SAP*&SICHERHEIT

EIN SUPPLEMENT VON S@PPORT

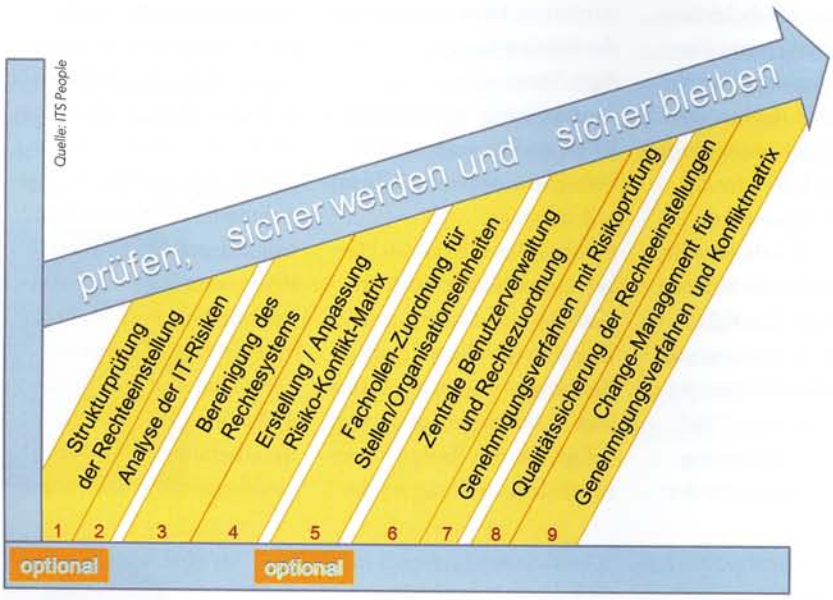
10_2010 | EINZELPREIS 9,– EURO

SICHERHEITS-KONZEPTE IM SAP-UMFELD

Einführung eines IT-gestützten Risikomanagement ist mehr als ein Lizenzkauf

„SICHERER WERDEN" REICHT NICHT, „SICHER BLEIBEN" IST DAS ZIEL

Bei der Einführung eines IT-gestützten Risikomanagement sind eine Vielzahl von organisatorischen Komplexitäten zu berücksichtigen. Das Fachkonzept muss nicht nur die gestellte Aufgabe lösen und den Ressourcenbedarf skizzieren, um „sicherer zu werden", sondern in letzter Konsequenz auch um „sicher zu bleiben". Nur so lassen sich spätere umfangreiche Investitionen vermeiden.



Projektphasen von Compliant Identity Management

*Von Rolf-Udo Gilbert, its-people Köln**

Nahezu jedes Unternehmen strebt durch IT-gestützte Maßnahmen nach mehr Sicherheit. Dabei gilt es für den Unternehmenslenker, Bedrohung und Risikowahrscheinlichkeit gegen die notwendigen Investitionen abzuwägen. Heutzutage ist das Einhalten von Vorgaben – Stichwort Compliance – für Unternehmen jeder Größenordnung zwingend. Vor diesem Kontext stellt sich die Frage: Reicht das Zusammenzählen von Lizenz- und Implementierungskosten aus, um den Aufwand für ein notwendiges Sicherheitsprojekt ganzheitlich und nachhaltig zu ermitteln?

Die erste unternehmerische Entscheidung bei der Einführung eines IT-gestützten Risikomanagement lautet: Wer hat die Verantwortung für ein solches Sicherheitsprojekt? Als eine Antwort bietet sich die Unternehmens-IT an. Sie ist maßgeblich das ausführende Organ – manche Unternehmen sprechen hier schon vom internen IT-Dienstleiter. Aber bei genauerem Hinsehen wird schnell klar: Die Budget- und Projektverantwortung muss aus der Revision oder dem Controlling kommen – allerdings in enger Abstimmung mit der Organisationsabteilung. Das Projekt muss aus dem Führungskreis initiiert und begleitet werden, da es Teil des unternehmensweiten Risikomanagements ist und auf alle Fachbereiche durchgreift.

Wer das Pflichtenheft für dieses Projekt erstellt, erkennt sofort die Wichtigkeit der Reihenfolgeplanung. Gleichgültig, welche Software oder Methode der diversen Anbieter für einen Bereich ausgewählt wird, am Anfang steht die IST-Aufnahme. Diese Analyse ermittelt recht schnell die Problembereiche: Einerseits kommen falsch eingestellte Berechtigungen zum Vorschein, andererseits zu viele Rechte bei den Benutzern, das Vorhandensein von unternehmensindividuellen Risikodefinitionen oder einer Qualitätssicherung bei sicherheitsrelevanten Abläufen. Das Fachkonzept muss nicht nur die Aufgabe lösen und den Ressourcenbedarf skizzieren, um „sicherer zu werden", sondern auch um „sicher zu bleiben".

Struktur- und Risikoanalyse ist der erste Schritt

Der erste Schritt der Projektarbeit beginnt mit der Struktur- und Risikoanalyse der Rechteeinstellungen. Ist hier bereits Hand-

* **Rolf-Udo Gilbert** *ist Geschäftsführer der Consonoit und Mitglied im its-people-Verbund. Er beschäftigt sich seit vielen Jahren mit Anwendungssicherheit in SAP-Systemen und unterstützt bei Auswahl und Einführung von Sicherheitslösungen. Er ist Mitautor des neuen „Best-Practice-Leitfaden zur Einführung der SAP BusinessObjects GRC-Lösungen" der DSAG. Dieser Leitfaden ist zu finden unter:* **http://www.dsag.de/fileadmin/media/Leitfaeden/100602_Leitfaden_SAP_BO_ACBP_screen.pdf**

lungsbedarf erkannt, kann diese Phase übersprungen werden. Danach geht es an die Überarbeitung der Einzel- und Sammelrollen, also der Rechte pro Unternehmensfunktion und Arbeitsplatz. Parallel ist die Transaktions-Konflikt-Matrix zu erstellen oder anzupassen, damit bei dieser Phase bereits Konfliktfreiheit mindestens auf der Ebene der Einzelrollen geprüft und eingehalten werden kann.

Die so überarbeiteten Rechte sollten den Stellen beziehungsweise Organisationseinheiten zugeordnet werden, um diese später an die Stelleninhaber einfacher vergeben zu können. Eine weitere Phase dient der zentralen Verwaltung der Benutzer über alle IT-Systeme hinweg.

Verwalten bedeutet dabei nicht nur das Anlegen und Löschen von Benutzern, sondern auch ihre Rechtezuweisung. Hierbei ist vorgeschrieben, dass über ein Vier-Augen-Prinzip – am besten mit einem durchgängigen IT-gestützten Genehmigungs-Workflow – das beantragte Recht von den Besitzern der Rechte (den so genannten Data-Owner) nachvollziehbar genehmigt und – möglichst automatisiert – zugewiesen wird. Parallel gilt es zu prüfen und zu entscheiden, ob beim Benutzer durch die neue Zuweisung ein Konflikt (etwa bei einem Zusammentreffen kritischer Funktionen) auftritt und wie auf diesen reagiert werden soll. Mögliche Optionen sind die Funktionstrennung oder eine andersartige organisatorische Kontrolle.

Das Erhalten der Sicherheit gehört zum Projekt

Sind diese Schritte für alle Unternehmensbereiche vollständig implementiert und durchgeführt, hat man die erste Aufgabe gelöst, das „sicher werden". Doch daran schließt sich die Frage an, wie man diesen Status langfristig erhalten kann, damit die Investition nicht in vier bis fünf Jahren zu wiederholen ist.

Hier kommen die Funktionsmodule Qualitätssicherung und Change-Management ins Spiel, um einerseits Rechteveränderungen nachhaltig zu kontrollieren und zu dokumentieren, und andererseits um Workflow-Modifikationen und Veränderungen in der Konfliktmatrix aufzuzeigen, da diese ja bei Programmerweiterungen sowie an das gestiegene Sicherheitsniveau angepasst werden müssen. Ebenso hilfreich für den nicht so IT-versierten Fachvorgesetzten ist eine Handlungsempfehlung, wie mit neuen Risiken umzugehen ist.

Weiterer Handlungsbedarf entsteht dann aber, um die Sinnhaftigkeit für die Einführung des neuen Sicherheitskonzeptes allen Beteiligten klar zu machen. Dazu muss man den Umgang mit den einzelnen Verfahren verständlich machen und die Mitarbeiter entsprechend schulen. Dabei stellt sich die Frage, wer zu diesen Beteiligten zählt. Um die IT-Sicherheitsvorgaben ganzheitlich umzusetzen und dabei über automatisierte Prozesse auch Aufwand und Zeit einsparen zu können, sind diese Aufgaben auf mehrere Schultern zu verteilen. Die Geschäftsführung definiert das Sicherheitsniveau, die Wirtschaftsprüfer entwerfen in Zusammenarbeit mit der internen Revision die Risiko-Kontroll-Matrix, die Fachbereiche sind verantwortlich für ihre Rechte und deren Genehmigung. Die Revision im Unternehmen entwirft die Genehmigungsverfahren und überprüft, ob die Kontrollanweisungen – falls Funktionstrennung nicht möglich ist – auch durchgeführt werden. Für die IT bleibt die Aufgabe, die Prozesse zeitnah zu implementieren und sie bei Bedarf anzupassen.

So gesehen umfasst die Einführung eines IT-Risikomanagements mehr als nur Lizenz- und Implementierungskosten. Sie verlangt die Gesamtsicht auf die Lösung, auch wenn erstmals nur Teile davon umgesetzt werden. Sie benötigt Mitarbeit und Ressourcen aus der gesamten Organisation. Sie schafft Transparenz in Abläufe und Verfahren und kann diese auch nachhaltig optimieren – eine Herausforderung und Chance, die man immer bei der Projektierung im Auge behalten sollte. *(rh)* @