Umsetzung von BSI IT-Grundschutz mit DocSetMinder

Die Veröffentlichung des modernisierten IT-Grundschutzes liegt drei Jahre zurück. Dank der möglichen stufenweisen Umsetzung eines Informationssicherheits-Managementsystems mittels Basis-, Kern- und Standardabsicherung und dem eigens für Kommunalverwaltungen konzipierten IT-Grundschutz-Profil erweist sich die BSI-Methodik als ausgewogenes Instrument für Organisationen, die effektiv und effizient ein angemessenes Sicherheitsniveau für ihre Daten und Informationen erreichen möchten.

Von Piotr W. Nürnberg, Allgeier CORE GmbH

Eine wirksamkeitsorientierte Umsetzung des Informationssicherheits-Managementsystems geht, unabhängig von der gewählten Vorgehensweise, mit einer adäquaten Gewichtung und sorgfältigen Planung des Projektes einher. Es ist ausschlaggebend, dass die Organisationsleitung die Verantwortung für die Etablierung des ISMS übernimmt, die notwendigen Ressourcen bereitstellt und für ein kompetentes Projektteam und Projektmanagement sorgt. Nicht zu vernachlässigen ist auch die Auswahl eines passenden Tools, mit dem die Planung und Umsetzung des Informationssicherheitsprozesses dokumentiert werden. Die im Tool erfassten Inhalte tragen zum einen zur strukturierten, transparenten und nachvollziehbaren Projektarbeit bei und ermöglichen zum anderen eine effektive und effiziente Verfügbarmachung des erstellten Informationssicherheitskonzeptes für interne und externe Zwecke, wie zum Beispiel Audits.

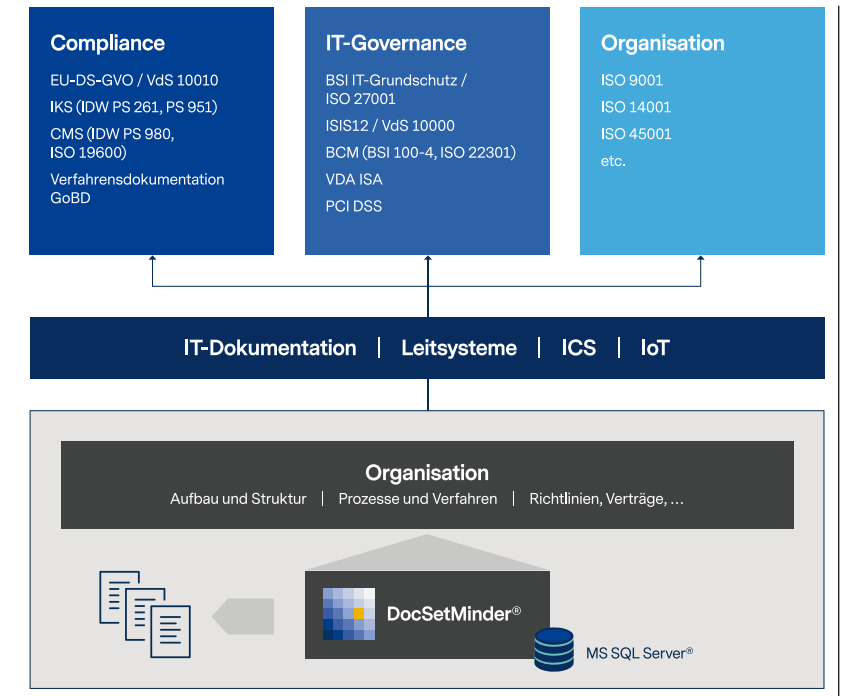
Strukturanalyse

Von elementarer Bedeutung für das Gelingen des Informationssicherheitsprozesses ist eine genaue Kenntnis der Aufbau- und Ablauforganisation ebenso wie der darunterliegenden IT-Infrastruktur. Diese werden im Rahmen einer sogenannten Strukturanalyse erfasst. Im Mittelpunkt der Analyse stehen die Geschäftsprozesse/Fachverfahren und die darin verarbeiteten Daten und Informationen. Sie stellen die oberste Ebene der Schutzbedarfsstellung dar. Der festgestellte Schutzbedarf wird anschließend auf die unterstützenden Anwendungen, IT-Systeme, Räume, Gebäude und Gelände unter Berücksichtigung von möglichen Redundanzen und Aggregationen vererbt. Ein geeigneter GSTool-Nachfolger, wie DocSetMinder, unterstützt die in das Projekt involvierten Mitarbeiter bei der Erfassung der Behörden- beziehungsweise Unternehmensorganisation im erforderlichen Detaillierungsgrad und entlang der BSI-Methodik. Neben einem Flowchart-Editor für Organigramme, Prozesslandkarten und Netzpläne stehen den Anwendern vorgefertigte, anpassbare Verzeichnisstrukturen und Dokumentklassen für Organisationseinheiten (Bereiche, Abteilungen, Teams), Geschäftsprozesse/Fachverfahren und Verantwortlichkeiten (Rollen) zur Verfügung. Für die Aufnahme der IT-Prozesse, wie Change- und Incident-Management, bietet DocSetMinder eine ITIL-konforme Struktur. Der nächste Schritt bei der Durchführung einer Strukturanalyse besteht in der Erfassung der IT-Infrastruktur und deren Verknüpfung mit der Aufbau- und Ablauforganisation zum Aufzeigen der Abhängigkeiten. Aufgrund einer starken Verbreitung von Inventarisierungs-Tools ermöglicht DocSetMinder einen automatischen, strukturierten und bei Bedarf auch systematischen Import der Inhalte aus anderen Systemen. Zur Vermeidung einer redundanten Datenhaltung kann optional mit Verlinkungen auf webbasierte Systeme gearbeitet werden. Die Struktur der IT-Dokumentation in DocSetMinder bildet das Schichtenmodell des IT-Grundschutz-Kompendiums ab und erleichtert im weiteren Projektverlauf die Gruppierung der Komponenten zu Zielobjekten und damit die Reduktion der Komplexität der Infrastruktur (Anwendungen, Daten/Informationen, Serversysteme, Arbeitsplätze, passive und aktive Netzwerkkomponenten, sowie Räume und Gebäude).

Modellierung

Der Informationsverbund (bzw. die Verbünde) in DocSetMinder bildet das Schichtenmodell aus dem BSI IT-Grundschutz-Kompendium vollständig ab. Bei Bedarf kann diese Struktur individuell erweitert werden. Bei der Modellierung der einzelnen Schichten und Zielobjekte schlägt DocSetMinder die zur jeweiligen Schicht und dem Zielobjekttyp passenden Bausteine automatisch vor. Bausteine, die für Schichten und Zielobjekte gleicher Art verwendet

wurden – im selben oder anderen Verbund – können kopiert oder verknüpft werden (Stammordner-Funktion). In Abhängigkeit von der gewählten Absicherungsmethode (Basis-, Standardabsicherung oder erhöhter Schutzbedarf) werden in den modellierten Bausteinen nur die der Methode entsprechenden Sicherheitsanforderungen mit dazugehörigen Umsetzungsanforderungen und Umsetzungshinweisen angezeigt. Beim Wechsel auf eine höhere Absicherungsstufe (z. B. von Basis- auf Standardabsicherung) werden die zusätzlichen Sicherheitsanforderungen automatisch hinzugefügt. Die in jedem Baustein hinterlegten Kreuzreferenztabellen erleichtern den bei hohem und sehr hohem Schutzbedarf des Zielobjektes erforderlichen Schritt der expliziten Risikoanalyse, indem die zu betrachtenden elementaren Gefährdungen aus dem Kompendium automatisch vorgeschlagen werden. Eine händische Anpassung durch den Anwender ist durch Aus- und Abwählen der entsprechenden Checkboxen möglich.



DocSetMinder ist modular aufgebaut

Risikoanalyse

Der Risikoanalyse im DocSetMinder-Modul „IT-Grundschutz“ liegt der BSI-Standard 200-3 zugrunde, welcher den Ablauf in klar definierte Schritte strukturiert. Die Identifikation der Risiken erfolgt auf Basis des G0-Kataloges aus dem IT-Grundschutz-Kompendium. Benutzerdefinierte Gefährdungen können bei Bedarf ergänzt werden. Die Risikobewertung definiert sich als Produkt von Auswirkung (Schadenshöhe) und Eintrittswahrscheinlichkeit. Sie wird mithilfe einer Risikomatrix durchgeführt, deren Dimensionierung (im Standard 4x4) und die zugrundeliegenden Parameter organisationsspezifisch festgelegt werden können. In Abhängigkeit von den Risikoakzeptanzkriterien wird eine Risikobehandlungsmethode ausgewählt: Akzeptanz, Vermeidung, Verlagerung oder Reduktion. Generell werden im Rahmen der Risikobehandlung technisch-organisatorische Maßnahmen geplant und umgesetzt. Nach der Umsetzung wird das verbleibende Restrisiko neu bewertet. DocSetMinder ermöglicht ein Kopieren und Verlinken der durchgeführten Risikoanalysen zwischen den Zielobjekten. Erwähnt sei auch, dass die betrachteten Grundwerte Vertraulichkeit, Integrität, Verfügbarkeit und (optional) Authentizität erweitert werden können (z. B. B3S oder Standard-Datenschutzmodell). Die Prozesse der Risikobeurteilung und -behandlung lassen sich übergreifend für ISMS, BCMS und DSMS umsetzen.

Reporting

Für die Auswertung des erstellten Informationssicherheitskonzeptes stehen den Anwendern die für den BSI IT-Grundschutz erforderlichen Berichte A0-A6 zur Verfügung. Darüber hinaus können schnell, unkompliziert und ohne Mitwirkung des Herstellers benutzerdefinierte Berichte konfiguriert werden. Die Definition der SQL-Abfrage und die Gestaltung von an der Corporate Identity der Institution ausgerichteten Layouts erfolgen bequem über einen grafischen, intuitiv aufgebauten Editor. Alle Berichte in DocSetMinder können nach spezifischen Parametern gefiltert (z. B. Anzeige der unbenutzten Bausteine oder der nicht umgesetzten Sicherheitsanforderungen) und in gängige Formate, wie PDF, Excel, RTF etc., exportiert werden.

Fazit

Die Compliance-Management-Software DocSetMinder bildet den IT-Grundschutz einschließlich Branchen- und Sektor-Profilen vollständig ab. Sie zeichnet sich durch ihre unmittelbar aus den BSI-Standards 200-1 bis 200-3 abgeleitete Struktur und Dokumentklassen mit Plausibilitäts-Checks und Automatismen (z. B. Schutzbedarfsvererbung), ebenso wie eine selbst in sehr großen Informationsverbünden stabile Performance aus. Der Funktionsumfang der Lösung macht den Einsatz von weiteren Tools oder Office-Anwendungen für die Planung, Umsetzung und Dokumentation des Informationssicherheitskonzeptes für eine mögliche Zertifizierung überflüssig. DocSetMinder ist Best Practice – und Sie sind jederzeit „Ready for Audit“.