Informationssicherheit in der Behörde mit DocSetMinder

BSI IT-Grundschutz – Migration oder Neuanfang

Seit der Veröffentlichung des modernisierten BSI IT-Grundschutzes im Oktober 2017 befassen sich viele Organisationen sehr intensiv mit seiner Einführung. Nach wie vor gibt es Fragen zur effizienten Planung, Umsetzung und Erstellung einer belastbaren Dokumentation eines Sicherheitskonzeptes gemäß BSI-Standards Reihe 200-x. Hier einige Hinweise aus den bereits realisierten Projekten der letzten Monate.

Von Krzysztof Paschke, GRC Partner GmbH

Für eine erfolgreiche Umsetzung des modernisierten BSI IT-Grundschutzes muss eine Reihe von wichtigen Aspekten beachtet werden. Neben der Beschaffung eines adäquaten GSTOOL-Nachfolgers müssen u. a. eine mögliche Migration von alten Sicherheitskonzepten, neuen Inhalten der Strukturanalyse, die Auswahl der Vorgehensweise für das Sicherheitskonzept, die Risikoanalyse, die Definition der KPI und Reifegradbestimmung sowie das Berichtwesen berücksichtigt werden. Die Umsetzung der genannten Aspekte, wie die Praxis zeigt, ist immer noch nicht als Routineaufgabe anzusehen. Diese Erfahrungen werden zurzeit sowohl bei den IS-Management-Teams als auch bei den Auditoren gewonnen.

Migration oder Neuanfang

Die erste wichtige Entscheidung des Informationssicherheitsbeauftragten (ISB) beziehungsweise des IS-Management-Teams betrifft die Migration des vorhandenen Sicherheitskonzeptes gemäß den abgekündigten BSI-Standards der Reihe 100-x in die Reihe 200-x. Es muss entschieden werden, ob das Sicherheitskonzept migriert oder vollständig neu konzipiert werden soll. Eine wertvolle Hilfe bei dieser Entscheidung liefert die „Anleitung zur Migration von Sicherheitskonzepten“ des BSI. Sie beschreibt eine schrittweise Übernahme der Sachverhalte des bestehenden Sicherheitskonzeptes in den modernisierten IT-Grundschutz. Gleichzeitig skizziert sie aber auch die Grenzen der Migration. Die Resonanz der Anwender auf die Migration von Sicherheitskonzepten ist geteilt und kann generell in zwei Gruppen unterteilt werden: partielle Migration oder Neuanfang. Aufgrund diverser, teilweise auch wesentlicher Unterschiede zwischen den BSI-Standards der Reihe 100-x und 200-x ist eine vollständige Migration nicht möglich. Im Wesentlichen liegt das an dem neuen Schichtenmodell des IT-Grundschutz-Kompendiums und an den Inhalten der Bausteine. DocSetMinder verfügt über einen grafisch orientierten Migrationsassistenten, in dem die Sachverhalte aus dem alten Sicherheitskonzept schrittweise übernommen und in die neue Struktur migriert werden können. Der Anwender kann entscheiden, welche Zielobjekte übernommen und welche als nicht mehr aktuelle „Altlasten“ nicht übernommen werden sollen. Es besteht die Möglichkeit, sehr präzise und selektiv vorzugehen. Im nächsten Schritt können pro Zielobjekt auch die dazugehörigen Bausteine für die Migration ausgewählt werden. Auch hier kann sehr selektiv vorgegangen werden. Idealerweise sollen alte Bausteine nur auf sogenannte „im Wesentlichen identische Bausteine“ [BSI] migriert werden. Sie erfordern nur eine überschaubare manuelle Nacharbeit. Bei allen anderen Bausteinen wird, aufgrund einer hohen manuellen Nacharbeit, von der Migration abgeraten und eine erneute Modellierung mit den aktuellen Bausteinen aus dem IT-Grundschutz-Kompendium Edition 2019 empfohlen.

Strukturanalyse

Die Strukturanalyse eines IT-Verbundes ist eine Grundvoraussetzung für die Erstellung eines Sicherheitskonzeptes. Um sie zu erstellen, ist eine genaue Kenntnis der Aufbau- und Ablauforganisation erforderlich. Neu in der Strukturanalyse ist die Betrachtung der Prozesslandschaft einer Organisation. Die Prozesse und Informationen/Daten als Ergebnis ihrer Ausübung bilden die oberste Ebene der Schutzbedarfsfeststellung. Der dort festgestellte Schutzbedarf wird weiter auf die verantwortli-

chen Anwendungen, IT-Systeme, ICS- und sonstige Geräte bis hin zu den Räumen, Gebäuden und gegebenenfalls dem Gelände vererbt. Das DocSetMinder-Modul „Organisation" bietet die notwendigen Strukturen und Dokumentklassen für eine effiziente Erfassung der Behörden- oder Unternehmensorganisation 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, wie zum Beispiel Incident- oder Change-Management, steht die ITIL-konforme Prozessstruktur zur Verfügung. 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 Netzwerkkomponenten 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. Beide Module „Organisation" und „IT-Dokumentation" erfüllen alle Anforderungen der BSI-Standards Reihe 200-x für die Dokumentation der Strukturanalyse.

Risikoanalyse

Die Risikoanalyse gemäß BSI-Standard 100-3 und 200-3 ist in ihrem Aufbau und ihrer Durchführungsmethodik inkompatibel. Eine automatische Migration der bestehenden Risikoanalyse gemäß dem BSI-Standard 100-3 ist somit nicht möglich und ein Versuch sie zu migrieren nicht ratsam. Es besteht zwar die Möglichkeit, sich an den verwendeten elementaren Gefährdungen aus dem BSI G0-Katalog und den dazugehörigen Zielobjekten zu orientieren, aber die eindeutige Empfehlung hier ist, die Risikoanalyse vollständig neu durchzuführen. Die Identifikation der Risiken erfolgt unter Einbeziehung des BSI G0-Kataloges. Bei der Auswahl der zutreffenden elementaren Gefährdungen nutzt DocSetMinder die sogenannten Kreuzreferenztabellen zum IT-Grundschutz-Kompendium. Die Auswahl erfolgt automatisch anhand des Zielobjektes (Typ) und der zugeordneten Bausteine. Sie kann darüber hinaus manuell ergänzt werden. Der BSI G0-Katalog kann um benutzerdefinierte Gefährdungen erweitert werden. Die Risikobewertung definiert sich als Produkt von Eintrittswahrscheinlichkeit und Auswirkung (Schadenshöhe) und wird mit Hilfe einer 4 x 4-dimensionierten Matrix durchgeführt. Die Dimension der Matrix kann individuell angepasst werden. Im weiteren Schritt wird die negative Beeinträchtigung der einzelnen Grundwerte durch das festgestellte Risiko betrachtet. Im BSI-Standard 200-3 handelt es sich dabei um Vertraulichkeit, Integrität, Verfügbarkeit und optional Authentizität (gemäß Vorgabe der Bafin für Kreditinstitute). Bei der Risikobehandlung stehen vier Methoden zur Verfügung: Behandlung, Transfer, Vermeidung und Akzeptanz. In Abhängigkeit der gewählten Behandlungsmethode können individuelle Korrekturmaßnahmen mit dem Status, Dringlichkeit und Kosten definiert werden. Nach der Umsetzung der Maßnahmen kann die Risikoanalyse erneut durchgeführt werden. Für die Auswertung der Risikoanalyse auf Basis von IT-Grundschutz stehen zwei Gruppen von vorgeschriebenen Reports zur Verfügung: A5 und A6. In den Reports werden die festgestellten, bewerteten und behandelten Risiken nach unterschiedlichen Kriterien für involvierte Mitarbeiter und die Leitungsebene ausgewertet und dargestellt.

Fazit

Unabhängig von der Tatsache, ob ein altes Sicherheitskonzept migriert oder neu erstellt wird, leistet DocSetMinder eine effiziente und effektive Umsetzung der IT-Grundschutz-Methodik gemäß dem BSI-Standard 200-2/-3. Der Funktionsumfang des GSTOOL-Nachfolgers berücksichtigt ohne Ausnahme alle Anforderungen der BSI-Standard Reihe 200-x. In Verbindung mit weiteren Modulen, wie zum Beispiel „Notfallmanagement", „EU-DS-GVO" oder „TISAX" lassen sich weitgehend alle Aspekte der Informationssicherheit einer Institution abdecken. Der Funktionsumfang der Software macht den Einsatz weiterer Tools oder Office-Anwendungen für die Dokumentation und Zertifizierung der umgesetzten 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". ■