itmanagement
SEPTEMBER 2018

MAGAZIN FÜR DIE ENTERPRISE IT

ERP-SYSTEME IM MITTELSTAND

# SAP LEICHT GEMACHT

Peter Arbitter, Leiter Portfolio- und Produktmanagement Geschäftskunden, Telekom Deutschland





## DEVOPS UND DIGITALISIERUNG

Neue Werte, Prinzipien & Praktiken

## VOICE SEARCH, & AVATARE

Die Suchmaschinen-(R)evolution geht weiter

## EFFIZIENTE ITSM-PROZESSE

Weniger Betriebskosten – mehr Unabhängigkeit

www.it-daily.net

# EIN ISMS

## INFORMATIONSSICHERHEIT GEHÖRT ZUM GUTEN TON DER ORGANISATION.

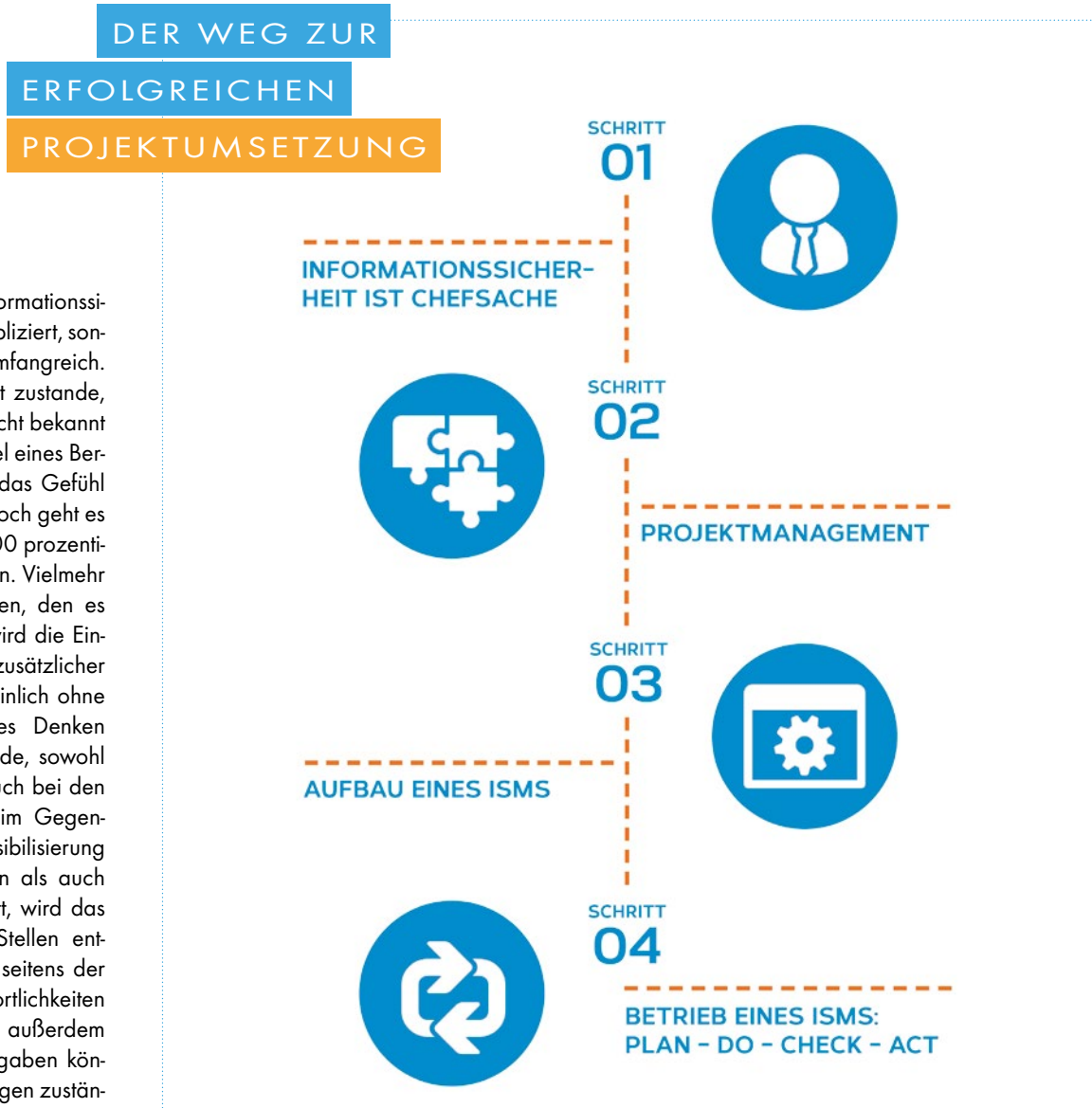
Informationssicherheit ist längst kein Fremdwort mehr. Im Gegenteil: Die Medien berichten beinah täglich von Spionage, Sabotage oder Datendiebstahl. Obwohl diese Gefahren also präsent sind, wird das Thema in vielen Organisationen immer noch nicht mit der notwendigen Ernsthaftigkeit betrachtet. „Uns wird schon nichts passieren" oder „Wir sind doch gar nicht so interessant für einen Hacker-Angriff oder Datendiebstahl" sind leider Aussagen, die einem in der Praxis viel zu oft begegnen. Die Folgen dieser Irrglauben können jedoch einen ernsthaften wirtschaftlichen Schaden in der Organisation anrichten, Imageschäden nach sich ziehen oder sogar die Existenz bedrohen.

**Aus dem Leben...**

In der Praxis ist das Thema Informationssicherheit im Grundsatz nicht kompliziert, sondern eher „unbequem" und umfangreich. Dieses Gefühl kommt jedoch oft zustande, weil das Ausmaß des Projekts nicht bekannt ist. Man könnte es mit dem Gipfel eines Berges vergleichen, bei dem man das Gefühl hat, diesen nie zu erreichen. Jedoch geht es bei einem ISMS nicht um die 100 prozentige Sicherheit in der Organisation. Vielmehr muss der ISMS-Prozess existieren, den es zu zertifizieren gilt. Weiterhin wird die Einführung des ISMS sehr oft als zusätzlicher Aufwand betrachtet, augenscheinlich ohne einen klaren Mehrwert. Dieses Denken verursacht oft innere Widerstände, sowohl bei der Geschäftsführung als auch bei den einzelnen Mitarbeitern. Findet im Gegensatz gleich zu Beginn eine Sensibilisierung sowohl der relevanten Personen als auch der gesamten Organisation statt, wird das Thema an allen zuständigen Stellen entsprechend vorangetrieben. Die seitens der Norm geforderten Verantwortlichkeiten ermöglichen der Organisation außerdem eine klare Rollenverteilung. Aufgaben können auf diese Weise an die richtigen zuständigen Stellen in der Organisation delegiert und wirksam abgearbeitet werden. Ferner fordert die Norm kaum etwas, was ein Unternehmen nicht ohnehin tun sollte, um sich zu schützen.

**Der Weg zur erfolgreichen Projektumsetzung**

1. **Informationssicherheit ist Chefsache**
   Der Geschäftsführung muss die Notwendigkeit einer ISMS-Einführung bewusst sein. Wichtiger noch: Die oberste Chefetage sollte die Einführung eines ISMS nicht als einmalige Zertifizierung betrachten, sondern die Mehrwerte bei der täglichen Arbeit und im weiteren Betrieb kennen und an die Mitarbeiter im Unternehmen kommunizieren. Vor Projektbeginn muss der Scope für ein ISMS, also der Geltungsbereich, definiert werden.



# ALS CHANCE SEHEN

EIN EHRLICHES ISMS SCHAFFT POTENTIALE, BRINGT SYNERGIEN HERVOR UND LÄSST SICH UNTER DER VOLLKOSTENBETRACHTUNG (TCO) KOSTENNEUTRAL EINFÜHREN UND BETREIBEN!

Jens Heidland, Lead Auditor ISO 27001 und IT-Sicherheitskatalog sowie Leiter Consulting, Contechnet | www.contechnet.de

**2. Projektmanagement**

Die Gründung einer Projektmanagement-Gruppe inklusive eines Lenkungsausschusses ist erforderlich, um den kontinuierlichen Stand des Projektes zu verfolgen und alle relevanten Beteiligten mit „im Boot" zu haben. Dafür sind Schulungen zur Mitarbeitersensibilisierung notwendig. Der Faktor Mensch ist hierbei entscheidend. Denn seien wir doch mal ehrlich: Wer macht schon gern Aufgaben oder verfolgt ein Ziel, bei dem sich ihm die Sinnhaftigkeit des Ganzen überhaupt nicht erschließt?

**3. Aufbau eines ISMS**

Vor dem Aufbau sollte betrachtet werden, welche Anforderungen in der Organisation bereits erfüllt werden. Organisationen, die zum Beispiel eine ISO 9001 Zertifizierung (Qualitätsmanagement) schon haben, haben viele Vorteile, da wesentliche Bestandteile des Managementsystems bereits vorhanden sind. So erfüllen etwa das Risikomanagement, die Festlegung von Rollen und Verantwortlichkeiten, der kontinuierliche Verbesserungsprozess und die Managementbewertung mit leichten Anpassungen bereits die Anforderungen an ein ISMS nach ISO/IEC 27001. Hat die Analyse stattgefunden, gilt es das Managementsystem an sich aufzusetzen und die Risikomethode festzulegen. Anhand der Risikoanalyse und -bewertung können dann entsprechende Maßnahmen ergriffen werden, um die identifizierten Risiken zu behandeln.

**4. Betrieb eines ISMS**

Zum Schluss geht es darum, das ISMS am Leben zu halten. Das heißt also den wiederkehrenden Zyklus (Plan - Do – Check – Act) einzuhalten und immer wieder anzustoßen. Ein ISMS muss als ein lebender Prozess in der Organisation integriert und dementsprechend auch gelebt werden. Steht nur die einmalige Zertifizierung im Fokus der Organisation, ist das Projekt zum Scheitern verurteilt und die Organisation wird spätestens im Zuge der Überwachungsaudits oder der Re-Zertifizierungen die Folgen dessen spüren.

**Und dafür benötige ich eine Softwarelösung?**

Die Einführung eines ISMS kann auf unterschiedliche Art und Weise erfolgen. An keiner Stelle der Norm wird gefordert, dass eine Softwarelösung zum Einsatz kommt oder mit welchem System die Anforderungen umgesetzt werden sollen. Es ist also der Organisation selbst überlassen, welchen Weg sie geht. Entscheidend ist auch an dieser Stelle nicht das „wie ich zum Ziel komme", sondern „dass ich zum Ziel komme". Das „wie" kann den Weg allerdings um ein Vielfaches erleichtern.

Eine entsprechende Softwarelösung liefert unterschiedliche Unterstützungsmöglichkeiten auf dem Weg zur Einführung eines ISMS sowie im weiteren Betrieb: Die strukturierte Vorgehensweise und damit die Umsetzungsstruktur wird durch die Lösung vorgegeben. Somit erhält der Anwender einen Leitfaden, wie er im Projekt vorzugehen hat. Die Norm-Texte sind um einfach nachvollziehbare Umsetzungsempfehlungen ergänzt. Diese ermöglichen dem Nutzer eine zeiteffiziente Dokumentation der geforderten Maßnahmen ohne das „Norm-Deutsch" zu beherrschen. Ein einfaches und zentral gesteuertes Risikomanagement dient als weitere Hilfestellung: Assets wie Prozesse, Personal und Infrastruktur, die dem gleichen Risiko zugeordnet sind, können in Gruppen zusammengefasst werden. Eine Risikoanalyse findet damit pro Gruppe statt. Auf diese Weise werden Analysen und Maßnahmen deutlich reduziert. Aufgaben zur Risikobehandlung können erstellt und den Assets zugeordnet werden. Vordefinierte Kriterien zur Risikoakzeptanz erleichtern die Priorisierung der Risikobehandlung. Das Aufgabenmanagement gibt einen übersichtlichen Überblick über die angelegten Aufgaben sowie Maßnahmen und zeigt den Fortschritt der Bearbeitung an. Ist ein ISMS mit der Softwarelösung, wie INDITOR ISO von CONTECHNET, eingeführt, unterstützt die Lösung auch im weiteren Betrieb und erleichtert die Pflege der Daten. Dies schafft Synergien und kann Kosten für die Maßnahmenplanung, -implementierung und den fortlaufenden Betrieb nachhaltig senken. Darüber hinaus können die angelegten Assets wie Prozesse, Personal und Infrastruktur für die IT-Notfallplanung und den Datenschutz verwendet werden. Die Praxis zeigt: Zentrale Lösungen lassen sich in der Regel ressourcenschonender, sicherer und zuverlässiger in der Organisation betreiben als konkurrierende und sich vielfach überschneidende Individuallösungen. Hierzu müssen die entsprechenden Stellen im Hause nur mal miteinander reden!

***Jens Heidland***