IT-Grundschutz-Kompendium

Migration des IT-Grundschutzes – am besten mit Tool

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seine IT-Grundschutz-Standards und Kataloge grundlegend modernisiert. Seit Oktober 2017 sind die BSI-Standards 200-x veröffentlicht; die 100-x-Reihe wird nach Ablauf einer Übergangsfrist ihre Gültigkeit verlieren. Für die Anwender des IT-Grundschutzes stellt sich nun die komplexe Thematik der Migration.

Von Tobias Seemann und Thomas Eimecke, HiScout GmbH

Um den stetig wachsenden Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) gerecht zu werden, hat das BSI seine alten 100-x-Standards grundlegend überarbeitet. Neben der Aufnahme neuer Themen und Aspekte spielte dabei aber vor allem auch die Fokussierung und Verschlankung der Inhalte eine große Rolle. Damit soll der Aufwand für die Umsetzung reduziert und somit die Hürde für die Anwendung des IT-Grundschutzes überwindbarer gestaltet werden.

Mit der Änderung der Methodik entsteht gleichzeitig aber auch die Herausforderung der Umstellung und Migration für die Anwender. Dementsprechend mussten auch die Tool-Hersteller ihre Produkte anpassen beziehungsweise umstellen. Dabei zeigt sich nun, wie flexibel die Konzepte der einzelnen Anbieter sind, um zum einen die neuen Anforderungen des BSI zügig umzusetzen und zum anderen die Anwender bei der Umstellung bestmöglich zu unterstützen.

Herausforderung hybrides Modell

Wo aber liegen die größten Herausforderungen für die Anwender und die Tool-Hersteller? Bis zum 30. September 2018 kann noch eine Zertifizierung nach BSI-Standard 100-2 mit den IT-Grundschutz-Katalogen beantragt werden. Diese Variante stellt auf den ersten Blick kein Problem für Anwender und Hersteller dar, denn es scheint so, als könne man noch drei Jahre (Zertifikatslaufzeit) komplett nach der alten Methodik arbeiten. Da aber die anschließende Re-Zertifizierung nur noch nach dem neuen BSI-Standard 200-2 möglich ist, ist eine Umstellung und Migration schon während der Zertifikatslaufzeit unvermeidlich. Für diese Variante ist es also erforderlich, dass ein Tool parallel beide Vorgehensweisen abbilden kann (hybrides Modell).

Eine zweite Möglichkeit ist die Beantragung der Zertifizierung gemäß neuem BSI-Standard 200-2 mit dem IT-Grundschutz-Kompendium. Das ist bereits seit Oktober 2017 möglich. Hierbei scheint die Herausforderung ausschließlich in der Abbildung der neuen Vorgehensweise zu liegen. Da das IT-Grundschutz-Kompendium zum aktuellen Zeitpunkt aber noch nicht alle Bereiche abdeckt, kann es erforderlich sein, die Lücken mit Bausteinen aus den alten Grundschutz-Katalogen zu schließen, bis entsprechende Bausteine im Kompendium vorhanden sind. Ebenso werden Anwender, die bereits länger mit dem IT-Grundschutz arbeiten, ihre bisher erarbeiteten Ergebnisse, soweit möglich, in die neue Vorgehensweise übernehmen wollen. Daher sollten auch hier durch das genutzte Tool beide Wege abgebildet werden.

Zwei Sicherheitswelten – eine Oberfläche

Die HiScout GmbH bildet im Modul „HiScout Grundschutz“ die neue Methodik nach den BSI Standards 200-2 und 200-3 vollständig ab. Ein wichtiger Vorteil für bisherige Anwender des „HiScout Grundschutzes“ ist dabei, dass sich der grundsätzliche Toolaufbau auch für die neuen Standards nicht verändert hat. Das erleichtert Nutzern den Umstieg auf den neuen IT-Grundschutz und die Arbeit damit.

Neben den neuen Standards wird im Modul „HiScout Grundschutz“ aber auch weiterhin das alte Vorgehen nach den BSI-Standards 100-x vollständig abgebildet. Der Anwender hat dadurch nicht nur die Möglichkeit, sich für eine Vorgehensweise zu entscheiden, sondern kann vielmehr beide parallel betreiben und jederzeit zwischen den Sichten der alten und der neuen Welt umschalten. Bei Bedarf kann so auch über einen längeren Zeitraum mit beiden Sicherheitsstandards gleichzeitig gearbeitet werden. Die Anwender können sich dabei vollständig auf die Inhalte konzentrieren und

müssen sich nicht mit der „Technik“ auseinandersetzen. Dieses hybride Modell bietet somit maximale Flexibilität und ermöglicht eine sukzessive Umstellung und Migration ohne Zeitdruck, um sich auf die Inhalte konzentrieren zu können.

Migration nach dem hybriden Modell

Ein weiterer entscheidender Vorteil des hybriden Modells im HiScout Grundschutz-Modul ist die Möglichkeit der teilautomatisierten Übernahme bestehender Umsetzungsdaten. Dadurch kann der Aufwand der Migration an einigen Stellen deutlich reduziert werden.

Die Migrationstabellen des BSI sind vollständig im Tool hinterlegt, werden aus beiden Richtungen (Kataloge und Kompendium) in der Oberfläche dargestellt und können über diese auch einfach angepasst werden. Das ermöglicht eine fachliche Überprüfung (vom BSI empfohlen) und bei Bedarf auch die Anpassung beziehungsweise Erweiterung des Mappings zwischen den alten Maßnahmen und den Anforderungen.

Auf Basis dieses Mappings werden in weiteren Sichten (pro Schicht) für die modellierten Anforderungen die entsprechenden Maßnahmen mit ihren Umsetzungsdaten angezeigt. Mithilfe dieser Informationen kann eine manuelle Übernahme und Zusammenführung der Umsetzungsdaten erfolgen.

Neben dieser manuellen Migration bietet HiScout aber auch einen Workflow für die automatische Übernahme der Umsetzungsdaten. Hierbei werden die Umsetzungsdaten aller Maßnahmen, die der Anforderung über die Migrationstabelle zugeordnet sind, automatisch übernommen. Dabei ist grundsätzlich zwischen folgenden Fällen zu unterscheiden:

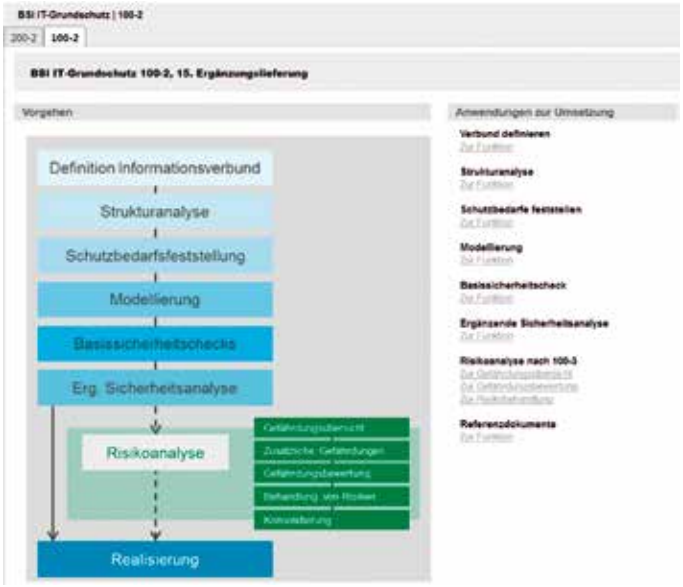

Abbildung 1: HiScout Oberfläche, Vorgehen nach BSI Standard 100-2 / 100-3

_____ Ist nur eine Maßnahme zugeordnet, welche die Anforderung auch vollständig abdeckt, werden die Daten 1:1 (inklusive Umsetzungsstatus) durch den Workflow übernommen.

_____ Ist nur eine Maßnahme zugeordnet, welche die Anforderung nicht vollständig abdeckt, werden die Daten 1:1 übernommen und der Umsetzungsstatus der Anforderung wird maximal auf „teilweise umgesetzt“ gestellt.

_____ Sind einer Anforderung mehrere Maßnahmen zugeordnet, die diese vollständig abdecken, werden die Daten aller Maßnahmen (mit der Information, aus welcher Maßnahme sie kommen) zusammengeführt und der Umsetzungsstatus nach dem Minimalprinzip ermittelt (der schwächste Status wird übernommen).

_____ Sind einer Anforderung mehrere Maßnahmen zugeordnet, die diese nicht vollständig abdecken, werden die Daten aller Maßnahmen (mit der Information, aus welcher Maßnahme sie kommen) zusammengeführt, der Umsetzungsstatus nach dem Minimalprinzip ermittelt und maximal auf „teilweise umgesetzt“ gesetzt.

Über diesen Workflow können vor allem Anwender, die schon sehr weit in der Umsetzung des IT-Grundschutzes sind beziehungsweise bereits zertifiziert sind, viel Zeit bei der Migration sparen. Denn zumindest für die Anforderungen des ersten Falls ist für die Migration keine weitere Bearbeitung notwendig und die Anforderungen der anderen Fälle sind so weit konsolidiert, dass die Migration meist mit einer kurzen Überarbeitung abgeschlossen werden kann.

Annäherung an die ISO-Standards

Sowohl das Datenmodell als auch Oberflächen, Berichte und Automatismen (Workflows) des HiScout Tools lassen sich an die Bedürfnisse der Kunden anpassen. Durch diesen grundlegenden Aufbau müssen sich Kunden auch nicht zwingend an die im Tool vorgegebene Vorgehensweise halten, sondern können ihre eigenen Prozesse und Verfahrensweisen, die sie sich im Laufe der Zeit erarbeitet haben, beibehalten und diese im Tool abbilden.

Mit seinen neuen 200-x-Standards hat sich das BSI auch 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 „Grundschutz“ und „ISO 27001“ angenähert und stärker miteinander verbunden. So greifen jetzt beide Module beispielsweise auf das gleiche Risikomanagement zu. ■