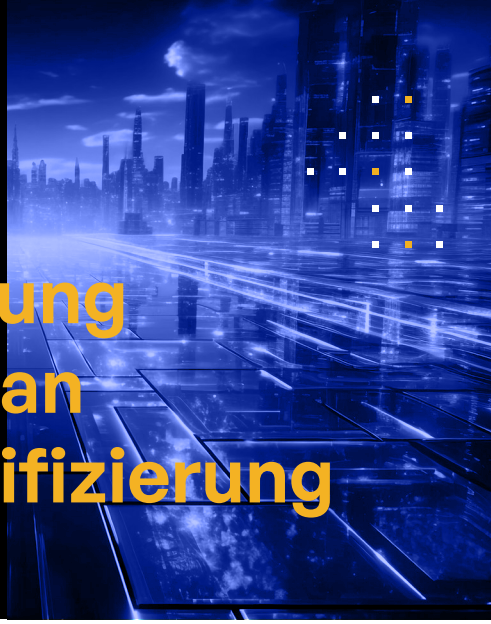
Kiteworks

Best Practices für die Erfüllung der CMMC-Anforderungen an Identifizierung und Authentifizierung



Die Einhaltung der CMMC-Vorschriften ist entscheidend für Unternehmen, die Verträge mit dem Verteidigungsministerium (DoD) sichern möchten. Die Umsetzung der folgenden Best Practices für die Benutzeridentifizierung und -authentifizierung im Rahmen der CMMC hilft Ihrem Unternehmen nicht nur, die strengen Anforderungen der CMMC effektiv zu erfüllen, sondern verbessert auch das gesamte Cybersicherheitsprofil Ihres Unternehmens.

- **1. Implementieren und Durchsetzen von eindeutigen Benutzer-IDs:** Weisen Sie jeder Person, die auf Ihre Systeme zugreift, eine eindeutige Benutzer-ID zu. Dies macht jeden Nutzer identifizierbar und verantwortlich für seine Handlungen innerhalb des Systems. Es ermöglicht Ihnen zu sehen und zu verfolgen, wer sich eingeloggt hat, welche Aktionen durchgeführt wurden und wann diese stattfanden.

- **2. Setzen Sie sichere Authentifizierungsmethoden ein:** Nutzen Sie fortschrittliche Verschlüsselungstechniken und Zwei-Faktor-Authentifizierung (2FA), um die Passwortsicherheit zu verstärken. Für die Biometrie verwenden Sie modernste Algorithmen und Hardware, um Identitäten genau zu verifizieren und gleichzeitig vor Spoofing und anderen Formen des biometrischen Betrugs zu schützen.

- **3. Verwalten von Benutzerzugriffsrechten:** Überprüfen und verwalten Sie regelmäßig die Benutzerzugriffsrechte, um sicherzustellen, dass Mitarbeiter nur den für ihre spezifischen Aufgaben erforderlichen Zugang haben. Eine effektive Verwaltung der Benutzerzugriffsrechte erfordert eine Kombination aus Durchsetzung von Richtlinien, automatisierten Tools und manuellen Überprüfungen.

- **4. Regelmäßige Aktualisierung von Passwörtern:** Implementieren Sie Richtlinien, die regelmäßige Aktualisierungen der Passwörter vorschreiben. Legen Sie Intervalle für Passwortänderungen fest, um das Risiko eines unbefugten Zugriffs zu minimieren. Stellen Sie außerdem sicher, dass die Passwörter den Komplexitätsanforderungen entsprechen und ermutigen Sie Mitarbeiter, Passphrasen oder eine Mischung aus nicht zusammenhängenden Wörtern und Zeichen zu verwenden.

- **5. Implementieren Sie kontinuierliches Monitoring:** Dokumentieren Sie systematisch, wer auf die Systeme zugreift und zu welchen spezifischen Zeiten, um ein klares und umfassendes Prüfprotokoll der Aktivitäten zu erstellen.

Best Practices für die Erfüllung der CMMC-Anforderungen an Identifizierung und Authentifizierung

- **6. Führen Sie regelmäßige Audits durch:** Überprüfen und bewerten Sie systematisch, wie gut Ihr Unternehmen Sicherheitsmaßnahmen zur Bestätigung der Identitäten von Anwendern und Systemen umsetzt. Identifizieren Sie anomales Verhalten wie unbefugte Zugriffsversuche oder Missbrauch von Anmeldeinformationen.

- **7. Schulen Sie Benutzer in Best Practices für Sicherheit:** Führen Sie regelmäßige Schulungen zur Sicherheitsbewusstsein durch, die die Bedeutung des Schutzes von Mitarbeiteranmeldedaten klar vermitteln. Behandeln Sie wesentliche Themen wie das Erstellen und Verwalten sicherer Passwörter, Techniken zur Identifizierung und Vermeidung von Phishing-Versuchen und andere entscheidende Sicherheitspraktiken.