IT-Grundschutz umsetzen mit DocSetMinder

Dokumentation eines ISMS und Kompendium-Update

Seit der Veröffentlichung des modernisierten BSI IT-Grundschutzes im Oktober 2017 hat eine Vielzahl von Organisationen erfolgreich ein Informationssicherheitsmanagementsystem (ISMS) nach der BSI-Standardreihe 200-x etabliert. Neben der initialen Dokumentation ist die Pflege und Aktualisierung des ISMS ein wichtiger Bestandteil. Der nachfolgende Text soll einen allgemeinen Überblick über die Umsetzung geben.

Von Benjamin Heruth, Allgeier GRC GmbH

Eine wichtige Komponente, die in Bezug auf die Umsetzung eines ISMS entschieden werden muss, ist unter anderem, wie die Dokumentation erfolgen soll. Viele Organisationen entscheiden sich zunächst für die Nutzung von zum Beispiel Office-Produkten. Die Verwendung einer auf Dokumentation von Managementsystemen spezialisierten Software wie DocSetMinder bietet bei der initialen Erstellung und fortlaufenden Pflege eines ISMS jedoch entscheidende Vorteile.

Strukturanalyse – die Basis der Dokumentation

Die Strukturanalyse wird in der ISMS-Lösung DocSetMinder grundsätzlich in den beiden Modulen „Organisation“ und „IT-Dokumentation“ vorgenommen. Das DocSetMinder-Modul „Organisation“, auf dessen Inhalte alle weiteren Module in DocSetMinder aufbauen, besteht im Wesentlichen aus drei Komponenten: der Dokumentation der Aufbauorganisation (z. B. organisatorische Einheiten, Rollen, Mitarbeiter:innen, Dienstleister, Behörden etc.), der Ablauforganisation (Prozesskatalog) und Organisationsanweisungen und Verträgen (z. B. Leit- und Richtlinien, Verträge, Versicherungen etc.).

Das Modul „IT-Dokumentation“ unterstützt den Anwender und die Anwenderin bei der Erfassung der IT-Infrastruktur. In dem Modul können unter anderem Geschäftsanwendungen, Server (physisch und virtuell), Arbeitsplätze, Netzwerke und Netzwerkverbindungen, Betriebssysteme, Gebäude, Räume etc. erfasst und die logischen Verbindungen der Objekte untereinander und zu den Prozessen und Verantwortlichkeiten im Organisationsmodul hergestellt werden.

Für die Erstellung der Strukturanalyse (das gilt grundlegend auch für alle anderen Module in DocSetMinder) stehen den Anwendern eine vorgefertigte Verzeichnisstruktur, welche sich an einschlägigen Normen und Standards sowie „Best Practice“ orientiert, und Dokumentvorlagen zur Verfügung. Sowohl die Verzeichnisstruktur als auch die Dokumentvorlagen sind grundsätzlich durch die Anwender selbst mit sehr geringem Aufwand an die individuellen Gegebenheiten seiner Organisation anpassbar. So unterstützt DocSetMinder zum einen gezielt bei der Dokumentation und bietet zum anderen auch genügend Flexibilität in Bezug auf die Anpassbarkeit der Anwendung.

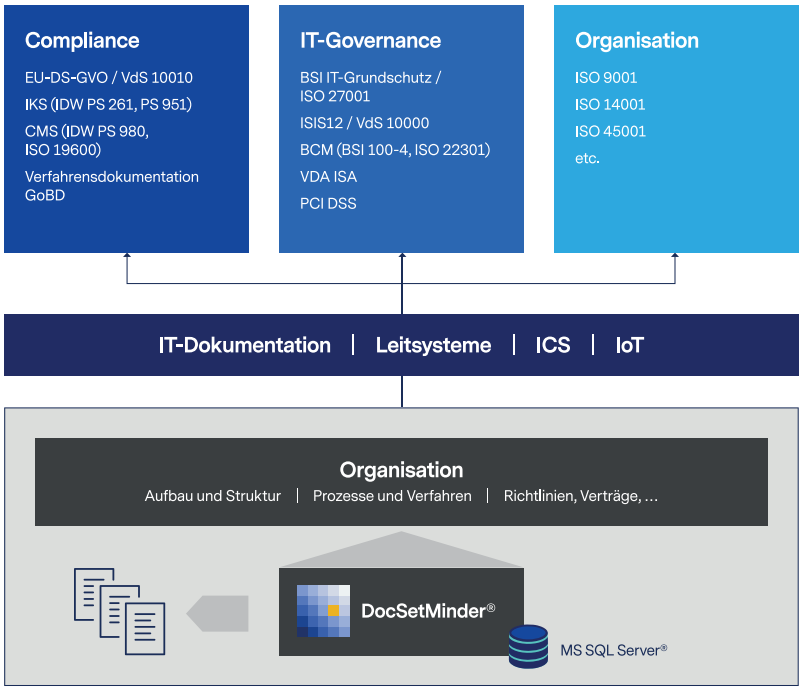
Modellierung, Risikoanalyse und Berichte

Das DocSetMinder-Modul „IT-Grundschutz“ bildet das Schichtenmodell des IT-Grundschutz-Kompendiums ab. Bei Bedarf lassen sich die Schichten jederzeit vom dazu berechtigten Benutzer erweitern. In den systemorientierten Schichten kann zunächst aus der Dokumentation der IT-Infrastruktur im Modul „IT-Dokumentation“ die Komplexitätsreduktion und Bildung von Zielobjekten vorgenommen werden. Anschließend werden den Zielobjekten ebenso wie den prozessorientierten Schichten die Bausteine aus dem IT-Grundschutz-Kompendium hinzugefügt.

Dabei erkennt DocSetMinder automatisch die jeweilige Schicht und schlägt die entsprechenden Bausteine vor. Bereits in anderen, gleichartigen Zielobjekten befindliche Bausteine lassen sich kopieren oder verlinken, was zu einer Reduktion des Dokumentationsaufwandes führt. Je nach gewählter Absicherungsmethode („Basis-Absicherung“, „Standard-Absicherung“ oder „erhöhter Schutzbedarf“) werden in den Bausteinen nur die der Methode entsprechenden Sicherheitsanforderungen dargestellt. Auf dieser Basis kann die Dokumentation der Umsetzung vorgenommen werden.

Eine Risikoanalyse nach dem BSI Standard 200-3 kann in DocSetMinder entweder auf einen ganzen IT-Verbund oder auf einzelne Zielobjekte durchgeführt werden sowie bei Bedarf losgelöst von Zielobjekten in eigenen Verzeichnissen. In Abhängigkeit von der Zuordnung der Bausteine zum Zielobjekt werden potenzielle Gefährdungen des G0-Katalogs anhand der BSI-Kreuzreferenztabellen bereits vorausgewählt; die Auswahl lässt sich vom Anwender reduzieren oder erweitern. Nach Bestätigung der relevanten Gefährdungen wird für jede ausgewählte Gefährdung eine Risikoanalyse erstellt, in der die Risikobewertung und die Risikobehandlung dokumentiert werden können. Hierzu wird zunächst die Beeinträchtigung der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit und optional auch Authentizität) dokumentiert, wobei auch hier DocSetMinder je nach betrachteter Gefährdung eine Vorauswahl für den Anwender trifft. Anschließend wird das Risiko vor und nach Umsetzung von ergänzenden Maßnahmen mit einer 4x4-Matrix nach Eintrittswahrscheinlichkeit und Auswirkung bewertet. Falls erforderlich, kann die Dimensionierung der Matrix leicht angepasst werden. Für die Dokumentation von ergänzenden Sicherheitsmaßnahmen kann man sich entweder der Sicherheitsanforderungen aus dem BSI-Kompendium bedienen oder eigene Maßnahmen dokumentieren und anschließend in den Risikoanalysen verlinken.

Für die Auswertung der im Modul „IT-Grundschutz“ erfassten Inhalte steht das Berichtsmodul in DocSetMinder zur Verfügung. Neben den Standard-Reports (A0-A6), die nach den Vorgaben des BSI entwickelt wurden, ist es möglich, mithilfe des integrierten Berichtsdesigners benutzerdefinierte Berichte zu erstellen oder die Standard-Berichte anzupassen, sollte diesbezüglich Bedarf bestehen.



DocSetMinder ist modular aufgebaut.

Kompendium Update in DocSetMinder

Wie zuvor beschrieben werden unter anderem bei der Dokumentation des IT-Grundschutzes die Bausteine aus dem IT-Grundschutz-Kompendium und die darin befindlichen Sicherheitsanforderungen genutzt. Die jeweils aktuelle Version des Kompendiums befindet sich in den Stammdaten (Katalogen) in der jeweiligen DocSetMinder-Installation (Datenbank). Auf Basis der Stammdaten werden die Bausteine und Sicherheitsanforderungen in den jeweiligen IT-Verbünden und Schichten beziehungsweise Zielobjekten hinzugefügt und deren Umsetzung dokumentiert.

Das BSI veröffentlicht jährlich im Februar eine neue Edition des Kompendiums. Die Kompendium-Aktualisierungen werden umgehend in DocSetMinder übernommen und können anschließend in die Kundeninstallation geladen werden. Der Benutzer kann selbst entscheiden, wann das Update der für die Modellierung verwendeten Bausteine stattfinden soll, zum Beispiel für den Fall, dass ein Audit unmittelbar bevorsteht. Im Zuge des Updates werden neue Bausteine und Sicherheitsanforderungen ergänzt und vorhandene aktualisiert. Entfallene Bausteine werden als solche gekennzeichnet. Sie stehen weiterhin zur Verfügung, lassen sich bei Bedarf aber komfortabel ausblenden.

Durch das Update erhalten alle angepassten Elemente einen gut erkennbaren Hinweis in den Metadaten des Dokuments, welcher ebenfalls als Parameter für eine automatisierte Suche nach aktualisierten Inhalten genutzt werden kann. Zusätzlich werden die jeweiligen Sicherheitsanforderungen mit einem speziellen Icon versehen. Dieses signalisiert dem Anwender, dass etwaige Änderungen bewertet werden sollten. Über das Änderungsprotokoll, das für jedes Element (Dokument) in DocSetMinder geführt wird, und die darin verfügbare Funktion, sich Änderungen anzeigen lassen zu können, kann der Anwender jederzeit komfortabel bewerten und entscheiden, ob bei der Dokumentation „nachgebessert“ werden muss. So kann die Dokumentation aktuell gehalten werden und Sie sind „Ready for Audit.“