ISMS für KRITIS

B3S mit DocSetMinder umsetzen

Sieben branchenspezifische Sicherheitsstandards (B3S) dienen der Umsetzung von § 8a (1) des BSI-Gesetzes. Weitere Standards befinden sich in der Eignungsprüfung. Die Compliance-Management-Software DocSetMinder spiegelt die Struktur der Handlungsempfehlungen von B3S wider und unterstützt alle Beteiligten bei der Umsetzung und Prüfung der verpflichtenden organisatorischen und technischen Sicherheitsmaßnahmen.

Von Krzysztof Paschke, Allgeier CORE GmbH

Zu den entscheidenden Erfolgsfaktoren bei der Umsetzung eines B3S gehört neben einem kompetenten Projektteam und Projektmanagement für das Informationssicherheits-Managementsystem (ISMS) auch das eingesetzte ISMS-Tool. Die hohen Anforderungen der Sicherheitsstandards an das Dokumentenmanagement und eine fachlich-inhaltliche Unterstützung während der Umsetzung und Aufrechterhaltung der Sicherheitsmaßnahmen lassen sich nur bedingt mit Office-Anwendungen realisieren. Die Compliance-Management-Software DocSetMinder stellt hier eine bewährte Alternative für eine effiziente Umsetzung der Informationssicherheit dar.

Geltungsbereich und Schutzziele

Eine genaue Kenntnis der Organisation und ihrer Assets ist eine elementare Voraussetzung für die Bestimmung von Geltungsbereich und KRITIS-Schutzzielen. Für das notwendige Asset-Management stehen in DocSetMinder die Module „Organisation“, „IT-Dokumentation“ und „Steuerungs- und Leitsysteme“ zur Verfügung. Die Module bieten alle nötigen Strukturen und Dokumentklassen für die Erfassung der Aufbau- und Ablauforganisation im erforderlichen Detaillierungsgrad. Erfasst werden können sämtliche Organisationseinheiten (z. B. Bereiche und Abteilungen) sowie Geschäftsprozesse, Verfahren und Verantwortlichkeiten (Rollen). Schnittstellen zu extern erbrachten Leistungen lassen sich transparent aufzeigen. Für die Dokumentation der IT-Prozesse steht die ITIL-Struktur zur Verfügung. Verträge und Richtlinien können erstellt, aktualisiert und beispielsweise via Browser kommuniziert werden. Der integrierte Flussdiagramm-Editor unterstützt die grafische Darstellung (u. a. nach BPMN) der Sachverhalte. Das Modul „IT-Dokumentation“ ermöglicht eine systematische Dokumentation der IT-Infrastruktur: Passive und aktive Netzwerkkomponenten, Serversysteme, Arbeitsplätze, Peripheriegeräte, Dienste und Anwendungen sowie Gebäude, Gebäudesicherheit und Räume. Die Dokumentation stellt die logischen Zusammenhänge zwischen Geschäftsprozessen, Software und Serversystemen sowie den Speicherorten für die verarbeiteten Daten dar. Das Modul „Steuerungs- und Leitsysteme“ bildet den IT-Sicherheitskatalog der Bundesnetzagentur und die Vorgaben des BDEW ab und ist in drei Technologiekategorien strukturiert: Leitsysteme und Systembetrieb, Übertragungstechnik und Kommunikation, Sekundär-, Automatisierungs- und Fernwirktechnik. Der zu berücksichtigende gesetzliche Rahmen wird im Rechtskataster erfasst.

ISMS – ISO/IEC 27001

Das Modul „ISO/IEC 27001“ in DocSetMinder bildet die High Level Structure der ISO-Welt ab und fördert den prozessorientierten Ansatz im PDCA-Zyklus. Die Software wird mit passenden Gefährdungs- und Maßnahmenkatalogen ausgeliefert. Dazu gehören neben Maßnahmen aus dem Annex A der ISO/IEC 27001 und den Katalogen/dem Kompendium des BSI die Maßnahmen der betreffenden B3S-Standards. Eine individuelle Erweiterung der Gefährdungs- und Maßnahmenkataloge ist problemlos möglich. Die Maßnahmen werden u.a. bei der automatischen Erstellung der Anwendbarkeitserklärung (SoA), der Projektplanung (Umsetzungsstatus der Maßnahmen und Verantwortlichkeiten) und der Planung von internen Audits verwendet. Das ISMS-Projektteam kann zwischen zwei Umsetzungsmethoden wählen:

ISO/IEC 27001 „nativ“ oder unter Einbeziehung einiger Aspekte aus dem BSI IT-Grundschutz, wie zum Beispiel Schutzbedarfsfeststellung und -vererbung. Alternativ kann das Modul „BSI IT-Grundschutz“ verwendet werden.

ISMS – BSI Standard 200-2

DocSetMinder bildet mit dem Modul „BSI IT-Grundschutz“ konsequent alle Anforderungen und die Methodik der BSI Standards 200-2/3 ab. Durchdachte Softwarefunktionen unterstützen die Anwender aktiv in jeder Phase des Sicherheitsprozesses. Den Kern des Moduls bildet das Schichtenmodell des IT-Grundschutz-Kompendiums für die Modellierung der prozess- und systemorientierten Bausteine. Das Schichtenmodell lässt sich bei Bedarf individuell erweitern. Während der Modellierung der einzelnen Schichten und Zielobjekte werden die passenden Bausteine automatisch vorgeschlagen. Bausteine, die bereits bei anderen Zielobjekten gleicher Art verwendet wurden, können kopiert oder verlinkt werden. Der festgestellte Schutzbedarf kann gemäß den BSI-Methoden auf die untergeordneten Schichten vererbt werden. Die Abhängigkeiten zwischen den Zielobjekten in unterschiedlichen Schichten lassen sich automatisch grafisch darstellen. Damit werden Ausfälle von Zielobjekten, wie zum Beispiel Storage, und deren Auswirkung auf die kritischen Dienstleistungen leicht simuliert.

Risikomanagement für kritische Dienstleistungen

KRITIS-Organisationen sind verpflichtet, ein geeignetes Management aller für die kritischen Dienstleistungen relevanten Risiken zu etablieren. Dafür stehen in DocSetMinder wahlweise das Risikomanagement gemäß BSI-Standard 200-3 und ISO 27005 zur Verfügung. Für die Risikoidentifikation werden in der Regel die genannten Gefährdungs- und Schwachstellenkataloge verwendet. Die Risikoanalyse unterstützt die Bewertung der Risiken unter Berücksichtigung von Eintrittswahrscheinlichkeit und Auswirkung in Form einer 4x4-Matrix. Die Dimensionen der Risikomatrix lassen sich bei Bedarf individuell anpassen. Die Auswirkung wird aus den beliebig definierbaren und erweiterbaren Schadenskategorien, zum Beispiel den des IT-Sicherheitskatalogs, errechnet.

Notfallmanagement

Für die Umsetzung des betrieblichen Kontinuitätsmanagements (BCM) steht das Modul „Notfallmanagement“ zur Verfügung. Mithilfe dieses Moduls kann das Notfallmanagement wahlweise gemäß BSI-Standard 100-4 oder nach ISO 22301 geplant und realisiert werden. Das Modul zeichnet sich durch seine klare Struktur mit funktionalen Vorlagen (Dokumentklassen) für die Dokumentation des Anwendungsbereichs, der Notfallorganisation, der Business-Impact-Analyse für kritische Dienstleistungen (inkl. Berechnungsformeln) und der Risikoanalyse aus. Das Handbuch für spezifische Notfallszenarien beinhaltet Handlungsanweisungen für drei Phasen des Notfalls: Alarmierung/Sofortmaßnahmen, Geschäftsfortführungspläne und Wiederherstellung des Normalbetriebes (Wiederanlauf). Das mit DocSetMinder generierte Notfallhandbuch lässt sich ausdrucken oder als HTML auf einen USB-Stick speichern. Zudem kann es allen involvierten Mitarbeitern (Notfallteams und Krisenstab) einer Institution per FTPS-Upload auf Mobilgeräten bereitgestellt werden. Die Notfallübungen können geplant, ihre Durchführung dokumentiert und bewertet werden. Festgestellte Unzulänglichkeiten können in Form von Korrekturmaßnahmen erfasst und umgesetzt werden.

Reporting und Word-Export

Für die Auswertung des Sicherheitskonzeptes gemäß B3S steht den Anwendern ein leistungsstarkes und intuitiv bedienbares Reporting zur Verfügung. Die Reports A0-A6 werden sowohl für das Modul „BSI IT-Grundschutz“ als auch „ISMS ISO 27001“ standardmäßig ausgeliefert. Sie können durch den Anwender selbständig und ohne Mitwirkung des Herstellers um individuelle Reports erweitert werden. Die bestehenden Reports lassen sich schnell und problemlos an die Anforderungen der Organisation anpassen. Die Reporting-Funktion ist benutzerfreundlich und verfügt über einen Editor für die Layout-Gestaltung. Im Report können beliebige Werte „verdichtet“ und in Form von Grafiken (Kreis-, Balkendiagramm etc.) angezeigt werden. Alternativ lässt sich die gesamte B3S-Dokumentation oder aber nur ihre ausgewählten Teile in MS Word oder PDF extrahieren.

Fazit

Die branchenspezifischen Sicherheitsstandards B3S können mit DocSetMinder vollständig geplant und umgesetzt werden. Die dokumentierten Sachverhalte dienen dem Nachweis gemäß § 8a (3) BSIG und können als Prüfgrundlage verwendet werden. Der Funktionsumfang der Software macht den Einsatz weiterer Tools oder Office-Anwendungen überflüssig. Die Lösung ist einfach zu implementieren und intuitiv bedienbar. Die gemeinsame Nutzung der erfassten Informationen in der Organisation bietet jedem Verantwortlichen einen enormen Mehrwert durch die Aktualität und eine signifikante Zeitersparnis bei der Vorbereitung von internen und externen Audits. DocSetMinder ist Best Practice - und Sie sind jederzeit „Ready for Audit“.