Kiteworks

Best Practices für die Erfüllung der CMMC-Zugriffskontrollanforderungen

Zugriffskontrollen sind entscheidend für den Schutz sensibler Inhalte. Für die Anforderung der Zugriffskontrolle des CMMC 2.0 sollten Verteidigungsunternehmer diese Best Practices unbedingt berücksichtigen:

- **1. Implementierung der rollenbasierten Zugriffskontrolle (RBAC):** Organisieren Sie die Rollen in Ihrem Unternehmen nach spezifischen Aufgabenbereichen und verteilen Sie Zugriffsberechtigungen basierend auf diesen Rollen. Die rollenbasierte Zugriffskontrolle (RBAC) stellt sicher, dass Mitarbeitern nur die für ihre Aufgaben notwendigen Berechtigungen gewährt werden.

- **2. Mehrstufige Authentifizierung durchsetzen:** Die mehrstufige Authentifizierung (MFA) erfordert, dass Mitarbeiter mehr als eine Methode zur Identitätsverifizierung eingeben müssen, bevor ihnen der Zugang zu Systemen oder Daten gewährt wird. Dieser mehrschichtige Ansatz schafft zusätzliche, erhebliche Hürden für potenzielle Angreifer.

- **3. Führen Sie regelmäßige Zugriffsprüfungen durch:** Überwachen und überarbeiten Sie kontinuierlich Zugriffsberechtigungen, um sensible Daten zu schützen. Dieser Prozess beinhaltet die routinemäßige Überprüfung, wer Zugang zu bestimmten Informationen hat und sicherzustellen, dass nur diejenigen, die aktuell autorisiert sind, diese einsehen oder ändern können. Berechtigungen sollten entzogen werden, wenn Mitarbeiter keinen Zugriff auf Inhalte mehr benötigen.

- **4. Implementieren Sie Audit-Logs und Monitoring:** Führen Sie detaillierte Audit-Logs aller Zugriffsaktivitäten, die jede Instanz aufzeichnen, bei der Benutzer oder Systeme auf Ressourcen innerhalb einer Umgebung zugreifen. Diese Logs sollten Informationen wie Benutzer-ID, Zeitstempel, Zugriffsart (z.B. Anmeldung, Dateizugriff, vorgenommene Änderungen), Quell-IP-Adresse und alle weiteren relevanten Parameter enthalten, die bei der Identifizierung helfen können, wer was und wann getan hat.

- **5. Schulen Sie Mitarbeiter in Zugriffskontrollrichtlinien:** Regelmäßige Schulungseinheiten sollten sich auf verschiedene Arten von Zugriffskontrollen konzentrieren, wie physische, administrative und technische Kontrollen, und verstehen, wie sie diese in ihrer täglichen Arbeit anwenden können. Mitarbeiter sollten auch über die neuesten Bedrohungen informiert und darauf geschult werden, wie sie potenzielle Sicherheitsverletzungen erkennen und darauf reagieren können.