IT-Security von Allgeier

Tools für den IT-Sicherheitsprozess

Zu den entscheidenden Erfolgsfaktoren bei der Planung und Etablierung eines Informationssicherheits-Managementsystems (ISMS) gehören neben einem kompetenten Projektteam und Projektmanagement auch die verwendeten Tools. Durchdacht eingesetzt helfen sie maßgeblich bei der Umsetzung einer Vielzahl von Sicherheitsanforderungen im gesamten IT-Sicherheitsprozess und liefern die benötigten Umsetzungsnachweise sowie die notwendige Dokumentation für das Audit.

Von Krzysztof Paschke, Allgeier CORE GmbH

Das IT-Security-Portfolio der Allgeier Technologie-Gruppe zeichnet sich durch aufeinander abgestimmte und sich gegenseitig ergänzende Produkte aus, die in allen Phasen des Lebenszyklus eines ISMS (P-D-C-A) eingesetzt werden können. Gekoppelt mit der langjährigen Erfahrung und kompetenten Beratung im Bereich der Informationssicherheit und der Compliance bietet Allgeier ein umfassendes Angebot für Lösungen und Services zur Cybersicherheit.

Organisation der IT-Sicherheit mit DocSetMinder

Die hohen Anforderungen der ISMS-Standards, insbesondere der Norm ISO/IEC 27001 und der BSI Standards 200-x, an die Dokumentation sowie fachlich-inhaltliche Unterstützung während der Planung, Umsetzung und Aufrechterhaltung der Sicherheitsmaßnahmen können nur bedingt mit Office-Anwendungen realisiert werden. In Abhängigkeit von den eingesetzten Modulen liefert die Compliance Management-Software DocSetMinder die notwendigen standardbedingten Softwarefunktionen, mit denen die Implementierung eines normkonformen Sicherheitsprozesses von der Planung über die Umsetzung und Dokumentation bis hin zum Audit effizient unterstützt wird. DocSetMinder setzt mit dem Modul „BSI IT-Grundschutz“ konsequent alle Anforderungen und die Methodik der BSI Standards 200-2/200-3 um. Kern des Moduls ist das Schichtenmodell des IT-Grundschutz-Kompendiums, welches die Modellierung der prozess- und systemorientierten Bausteine detailliert abbildet. Das Schichtenmodell kann individuell erweitert werden. Während der Modellierung der einzelnen Schichten und Zielobjekte werden die entsprechenden Bausteine automatisch vorgeschlagen. Bausteine, die bereits bei Zielobjekten gleicher Art verwendet wurden, kann man optional übernehmen. Der festgestellte Schutzbedarf lässt sich gemäß den BSI-Methoden auf die untergeordneten Schichten vererben. Zudem können die Abhängigkeiten zwischen den Zielobjekten in unterschiedlichen Schichten automatisch grafisch dargestellt werden.

Auch der Ausfall von Zielobjekten wie Storages und deren Auswirkung auf die kritischen Dienstleistungen lassen sich simulieren. Die in den prozessorientierten Bausteinen (ISMS, ORP, CON, OPS, DER) gestellten Sicherheitsanforderungen können in Form von Richtlinien, Prozessen, Verfahren und Konzepten mit dem integrierten Texteditor und Flowcharter detailliert beschrieben werden. Das vom BSI empfohlene Rollenkonzept kann inklusive Stellenbeschreibungen und Anforderungsprofile an die Mitarbeiterqualifikation umgesetzt werden. Die identifizierten rechtlichen Rahmenbedingungen werden im integrierten Rechtskataster mit den betriebsrelevanten Rechtspflichten dokumentiert. Die Umsetzungsnachweise für die Umsetzung der systemorientierten Bausteine (APP, SYS, NET, INF, IND) werden direkt in den den Zielobjekten zugeordneten Sicherheitsanforderungen dokumentiert.

Das Modul „ISO/IEC 27001“ bildet die High Level Structure der ISO-Welt ab und fordert somit den prozessorientierten Ansatz im PDCA-Zyklus. Ergänzend stehen in den Stammdaten von DocSetMinder diverse Gefährdungs- und Maßnahmenkataloge zur Verfügung. Dazu gehören vor allem die Maßnahmen aus dem Annex A der ISO/IEC 27001, optional die Maßnahmen der ISO 27019 und der BSI-Grundschutz-Kataloge. Eine individuelle Erweiterung der Gefährdungs- und Maßnahmenkataloge ist jederzeit

möglich. Die Maßnahmen aus dem Annex A und der ISO 27019 werden bei der automatischen Erstellung der Anwendbarkeitserklärung (SoA), der Projektplanung (Umsetzungsstatus der Maßnahmen und Verantwortlichkeiten) und Planung der internen Audits verwendet. Das ISMS-Projektteam kann zwischen zwei Umsetzungsmethoden wählen: ISO/IEC 27001 „nativ" oder unter Einbeziehung einiger Aspekte des BSI IT-Grundschutzes, wie Schutzbedarfsfeststellung und -vererbung. Alternativ kann das Modul „BSI IT-Grundschutz" verwendet werden.

Netzwerkmanagement mit SCUDOS

Die SCUDOS-Plattform ist eine adaptive Sicherheitsmanagementlösung für Netzwerkinfrastruktur und eine ideale Ergänzung für DocSetMinder. Durch Einsatz von agentenlosen Mapping- und Fingerprinting-Techniken wird das Netzwerk vollständig gescannt und seine Topologie mit den inventarisierten IT-Komponenten in Echtzeit dargestellt (Netzplan). Mithilfe von SCUDOS-Plattform-APIs werden die eingesetzten IoT- und POC-Systeme, Industriesensoren sowie BYOD-Geräte ebenfalls erfasst und sichtbar gemacht. Die damit erreichte Transparenz liefert die notwendigen Informationen für die Durchführung der Strukturanalyse als Ausgangspunkt jedes IT-Sicherheitskonzeptes. Gleichzeitig deckt sie den Einsatz von nicht autorisierten Geräten auf und verhindert unbefugten Zugriff auf die Netzwerkinfrastruktur mithilfe von Whitelisting. Die automatischen Bedrohungsabwehrmechanismen initiieren proaktive Sicherheitsmaßnahmen, indem zum Beispiel ein Gerät vom Netzwerk getrennt oder in die Quarantäne vorschoben wird. Die SCUDOS-Plattform kombiniert Netzwerkzugangskontrolle mit Geräteinventarisierung sowie Risikobewertung mit der Orchestrierung von Sicherheitsvorfällen und wandelt so traditionelle Netzwerke in transparente und hochsichere IT-Infrastrukturen um. SCUDOS mit seinen Softwarefunktionen erfüllt diverse Sicherheitsanforderung des BSI IT-Grundschutzes und der ISO/IEC 27001.

Schulung und Awareness mit Layer8

Bei der Implementierung der Informationssicherheit einer Institution muss der Faktor Mensch kritisch betrachtet werden. Der BSI IT-Grundschutz spezifiziert eine Reihe von Sicherheitsanforderungen, die sich mit der Sensibilisierung und Schulung der Mitarbeiter zur Informationssicherheit befassen. Vergleichbar behandelt die Norm ISO/IEC 27001 das Thema. Die in den Standards genannten Maßnahmen fordern geplante, themenbezogene und regelmäßige Schulungen von Mitarbeitern sowie einen entsprechenden Nachweis über die Durchführung. Bei einem Unternehmen mit mehreren hundert oder tausend Mitarbeitern können durch diese Sicherheitsanforderungen erhebliche Kosten entstehen. Hierbei sind nicht nur die Kosten für die Schulung der Mitarbeiter zu betrachten, sondern ebenso der Produktivitätsverlust, der durch die kontinuierlichen Schulungen entsteht. Die Security-Awareness-Plattform Layer8 bietet die Möglichkeit, vielfältige Security-Awareness-Trainings und Phishing-Simulationen durchzuführen. Mithilfe von diversen Schulungsvideos zu aktuellen Themen und interaktiven Schulungskampagnen (online) wird den Mitarbeitern das notwendige Wissen vermittelt. Die Schulungen können langfristig unter Berücksichtigung der Sicherheitsanforderungen und der Kosten geplant werden. Die auf den Warnungen des BSI basierenden Phishing-Templates ermöglichen realistische Simulationen, um die Beschäftigten auf diese Angriffe vorzubereiten. Durch die Kombination aus Schulung, Sensibilisierung und Auswertung kann ein tagesaktuelles Bild über das Sicherheitsbewusstsein der Mitarbeiter einer Institution erstellt werden. Über den Allgeier CORE Awareness Rahmenvertrag „Sicher gewinnt" mit der Bundesakademie für öffentliche Verwaltung sind Behörden in der Lage, ihre Mitarbeiter über zielgruppen- und themenspezifische Veranstaltungen zu sensibilisieren.

julia mailoffice

Kommunikation ohne E-Mail ist heutzutage unvorstellbar. Ein Marktführer im Bereich der E-Mail-Sicherheit ist julia mailoffice, welches zum Beispiel die virtuelle Poststelle des Bundes ist, aber auch von zahlreichen Bundesbehörden sowie namhaften Unternehmen eingesetzt wird. julia mailoffice bietet unter anderem die elektronische Ver- und Entschlüsselung sowie digitale Signatur/-prüfung für E-Mails. Über ein Regelwerk werden die Daten systematisch verschlüsselt und für den Empfänger sicher bereitgestellt, ohne dass der Absender aktiv handeln muss. Weitere Features, die julia mailoffice bietet, sind die Klassifikation eines Dokuments, Steuerung des sicheren Versands (Verschlüsselungsverfahren) durch den Empfänger, ein Outlook-Plug-in für die Wahl der Verschlüsselungs- und Versandoption durch den Versender, eine Kryptovorschau für den internen Benutzer zur Wahl der Verschlüsselungs- und Versandoptionen, die dynamische Verwaltung von PDF- und ZIP-Passwörtern, die Anbindung beliebiger Trustcenter.

Fazit

Das IT-Security-Portfolio der Allgeier Technologie-Gruppe ist ein Gesamtpaket zur Umsetzung eines ISMS. Die vorgestellten Produkte können auch unabhängig voneinander eingesetzt werden. Sie sind einfach zu implementieren, intuitiv bedienbar und können branchenunabhängig in Unternehmen und Behörden jeder Größe eingesetzt werden – und Sie sind jederzeit „Ready for Audit". ■