Die Annäherung von Grundschutz und ISO 27001

Mit seinen neuen 200-x-Standards hat sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) weiter der ISO 2700x-Normenreihe angenähert. So haben zum Beispiel die Anforderungen des IT-Grundschutz-Kompendiums jetzt einen ähnlichen Charakter wie die Controls der ISO-Standards. Die HiScout GmbH hat daher im Zuge der Modernisierung auch seine beiden Module „HiScout Grundschutz nach BSI IT-Grundschutz" und „HiScout ISM nach ISO 27001" angenähert und stärker miteinander verbunden.

Von Thomas Eimecke, HiScout GmbH

Für viele Unternehmen und Behörden ist die Einführung und Etablierung eines Informationssicherheitsmanagementsystems (ISMS) eine der größten Herausforderungen, denen sie sich bislang stellen mussten. Das Ziel, ein integriertes GRC-Managementsystem zu etablieren, scheint daher häufig unerreichbar.

Oftmals sind allein schon die organisatorischen Hürden unüberwindbar und eine Zusammenarbeit der jeweiligen Fachbereiche ist nicht immer selbstverständlich. Spätestens aber bei der Frage der Tool-Unterstützung wird es kompliziert. Denn für die einzelnen Bereiche des GRC-Umfelds gibt es viele hoch spezialisierte und gut geeignete Tools. Da diese aber eben nur einen Teilbereich bedienen, sind in den meisten Unternehmen mehrere parallel im Einsatz. Diese müssen dann, sofern überhaupt möglich, über Schnittstellen miteinander verbunden werden. Zusätzlich gibt es dann meist noch verschiedene Systeme für die Erfassung und Pflege der Stammdaten (z. B. Assets).

Diese komplexen Strukturen können mit einem geeigneten, integrativen GRC-Tool vermieden beziehungsweise abgelöst werden. Hierfür sollten im Tool die einzelnen Anwendungsgebiete zwar separat darstellbar sein, aber eben auf eine gemeinsame Datenbasis (Stammdaten) zugreifen.

Die HiScout GmbH verfolgt mit ihrer Plattform genau diesen Ansatz. Alle Module basieren auf einem flexiblen objektorientierten Datenmodell mit einem individuell konfigurierbaren Berechtigungssystem. Die einzelnen Module sind dabei speziell für ihr Anwendungsgebiet gestaltet, aber immer über die gemeinsame Datenbasis miteinander verbunden.

Geschäftsprozesse – Ein weiterer Schritt

Neben der gemeinsamen Datenbasis werden die Module der HiScout-Plattform aber auch über die Zusammenführung gemeinsamer Arbeitsschritte miteinander verbunden. So sind die Prozessschritte „Strukturanalyse" und „Schutzbedarfsfeststellung" des „HiScout Grundschutz" und „HiScout ISM" seit jeher gleich gestaltet und nutzen das gleiche Vorgehen.

So waren im HiScout-Standard auch schon für die alte Grundschutz-Vorgehensweise die Geschäftsprozesse die Basis der Schutzbedarfsaufnahme. Über die hohe Flexibilität und Anpassbarkeit der Plattform war es immer möglich, diese Erfassung, wie in den 100-x-Standards beschrieben, auf die Anwendungen umzustellen, aber eine Erfassung auf Ebene der Geschäftsprozesse war auch nie ein Hinderungsgrund für die Zertifizierung nach den 100-x-Standards.

Mit seinen neuen 200-x-Standards hat das BSI nun offiziell die Geschäftsprozesse in den Fokus der Bewertung gestellt. Das ist ein sehr guter und wichtiger Schritt in der Annäherung an die ISO 2700x-Normenreihe. Denn durch die Schutzbedarfsaufnahme auf Ebene der Geschäftsprozesse werden die größten Wissensträger der im Unternehmen verarbeiteten Informationen in den Informationssicherheitsprozess einbezogen. Damit kann eine größere Detailtiefe und Qualität der erfassten Daten erreicht, aber gleichzeitig auch mehr Awareness für die Informationssicherheit bei den Fachanwendern geschaffen werden. Auf diese Weise kann insgesamt ein höherer Reifegrad des ISMS erreicht werden.

Grundschutzanforderungen und ISO-Controls

Die neuen 200-x-Standards ergeben aber noch weitere Annäherungspunkte an die ISO 2700x-Normenreihe. So haben die An-

forderungen des IT-Grundschutz-Kompendiums im Vergleich zu den Grundschutzmaßnahmen der alten Grundschutzkataloge jetzt einen höheren Abstraktionsgrad und damit einen vergleichbaren Charakter zu den Controls der ISO 27001 erlangt.

In der HiScout-Plattform werden daher die Grundschutzanforderungen und die anwendbaren ISO-Controls gleich behandelt. Diese können so beispielsweise auch im IT-Grundschutzcheck herangezogen werden. Gleichzeitig können aber auch die Grundschutzanforderungen als Prüfpunkte im Self-Assessment des „HiScout ISM" genutzt werden. Damit wird den Anwendern beider Vorgehensweisen eine breitere und umfassendere Basis an Prüfkriterien zur Verfügung gestellt.

Risikoklassifikation über den matrixbasierten Ansatz

Einen weiteren wichtigen Schritt hat das BSI mit seinem 200-3-Standard gemacht. Über die Einführung des matrixbasierten Risikoansatzes kommt endlich eine belastbare Klassifizierungsmöglichkeit in das Risikomanagement der Grundschutz-Vorgehensweise. Eine solche Klassifizierung anhand von Eintrittswahrscheinlichkeit und Schadenshöhe ist im Bereich der ISO 2700x-Normenreihe bereits seit einigen Jahren ein etablierter Standard. Über die Einstufung der Risiken anhand der Matrix wird eine größere Detailtiefe der Bewertung erreicht. Die einzelnen Risiken können dadurch besser miteinander verglichen und priorisiert werden.

Des Weiteren lassen sich durch diese Annäherung die Ergebnisse der Grundschutz-Risikoanalyse auch besser in ein OpRisk-Management integrieren. Denn über die Klassifizierung werden sie vergleichbarer mit den Ergebnissen der Risikoanalysen aus anderen Managementsystemen.

In der HiScout-Plattform ist dieser matrixbasierte Ansatz übergreifend eingebunden. Das bedeutet, dass eine für das Unternehmen festgelegte Bewertungslogik die Basis der Risikoeinstufung in den unterschiedlichen Managementdisziplinen bildet. Die Matrix ist über die Oberfläche frei konfigurierbar und bildet die Grundlage für die im Hintergrund laufende automatische Einstufung in eine Risikoklasse. Der für die jeweilige Risikoanalyse Verantwortliche muss also nur die Eintrittswahrscheinlichkeit und Schadenshöhe bewerten und es ergibt sich automatisch die entsprechende Risikoklasse.

Bausteine als Risikoprofile

Ein Vorteil, den die Grundschutz-Vorgehensweise seit jeher bietet, ist die Vernetzung von Bausteinen und Gefährdungen. Schon für die alte Grundschutz-Vorgehensweise war im „HiScout Grundschutz" eine automatisierte Übernahme der aus der Modellierung mit Bausteinen resultierenden Gefährdungen möglich. Auch für das neue Vorgehen ist diese Übernahme weiterhin möglich und schafft somit eine wesentliche Erleichterung für den jeweiligen Risikomanager.

Diese Erleichterung kann auch im „HiScout ISM" genutzt werden. Hierbei dienen die Bausteine als eine Art Risikoprofil für die Assets. Bei der Erstellung einer Risikoanalyse kann so über die zugeordneten Profile ein Vorschlag für möglicherweise relevante Gefährdungen direkt in die Risikoanalyse übernommen werden.

Die im Vorfeld durchzuführende Zuordnung zu den Profilen kann dabei, in Anlehnung an die Modellierung des Grundschutzes, auf Einzel-Asset-Ebene (z. B. Anwendung „Outlook") durchgeführt werden, aber ebenso auch auf der Basis von Asset-Typen (z. B. E-Mail-Anwendung) erfolgen. Die Zuordnung der Grundschutzbausteine zu einzelnen Asset-Typen bildet im „HiScout Grundschutz" auch die Grundlage für die automatisierte Modellierung und wird von HiScout mitgeliefert.

Die Nutzung der neuen Grundschutzbausteine als Risikoprofile bietet eine fachlich fundierte Basis und kann natürlich durch eigene Profile erweitert werden. Diese können dann wiederum im „HiScout Grundschutz" als benutzerdefinierte Bausteine genutzt werden.

Annäherung schafft Synergieeffekte

Insgesamt lässt sich feststellen, dass sich die Grundschutz-Vorgehensweise durch die Annährungen an die ISO 2700x-Normenreihe zu einem immer kompletter werdenden Standard entwickelt hat. Während in der alten Vorgehensweise noch die umfänglichen Kataloge und die darin enthaltenen Verknüpfungen der Hauptvorteil waren, verbindet die aktuelle Vorgehensweise nun die guten Ansätze der ISO 2700x-Normenreihe mit einem umfangreichen Kompendium. Des Weiteren ist festzustellen, dass sich die über diese Annäherungen entstehenden Synergieeffekte durch ein Tool mit einem integrativen Ansatz sehr gut nutzen lassen.

Messestand: Halle 10.0, Stand 10.0-310