IT-Sicherheit, Notfallmanagement und Datenschutz effizient umsetzen

DocSetMinder - ein Integriertes Managementsystem für IT-Sicherheit und Notfallmanagement

Eine zertifizierungsreife Implementierung der IT-Sicherheit und des Notfallmanagements ist eine aufwendige und nicht zu unterschätzende Aufgabe. Die Lösung DocSetMinder der GRC Partner GmbH ist ein Integriertes Managementsystem und berücksichtigt die Gemeinsamkeiten und Schnittstellen der umzusetzenden Sicherheitsstandards in ihrem gesamten Lebenszyklus (PDCA).

Von Krzysztof Paschke, GRC Partner GmbH

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, Standard oder gesetzliche Anforderung einzeln zu planen und wohl möglich mit unterschiedlichen Tools zu realisieren, ist eine globale Betrachtung von enormem Vorteil. Die Gemeinsamkeiten bei der Planung, Umsetzung und Aufrechterhaltung der Sicherheitsstandards sind vor allem in folgenden Bereichen deutlich: Projektmanagement, Strukturanalyse, Risikoanalyse, Überwachung und Audits.

Da das Notfallmanagement ein fester Bestandteil eines Informationssicherheitsmanagementsystems (ISMS) gemäß ISO 27001 und BSI Standard 100-2 ist, kann die Synergie bei der Bildung der Projektteams sowie bei der Planung und Umsetzung der Maßnahmen im Rahmen des gleichen Projektes berücksichtigt werden.

Eine gemeinsame, gut geplante Strukturanalyse wird in der Regel nur einmal durchgeführt. Sie liefert für die Erstellung des Sicherheitskonzeptes, einer Business Impact Analyse und einer Risikoanalyse notwendige Informationen über organisatorische Einheiten, Verantwortlichkeiten, Prozesse und deren Abhängigkeiten von Anwendungen, IT-Systemen, Räumen, Leitungen etc.

Eine schlüssige Risikolandkarte aller IT-Sicherheitsrisiken liefert eine gleichzeitig für ISMS und Notfallmanagement durchgeführte Risikoanalyse. Die erreichte Effizienz hier: die Wiederverwendbarkeit der Risikoanalyse für die gleichen Unternehmenswerte und des Schutzziels „Verfügbarkeit“.

Überschrift: DocSetMinder - ein Integriertes Managementsystem

Die Compliance Management Software DocSetMinder der GRC Partner GmbH ist bereits im Jahre 2004 für die Etablierung von unterschiedlichen Normen und Standards im Unternehmen und in der Behörde entwickelt worden. Der Funktionsumfang deckt alle Anforderungen der Normen an die Lenkung der geforderten Informationen ab. Dazu gehören u.a.: Revisionssicherheit und Versionskontrolle, Protokollierung von Änderungen, Dokumentenkategorien (frei definierbar), Workflowmanagement, Aufgaben- und Maßnahmenplanung, Flussdiagrammdesigner (BPMN, ISO), Texteditor, Import- /Export-Schnittstelle und Reporting, Ausgabe der Dokumentation (Word, HTML), Jahresabschluss /Periodenabgrenzung, Volltextsuche, Mandantenfähigkeit, verschlüsselte SQL DB (AES 256).

Um die Mindestanforderungen der Sicherheitsstandards und Datenschutzgesetze (EU, Bund und Länder) effizient und vollständig umzusetzen und aktuell zu halten, stehen den Unternehmen und Behörden 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 jeder Zeit zu einem Integrierten Managementsystem erweitert werden.

Überschrift: 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 z.B. 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.

Überschrift: 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 Speicherorte 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.

Überschrift: Modul „Steuerungs- und Telekommunikationssysteme“

Das Modul ist exklusiv für die Umsetzung des IT-Sicherheitskataloges gemäß § 11 Absatz 1a Energiewirtschaftsgesetz bei Energieversorgern konzipiert worden und dient der Erfassung von Leitsystemen, Übertragungstechnik, Kommunikationstechnik sowie Steuerungs- und Automatisierungstechnik. Die hier erfassten Informationen sind notwendig für die Umsetzung und Zertifizierung gemäß der DIN ISO/IEC TR 27019.

Überschrift: 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 Bedingung, 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.

Überschrift: 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 ISMS-Leitlinie, eine Analyse und Bewertung der Risiken sowie die Definition der Maßnahmenziele und Maßnahmen zur Behebung der festgestellten Risiken.

Überschrift: 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. Das Modul 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.

Überschrift: Modul „Datenschutz“

Das Modul unterstützt den betrieblichen Datenschutzbeauftragten bei der Umsetzung, Kontrolle und Dokumentation der Datenschutzbestimmungen des Bundes und der Länder (BDSG und LDSG) im Unternehmen

und der Behörde. Die Modulstruktur grenzt das öffentliche Verfahrensverzeichnis von der Verfahrensakte ab, in der die einzelnen internen Verfahrensübersichten dokumentiert sind. Die strengen Anforderungen an die Dokumentation der Verfahren, ihre Zweckbestimmung, betroffenen Personengruppen, Datenkategorien und Fristen können revisionssicher erfasst werden. Für die Dokumentation der technischen und organisatorischen Sicherheitsmaßnahmen steht eine detaillierte Vorlage zur Verfügung.

Überschrift: Risikoanalyse

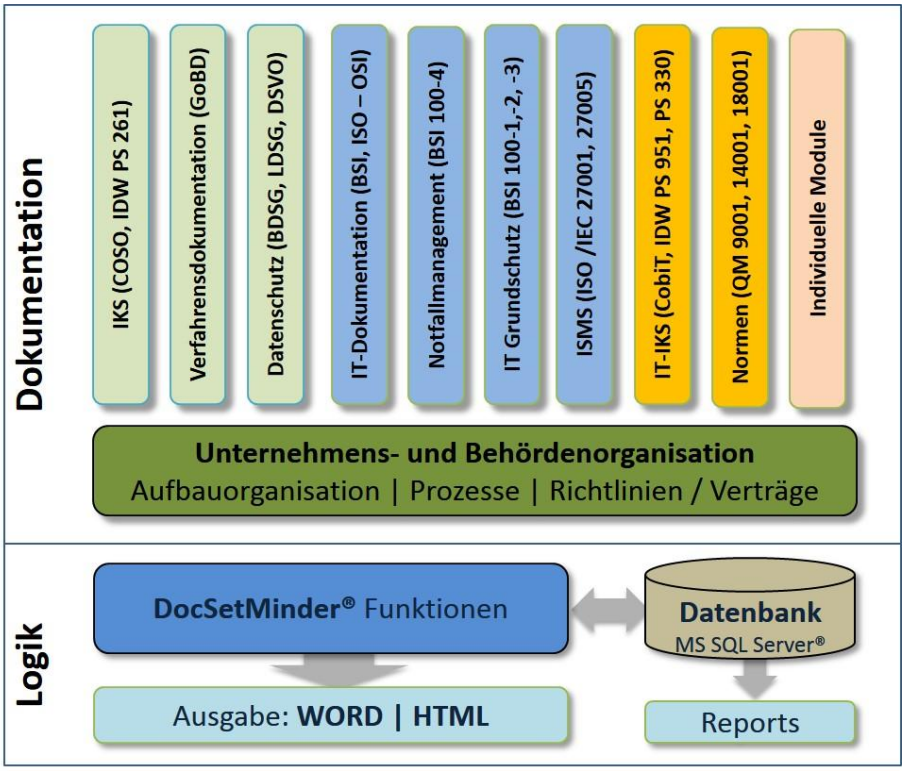
Für die Durchführung der Risikoanalyse stehen den Anwendern zurzeit zwei unterschiedliche Methoden zur Verfügung: BSI-Standard 100-3 und DIN ISO/IEC 27005. Die Norm DIN ISO/IEC 27005 ist aus der DIN ISO 31000 abgeleitet und unterstützt in einfacher Form die Berechnung der Risiken unter Berücksichtigung von Eintrittswahrscheinlichkeit und Auswirkung. Optional können weitere Faktoren, wie z.B. Häufigkeit (Exposition) oder Business Impact, berücksichtigt werden.

Überschrift: Maßnahmenkataloge

Für die Umsetzung der Sicherheitsmaßnahmen gemäß BSI IT-Grundschutz, DIN ISO/IEC 27001 oder des IT-Sicherheitskataloges gemäß EnWG stehen dem Anwender wahlweise die IT-Grundschutz-Kataloge, der Katalog der Maßnahmenziele und Maßnahmen der Normen ISO/IEC 27001/2, ISO/IEC 27019 zur Verfügung. Die Kataloge können individuell erweitert werden. Die BSI- oder ISO-Updates/ Ergänzungen der Bausteine oder Maßnahmen werden mit der bestehenden Dokumentation synchronisiert.

Überschrift: Fazit

DocSetMinder 3.1 bildet anerkannte IT-Sicherheits-, 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 umgesetzten Standards überflüssig. DocSetMinder 3.1 ist einfach zu implementieren und intuitiv 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.



Die Abbildung zeigt den modularen Aufbau der Compliance-management-Software DocSetMinder

Von Wirt.- Inf. (BA) Krzysztof M. Paschke