Die 10 besten Sicherheitsmethoden für die Sicherung von Backups in AWS

AWS Prescriptive Guidance

AWS Prescriptive Guidance: Die 10 besten Sicherheitsmethoden für die Sicherung von Backups in AWS

Table of Contents

Einführung 1
Best Practices 2
Eine Strategie implementieren 2
Ransomware 3
Anforderungen an die Aufbewahrung 3
Compliance 3
Backup in DR und BCP 4
Backup automatisieren 4
Mechanismen für die Zugriffskontrolle 5
Backup-Daten und Tresor verschlüsseln 6
Backups schützen 7
Überwachen und Warnen 9
Backup-Konfiguration überprüfen 10
Testen der Datenwiederherstellung 11
Plan zur Reaktion auf Vorfälle 12
Nächste Schritte 14
Ressourcen 15
AWS Präskriptive Leitlinien 15
AWS Dokumentation 15
Blog-Posts 15
GitHub Repositorien 16
Dokumentverlauf 17
..... xviii

Die 10 besten Sicherheitsmethoden für die Sicherung von Backups in AWS

Ibukun (IB) Oyewumi, Amazon Web Services (AWS)

Mai 2022 (Dokumentverlauf)

Sicherheit ist eine geteilte Verantwortung zwischen Amazon Web Services (AWS) und Kunden. Kunden haben nach Möglichkeiten gefragt, wie sie ihre Backups sichern können AWS. Da sich die Sicherheitspraktiken ständig weiterentwickeln, um neue Risiken zu minimieren, ist es wichtig, dass Sie regelmäßige Risikobewertungen durchführen, um die Anwendbarkeit von Sicherheitskontrollen zu ermitteln, und mehrere Kontrollebenen implementieren, um die Risiken für Ihre Daten zu minimieren.

Dieses Dokument führt Sie durch eine kuratierte Liste der 10 besten Sicherheitsmethoden zum Schutz Ihrer Backup-Daten und -Vorgänge in AWS. Dieses Handbuch konzentriert sich zwar auf Backup-Daten und Operationen mit dem AWS Backup-Service, diese empfohlenen bewährten Sicherheitsmethoden können aber zusammen mit anderen Backup-Lösungen verwendet werden, z. B. mit Backup-Tools von AWS Marketplace.

Best Practices

Wir empfehlen AWS, beim Sichern von Backups den folgenden Ansatz zu verwenden:

Themen

- Schritt 1. Eine Backup-Strategie implementieren
- Schritt 2. Integrieren Sie das Backup in DR und das BCP
- Schritt 3. Backup-Aufgaben automatisieren
- Schritt 4. Mechanismen für die Zugriffskontrolle implementieren
- Schritt 5. Backup-Daten und Tresor verschlüsseln
- Schritt 6: Backups mit unveränderlichem Speicher schützen
- Schritt 7. Implementieren Sie Backup-Überwachung und Warnmeldungen
- Schritt 8. Backup-Konfiguration überprüfen
- Schritt 9. Funktionen zur Datenwiederherstellung testen
- Schritt 10. Integrieren Sie Backups in Ihren Plan zur Reaktion auf Vorfälle

Schritt 1. Eine Backup-Strategie implementieren

Eine umfassende Backup-Strategie ist ein wesentlicher Bestandteil des Datenschutzplans einer Organisation, um etwaigen Auswirkungen eines Sicherheitsvorfalls standzuhalten, sie zu verringern und sich zu erholen. Erstellen Sie eine umfassende Backup-Strategie, die festlegt, welche Daten gesichert werden müssen, wie oft Daten gesichert werden müssen und wie Backup- und Wiederherstellungsaufgaben überwacht werden.

Wenn Sie eine umfassende Strategie für Backup und Wiederherstellung von Daten entwickeln, sollten Sie zunächst mögliche Unterbrechungen und deren potenzielle Auswirkungen auf das Geschäft identifizieren.

Ihr Ziel ist es, eine Wiederherstellungsstrategie zu entwickeln, die Ihren Workload wieder erhöht oder Ausfallzeiten innerhalb der akzeptablen Bereichs Ziele für die Wiederherstellung, Recovery Time Objective (RTO) und Recovery Point Objective (RPO) vermeidet. Das RTO ist die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Services. RPO ist die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Ziehen Sie eine detaillierte Backup-Strategie in Betracht, die alle folgenden Punkte umfasst:

- Kontinuierlicher Backup-Takt
- Point-in-Time Wiederherstellung (PITR)
- Wiederherstellung auf Dateiebene
- Wiederherstellung auf Anwendungsdatenebene
- Wiederherstellung auf Volume-Ebene
- Wiederherstellung auf Instance-Ebene

Ransomware

Eine gut durchdachte Backup-Strategie sollte Maßnahmen zum Schutz und zur Wiederherstellung Ihrer Ressourcen vor Ransomware enthalten, mit detaillierten Wiederherstellungsanforderungen für Ihre Anwendungen und deren Datenabhängigkeiten. Während Sie beispielsweise präventive und detektive Kontrollen einrichten, um das Risiko von Ransomware zu minimieren, stellen Sie sicher, dass Sie auch die angemessene Granularität für kontoübergreifende AWS-Region oder kontoübergreifende Kopier- und Wiederherstellungsmuster festlegen, um sicherzustellen, dass Administratoren nach dem Sicherheitsereignis keine beschädigten Backup-Daten wiederherstellen.

Anforderungen an die Aufbewahrung

In einigen Branchen müssen Sie bei der Entwicklung einer Backup-Strategie auch die Vorschriften für die Datenaufbewahrung berücksichtigen. Stellen Sie sicher, dass Ihre Backup-Strategie so konzipiert ist, dass sie ausreichend ist, um Ihre gesetzlichen Anforderungen für jede Datenklassifizierungsebene und jeden Ressourcentyp zu erfüllen.

Compliance

Lassen Sie sich von Ihren Sicherheits-Compliance-Teams beraten, ob Ihre Backup-Ressourcen und -Prozesse in den Geltungsbereich Ihrer Konformitäts-Programme aufgenommen oder aus diesem herausgenommen werden sollten. Wenn Sie Backup und Recovery als wichtigen Bestandteil Ihres Sicherheitsprogramms einbeziehen, können Sie besser verstehen, wo sich die Daten in Ihrer Umgebung befinden, und den Umfang der Einhaltung der Vorschriften entsprechend definieren.

Bewährte Architekturmethoden für die Entwicklung und den Betrieb zuverlässiger, sicherer, effizienter und kostengünstiger Workloads in der Cloud finden Sie unter Backup- und Wiederherstellungsansätze mit AWS und Reliability Pillar — AWS Well-Architected Framework.

Schritt 2. Integrieren Sie das Backup in DR und das BCP

Notfallwiederherstellung (DR) ist der Prozess der Vorbereitung auf eine Katastrophe, der Reaktion darauf und der Wiederherstellung nach einer Katastrophe. Der DR-Plan ist ein wichtiger Teil Ihrer Resilienzstrategie und befasst sich damit, wie Ihr Workload im Katastrophenfall reagiert. Eine Katastrophe kann ein technisches Versagen, eine menschliche Handlung oder ein Naturereignis sein. Der Plan zur Geschäftskontinuität (BCP) beschreibt, wie eine Organisation beabsichtigt, den normalen Geschäftsbetrieb während einer ungeplanten Unterbrechung fortzusetzen.

Ihr DR-Plan sollte Teil des BCP Ihrer Organisation sein. Das BCP sollte auch Verfahren enthalten. AWS Backup Ein Sicherheitsereignis, das sich auf Produktionsdaten auswirkt, kann es beispielsweise erforderlich machen, dass Sie einen DR-Plan aufrufen, der für ein Failover AWS Backup auf Backup-Daten von einem anderen System verwendet wird. AWS-Region Stellen Sie sicher, dass Ihre Mitarbeiter mit Ihren organisatorischen Abläufen vertraut sind und deren Anwendung AWS Backup geübt haben, damit Ihr Unternehmen im Notfall seinen normalen Betrieb ohne oder mit geringen Betriebsunterbrechungen fortsetzen kann. Weitere Informationen zur Verwendung AWS Backup finden Sie in anderen Abschnitten dieses Handbuchs.

Schritt 3. Backup-Aufgaben automatisieren

Die Backup-Pläne und Ressourcenzuweisungen Ihres Unternehmens sollten so konfiguriert werden, dass sie den Datenschutzrichtlinien Ihrer Organisation entsprechen. Durch Automatisierung und Bereitstellung von Backup-Richtlinien oder organisationsweiten Backup-Plänen können Sie Ihre Backup-Strategie standardisieren und skalieren. Mit AWS Organizations können Sie Backup-Richtlinien zentral automatisieren, um Backup-Aktivitäten über unterstützte AWS Backup-Ressourcen hinweg zu implementieren, zu konfigurieren, zu verwalten und zu steuern, indem Sie Backup-Vorgänge planen.

Um die Produktivität zu verbessern und den Infrastrukturbetrieb in Umgebungen mit mehreren Konten zu steuern, sollten Sie die Implementierung von Infrastructure-as-Code (IaC) und ereignisgesteuerter Architektur als wesentliche Bestandteile Ihrer digitalen Transformations- und Backup-Strategie in Betracht ziehen. Die Automatisierung von Backups bietet die folgenden Vorteile:

- Reduzierung des manuellen Aufwands, der durch die zeitaufwändige Konfiguration Ihrer Backups entsteht
- Minimierung des Fehlerrisikos
- Sorgt für Transparenz bei der Drifterkennung

- Verbessert die Einhaltung von Backup-Richtlinien für mehrere AWS Workloads oder Konten

Durch die Implementierung von Backup-Richtlinien als Code können Sie die Datenschutzbestimmungen wie folgt einhalten:

- Konfiguration verschiedener Anforderungen für Ihre Ressourcentypen
- Skalierung Ihrer Unternehmens-Datenschutzstrategie
- Implementierung von Lebenszyklusregeln, um festzulegen, wie lange es dauert, bis ein Recovery Point entweder in den Cold Storage übergeht oder gelöscht wird, wodurch Sie Ihre Kosten optimieren können

Bei der Automatisierung Ihrer Backup-Operationen können Sie die Optionen für die Ressourcenzuweisung skalieren, indem Sie mithilfe von AWS Tags und Ressourcen automatisch die AWS Ressourcen identifizieren, die Daten für Ihre geschäftskritischen Anwendungen speichern, und Ihre Daten mithilfe unveränderlicher Backups schützen. IDs Dies kann Ihnen helfen, Sicherheitskontrollen wie Zugriffsberechtigungen und Backup-Pläne oder Richtlinien zu priorisieren.

Schritt 4. Mechanismen für die Zugriffskontrolle implementieren

Wenn Sie über die Sicherheit in der Cloud nachdenken, sollte Ihre grundlegende Strategie mit einer starken Identitätsbasis beginnen, um sicherzustellen, dass ein Benutzer über die richtigen Berechtigungen für den Zugriff auf Daten verfügt. Angemessene Authentifizierung und Autorisierung können das Risiko von Sicherheitsereignissen minimieren. Das Modell der gemeinsamen Verantwortung sieht vor, dass AWS Kunden Richtlinien zur Zugriffskontrolle implementieren. Um Zugriffsrichtlinien in großem Umfang zu erstellen und zu verwalten, können Sie AWS Identity and Access Management (IAM) verwenden.

Setzen Sie bei der Konfiguration von Zugriffsrechten und Berechtigungen das Prinzip der geringsten Berechtigung um, indem Sie sicherstellen, dass jeder Benutzer oder jedes System, das auf Ihre Backupdaten oder den Tresorraum zugreift, nur die Berechtigungen erhält, die zur Erfüllung seiner Aufgaben erforderlich sind. Verwenden Sie AWS Backup es, um Zugriffsrichtlinien für Backup-Tresore festzulegen, um Ihre Cloud-Workloads zu schützen.

Durch die Implementierung von Zugriffskontrollrichtlinien können Sie Benutzern beispielsweise Zugriff auf die Erstellung von Backup-Plänen und On-Demand-Backups gewähren und gleichzeitig ihre Fähigkeit einschränken, Wiederherstellungspunkte zu löschen. Mithilfe von Richtlinien für

den Tresorzugriff können Sie je nach Ihren Geschäftsanforderungen einen Ziel-Backup-Tresor mit einer Quell AWS-Konto - oder IAM-Rolle teilen. Sie können auch Zugriffsrichtlinien verwenden, um einen Backup-Tresor mit einem oder mehreren Konten oder mit Ihrer gesamten Organisation in AWS Organizations gemeinsam zu nutzen. Weitere Informationen finden Sie in der AWS Backup - Dokumentation.

Wenn Sie Ihre Workloads skalieren oder dorthin migrieren AWS, müssen Sie möglicherweise die Berechtigungen für Ihre Backup-Tresore und Betriebsabläufe zentral verwalten. Verwenden Sie Richtlinien zur Dienststeuerung (SCPs), um eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für alle Konten in Ihrer Organisation zu implementieren. SCPs bieten umfassenden Schutz und stellen sicher, dass Ihre Benutzer die definierten Richtlinien für die Zugriffskontrolle einhalten. Weitere Informationen finden Sie unter Verwaltung des Zugriffs auf Backups mithilfe von Service-Kontrollrichtlinien mit AWS Backup.

Um Sicherheitsrisiken wie den unbeabsichtigten Zugriff auf Ihre Backup-Ressourcen und -Daten zu minimieren, verwenden Sie IAM Access Analyzer, um alle AWS Backup IAM-Rollen zu identifizieren, die mit den folgenden Personen gemeinsam genutzt werden:

- Eine externe Entität wie AWS-Konto
- Ein Root-Benutzer
- Ein IAM-Benutzer oder eine IAM-Rolle
- Ein Verbundbenutzer
- Ein AWS-Service
- Ein anonymer Benutzer
- Jede andere Entität, die zum Erstellen eines Filters verwendet werden könnte

Schritt 5. Backup-Daten und Tresor verschlüsseln

Organisationen müssen zunehmend ihre Datensicherheitsstrategie verbessern und müssen möglicherweise bei der Skalierung in der Cloud Datenschutzbestimmungen einhalten. Die korrekte Implementierung von Verschlüsselungsmethoden kann eine zusätzliche Schutzschicht über die grundlegenden Zugangskontrollmechanismen hinaus schaffen. Diese zusätzliche Ebene bietet Abschwächung für den Fall, dass Ihre primären Zugriffskontrollrichtlinien fehlschlagen.

Wenn Sie beispielsweise übermäßig freizügige Richtlinien zur Zugriffskontrolle auf Ihre AWS Backup -Daten konfigurieren, können Ihr Schlüsselverwaltungssystem oder -prozess die maximalen

Auswirkungen eines Sicherheitsereignisses abschwächen. Dies liegt daran, dass es separate Autorisierungsmechanismen für den Zugriff auf Ihre Daten und Ihren Verschlüsselungsschlüssel gibt, was bedeutet, dass die Backup-Daten nur als Chiffriertext sichtbar sind.

Um das Beste aus der AWS Cloud Verschlüsselung herauszuholen, verschlüsseln Sie Daten sowohl bei der Übertragung als auch bei der Speicherung. Um Daten während der Übertragung zu schützen, AWS verwendet veröffentlichte API-Aufrufe für den Zugriff AWS Backup über das Netzwerk mithilfe des TLS-Protokolls, um die Verschlüsselung zwischen Ihnen, Ihrer Anwendung und dem AWS Backup Dienst zu gewährleisten. Um Daten im Ruhezustand zu schützen, können Sie AWS Cloud-native AWS Key Management Service(AWS KMS) oder AWS CloudHSMverwenden. Ein cloudbasiertes Hardware-Sicherheitsmodell (HSM), AWS CloudHSM verwendet den Advanced Encryption Standard (AES) mit 256-Bit-Schlüsseln (AES-256), einen starken, in der Branche verwendeten Algorithmus zum Verschlüsseln von Daten. Prüfen Sie Ihre Datenverwaltung und Ihre regulatorischen Anforderungen und wählen Sie den geeigneten Verschlüsselungsservice für die Verschlüsselung Ihrer Cloud-Daten und Backup-Tresore aus.

Die Verschlüsselungskonfiguration unterscheidet sich je nach Ressourcentyp und Backup-Vorgängen zwischen Konten oder Regionen. Manche Ressourcentypen unterstützen die Möglichkeit zum Verschlüsseln Ihrer Backups mit einem separaten Verschlüsselungsschlüssel aus dem Schlüssel, der zur Verschlüsselung der Quellressource verwendet wurde. Da Sie für die Verwaltung der Zugriffskontrollen verantwortlich sind, um zu bestimmen, wer unter welchen Bedingungen auf Ihre AWS Backup Daten oder Tresorverschlüsselungsschlüssel zugreifen kann, sollten Sie die Richtliniensprache von verwenden, AWS KMS um Zugriffskontrollen für Schlüssel zu definieren. Sie können auch AWS Backup Audit Manager verwenden, um zu bestätigen, dass Ihr Backup ordnungsgemäß verschlüsselt ist. Weitere Informationen finden Sie unter Verschlüsselung während der Übertragung in AWS Backup.

Sie kännen AWS KMS-Schlüssel für mehrere Regionen verwenden, um Schlüssel von einer Region in eine andere zu replizieren. Schlüssel für mehrere Regionen wurden entwickelt, um das Verschlüsselungsmanagement zu vereinfachen, wenn Ihre verschlüsselten Daten zur Notfallwiederherstellung in andere Regionen kopiert werden müssen. Prüfen Sie, ob es notwendig ist, AWS KMS Schlüssel für mehrere Regionen als Teil Ihrer gesamten Backup-Strategie zu implementieren.

Schritt 6: Backups mit unveränderlichem Speicher schützen

Organisationen können unveränderlichen Speicher verwenden, um Daten in einen WORM-Status (Write Once Read Many) zu schreiben. In einem WORM-Status können Daten einmal

geschrieben und nach dem Festschreiben oder Schreiben auf das Speichermedium beliebig oft gelesen und verwendet werden. Unveränderlicher Speicher trägt dazu bei, die Integrität der Daten zu gewährleisten. Er bietet auch Schutz vor folgenden Bedrohungen:

- Löschvorgänge
- Überschreibungen
- Unbeabsichtigter und unbefugter Zugriff
- Gefährdung durch Ransomware

Unveränderlicher Speicher bietet einen effizienten Mechanismus zur Abwehr potenzieller Sicherheitsereignisse, die echte Auswirkungen auf Ihren Geschäftsbetrieb haben könnten.

In Kombination mit strengen SCP-Einschränkungen können Sie unveränderlichen Speicher für eine bessere Verwaltung verwenden. Sie können unveränderlichen Speicher auch in einem WORM-Konformitäts-Modus verwenden, wenn für die gesetzlichen Vorschriften (z. B. aufgrund einer gesetzlichen Aufbewahrungsfrist) der Zugriff auf unveränderliche Daten erforderlich ist.

Um die Verfügbarkeit und Integrität der Daten aufrechtzuerhalten, können Sie AWS Backup Vault Lock verwenden, um Ihre Backups zu schützen. Wenn Sie AWS Backup Vault Lock verwenden, können unbefugte Entitäten Ihre Kunden- oder Geschäftsdaten während des erforderlichen Aufbewahrungszeitraums nicht löschen, ändern oder beschädigen. AWS Backup Vault Lock hilft Ihnen dabei, die Datenschutzrichtlinien Ihres Unternehmens einzuhalten, indem es Folgendes verhindert:

- Löschungen durch privilegierte Benutzer (einschließlich des AWS-Konto Root-Benutzers)
- Änderungen an Ihren Backup-Lebenszyklus-Einstellungen
- Aktualisierungen, die Ihren definierten Aufbewahrungszeitraum ändern

AWS Backup Vault Lock gewährleistet Unveränderlichkeit und fügt eine zusätzliche Schutzebene hinzu, die Backups (Wiederherstellungspunkte) in Ihren Backup-Tresoren schützt. Dies ist besonders in stark regulierten Branchen nützlich, in denen strenge Integritätsanforderungen für Backups und Archive gelten. AWS Backup Vault Lock stellt sicher, dass Ihre Daten zusammen mit einer Sicherungskopie aufbewahrt werden, aus der Sie sie im Falle unbeabsichtigter oder böswilliger Aktionen wiederherstellen können.

⚠ Important

- AWS Backup Vault Lock wurde noch nicht auf seine Einhaltung der Regeln 17a-4 (f) der Securities and Exchange Commission (SEC) und der Commodity Futures Trading Commission (CFTC) in Regel 17 C.F.R. 1.31 (b) — (c) geprüft.
- AWS Backup Vault Lock wird sofort wirksam. Es gibt Ihnen eine Bedenkzeit von mindestens drei Tagen (72 Stunden), um die Konfiguration zu löschen oder zu aktualisieren, bevor Ihr Tresor dauerhaft gesperrt wird. Sie können die Dauer dieser Bedenkzeit optional verlängern. Nutzen Sie diese Bedenkzeit, um AWS Backup Vault Lock anhand Ihrer Workloads und Anwendungsfälle zu testen. Nach Ablauf Ihrer Bedenkzeit AWS Support können weder Sie noch Sie AWS Backup Vault Lock oder den Inhalt Ihres gesperrten Tresors löschen oder anderweitig ändern. Weitere Informationen finden Sie in der Dokumentation zu AWS Backup Vault Lock.

Schritt 7. Implementieren Sie Backup-Überwachung und Warnmeldungen

Backup-Aufgaben können fehlschlagen. Ein fehlgeschlagener Auftrag, z. B. eine Backup, Wiederherstellungs- oder Kopieraufgabe, kann sich auf nachfolgende Schritte in einem Prozess auswirken. Wenn die erste Backup-Aufgabe fehlschlägt, besteht eine hohe Wahrscheinlichkeit, dass auch andere nachfolgende Aufgaben fehlschlagen. In einem solchen Szenario können Sie den Verlauf der Ereignisse am besten anhand von Überwachung und Benachrichtigung nachvollziehen. Durch Überwachung und Warnmeldungen kann die Organisation über Ihre Backup-Aufgaben informiert werden, sodass Sie besser auf Backup-Ausfälle reagieren können.

Aktivierung und Konfiguration von Benachrichtigungen für Aufgaben für die Überwachung von AWS Backup bietet die folgenden Vorteile:

- Sie gibt Ihnen einen Überblick über Ihre Backup-Aktivitäten
- Hilft sicherzustellen, dass Sie wichtige Service Level Agreements einhalten () SLAs
- Verbessert Ihre Überwachung business-as-usual
- Hilft Ihnen bei der Einhaltung von Konformitäts-Verpflichtungen

Sie können die Backup-Überwachung für Ihre Workloads implementieren, indem Sie sie AWS Backup mit anderen Systemen AWS-Services und Ticketsystemen integrieren, um automatisierte Ermittlungs- und Eskalationsabläufe durchzuführen. Sie können z. B. Folgendes tun:

- Verwenden Sie Amazon, CloudWatch um Kennzahlen zu verfolgen, Alarme zu erstellen und Dashboards anzuzeigen.
- Verwenden Sie Amazon EventBridge, um AWS Backup Prozesse und Ereignisse zu überwachen.
- Benutzen Sie AWS CloudTrail, um AWS Backup -API-Aufrufe mit detaillierten Informationen zu Uhrzeit, Quell-IP, Benutzern und Konten, die diese Aufrufe ausführen, zu überwachen.
- Verwenden Sie Amazon Simple Notification Service (Amazon SNS), um AWS Backup verwandte Themen wie Sicherungs-, Wiederherstellungs- und Kopierereignisse zu abonnieren.

Sie können AWS Backup Audit Manager verwenden, um automatisch Nachweise für Ihre täglichen Backup-Auditberichte für jedes Konto und jede Region zu generieren. Sie können Ihre Backup-Überwachung auch auf mehrere Konten skalieren, indem Sie eine Reihe von Automatisierungsvorlagen und Dashboards (die so genannte Backup-Observer-Lösung) verwenden, um täglich aggregierte, kontenübergreifende Berichte für mehrere Regionen zu erhalten. AWS Backup

Schritt 8. Backup-Konfiguration überprüfen

Um sicherzustellen, dass das Backup-Programm ordnungsgemäß funktioniert, und um etwaige Anomalien bei Backup-Prozessen zu identifizieren und zu korrigieren, überprüfen Sie die Einhaltung der AWS Backup Richtlinien anhand definierter Kontrollen, wie z. B. der festgelegten Backup-Frequenz. Um Backup-Operationen oder Ressourcen zu finden und zu untersuchen, die nicht Ihren Geschäftsanforderungen entsprechen, können Sie Ihre Backup-Aktivitäten kontinuierlich und automatisch verfolgen und automatische Berichte erstellen.

AWS Backup Audit Manager bietet integrierte, anpassbare Compliance-Kontrollen, die auf Ihre geschäftlichen und behördlichen Anforderungen abgestimmt sind. Sie können vorgefertigte und anpassbare Kontrollen als Prüfungs-Frameworks zur Bewertung Ihrer AWS Backup -Praktiken verwenden. Die Kontrollen umfassen:

- Durch Backup-Pläne geschützte Backup-Ressourcen
- Mindesthäufigkeit und Mindestspeicherung des Backup-Plans
- Verschlüsselter Backup-Wiederherstellungspunkt

- Manuelles Löschen des Backup-Wiederherstellungspunkts
- Mindestaufbewahrungsdauer für Backup-Wiederherstellungspunkte
- Regionsübergreifedner COPY-Befehl
- Kontoübergreifend kopieren
- Backup-Tresorsperre

Für die Automatisierung von Infrastructure As-Code (IaC) können Sie AWS Backup Audit Manager mit verwenden. AWS CloudFormation

AWS Security Hub CSPMbietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus in. AWS Es hilft Ihnen auch dabei, Ihre Umgebung anhand bewährter Sicherheitsverfahren und Industriestandards zu überprüfen, wie z. B. Grundlegende Kontrollen für bewährte Sicherheitsmethoden von AWS. Wenn Sie Security Hub CSPM in Ihrer Cloud-Umgebung verwenden, empfehlen wir Ihnen, den Standard AWS Foundational Security Best Practices zu aktivieren, da er Erkennungskontrollen enthält, die bei der Sicherung von Backups helfen können. AWS Die meisten Detektivkontrollen in AWS Backup Audit Manager und Security Hub CSPM sind auch als AWS Config verwaltete Regeln verfügbar.

Schritt 9. Funktionen zur Datenwiederherstellung testen

Ihre Backup-Strategie muss das Testen Ihrer Backups beinhalten. Eine Backup-Strategie ist nicht wirksam, wenn gesicherte Daten nicht wiederhergestellt werden können. Testen Sie regelmäßig Ihre Fähigkeit, bestimmte Wiederherstellungspunkte zu finden und wiederherzustellen.

Die Tags AWS Backup werden zwar automatisch von den geschützten Ressourcen auf die Wiederherstellungspunkte kopiert, sie werden jedoch standardmäßig nicht von den Wiederherstellungspunkten auf die entsprechenden wiederhergestellten Ressourcen kopiert. Um Ihre Inventarverwaltung zu skalieren und Wiederherstellungspunkte zu lokalisieren, sollten Sie erwägen, AWS Backup Ereignisse zu verwenden, um eine Tag-Replikation für Ressourcen einzuleiten, die durch AWS Backup Wiederherstellungsaufträge erstellt wurden.

Sie können Ihren Datenwiederherstellungs-Workflow starten, indem Sie Datenwiederherstellungsmuster festlegen und diese dann regelmäßig testen. Um das Vertrauen in Ihre Fähigkeit zur Wiederherstellung von Backup-Daten zu stärken, sollten Sie einen grundlegenden, wiederholbaren Prozess für die Durchführung kontinuierlicher Datenwiederherstellungstests einrichten. Sie können beispielsweise ein Muster erstellen, um eine konten- und regionenübergreifende Wiederherstellung von einem zentralen DR-Backup-Depot, das

mit einem vom Kunden verwalteten AWS KMS -Schlüssel verschlüsselt ist, zu einem Quellkonto-Backup-Depot zu testen, das mit einem anderen vom Kunden verwalteten AWS KMS -Schlüssel verschlüsselt ist.

Wenn Sie solche Wiederherstellungsvorgänge nicht häufig testen, stellen Sie möglicherweise fest, dass Ihre Annahmen zur AWS KMS Verschlüsselung von konto- und regionsübergreifenden Vorgängen falsch sind. Oft ist das einzige Backup-Wiederherstellungsmuster, das tatsächlich funktioniert, der Pfad, den Sie häufig testen. Durch routinemäßige Tests der unterstützten Backup-Ressourcentypen können Sie Frühwarnungen erkennen, die möglicherweise zu zukünftigen Störungen und zum Verlust kritischer Daten führen könnten. Halten Sie nach Möglichkeit eine begrenzte, aber praktikable Anzahl von Wiederherstellungspfaden und -mustern bereit, um ungenutzten Speicherplatz zu vermeiden, Kosten zu optimieren und Zeit zu sparen. Das Problem zu beheben, wenn ein Wiederherstellungstest fehlschlägt, ist einfacher als der Verlust wertvoller oder kritischer Daten.

Schritt 10. Integrieren Sie Backups in Ihren Plan zur Reaktion auf Vorfälle

Simulationen zur Reaktion auf Sicherheitsvorfälle (SIRS) sind interne Ereignisse, die eine strukturierte Gelegenheit bieten, Ihren Plan und Ihre Verfahren zur Reaktion auf Vorfälle in einem realistischen Szenario zu üben. Es ist nützlich, Ihre Backup-Daten und -Operationen im Rahmen kreativer SIRS-Aktivitäten zu testen, um sich selbst mit Unerwartetem zu testen. Auf diese Weise können Sie überprüfen, ob Ihre Organisation bereit ist, und sich mit den seltenen und unerwarteten Situationen vertraut machen. Ihre Simulationen müssen realistisch sein und funktionsübergreifende Organisationsteams einbeziehen, die auf Ereignisse reagieren müssen.

Beginnen Sie mit grundlegenden Simulationsübungen und arbeiten Sie auf ein vollständiges, komplexes Ereignis hin. Sie können beispielsweise ein realistisches Modell erstellen, das aus einer Virtual Private Cloud (VPC) und zugehörigen Ressourcen besteht, die eine unbeabsichtigte Überoffenlegung von Informationen oder eine potenzielle Datenschutzverletzung simulieren, die durch Änderungen an Richtlinien und Zugriffskontrolllisten verursacht wird. Um zu beurteilen, wie gut Ihr Plan zur Reaktion auf Vorfälle funktioniert hat, dokumentieren Sie die gewonnenen Erkenntnisse und identifizieren Sie Verbesserungen, die an zukünftigen Reaktionsverfahren vorgenommen werden müssen.

Sie können AWS Backup damit automatische Backups auf Instanzebene als Amazon Machine Images (AMIs) und Backups auf Volume-Ebene als Snapshots über mehrere einrichten. AWS-

Konten Dies kann Ihrem Team zur Reaktion auf Vorfälle helfen, seine forensischen Prozesse zu verbessern, wie z. B. automatisierte forensische Festplattensammlung, durch die Bereitstellung eines Wiederherstellungspunkts, der den Umfang und die Auswirkungen potenzieller Sicherheitsereignisse wie Ransomware verringern könnte.

Nächste Schritte

In diesem Leitfaden wurden die 10 besten Sicherheitsmethoden und -kontrollen zum Schutz Ihrer Backup-Daten beschrieben AWS. Wir empfehlen, diese bewährten Methoden zu verwenden, um eine Backup- und Wiederherstellungsstrategie und -architektur mit mehreren Steuerebenen zu entwerfen und zu implementieren, die skalierbar ist und Ihre Geschäftsanforderungen erfüllt. Weitere Informationen zu AWS Backup finden Sie in der AWS Backup Dokumentation.

Wenn Sie Fragen zu diesem Leitfaden haben, starten Sie einen neuen Thread im AWS Backup-Forum oder kontaktieren Sie AWS Support.

Ressourcen

AWS Präskriptive Leitlinien

- Backup und Wiederherstellung in AWS (Anleitung)

AWS Dokumentation

- AWS Backup
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon EventBridge
- IAM
- AWS KMS
- AWS Organizations
- AWS Security Hub CSPM
- Amazon SNS

Blog-Posts

- Automatisieren Sie zentralisierte Backups in großem Umfang AWS-Services über AWS Backup
- Disaster Recovery (DR) -Architektur weiter AWS, Teil I: Strategien für die Wiederherstellung in der Cloud
- Die Bedeutung von Verschlüsselung und wie AWS sie helfen kann
- Verbessern Sie den Sicherheitsstatus Ihrer Backups mit AWS Backup Vault Lock
- Überwachung, Bewertung und Nachweis der Backup-Compliance mit AWS Backup Audit Manager
- Erstellen und teilen Sie verschlüsselte Backups über Konten und Regionen hinweg mit AWS Backup

- Vereinfachen Sie die Prüfung Ihrer Datenschutzrichtlinien mit AWS Backup Audit Manager
- Verwaltung des Zugriffs auf Backups mithilfe von Richtlinien zur Servicesteuerung mit AWS Backup
- Erhalten Sie täglich aggregierte, kontenübergreifende Berichte für mehrere Regionen AWS Backup

GitHub Repositorien

Die folgenden Code-Repositorys bieten Ihnen eine Verwaltungs- und Bereitstellungslösung für die Implementierung von Backup und Recovery AWS Backup in Ihrer gesamten AWS Organizations Organisation, die sich über mehrere Konten erstreckt und. AWS-Regionen

- Implementieren Sie mit AWS BackupAWS
- Implementieren AWS Backup Sie mithilfe von CI/CD-Pipelines

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	13. Mai 2022

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.