Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

CSI-UMSETZUNGSMODELL

GO CLOUD GO SECURE

Phase 1: ANALYSIEREN

- Schritt 1: Verzeichnis der Cloud-Dienste
- Schritt 2: Risiken erfassen und zuordnen
- Schritt 3: Compliance

Phase 2: DEFINIEREN

- Schritt 4: Rollen und Verantwortlichkeiten
- Schritt 3: Kontrollziele festlegen
- Schritt 2: Risiken priorisieren
- Schritt 1: Richtlinien entwickeln

Phase 3: PLANEN

- Schritt 1: Maßnahmen zur Risikominderung
- Schritt 2: Kontrollen zuordnen
- Schritt 3: Dokumentation
- Schritt 4: Schulungsprogramm

Phase 4: UMSETZEN

- Schritt 2: Schulung und Sensibilisierung
- Schritt 1: Technische Maßnahmen

Phase 5: ÜBERPRÜFEN

- Schritt 1: Testen
- Schritt 2: Überwachen
- Schritt 3: Rückmeldung

Kofinanziert von der Europäischen Union

Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

CSI-UMSETZUNGSMODELL

GO CLOUD GO SECURE

Phase 1: ANALYSIEREN

Schritt 1: Verzeichnis der Cloud-Dienste

Erstellen Sie eine vollständige Übersicht über alle Cloud-Dienste, die in Ihrer Organisation genutzt werden. Vor der Bewertung ist es entscheidend zu wissen, welche Dienste im Einsatz sind und welche davon für den Betrieb besonders wichtig sind.

Schritt 2: Risiken erfassen und zuordnen

Die CSI-Matrix erfasst Bedrohungen, Schwachstellen und Risiken für jeden Cloud-Dienst und vermittelt so ein klares Bild der wichtigsten Schwachstellen Ihrer Organisation.

Schritt 3: Compliance

Prüfen Sie, ob Ihre Organisation die geltenden EU-Vorschriften und internationalen Standards einhält, um Geldbußen, Datenverluste und Reputationsschäden zu vermeiden. Einige Vorgaben verlangen konkrete Kontrollen wie die Protokollierung von Zugriffen, Verschlüsselung und die Meldung von Sicherheitsvorfällen.

Phase 2: DEFINIEREN

Schritt 1: Richtlinien entwickeln

Erarbeiten Sie eine Cloud-Sicherheitsrichtlinie, die Regeln für die sichere Nutzung von Cloud-Diensten, die Zugriffskontrolle und den Schutz von Daten festlegt. Sie bildet das Fundament Ihres Sicherheitsrahmens.

Schritt 2: Risiken priorisieren

Nutzen Sie die CSI-Matrix, um Risiken anhand ihrer Eintrittswahrscheinlichkeit und ihrer möglichen Auswirkungen zu bewerten. Konzentrieren Sie sich zunächst auf die dringendsten Risiken, um geeignete Maßnahmen zur Risikominderung festzulegen.

Schritt 3: Kontrollziele festlegen

Definieren Sie für jedes hoch priorisierte Risiko in der CSI-Matrix klare Ziele zur Risikominderung. So werden identifizierte Risiken in konkrete und passgenaue Maßnahmenpläne überführt.

Schritt 4: Rollen und Verantwortlichkeiten

Weisen Sie die Aufgaben eindeutig zu: Der Cloud-Administrator verwaltet die Plattformen, der Datenverantwortliche steuert den Zugriff auf Daten, der Sicherheitsbeauftragte übernimmt Überwachung und Vorfallmanagement und der Compliance-Verantwortliche stellt die Einhaltung regulatorischer Vorgaben sicher.

Phase 3: PLANEN

Schritt 1: Maßnahmen zur Risikominderung

Legen Sie für jedes hoch priorisierte Risiko in der CSI-Matrix konkrete und umsetzbare Maßnahmen fest. Dadurch wird eine schnelle und einheitliche Umsetzung unterstützt, insbesondere in KMU, die nicht über eigenes Sicherheitspersonal in Vollzeit verfügen.

Schritt 2: Kontrollen zuordnen

Erstellen Sie eine Zuordnungstabelle, in der die Maßnahmen zur Risikominderung mit den jeweiligen Cloud-Diensten verknüpft werden. So wird deutlich, was geschützt wird und wie die Kontrollen angewendet werden.

Schritt 3: Dokumentation

Bereiten Sie Vorlagen und Checklisten vor, beispielsweise Umsetzungschecklisten, Vorlagen für die Reaktion auf Sicherheitsvorfälle und Formulare zur Überprüfung von Audit-Protokollen. Diese Unterlagen unterstützen die Durchsetzung von Richtlinien, Audits und die kontinuierliche Verbesserung.

Schritt 4: Schulungsprogramm

Entwickeln Sie ein praxisnahes CSI-Schulungsprogramm, das Grundlagen der Cloud-Nutzung, zentrale Schwachstellen und Fehlkonfigurationen behandelt. Ziel ist es, Mitarbeitende wirksam zu schulen und einen großen Teil der Sicherheitsvorfälle in Cloud-Umgebungen zu vermeiden.

Kofinanziert von der Europäischen Union

Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

CSI-UMSETZUNGSMODELL

GO CLOUD GO SECURE

Phase 4: UMSETZEN

Setzen Sie die technischen Maßnahmen aus dem Fahrplan der Phase 3 um, zum Beispiel die Aktivierung der Multi-Faktor-Authentifizierung, Verschlüsselung, Richtlinien für Identitäts- und Zugriffsmanagement sowie rollenbasierte Zugriffskontrollen. Nutzen Sie dafür integrierte Werkzeuge wie AWS Config und Azure Security Center und beginnen Sie mit schnell umsetzbaren Maßnahmen wie MFA und RBAC.

Schritt 1: Technische Maßnahmen

Setzen Sie den in Phase 3 entwickelten Schulungsplan um. Nutzen Sie dabei die CSI-Matrix und die Schulungsunterlagen und arbeiten Sie mit kurzen, praxisorientierten Modulen, die an die technische Umgebung und das Risikoprofil Ihrer Organisation angepasst sind.

Schritt 2: Schulung und Sensibilisierung

Phase 5: ÜBERPRÜFEN

Schritt 1: Testen

Führen Sie Resilienztests in Form von Übungen, simulierten Angriffen, Kontrollprüfungen und Sicherheitsbewertungen durch. Damit wird überprüft, ob die Maßnahmen zur Risikominderung korrekt umgesetzt, wirksam und auf dem neuesten Stand sind und ob Ihre Organisation auf reale Bedrohungen vorbereitet ist.

Schritt 2: Überwachen

Legen Sie Kennzahlen fest, mit denen die Cloud-Sicherheit überwacht, Verbesserungen nachvollzogen und Risiken frühzeitig gesteuert werden können. Zu den wichtigen Kennzahlen gehören fehlgeschlagene Anmeldeversuche, Warnungen zu Fehlkonfigurationen und veraltete Sicherheitsupdates. Die Ergebnisse sollten in einem einfachen Kennzahlen-Dashboard dargestellt werden.

Schritt 3: Rückmeldung

Führen Sie ein Vorfallregister, in dem zu jedem Ereignis die Einzelheiten, Ursachen, Auswirkungen und Gegenmaßnahmen dokumentiert werden. Nutzen Sie diese Informationen, um Risikobewertungen zu aktualisieren, Richtlinien zu verbessern und Schulungsmaßnahmen anzupassen. So bleibt der Sicherheitsrahmen dynamisch und entwickelt sich laufend weiter.

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden.

Kofinanziert von der Europäischen Union