AWS Cloud-Sicherheits-Checkliste

Diese Checkliste hilft Ihnen, eine sichere und konforme Umgebung in AWS zu schaffen.

Durch die Umsetzung dieser Schritte stärken Sie Ihre Cloud-Sicherheitsstrategie, schützen sensible Daten und reduzieren das Risiko von unbefugtem Zugriff oder Sicherheitsverletzungen.

 # 1. Konto- und Identitätsmanagement

☐ Aktivieren Sie Multi-Faktor-Authentifizierung (MFA) für Root- und IAM-Benutzerkonten.
☐ Beschränken Sie die Nutzung des Root-Kontos; verwenden Sie es nur für wesentliche administrative Aufgaben.
☐ Erstellen Sie IAM-Rollen für administrative und servicebezogene Zugriffe anstelle von gemeinsam genutzten Anmeldedaten.
☐ Befolgen Sie das Prinzip der minimalen Rechtevergabe, indem Sie Benutzern und Rollen nur die nötigsten Berechtigungen zuweisen.
☐ Überprüfen und rotieren Sie regelmäßig IAM-Zugangsdaten, Zugriffsschlüssel und API-Schlüssel.
☐ Verwenden Sie AWS Identity Center (ehemals SSO) für eine zentrale Verwaltung von Benutzern und Rollen.

 # 2. Netzwerksicherheit

☐ Implementieren Sie eine Virtual Private Cloud (VPC) mit Subnetzen für isolierte Arbeitslasten.
☐ Verwenden Sie Sicherheitsgruppen und Netzwerk-Zugriffssteuerungslisten (NACLs), um eingehenden/ausgehenden Datenverkehr zu beschränken.
☐ Richten Sie Bastion Hosts für sicheren administrativen Zugriff ein.
☐ Erzwingen Sie Ende-zu-Ende-Verschlüsselung für alle Datenübertragungen mit HTTPS, VPNs oder privaten Links.
☐ Aktivieren Sie AWS Shield, um sich vor DDoS-Angriffen zu schützen.
☐ Überprüfen Sie regelmäßig offene Ports und IP-Bereiche in Sicherheitsgruppen, um die Angriffsfläche zu minimieren.

 # 3. Datenschutz

☐ Verschlüsseln Sie alle sensiblen Daten im Ruhezustand mit AWS Key Management Service (KMS).

☐ Aktivieren Sie die Verschlüsselung für S3-Buckets und beschränken Sie den öffentlichen Zugriff.
☐ Verwenden Sie CloudFront mit SSL-Zertifikaten, um die Inhaltsübertragung zu sichern.
☐ Sichern Sie kritische Daten regelmäßig mit AWS Backup oder Snapshots für die Notfallwiederherstellung.
☐ Aktivieren Sie Amazon Macie, um sensible Daten in AWS zu identifizieren und zu schützen.
☐ Stellen Sie sicher, dass Ihre Datenverarbeitungsrichtlinien und regulatorischen Anforderungen (z. B. DSGVO, PCI) eingehalten werden.

 # 4. Protokollierung und Überwachung

☐ Aktivieren Sie AWS CloudTrail, um API-Aufrufe zu protokollieren und Kontoaktivitäten zu überwachen.
☐ Verwenden Sie Amazon CloudWatch, um Alarme einzurichten und die Systemleistung zu überwachen.
☐ Aktivieren Sie AWS Config, um Ressourcen Konfigurationen zu verfolgen und zu prüfen.
☐ Konfigurieren Sie VPC Flow Logs, um Netzwerkverkehr zu erfassen und zu überwachen.
☐ Nutzen Sie AWS Guard Duty für kontinuierliche Bedrohungserkennung und Sicherheitsüberwachung.

 # 5. Anwendungssicherheit

☐ Verwenden Sie AWS Web Application Firewall (WAF), um sich vor gängigen Web-Schwachstellen zu schützen.
☐ Scannen Sie regelmäßig containerisierte Anwendungen mit Amazon Inspector oder Drittanbieter-Tools.
☐ Verwenden Sie AWS Secrets Manager, um Anwendungsgeheimnisse sicher zu speichern und zu verwalten.
☐ Implementieren Sie Sicherheit Best Practices in Ihrer CI/CD-Pipeline für automatisierte Deployments.

 # 6. Compliance und Governance

☐ Verwenden Sie AWS Organizations, um mehrere Konten mit zentralisierter Abrechnung und Governance zu verwalten.
☐ Aktivieren Sie Service Control Policies (SCPs), um Sicherheitsrichtlinien über Konten hinweg durchzusetzen.
☐ Führen Sie regelmäßig Sicherheitsbewertungen mit AWS Trusted Advisor oder Drittanbieter-Tools durch.
☐ Implementieren Sie Tagging-Strategien, um Ressourcen effektiv zu verfolgen und zu verwalten.
☐ Dokumentieren Sie Sicherheitskonfigurationen ordnungsgemäß für Compliance-Audits.

 # 7. Incident Response und Wiederherstellung

☐ Erstellen Sie einen Incident-Response-Plan, der auf Ihre AWS-Umgebung zugeschnitten ist.
☐ Testen Sie Ihre Notfallwiederherstellung Strategie mit AWS Backup oder Failover-Simulationen.
☐ Aktivieren Sie AWS Config Rules, um Fehlkonfigurationen zu erkennen und zu beheben.
☐ Verwenden Sie Amazon Detective, um potenzielle Sicherheitsvorfälle zu untersuchen und zu analysieren.

Brauchen Sie beim nächsten Schritt Hilfe?

Wenn Sie zu einem dieser Schritte eine Frage haben oder Hilfe beim Einrichten einer fortgeschritteneren oder maßgeschneiderten Lösung benötigen, sind wir für Sie da!

Senden Sie uns einfach eine E-Mail an contact@403bits.com.

Bei einfacheren Fragen geben wir Ihnen gerne Ratschläge oder weisen Sie in die richtige Richtung – kostenlos!

Und wenn Sie vor einer komplexeren Herausforderung stehen oder Zeit sparen möchten, können unsere Experten übernehmen und eine umfassende Einrichtung bereitstellen, die perfekt zu Ihren Anforderungen passt.

Wir sind hier, um Ihnen beim Aufbau von Sicherheit und Effizienz zu helfen, damit Sie sich auf das Wachstum Ihres Unternehmens konzentrieren können!

Wenn Ihnen diese Checkliste gefallen ist oder Sie Verbesserungsvorschläge haben, lassen Sie es uns unter contact@403bits.com wissen.