AUDI AG

Bereinigung von RFC-Schnittstellen - Berechtigungen mit System

Mit einem automatisierten Werkzeug des SAP-Partners Xiting hat die AUDI AG die Berechtigungen von mehr als 500 Schnittstellen einer komplexen SAP-Systemlandschaft überprüft und so potenzielle Sicherheitslücken geschlossen – ohne Unterbrechung des laufenden Betriebs.

AUF EINEN BLICK

Unternehmen

- Name: AUDI AG
- Standort: Ingolstadt
- Branche: Automotive
- Produkte und Services: Automobile
- Umsatz: EUR 48.7 Mrd
- Angestellte: 63,800
- Internetadresse: www.audi.com
- Genutzte Xiting-Lösungen:
  Xiting Authorizations Management Suite (XAMS)
- Partner: SAP Consulting

Projektziele

- Minimierung der Angriffsrisiken auf RFC-Schnittstellen
- Resourcenoptimierung
- Bereinigung und Neuberechtigung von über 500 RFC-Schnittstellen

Herausforderungen

- Garantierter und sicherer Go-Live
- Keine Unterbrechung des laufenden Betriebs

SAP-Systeme im Projekt-Scope:

- ERP, HR, CRM, BW, SOLMAN

Highlights

- Durchführung des gesamten Projekts in nur 3 Monaten
- Analyse und Neuberechtigung im laufenden Betrieb
- Automatisiertes Werkzeug
- Kein Performance-Verlust
- Permanentes Monitoring möglich

Unternehmensnutzen:

- IKS-konforme Berechtigung der RFC-Schnittstellen
- Mehr Produktivität durch unterbrechungsfreies Arbeiten
- Basis für sichere RFC-Schnittstellenverwaltung

Xiting GmbH
Obere Ringstraße 17
79859 Schluchsee
Deutschland
Tel.: +49 7656 98881-55
Fax: +49 2861 95882-95
E-Mail: info@xiting.de

Xiting AG
Chüchelacherstrasse 5
8165 Schöfflisdorf
Schweiz
Tel.: +41 43422 8803
Fax: +41 43422 8793
E-Mail: info@xiting.ch

AUDI AG Bereinigung von RFC-Schnittstellen - Berechtigungen mit System

SAP-Landschaften kommunizieren in aller Regel über RFC-Schnittstellen. Doch welche Daten dürfen über eine Schnittstelle transportiert werden? Von woher nach wohin darf sie zugreifen? Und warum liegt in diesen einfachen Fragen Zündstoff? „Komplexe SAP-Landschaften, in denen mehrere Lösungen über viele RFC-Schnittstellen verbunden sind, bergen Risiken“, weiß Patrick Bockel vom SAP-Partner Xiting. Denn: „RFC-Schnittstellen mit zu starken Berechtigungen machen Missbrauch möglich – wenn zum Beispiel ERP-Anwender in die HR-Lösung gelangen und dort die Löhne ihrer Kollegen einsehen können.“

Kleine Fehler bei der Bereinigung …

Der langjährige SAP-Kunde Audi ist sich dieser Problematik bewusst. Der Automobilhersteller betreibt mehrere SAP-Systemlandschaften, etwa für ERP, Personalmanagement, Kundenbeziehungsmanagement, Business Warehousing, und nutzt zudem die Lösung zur Anwendungsverwaltung SAP Solution Manager. „Diese SAP-Systeme und auch diverse Nicht-SAP-Lösungen sind über mehr als 500 RFC-Schnittstellen miteinander verbunden, die bis vor Kurzem zu stark berechtigt waren“, schildert Dieter Krebs, IT-Projektleiter bei Audi.

Um das Geflecht von RFC-Berechtigungen zu prüfen und ohne Unterbrechung des laufenden Betriebs zu korrigieren, hat Xiting zusammen mit den Organisationen SAP Consulting und SAP Active Global Support einen speziellen Service etabliert, auf den im SAP-Hinweis 1682316 explizit aufmerksam gemacht wird. „Eine Bereinigung der Berechtigungen von ca. 500 Schnittstellen wie bei Audi kann ohne Risiken für den laufenden Betrieb nur mit einem automatisierten Werkzeug konsistent durchgeführt werden“, erklärt Patrick Bockel.

… können große Folgen haben

Denn wird nur eine Schnittstelle vergessen, kann diese potenziell von einer hohen Anzahl von Anwendern missbraucht werden – auch von externen Zulieferern, wie sie in der Automobilbranche üblich sind. Stellt andererseits eine Schnittstelle die Arbeit ein, weil ihr zu viele Berechtigungen entzogen wurden, kann das dazu führen, dass Folgeverarbeitungen nicht mehr möglich sind. Bezogen auf einen Automobilhersteller bedeutet das im schlimmsten Fall, dass die Just-in-time-Lieferung nicht mehr funktioniert – und die Bandstraßen in der Produktion zum Stillstand kommen.

„Selbst wenn es zu kleinen Fehlern bei der Bereinigung von Schnittstellen kommt, kann das also Millionenkosten zur Folge haben. Dieses Risiko wollten wir nicht eingehen“, sagt Dieter Krebs von Audi – und hat sich aus diesem Grund wie viele andere Kunden für den Service von Xiting entschieden.

„Zunächst nehmen wir in einem eintägigen Workshop den Status quo der Schnittstellenlandschaft beim Kunden auf“, erläutert Patrick Bockel die Vorgehensweise. Anschließend werden die sogenannten Schnittstellenbenutzer benannt: Welche Schnittstellen aus welchen Vorsystemen greifen auf die gerade untersuchte Schnittstelle zu? Diese Benutzer werden dann nach ihrem Kontext gruppiert: Greifen sie HR-Daten ab oder Finanzinformationen? „Aus diesen Informationen erstellen wir dann eine Matrix, der zu entnehmen ist, welche Schnittstelle welche Rechte benötigt und was an Benutzern zu bereinigen ist.“

Sicherheit durch automatisiertes Monitoring

„Um Fehler jeder Art auszuschließen, ist bei der dann anstehenden Neuberechtigung der Schnittstellen eine automatisierte, technische Vorgehensweise enorm wichtig“, so Bockel weiter. Zunächst laufen alle Schnittstellen mit ihren alten Berechtigungen weiter. Parallel dazu wird die Xiting Authorizations Management Suite (XAMS) installiert, die auf jeder Schnittstelle einen Agenten laufen lässt – für einen Beobachtungszeitraum von rund drei Monaten.

„Mit unserer XAMS zeichnen wir zum einen auf, welche RFC-Aufrufe eingehen und wie der Kontext lautet. Daraus erstellen wir eine Rolle, die die notwendigen RFC-Berechtigungen enthält. Anschließend überprüft ein Agent, ob diese Berechtigungen auch tatsächlich ausreichen.“ Erst wenn die XAMS im laufenden Betrieb die Querverbindungen und Berechtigungen aller Schnittstellen automatisiert überprüft und wenn nötig korrigiert hat, werden die neuen Berechtigungen live geschaltet.

Drei Tage Workshop in der Vorphase, drei Monate Agentenmonitoring, dann das Go-live – bei Audi lief alles wie aus dem Lehrbuch: „Die 500 Verbindungen wurden sauber neu berechtigt, ohne Störung des laufenden Betriebs – aus unserer Sicht ein gelungenes Projekt“, bilanziert Audi-Projektleiter Krebs. „Ohne automatisierte Werkzeuge wie die Xiting Authorizations Management Suite lassen sich solche Bereinigungsprojekte nicht ohne Risiken durchführen“, schließt Patrick Bockel von Xiting. „Daher haben sich bisher all unsere Kunden dazu entschlossen, die Suite nach Durchführung des jeweiligen Projekts zu behalten und voll zu lizenzieren.“ Denn das gibt den Unternehmen die Möglichkeit, neben den Schnittstellen kontinuierlich auch alle Hintergrundbenutzer (BTCH) und Dialogbenutzer zu bereinigen und so Missbrauchsfällen dauerhaft vorzubeugen.