ISMS für KRITIS

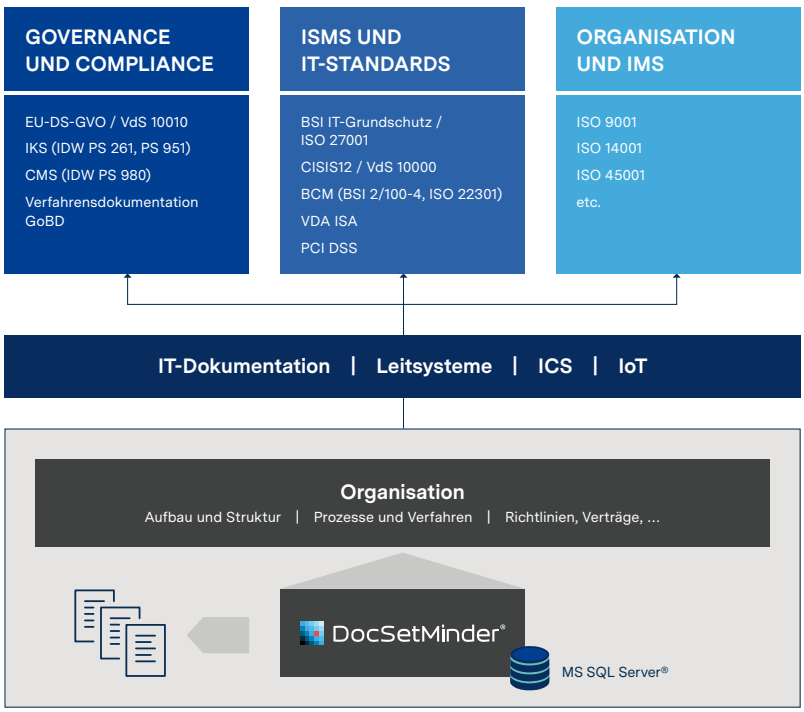
Umsetzung eines Informations-sicherheits-Managementsystems mit DocSetMinder

Um die Versorgung der Bevölkerung mit kritischen Dienstleistungen zu gewährleisten, nimmt der Gesetzgeber die Betreiber in die Pflicht, für die Sicherheit der von ihnen verarbeiteten Daten und Informationen angemessen zu sorgen. Zwar verfügen KRITIS-Organisationen in der Regel seit mehreren Jahren über ein funktionierendes ISMS, in vielen Fällen erweisen sich die gewählten Dokumentations-Tools aber als ungeeignet für eine langfristige Fortschreibung des Informationssicherheitskonzepts.

Von Piotr W. Nürnberg, Allgeier GRC GmbH

Sorgfältige Planung und adäquate Gewichtung des Informationssicherheits-Managementsystems (ISMS) stellen eine Grundvoraussetzung für dessen nachhaltige Umsetzung in Organisationen jeglicher Art und Größe dar. So muss die Leitungsebene die Verantwortung für die Informationssicherheit übernehmen, für den Aufbau eines qualifizierten Teams und ein Prozessmanagement sorgen; dieses muss sie fortan auch mit den notwendigen Ressourcen ausstatten. Da die Planung und Umsetzung des Informationssicherheits-Managementsystems konkreten normativen Anforderungen an die Dokumentation unterliegen, prägt die Auswahl eines geeigneten ISMS-Tools maßgeblich die Arbeit aller Beteiligten. Die im Tool dokumentierten Inhalte schaffen Struktur und Transparenz im Informationssicherheitsprozess und dienen in ihrer Gesamtheit der Nachweiserbringung gegenüber den Prüfern im ISMS-Audit.

Aufbau von DocSetMinder



Asset-Management

Ein wirksamer Schutz vor Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen ist erst dann möglich, wenn sowohl sie selbst als auch die zu ihrer Verarbeitung eingesetzten anderen Assets eindeutig identifiziert sind. Die genaue Kenntnis der Aufbauorganisation, der Prozesslandschaft und der für die Ausübung der Prozesse erforderlichen IT-Infrastruktur ist deshalb eine Grundvoraussetzung für einen nachhaltigen Erfolg des Informationssicherheitsprozesses. Für die fortlaufende Inventarisierung der Assets bietet das ISMS-Tool DocSetMinder die Module „Organisation“, „IT-Dokumentation“ und „Steuerungs- und Leitsysteme“ mit vordefinierten Verzeichnisstruk-

turen und Dokumentvorlagen im erforderlichen Detaillierungsgrad. Die logischen Zusammenhänge zwischen den Prozessen, Software und Serversystemen sowie den Speicherorten für die verarbeiteten Daten lassen sich bequem mittels Verknüpfungen darstellen. DocSetMinder bietet außerdem einen integrierten Editor für Organigramme, Prozesslandkarten und Netzpläne. Organisationen, die ihre Assets bereits mit anderen Tools verwalten, können die für die Umsetzung ihres Informationssicherheits-Managementsystems erforderlichen Informationen automatisiert in die MS SQL-Datenbank von DocSetMinder importieren. Zur Vermeidung von Redundanzen sind auch Verlinkungen auf webbasierte Systeme möglich. Das ISMS-Tool DocSetMinder deckt mit seinem Funktionsumfang die Anforderungen an die Lenkung von Informationen, wie Revisionssicherheit und Versionierung, Protokollierung der Änderungen und Freigaben ab.

Business-Impact-Analyse und Risikoanalyse

Da die Relevanz für die Erbringung der kritischen Dienstleistungen je nach Organisationseinheit und Prozess variiert, hilft eine Business Impact Analyse (BIA) einen Vergleich der Prozesse und Ressourcen anhand des bei ihrem Ausfall drohenden Schadens herzustellen und damit diese methodisch für die Absicherung zu priorisieren. Die anschließende Risikoanalyse liefert Auskunft über die möglichen Ursachen des Ausfalls und die Behandlungsmethode (Reduktion/Mitigation, Vermeidung, Verlagerung, Akzeptanz) in Abhängigkeit davon, wie stark das spezifische Risiko ausgeprägt ist. Für die Identifikation, Analyse, Bewertung und Behandlung von Risiken bietet das ISMS-Tool DocSetMinder ein Risikomanagement gemäß der Norm ISO 31000 und daraus abgeleitete Risikoanalysemethoden nach ISO 27005 und BSI-Standard 200-3. Für die Risikoidentifikation können Verantwortliche auf mehrere direkt im Tool hinterlegte Kataloge mit Bedrohungen, Schwachstellen und Gefährdungen zurückgreifen (BSI-Kompendium, Annex C und D der ISO 27005, B3S etc.). Die Risikoanalyse unterstützt die qualitative Bewertung der Risiken im Hinblick auf die Auswirkung und Eintrittswahrscheinlichkeit in einer 4x4-Matrix. Sowohl die Dimensionierung der Matrix als auch die Schadenskategorien lassen sich organisationsspezifisch bestimmen. Für die Definition von organisatorischen und technischen Maßnahmen bietet DocSetMinder ebenfalls entsprechende Stammdaten (z.B. Annex A der ISO 27001/2, 27019, B3S und BSI-Kompendium). Bei Bedarf können die Kataloge um benutzerdefinierte Inhalte erweitert werden. Die zur Behandlung der Risiken definierten Maßnahmen können mithilfe der Funktion „Aufgaben & Workflows“ an die zuständigen Mitarbeiter bzw. Mitarbeitergruppen zur Erledigung delegiert und der Arbeitsfortschritt überwacht werden.

Reporting

Für die Auswertung des Informationssicherheitszustands in der Organisation bietet DocSetMinder den Verantwortlichen vorgefertigte und bei Bedarf einfach adaptierbare Standardberichte (z. B. BSI A0-A6). Außerdem verfügt das ISMS-Tool über einen integrierten Editor, mit dem herstellerunabhängig neue Berichte konfiguriert werden können. Die Definition der Datenbankabfrage und die Gestaltung des Berichtsdesigns entlang des eigenen Corporate Styleguides sind intuitiv und erfordern nur wenige Mausklicks. Die Berichte können problemlos nach gegebenen Dokumenteigenschaften gefiltert werden, zum Beispiel nach Umsetzungsstatus der Maßnahmen, Stichtag oder Verantwortlichkeiten. Eine Verdichtung der Ergebnisse mit Darstellung als Balken-, Kreis- oder Spinnennetzdiagramm ist ebenso möglich wie der Export in gängige Formate wie PDF, MS Excel, HTML, RTF zur Vorlage der Berichte bei der Leitungsebene oder einem externen Prüfer.

Fazit

Der Druck auf die kritischen Infrastrukturen, ein angemessenes Sicherheitsniveau für die verarbeiteten Daten und Informationen zu gewährleisten, rührt von der Relevanz der zu erbringenden Dienstleistung für das Allgemeinwesen her und ist seit Jahren gesetzlich verankert. Nicht wenige KRITIS-Organisationen greifen bei der Etablierung ihres Informationssicherheits-Managementsystems zunächst zu einfachen Bordmitteln wie Kalkulationstabelle und Schreibprogramm oder zu Einzelplatzversionen von ISMS-Tools und übersehen dabei die mittel- und langfristigen Nachteile für die Erstellung und fortlaufende Pflege ihrer Dokumentationen, beispielsweise aufwändige Rücksprachen, Inkonsistenzen und Medienbrüche. DocSetMinder bildet die anerkannten Standards ISO 27001 und BSI 200-x inklusive der branchenspezifischen Sicherheitsstandards (B3S) und der IT-Grundschutz-Profile über alle Phasen des Informationssicherheitsprozesses hinweg (Plan-Do-Check-Act) ab. Das seit 2004 kontinuierlich weiterentwickelte ISMS-Tool ist mandanten- und mehrbenutzerfähig. Es bietet den Verantwortlichen standardkonforme Dokumentvorlagen mit Plausibilitäts-Checks und Automatismen für zum Beispiel Schutzbedarfsvererbung und Risikoanalyse. Die integrierten Funktionen fürs Aufgaben- und Workflow-Management und das Berichtswesen sorgen für eine signifikante Zeitersparnis bei der Erstellung, Aktualisierung und Auswertung von Inhalten. DocSetMinder ist Best Practice – und Sie sind jederzeit „Ready for Audit“. Nach einem vollständigen Redesign im Jahr 2021 ist DocSetMinder auch als Webversion verfügbar.