JOST-Werke

Erfolgreiche Etablierung eines internen Kontrollsystems (IKS) für das SAP-Berechtigungswesen

Die dauerhafte Nutzung temporär vergebener SAP-Berechtigungen und kritische Berechtigungskombinationen soll es bei den JOST-Werken nicht mehr geben. Das für die SAP-Basis verantwortliche Team hat ein internes Kontrollsystem etabliert, das in regelmäßigen Reviews mit Fachabteilungsverantwortlichen das Berechtigungswesen kritisch hinterfragt und Wildwuchs vermeiden soll: temporäre Berechtigungen werden rückgängig gemacht, Rollen bereinigt und SAP-Berechtigungen auf das für die Arbeit Notwendige reduziert.

Der Nutzen

- 80% Zeitersparnis im Vergleich zur manuellen Erstellung und Pflege der Regelwerke
- 95% Zeitersparnis für die Realisierung der Compliance-Anforderungen
- 90% Zeitersparnis für die Erstellung der detaillierten Prüfungsberichte

Die hierzu benötigten Hinweise zum Klärungsbedarf bekommt das Basis-Team der JOST-Werke unter anderem aus einer Softwarelösung namens „CheckAud®“: Mit ihr kann das Berechtigungssystem jederzeit in Echtzeit gegen rund 2.500 vorgefertigte und selbst erstellte Prüfabfragen validiert werden. Reports enthalten ein Dashboard mit Risiko-Scores für jeden Prüfbereich und für das SAP-Gesamtsystem, eine Übersicht der vergebenen SAP-Berechtigungen und detaillierte Beschreibungen betriebswirtschaftlicher, handelsrechtlicher, IT-sicherheitsspezifischer und datenschutzrechtlicher Risiken.

IBS Schreiber GmbH • Zirkusweg 1 • 20359 Hamburg • Tel: +49 40 69 69 85-82 • www.ibs-schreiber.de • kontakt@ibs-schreiber.de

SAP-Berechtigungswesen schon immer ernst genommen

„Wir sind 2014 mit einem soliden SAP-Berechtigungswesen gestartet, haben es regelmäßig aktualisiert und hatten somit keine kritische Situation. Trotzdem wollten wir unser Berechtigungswesen handhabbarer machen, um veränderten Unternehmensstrukturen, internationalem Wachstum und steigenden Compliance-Anforderungen Rechnung zu tragen“, erläutert Sandeep Sheth, einer der SAP-Basisverantwortlichen bei den JOST-Werken. Gemeinsam mit seiner Kollegin Nurgul Omorova-Obst konzipierte er ein internes Kontrollsystem (IKS), um permanent über das Sicherheitsniveau des SAP-Berechtigungswesens aussagefähig und compliant zu sein.

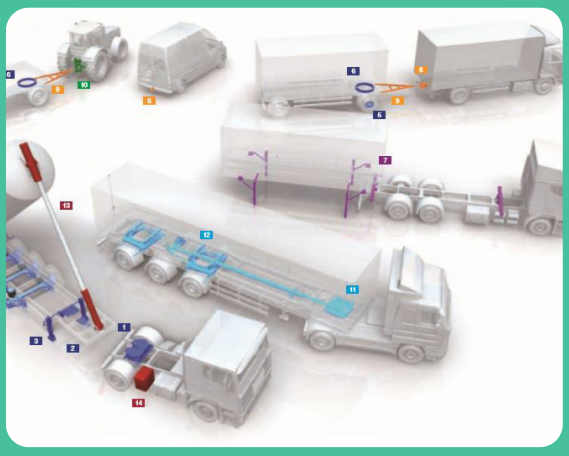
Gefahr des Wildwuchses und permanent steigenden Berechtigungen

In IT-Systemen ist es typisch, dass Mitarbeiter über die Zeit mehr Berechtigungen haben, als sie für ihre Arbeit benötigen. Es wird beispielsweise vergessen, temporäre Berechtigungen wieder zurückzunehmen oder beim Abteilungs- oder Zuständigkeitswechsel nicht mehr benötigte Rechte zu entziehen. Für besondere Aufgaben erhalten Mitarbeiter Berechtigungen für individuelle SAP-Transaktionen — und wenn man nicht aufpasst, darf mit der Zeit fast jeder fast alles. Durch derartigen Wildwuchs können erhebliche Sicherheits- und Compliance-Risiken entstehen. Aber die JOST-Werke passen auf: „Mit regelmäßigen Reviews beugen wir Wildwuchs vor. Verantwortliche aus Fachabteilung und IT bewerten gemeinsam, ob Rollen und Mitarbeiter noch passend sind oder zu weitreichende Berechtigungen existieren.“ Wo konkreter Handlungsbedarf besteht, erfahren die Experten aus Reports der Softwarelösung CheckAud®, die von den Hamburger Sicherheitsexperten IBS Schreiber entwickelt wird.

Sicherheitsprüfung bei Vergabe von Rollen und Berechtigungen

„Im Tagesgeschäft brauchen wir ständige Transparenz, weil bereits kleine Änderungen große Auswirkungen auf die Compliance haben können“, meint Nurgul Omorova-Obst und ergänzt: „Bei Änderungen an Rollen und Rechten prüfen wir, ob wir sicherheitsrelevante Aspekte übersehen haben.“ Die CheckAud®-Lösung wird im Tagesgeschäft zur Direktprüfung bei der Vergabe und der Administration von Berechtigungen und Rollen eingesetzt, um sicherzustellen, dass das Berechtigungssystem compliant bleibt.

Nurgul Omorova-Obst und Sandeep Sheth, Teamleiter SAP-Basis



Produktportfolio der JOST-Werke

Komplexes Sicherheitskonzept manuell schwer wartbar

„Die wachsende Konzerngröße, die steigende Anzahl der weltweiten SAP-Nutzer und zusätzliche Compliance-Anforderungen seit dem Börsengang 2017 sind weitere Argumente für zusätzliche Optimierungen und die Softwarenutzung im Bereich der SAP-Basisadministration“, sagt Sandeep Sheth. Er ergänzt: „Manuell lässt sich ein derartig komplexes Konstrukt kaum noch durchschauen, und unsere Prüfsoftware hilft bei der Priorisierung der wichtigsten Aufgaben.“ Kritische Bereiche lassen sich damit thematisieren, analysieren und Konflikte bereinigen. Das geschieht natürlich permanent und nicht erst, wenn eine Revision oder Audit ansteht.

CheckAud® erkennt Sicherheitsrisiken und kritische Kombinationen

„Im Vergabeprozess für SAP-Rollen und SAP-Berechtigungen können wir heute besser einschätzen, ob es Risikopotenziale gibt", ergänzt Nurgul Omorova-Obst. CheckAud® wird mit Standard-Regelwerken und über 2.500 Prüfabfragen ausgeliefert. DSAG-Prüfleitfaden, DSAG-Datenschutzleitfaden, HGB-, DSGVO- und andere gesetzlich verbindliche Vorgaben werden damit abgedeckt. Alleine rund 280 Prüfabfragen beziehen sich übrigens auf kritische Berechtigungskombinationen (SoD / Segregation of Duties), u.a. in Purchase-to-Pay und Order-to-Cash Prozessen. Die Standardregelwerke werden halbjährlich von IBS Schreiber aktualisiert. Zusätzlich können kundenindividuelle Regelwerke genutzt werden, um die eigenen Compliance-Richtlinien abzubilden, diese bei Änderungen anzupassen und regelmäßig alle SAP-Systemeinstellungen und Systemparameter automatisch dahingehend zu prüfen. Die Wirtschaftsprüfer beurteilen das entstandene interne Kontrollsystem nach Angaben der JOST-Werke positiv – sicher auch, weil sie auf Knopfdruck die SAP-Landschaft scannen, eine Risikobewertung und eine Dokumentation der Änderungen seit dem letzten Audit bekommen können.

Nur geringe Unterstützung durch den Hersteller notwendig

IBS Schreiber unterstützte das SAP-Basisteam bei der Tooleinführung und in der Probephase. Seitdem nutzen die JOST-Werke das Tool weitestgehend ohne Support. Aktuell ist IBS Schreiber mit der Aktualisierung des Berechtigungskonzepts beauftragt, auch hierbei kommt das Tool zum Einsatz.„Man sollte Rollen und Berechtigungen schon auf Sicherheit und Compliance prüfen, bevor sie in die Produktivsysteme gelangen. Damit erreicht man von Anfang an das Ziel von gesetzeskonformen und konfliktfreien Rollen", erläutert Lisa Niekamp, Head of Direct Sales vom Hersteller IBS Schreiber.

Fazit

„Die Vergabeprozesse unternehmensweit bekannt und für die Mitarbeiter verständlich zu machen, kostet in einer weltweit verteilten Organisation viel Aufwand. Umso wichtiger ist es, im Tagesgeschäft und systemseitig reibungslose und sichere Prozesse zu haben", fasst Sandeep Sheth zusammen. Er sieht für die JOST-Werke die Unterstützung bei der sicheren Vergabe und Dokumentation von Berechtigungen und die schnelle Prüfbarkeit eines Berechtigungskonzepts mit entsprechendem Risiko-Reporting als Hauptvorteile der CheckAud®-Lösung. Letzteres stellt einen wichtigen Grundpfeiler für den Aufbau des internen Kontrollsystems für die SAP-Sicherheit dar.