Cloud Security Assessment – Management Summary

Dieses Dokument fasst die Ergebnisse des Cloud Security Assessments zusammen. Es richtet sich an das Management und gibt einen Überblick über Risiken, Compliance-Bezug und empfohlene Maßnahmen.

1. Zentrale Ergebnisse

Bereich	Finding	Risiko
AWS S3 Buckets	Öffentliche Zugriffe entdeckt	Hoch
Azure IAM	Benutzer ohne MFA	Hoch
Netzwerksicherheit	Offene Ports (0.0.0.0/0) auf RDP	Hoch
Monitoring	CloudTrail / Azure Monitor nicht aktiv	Mittel
Verschlüsselung	Unverschlüsselte Datenbanken und Volumes	Mittel

2. Compliance Mapping

Die Findings wurden mit relevanten Standards abgeglichen:
- ISO/IEC 27017: Controls für Cloud Services
- NIST CSF: PR.AC (Access Control), PR.DS (Data Security), DE.CM (Continuous Monitoring)
- CIS Benchmarks: AWS Foundations, Azure Security Baseline
- GDPR: Art. 32 (Sicherheit der Verarbeitung)

3. Handlungsempfehlungen

- Aktivierung von MFA für alle Benutzerkonten.
- Block Public Access auf allen S3 Buckets und Blob Storage.
- Restriktive Security Group Regeln: keine 0.0.0.0/0 für kritische Ports.
- Zentralisiertes Logging aktivieren (CloudTrail, Azure Monitor).
- Standardmäßige Verschlüsselung aktivieren (KMS, Key Vault).