

Vorwort

Grabe den Brunnen, bevor Du Durst hast
(Chinesisches Sprichwort)

Während in der heutigen Zeit die Öffnung alter Strukturen und damit auch die zugrunde liegende Technik für uns neue Chancen und Flexibilität bieten, können wir nicht außer Acht lassen, dass diese auch neue Risiken mit sich bringen.

Die Notwendigkeit, Sicherheit und Risikomanagement als permanente Prozesse im Unternehmen zu betreiben, resultiert aus verschiedenen Beweggründen. Zum einen ist es erforderlich, gegenüber Kunden und Geschäftspartnern Produkte und Dienstleistungen zuverlässig und in hoher Qualität zur Verfügung zu stellen. Zum anderen gilt es, den Fortbestand des Unternehmens zu sichern.

Die Geschäftstätigkeiten und die Geschäftsprozesse werden oftmals nur noch mit Hilfe von Informationstechnik (IT) durchgeführt. Viele Geschäftsprozesse werden elektronisch unterstützt, große Mengen von Informationen elektronisch gespeichert, genutzt, verarbeitet und teilweise in öffentlichen Netzen übermittelt. Darüber hinaus sind auch Sicherheitsaspekte wie Haus- und Gebäudeschutz, personelle Sicherheitsmaßnahmen, Arbeitsplatzschutz und im Gesamtkontext auch die Ausfall- und Kontinuitätsplanung mit zu betrachten.

Insbesondere sind die Geschäftstätigkeiten des Unternehmens in hohem Maße abhängig vom einwandfreien Funktionieren der eingesetzten IT. Dieses kann nur durch ordnungsgemäßen und entsprechend verfügbaren Einsatz der IT-Systeme und den verantwortungsbewussten Umgang aller Mitarbeiter mit den IT-Anwendungen und zugehörigen sensitiven Daten oder anderen eingesetzten Ressourcen (externe Dienstleistungen) garantiert werden. Darüber hinaus ist die Entwicklung und Erhaltung sicherer Geschäftsprozesse von entscheidender Bedeutung.

Weiterhin greifen gesetzliche Bestimmungen, Aufsichtspflichten und Verordnungen in die Geschäftstätigkeit regelnd ein. Ein großer Teil dieser Daten unterliegt dem Geschäftsgeheimnis und dem Datenschutzgesetz. Darüber hinaus gelten weitere Gesetzestexte für Finanzinstitute, wie das KWG und das WpHG. Seit 1998 sieht der Gesetzgeber mit dem KonTraG eine persönliche Haftung von Geschäftsführern und Vorständen in den Fällen vor, in denen gravierende Notsituationen oder Ereignisse frühzeitig hätten erkannt werden müssen. Diese Verpflichtung gilt auch für die Sicherheit und die Kontinuität von Geschäftsprozessen.

Sicherheitsanspruch und Risikomanagement stehen vordergründig oftmals im Interessenkonflikt mit der betriebswirtschaftlichen Seite und der Nutzen ist häufig nicht unmittelbar erkennbar. Der Anspruch bzgl. der Qualität von Produkten und Dienstleistungen für Kunden und Geschäftspartner sowie die Aufrechterhaltung der Geschäftsprozesse des Unternehmens und die Einhaltung gesetzlicher Regelungen verpflichten generell, eine sichere und funktionsfähige IT als wirtschaftliches Gut zu betrachten und als ein Unternehmensziel zu definieren.

Sicherheit und Risikomanagement können nicht alleine von der Geschäftsführung und vom Management getragen werden, sondern erfordern die Mitwirkung aller Mitarbeiter in ihrer täglichen Arbeit, um das erforderliche Niveau aufrechtzuerhalten. Die aufgeführten Verfahren und Methoden sollen zur Verbesserung und Aufrechterhaltung eines angemessenen Sicherheitsniveaus als Leitlinie im Sinne der „Best Practices“ dienen.

Management operationaler IT- und Prozess-Risiken

Methoden für eine Risikobewältigungsstrategie

Thies, K.H.W.

2008, XI, 148 S. 31 Abb., Hardcover

ISBN: 978-3-540-69006-1