inspector untersucht kontinuierlich AWS-Workloads auf Softwareprobleme und nicht beabsichtigte Netzwerkzugriffe. AWS Systems Manager Patch Manager hilft bei der Verwaltung des Patchings für Ihre Amazon EC2-Instances. Amazon Inspector und Systems Manager können in AWS Security Hub angezeigt werden. Dieser Managementservice für den Cloud-Sicherheitsstatus hilft dabei, AWS-Sicherheitsprüfungen zu automatisieren und Sicherheitsbenachrichtigungen zu zentralisieren.

Amazon CodeGuru kann mit der Analyse von statischem Code dabei helfen, potenzielle Probleme in Java- und Python-Anwendungen zu erkennen.

Implementierungsschritte

- Konfigurieren Sie Amazon Inspector: Amazon Inspector erkennt automatisch neu gestartete Amazon EC2-Instances, Lambda-Funktionen und infrage kommende Container-Images, die an Amazon ECR übertragen wurden, und untersucht diese sofort auf Softwareprobleme, potenzielle Fehler und unbeabsichtigte Netzwerkoffenlegung.
- Untersuchen Sie den Quellcode: Überprüfen Sie Bibliotheken und Abhängigkeiten auf Probleme und Fehler. Amazon CodeGuru kann diese Überprüfungen vornehmen und Empfehlungen zur Behebung verbreiteter Sicherheitsprobleme für Java- und Python-Anwendungen bereitstellen. Die OWASP Foundation veröffentlicht eine Liste von Quellcodeanalysetools (auch als SAST-Tools bezeichnet).
- Implementieren Sie einen Mechanismus zur Untersuchung und zum Patching Ihrer bestehenden Umgebung sowie zur Untersuchung im Rahmen eines CI/CD-Pipeline-Erstellungsprozesses: Implementieren Sie einen Mechanismus zur Untersuchung und zum Patching von Problemen in Ihren Abhängigkeiten und Betriebssystemen, um Schutz gegen neue Bedrohungen zu bieten. Lassen Sie diesen Mechanismus regelmäßig laufen. Das Software-Schwachstellenmanagement ist wichtig, um zu verstehen, wo Patches angebracht oder Softwareprobleme behoben werden müssen. Priorisieren Sie die Abhilfemaßnahmen zu potenziellen Sicherheitsproblemen durch die frühzeitige Einbettung von Schwachstellenanalysen in Ihre Pipeline für kontinuierliche Integration

und kontinuierliche Bereitstellung (Continuous Integration/Continuous Delivery, CI/CD). Ihr Konzept kann je nach den von Ihnen genutzten AWS-Services variieren. Fügen Sie zur Prüfung auf potenzielle Probleme in der Software, die in Amazon EC2-Instances ausgeführt wird, Ihrer Pipeline Amazon Inspector hinzu, damit Sie benachrichtigt werden und den Prozess anhalten können, wenn Probleme oder mögliche Fehler erkannt werden. Amazon Inspector überwacht Ressourcen kontinuierlich. Sie können auch Open-Source-Produkte wie OWASP Dependency-Check, Snyk, OpenVAS, Paketmanager oder AWS Partner-Tools für das Schwachstellenmanagement verwenden.

- Verwenden Sie AWS Systems Manager: Sie sind für das Patch-Management für Ihre AWS-Ressourcen verantwortlich, einschließlich Amazon Elastic Compute Cloud (Amazon EC2)-Instances, Amazon Machine Images (AMIs) und anderer Datenverarbeitungsressourcen. AWS Systems Manager Patch Manager automatisiert das Patchen verwalteter Instances mit sicherheitsrelevanten und anderen Arten von Updates. Patch Manager kann für die Durchführung von Patches auf Amazon EC2-Instances für Betriebssysteme und Anwendungen verwendet werden, darunter Microsoft-Anwendungen, Windows-Service Packs und kleinere Versionsaktualisierungen für auf Linux basierende Instances. Zusätzlich zu Amazon EC2 kann Patch Manager auch für das Patching von On-Premises-Servern genutzt werden.

  Eine Liste der unterstützten Betriebssysteme finden Sie unter Unterstützte Betriebssysteme im Systems Manager-Benutzerhandbuch. Sie können Instances scannen, um nur fehlende Patches anzuzeigen, oder Sie können scannen und automatisch alle fehlenden Patches installieren.
- Verwenden Sie AWS Security Hub: Security Hub bietet eine umfassende Ansicht Ihres Sicherheitszustands in AWS. Es erfasst Sicherheitsdaten über mehrere AWS-Services hinweg und stellt diese Ergebnisse in einem standardisierten Format bereit, damit Sie die Sicherheitsergebnisse für AWS-Services priorisieren können.
- Verwenden Sie AWS CloudFormation: AWS CloudFormation ist ein Infrastructure-as-Code (Iac)-Service, der das Schwachstellenmanagement durch die Automatisierung der Ressourcenbereitstellung und die Standardisierung der Ressourcenarchitektur über mehrere Konten und Umgebungen hinweg unterstützt.

Ressourcen

Zugehörige Dokumente:

- AWS Systems Manager
- Security Overview of AWS Lambda (Übersicht zur Sicherheit von AWS Lambda)

- Amazon CodeGuru
- Improved, Automated Vulnerability Management for Cloud Workloads with a New Amazon Inspector (Verbessertes und automatisiertes Schwachstellenmanagement für Cloud-Workloads mit einem neuen Amazon Inspector)
- Automate vulnerability management and remediation in AWS using Amazon Inspector and AWS Systems Manager – Part 1 (Automatisierung des Schwachstellenmanagements und von Abhilfemaßnahmen in AWS mit Amazon Inspector und AWS Systems Manager – Teil 1)

Zugehörige Videos:

- Securing Serverless and Container Services (Schutz von Serverless- und Container-Services)
- Security best practices for the Amazon EC2 instance metadata service (Bewährte Sicherheitsmethoden für den Amazon EC2-Instance-Metadatenservice)

SEC06-BP02 Bereitstellen von Datenverarbeitung über gehärtete 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 Einführung 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 den Aufwand für die Systemhärtung verringern, indem Sie Anleitungen nutzen, die von vertrauenswürdigen Quellen bereitgestellt werden, wie z. B. dem Center for Internet Security (CIS) und die Security Technical Implementation Guides (STIGs) der Defense Information Systems Agency (DISA). Wir empfehlen Ihnen, mit einem Amazon Machine Image (AMI) zu beginnen, das von AWS oder einem APN-Partner veröffentlicht wurde. Ferner empfehlen wir die Verwendung von AWS EC2 Image Builder, um die Konfiguration gemäß einer geeigneten Kombination von CIS- und STIG-Kontrollen zu automatisieren.

Es gibt zwar gehärtete Images und EC2 Image Builder-Rezepte, die die CIS- oder DISA-STIG-Empfehlungen anwenden. Sie werden jedoch möglicherweise feststellen, dass deren Konfiguration die erfolgreiche Ausführung Ihrer Software verhindert. In dieser Situation können Sie von einem nicht

gehärteten Basis-Image ausgehen, Ihre Software installieren und dann schrittweise CIS-Kontrollen anwenden, um deren Auswirkungen zu testen. Testen Sie bei jeder CIS-Kontrolle, die die Ausführung Ihrer Software verhindert, ob Sie stattdessen die detaillierteren Härtungsempfehlungen der DISA implementieren können. Behalten Sie den Überblick über die verschiedenen CIS-Kontrollen und DISA-STIG-Konfigurationen, die Sie erfolgreich anwenden können. Verwenden Sie diese, um Ihre Rezepte für die Imagehärtung in EC2 Image Builder entsprechend zu definieren.

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

Ähnlich wie bei Betriebssystemen und Container-Images können Sie auch Code-Pakete (oder Bibliotheken) aus öffentlichen Repositorys beziehen, und zwar mithilfe von Tools wie pip, npm, Maven und 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 Aktualisieren von Paketen für Sie übernehmen. Ihre Anwendungserstellungsprozesse können dann die neueste Version dieser Pakete zusammen mit Ihrer Anwendung abrufen und testen, wobei Techniken wie Software Composition Analysis (SCA), Static Application Security Testing (SAST) und Dynamic Application Security Testing (DAST) zum Einsatz kommen.

Für Serverless Workloads, die AWS Lambda verwenden, vereinfachen Sie die Verwaltung von Paketabhängigkeiten mit Lambda-Ebenen. 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 durch einen eigenen Erstellungsprozess erstellen und pflegen, sodass Ihre Funktionen immer auf dem neuesten Stand sind.

Implementierungsschritte

- Härten des Betriebssystems. Verwenden Sie Basis-Images aus vertrauenswürdigen Quellen als Grundlage für die Erstellung Ihrer gehärteten AMIs. Mit EC2 Image Builder können Sie die auf Ihren Images installierte Software anpassen.
- Härten von containerisierten Ressourcen. Konfigurieren Sie containerisierte Ressourcen so, dass sie den bewährten Methoden im Bereich Sicherheit entsprechen. Implementieren Sie bei der Verwendung von Containern ECR Image Scanning in Ihrer Build-Pipeline und in regelmäßigen Abständen im Vergleich mit Ihrem Image-Repository, um nach CVEs in Ihren Containern zu suchen.

- Wenn Sie eine Serverless-Implementierung mit AWS Lambda verwenden, nutzen Sie Lambda-Ebenen, um den Funktionscode der Anwendung und gemeinsam genutzte abhängige Bibliotheken zu segmentieren. Konfigurieren Sie Codesignierung für Lambda, um sicherzustellen, dass nur vertrauenswürdiger Code in Ihren Lambda-Funktionen ausgeführt wird.

Ressourcen

Zugehörige bewährte Methoden:

- OPS05-BP05 Durchführen der Patch-Verwaltung

Zugehörige Videos:

- Deep dive into AWS Lambda security

Zugehörige Beispiele:

- Quickly build STIG-compliant AMI using EC2 Image Builder
- Building better container images
- Using Lambda layers to simplify your development process
- Develop & Deploy AWS Lambda Layers using Serverless Framework
- Building end-to-end AWS DevSecOps CI/CD pipeline with open source SCA, SAST and DAST tools

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 lokale 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 Einführung 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. Der AWS 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:

- Ersetzen des SSH-Zugriffs zur Reduzierung des Verwaltungs- und Sicherheitsaufwands durch AWS Systems Manager

Zugehörige Tools:

- AWS Systems Manager

Zugehörige Videos:

- Kontrolle des Zugriffs von Benutzersitzungen auf Instances in AWS Systems Manager-Sitzungsmanager

SEC06-BP04 Validieren der Softwareintegrität

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 Einführung 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, wenn diese bewährte Methode nicht eingeführt wird: 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:

- EC2 Image Builder: Verify the signature of the AWSTOE installation download

- AWS Systems Manager: Verifying the signature of SSM Agent
- Amazon CloudWatch: Verifying the signature of the CloudWatch agent package

Integrieren Sie die Überprüfung digitaler Signaturen in die Prozesse, die Sie zur Beschaffung und Härtung von Images verwenden, wie in SEC06-BP02 Bereitstellen von Datenverarbeitung über gehärtete 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
- Best Practices to help secure your container image build pipeline by using AWS Signer
- Announcing Container Image Signing with AWS Signer and Amazon EKS
- Configuring code signing for AWS Lambda
- Best practices and advanced patterns for Lambda code signing
- Code signing using AWS Certificate Manager Private CA and AWS Key Management Service asymmetric keys

Zugehörige Beispiele:

- Automate Lambda code signing with Amazon CodeCatalyst and AWS Signer
- Signing and Validating OCI Artifacts with 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 Einführung 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. SEC06-BP01 Schwachstellenmanagement beschreibt, 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 AWS Systems 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. Siehe SEC06-BP03 Reduzieren der manuellen Verwaltung und des interaktiven Zugriffs, um mehr zu erfahren.

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. Ihr 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 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 kann erkennen, wenn EC2 Instances IMDSv1 verwenden und eine automatische Abhilfe einleiten. Erfahren Sie mehr über automatische Erkennung und Abhilfemaßnahmen in 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
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 Patch Manager verwenden, um Patches für Betriebssysteme und Anwendungen anzuwenden.
    a. AWS Systems Manager Incident 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 lokalen 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 Einführung 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 Kategorisierung von sensiblen Daten innerhalb Ihres Workloads zu erleichtern, sollten Sie, sofern verfügbar, Ressourcen-Tags verwenden. Sie können zum Beispiel ein Tag mit dem Tag-Schlüssel `Klassifizierung` und dem Tag-Wert `PHI` für geschützte Gesundheitsinformationen (Protected Health Information, PHI) und ein weiteres Tag mit dem Tag-Schlüssel `Sensibilität` und dem Tag-Wert `Hoch` 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, einer Funktion 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. Vergewissern Sie sich, dass sensible Daten in Ihrem Workload gemäß Ihrer Richtlinie gespeichert und geschützt werden. Nutzen Sie Techniken wie automatisierte Tests, um die Wirksamkeit Ihrer Kontrollen zu überprüfen.
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

Vorteile der Einführung 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 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
- Best Practices for Security, Identify, & 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 Einführung 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. 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 Macie durchsucht zu werden.

2. Konfigurieren Sie laufende Scans Ihrer Umgebungen.
   a. Die automatische Erkennungsfunktion für sensible Daten von 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 Macie ausgeschlossen werden.
3. 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.
4. Implementieren Sie ein System oder Runbook, um Maßnahmen zu ergreifen, wenn sensible Daten an nicht autorisierten Orten gefunden werden.

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 Einführung 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, wenn diese bewährte Methode nicht eingeführt wird: 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.

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.

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 Ihrem 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 der 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, die es als Token ersetzt. 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 aufbewahrt werden.

Überprüfen der Verwendung von Verschlüsselungsschlüsseln: Vergewissern Sie sich, dass Sie die Verwendung von Verschlüsselungsschlüsseln verstehen und überprüfen, um zu validieren, 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 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 Durchsetzen der Zugriffskontrolle

SEC08-BP01: Implementieren einer sicheren Schlüsselverwaltung

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

Gewünschtes Ergebnis: Ein skalierbarer, wiederholbarer und automatisierter Schlüsselverwaltungsmechanismus. Der Mechanismus sollte die Möglichkeit bieten, den Zugriff mit den geringsten Berechtigungen auf Schlüsseldaten zu erzwingen, und das richtige Gleichgewicht zwischen Schlüsselverfügbarkeit, Vertraulichkeit und Integrität bieten. Der Zugriff auf Schlüssel sollte überwacht werden und Schlüsseldaten sollten mit einem automatisierten Prozess rotiert werden. Schlüsseldaten sollten niemals für menschliche Identitäten zugänglich sein.

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 Ihren Workload einrichten, können Sie dazu beitragen, Ihre Inhalte vor unbefugtem Zugriff zu schützen. Darüber hinaus gelten möglicherweise gesetzliche Anforderungen zur Verschlüsselung Ihrer Daten. Eine effektive Schlüsselverwaltungslösung kann technische Mechanismen bereitstellen, die diesen Vorschriften zum Schutz von Schlüsseldaten entsprechen.

Risikostufe bei fehlender Befolgung dieser Best Practice: Hoch

Implementierungsleitfaden

Viele regulatorische Anforderungen und bewährte Methoden beinhalten die Verschlüsselung von Daten im Ruhezustand als grundlegende Sicherheitskontrolle. Um diese Bedingung zu erfüllen, benötigt Ihr Workload einen Mechanismus, mit dem Schlüsseldaten, die zur Verschlüsselung Ihrer Daten im Ruhezustand verwendet werden, sicher gespeichert und verwaltet werden können.

AWS bietet AWS Key Management Service (AWS KMS) zur dauerhaften, sicheren und redundanten Speicherung von AWS KMS-Schlüsseln. Viele AWS-Services lassen sich in AWS KMS integrieren,

um die Verschlüsselung Ihrer Daten zu unterstützen. AWS KMS verwendet FIPS 140-2 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 Strategie für mehrere Konten gilt es als bewährte Methode, AWS KMS-Schlüssel im selben Konto zu speichern wie der Workload, der sie verwendet. In diesem verteilten Modell liegt die Verantwortung für die Verwaltung der AWS KMS-Schlüssel beim Anwendungsteam. In anderen Anwendungsfällen können sich Unternehmen 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 streng kontrolliert werden. Schlüsselrichtlinien sind die wichtigste Methode, um den Zugriff auf einen AWS KMS-Schlüssel zu kontrollieren. Darüber hinaus können AWS KMS-Schlüsselzuweisungen den Zugriff auf AWS-Services ermöglichen, mit denen Daten in Ihrem Namen ver- und entschlüsselt werden. Nehmen Sie sich Zeit, um die bewährten Methoden für die Steuerung des Zugriffs auf AWS KMS-Schlüsseldurchzugehen.

Es hat sich bewährt, die Verwendung von Verschlüsselungsschlüsseln zu überwachen, um ungewöhnliche Zugriffsmuster zu erkennen. 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. Besondere Aufmerksamkeit sollte dabei der Überwachung von Schlüsselzerstörungsereignissen gelten. Um die versehentliche oder böswillige Zerstörung von Schlüsseldaten zu verhindern, werden Schlüsseldaten bei Schlüsselzerstörungsereignissen nicht sofort gelöscht. Für Versuche, Schlüssel in AWS KMS zu löschen, gilt eine Wartezeit, die standardmäßig auf 30 Tage festgelegt ist. So haben Administratoren Zeit, diese Aktionen zu überprüfen und die Anfrage gegebenenfalls rückgängig zu machen.

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, empfiehlt sich eine Umschlagverschlüsselung zum Schutz Ihrer Daten. Das AWS-Verschlüsselungs-SDK kann Ihren Anwendungen clientseitige Verschlüsselungsprimitive 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 vom Kunden verwaltet) für den Schlüssel.
   - 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.
   - 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 einem externen Schlüsselspeicher.
2. Gehen Sie die Liste der Services durch, die Sie für Ihren 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 wir die versehentliche Offenlegung unverschlüsselter Snapshot-Daten verhindert.
   - So nutzen AWS-Services AWS KMS
   - Ausführliche Informationen zu den Verschlüsselungsoptionen, die ein AWS-Service bietet, finden Sie im Thema „Verschlüsselung im Ruhezustand“ im Benutzerhandbuch oder Entwicklerhandbuch für den Service.
3. Implementieren Sie AWS KMS: AWS KMS erleichtert Ihnen das Erstellen und Verwalten von Schlüsseln sowie die Kontrolle der Verschlüsselung in einer Vielzahl von AWS-Services und in Ihren Anwendungen.
   - Erste Schritte mit AWS Key Management Service (AWS KMS)
   - Lesen Sie die bewährten Methoden für die Steuerung des Zugriffs auf AWS KMS-Schlüssel.
4. Erwägen Sie die Verwendung des AWS Encryption SDK: Verwenden Sie das AWS Encryption SDK mit AWS KMS-Integration, wenn Ihre Anwendung Daten clientseitig verschlüsseln muss.
   - 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.
6. Aktivieren Sie Security Hub, 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.
    - Einige Organisationen ziehen es vor, die AWS KMS-Protokollierungsaktivitäten in einem eigenen Pfad zu separieren. Weitere Details finden Sie im Abschnitt Logging AWS KMS API calls with CloudTrail (Protokollieren von AWS KMS-API-Aufrufen mit CloudTrail) im AWS KMS-Entwicklerhandbuch.

Ressourcen

Zugehörige Dokumente:

- AWS Key Management Service
- AWS cryptographic services and tools (Kryptografische AWS-Services und -Tools)
- Protecting Amazon S3 Data Using Encryption (Schutz von S3-Daten durch Verschlüsselung)
- Umschlagverschlüsselung
- Das Versprechen zu digitaler Souveränität
- Demystifying AWS KMS key operations, bring your own key, custom key store, and ciphertext portability (Das Geheimnis von AWS KMS-Schlüsselvorgängen, Bring Your Own Key, benutzerdefinierten Schlüsselspeichern und Portabilität von Geheimtext)
- AWS Key Management Service cryptographic details (Kryptografische Details in AWS Key Management Service)

Zugehörige Videos:

- How Encryption Works in AWS (So funktioniert die Verschlüsselung in AWS)
- Securing Your Block Storage on AWS (Sichern Ihres Blockspeichers in AWS)
- AWS data protection: Using locks, keys, signatures, and certificates (Datenschutz in AWS: Verwenden von Schlössern, Schlüsseln, Signaturen und Zertifikaten)

Zugehörige Beispiele:

- Implement advanced access control mechanisms using AWS KMS (Implementieren erweiterter Zugriffskontrollmechanismen mit AWS KMS)

SEC08-BP02 Erzwingen der Verschlüsselung im Ruhezustand

Sie sollten die Verwendung der Verschlüsselung von Daten im Ruhezustand erzwingen. Durch die Verschlüsselung wird die Vertraulichkeit sensitiver Daten im Falle eines unautorisierten Zugriffs oder einer unbeabsichtigten Offenlegung gewahrt.

Gewünschtes Ergebnis: Private Daten sollten im Ruhezustand standardmäßig verschlüsselt werden. Die Verschlüsselung wahrt die Vertraulichkeit der Daten und bietet eine zusätzliche Schutzebene gegen beabsichtigte oder unbeabsichtigte Datenoffenlegung oder Exfiltration. Verschlüsselte Daten können ohne vorherige Entschlüsselung nicht gelesen oder genutzt werden. Alle unverschlüsselt gespeicherten Daten sollten inventarisiert und kontrolliert werden.

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 den Datenklassifizierungen in Ihren Workloads Verschlüsselungsschlüssel zu. Dies hilft beim Schutz vor Zugriffsmöglichkeiten mit zu vielen Berechtigungen bei Verwendung eines einzigen oder sehr weniger Verschlüsselungsschlüssel für Ihre Daten (vgl. 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 Simple Storage Service (Amazon S3) können Sie beispielsweise die Standardverschlüsselung für einen Bucket festlegen, sodass neue Objekte automatisch verschlüsselt werden. Berücksichtigen Sie bei der Verwendung von AWS KMS, wie eng die Daten eingeschränkt werden müssen. Standard- und servicegesteuerte AWS KMS-Schlüssel werden für Sie von AWS verwaltet und verwendet. Ziehen Sie für sensible

Daten, die einen differenzierten Zugriff auf den zugrunde liegenden Verschlüsselungsschlüssel erfordern, kundenverwaltete Schlüssel (CMKs) in Betracht. Sie haben die vollständige Kontrolle über CMKs, einschließlich Rotation und Zugriffsmanagement mithilfe von Schlüsselrichtlinien.

Zudem unterstützen Amazon Elastic Compute Cloud (Amazon EC2) und Amazon S3 das Erzwingen der Verschlüsselung durch Festlegen einer Standardverschlüsselung. Sie können AWS-Config-Regeln verwenden, um automatisch zu überprüfen, ob Sie die Verschlüsselung nutzen, z. B. für Amazon Elastic Block Store (Amazon EBS)-Volumes, Amazon Relational Database Service (Amazon RDS)-Instances und Amazon S3-Buckets.

AWS bietet auch Optionen für die clientseitige Verschlüsselung, mit der Sie Daten vor dem Laden in die Cloud verschlüsseln können. Das AWS Encryption SDK bietet eine Möglichkeit zur Verschlüsselung Ihrer Daten mit Umschlagverschlüsselung. Sie stellen den Wrapping-Schlüssel bereit und das AWS Encryption SDK generiert einen eindeutigen Datenschlüssel für jedes verschlüsselte Datenobjekt. Ziehen Sie 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 zu AWS geladen werden. DerAmazon DynamoDB Encryption Client ermöglicht darüber hinaus das Verschlüsseln und Signieren von Elementen vor dem Laden in eine DynamoDB-Tabelle.

Implementierungsschritte

- Erzwingen Sie die Verschlüsselung von Daten im Ruhezustand für Amazon S3: Implementieren Sie die Standardverschlüsselung für Amazon S3-Buckets.

  Konfigurieren Sie die Standardverschlüsselung für neue Amazon EBS-Volumes: Legen Sie fest, 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 Sie verschlüsselte Amazon Machine Images (AMIs): Beim Kopieren eines vorhandenen AMI mit aktivierter Verschlüsselung werden Root-Volumes und Snapshots automatisch verschlüsselt.

Konfigurieren Sie die Amazon RDS-Verschlüsselung: Konfigurieren Sie die Verschlüsselung für Ihre Amazon RDS-Datenbank-Cluster und Snapshots im Ruhezustand durch Aktivieren der Verschlüsselungsoption.

Erstellen und konfigurieren Sie AWS KMS-Schlüssel mit Richtlinien, die den Zugriff für jede Datenklassifizierung auf die jeweiligen Prinzipale beschränken: Erstellen Sie beispielsweise einen AWS KMS-Schlüssel für die Verschlüsselung von Produktionsdaten und einen anderen Schlüssel für Entwicklungs- oder Testdaten. Sie können den Schlüsselzugriff auch für andere AWS-Konten 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 Sie Verschlüsselung in weiteren AWS-Services: Sehen Sie sich die Sicherheitsdokumentation zu anderen verwendeten AWS-Services an, um die entsprechenden Verschlüsselungsoptionen festzustellen.

Ressourcen

Zugehörige Dokumente:

- AWS Crypto Tools
- Dokumentation zu AWS
- AWS Encryption SDK
- Whitepaper: Einführung in die kryptografischen Details von AWS KMS
- AWS Key Management Service
- AWS cryptographic services and tools (Kryptografische Services und Tools von AWS)
- Amazon EBS-Verschlüsselung
- Default encryption for Amazon EBS volumes (Standardverschlüsselung für Amazon EBS-Volumes)
- Verschlüsseln von Amazon RDS-Ressourcen
- How do I enable default encryption for an Amazon S3 bucket? (Wie kann ich die Standardverschlüsselung für einen Amazon S3-Bucket aktivieren?)

- Protecting Amazon S3 Data Using Encryption (Schutz von Amazon S3-Daten durch Verschlüsselung)

Zugehörige Videos:

- How Encryption Works in AWS (So funktioniert die Verschlüsselung in AWS)
- Securing Your Block Storage on AWS (Sichern Ihres Blockspeichers in AWS)

SEC08-BP03 Automatisieren des Schutzes von Daten im Ruhezustand

Nutzen Sie die 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 die 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 Datenspeicher auf Fehlkonfigurationen der Kontrollen, unbefugten Zugriff und unerwartete Nutzung. Die Erkennung von falsch konfigurierten Speicherorten leitet automatische Abhilfemaßnahmen ein. Automatisierte Prozesse erstellen Datensicherungen 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 Durchsetzung der Einstellungen für den öffentlichen Zugriff auf Speicherservices.
- Keine Überwachung und Prüfung Ihrer Kontrollen zum Schutz von Daten im Ruhezustand.

Vorteile der Einführung dieser bewährten Methode: Die Automatisierung hilft, das Risiko einer Fehlkonfiguration Ihrer Datenspeicher zu vermeiden. Dieses Vorgehen hilft zu verhindern, dass Fehlkonfigurationen in Ihre Produktionsumgebungen gelangen. Diese bewährte Methode trägt außerdem dazu bei, Fehlkonfigurationen zu erkennen und zu beheben, falls sie auftreten.

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. SEC01-BP06 Automatisieren der Bereitstellung von Standard-Sicherheitskontrollen beschreibt, wie Sie die Konfiguration Ihrer Ressourcen mithilfe von Infrastructure as Code (IaC)-Vorlagen erfassen können, z. B. 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, z. B. für die Verschlüsselungseinstellungen in 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. Sie können Einstellungen, die noch nicht in CloudFormation oder anderen IaC-Tools verfügbar sind, mit AWS Config auf Fehlkonfigurationen überwachen. Warnungen, die Config für Fehlkonfigurationen erzeugt, können automatisch behoben werden, wie in SEC04-BP04 Initiate remediation for non-compliant resources beschrieben.

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

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

Befolgen Sie die Praktiken in REL09 Daten sichern, um eine automatisierte Datensicherungs- und Wiederherstellungsstrategie zu entwickeln. Datensicherung und -wiederherstellung sind für die Wiederherstellung nach Sicherheitsereignissen ebenso wichtig wie für betriebliche Ereignisse.

Implementierungsschritte

1. Erfassen Sie die Konfiguration des Datenspeichers in IaC-Vorlagen. Verwenden Sie automatische Prüfungen in Ihren CI/CD-Pipelines, um Fehlkonfigurationen zu erkennen.
   a. Sie können <ulink type="marketing" url="cloudformation">&CFN;</ulink> für Ihre IaC-Vorlagen verwenden und CloudFormation Guard um Vorlagen auf Fehlkonfigurationen zu überprüfen.
   b. Verwenden Sie AWS Config, um Regeln in einem proaktiven Bewertungsmodus auszuführen. Verwenden Sie diese Einstellung, um die Konformität einer Ressource als Schritt in Ihrer CI/CD-Pipeline zu prüfen, bevor Sie sie erstellen.
2. Überwachen Sie Ressourcen auf Fehlkonfigurationen des Datenspeichers.
   a. Legen Sie AWS Config fest, um Datenspeicher-Ressourcen auf Änderungen der Kontrollkonfigurationen zu überwachen und Warnungen zu generieren, um Abhilfemaßnahmen aufzurufen, wenn eine Fehlkonfiguration entdeckt 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 die Berechtigungen möglicherweise reduziert werden können.
4. Überwachen Sie anomales Datenzugriffsverhalten und geben Sie entsprechende Warnmeldungen.
   a. GuardDuty überwacht sowohl bekannte Bedrohungssignaturen als auch Abweichungen vom grundlegenden Zugriffsverhalten 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 Warnmeldungen.
   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 von verschiedenen Datenquellen in AWS erstellt. Mit Elastic Disaster Recovery können Sie komplette Workloads von Servern 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 Datensicherungen 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: Automatically encrypt existing and new Amazon EBS volumes
- Ransomware Risk Management on AWS Using the NIST Cyber Security Framework (CSF)

Zugehörige Beispiele:

- How to use AWS Config proactive rules and AWS CloudFormation Hooks to prevent creation of noncompliant cloud resources
- Automate and centrally manage data protection for Amazon S3 with AWS Backup
- AWS re:Invent 2023 – Implement proactive data protection using Amazon EBS snapshots
- AWS re:Invent 2022 – Build and automate for resilience with modern data protection

Zugehörige Tools:

- AWS CloudFormation Guard
- AWS CloudFormation Guard Rules Registry
- IAM Access Analyzer

- Amazon Macie
- AWS Backup
- Elastic Disaster Recovery

SEC08-BP04 Durchsetzen der Zugriffskontrolle

Um Ihre Daten im Ruhezustand zu schützen, sollten Sie Zugriffskontrollen über Mechanismen wie das Isolieren und die Versionsverwaltung durchsetzen und das Prinzip der geringsten Berechtigung anwenden. Verhindern Sie den öffentlichen Zugriff auf Ihre Daten.

Gewünschtes Ergebnis: Sie stellen sicher, dass nur autorisierte Benutzer auf Daten zugreifen können, wenn dies unbedingt erforderlich ist. Sie schützen Ihre Daten mit regelmäßigen Backups und Versionsverwaltung vor beabsichtigten oder unbeabsichtigten Änderungen oder Löschungen. Sie isolieren wichtige Daten von anderen Daten, um die Vertraulichkeit und Datenintegrität zu schützen.

Typische Anti-Muster:

- gemeinsame Speicherung von Daten mit unterschiedlichen Anforderungen hinsichtlich Vertraulichkeit oder verschiedenen Klassifizierungen
- Verwendung von übermäßig großzügigen Berechtigungen für Entschlüsselungsschlüssel
- inkorrekte Klassifizierung von Daten
- keine Aufbewahrung von Sicherheitskopien wichtiger Daten
- Ermöglichen des dauerhaften Zugriffs auf Produktionsdaten
- keine Prüfung des Datenzugriffs bzw. keine regelmäßige Prüfung der Berechtigungen

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: niedrig

Implementierungsleitfaden

Mehrere Kontrollen können zum Schutz Ihrer Daten im Ruhezustand beitragen, einschließlich Zugriff (unter Verwendung des Prinzips der geringsten Berechtigung), Isolierung und Versionsverwaltung. Der Zugriff auf Ihre Daten sollte mit Erkennungsmechanismen wie beispielsweise AWS CloudTrail und Service-Level-Protokollen (z. B. Amazon Simple Storage Service (Amazon S3)-Zugriffsprotokolle) überprüft werden. Sie sollten inventarisieren, welche Daten öffentlich zugänglich sind, und einen Plan erstellen, wie Sie die Menge an öffentlich verfügbaren Daten im Laufe der Zeit reduzieren können.

Amazon S3 Glacier Vault Lock und Amazon S3 Object Lock bieten eine obligatorische Zugriffskontrolle für Objekte in Amazon S3. Sobald eine Tresorrichtlinie mit der Compliance-Option gesperrt ist, kann sie nicht einmal der Root-Benutzer ändern, bis die Sperre abläuft.

Implementierungsschritte

- Erzwingen der Zugriffskontrolle: Erzwingen Sie die Zugriffskontrolle nach dem Prinzip der geringsten Berechtigung, einschließlich des Zugriffs auf Verschlüsselungsschlüssel.
- Trennen von Daten anhand unterschiedlicher Klassifizierungsstufen: Verwenden Sie unterschiedliche AWS-Konten für die Datenklassifizierungsstufen und verwalten Sie diese Konten mit AWS Organizations.
- Überprüfen von AWS Key Management Service (AWS KMS)-Richtlinien: Überprüfen Sie die gewährte Zugriffsebene in den AWS KMS-Richtlinien.
- Überprüfen der Berechtigungen für Amazon S3-Buckets und -Objekte: Überprüfen Sie regelmäßig den in S3-Bucket-Richtlinien gewährten Zugriff. Als bewährte Methode gilt, keine öffentlich lesbaren oder schreibbaren Buckets zu haben. Erwägen Sie, AWS Config zur Erkennung von öffentlich verfügbaren Buckets und Amazon CloudFront für die Bereitstellung von Inhalten aus Amazon S3 zu verwenden. Stellen Sie sicher, dass Buckets, die den öffentlichen Zugriff nicht gewähren sollten, so konfiguriert sind, dass ein öffentlicher Zugriff verhindert wird. Standardmäßig sind alle S3 Buckets privat. Der Zugriff ist nur für Benutzer möglich, denen der Zugriff ausdrücklich gewährt wurde.
- Aktivieren von AWS IAM Access Analyzer: IAM Access Analyzer analysiert Amazon S3-Buckets und generiert ein Ergebnis, wenn eine S3-Richtlinie Zugriff auf eine externe Entität gewährt.
- Aktivieren der Amazon S3-Versionsverwaltung und der Objektsperre, wenn dies angemessen ist.
- Verwenden von Amazon S3 Inventory: Amazon S3 Inventory kann verwendet werden, um den Replikations- und Verschlüsselungsstatus Ihrer S3-Objekte zu prüfen und zu melden.
- Überprüfen von Amazon EBS- und AMI-Freigabeberechtigungen: Mit Freigabeberechtigungen können Images und Volumes für AWS-Konten außerhalb Ihres Workloads freigegeben werden.
- Regelmäßiges Überprüfen der Freigaben von AWS Resource Access Manager, um zu bestimmen, ob Ressourcen weiterhin freigegeben werden sollten. Resource Access Manager ermöglicht die Freigabe von Ressourcen wie beispielsweise Richtlinien für AWS Network Firewall, Amazon Route 53-Resolver-Regeln und Subnetzen innerhalb Ihrer Amazon VPCs. 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:

- Whitepaper: Einführung in die kryptografischen Details von AWS KMS
- 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: A Match Made in the Cloud (Amazon S3 + Amazon CloudFront: Die perfekte Kombination in der Cloud)
- Verwenden der Versionsverwaltung
- Locking Objects Using Amazon S3 Object Lock (Sperren von Objekten mit der Amazon S3-Objektsperre)
- Teilen eines Amazon EBS-Snapshots
- Gemeinsame AMIs
- Hosting a single-page application on Amazon S3 (Hosten einer Single-Page-Anwendung in Amazon S3)

Zugehörige Videos:

- Securing Your Block Storage on AWS (Sichern Ihres Blockspeichers in AWS)

Schutz von Daten während der Übertragung

Daten im Transit verstehen wir alle Daten, die von einem System an ein anderes gesendet werden. Hierzu zählt auch die Kommunikation zwischen Ressourcen innerhalb Ihres Workloads 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 Diensten 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 einer Verschlüsselung bei der Übertragung
- SEC09-BP03 Authentifizieren der Netzwerkkommunikation

SEC09-BP01 Implementieren einer sicheren Schlüssel- und Zertifikatverwaltung

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

Gewünschtes Ergebnis: Ein sicheres Zertifikatverwaltungssystem, das Zertifikate in einer Public-Key-Infrastruktur (PKI) bereitstellen, speichern und verlängern kann. Ein sicherer Schlüssel- und Zertifikatsverwaltungsmechanismus verhindert die Offenlegung von Zertifikatsmaterial mit privaten Schlüsseln und erneuert das Zertifikat automatisch in regelmäßigen Abständen. Es lässt sich auch in andere Services integrieren, um eine sichere Netzwerkkommunikation und Identität für Maschinenressourcen innerhalb Ihres Workloads 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 Entwurf 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 wird mithilfe von TLS-Zertifikaten gefördert.
- Sicherheit und Überprüfbarkeit der von der Zertifizierungsstelle ausgeführten Zertifikataktionen werden gesteigert.
- Verwaltungsaufgaben werden auf verschiedenen Ebenen der CA-Hierarchie angeordnet.

Risikostufe bei fehlender Befolgung dieser Best Practice: Hoch

Implementierungsleitfaden

Moderne Workloads nutzen verschlüsselte Netzwerkkommunikation mithilfe von PKI-Protokollen wie TLS in großem Umfang. Die Verwaltung von PKI-Zertifikaten kann komplex sein, durch automatisierte Bereitstellung und Verlängerung von Zertifikaten können aber Reibungsverluste im Zusammenhang mit der Zertifikatverwaltung verringert werden.

AWS bietet zwei Services zur Verwaltung von allgemeinen PKI-Zertifikaten: 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 Zertifikate mithilfe von AWS Private CA aus und lässt sich in viele andere verwaltete AWS-Services zur Bereitstellung sicherer TLS-Zertifikate für Workloads integrieren.

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 kontrollieren 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 das groß angelegte Onboarding von IoT-Geräten in Ihre Public-Key-Infrastruktur.

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 Planung Ihrer AWS Private CA-Bereitstellung .

Implementierungsschritte

1. Ermitteln Sie die relevanten AWS-Services, die für Ihren Anwendungsfall erforderlich sind:
    - Viele Anwendungsfälle können die bestehende Public-Key-Infrastruktur von AWS mithilfe von AWS Certificate Managernutzen. ACM kann zur Bereitstellung von TLS-Zertifikaten für Webserver, Load Balancer oder für andere Zwecke für öffentlich vertrauenswürdige Zertifikate verwendet werden.
    - Erwägen Sie die AWS Private CA , wenn Sie Ihre eigene private Zertifizierungsstellenhierarchie einrichten müssen oder Zugriff auf exportierbare Zertifikate benötigen. Mit ACM können dann viele Arten von Endentitätszertifikaten mit dem AWS Private CA ausgegeben werden.

- Für Anwendungsfälle, in denen Zertifikate für eingebettete Geräte des Internet der Dinge (IoT) in großem Umfang bereitgestellt werden müssen, erwägen Sie den Einsatz von AWS IoT Core.

2. Implementieren Sie nach Möglichkeit eine automatische Zertifikatsverlängerung:
   - Verwenden Sie ACM verwaltete Verlängerung für Zertifikate, die von ACM zusammen mit integrierten AWS Managed Services ausgestellt wurden.
3. Richten Sie die Sie Protokollierung und Prüfpfade ein:
   - Aktivieren Sie CloudTrail-Protokolle, um Zugriff 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, Zertifikatssperrliste) zu speichern. Anleitungen zur Konfiguration dieses S3-Buckets basierend auf den Anforderungen Ihres Workloads finden Sie unter Planung einer Zertifikatssperrliste (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 Certificate Manager Private CA (Workshop)

Zugehörige Beispiele:

- Private CA-Workshop
- Workshop zur IOT-Geräteverwaltung (einschließlich der Gerätebereitstellung)

Zugehörige Tools:

- Plugin für Kubernetes-Zertifikatmanager für die Verwendung von AWS Private CA

SEC09-BP02 Erzwingen einer Verschlüsselung bei der Übertragung

Erzwingen Sie Ihre definierten Verschlüsselungsanforderungen basierend auf den Richtlinien, regulatorischen Verpflichtungen und Standards Ihrer Organisation, damit Sie Ihre Unternehmens-, Rechts- und Compliance-Anforderungen erfüllen können. Verwenden Sie nur Protokolle mit Verschlüsselung, wenn Sie vertrauliche Daten außerhalb Ihrer Virtual Private Cloud (VPC) übertragen. Verschlüsselung hilft bei der Wahrung der Datenvertraulichkeit auch dann, wenn die Daten nicht vertrauenswürdige Netzwerke durchqueren.

Gewünschtes Ergebnis: Alle Daten sollten während der Übertragung mithilfe von sicheren TLS-Protokollen und Verschlüsselungssammlungen verschlüsselt werden. Der Netzwerkverkehr zwischen Ihren Ressourcen und dem Internet muss verschlüsselt werden, um nicht autorisierten Zugriff auf die Daten zu verhindern. Nur der Netzwerkverkehr in Ihrer internen AWS-Umgebung sollte wenn möglich mit TLS verschlüsselt werden. Das interne AWS-Netzwerk ist standardmäßig verschlüsselt und der Netzwerkverkehr innerhalb einer VPC kann nicht manipuliert oder analysiert werden, es sei denn, eine unbefugte Partei hat sich Zugang zu der Ressource verschafft, die den Datenverkehr generiert (wie beispielsweise Amazon EC2-Instances und Amazon ECS-Container). Überlegen Sie, ob Sie den Netzwerk-zu-Netzwerk-Datenverkehr mit einem IPsec Virtual Private Network (VPN) schützen sollten.

Typische Anti-Muster:

- Verwendung veralteter Versionen von SSL, TLS und Komponenten von Verschlüsselungssammlungen (z. B. SSL v3.0, RSA-Schlüssel mit 1 024 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 von selbstsignierten X.509-Zertifikaten 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 Protokolle wie HTTP können in einer VPC durch die Verwendung von Sicherheitsgruppen überprüft und blockiert werden. HTTP-Anfragen können in Amazon CloudFront oder einem Application Load Balancer auch automatisch an HTTPS umgeleitet werden. Sie haben uneingeschränkte Kontrolle über Ihre Datenverarbeitungsressourcen und können die Verschlüsselung während der Übertragung in alle Ihre Services implementieren. Darüber hinaus können Sie die VPN-Konnektivität mit Ihrer VPC von einem externen Netzwerk oder AWS Direct Connect aus verwenden, um die Verschlüsselung des Datenverkehrs zu erleichtern. Stellen Sie sicher, dass Ihre Kunden AWS-API-Aufrufe mindestens mit TLS 1.2 tätigen, da AWS die Verwendung von TLS 1.0 und 1.1 im Juni 2023 einstellt. Sollten Sie besondere Anforderungen haben, finden Sie Lösungen von Drittanbietern im AWS Marketplace.

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 bei Edge-Services: Konfigurieren Sie HTTPS mit Amazon CloudFront und verwenden Sie ein für Ihren Sicherheitsstatus und Ihren Anwendungsfall geeignetes Sicherheitsprofil.
- Verwenden eines VPN für die externe Konnektivität: Ziehen Sie ein IPsec-VPN in Betracht, um Punkt-zu-Punkt- oder Netzwerk-zu-Netzwerk-Verbindungen zu sichern und so den Datenschutz und die 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 in Amazon Redshift: Konfigurieren Sie Ihren Cluster so, dass eine Verbindung über Secure Socket Layer (SSL) or Transport Layer Security (TLS) vorgeschrieben ist.
- 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 Richtlinienkontrolle für Amazon S3-Buckets, um sicheren Zugriff auf Daten zu erzwingen.
- Erwägen der Verwendung von AWS Certificate Manager: ACM ermöglicht das Bereitstellen und Verwalten von öffentlichen TLS-Zertifikaten zur Verwendung mit AWS-Services.
- Erwägen der Verwendung von AWS Private Certificate Authority für private PKI-Anforderungen: AWS Private CA ermöglicht das Erstellen privater Zertifizierungsstellenhierarchien, um X.509-Endentitätszertifikate auszustellen, die zum Erstellen verschlüsselter TLS-Kanäle verwendet werden können.

Ressourcen

Zugehörige Dokumente:

- Dokumentation zu AWS
- Verwenden von HTTPS mit CloudFront
- Verbinden Ihrer VPC mit Remote-Netzwerken über AWS Virtual Private Network
- Create an HTTPS listener for your Application Load Balancer (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 Identität der Kommunikation mithilfe von Protokollen, die die Authentifizierung unterstützen, wie Transport Layer Security (TLS) oder IPsec.

Entwerfen Sie Ihren 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, bietet eine strengere Kontrolle über den Netzwerkfluss und reduziert die Auswirkungen von nicht autorisiertem Zugriff.

Gewünschtes Ergebnis: Ein Workload mit klar definierten Datenflüssen auf der Daten- und Steuerebene zwischen den Services. Die Datenflüsse verwenden authentifizierte und verschlüsselte Netzwerkprotokolle, sofern dies technisch möglich ist.

Typische Anti-Muster:

- Unverschlüsselte oder unauthentifizierte Datenflüsse innerhalb Ihres Workloads
- Wiederverwendung von Authentifizierungsdaten für mehrere Benutzer oder Entitäten
- Die alleinige Verwendung von Netzwerkkontrollen als Zugriffskontrolle
- Erstellen eines benutzerdefinierten Authentifizierungsmechanismus, anstatt sich auf die Standard-Authentifizierungsmechanismen der Branche zu verlassen
- Übermäßig freizügige Datenflüsse zwischen Servicekomponenten 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 Diensten, indem die vorgesehenen Schnittstellen für die Datenübertragung klar definiert und durchgesetzt werden
- Verbessert die Überwachung, Protokollierung und Reaktion auf Vorfälle durch die Zuordnung von Anfragen und gut 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 Netzwerkverkehrsmuster Ihres Workloads lassen sich in zwei Kategorien einteilen:

- Der Ost-West-Verkehr steht für Datenflüsse zwischen Services, die einen Workload ausmachen.
- Der Nord-Süd-Verkehr stellt die Datenflüsse zwischen Ihrem Workload und den Verbrauchern dar.

Während es üblich ist, den Nord-Süd-Verkehr zu verschlüsseln, ist die Sicherung des Ost-West-Verkehrs mit authentifizierten Protokollen weniger verbreitet. Moderne Sicherheitspraktiken empfehlen, 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 Anfrage 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, ob die Aktion erlaubt werden soll oder nicht.

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 auf der AWS-fremden Ressource verwenden, um temporäre AWS-Anmeldeinformationen zu erhalten. Diese Anmeldeinformationen können verwendet werden, um Anfragen an Services zu signieren, die mit SigV4 den Zugriff autorisieren.

Ein weiterer gängiger Mechanismus zur Authentifizierung des Ost-West-Verkehrs ist die gegenseitige TLS-Authentifizierung (mTLS). Viele Internet der Dinge (IoT)- 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 und AWS App Mesh verwenden, um die mTLS-Authentifizierung für die Kommunikation zwischen oder innerhalb eines Workloads bereitzustellen. Während mTLS Authentifizierungsinformationen für beide Seiten einer TLS-Kommunikation bereitstellt, bietet es keinen Mechanismus zur Autorisierung.

Nicht zuletzt sind OAuth 2.0 und OpenID Connect (OIDC) zwei Protokolle, die in der Regel für die Kontrolle des Zugriffs von Benutzern auf Services verwendet werden, jetzt aber auch für den Datenverkehr von Service zu Service immer beliebter werden. 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 Ihres Workloads: Der erste Schritt bei der Implementierung einer umfassenden Verteidigungsstrategie ist die Definition der Datenflüsse Ihres Workloads.
  - Erstellen Sie ein Datenflussdiagramm, das klar definiert, wie Daten zwischen den verschiedenen Services, aus denen Ihr Workload besteht, übertragen werden. Dieses Diagramm ist der erste Schritt zur Durchsetzung 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 in SEC01-BP07 Identifizierung von Bedrohungen und Priorisierung von Abhilfemaßnahmen unter Verwendung eines Bedrohungsmodells beschrieben.
- Einrichten von Netzwerkkontrollen: Erwägen Sie AWS-Funktionen, um Netzwerkkontrollen einzurichten, die auf Ihre Datenflüsse abgestimmt sind. Netzwerkgrenzen sollten zwar nicht die einzige Sicherheitskontrolle sein, aber sie stellen eine Stufe der umfassenden Verteidigungsstrategie zum Schutz Ihres Workloads dar.
  - Verwenden Sie Sicherheitsgruppen, um den Datenfluss zwischen Ressourcen zu definieren und einzuschränken.
  - Verwenden Sie AWS PrivateLink, um sowohl mit AWS als auch mit Drittanbieterservices 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 Ihrem Workload: Wählen Sie die AWS-Services aus, die am besten geeignet sind, um authentifizierte, verschlüsselte Datenflüsse in Ihrem Workload bereitzustellen.
  - Ziehen Sie Amazon VPC Lattice in Erwägung, um die Kommunikation von Service zu Service zu sichern. VPC Lattice kann SigV4-Authentifizierung in Kombination mit Authentifizierungsrichtlinien verwenden, um den Zugriff von Service zu Service zu kontrollieren.

  - Für die serviceübergreifende Kommunikation mit mTLS sollten Sie API Gateway oder App Mesh in Betracht ziehen. AWS Private CA kann verwendet werden, um eine private CA-Hierarchie einzurichten, die Zertifikate für die Verwendung mit mTLS ausstellen kann.
  - Bei der Integration mit Services, die OAuth 2.0 oder OIDC verwenden, sollten Sie API Gateway unter Verwendung des JWT-Genehmigers in Betracht ziehen.
  - Für die Kommunikation zwischen Ihrem Workload und IoT-Geräten sollten Sie AWS IoT Core in Betracht ziehen, das mehrere Optionen für die Verschlüsselung und Authentifizierung des Netzwerkverkehrs bietet.
- Überwachung auf nicht autorisierten Zugriff: Überwachen Sie kontinuierlich unbeabsichtigte Kommunikationskanäle, nicht autorisierte Auftraggeber, die versuchen, auf geschützte Ressourcen zuzugreifen, und andere unzulässige Zugriffsmuster.
  - Wenn Sie VPC Lattice zur Verwaltung des Zugriffs auf Ihre Services verwenden, sollten Sie die Zugriffsprotokolle von VPC Lattice aktivieren und überwachen. Diese Zugriffsprotokolle enthalten Informationen über die anfragende Entität, Netzwerkinformationen einschließlich Quell- und Ziel-VPC und Metadaten der Anfrage.
  - 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:

- Evaluating access control methods to secure Amazon API Gateway APIs
- Configuring mutual TLS authentication for a REST API
- How to secure API Gateway HTTP endpoints with JWT authorizer

- Authorizing direct calls to AWS services using AWS IoT Core credential provider
- AWS Security Incident Response Guide

Zugehörige Videos:

- AWS re:invent 2022: Introducing VPC Lattice
- AWS re:invent 2020: Serverless API authentication for HTTP APIs on AWS

Zugehörige Beispiele:

- Amazon VPC Lattice Workshop
- Zero-Trust Episode 1 – The Phantom Service Perimeter workshop

Vorfallsreaktion

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

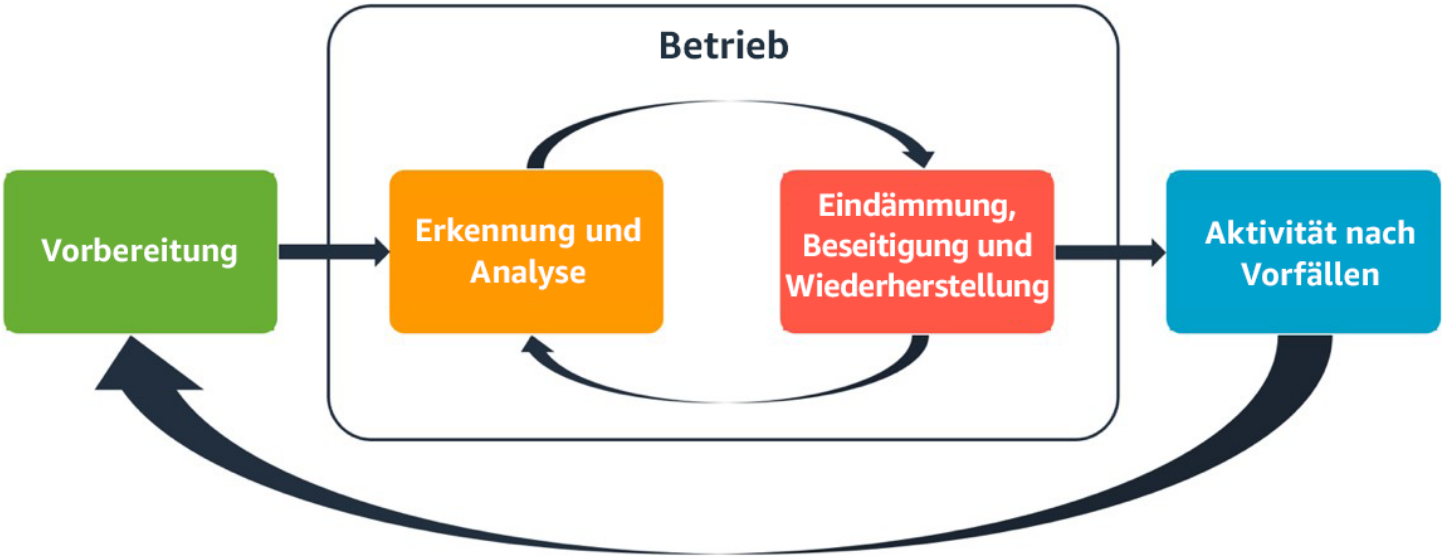
Alle AWS-Benutzer innerhalb eines Unternehmens sollten ein grundlegendes Verständnis der Prozesse zur Reaktion auf Sicherheitsvorfälle haben und das Sicherheitspersonal sollte wissen, wie auf Sicherheitsprobleme zu reagieren ist. Ausbildung, Schulung und Erfahrung sind für ein erfolgreiches Programm 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, Betriebund Aktivität nach Vorfällen.

Im Folgenden werden diese Aspekte genauer beschrieben:

- Vorbereitung: Bereiten Sie Ihr Vorfallsreaktionsteam 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 im NIST SP 800-61: Computer Security Incident Handling Guidedefiniert 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: Legen Sie in Zusammenarbeit mit den Beteiligten, dem Rechtsbeistand und der Unternehmensleitung das Ziel der Reaktion auf einen Vorfall fest. 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 Vorfallsreaktion 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 fehlerhafte Konfiguration zurückzuführen ist, kann die Abhilfe so einfach sein wie die Beseitigung der Abweichung durch die Neuverteilung von 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 Ihres Unternehmens 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:

- Mitarbeiter: Um Ihre Mitarbeiter auf einen Sicherheitsvorfall vorzubereiten, müssen Sie die für die Reaktion auf Vorfälle relevanten Personen identifizieren und sie in den Bereichen Vorfallsreaktion 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 Vorfallsreaktionsprogramm 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, die Ihre Organisation bei der Reaktion auf einen Vorfall unterstützen.

Gewünschtes Ergebnis: Sie haben eine Liste der wichtigsten Mitarbeiter, deren Kontaktinformationen und die Rollen, die sie bei der Reaktion auf ein Sicherheitsereignis spielen. 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 Sicherheitspartner, Cloud-Anbieter 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 sich zu erholen.

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 Menschen, Abhängigkeiten, Infrastruktur und Lösungen bei der Reaktion auf ein Ereignis und bei der Wiederherstellung nach einem Ereignis versteht
- Fehlen eines Dokuments oder eines Wissensspeichers, der die wichtigsten Infrastruktur- oder Anwendungsdesigns darstellt
- Fehlen von angemessenen Einarbeitungsprozessen für neue Mitarbeiter, um effektiv zur Reaktion auf ein Sicherheitsereignis beizutragen, wie z. B. die Durchführung von Ereignissimulationen
- Fehlen eines Eskalationspfades für den Fall, dass wichtige Mitarbeiter vorübergehend nicht verfügbar sind oder bei Sicherheitsereignissen nicht reagieren können

Vorteile der Einführung 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 Wiederherstellung nach einem Ereignis 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.
- 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.

Benutzen Sie die Funktion 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 den Workload auf alle Eigentümer verteilt wird. Dies fördert gute Praktiken wie die Ausgabe relevanter Metriken und Protokolle sowie die Definition von Alarmschwellen, die für den Workload von Bedeutung sind.

Externe Partner identifizieren: Unternehmen nutzen Tools, die von unabhängigen Softwareanbietern (ISVs), Partnern und Subunternehmern entwickelt wurden, um differenzierte Lösungen für ihre Kunden zu erstellen. Engagieren Sie wichtige Mitarbeiter dieser Parteien, die Ihnen bei der Reaktion auf einen Vorfall und bei dessen Bewältigung helfen können. Wir empfehlen Ihnen, sich für die entsprechende Stufe von AWS 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. 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 für die Benachrichtigung externer Stellen zuständig sein könnten, auch wenn diese nicht direkt an der Lösung des Vorfalls beteiligt sind.

Ressourcen

Zugehörige bewährte Methoden:

- OPS02-BP03 Betriebsaktivitäten haben feste Eigentümer, die für ihre Leistung verantwortlich sind

Zugehörige Dokumente:

- AWS-Leitfaden für Security Incident Response

Zugehörige Beispiele:

- AWS Customer Playbook Framework
- Prepare for and respond to security incidents in your AWS environment

Zugehörige Tools:

- AWS Systems Manager Incident Manager

Zugehörige Videos:

- Amazon's approach to security during development

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 gründlicher 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 bestehende Prozesse zur Vorfallreaktion. Unabhängig von Ihrem aktuellen Status ist es wichtig, Ihre Prozesse zur Vorfallreaktion regelmäßig zu aktualisieren, zu wiederholen und zu testen.

Risikostufe bei fehlender Befolgung dieser Best Practice: Hoch

Implementierungsleitfaden

Ein Vorfallreaktionsplan 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 zeitgerechte Reaktion darauf.

In der Cloud gibt es viele der betrieblichen Rollen und Anforderungen, die auch für eine On-Premises-Umgebung typisch sind. Bei der Erstellung eines Vorfallmanagementplans ist es wichtig, Reaktions- und Wiederherstellungsstrategien zu berücksichtigen, die optimal zu Ihren Anforderungen an geschäftliche Ergebnisse und Compliance passen. Wenn Sie beispielsweise Workloads in AWS bearbeiten, die mit FedRAMP in den USA kompatibel sind, sollten Sie den NIST SP 800-61 Computer Security Handling Guide berücksichtigen. Ähnlich gilt beim Betrieb von Workloads mit persönlich identifizierbaren Informationen (PII) in Europa, dass Sie an Szenarien denken sollten, in denen Sie diese schützen und auf Probleme reagieren müssen, die im Zusammenhang mit den Bestimmungen zu Datenspeicherorten der Regulierungen der Datenschutz-Grundverordnung (DSGVO) der EU stehen.

Wenn Sie einen Vorfallmanagementplan für Ihre Workloads in AWS erstellen, beginnen Sie mit dem AWS-Modell der geteilten Verantwortung zum Aufbau eines gründlichen Verteidigungskonzepts im Rahmen Ihrer Vorfallreaktionen. In diesem Modell kümmert sich AWS um die Sicherheit der Cloud und Sie sind für die Sicherheit in der Cloud verantwortlich. Dies 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 cloudbasierten Vorfallmanagementplans.

Ein effektiver Vorfallmanagementplan muss kontinuierlich iteriert 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

Definieren von Rollen und Zuständigkeiten

Der Umgang mit Sicherheitsereignissen erfordert organisationsübergreifende Disziplin und Handlungsbereitschaft. Innerhalb Ihrer Organisationsstruktur sollte es viele Personen geben, die für einen Vorfall verantwortlich, rechenschaftspflichtig, konsultiert oder auf dem Laufenden gehalten werden, z. B. Vertreter der Personalabteilung (HR), des Führungsteams und der Rechtsabteilung. Berücksichtigen Sie diese Rollen und Verantwortlichkeiten und ob Dritte beteiligt sein müssen. Beachten Sie, dass in vielen Regionen lokale Gesetze gelten, die regeln, was getan werden sollte und was nicht. Auch wenn es bürokratisch erscheinen mag, ein Diagramm für Verantwortung, Rechenschaftspflicht, Berater und zu Informierende (RACI) für Ihre Sicherheitspläne zu erstellen, erleichtert dies eine schnelle und direkte Kommunikation und gibt einen klaren Überblick über die Führungskräfte in den verschiedenen Phasen des Ereignisses.

Bei einem Vorfall ist es von entscheidender Bedeutung, die Eigentümer und Entwickler der betroffenen Anwendungen und Ressourcen einzubeziehen, da es sich um Fachexperten (SMEs) handelt, die Informationen und Zusammenhänge bereitstellen können, um die Auswirkungen zu messen. Üben Sie und bauen Sie Beziehungen zu den Entwicklern und Anwendungsbesitzern auf, bevor Sie sich bei der Vorfallreaktion auf deren Fachwissen verlassen. Anwendungsinhaber oder SMEs, wie Ihre Cloud-Administratoren oder Techniker, müssen möglicherweise in Situationen handeln, in denen die Umgebung nicht vertraut oder komplex ist oder in denen die Handelnden keinen Zugriff haben.

Schließlich könnten vertrauenswürdige Partner in die Untersuchung oder Reaktion einbezogen werden, da sie zusätzliches Fachwissen und wertvolle Einblicke bereitstellen können. Wenn Sie in Ihrem eigenen Team nicht über diese Fähigkeiten verfügen, sollten Sie eine externe Partei mit der Unterstützung beauftragen.

Die AWS-Reaktionsteams und der Support

- AWS Support
  - AWS Support bietet eine Reihe von Tarifen, die den Zugriff auf Tools und Fachwissen ermöglichen, um den Erfolg und die Betriebssicherheit Ihrer AWS-Lösungen zu unterstützen. 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 Management Console (Anmeldung erforderlich) ist Ihre zentrale Anlaufstelle, um Unterstützung bei Problemen zu erhalten, die sich auf Ihre AWS-Ressourcen auswirken. Der Zugriff auf den AWS Support wird über AWS Identity and Access Management gesteuert. Weitere Informationen zum Zugriff auf AWS Support-Funktionen finden Sie unter Erste Schritte mit AWS 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.
  - Wenn das AWS-CIRT Sie unterstützt, bietet es Hilfe bei der Fehlererkennung und Wiederherstellung eines aktiven Sicherheitsereignisses auf AWS an. Sie können mithilfe von AWS-Serviceprotokollen 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 AWS Support-Fall.
- Unterstützung für DDoS-Response
  - AWS bietet AWS Shield, das einen verwalteten Distributed Denial of Service (DDoS)-Schutzservice bereitstellt, der laufende Webanwendungen auf AWS 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 AWS Support kontaktieren, um vom DDoS-Schutz zu profitieren. Es gibt zwei Stufen von Shield: AWS Shield Standard und AWS Shield Advanced. Weitere Informationen zu den Unterschieden zwischen diesen beiden Stufen finden Sie unter 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 Warnmeldungen an. Wenn eine Warnung ausgelöst wird, befolgt AMS eine Reihe automatisierter und manueller Standard-Playbooks, um sicherzustellen, dass eine konsistente Reaktion gewährleistet ist. Diese Playbooks werden den AMS-Kunden während des Onboardings zur Verfügung gestellt, damit sie eine Antwort 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:

- Ein Überblick über das Vorfallreaktionsteam: Er enthält die Ziele und Funktionen des Vorfallreaktionsteams.
- Rollen und Zuständigkeiten: Hier sind die für die Vorfallreaktion zuständigen Interessenvertreter aufgeführt und ihre Rollen im Falle eines Vorfalls werden beschrieben.
- Ein Kommunikationsplan: Dieser enthält Kontaktinformationen und gibt an, wie Sie während eines Vorfalls kommunizieren.
- Alternative Kommunikationsmethoden: Es hat sich bewährt, Out-of-Band-Kommunikation als Backup 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 (z. B. 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 jedes Unternehmen einzigartig. Sie müssen einen Vorfallreaktionsplan erstellen, der für Ihr Unternehmen am besten geeignet ist.

Ressourcen

Zugehörige bewährte Methoden:

- SEC04 (Wie erkenne und untersuche ich Sicherheitsereignisse?)

Zugehörige Dokumente:

- Leitfaden für AWS Security Incident Response
- NIST: Computer Security Incident Handling Guide

SEC10-BP03 Vorbereiten forensischer Funktionen

Im Vorfeld eines Sicherheitsvorfalls sollten Sie erwägen, forensische Funktionen zur Unterstützung der Untersuchung von Sicherheitsereignissen zu entwickeln.

Risikostufe bei fehlender Befolgung dieser Best Practice: Mittel

Konzepte aus der traditionellen On-Premises-Forensik gelten für AWS. Wichtige Informationen für den Einstieg in den Aufbau forensischer Funktionen finden Sie AWS Cloud in den Strategien für forensische Untersuchungsumgebungen in der AWS Cloud.

Sobald Sie Ihre Umgebung und AWS-Konto-Struktur für die Forensik eingerichtet haben, definieren Sie die Technologien, die für die effektive Durchführung 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 daraus Schlüsse 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. Sie können Organisationseinheiten (OEs) verwenden, um Konten zu gruppieren und als eine einzige Einheit zu verwalten.

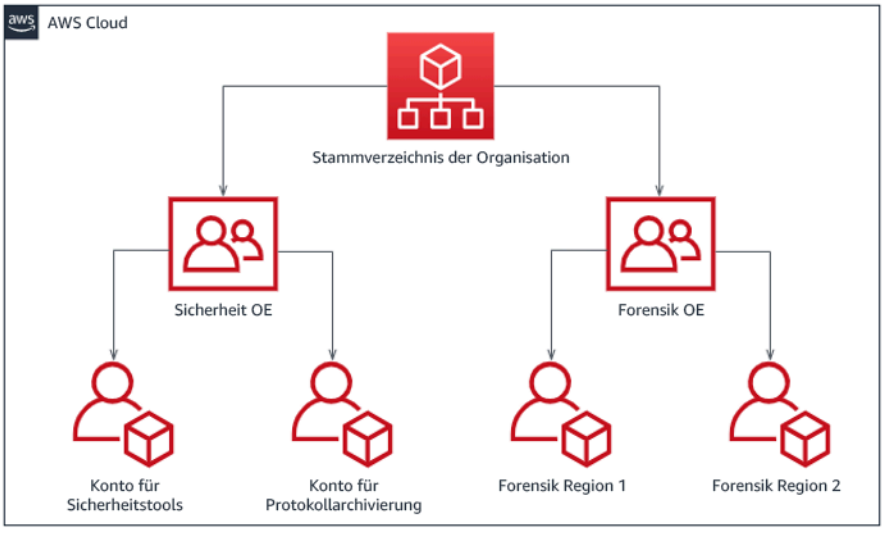
Für die Reaktion auf Vorfälle ist es hilfreich, eine AWS-Konto-Struktur zu haben, die die Funktionen der Vorfallsreaktion unterstützt. Dazu gehören eine Sicherheits-OE und eine Forensik-OE. Innerhalb der Sicherheits-OE sollten Sie Konten für Folgendes haben:

- Archivierung des Protokolls: Aggregieren Sie Protokolle in einem AWS-Konto für Protokollarchivierung mit eingeschränkten Berechtigungen.
- Sicherheitstools: Zentralisieren Sie Sicherheitsservices in einem AWS-Konto für Sicherheitstools. Dieses Konto fungiert als delegierter Administrator für Sicherheitsservices.

Innerhalb der Forensik-OE haben Sie die Möglichkeit, für jede Region, in der Sie tätig sind, ein oder mehrere forensische Konten zu implementieren, je nachdem, welche 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 US East (N. Virginia) Region (`us-east-1`) und US West (Oregon) (`us-west-2`) arbeiten, hätten Sie zwei Konten in der forensischen Organisationseinheit: eine für `us-east-1` und eine für `us-west-2`.

Sie können ein forensisches AWS-Konto für mehrere Regionen erstellen. Sie sollten beim Kopieren von AWS-Ressourcen auf dieses Konto Vorsicht walten lassen, um sicherzustellen, dass Sie Ihre Anforderungen an die Datensouveränität einhalten. Da die Bereitstellung neuer Konten einige Zeit in Anspruch nimmt, ist es unerlässlich, die forensischen Konten rechtzeitig vor einem Vorfall einzurichten und zu instrumentieren, damit die Notfallteams darauf vorbereitet sind, sie effektiv für die Reaktion zu nutzen.

Das folgende Diagramm zeigt eine Beispiel-Kontenstruktur mit einer Forensik-OE mit regionalen forensischen Konten:



Regionale Kontenstruktur für die Vorfallsreaktion

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 in ihren vorherigen sicheren Zustand zurückversetzen. 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 und 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 zur Sicherung Ihrer Backups finden Sie in den 10 besten Sicherheitsmethoden für die Sicherung von Backups in AWS. Zusätzlich zur Sicherung 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 Vorfallsreaktionsteam in der Lage sein, schnell Nachweise zu sammeln und zu analysieren und gleichzeitig die Genauigkeit für den Zeitraum rund um das Ereignis aufrechtzuerhalten (z. B. das Erfassen von Protokollen zu einem bestimmten Ereignis oder einer bestimmten Ressource oder das Erfassen von Speicherabbildern einer Amazon EC2-Instance). Für das Vorfallsreaktionsteam ist es sowohl schwierig als auch zeitaufwändig, die relevanten Beweise manuell zu erfassen, insbesondere bei einer großen Anzahl von Instances und Konten. Darüber hinaus kann die manuelle Erfassung anfällig für menschliche Fehler sein. Aus diesen Gründen sollten Sie die Automatisierung für die Forensik so weit wie möglich entwickeln und implementieren.

AWS bietet eine Reihe von Automatisierungsressourcen für die Forensik, die im Abschnitt Ressourcen unten aufgeführt sind. Diese Ressourcen sind Beispiele für forensische Muster, die wir entwickelt und Kunden implementiert haben. 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:

- AWS-Sicherheits- und Vorfallsreaktionsanleitung – Forensische Funktionen entwickeln
- AWS-Sicherheits- und Vorfallsreaktionsanleitung – Forensische Ressourcen
- Strategien für forensische Untersuchungsumgebungen in der AWS Cloud
- Automatisieren der forensischen Datenträgererfassung in AWS
- Präskriptive AWS-Anleitung – Automatisieren der Vorfallsreaktion und Forensik

Zugehörige Videos:

- Automating Incident Response and Forensics

Zugehörige Beispiele:

- Framework für automatisierte Vorfallsreaktion und 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 Vorfallsreaktion ist die Entwicklung von Playbooks. Playbooks für die Vorfallsreaktion enthalten eine Reihe von präskriptiven Anleitungen und Schritten, die Sie befolgen müssen, wenn ein Sicherheitsereignis eintritt. Eine klare Struktur und klare Schritte vereinfachen die Reaktion und verringern die Wahrscheinlichkeit menschlicher Fehler.

Risikostufe bei fehlender Befolgung dieser Best Practice: Mittel

Implementierungsleitfaden

Playbooks sollten für Vorfallsszenarien 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 Ihre bekannten Sicherheitserkenntnisse und Warnmeldungen wie GuardDuty-Ergebnisse erstellen. Möglicherweise erhalten Sie eine GuardDuty-Erkenntnis und denken: „Wie geht es weiter?“ Um zu verhindern, dass eine GuardDuty-Erkenntnis unsachgemäß gehandhabt oder ignoriert wird, sollten Sie für jede

potenzielle GuardDuty-Erkenntnis ein Playbook erstellen. Einige Einzelheiten und Anleitungen zur Mängelbeseitigung finden Sie in der GuardDuty-Dokumentation. Es ist erwähnenswert, dass GuardDuty standardmäßig nicht aktiviert ist und dafür Kosten anfallen. Weitere Informationen finden GuardDuty Sie in Anhang A: Definitionen der Cloud-Funktionen –Sichtbarkeit und Warnmeldungen.

Playbooks sollten technische Schritte enthalten, die ein Sicherheitsanalyst ausführen muss, um einen potenziellen Sicherheitsvorfall angemessen zu untersuchen und darauf zu reagieren.

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 ihre Kontaktinformationen? Welche Verantwortlichkeiten haben die einzelnen Interessenvertreter?
- Reaktionsschritte: Welche taktischen Maßnahmen sollten in allen Phasen der Vorfallsreaktion 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 Vorfallsreaktion
- Entwickeln eigener Playbooks für die Vorfallsreaktion
- Beispiele von Playbooks für die Vorfallsreaktion
- Entwicklung eines Runbooks für die Vorfallsreaktion 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:

- Verwenden des Root-Kontos für die Reaktion auf Vorfälle
- Verändern bestehender Benutzerkonten
- Direkte Manipulation von IAM-Berechtigungen bei Bereitstellung von Just-in-time-Berechtigungserhöhungen

Risikostufe, wenn diese bewährte Methode nicht genutzt wird: Mittel

Implementierungsleitfaden

AWS empfiehlt die Reduzierung oder Ausschaltung der Abhängigkeit von langlebigen Anmeldeinformationen wenn möglich und ihren Ersatz durch Just-in-Time-Berechtigungseskalationsmechanismen. Langlebige Anmeldeinformationen sind anfällig für Sicherheitsrisiken und erhöhen den Verwaltungsaufwand. Für die meisten Managementaufgaben sowie für Vorfallreaktionsaufgaben empfehlen wir die Implementierung eines Identitätsverbunds neben der temporären Eskalierung für den administrativen Zugriff. In diesem Modell beantragt ein Benutzer seine Erhöhung auf eine höhere Berechtigungsstufe (etwa zu einer Vorfallreaktionsrolle). Anschließend wird, sofern der Benutzer grundsätzlich dafür infrage kommt, eine Anfrage an einen Genehmiger gesendet. Wenn die Anfrage genehmigt wurde, erhält der Benutzer einen Satz temporärer AWS-Anmeldeinformationen für die Durchführung seiner Aufgaben. Wenn diese Anmeldeinformationen ablaufen, muss der Benutzer eine neue Erhöhungsanfrage stellen.

Wir empfehlen für die meisten Vorfallreaktionsszenarien die Verwendung temporärer Berechtigungseskalierungen. Die korrekte Vorgehensweise ist die Verwendung von AWS Security Token Service und von Sitzungsrichtlinien zur Festlegung der Zugriffsbereiche.

Es gibt Szenarien, in denen Verbundidentitäten nicht verfügbar sind, zum Beispiel:

- Ausfall durch Problem mit einem Identitätsanbieter (IdP)
- Fehlerhafte Konfiguration oder menschlicher Fehler, die/der das Managementsystem für den Verbundzugriff beschädigt
- Böswillige Aktivität, z. B. ein DDoS-Angriff (Distributed Denial of Service) oder anderweitig verursachte Nichtverfügbarkeit des Systems

Für diese Fälle sollte Notfall- „Break Glass“- Zugriff konfiguriert werden, um Untersuchungen und die schnelle Behebung des Vorfalls zu ermöglichen. Wir empfehlen die Verwendung eines IAM-Benutzers mit ausreichenden Berechtigungen für die Durchführung von Aufgaben und den Zugriff auf AWS-Ressourcen. Verwenden Sie die Root-Anmeldeinformationen nur für Aufgaben, die Root-Benutzerzugriff erfordern. Zur Prüfung, ob die Vorfallreaktionskräfte über die korrekte Zugriffsstufe auf AWS und andere relevante Systeme verfügen, empfehlen wir die Bereitstellung dedizierter Benutzerkonten. Die Benutzerkonten erfordern privilegierten Zugriff und müssen eng 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 Teil des Vorfallmanagementplans sind.

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 es unklar, welche Zugriffsmöglichkeiten Benutzer während eines Vorfalls hatten, und birgt die Gefahr, dass die eskalierten Berechtigungen später nicht widerrufen werden.

Es ist wichtig, so viele Abhängigkeiten wie möglich zu entfernen, um sicherzustellen, dass Zugriff bei einer möglichst großen Anzahl von Ausfallszenarien möglich ist. Erstellen Sie deshalb ein Playbook, um sicherzustellen, dass Vorfallreaktionsbenutzer als AWS Identity and Access Management-Benutzer in einem dedizierten Sicherheitskonto erstellt und nicht durch einen vorhandenen Verbund oder eine Single Sign-On (SSO)-Lösung verwaltet werden. Alle einzelnen Reaktionskräfte müssen ein eigenes benanntes Konto haben. Die Kontokonfiguration muss eine Richtlinie für sichere Passwörter und Multi-Faktor-Authentifizierung (MFA) durchsetzen. Wenn die Playbooks zur Vorfallreaktion nur Zugriff auf die AWS Management Console benötigen, sollten für den Benutzer keine Zugriffsschlüssel konfiguriert werden und er sollte auch explizit keine Zugriffsschlüssel erstellen

dürfen. Dies kann mit IAM-Richtlinien oder Service-Kontrollrichtlinien (SCPs) konfiguriert werden, wie in den bewährten AWS-Sicherheitsmethoden für AWS Organizations SCPs erläutert. Die Benutzer sollten keine Berechtigungen außer der Möglichkeit zur Übernahme von Vorfallreaktionsrollen in anderen Konten haben.

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.

Zur Sicherstellung, dass die Verwendung von Vorfallreaktionsrollen in korrekter Weise überwacht und geprüft werden kann, ist es entscheidend, dass die für diesen Zweck erstellten IAM-Benutzerkonten nicht zwischen Personen weitergegeben werden und dass der AWS-Konto-Root-Benutzer nicht verwendet wird, sofern dies nicht für eine bestimmte Aufgabe erforderlich ist. Wenn der Root-Benutzer erforderlich ist (zum Beispiel wenn der IAM-Zugriff auf ein bestimmtes Konto nicht verfügbar ist), verwenden Sie einen separaten Prozess mit einem Playbook, um die Verfügbarkeit des Root-Benutzer-Passworts und des MFA-Tokens zu prüfen.

Erwägen Sie zur Konfiguration der IAM-Richtlinien für die Vorfallreaktionsrollen die Verwendung von IAM Access Analyzer zum Erstellen von Richtlinien auf der Grundlage von AWS CloudTrail-Protokollen. Gewähren Sie dazu der Vorfallreaktionsrolle in einem Nicht-Produktionskonto Administratorzugriff und durchlaufen Sie das Playbook. Sobald dies geschehen ist, kann eine Richtlinie erstellt werden, die nur die entsprechenden 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 Vorfallreaktionsbenutzerkonten zur Annahme dedizierter Vorfallreaktions-IAM-Rollen in anderen AWS-Konten. 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 kontrollieren. Stellen Sie sicher, dass alle `AssumeRole-` Anfragen 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-Benutzerkonten und die IAM-Rollen deutlich zu benennen, damit sie in CloudTrail-Protokollen leicht zu finden sind. Ein Beispiel ist die Benennung der IAM-Konten als *<USER_ID>*-BREAK-GLASS und der IAM-Rollen als BREAK-GLASS-ROLE.

CloudTrail wird verwendet, um API-Aktivitäten in Ihren AWS-Konten zu protokollieren, und sollte zur Konfiguration von Alarmen zur Nutzung der Vorfallreaktionsrollen eingesetzt werden. Weitere Informationen finden Sie im Blog-Beitrag zur Konfiguration von Alarmen bei Verwendung von Root-Schlüsseln. Die Anweisungen können können geändert werden, um die Metrik Amazon CloudWatch so zu konfigurieren, dass sie nach `AssumeRole-` Ereignissen gefiltert wird, die mit der Vorfallreaktions-IAM-Rolle 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 Alarme an eine breite Gruppe gehen und dass sofort darauf reagiert wird.

Während eines Vorfalls kann es geschehen, dass eine Reaktionskraft Zugriff auf Systeme benötigt, die nicht direkt von IAM gesichert sind. Dazu können Amazon Elastic Compute Cloud-Instances, Amazon Relational Database Service-Datenbanken oder 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) kontrolliert werden. Es kann auch möglich sein, Teile Ihrer Playbooks mit AWS Systems Manager-Run-Command-Dokumentenzu automatisieren, wodurch sich möglicherweise Benutzerfehler reduzieren und Wiederherstellungszeiten verkürzen lassen. Für den Zugriff auf Datenbanken und Tools von Drittanbietern empfehlen wir die Speicherung von Anmeldeinformationen in AWS Secrets Manager und die Gewährung des Zugriffs auf die Vorfallreaktionsrollen.

Schließlich sollte die Verwaltung der Vorfallreaktions-IAM-Benutzerkonten 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 für AWS Security Incident Response
- 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-Servicekontrollrichtlinien in einer Mehrkontenumgebung
- Empfang von Benachrichtigungen, wenn die Root-Zugriffsschlüssel Ihres AWS-Kontos verwendet werden
- Erstellen detaillierter Sitzungsberechtigungen mithilfe von IAM-verwalteten Richtlinien

Zugehörige Videos:

- Automating Incident Response and ForensicsAWS (Automatisieren der Vorfallreaktion und Forensik in AWS)
- DIY guide to runbooks, incident reports, and incident response (DIY-Leitfaden für Runbooks, Vorfallberichte und Vorfallreaktion)
- Prepare for and respond to security incidents in your AWS environment (Vorbereiten und Reagieren auf Sicherheitsvorfälle in Ihrer AWS-Umgebung)

Zugehörige Beispiele:

- Übung: AWS-Kontoeinrichtung und Root-Benutzer
- Übung: Vorfallreaktion mit AWS-Konsole und CLI

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 bei fehlender Befolgung dieser Best Practice: Mittel

Implementierungsleitfaden

Zur Automatisierung von Sicherheitsreaktionen und Betriebsfunktionen können Sie eine umfassende Palette von APIs und Tools von AWS verwenden. Sie können die Identitätsverwaltung, Netzwerksicherheit, Datenschutz und Überwachungsfunktionen vollständig automatisieren und diese mithilfe gängiger Softwareentwicklungsmethoden bereitstellen, die Sie bereits eingerichtet haben. Wenn Sie die Sicherheitsautomatisierung erstellen, kann Ihr System eine Reaktion überwachen, prüfen und initiieren, statt nur Ihre Sicherheitslage zu überwachen und manuell auf Ereignisse zu reagieren.

Wenn Ihre Vorfallreaktionsteams auf Warnungen weiterhin auf die gleiche Weise reagieren, riskieren sie eine Abstumpfung der Warnung. 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 von Warnungen zu vermeiden, indem Funktionen verwendet werden, die sich wiederholende und gewöhnliche Warnungen verarbeiten, sodass Mitarbeiter die nötigen freien Kapazitäten haben, um sich um sensible und einzigartige 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 schwellenwertbasierte Warnmeldungen verursachten Aufwand reduzieren.

Sie können manuelle Prozesse verbessern, indem Sie die Schritte im Prozess 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 verarbeiten.

Bei einer Sicherheitsuntersuchung 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- und Abrufmechanismen auszuwählen, zu aktivieren, zu speichern und einzurichten sowie die Alarmierung einzurichten. Darüber hinaus besteht eine effektive Möglichkeit zur Nutzung von Tools zum Durchsuchen von Protokolldaten in Amazon Detective.

AWS bietet über 200 Cloud-Services und Tausende von Funktionen. Wir empfehlen Ihnen, die Services zu konsultieren, die Ihre Strategie zur Vorfallsreaktion unterstützen und vereinfachen können.

Zusätzlich zur Protokollierung sollten Sie eine Markierungsstrategie entwickeln und implementieren. Die Markierung kann dabei helfen, einen Kontext zum 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 Vorfallsreaktion:

- Protokollierungsstrategien für die Reaktion auf Sicherheitsvorfälle
- SEC04-BP01 Konfigurieren der Service- und Anwendungsprotokollierung

Aktivieren von Sicherheitsservices zur Unterstützung von Erkennung und Reaktion

AWS bietet native Erkennungs-, Präventions- und Reaktionsfunktionen, und andere Services können für den Aufbau benutzerdefinierter Sicherheitslösungen verwendet werden. Eine Liste der wichtigsten Services für die Reaktion auf Sicherheitsvorfälle finden Sie unter Definitionen der Cloud-Funktionen.

Entwickeln und Implementieren einer Markierungsstrategie

Es kann schwierig sein, kontextbezogene Informationen zum geschäftlichen Anwendungsfall und zu relevanten internen Interessenvertretern rund um eine AWS-Ressource zu erhalten. Eine Möglichkeit, dies zu tun, 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 die Reaktionszeiten verkürzen 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. Danach implementieren Sie diese Markierungsstrategie und setzen sie durch. Weitere Einzelheiten zur Umsetzung und Durchsetzung 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
- Cloud-Capability-Definitionen für die Vorfallsreaktion

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

Ebenso wie Unternehmen im Laufe der Zeit wachsen und sich weiterentwickeln, wächst auch 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 (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
- Die 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: Der Tabletop-Ansatz für Simulationen besteht aus einer Diskussionsrunde, in der die verschiedenen Interessenvertreter des Bereichs Vorfallreaktion teilnehmen, um Rollen und Verantwortlichkeiten zu üben und etablierte Kommunikationstools und Playbooks zu verwenden. Die Übung kann in der Regel an einem ganzen Tag an einem virtuellen Ort, einem physischen Veranstaltungsort oder einer Kombination daraus 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 praktischen Übung.
- Lila Teamübungen: Lila Teamübungen 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 Interessenvertreter einbeziehen, die an einem tatsächlichen Cybereereignis beteiligt wären. Das rote Team besteht aus einem Penetrationstest-Team oder wichtigen Interessenvertretern, die in offensiver Sicherheit trainiert sind. Das rote Team arbeitet bei der Planung eines Szenarios mit den Übungsleitern zusammen, damit das Szenario korrekt und durchführbar ist. Bei den lila Teamübungen liegt das Hauptaugenmerk auf den Erkennungsmechanismen, den Tools und den Standard-Betriebsabläufen (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 Umfang 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 mit weniger komplexen Simulationstypen beginnen (z. B. mit Tabletop-Übungen) und zu komplexeren Simulationstypen übergehen (Übungen des roten Teams). Wählen Sie einen Simulationstyp anhand Ihres Sicherheitsgrads, Ihrer Ressourcen und der gewünschten Ergebnisse 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 den Führungskräften akzeptiert werden.
2. Identifizieren Sie die wichtigsten Interessenvertreter: Für eine Übung sind mindestens Übungsleiter und Teilnehmer erforderlich. Je nach Szenario können weitere Interessengruppen wie Recht, Kommunikation oder Geschäftsleitung einbezogen werden.
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 Moderationstaktiken 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, die gut gelaufen sind, diejenigen, die verbessert werden können, und potenzielle Lücken. Der AAR sollte die Effektivität der Simulation sowie die Reaktion des Teams auf das simulierte Ereignis messen, damit der Fortschritt mit zukünftigen Simulationen im Laufe der Zeit verfolgt werden kann.

Ressourcen

Zugehörige Dokumente:

- AWS Incident Response Guide

Zugehörige Videos:

- AWS GameDay – Sicherheitsausgabe

Betrieb

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, Beseitigungund 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 Beurteilung des Umfangs des Vorfalls.
Eindämmung	Minimieren und Beschränken des Umfangs des Sicherheitsereignisses.
Beseitigung	Entfernen nicht autorisierter Ressourcen oder Artefakte im Zusammenhang mit dem Sicherhei tsereignis. Implementieren von Abhilfema ßnahmen 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 Information finden Sie im Abschnitt Betrieb des Leitfadens für AWS Security Incident Response.

Aktivität nach Vorfällen

Die Bedrohungslage ändert sich ständig, und es ist wichtig, dass Ihr Unternehmen 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 Ihr Unternehmen 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 für Erkenntnisse und der Fähigkeit zur Ursachenanalyse trägt nicht nur dazu bei, die Reaktionsfähigkeit auf Vorfälle zu verbessern, sondern auch zu verhindern, dass sich der Vorfall wiederholt. Indem Sie aus jedem Vorfall lernen, können Sie verhindern, dass dieselben Fehler, Risiken oder Fehlkonfigurationen wiederholt werden. Dies verbessert nicht nur Ihre Sicherheitslage, sondern minimiert auch den Zeitverlust durch vermeidbare Situationen.

Risikostufe bei fehlender Befolgung dieser Best Practice: Mittel

Implementierungsleitfaden

Die Implementierung eines Erkenntnis-Frameworks ist wichtig, der die folgenden Punkte allgemein festlegt und erreicht:

- Wann finden Erkenntnisse statt?

- Was beinhaltet der Erkenntnisprozess?
- Wie werden Erkenntnisse durchgeführt?
- Wer ist am Prozess beteiligt und wie?
- 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. Beachten 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?
- Welche Systeme haben über die Aktivität alarmiert?
- 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:
  - Mitarbeiter
    - Waren die Mitarbeiter, die kontaktiert werden mussten, tatsächlich verfügbar und war die Kontaktliste auf dem neuesten Stand?
    - Fehlten den Mitarbeitern Trainings 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?
    - Wurden Prozesse und Verfahren für diese(n) (Art von) Vorfall dokumentiert und waren sie dafür verfügbar?
    - Fehlten die erforderlichen 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 werden oder müssen neue Warnungen für diese(n) (Art von) Vorfall erstellt werden?
    - Ermöglichten die vorhandenen Tools eine effektive Untersuchung (Suche/Analyse) des Vorfalls?
    - Was kann getan werden, um diese(n) (Art von) Vorfall früher zu erkennen?
    - Was kann getan werden, um zu verhindern, dass sich diese(r) (Art von) Vorfall wiederholt?
    - Wem gehört der Verbesserungsplan und wie testen Sie, ob er umgesetzt wurde?
    - Wie sieht der Zeitplan für die Implementierung und das Testen zusätzlicher Überwachungs- oder präventiver Kontrollen und Prozesse aus?

Diese Liste ist nicht vollständig, soll aber 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 es, zunächst die Erkenntnisse als Standardbestandteil Ihres Prozesses zur Vorfallsreaktion, der Dokumentation und der Erwartungen der Interessenvertreter zu berücksichtigen.

Ressourcen

Zugehörige Dokumente:

- AWS-Sicherheits- und Vorfallreaktionsanleitung – Entwickeln eines Frameworks, um aus Vorfällen zu lernen
- NCSC-CAF-Leitfaden – Erkenntnisse

Anwendungssicherheit

Anwendungssicherheit (Application security, AppSec) beschreibt den gesamten Prozess des Designens, Entwickelns und Testens der Sicherheitseigenschaften von Workloads, die Sie entwickeln. Sie sollten die Menschen in Ihrem Unternehmen entsprechend geschult haben, die Sicherheitseigenschaften Ihres Builds und der Infrastruktur Ihrer Softwareveröffentlichung verstehen sowie 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.

Diese Implementierungsrichtlinien konzentrieren sich auf vier Bereiche: Organisation und Kultur, Sicherheit der Pipeline, Sicherheit in der Pipeline und Abhängigkeitsverwaltung. 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.

Bewährte Methoden

- SEC11-BP01 Für Anwendungssicherheit schulen
- SEC11-BP02 Das Testen während des Entwicklungs- und Veröffentlichungslebenszyklus automatisieren
- SEC11-BP03 Regelmäßig Penetrationstests durchführen
- SEC11-BP04 Manuelle Codeüberprüfungen
- SEC11-BP05 Services für Pakete und Abhängigkeiten zentralisieren
- SEC11-BP06 Software programmgesteuert bereitstellen
- 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

Bieten Sie den Entwicklern in Ihrer Organisation Schulungsmöglichkeiten zu allgemeinen Praktiken für die sichere Entwicklung und den sicheren Betrieb von Anwendungen. Die Einführung sicherheitsbezogener Entwicklungsmethoden hilft, die Wahrscheinlichkeit von Problemen zu verringern, die nur während der Phase der Sicherheitsüberprüfung erkannt werden.

Gewünschtes Ergebnis: Beim Entwerfen und Entwickeln von Software sollte Sicherheit berücksichtigt werden. Wenn Entwickler in einer Organisation hinsichtlich sicherer Entwicklungspraktiken, die mit einem Bedrohungsmodell beginnen, geschult sind, wird die gesamte Qualität und Sicherheit der entwickelten Software verbessert. Mithilfe dieses Ansatzes kann die Zeit bis zum Ausliefern von Software oder Funktionen verringert werden, da der Überarbeitungsaufwand nach Sicherheitsüberprüfungen kleiner ist.

Für den Zweck dieser bewährten Methode bezieht sich sichere Entwicklung auf die Software, die geschrieben wird, und die Tools oder Systeme, die den Softwareentwicklungs-Lebenszyklus (SDLC) unterstützen.

Typische Anti-Muster:

- Auf eine Sicherheitsüberprüfung warten und dann die Sicherheitseigenschaften eines Systems berücksichtigen.

- Alle sicherheitsbezogenen Entscheidungen dem Sicherheitsteam überlassen.
- Nicht kommunizieren, wie sich die im Softwareentwicklungs-Lebenszyklus getroffenen Entscheidungen auf die allgemeinen Sicherheitserwartungen- oder -richtlinien der Organisation beziehen.
- Den Sicherheitsüberprüfungsprozess zu spät einsetzen.

Vorteile der Nutzung dieser bewährten Methode:

- Bessere Kenntnis der Unternehmensanforderungen hinsichtlich Sicherheit früh im Entwicklungszyklus.
- Raschere Lieferung von Funktionen durch das schnelle Identifizieren und Lösen potenzieller Sicherheitsproblemen.
- Verbesserte Qualität von Software und Systemen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: mittel

Implementierungsleitfaden

Bieten Sie den Entwicklern in Ihrem Unternehmen Schulungen. Ein Kurs über Bedrohungsmodellierung ist ein guter Start, um einen Grundstein für Sicherheitsschulungen zu legen. Idealerweise sollten Entwickler selbständig auf die Informationen zugreifen können, die für ihre Workloads relevant sind. Dieser Zugriff hilft ihnen dabei, informierte Entscheidungen zu den Sicherheitseigenschaften der Systeme zu treffen, die sie entwickelt haben, ohne ein anderes Team kontaktieren zu müssen. Der Vorgang zum Einbinden von Sicherheitsteams in Überprüfungen sollte klar definiert und einfach zu befolgen sein. Die Schritte des Überprüfungsprozesses sollten Inhalt der Sicherheitsschulung sein. Dort, wo bekannte Implementierungsmuster oder -vorlagen verfügbar sind, sollten sie einfach zu finden und mit den allgemeinen Sicherheitsanforderungen verknüpft sein. Erwägen Sie, AWS CloudFormation, AWS Cloud Development Kit (AWS CDK)-Konstrukte, Service Catalog oder andere Vorlagen-Tools zu verwenden, um den Bedarf nach einer benutzerspezifischen Konfiguration zu verringern.

Implementierungsschritte

- Ein Kurs über Bedrohungsmodellierung ist für Ihre Entwickler ein guter Start, um einen Grundstein für Sicherheitsüberlegungen zu legen.

- Bieten Sie Zugriff auf AWS Training and Certification und Branchen- oder AWS-Partner-Schulungen.
- Bieten Sie Schulungen zum Sicherheitsüberprüfungsprozess Ihres Unternehmens an, die die Aufteilung von Verantwortlichkeiten zwischen Sicherheitsteams, Workload-Teams und anderen Beteiligten klären.
- Veröffentlichen Sie Self-Service-Anweisungen zum Erfüllen von Sicherheitsanforderungen, einschließlich Codebeispielen und Vorlagen, wenn verfügbar.
- Erhalten Sie regelmäßig Feedback von Entwicklerteams zu ihrer Erfahrung mit dem Sicherheitsüberprüfungsprozess und -schulungen und verwenden Sie dieses Feedback, um Verbesserungen zu implementieren.
- Führen Sie Ernstfallübungen oder Kampagnen zum Beseitigen von Bugs durch, um die Anzahl von Fehlern zu verringern und die Fähigkeiten Ihrer Entwickler auszuweiten.

Ressourcen

Zugehörige bewährte Methoden:

- SEC11-BP08 Ein Programm entwickeln, das den Workload-Teams die Verantwortung für die Sicherheit überträgt

Zugehörige Dokumente:

- AWS Training und Zertifizierung
- How to think about cloud security governance (Über Cloud-Sicherheits-Governance nachdenken)
- How to approach threat modeling (Konzepte für Bedrohungsmodellierung)
- Accelerating training – The AWS Skills Guild (Schulungen beschleunigen – AWS Skills Guild)

Zugehörige Videos:

- Proactive security: Considerations and approaches (Proaktive Sicherheit: Überlegungen und Ansätze)

Zugehörige Beispiele:

- Workshop on threat modeling (Workshop zur Bedrohungsmodellierung)

- Industry awareness for developers (Branchenbewusstsein für Entwickler)

Zugehörige Services:

- AWS CloudFormation
- AWS Cloud Development Kit (AWS CDK) (AWS CDK) Konstrukte
- Service Catalog
- AWS BugBust

SEC11-BP02 Das Testen während des Entwicklungs- und Veröffentlichungslebenszyklus automatisieren

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 bei der bereitgestellten Software verringert.

Gewünschtes Resultat: 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 Komponententestsuites 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 nicht kommunizieren.
- Automatisiertes Testen nur vor einer Veröffentlichung durchführen.
- Testfälle mit sich häufig ändernden Anforderungen automatisieren.
- Keine Anweisungen für den Umgang mit den Ergebnissen von Sicherheitstests bieten.

Vorteile der Nutzung dieser bewährten Methode:

- Verringerte Abhängigkeit von Menschen, um die Sicherheitseigenschaften eines Systems zu evaluieren.
- Beständige Resultate bei mehreren Arbeitsabläufen verbessern die Konsistenz.
- Verringerte Wahrscheinlichkeit, dass Sicherheitsprobleme in die Softwareproduktion eingeschleppt werden.
- Kürzeres Zeitfenster zwischen der Erkennung und Lösung von Softwareproblemen, da sie früher entdeckt werden.
- Erhöhte Sichtbarkeit von systemischem oder wiederholtem Verhalten bei mehreren Arbeitsabläufen, dank derer unternehmensweite 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.

Statisches Anwendungssicherheitstesten (SAST) untersucht Ihren Quellcode auf Anomalien bei Sicherheitsmustern und bietet Hinweise auf einen fehleranfälligen Code. SAST nutzt statische Eingaben, wie 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 von großen Codemengen zu beschleunigen. Die NIST Quality Group bietet einen Vergleich von Source Code Security Analyzers, die Open-Source-Tools für Byte Code Scanner und Binary Code Scanner enthalten.

Ergänzen Sie Ihr statisches Testen mit Methodologien zum dynamischen Anwendungssicherheitstesten (DAST), wobei die Anwendung bei ihrer Ausführung getestet wird, 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 der Code-Repository-, Build- und Pipeline-Stadien ermöglicht Ihnen, nach unterschiedlichen Arten potenzieller Fehler in Ihrem Code zu suchen. Amazon CodeWhisperer bietet Codeempfehlungen, einschließlich Sicherheitsscans in der IDE des Entwicklers. Amazon CodeGuru Reviewer kann kritische Fehler, Sicherheitsprobleme und schwer zu findende Bugs während der Anwendungsentwicklung identifizieren und bietet Empfehlungen zur Verbesserung der Codequalität.

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-Testmethodologien 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 adressiert 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 integrierte Entwicklungsumgebung, Codeüberprüfung und CI/CD-Tools, die Sicherheitstests enthalten.
- Überlegen Sie, wo im Softwareentwicklungs-Lebenszyklus Pipelines blockiert werden können, anstatt Entwickler darüber zu informieren, dass Probleme behoben werden müssen.
- Der Workshop „Security for Developers“ bietet ein Beispiel für das Integrieren von statischem und dynamischem Testen in eine Veröffentlichungs-Pipeline.
- Das Durchführen von Tests oder Codeanalyse mithilfe von automatisierten Tools, wie Amazon CodeWhisperer, das mit IDEs von Entwicklern integriert ist, und Amazon CodeGuru Reviewer für das Scannen von Code beim Commit, ermöglicht 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.
- Der AWS CI/CD-Workshop bietet einen Ausgangspunkt für das Entwickeln von CI/CD-Pipelines auf AWS.

- Wenn automatisiertes Testen bei CI/CD-Pipelines enthalten ist, sollten Sie ein Ticketing-System verwenden, um das Melden und Lösen von Softwareproblemen nachzuverfolgen.
- Bei Sicherheitstests, die möglicherweise Erkenntnisse liefern, sollten Sie Lösungsanweisungen bieten, damit Entwickler die Codequalität verbessern können.
- Analysieren Sie von automatisierten Tools gewonnenen Einblicke, um die nächste Automatisierung, Entwicklerschulung oder Bewusstmachungskampagne zu planen.

Ressourcen

Zugehörige Dokumente:

- Continuous Delivery und Continuous Deployment

- AWS DevOps Competency Partners (AWS-Dev-Ops-Kompetenzpartner)
- AWS Security Competency Partners for Application Security (Sicherheitskompetenzpartner für Anwendungssicherheit)
- Choosing a Well-Architected CI/CD approach (Auswählen eines Well-Architected-CI/CD-Ansatzes)
- Monitoring CodeCommit events in Amazon EventBridge and Amazon CloudWatch Events (Überwachen von AWS-CodeCommit-Ereignissen in Amazon EventBridge und Amazon CloudWatch Events)
- Secrets detection in Amazon CodeGuru Review (Secrets-Erkennung bei der Code-Überprüfung in CodeGuru Reviewer)
- Accelerate deployments on AWS with effective governance (Beschleunigen von Bereitstellungen auf AWS mit effektiver Governance)
- How AWS approaches automating safe, hands-off deployments (Wie AWS die Automatisierung sicherer, vollautomatischer Bereitstellungen durchführt)

Zugehörige Videos:

- Hands-off: Automating continuous delivery pipelines at Amazon (Vollständige Automatisierung: Automatisieren der Pipelines für kontinuierliche Bereitstellung bei Amazon)
- Automating cross-account CI/CD pipelines (Automatisieren von kontoübergreifenden CI/CD-Pipelines)

Zugehörige Beispiele:

- Industry awareness for developers (Branchenbewusstsein für Entwickler)
- AWS CodePipeline Governance (GitHub)
- Workshop „Security for Developers“ (Workshop „Sicherheit für Entwickler“)
- AWS-CI/CD-Workshop

SEC11-BP03 Regelmäßig Penetrationstests durchführen

Führen Sie regelmäßige Penetrationstests bei Ihrer 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 sollten feststellen, ob es möglich ist, die Software so zu beeinflussen, dass sie auf unerwartete Weise ausgeführt wird, beispielsweise das Freigeben von Daten, die geschützt sein sollten, oder die Gewährung umfassenderer Berechtigungen als erwartet.

Gewünschtes Ergebnis: Penetrationstests werden verwendet, um die Sicherheitseigenschaften Ihrer Anwendung zu erkennen, zu lösen und zu validieren. Regelmäßige und geplante Penetrationstests sollten als Teil des Softwareentwicklungs-Lebenszyklus durchgeführt werden. Die aus Penetrationstests gewonnenen Erkenntnisse sollten vor der Veröffentlichung der Software adressiert werden. Sie sollten die Ergebnisse von Penetrationstests verwenden, um festzustellen, ob es sich um Probleme handelt, die mithilfe von Automatisierung gefunden werden könnten. Ein regelmäßiger und wiederholbarer Prozess für Penetrationstests, der einen aktiven Feedback-Mechanismus umfasst, fließt in die Anweisungen für Entwickler ein und verbessert die Softwarequalität.

Typische Anti-Muster:

- Penetrationstests nur für bekannte oder weit verbreitete Sicherheitsprobleme verwenden.
- Penetrationstests bei Anwendungen ohne abhängige Drittanbieter-Tools und -Bibliotheken durchführen.
- Penetrationstests nur bei Paketsicherheitsproblemen durchführen und die implementierte Geschäftslogik nicht evaluieren.

Vorteile der Nutzung dieser bewährten Methode:

- Gesteigertes Vertrauen in die Sicherheitseigenschaften der Software vor der Veröffentlichung.
- Die Möglichkeit, bevorzugte Anwendungsmuster zu identifizieren, wodurch die Softwarequalität erhöht wird.
- Verbresserte Sicherheitseigenschaften von Software durch eine Feedbackschleife, die früher im Entwicklungszyklus bestimmt, wo Automatisierung oder zusätzliche Schulungen erforderlich sind.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Penetrationstests sind eine strukturierte Sicherheitstestübung, wobei Sie Szenarios mit geplanten Sicherheitsverstößen durchführen, um Sicherheitskontrollen zu erkennen, zu lösen und zu validieren. Penetrationstests starten mit einer Erkundung, bei der Daten basierend auf dem aktuellen Design der Anwendung und ihrer Abhängigkeiten erfasst werden. Eine kuratierte Liste an sicherheitsspezifischen Testszenarios wird entwickelt und ausgeführt. Der wesentliche Zweck dieser Tests ist, die Sicherheitsprobleme in Ihrer Anwendung aufzudecken, die dazu genutzt werden könnten, unbeabsichtigten Zugriff auf Ihre Umgebung oder unautorisierten Zugriff auf Daten zu erhalten. Sie sollten Penetrationstests durchführen, wenn Sie neue Funktionen einführen oder wenn bei Ihrer Anwendung wesentliche Änderungen hinsichtlich der Funktion oder technischen Implementierung erfolgt sind.

Sie sollten in Ihrem Entwicklungslebenszyklus die am besten geeignete Phase bestimmen, um Penetrationstests durchzuführen. Das Testen sollte so spät stattfinden, dass sich das System nahe am vorgesehenen Veröffentlichungszustand befindet, aber es sollte ausreichend Zeit vorhanden sein, damit Probleme behoben werden können.

Implementierungsschritte

- Implementieren Sie einen strukturierten Prozess für den Umfang der Penetrationstests und dieser Prozess sollte auf einem Bedrohungsmodell basieren, um den Kontext zu bewahren.
- Bestimmen Sie den geeigneten Zeitpunkt im Entwicklungszyklus zum Durchführen von Penetrationstests. Penetrationstests sollten dann erfolgen, wenn die geringsten Änderungen an der Anwendung erwartet werden, aber noch ausreichend Zeit für die Fehlerbehebung übrig ist.
- Schulen Sie Ihre Entwickler in Bezug darauf, was sie von den Ergebnissen von Penetrationstests erwarten und wie Informationen zur Mängelbeseitigung erhalten können.
- Verwenden Sie Tools zum Beschleunigen des Penetrationstestvorgangs, indem Sie gängige oder wiederholbare Tests automatisieren.

- Analysieren Sie Ergebnisse von 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 Das Testen während des Entwicklungs- und Veröffentlichungslebenszyklus automatisieren

Zugehörige Dokumente:

- AWS-Penetrationstest bieten ausführliche Anweisungen für Penetrationstests mit AWS
- Accelerate deployments on AWS with effective governance (Beschleunigen von Bereitstellungen auf AWS mit effektiver Governance)
- AWS Security Competency Partners (AWS-Kompetenzpartner für Sicherheit)
- Modernize your penetration testing architecture on AWS Fargate (Modernisieren Ihrer Penetrationstestarchitektur auf AWS Fargate)
- AWS Fault Injection Simulator

Zugehörige Beispiele:

- Automate API testing with AWS CodePipeline (Automatisieren von API-Testen mit AWS Codepipeline mit Postman) (GitHub)
- Automated security helper (Automatisierter Sicherheitshelfer) (GitHub)

SEC11-BP04 Manuelle Codeüberprüfungen

Führen Sie eine manuelle Codeüberprüfung der von Ihnen produzierten Software durch. Dieser Prozess hilft zu verifizieren, dass die Person, die den Code geschrieben hat, die Qualität des Codes nicht allein überprüft.

Gewünschtes Ergebnis: Das Hinzufügen einer manuellen Codeüberprüfung während der Entwicklung erhöht die Qualität der geschriebenen Software, hilft dabei, weniger erfahrene Teammitglieder

weiterzubilden, und bietet eine Möglichkeit, Stellen zum Einsetzen von Automatisierung zu identifizieren. Manuelle Codeüberprüfungen können von automatisierten Tools und Tests unterstützt werden.

Typische Anti-Muster:

- Keine Codeüberprüfungen vor der Bereitstellung durchführen.
- Die gleiche Person zum Schreiben und Überprüfen des Codes einsetzen.
- Keine Automatisierung zum Unterstützen und Orchestrieren von Codeüberprüfungen einsetzen.
- Entwickler nicht hinsichtlich Anwendungssicherheit schulen, bevor sie Code überprüfen.

Vorteile der Nutzung dieser bewährten Methode:

- Verbesserte Codequalität.
- Erhöhte Konsistenz bei der Codeentwicklung durch das erneute Verwenden von gängigen Ansätzen.
- 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

Der Überprüfungsschritt sollte als Teil des allgemeinen Codeverwaltungs-Flows implementiert werden. Die Details hängen vom Ansatz an, der für Verzweigen, Pull-Anforderungen und Zusammenführen verwendet wird. Sie verwenden möglicherweise AWS CodeCommit oder Drittanbieterlösungen wie GitHub, GitLab oder Bitbucket. Welche Methode auch immer Sie verwenden – es ist wichtig, dass Sie verifizieren, dass Ihre Prozesse eine Überprüfung von Code erfordern, bevor dieser in einer Produktionsumgebung bereitgestellt wird. Das Verwenden von Tools wie Amazon CodeGuru Reviewer kann das Orchestrieren des Codeüberprüfungsvorgangs vereinfachen.

Implementierungsschritte

- Implementieren Sie einen Schritt zur manuellen Überprüfung als Teil Ihres Codeverwaltungs-Flows und führen Sie diese Überprüfung durch, bevor Sie fortfahren.

- Erwägen Sie Amazon CodeGuru Reviewer für das Verwalten und Unterstützen bei Codeüberprüfungen.
- Implementieren Sie einen Genehmigungs-Workflow, bei dem eine Codeüberprüfung erforderlich ist, bevor Code zur nächsten Stufe übergehen kann.
- Verifizieren Sie, dass es einen Vorgang gibt, um Probleme bei manuellen Codeüberprüfungen zu finden, die automatisch erkannt werden könnten.
- Integrieren Sie den Schritt zur manuellen Codeüberprüfung auf eine Weise, die mit Ihren Codeentwicklungspraktiken übereinstimmt.

Ressourcen

Zugehörige bewährte Methoden:

- SEC11-BP02 Das Testen während des Entwicklungs- und Veröffentlichungslebenszyklus automatisieren

Zugehörige Dokumente:

- Working with pull requests in AWS CodeCommit repositories (Arbeiten Mit Pull-Anforderungen in AWS CodeCommit)
- Working with approval rule templates in AWS CodeCommit (Arbeiten mit Genehmigungsregelvorlagen in AWS CodeCommit)
- About pull requests in GitHub (Informationen über Pull-Anforderungen auf GitHub)
- Automate code reviews with Amazon CodeGuru Reviewer (Automatisieren von Codeüberprüfungen mit Amazon CodeGuru Reviewer)
- Automating detection of security vulnerabilities and bugs in CI/CD pipelines using Amazon CodeGuru Reviewer CLI (Automatisieren der Erkennung von Sicherheitsschwachstellen und Bugs in CI/CD-Pipelines mithilfe der CLI von Amazon CodeGuru Reviewer

Zugehörige Videos:

- Continuous improvement of code quality with Amazon CodeGuru (Kontinuierliche Verbesserung der Codequalität mit Amazon CodeGuru)

Zugehörige Beispiele:

- Security for Developers workshop (Workshop „Sicherheit für Entwickler“)

SEC11-BP05 Services für Pakete und Abhängigkeiten zentralisieren

Stellen Sie zentralisierte Services für Entwicklungsteams bereit, sodass sie Softwarepakete und andere Abhängigkeiten erhalten können. Dadurch können Pakete validiert werden, bevor sie in die von Ihnen geschriebene Software integriert werden, und es kann eine Datenquelle für die Analyse der Software bereitgestellt werden, die in Ihrer Organisation verwendet wird.

Gewünschtes Ergebnis: Software besteht aus einem Set aus anderen Softwarepaketen zusätzlich zum Code, der geschrieben wird. Dadurch wird die Implementierung von häufig verwendeten Funktionen vereinfacht, wie einem JSON-Parser oder einer Verschlüsselungsbibliothek. Das logische Zentralisieren der Quellen und Abhängigkeiten für diese Pakete bietet einen Mechanismus für Sicherheitsteams, damit diese die Eigenschaften der Pakete validieren können, bevor sie verwendet werden. Dieser Ansatz verringert auch das Risiko, dass ein unerwartetes Problem durch die Änderung eines vorhandenen Pakets verursacht wird oder dass Entwicklungsteams beliebige Pakete direkt aus dem Internet einbeziehen. Verwenden Sie diesen Ansatz zusammen mit manuellem und automatischem Testen, um das Vertrauen in die Qualität der entwickelten Software zu steigern.

Typische Anti-Muster:

- Pakete aus beliebigen Repositorys im Internet abrufen.
- Neue Pakete nicht testen, bevor sie für Entwickler verfügbar gemacht werden.

Vorteile der Nutzung dieser bewährten Methode:

- Besseres Verständnis darüber, 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 Ihrer Software enthalten ist.

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 Möglichkeit zum Hinzufügen von Paketen zum Repository implementieren, wenn Updates erfolgen oder neue Anforderungen aufkommen. Mithilfe von AWS-Services wie AWS CodeArtifact oder ähnlichen AWS-Partnerlösungen kann diese Funktion geboten werden.

Implementierungsschritte:

- Implementieren Sie einen logisch zentralisierten Repository-Service, der in allen Umgebungen, in welchen die Software entwickelt wird, verfügbar ist.
- Fügen Sie den Zugriff auf das Repository als Teil des AWS-Konto-Vergabeprozesses hinzu.
- 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 Entwicklungsteams einen automatisierten Mechanismus bereit, damit sie neue Pakete anfordern und Feedback abgeben können.
- Scannen Sie regelmäßig Pakete in Ihrem Repository, um die Auswirkungen von kürzlich entdecken Problemen zu identifizieren.

Ressourcen

Zugehörige bewährte Methoden:

- SEC11-BP02 Das Testen während des Entwicklungs- und Veröffentlichungslebenszyklus automatisieren

Zugehörige Dokumente:

- Accelerate deployments on AWS with effective governance (Beschleunigen von Bereitstellungen auf AWS mit effektiver Governance)

- Tighten your package security with CodeArtifact Package Origin Control toolkit (Erhöhen Ihrer Paketsicherheit mit dem Toolkit von CodeArtifact Package Origin Control)
- Detecting security issues in logging with Amazon CodeGuru Reviewer (Erkennen von Sicherheitsproblemen beim Protokollieren mit Amazon CodeGuru Reviewer)
- Supply chain Levels for Software Artifacts (SLSA) (Lieferkettenebenen für Software-Artefakte)

Zugehörige Videos:

- Proactive security: Considerations and approaches (Proaktive Sicherheit: Überlegungen und Ansätze)
- The AWS Philosophy of Security (re:Invent 2017) (Die AWS-Philosophie zu Sicherheit)
- When security, safety, and urgency all matter: Handling Log4Shell (Wenn Sicherheit und Dringlichkeit von Bedeutung sind: Umgang mit Log4Shell)

Zugehörige Beispiele:

- Multi Region Package Publishing Pipeline (Mehrregions-Veröffentlichungs-Pipeline für Pakete) (GitHub)
- Publishing Node.js Modules on AWS CodeArtifact using AWS CodePipeline (Node.js-Module auf AWS CodeArtifact mithilfe von AWS CodePipeline veröffentlichen) (GitHub)
- AWS CDK Java CodeArtifact Pipeline Sample (Beispiel für eine Java-CodeArtifact-Pipeline) (GitHub)
- Distribute private .NET NuGet packages with AWS CodeArtifact (Verteilen von privaten .NET-NuGet-Pakete mit AWS CodeArtifact) (GitHub)

SEC11-BP06 Software programmgesteuert bereitstellen

Führen Sie Bereitstellungen von Software möglichst programmgesteuert durch. Dieser Ansatz verringert die Wahrscheinlichkeit eines Bereitstellungsfehlers oder der Einführung eines unerwarteten Problem aufgrund eines menschlichen Fehlers.

Gewünschtes Ergebnis: Menschen von Daten fernhalten ist eines der Prinzipien für sicheres Entwickeln in der AWS Cloud. Dieses Prinzip umfasst, wie Sie Ihre Software bereitstellen.

Wenn Sie sich nicht auf Menschen verlassen müssen, um Software bereitzustellen, bietet dies den Vorteil, dass Sie mehr Vertrauen darin haben können, dass das, was getestet wird, auch das ist, was

bereitgestellt wird, und dass die Bereitstellung jedes Mal konsistent durchgeführt wird. Die Software sollte nicht geändert werden müssen, um in unterschiedlichen Umgebungen zu funktionieren. Mithilfe der Prinzipien der 12-Faktor-Anwendungsentwicklung, insbesondere dem Externalisieren der Konfiguration, können Sie denselben Code ohne Änderungen in mehreren Umgebungen bereitstellen. Das kryptografische Signieren von Softwarepaketen ist eine gute Möglichkeit, zu verifizieren, dass sich zwischen den Umgebungen nichts geändert hat. Das Gesamtergebnis dieses Ansatzes ist die Risikoverringerung bei Ihrem Änderungsprozess und die Verbesserung der Konsistenz von Softwareveröffentlichungen.

Typische Anti-Muster:

- Software manuell in die Produktion bereitstellen.
- Manuelle Änderungen an Software durchführen, um unterschiedliche Umgebungen zu bedienen.

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.
- Die Möglichkeit, kryptografisch zu beweisen, dass es sich bei der getesteten Software um die bereitgestellte Software handelt.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: hoch

Implementierungsleitfaden

Entwickeln Sie Ihre AWS-Konto-Struktur, um den fortlaufenden menschlichen Zugriff über Umgebungen zu verhindern und CI/CD-Tools zum Durchführen von Bereitstellungen zu verwenden. Entwerfen Sie Ihre Anwendungen so, dass umgebungsspezifische Konfigurationsdaten von externen Quellen gewonnen werden, wie AWS Systems Manager Parameter Store. Signieren Sie Pakete, nachdem sie getestet wurden, und validieren Sie diese Signaturen während der Bereitstellung. Konfigurieren Sie Ihre CI/CD-Pipelines, um den Anwendungscode zu übertragen und verwenden Sie Canaries, um die erfolgreiche Bereitstellung zu bestätigen. Verwenden Sie Tools wie AWS CloudFormation oder AWS CDK, um Ihre Infrastruktur zu definieren, und verwenden Sie dann AWS CodeBuild und AWS CodePipeline, um CI/CD-Vorgänge durchzuführen.

Implementierungsschritte

- Entwicklen Sie gut definierte CI/CD-Pipelines, um den Bereitstellungsprozess zu optimieren.
- Die Verwendung von AWS CodeBuild und AWS Code Pipeline, um die CI/CD-Funktionalität zu bieten, vereinfacht das Integrieren von Sicherheitstesten in Ihre Pipelines.
- Befolgen Sie die Anweisungen für die Trennung von Umgebungen im Whitepaper Organisation Ihrer AWS-Umgebung mit mehreren Konten.
- Verifzieren Sie, dass es keinen fortlaufenden Zugriff durch Personen auf Umgebungen gibt, in welchen Produktions-Workloads ausgeführt werden.
- Entwickeln Sie Ihre Anwendungen so, dass sie die Externalisierung von Konfigurationsdaten unterstützen.
- Ziehen Sie eine Bereitstellung mithilfe eines Blau/Grün-Modells in Betracht.
- Setzen Sie Canaries ein, um die erfolgreiche Bereitstellung der Software zu validieren.
- Verwenden Sie kryptografische Tools wie AWS Signer oder AWS Key Management Service (AWS KMS), um die Softwarepakete, die Sie bereitstellen, zu signieren und zu verifizieren.

Ressourcen

Zugehörige bewährte Methoden:

- SEC11-BP02 Das Testen während des Entwicklungs- und Veröffentlichungslebenszyklus automatisieren

Zugehörige Dokumente:

- AWS-CI/CD-Workshop
- Accelerate deployments on AWS with effective governance (Beschleunigen von Bereitstellungen auf AWS mit effektiver Governance)
- Automating safe, hands-off deployments (Automatisierung sicherer, vollautomatischer Bereitstellungen)
- Code signing using AWS Certificate Manager Private CA and AWS Key Management Service asymmetric keys (Codesignatur mithilfe von AWS Certificate Manager Private CA und asymmetrischen Schlüsseln von AWS Key Management Service)
- Code Signing, a Trust and Integrity Control for AWS Lambda (Codesignatur, eine Vertrauens- und Integritätskontrolle für AWS Lambda)

Zugehörige Videos:

- Hands-off: Automating continuous delivery pipelines at Amazon (Vollständige Automatisierung: Automatisieren der Pipelines für kontinuierliche Bereitstellung bei Amazon)

Zugehörige Beispiele:

- Blue/Green deployments with AWS Fargate (Blau/Grün-Bereitstellungen mit AWS Fargate)

SEC11-BP07 Die Sicherheitseigenschaften der Pipelines regelmäßig bewerten

Wenden Sie die Prinzipien der Säule der Well-Architected-Sicherheit bei Ihren Pipelines an und achten Sie dabei besonders auf die Trennung von Berechtigungen. Bewerten Sie die Sicherheitseigenschaften Ihrer Pipeline-Infrastruktur regelmäßig. Durch die effektive Verwaltung der Pipeline-Sicherheit können Sie bei der Software, die diese Pipelines durchläuft, für Sicherheit sorgen.

Gewünschtes Ergebnis: Die Pipelines, die zum Entwickeln und Bereitstellen Ihrer Software verwendet werden, sollten dieselben empfohlenen Praktiken wie jeder andere Workload in Ihrer Umgebung befolgen. Die Tests, die in den Pipelines implementiert sind, sollten nicht von Entwicklern bearbeitet werden können, die sie verwenden. Die Pipelines sollten nur Berechtigungen für die Bereitstellungen haben, die sie durchführen, und sollten Sicherheitsmaßnahmen zum Verhindern von Bereitstellungen in den falschen Umgebungen implementieren. Pipelines sollten sich nicht auf langfristige Anmeldeinformationen verlassen und sollten konfiguriert sein, um den Status auszugeben, sodass die Integrität der Entwicklungsumgebung validiert werden kann.

Typische Anti-Muster:

- Sicherheitstests können von Entwicklern umgangen werden.
- Berechtigungen für Bereitstellungs-Pipelines sind übermäßig breit gefasst.
- Pipelines sind nicht konfiguriert, um Eingaben zu validieren.
- Berechtigungen in 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

Durch den Beginn mit CI/CD-Services, die IAM-Rollen unterstützen, wird das Risiko von Anmeldeinformationslecks verringert. Durch das Anwenden der Prinzipien der Säule „Sicherheit“ auf Ihre CI/CD-Pipeline-Infrastruktur können Sie bestimmen, wo Sicherheitsverbesserungen durchgeführt werden können. Das Befolgen der AWS Deployment Pipelines Reference Architecture (Referenzarchitektur für AWS-Bereitstellungs-Pipelines) ist ein guter Startpunkt für das Erstellen Ihrer eigenen CI/CD-Umgebungen. Regelmäßige Überprüfungen der Pipeline-Implementierung und Untersuchungen von Protokollen auf unerwartetes Verhalten können Ihnen dabei helfen, die Verwendungsmuster der Pipelines, die zum Bereitstellen der Software verwendet werden, besser zu verstehen.

Implementierungsschritte

- Beginnen Sie mit der AWS Deployment Pipelines Reference Architecture (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, sodass Sie über unerwartete oder abnorme Aktivitäten benachrichtigt werden. Bei von AWS verwalteten Services können Sie mithilfe von Amazon EventBridge Daten zu Zielen wie AWS Lambda oder Amazon Simple Notification Service (Amazon SNS) umleiten.

Ressourcen

Zugehörige Dokumente:

- AWS Deployment Pipelines Reference Architecture (Referenzarchitektur für AWS-Bereitstellungs-Pipelines)
- Monitoring AWS CodePipeline (Überwachen von AWS CodePipeline)

- Security best practices for AWS CodePipeline (Bewährte Methoden für die Sicherheit mit AWS CodePipeline)

Zugehörige Beispiele:

- DevOps monitoring dashboard (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, 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, doch macht das Übertragen der Sicherheitsverantwortlichkeit auf Entwicklerteams eine schnellere und sicherer Workload-Erstellung möglich. Zudem fördert dieser Mechanismus eine Kultur der Verantwortlichkeit, die einen positiven Einfluss auf den Betrieb der von Ihnen entwickelten Systeme hat.

Gewünschtes Ergebnis: Um Entwicklungsteams Verantwortung und Entscheidungsfindung zu überlassen, können Sie entweder Entwickler in Bezug darauf schulen, wie sie über Sicherheit nachdenken, oder Sie können ihre Schulung mithilfe von Sicherheitsexperten verbessern, die Teil des Entwicklungsteams sind oder damit in Kontakt stehen. Beide Ansätze sind valide und ermöglichen dem Team, bessere Sicherheitsentscheidungen früher im Entwicklungszyklus zu treffen. Dieses Verantwortungsmodell basiert auf Schulungen in Anwendungssicherheit. Wenn Sie mit einem Bedrohungsmodell für den bestimmten Workload beginnen, hilft Ihnen dies dabei, das Design Thinking auf den entsprechenden Kontext zu konzentrieren. Ein weiterer Vorteil, eine Community an sicherheitsorientierten Entwicklern oder eine Gruppe an Sicherheitstechnikern zu haben, die mit Entwicklungsteams zusammenarbeiten, ist, dass Sie ein besseres Verständnis darüber erlangen, wie Code geschrieben wird. Dieses Verständnis hilft Ihnen dabei, die nächsten verbesserungswürdigen Bereiche bei Ihrem Automatisierungsunterfangen zu bestimmen.

Typische Anti-Muster:

- Einem Sicherheitsteam alle Entscheidungen bezüglich des Sicherheitsdesigns überlassen.
- Sicherheitsanforderungen nicht früh genug im Entwicklungsprozess adressieren.

- Kein Feedback bezüglich des Programmbetriebs von Entwicklern und Sicherheitsexperten einholen.

Vorteile der Nutzung dieser bewährten Methode:

- Kürzere Dauer zum Abschließen von Sicherheitsüberprüfungen.
- Verringerung von Sicherheitsproblemen, die nur auf der Ebene der Sicherheitsüberprüfung erkannt werden.
- Verbesserung der gesamten Qualität der Software, die geschrieben wird.
- Die Möglichkeit, systemische Probleme oder Bereiche mit hoher Wertverbesserung zu identifizieren und zu verstehen.
- Verringerung der erforderlichen Überarbeitung aufgrund von Erkenntnissen in Bezug auf Sicherheit.
- Verbesserung der Wahrnehmung von Sicherheitsfunktionen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: niedrig

Implementierungsleitfaden

Beginnen Sie mit den Anweisungen unter SEC11-BP01 Für Anwendungssicherheit schulen. Bestimmen Sie danach das Betriebsmodell für das Programm, von dem Sie denken, dass es am besten für Ihr Unternehmen funktioniert. Die zwei Hauptmuster bestehen daraus, Entwickler zu schulen oder Sicherheitsexperten in in Entwicklungsteams zu positionieren. Nachdem Sie sich für eine anfängliche Verfahrensweise entschieden haben, sollten Sie einen Pilotlauf mit einem einzelnen Team oder einer kleinen Gruppe von Workload-Teams durchführen, um zu bestätigen, dass das Modell für Ihr Unternehmen funktioniert. Unterstützung der Führungskräfte aus den Entwicklungs- und Sicherheitsbereichen des Unternehmens hilft Ihnen beim Durchführen und dem Erfolg des Programms. Während Sie dieses Programm entwickeln, ist es wichtig, Metriken auszuwählen, die auf den Wert des Programms hinweisen. Zu erfahren, wie AWS mit diesem Problem umgegangen ist, bietet eine gute Lernerfahrung. Die bewährte Methode konzentriert sich auf die Veränderung und Kultur des Unternehmens. Die von Ihnen eingesetzten Tools sollten die Zusammenarbeit zwischen den Entwicklung- und Sicherheits-Communities unterstützen.

Implementierungsschritte

- Beginnen Sie damit, Ihre Entwickler im Bereich der Anwendungssicherheit zu schulen.

- Schaffen Sie eine Community und ein Onboarding-Programm zum Schulen der Entwickler.
- Geben Sie dem Programm einen Namen. Guardians, Champions oder Advocates werden häufig verwendet.
- Bestimmen Sie das Modell, das verwendet werden soll: Schulen Sie Entwickler und bringen Sie Sicherheitstechniker oder andere verwandte Sicherheitsrollen ein.
- Identifizieren Sie Projektsponsoren aus Sicherheitsexperten, Entwicklern und anderen potenziell relevanten Gruppen.
- Verfolgen Sie Metriken für die Anzahl der im Programm involvierten Personen, die für Überprüfungen erforderliche Zeit und das Feedback von Entwicklern und Sicherheitsexperten. Nutzen Sie diese Metriken, um Verbesserungen vorzunehmen.

Ressourcen

Zugehörige bewährte Methoden:

- SEC11-BP01 Für Anwendungssicherheit schulen
- SEC11-BP02 Das Testen während des Entwicklungs- und Veröffentlichungslebenszyklus automatisieren

Zugehörige Dokumente:

- How to approach threat modeling (Konzepte für Bedrohungsmodellierung)
- How to think about cloud security governance (Über Cloud-Sicherheits-Governance nachdenken)

Zugehörige Videos:

- Proactive security: Considerations and approaches (Proaktive Sicherheit: Überlegungen und Ansätze)

Fazit

Sicherheit ist ein permanentes Thema. Vorfälle sollten als Chancen zur Verbesserung der Sicherheit einer Architektur betrachtet werden. Jedes Unternehmen sollte tiefgreifende Verteidigungsmechanismen haben, wie etwa starke Identitätskontrollen, automatisierte Reaktionen auf Sicherheitsvorfälle, Schutzmechanismen auf mehreren Ebenen der Infrastruktur sowie die Verschlüsselung gut klassifizierter Daten. Die in diesem Whitepaper erörterten programmgesteuerten Funktionen und AWS-Funktionen und -Services erleichtern dies.

AWS unterstützt Sie beim Aufbau und Betrieb von Architekturen, die Ihre Informationen, Systeme und Ressourcen schützen und gleichzeitig einen Mehrwert für das Unternehmen bieten.

Mitwirkende

Dieses Dokument ist unter der Mitarbeit folgender Personen und Organisationen entstanden:

- Sarita Dharankar, Security Pillar Lead, Well-Architected, Amazon Web Services
- Adam Cerini, Senior Solution Architect, Amazon Web Services
- Bill Shinn, Senior Principal, Office of the CISO, Amazon Web Services
- Brigid Johnson, Senior Software Development Manager, AWS Identity, Amazon Web Services
- Byron Pogson, Senior Solution Architect, Amazon Web Services
- Charlie Hammell, Principal Enterprise Architect, Amazon Web Services
- Darran Boyd, Principal Security Solutions Architect, Financial Services, Amazon Web Services
- Dave Walker, Principal Specialist Solutions Architect, Security and Compliance, Amazon Web Services
- John Formento, Senior Solution Architect, Amazon Web Services
- Paul Hawkins, Principal, Office of the CISO, Amazon Web Services
- Sam Elmalak, Senior Technology Leader, Amazon Web Services
- Pat Gaw, Principal Security Consultant, Amazon Web Services
- Daniel Begimher, Senior Consultant, Security, Amazon Web Services
- Danny Cortegaca, Senior Security Solutions Architect, Amazon Web Services
- Ana Malhotra, Security Solutions Architect, Amazon Web Services
- Debashis Das, Principal, Office of the CISO, Amazon Web Services
- Reef Dsouza, Principal Solutions Architect, Amazon Web Services
- Brad Burnett, Security Solutions Architect, Identity, Amazon Web Services
- Anna McAbee, Senior Security Solutions Architect, Threat Detection and Incident Response, Amazon Web Services
- Jason Garman, Principal Security Solutinos Architect, Amazon Web Services

Weitere Informationen

Weitere Informationen finden Sie in den folgenden Quellen:

- AWS Well-Architected Framework Whitepaper
- AWS-Architekturzentrum

Dokumentversionen

Abonnieren Sie den RSS-Feed, um über Aktualisierungen des Whitepapers benachrichtigt zu werden.

Änderung	Beschreibung	Datum
Leitfäden zu bewährten Methoden aktualisiert	Bewährte Methoden wurden mit neuen Leitfäden für die Säule aktualisiert.	June 27, 2024
Leitfäden zu bewährten Methoden aktualisiert	Die bewährten Methoden wurden mit neuen Leitfäden in den folgenden Bereichen aktualisiert: Sicheres Betreiben Ihres Workloads und Schutz von Daten während der Übertragung.	December 6, 2023
Leitfäden zu bewährten Methoden aktualisiert	Wichtige Aktualisierungen der Leitfäden und bewährten Methoden für die Vorfallre aktion. Mehrere bewährte Methoden unter Vorbereitung aktualisiert. Zwei neue Bereiche wurden zur Vorfallreaktion hinzugefü gt: Betrieb und Aktivität nach Vorfällen. Neue bewährte Methode unter SEC10-BP08 Entwickeln eines Framework s, um aus Vorfällen zu lernen hinzugefügt.	October 3, 2023
Leitfäden zu bewährten Methoden aktualisiert	Bewährte Methoden wurden mit neuen Leitfäden in	July 13, 2023

	den folgenden Bereichen aktualisiert: Vorbereitung and Simulieren.	
Updates für das neue Framework	Bewährte Methoden mit verbindlichen Anleitung en aktualisiert und neue bewährte Methoden hinzugefü gt. Abschnitt für bewährte Methoden für die Anwendung ssicherheit (AppSec) hinzugefügt.	April 10, 2023
Whitepaper aktualisiert	Bewährte Methoden mit neuen Implementierungsanleitungen aktualisiert.	December 15, 2022
Whitepaper aktualisiert	Weitere bewährte Methoden und Verbesserungspläne hinzugefügt.	October 20, 2022
Kleineres Update	IAM-Information aktualisiert, um die aktuellen bewährten Methoden widerzuspiegeln.	June 28, 2022
Kleineres Update	Zusätzliche AWS PrivateLink-Informationen hinzugefügt und fehlerhafte Links korrigiert.	May 19, 2022
Kleineres Update	AWS PrivateLink hinzugefügt.	May 6, 2022
Kleineres Update	Nicht inklusive Sprache entfernt.	April 22, 2022
Kleineres Update	Informationen über den VPC Network Access Analyzer hinzugefügt.	February 2, 2022

Kleineres Update	Säule „Nachhaltigkeit“ wurde zur Einführung hinzugefügt.	December 2, 2021
Kleineres Update	Fehlerhafter Link behoben.	May 27, 2021
Kleineres Update	Redaktionelle Änderungen im gesamten Dokument.	May 17, 2021
Größere Aktualisierung	Abschnitt über Governanc e hinzugefügt, verschied ene Abschnitte detaillierter gestaltet, neue Funktionen und Services hinzugefügt.	May 7, 2021
Kleineres Update	Aktualisierte Links.	March 10, 2021
Kleineres Update	Fehlerhafter Link behoben.	July 15, 2020
Updates für das neue Framework	Aktualisierte Anleitung zur Konto-, Identitäts- und Berechtigungsverwaltung.	July 8, 2020
Updates für das neue Framework	Aktualisiert mit zusätzlic hen Ratschlägen in allen Bereichen sowie neuen bewährten Methoden, Services und Funktionen.	April 30, 2020
Whitepaper aktualisiert	Aktualisierungen bezüglich neuer AWS-Services und -Funktionen sowie aktualisierte Verweise.	July 1, 2018
Whitepaper aktualisiert	Aktualisierung des Abschnitt s „Konfiguration und Wartung der Systemsicherheit“ mit neuen AWS-Services und -Funktionen.	May 1, 2017

Erstveröffentlichung	Säule für Sicherheit des AWS-Well-Architected-Framework veröffentlicht.	November 1, 2016

Hinweise

Kunden sind eigenverantwortlich für die unabhängige Bewertung der Informationen in diesem Dokument zuständig. Dieses Dokument: (a) dient rein zu Informationszwecken, (b) spiegelt die aktuellen AWS-Produktangebote und Verfahren wider, die sich ohne vorherige Mitteilung ändern können, und (c) impliziert keinerlei Verpflichtungen oder Zusicherungen seitens AWS und dessen Tochtergesellschaften, Lieferanten oder Lizenzgebern. AWS-Produkte oder -Services werden im vorliegenden Zustand und ohne ausdrückliche oder stillschweigende Gewährleistungen, Zusicherungen oder Bedingungen bereitgestellt. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden wird durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Teil der Vereinbarungen zwischen AWS und seinen Kunden und ändert diese Vereinbarungen auch nicht.