

SAP Customer Success Story SAP Governance, Risk und Compliance



„Der Einsatz der SAP-Lösung für die Zugriffs- und Berechtigungssteuerung erhöht unsere IT-Sicherheit: Wir schließen Überwachungslücken, können die Bestimmungen zur Funktionstrennung besser gewährleisten und Risiken minimieren.“

Jörg Hahne, Director IT, Johnson Controls Power Solutions Europe

AUF EINEN BLICK

Unternehmen

- Name: Johnson Controls Power Solutions Europe
- Standort: Hannover
- Branche: Automotive
- Geschäftsfelder: Herstellung und Vertrieb von Batterien für Autos, Nutzfahrzeuge, Motorräder, elektrische Hybridfahrzeuge und Boote
- Umsatz: 1,1 Mrd. Euro
- Mitarbeiter: 3.500
- Internetadresse: www.jci.com
- Partner: Hans-Joachim Gaebert, Unternehmensberatung für IT-Sicherheit und IT-Revision (Hamburg)

Die wichtigste Herausforderung

Umsetzung von Compliance-Anforderungen im SAP-Berechtigungskonzept

Projektziele

- Evaluierung, Test und Realisierung von Zugriffsregeln und Berechtigungen für ein zentrales SAP-System mit ca. 1.000 Benutzern an verschiedenen Standorten in mehreren europäischen Ländern
- Identifizierung von Funktionstrennungs-Risiken (SoD) und deren Minimierung bzw. Vermeidung
- Einrichtung regelmäßiger Überprüfungen zur Sicherstellung eines Compliance-konformen IT-Betriebs

Lösungen und Services

SAP GRC Access Control, Teil der SAP-Lösungen für Governance, Risk und Compliance

Highlights der Implementierung

Umsetzung des Projektes in den Schritten Risikoerkennung, Regelaufstellung, Risikoanalyse, -vermeidung, und -reduzierung sowie Implementierung kontinuierlicher Audits

Entscheidung für SAP

- Einbindung in vorhandene SAP-Landschaft
- Überzeugende Funktionalität
- Zukunftssicherheit

Hauptnutzen für den Kunden

- Minimierung und Ausschaltung von Risiken hinsichtlich von Manipulation und Betrug auf Benutzerebene
- Präventive Simulation von Risiken
- Vermeidung potenzieller Risiken durch Funktionstrennung
- Automatisierte Kontrollen
- Zeitnahe Auswertungen über den Status von Risiken und mögliche Verletzungen
- SOX-gemäßer Schutz der Integrität von Finanzdaten
- Abnahme der Ergebnisse durch Wirtschaftsprüfer
- Verbesserung der gesamten IT-Sicherheit

Vorhandene Systemlandschaft

SAP-Anwendungen für alle Anwendungsbereiche außer Personalwesen

Integration von Nicht-SAP-Produkten

- Hardware: Hewlett Packard
- Betriebssystem: HP-UX 11i

JOHNSON CONTROLS POWER SOLUTIONS EUROPE

Mehr IT-Sicherheit durch Umsetzung eines Berechtigungskonzepts für 1.000 SAP®-Anwender in Europa

Mobile Energiequellen

Ob kräftige Startkraft für Auto und Lastwagen verlangt ist oder zuverlässige Energieversorgung auf Booten und Yachten: Wo immer mobile Energie benötigt wird, kommen Batterien von Johnson Controls Power Solutions zum Einsatz. Das mit dem Hauptsitz in Hannover ansässige Unternehmen ist das europäische Standbein von Johnson Controls, einem global tätigen US-Konzern mit über 32 Milliarden US-Dollar Umsatz im Geschäftsjahr 2005/2006. Im Jahr 2002 übernahm Johnson Controls in Europa das Autobatteriegeschäft der VARTA AG und stieg damit zum weltweit führenden Anbieter von Batterien für Fahrzeuge auf.

Gesetzliche Anforderungen verlangen aktives Handeln

Bereits seit den frühen 90er Jahren steuert Varta das europäische Autobatteriegeschäft auf der Plattform von SAP®-Anwendungen. Mit der Übernahme durch Johnson Controls rückten die strengen Auditierungsregeln des Sarbanes-Oxley Acts (SOX) in den Vordergrund – und damit ein Thema, das in den USA notierte Börsengesellschaften zwar direkt betrifft, aber auf freiwilliger Basis auch andere europäische und deutsche Unternehmen außerhalb dieses Kreises immer mehr beschäftigt.

Gründe dafür sind zum einen das Streben nach mehr Transparenz in der Darstellung der Unternehmenssituation und zum anderen die generelle Zielsetzung, die IT-Sicherheit zu erhöhen. Für beides liefern SOX-basierte Projekte einen zuverlässigen Handlungsrahmen.

Im Fall von Johnson Controls Power Solutions konzentrierte sich der Handlungsbedarf insbesondere auf den Bereich der abzubildenden Gewaltenteilung innerhalb der SAP-Anwendungen. „Benutzerrechtsverstößen einen Riegel vorschieben und das

Berechtigungskonzept auflagegerecht gestalten“, so definiert Martin Wallner in seiner Funktion als Manager IT Governance and Quality die damit verbundene Aufgabenstellung. Sie zielt vor allem darauf ab, die Integrität von Finanzdaten sicherzustellen, damit verbundene Risiken zu identifizieren, zu minimieren und möglichst nachhaltig auszuschalten. Den IT-Anwendungen kommt in diesem

Zusammenhang besondere Bedeutung zu, laufen doch nahezu alle für die Rechnungslegung relevanten Geschäftsprozesse innerhalb des informationstechnischen Netzwerkes ab.

„Die Software beweist sich als permanenter Systemprüfer, der uns die Sicherheit gibt, die Compliance im Berechtigungswesen in Echtzeit und rund um die Uhr zu kontrollieren und zu gewährleisten.“

Martin Wallner, Manager IT Governance and Compliance, Johnson Controls Power Solutions Europe

Benutzerrechtsverstößen einen Riegel vorschieben

Rund 1.000 Mitarbeiter arbeiten bei Johnson Controls Power Solutions mit SAP-Anwendungen – in Deutschland ebenso wie an anderen europäischen Standorten. Die Sarbanes-Oxley-Act-Compliance über diese grenzüberschreitende IT-Landschaft hinweg sicherzustellen war die Herausforderung. Ihr stellte sich ein Projektteam aus internen IT-Spezialisten, Administratoren und Key-Usern aus den Fachabteilungen. Externe Unterstützung leistete der auf IT-Sicherheitsmanagement spezialisierte Unternehmensberater Hans-Joachim Gaebert.

Die passende Software lieferte SAP mit SAP GRC Access Control, der Anwendung für die Zugriffs- und Berechtigungssteuerung innerhalb der SAP-Lösungen für Governance, Risk und Compliance. Nach kurzer Analyse hatte man sich in Hannover für ein neues, rollenbasiertes Nutzerkonzept entschieden und mit der SAP-Anwendung die dafür am besten ge-

eignete Software identifiziert. Sie überwacht zeitnah und automatisiert sämtliche relevanten Bestimmungen: „Die Software beweist sich als permanenter Systemprüfer, der uns die Sicherheit gibt, die Compliance im Berechtigungswesen in Echtzeit und rund um die Uhr zu kontrollieren und zu gewährleisten“, hebt Martin Wallner hervor.

Schrittweise zum Ziel lückenloser Compliance

Auf dem Weg zum Ziel einer lückenlosen Compliance ging es dem Projektteam vor allem darum, die größten Gefahren für die materielle Richtigkeit des Jahresabschlusses zu identifizieren und auf dieser Basis Maßnahmen zur Risikominderung und -vermeidung zu treffen.

Zunächst wurden Funktionen mit möglichen Risikoanteilen untersucht, kritische Risiken identifiziert und in einer Matrix gebündelt. Im nächsten Schritt nahm sich das Projektteam der Erstellung von Regeln an, mit deren Hilfe selbsttätig Risiken in SAP-Rollen erkannt und beispielsweise Konflikte im Hinblick auf Funktionstrennungen oder kritische Transaktionen aufgedeckt werden können. „Dabei haben wir in besonderer Weise von der Sammlung von Regeln profitiert, die SAP für die Funktionstrennung in vordefinierter Form anbietet“, erklärt Hans-Joachim Gaebert von der gleichnamigen Unternehmensberatung für IT-Sicherheit und IT-Revision, die das Projekt begleitete.

In der Tat: SAP GRC Access Control beinhaltet eine der umfassendsten Datenbanken von Regelungen, um Verstößen gegen die Funktionstrennung auf die Spur zu kommen. Was dabei besonders positiv zu Buche schlägt ist, nach Meinung der Verantwortlichen in Hannover, die gängige Sprache des Regelwerks.

Der bewusst betriebswirtschaftlich geprägte Stil erleichterte es, die Zuordnung von Berechtigungen dezentral auszurichten: „Hier weiß man am besten, was die einzelnen Benutzer tun und welche relevanten Risiken damit verbunden sind“, argumentiert Martin Wallner. Die Pflege der Berechtigungen übernimmt bei Johnson Controls Power Solutions die zentrale IT.

Prävention durch Simulation

Ausführliche Risikoanalysen begleiteten bei Johnson Controls Power Solutions den Weg zum Ziel. Dabei bewiesen sich die integrierten Simulationsmöglichkeiten als ein nützliches Werkzeug. „Wenn man feststellen kann, was geschieht, wenn Berechtigungen entzogen, umverteilt oder neu zugewiesen werden, können Sicherheitsrisiken bereits im Vorfeld erkannt werden“, hebt Martin Wallner hervor. Er misst den Projekterfolg auch daran, dass sämtliche Einstellungen und Ergebnisse den kritischen Augen von Wirtschaftsprüfern standhielten und abgenommen wurden.

„Wenn man feststellen kann, was geschieht, wenn Berechtigungen entzogen, umverteilt oder neu zugewiesen werden, können Sicherheitsrisiken bereits im Vorfeld erkannt werden.“

Martin Wallner, Manager IT Governance and Compliance, Johnson Controls Power Solutions Europe

Regelmäßige Prüfungen

Um die Compliance dauerhaft zu schützen, wurde bei Johnson Controls Power Solutions ein Sicherheits-Administrator installiert. Bei ihm laufen die von der Anwendung erzeugten Reports und Auswertungen zusammen, sodass jederzeit ein zeitnahe Überblick über den Stand von Risiken und aktuelle Verletzungen vorgegebener Regeln gegeben ist. Unabhängig davon lässt Johnson Controls Power Solutions seine Compliance-Lösung regelmäßig durch interne und externe Auditoren überprüfen.

THE BEST-RUN BUSINESSES RUN SAP™



**SAP Deutschland
AG & Co. KG**

Hasso-Plattner-Ring 7

69190 Walldorf

T 08 00/5 34 34 24*

F 08 00/5 34 34 20*

* gebührenfrei in Deutschland

T +49/18 05/34 34 24**

F +49/18 05/34 34 20**

** gebührenpflichtig

E info.germany@sap.com

www.sap.de

Kostenloser Online Newsletter

www.sap.de/sapimfokus

50 086 444 (07/09)

© 2007 SAP AG. Alle Rechte vorbehalten. SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge und weitere im Text erwähnte SAP-Produkte und -Dienstleistungen sowie die entsprechenden Logos sind Marken oder eingetragene Marken der SAP AG in Deutschland und anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen. Die Angaben im Text sind unverbindlich und dienen lediglich zu Informationszwecken. Produkte können länderspezifische Unterschiede aufweisen.

In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die vorliegenden Angaben werden von SAP AG und ihren Konzernunternehmen („SAP-Konzern“) bereitgestellt und dienen ausschließlich Informationszwecken. Der SAP-Konzern übernimmt keinerlei Haftung oder Garantie für Fehler oder Unvollständigkeiten in dieser Publikation. Der SAP-Konzern steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Aus den in dieser Publikation enthaltenen Informationen ergibt sich keine weiterführende Haftung.