Cybersicherheit und betriebliches Kontinuitätsmanagement mit DocSetMinder

Die aktuelle Studie der Allianz „Allianz Risk Barometer – Die 10 größten Geschäftsrisiken 2016" weist die Betriebsunterbrechung und Cybervorfälle unter den drei größten Unternehmensrisiken auf. Trotz der eindeutigen Sicherheitslage herrscht in vielen Unternehmen und Behörden immer noch die Illusion der Sicherheit.

Von Krzysztof Paschke, GRC Partner GmbH

Hauptaufgabe der Unternehmensleitung ist die Umsetzung der geplanten Unternehmensziele und eine langfristige Marktbehauptung. Grundvoraussetzung hierfür ist ein kontinuierlicher und störungsfreier Geschäftsbetrieb, insbesondere in den globalisierten und sich schnell verändernden Märkten. Durch die Verkettung der Geschäftsprozesse von Lieferanten und Auftraggebern ist ein hoher Grad an wirtschaftlicher Abhängigkeit erreicht. Sehr deutlich zu erkennen ist dies bei der Betrachtung der „just-in-time"-Lieferketten. Eine Unterbrechung der Lieferung kann nicht nur einen wirtschaftlichen, sondern auch einen Imageschaden bedeuten. Das Image eines langjährigen zuverlässigen Geschäftspartners wird über Jahre durch die sorgfältige Erfüllung der vereinbarten Leistungen aufgebaut. Bereits geringe Zweifel des Auftraggebers an der genannten Zuverlässigkeit können zum Verlust der Marktposition führen – unter Umständen mit gravierenden wirtschaftlichen und sozialen Folgen.

Die bereits zum fünften Mal durchgeführte Studie der Allianz „Allianz Risk Barometer" identifizierte die größten Geschäftsrisiken im Jahr 2016. Unter den zehn größten Unternehmensrisiken belegt die Betriebsunterbrechung (inkl. Lieferkettenunterbrechung) Platz 1 und Cybervorfälle (Cyberkriminalität, Verletzung der Datenschutzrechte) Platz 3. Die Studie prognostiziert, dass in den nächsten zehn Jahren Cybervorfälle, Betriebsunterbrechung und Terrorismus die Plätze 1 bis 3 bei den wichtigsten Risiken belegen werden.

Trotz der eindeutigen Sicherheitslage herrscht in vielen Unternehmen und Behörden immer noch die Illusion der Sicherheit. Mutige Aussagen wie „Bei uns ist noch nie etwas passiert" verdeutlichen, wie gering der Stellenwert der IT-Sicherheit und des Notfallmanagements in einer Organisation ist. Eine weitere Studie im Auftrag des Digitalverbands Bitkom (April 2015) bestätigt den aktuellen Status. Nur knapp die Hälfte (49 %) der Befragten 1074 Unternehmen verfügt über ein Notfallmanagement. Ein wesentliches Hindernis bei der Einführung der IT-Sicherheit und des Notfallmanagements ist, neben der zeitintensiven Planung und Umsetzung der Sicherheitsmaßnahmen, die dazu gehörende sehr aufwändige Projektdokumentation für das Audit. Der Einsatz von Office-Produkten ist zwar möglich, stellt aber keine echte Alternative zu einem speziell dafür konzipierten Tool dar. DocSetMinder bietet zum Thema IT-Sicherheit eine komplette Suite von aufeinander abgestimmten Modulen mit Dokumentstrukturen und Vorlagen, mit denen die Cybersicherheit und ein betriebliches Kontinuitätsmanagement vollständig abgebildet werden können.

Effektive Umsetzung mit DocSetMinder

Bei der Vielzahl der gesetzlichen Auflagen und Normanforderungen ist es empfehlenswert, einen organisationsweiten ganzheitlichen Planungs- und Dokumentationsansatz in Form eines „Integrierten Managementsystems" (IMS) zu etablieren. Wie eine effiziente und effektive Umsetzung der technischen und organisatorischen Maßnahmen funktioniert, kann aus der ISO-Welt abgeleitet werden. Anstatt jede Norm, jeden Standard oder gesetzliche Anforderung einzeln zu planen und mit unterschiedlichen Tools zu realisieren, ist eine globale Betrachtung von enormem Vorteil. Gemeinsamkeiten bei der Planung, Umsetzung und Aufrechterhaltung der Sicherheitsstandards sind vor allem in Bereichen des Projektmanagements, der Strukturanalyse, Risikoanalyse, Überwachung und Audits vorhanden. Um die Mindestanforderungen der Sicherheitsstandards und Datenschutzgesetze (EU, Bund und Länder) effizient und vollständig umzusetzen und aktuell zu halten, stehen den involvierten Mitarbeitern

diverse DocSetMinder Module und Maßnahmenkataloge zur Verfügung. In Verbindung mit dem Microsoft SQL Server als zentrale Repository ist der DocSetMinder beliebig skalierbar und eignet sich für Unternehmen und Behörden jeder Größe. Durch den modularen Aufbau kann ein bereits umgesetzter Standard um zusätzliche Normen jederzeit zu einem Integrierten Managementsystem erweitert werden.

Modul „Organisation"

Die genaue Kenntnis der Unternehmens- und Behördenorganisation ist eine elementare Voraussetzung für die Durchführung der Strukturanalyse. Das Modul stellt die notwendigen Strukturen und Vorlagen für die Dokumentation der Aufbau- und Ablauforganisation in gewünschter Tiefe zur Verfügung. Erfasst werden sämtliche Organisationseinheiten, wie Bereiche, Abteilungen, Gruppen, sowie Geschäftsprozesse mit den Verantwortlichkeiten (Rollen) in der Organisation. Darüber hinaus werden in diesem Modul auch unternehmensrelevante Dokumente wie Verträge, Leitlinien, Richtlinien, Berichte, Eintragungen und Urkunden aufbewahrt oder erstellt. Die hier erfassten Informationen werden in allen Modulen verwendet. Somit werden Redundanzen verhindert und Aktualisierungen vereinfacht.

Modul „IT-Dokumentation"

Ein weiterer Baustein der Strukturanalyse ist die Dokumentation des IT-Verbundes. Das Modul „IT-Dokumentation" erlaubt eine systematische Dokumentation der IT-Infrastruktur der passiven und aktiven Netzwerkkomponenten, Server-Systeme, Arbeitsplätze, Peripheriegeräte, Dienste und Anwendungen sowie Gebäude, Gebäudesicherheit und Räume. Durch den Einsatz von DocSetMinder-Schnittstellen können wesentliche Informationen aus Active-Directory- und Inventory-Systemen regelmäßig importiert werden. Die Dokumentation stellt die logischen Zusammenhänge zwischen Geschäftsprozessen, dafür verantwortlicher Software und Serversystemen sowie Speicherorten für die entstehenden Daten dar. Jede IT-Komponente kann dem fachlich und technisch zuständigen Mitarbeiter zugeordnet werden. Die hier erfassten Informationen werden in allen Modulen verwendet. Somit werden Redundanzen verhindert und Aktualisierungen vereinfacht.

Modul „IT-Grundschutz"

Das Modul bildet den BSI-Standard 100-2 vollständig ab. Die BSI-Methodik der Sicherheitskonzeption ist in die Modulstruktur detailliert integriert und unterstützt eine intuitive Bedienung, Umsetzung und Dokumentation des IT-Grundschutzes. Die Schutzbedarfsdefinition, Schutzbedarfsfeststellung und ihre Vererbung durch das Maximumprinzip sowie die Modellierung des IT-Verbundes ist durch die Softwareunterstützung einfach und schnell umsetzbar. Für die Überwachung der Umsetzung der festgelegten Maßnahmen kann sehr effektiv der Aufgaben- und Maßnahmenplaner sowie Reporting Services verwendet werden. GRC Partner bietet das Modul „IT-Grundschutz" für unmittelbare Bundes-, Landes- und Kommunalverwaltungen der Bundesrepublik Deutschland kostenlos an.

Modul „ISMS ISO/IEC 27001"

Die Norm ISO/IEC 27001 ist für die Planung, Umsetzung, Überwachung und stetige Verbesserung des Informationssicherheitsmanagementsystems (ISMS) konzipiert. Das Modul bildet die Anforderungen der Norm ISO/IEC 27001 vollständig und detailliert ab. Die Modulstruktur (High Level Structure) erlaubt die Definition und Dokumentation des Anwendungsbereichs, der Verantwortlichkeiten, der Anwendbarkeitserklärung (SoA), der ISMS-Leitlinie, eine Analyse und Bewertung der Risiken sowie die Definition der Maßnahmenziele und Maßnahmen zur Behebung der festgestellten Risiken.

Modul „(IT-)Notfallmanagement"

Das Modul basiert auf dem BSI-Standard 100-4, ISO 22301 und BCI-GPG 2013 und bildet die Methodik zur Etablierung eines adäquaten Notfallmanagementsystems im Unternehmen oder einer Behörde ab. Es erlaubt eine vollständige Erstellung und Pflege von Dokumentationen des Anwendungsbereichs, der Notfallorganisation, der Business Impact Analyse, der Risikoanalyse sowie der Alarmierung und Eskalation bis hin zu Geschäftsfortführungs- und Wiederanlaufplänen (Notfallhandbücher). Die Planung und Durchführung von Notfallübungen und der Verbesserungsprozess der Notfallorganisation (P-D-C-A) werden ebenfalls strukturiert unterstützt.

Fazit

DocSetMinder bildet anerkannte IT-Sicherheits- sowie Notfallmanagementstandards und den Datenschutz vollständig ab. Der Funktionsumfang der Software macht den Einsatz von weiteren Tools oder Office-Anwendungen für die Planung, Umsetzung und Dokumentation der Standards überflüssig. DocSetMinder ist einfach zu implementieren und leicht bedienbar. Die gemeinsame Nutzung der erfassten Informationen bietet für jeden Verantwortlichen einen enormen Mehrwert durch die Aktualität und Zeitersparnis bei der Vorbereitung von internen und externen Audits. Ready for Audit!

GRC Partner GmbH auf der it-sa: Halle 12, Stand 650