Berechtigungskonzept

Ein dokumentiertes und personifiziertes Berechtigungskonzept für IT-Systeme in Unternehmen ist unerlässlich, um die Sicherheit der (teilweise sensiblen) Informationen zu gewährleisten und unberechtigte Zugriffe auf diese zu verhindern. Es ermöglicht eine genaue Kontrolle darüber, wer Zugriff auf welche Informationen und Ressourcen hat und trägt damit zur Einhaltung von Datenschutzvorschriften und zur Minimierung von Sicherheitsrisiken bei. Durch die Definition klarer Zugriffsrechte wird auch die Effizienz gesteigert, indem den Beschäftigten die zur Erfüllung ihrer Aufgaben erforderlichen Werkzeuge und Informationen zur Verfügung gestellt werden, ohne die Systemsicherheit zu gefährden.

Rahmenbedingungen

Die Rechte werden in einem **geregelten und dokumentierten** Prozess vergeben. Dieser Prozess wird bei Einstellungen durch die Personalabteilung angestoßen. Dabei muss immer der jeweilige Laufwerks- oder Programmbesitzer die Zugriffsberechtigung in einem dokumentierten Prozess freigeben. Die IT-Abteilung richtet die Berechtigungen nach erfolgreichem Freigabeprozess ein.

Änderung und Löschung von Zugriffsberechtigungen erfolgen ebenfalls in einem **dokumentierten** Prozess. Hier kann jedoch neben der Personalabteilung auch eine Führungskraft die Änderung oder Löschung veranlassen.

Best Practices

- **Zero-Trust**: Grundsätzlich sollte niemand – ob User, App, Dienst oder Gerät – im ersten Schritt als vertrauenswürdig eingestuft werden und somit keinerlei Zugriffsrechte erhalten.
- **Need-to-know**: Zugriffsrechte dürfen nur auf der Grundlage des tatsächlichen Bedarfs erteilt werden. Personen dürfen nur auf die Informationen und Ressourcen zugreifen können, die sie für ihre Arbeit benötigen.
- **Role Based Access Control**: Definieren Sie klare Rollen innerhalb Ihrer Organisation und weisen Sie diesen Rollen spezifische Berechtigungen zu. Rollenbasierte Zugriffskontrolle erleichtert die Verwaltung von Berechtigungen.
- **Regelmäßige Überprüfung und Anpassung**: Berechtigungen sollten regelmäßig überprüft und angepasst werden, um sicherzustellen, dass sie noch den aktuellen Anforderungen entsprechen. Dazu gehört auch die Überprüfung inaktiver Konten und die Entfernung von Zugriffsrechten ehemaliger Beschäftigter sowie die Löschung der Benutzerkonten von ehemaligen Beschäftigten.
- **Transparente Dokumentation**: Alle Berechtigungen und Änderungen sollten dokumentiert und protokolliert werden. Dies ermöglicht die Nachvollziehbarkeit von Entscheidungen und erfüllt die Rechenschaftspflicht.

Prozessbeschreibung der Rechtevergabe