



OPTIMALE SICHERHEIT IM WELTWEITEN PRODUKTIVBETRIEB

CONSULTING-SERVICES FÜR SAP S/4HANA VON SPIRIT/21

KUNDENPROFIL

BRANCHE	Fertigungsindustrie
MITARBEITERZAHL	> 35.000
UMSATZ	> 5 Mrd. Euro

Die Daten eines Unternehmens sind heute oft sein wichtigstes Kapital. Je größer die Organisation, je verschachtelter die Strukturen, desto wichtiger sind klare Zugangsberechtigungen.

Aber auch bei mittleren und kleinen Unternehmen wird das Thema Datensicherheit immer wichtiger.

Auch hier steigt die Menge der sensiblen Daten stetig und somit auch die Notwendigkeit eines Sicherheitskonzepts, das die jeweiligen Anforderungen optimal erfüllt.

HERAUSFORDERUNG

Sicherheit, Flexibilität und Geschwindigkeit – diese drei Ziele gleichzeitig zu erreichen, gelingt nur in den seltensten Fällen.

Die Einführung und kontinuierliche Aktualisierung von Berechtigungen ist schon in einem klassischen SAP-System nicht zu unterschätzen. Die Konzeption und Umsetzung klarer Berechtigungsstrukturen mit SAP S/4HANA ist dagegen nochmals eine weit anspruchsvollere Herausforderung.

Bei einem Wechsel zu SAP S/4HANA werden nicht mehr alle altbekannten transaktionsbezogenen Berechtigungen vorhanden sein. Gleichzeitig wird SAP S/4HANA um die Möglichkeiten der APP-basierten Berechtigungen erweitert.

Somit muss in einem zukunftssträchtigen Berechtigungskonzept eine Kombination aus alten transaktionellen Berechtigungen und den neuen APP-Berechtigungen geschaffen werden.

ANALYSE

Zunächst muss grundsätzlich festgelegt werden, welche Unternehmensbereiche mit welchen Berechtigungskonzepten arbeiten. Außerdem stellt sich gleich zu Beginn die wichtige Frage, ob und gegebenenfalls wo es Gefährdungspotenziale gibt.

In einer umfassenden Analyse können Spezialisten von **SPIRIT/21** den Ist-Zustand ermitteln. Folgende Fragestellungen bilden dabei die Basis:

- Welche Gültigkeitsbereiche müssen die Berechtigungen abdecken – national und international?
- Sind länderspezifische Anforderungen zu berücksichtigen?
- Welche Arbeitsbereiche müssen mit welcher Berechtigungstiefe abgedeckt werden?
- Wie teilen sich die Berechtigungen auf? Welche sind als transaktionale Berechtigungen und welche nur noch als APP-Berechtigungen vorhanden?
- Sind alle technischen Anforderungen für die APP-Berechtigungen erfüllt? Z.B. Frontend-System mit Anbindung an das Backend-System, Einrichten der UI2-OData-Services, Zugang zum SAP FIORI Launchpad usw.
- Können alle Anforderungen mit SAP Standardmitteln erfüllt werden oder sind zusätzliche Tools nötig?
- Soll das Konzept einem Template-Ansatz folgen?

UMSETZUNG

Um die im Konzept festgelegten Kombinationen der unterschiedlichen Berechtigungen zu designen, müssen im ersten Schritt alle technischen Anbindungen erfolgt sein. Wenn diese vorhanden sind, können die transaktionsbasierten Berechtigungen wie bisher in Rollen zusammengefasst werden.

Um diese mit den neuen APP-basierten Berechtigungen zu ergänzen, müssen die Zugänge zum SAP FIORI Launchpad zur Verfügung gestellt werden.

Nun können über die von SAP ausgelieferten oder selbst designten APP-Kataloge und Gruppen auch zu den neuen APP-basierten Berechtigungen Rollen erstellt werden. Diese Rollen haben dabei nichts mit den bisher bekannten Rollen in den transaktionalen Berechtigungen zu tun!

Um den Anwendern diese neuen Rollen zur Verfügung stellen zu können, müssen die Berechtigungen anschließend gepflegt und geprüft werden.

Im letzten Schritt wird ein umfassender Test der vergebenen Berechtigungen durchgeführt. Dieser sollte als letzte Prüfung zur Sicherheit auch einen ‚Negativ-Test‘ umfassen – d.h. die Kontrolle, dass nicht zu viele Berechtigungen vergeben wurden.

VORTEILE

Mit diesem Vorgehen erhalten Sie ein für Systemprüfungen wichtiges und umfassendes Konzept der neuen Berechtigungskombinationen. Auch der Berechtigungsumfang ist hierbei dokumentiert und kann zu Prüfzwecken stets weitergeschrieben werden. Damit haben Sie ein zentrales und somit gut zu steuerndes Berechtigungswesen.