Governance, Risk and Compliance

BSI IT-Grundschutz und EU-DSGVO mit DocSetMinder umsetzen

Positive Erfahrungen aus einer Vielzahl von Migrationsprojekten und lobendes Feedback von Sicherheitsexperten diverser Organisationen bescheinigen eine praxisnahe und intelligente Abbildung des modernisierten IT-Grundschutzes und der EU-DSGVO mit DocSetMinder. Die Benutzerführung bei der Umsetzung der Standards, der Funktionsumfang und die Bedienbarkeit von DocSetMinder sind nur einige wichtige Vorteile. Unser Beitrag skizziert einzelne Implementierungsaspekte eines Managementsystems für Informationssicherheit (ISMS).

Von Krzysztof Paschke, GRC Partner GmbH

Die hohe Akzeptanz von DocSetMinder ist vor allem der sehr guten Umsetzung der BSI-Standards 200-2/-3, der Option eines Parallelbetriebes für den Übergang der BSI-Standards 100-2/-3 zu 200-2/-3 sowie seinem an die oftmals überschaubaren Ressourcen von Organisationen angepassten Lizenzmodell zuzuschreiben. Einen wesentlichen Beitrag zur Entwicklung der Software haben, neben dem Berater- und Softwareentwicklungsteam der GRC Partner GmbH, mehrere zertifizierte IT-Grundschutz-Experten aus diversen Organisationen geleistet. DocSetMinder setzt mit dem Modul „IT-Grundschutz" konsequent alle Anforderungen und die Methodik des modernisierten IT-Grundschutzes um. Durchdachte Softwarefunktionen unterstützen die Anwender aktiv in jeder Phase des Sicherheitsprozesses, von der Planung über die Umsetzung und Dokumentation, bis hin zum Audit. Der folgende Beitrag skizziert einige wichtige Aspekte der Umsetzung in einem ISMS-Projekt.

Strukturanalyse – Fundament eines Sicherheitskonzeptes

Die Dokumentation der Geschäftsprozesse einer Organisation und Identifizierung der zugehörigen Informationen liefern die Grundinformationen für die Umsetzung des BSI-Standards 200-2, 200-3, 100-4 und des Datenschutzes nach EU-DSGVO. Für eine effiziente Durchführung der Strukturanalyse stehen im DocSetMinder zwei Module zur Verfügung: „Organisation" und „IT-Dokumentation". Das Modul „Organisation" bietet die notwendigen Strukturen und Dokumentklassen für die Dokumentation der Organisation im erforderlichen Detaillierungsgrad. Erfasst werden können sämtliche Organisationseinheiten, Geschäftsprozesse und die Verantwortlichkeiten (Rollen) in der Organisation. Für die Dokumentation der IT-Prozesse steht die ITIL-V.3-Struktur zur Verfügung. Die Organigramme und die Prozesslandschaft können mit dem integrierten DocSetMinder-Flowchart-Editor grafisch nach ISO- und BPMN-Standards abgebildet werden. Das Modul enthält ein sehr effizientes Richtlinienmanagement, zur Verwaltung aller notwendigen Leit- und Richtlinien (EU-DSGVO, ISMS, QM etc.). Für eine effektive Einbindung der externen Dienstleister und deren Aufgaben steht ein leistungsfähiges Vertragsmanagement für die Erfassung der Dienstleistungs- und Datenschutzverträge (SLAs und ADVs) zur Verfügung. Das Modul „IT-Dokumentation" unterstützt die Anwender bei der systematischen Dokumentation der IT-Infrastruktur: Netzwerkkomponenten, Kommunikationsverbindungen, Server-Systeme, Arbeitsplätze, Peripheriegeräte, Dienste und Anwendungen sowie Standorte, Gebäude, Gebäudesicherheit und Räume. Die Dokumentation stellt alle logischen Zusammenhänge zwischen Geschäftsprozessen, Anwendungen, Serversystemen inklusive Cloud-Landschaft, sowie den Speicherorten für die entstehenden Informationen (Daten) dar. Die beiden Module „Organisation" und „IT-Dokumentation" stellen das Fundament eines jeden Sicherheitskonzeptes dar.

Modellierung

DocSetMinder bildet das Schichtenmodell des IT-Grundschutz-Kompendiums, für die Modellierung der prozess- und systemorientierten Bausteine, detailliert ab. Für die Übergangsphase vom BSI 100-2/-3 zu 200-2/-3 können beide Schichtenmodelle angezeigt werden. Das Schichtenmodell kann individuell erweitert werden. Während der Modellierung der einzelnen Schichten und Zielobjekte werden

die entsprechenden Bausteine automatisch vom DocSetMinder vorgeschlagen. Bausteine, die bereits bei Zielobjekten gleicher Art verwendet wurden, können optional mit den Inhalten übernommen werden. In Abhängigkeit vom gewählten Sicherheitsniveau (Basis-, Standard-Anforderung und Anforderungen für erhöhten Schutzbedarf) werden bei den modellierten Bausteinen nur die Sicherheitsanforderungen und Umsetzungshinweise angezeigt, die zu der ausgewählten Kategorie, gemäß dem BSI IT-Grundschutz-Kompendium, gehören. Bei einem Wechsel auf eine höhere Kategorie der Absicherung werden die Sicherheitsanforderungen automatisch erweitert angezeigt.

Risikoanalyse

Die Identifikation der Risiken erfolgt unter Einbeziehung des BSI G0-Kataloges des IT-Grundschutz-Kompendiums. Bei der Zuordnung der elementaren Gefährdungen werden die BSI-Kreuzreferenztabellen genutzt. DocSetMinder erkennt den Typ der jeweiligen Zielobjekte mit den bereits modellierten Bausteinen und schlägt die dazu gehörigen Gefährdungen vor. Die Risikobewertung definiert sich als Produkt von Eintrittswahrscheinlichkeit und Auswirkung (Schadenshöhe) und wird mithilfe einer 4x4-dimensionierten Matrix durchgeführt. Die Dimension der Matrix kann individuell angepasst werden. Bei der Betrachtung der Grundwerte können drei Optionen gewählt werden: BSI-Standard (Vertraulichkeit, Integrität und Verfügbarkeit). Zusätzlich stehen Authentizität und das Standard-Datenschutzmodell (SDM der Datenschutzbehörden des Bundes und der Länder) zur Auswahl. Mit einer gut geplanten Risikoanalyse können EU-DSGVO, ISMS, Notfallmanagement und weitere Normen in der Organisation gleichzeitig effektiv und effizient behandelt werden. Ähnliches gilt auch für eine Reihe von technisch-organisatorischen Maßnahmen, die gleichermaßen für EU-DSGVO und ISMS gelten können.

Klassifikation von Informationen

Ein angemessener Schutz der Informationen beginnt mit ihrer Kennzeichnung. Dafür stehen im DocSetMinder® optional drei unterschiedliche Methoden zur Verfügung: Klassifikationsschema gemäß dem staatlichen Geheimschutz (VS), Traffic Light Protocol (TLP) und Basisklassifikation (öffentlich, interner Gebrauch, vertraulich). Bei der Erstellung der Informationen wird im Hintergrund protokolliert, wer der Ersteller, Prüfer und Genehmiger ist. Über die Systemberechtigung wird bestimmt, wer die Informationen nutzen darf. Bei der Ausgabe des Sicherheitskonzeptes, zum Beispiel in Microsoft Word, wird die Dokumentation automatisch mit einem Wasserzeichen, gemäß der ausgewählten Kennzeichnungsstufe, deutlich sichtbar markiert.

GSTOOL und die Datenübernahme

Die Praxis zeigt, dass eine vollständige Datenübernahme aus dem GSTOOL nicht möglich ist. Der wesentliche Grund dafür sind die Unterschiede zwischen den BSI-Standards 100-2/-3 und 200-2/-3. Es besteht zwar die Möglichkeit einer teilweisen Datenübernahme, ihre zukünftige Verwendbarkeit ist aber mehr als fraglich. Die „Anleitung zur Migration von Sicherheitskonzepten“ und die Migrationstabellen des BSI sind zwar wichtige Hilfsmittel, entpflichten allerdings nicht vom konzeptionellen Aufwand. Erfahrungsgemäß ist es sinnvoll zu bewerten, inwieweit eine Neuerfassung der Zielobjekte und ihre Modellierung effizienter ist als die Datenübernahme und die nachträgliche manuelle Nachbereitung. Leider wird die vollständige Datenübernahme aus dem GSTOOL in vielen Ausschreibungen als K.-o.-Kriterium genannt und führt zur Wettbewerbsverzerrung.

Reporting

Für die Auswertung des Sicherheitskonzeptes steht den Anwendern eine sehr leistungsfähige Reporting-Funktion zur Verfügung. Neben den erforderlichen Reports A0-A6 kann der Anwender selbstständig und ohne Wirkung des Herstellers weitere Reports erstellen oder die Bestehenden anpassen. Dafür sind keine besonderen SQL oder sonstige technische Kenntnisse erforderlich. Die Reporting-Funktion ist benutzerfreundlich und verfügt über einen Report-Layout-Generator. Beliebige Werte können „verdichtet“ und in Form von Grafiken (Torte, Balken etc.) angezeigt werden.

Fazit

DocSetMinder bildet die Normen und Standards von Informationssicherheit und Datenschutz vollständig ab. Der Funktionsumfang von DocSetMinder macht den Einsatz weiterer Tools oder Office-Anwendungen für die Dokumentation und Zertifizierung der umgesetzten Normen und Standards überflüssig. Die Lösung ist einfach zu implementieren und intuitiv bedienbar. Die gemeinsame Nutzung der erfassten Informationen bietet allen beteiligten Mitarbeitern und Verantwortlichen einen enormen Mehrwert durch die Aktualität der Dokumentation und eine signifikante Zeitersparnis bei der Vorbereitung interner und externer Audits. DocSetMinder ist Best Practice – und Sie sind jederzeit „Ready for Audit“. ■