Digitalen Bedrohungen mit DocSetMinder entgegenwirken

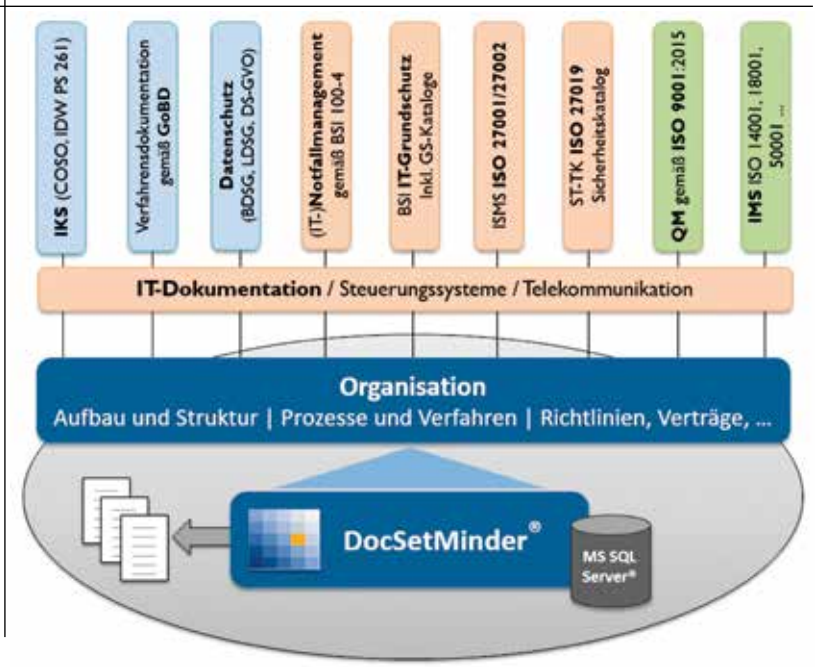
Die Innovationen der digitalen Welt sind unerlässlich für die Entwicklung unserer Gesellschaft. Doch der schnelle technologische Fortschritt und die stetig wachsende Abhängigkeit von der IT bergen viele Risiken – sie bleiben eine Herausforderung für die Informationssicherheit, der sich jede Organisation heute stellen muss.

Von Krzysztof Paschke, GRC Partner GmbH

Im Schatten steigender Komplexität und zunehmender globaler Vernetzung der IT-Welt entwickelte sich die Cyberkriminalität rasant. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Medien bestätigen täglich zahlreiche, technisch sehr gut durchdachte und gezielte Hackerangriffe auf die Wirtschaft wie auch auf die Privatsphäre der Bürger. Trotz der eindeutigen Lage herrscht in vielen Unternehmen und Behörden immer noch die Illusion von Sicherheit, nicht selten kommt es zur Vernachlässigung der IT-Risiken. Die häufig gestellte Frage: „Wie sicher sind unsere Daten und unsere IT?“ kann noch immer viel zu oft nicht eindeutig beantwortet werden.

Eine wirksame Methode, den digitalen Bedrohungen ganzheitlich und effektiv entgegenzuwirken, ist die Planung und Umsetzung eines Informationssicherheits-Managementsystems (ISMS) gemäß einer der anerkannten Normen unter Berücksichtigung des Datenschutzes gemäß der aktuellen EU-Datenschutz-Grundverordnung (DS-GVO). Aufgrund der Komplexität eines ISMS und der DS-GVO ist es empfehlenswert, einen organisationsweiten und ganzheitlichen Planungs- und Dokumentationsansatz mit DocSetMinder als „Integriertes Managementsystem“ (IMS) zu etablieren.

Anstatt jede Norm, jeden Standard oder gesetzliche Anforderung einzeln zu planen und mit unterschiedlichen Tools zu realisieren, ist eine globale Betrachtung von enormem Vorteil. Um die Mindestanforderungen der Sicherheitsstandards und Datenschutzgesetze effizient und vollständig umzusetzen und aktuell zu halten, stehen den involvierten Mitarbeitern in DocSetMinder diverse Module und standardisierte Maßnahmenkataloge zur Verfügung.



Aufbau der Compliance Management Software DocSetMinder.

Modul „Organisation“

Die genaue Kenntnis der Unternehmens- und Behördenorganisation ist eine elementare Voraussetzung für die Durchführung der Strukturanalyse und für die Planung der technischen und organisatorischen Sicherheitsmaßnahmen. Das Modul stellt die notwendigen Strukturen und Vorlagen für die Dokumentation der Aufbau- und Ablauforganisation im erforderlichen Detaillierungsgrad zur Verfügung. Erfasst werden sämtliche Organisationseinheiten (zum Beispiel Bereiche und Abteilungen) sowie Geschäftsprozesse und Verfahren mit den Verantwortlichkeiten (Rollen) in der Organisation. Für die Dokumentation der IT-Prozesse steht die ITIL V.3 Struktur zur Verfügung. Verträge und Richtlinien werden erstellt, aktualisiert und den Mitarbeitern kommuniziert. Der integrierte grafische Flussdiagramm-Editor unterstützt die grafische Darstellung (u.a. nach BPMN) der Sachverhalte.

Modul „IT-Dokumentation“

Ein weiterer Baustein der Strukturanalyse ist die Dokumentation des IT-Verbundes. Das Modul „IT-Dokumentation“ erlaubt eine systematische Dokumentation der IT-Infrastruktur: Passive und aktive Netzwerkkomponenten, Server-Systeme, Arbeitsplätze, Peripheriegeräte, Dienste und Anwendungen sowie Gebäude, Gebäudesicherheit und Räume. Die Dokumentation stellt die logischen Zusammenhängte zwischen Geschäftsprozessen, Software und Serversystemen sowie den Speicherorten für die entstehenden Daten dar. Die hier erfassten Informationen werden in den Modulen „IT-Grundschutz“, „ISO 27001“, „Notfallmanagement“ und „DS-GVO“ verwendet. Somit werden Redundanzen verhindert und Aktualisierungen vereinfacht.

Modul „IT-Grundschutz“

Das Modul bildet den BSI-Standard 100-2 und seine Methodik vollständig und ohne Einschränkung ab. Die Schutzbedarfsdefinition, Schutzbedarfsfeststellung und ihre Vererbung durch das Maximumprinzip sowie die Modellierung des IT-Verbundes ist durch die Softwareunterstützung einfach und schnell umsetzbar. Die Überwachung der festgelegten Maßnahmen kann sehr effektiv mit dem Aufgaben- und Maßnahmenplaner sowie der Reporting-Funktion realisiert werden. Das Modul „IT-Grundschutz“ ist offizieller Nachfolger des BSI GS-Tools und für Behörden kostenlos erhältlich.

Modul „ISMS ISO/IEC 27001“

Die Modulstruktur entspricht der ISO High Level Structure und erlaubt eine nahtlose Integration mit anderen bereits umgesetzten ISO-Normen in der Organisation. Die High Level Structure wird in der Praxis als Leitfaden bei der Umsetzung der Anforderungen aus Kapitel 4 bis 10 sowie der Maßnahmen aus dem Annex A der Norm. Die Vorlagen (Dokumentklassen) für die Erstellung der zertifizierungsrelevanten Dokumente, wie Leitlinie, Anwendbarkeitserklärung (SoA), Risikoanalyse und Behandlung vervollständigen das praxisnahe ISMS Modul.

Modul „(IT-)Notfallmanagement“

Mit Hilfe dieses Moduls kann das Notfallmanagement wahlweise gemäß BSI-Standard 100-4 oder nach ISO 22301 geplant und realisiert werden. Das Modul zeichnet sich aus durch eine klare Struktur mit funktionalen Vorlagen (Dokumentklassen) für die Dokumentation beispielsweise des Anwendungsbereichs, der Notfallorganisation, der Business-Impact-Analyse (inkl. Berechnungsformeln) und der Risikoanalyse. Die Alarmierung, Sofortmaßnahmen, Geschäftsfortführungs- und Wiederanlaufpläne können durch autorisierte Personen jederzeit extrahiert und als Notfallhandbücher für mobile Geräte offline zur Verfügung gestellt werden.

Modul „Katastrophenschutzplan“

Ziel des Katastrophenschutzes ist die Gewährleistung einer wirksamen Gefahrenabwehr durch das Zusammenwirken vieler Beteiligter (wie Brandschutz, Hilfeleistung und Katastrophenschutz) in Zusammenarbeit mit öffentlichen und privaten Organisationen. Dies beinhaltet alle Maßnahmen zum Schutz der Bevölkerung bei Großeinsatzlagen und Katastrophen. Das Modul unterstützt die Verantwortlichen des Katastrophenschutzes bei der Planung und Umsetzung der erforderlichen Maßnahmen sowie deren koordinierte Kommunikation an alle Beteiligte.

Risikoanalyse

Für die Durchführung der Risikoanalyse stellt DocSetMinder fünf unterschiedliche Methoden zur Verfügung, u.a. BSI-Standard 100-3, BSI-Standard 200-3 (als DRAFT) und ISO 27005. Die Risikoanalyse unterstützt die Bewertung der Risiken unter Berücksichtigung von Eintrittswahrscheinlichkeit und Auswirkung in Form einer 4x4 Matrix. Optional können weitere Faktoren und Dimensionen, wie Häufigkeit (Exposition), MxN-Matrix oder Business Impact (auch für EVU) berücksichtigt werden.

Maßnahmenkataloge

Für die Umsetzung der Sicherheitsmaßnahmen gemäß BSI IT-Grundschutz, ISO 27001 oder des IT-Sicherheitskataloges gemäß EnWG stehen dem Anwender in DocSetMinder wahlweise die IT-Grundschutz-Kataloge oder die Maßnahmen des Annex A der Normen ISO 27001 und ISO 27019 zur Verfügung. Die Kataloge können individuell erweitert werden. Die nachträglich durch BSI oder ISO bereitgestellten Ergänzungen von Bausteinen oder Maßnahmen werden mit der bestehenden Dokumentation synchronisiert.

Fazit

DocSetMinder bildet die anerkannten Standards der Informationssicherheit wie auch den Datenschutz vollständig ab. 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 für jeden Verantwortlichen einen enormen Mehrwert durch die Aktualität und eine signifikante Zeitersparnis bei der Vorbereitung von internen und externen Überprüfungen. Mit DocSetMinder sind Sie jederzeit „Ready for Audit“.

Messestand: Halle 5, Stand F38