Governance, Risk and Compliance mit DocSetMinder umsetzen

IT-Grundschutz mit DocSetMinder – ein Rückblick

Seit der Veröffentlichung des modernisierten BSI IT-Grundschutzes im Oktober 2017 befassen sich viele Organisationen sehr intensiv mit dessen Umsetzung. Berater und Partner der GRC Partner GmbH begleiten viele Migrationsprojekte und liefern neben der inhaltlichen Expertise mit DocSetMinder auch die erforderliche softwareseitige Unterstützung. Unser Beitrag zeigt einige Implementierungsaspekte im Rückblick.

Von Krzysztof Paschke, GRC Partner GmbH

Bereits zur letzten it-sa im Oktober 2017 präsentierte die GRC Partner GmbH ihren vollständig nach den neuen BSI-Standards 200-2 und 200-3 ausgerichteten GSTool-Nachfolger DocSetMinder. Positive Erfahrungen aus einer Vielzahl von Migrationsprojekten und lobendes Feedback von Sicherheitsexperten diverser Organisationen bescheinigen eine praxisnahe und smarte Abbildung des modernisierten IT-Grundschutzes in DocSetMinder. Die hohe Akzeptanz des GSTool-Nachfolgers ist vor allem der 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 zahlreichen Projekten.

Organisation

Die genaue Kenntnis der Aufbau- und Ablauforganisation ist eine elementare Voraussetzung für die Durchführung der Strukturanalyse, Schutzbedarfsfeststellung, Modellierung und schließlich für die Durchführung des IT-Grundschutz-Checks. Sie ist auch unerlässlich für die Umsetzung der EU-DSGVO und des Notfallmanagements. Der Großteil der Organisationen verfügte über eine sehr rudimentäre Dokumentation in Form von Organigrammen mit einem nicht ausreichenden Detaillierungsgrad und von mangelhafter Aktualität. Nur wenige Organisationen konnten eine gute bis sehr gute Dokumentation vorweisen, die zumeist mit dafür speziell konzipierten Tools erstellt worden war. Hier stellte sich die Frage: Importieren oder integrieren? Das Modul „Organisation" bietet die notwendigen Strukturen und Dokumentklassen für die Dokumentation der Organisation im erforderlichen Detaillierungsgrad. Erfasst werden können sämtliche Organisationseinheiten (z. B. Bereiche und Abteilungen), Geschäftsprozesse und die Verantwortlichkeiten (Rollen) in der Organisation. Für die Dokumentation der IT-Prozesse steht die ITIL-V.3-Struktur zur Verfügung. Das Modul enthält auch ein sehr effizientes Richtlinienmanagement zur Verwaltung aller notwendigen Leit- und Richtlinien (EU-DSGVO, ISMS, QM etc.). Im Vertragsmanagement werden sämtliche Sachverhalte zur Auftragsverarbeitung (Auftraggeber und -nehmer) erfasst und verwaltet. Bei bereits vorhandenen Dokumentationen können entsprechende Sachverhalte wie Rollen, organisatorische Einheiten und Prozesse einmalig oder wiederholend importiert werden. Bei webbasierten (Fremd-) Tools kann eine Verlinkung auf die Sachverhalte erstellt werden.

IT-Dokumentation

Ein weiterer Baustein der Strukturanalyse ist die Dokumentation der IT-Komponenten, ihrer Zusammenhänge mit der Prozesslandschaft und Organisation. Um sie zu erstellen, verwenden viele IT-Spezialisten die bereits stark verbreiteten Inventarisierungs-Tools. Auch hier stellte sich die Frage: Die CMDB importieren oder integrieren? Das Modul „IT-Dokumentation" erlaubt eine systematische, manuelle oder automatische Dokumentation durch Importe. Die Modulstruktur ist abgeleitet aus dem Schichtenmodell des BSI-Kompendiums und vereinfacht im Verlauf des Sicherheitskonzeptes die Bildung von Zielobjekten und Reduktion der Komplexität der IT-Infrastruktur (Anwendungen, Daten/Informationen, Serversysteme, Arbeitsplätze, passive und aktive Netz-

werkkomponenten sowie Räume und Gebäude). Die Dokumentation stellt die logischen Zusammenhänge zwischen Geschäftsprozessen, Software und Serversystemen sowie den Speicherorten für die entstehenden Informationen/Daten dar. Bei webbasierten CMDBs kann einfach mit Verlinkungen auf die betreffenden Sachverhalte gearbeitet werden.

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 sind als die Datenübernahme und nachträgliche manuelle Nachbereitung. Leider wird die vollständige Datenübernahme aus dem GSTool in vielen Ausschreibungen als K.-o.-Kriterium genannt und führt zur Wettbewerbsverzerrung.

Integration weiterer Standards und Gesetze

Bei der zunehmenden Anzahl gesetzlicher Auflagen und Normanforderungen empfiehlt es sich, einen organisationsweiten, ganzheitlichen Planungs- und Dokumentationsansatz in Form eines GRC-Tools zu etablieren. Anstatt jede Norm, gesetzliche Anforderung und jeden Standard einzeln zu planen und womöglich mit unterschiedlichen Tools zu realisieren, ist eine globale Betrachtung von enormem Vorteil. Die Gemeinsamkeiten bei der Planung, Umsetzung, Dokumentation und Aufrechterhaltung werden insbesondere in folgenden Bereichen deutlich: Projektmanagement, Strukturanalyse, Risikoanalyse, Überwachung und Audits. Um die Mindestanforderungen der Standards und Gesetze effizient und vollständig umzusetzen sowie aktuell zu halten, stehen den Organisationen diverse DocSetMinder-Module und Maßnahmenkataloge zur Verfügung. Dazu gehören zurzeit dreiunddreißig GRC-Module. Die Anforderungen an ein GRC-Tool lassen sich am besten von den Anforderungen an die Zertifizierung großer Rechenzentren ableiten: ISMS (BSI oder ISO 27001), Notfallmanagement (BSI oder ISO), Datenschutz (EU-DSGVO), Compliance Management (ISO oder IDW), Rechenzentrumsbetrieb (DIN 50600), Internes Kontrollsystem (IDW PS 261 oder PS 951), VdS-Reihe und Verfahrensdokumentation gemäß GoBD.

Risikoanalyse

Eine Übernahme der Risikoanalyse aus dem GSTool ist nicht möglich. Die Unterschiede zwischen der Risikoanalyse gemäß BSI-Standard 100-3 und 200-3 sind zu gravierend. Es besteht zwar die Möglichkeit, sich an den verwendeten G0-Gefährdungen und den dazugehörigen Zielobjekten zu orientieren, aber die eindeutige Empfehlung hier ist, die Risikoanalyse vollständig neu durchzuführen. Die Identifikation der Risiken wird unter Einbeziehung der BSI Gefährdungskataloge (G0 bis G5) oder des BSI G0-Kataloges (IT-Grundschutz-Kompendium) mit seinen elementaren Gefährdungen erfolgen. Die Kataloge können um benutzerdefinierte Gefährdungen erweitert werden. 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. Im weiteren Schritt wird die negative Beeinträchtigung der einzelnen Grundwerte oder Gewährleistungsziele durch das festgestellte Risiko betrachtet. Im BSI-Standard 200-3 handelt es sich dabei um Vertraulichkeit, Integrität, Verfügbarkeit und optional Authentizität. Sollte bei der Umsetzung der EU-DSGVO das Standard-Datenschutzmodell (SDM) (Datenschutzbehörden des Bundes und der Länder) berücksichtigt werden, können in der Risikobewertung weitere Gewährleistungsziele (u. a. Belastbarkeit, Authentizität, Nichtverkettung) betrachtet werden. Mit einer gut geplanten Risikoanalyse können EU-DSGVO, ISMS, Notfallmanagement und weitere Normen in der Organisation gleichzeitig effizient behandelt werden. Ähnliches gilt auch für eine Reihe von technisch-organisatorischen Maßnahmen, die gleichermaßen für EU-DSGVO und ISMS gelten können.

Fazit

DocSetMinder bildet die Normen und Standards der Informationssicherheit und des Datenschutzes vollständig ab. Mit ihrem umfassenden Angebot an verfügbaren Modulen reflektiert die Software zudem den Umstand, dass eine GRC-Suite im eigentlichen Sinne sich nicht ausschließlich auf die Umsetzung eines ISMS oder DSMS reduzieren darf.

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". ■