Incident-Response-Plan für ein cloudbasiertes Unternehmen

1. Vorbereitung

Schulung und Sensibilisierung: Regelmäßige Schulungen für Mitarbeiter zu Sicherheitsrichtlinien und Vorfallmeldungen.
Ressourcenzuweisung: Bestimmung eines Incident-Response-Teams (IRT) mit klaren Rollen und Verantwortlichkeiten.
Tools und Technologien: Implementierung von Sicherheitslösungen (z. B. SIEM, IDS/IPS) zur Überwachung und Erkennung von Vorfällen.

2. Identifikation

Überwachung: Kontinuierliche Überwachung von Systemen und Netzwerken auf verdächtige Aktivitäten.
Meldesystem: Einrichtung eines klaren Prozesses für Mitarbeiter, um Vorfälle zu melden (z. B. über ein Ticket-System).
Erste Analyse: Schnelle Bewertung der gemeldeten Vorfälle, um die Schwere und den Umfang zu bestimmen.

3. Eindämmung

Sofortige Maßnahmen: Sofortige Maßnahmen zur Eindämmung des Vorfalls (z. B. Trennung betroffener Systeme vom Netzwerk).
Kurzfristige Eindämmung: Implementierung von temporären Lösungen, um den Vorfall zu isolieren, während eine detaillierte Analyse durchgeführt wird.

4. Beseitigung

Ursachenanalyse: Identifikation der Ursachen des Vorfalls und der betroffenen Systeme.
Entfernung von Bedrohungen: Beseitigung von Malware, Schadhafter Software oder anderen Bedrohungen aus den betroffenen Systemen.
Systemwiederherstellung: Wiederherstellung der Systeme aus sicheren Backups, falls erforderlich.

5. Wiederherstellung

Systemüberprüfung: Überprüfung der Systeme auf Sicherheit und Integrität, bevor sie wieder in Betrieb genommen werden.
Monitoring: Fortlaufende Überwachung der Systeme nach der Wiederherstellung, um sicherzustellen, dass keine weiteren Vorfälle auftreten.

6. Nachbereitung

Dokumentation: Detaillierte Dokumentation des Vorfalls, der Reaktionen und der getroffenen Maßnahmen.
Analyse und Verbesserung: Durchführung einer Nachbesprechung, um den Vorfall zu analysieren und Verbesserungsmöglichkeiten zu identifizieren.
Aktualisierung des Plans: Anpassung des Incident Response Plans basierend auf den Erkenntnissen aus dem Vorfall.

7. Kommunikation

Interne Kommunikation: Informieren aller relevanten internen Stakeholder über den Vorfall und die ergriffenen Maßnahmen.
Externe Kommunikation: Gegebenenfalls Kommunikation mit Kunden, Partnernoder der Öffentlichkeit, um Transparenz zu gewährleisten und Vertrauen
zu erhalten.