VOM ALPTRAUM ZUR ROUTINEAUFGABE

AD HOC-MANAGEMENTBERICHTE FÜR COMPLIANCE UND INFORMATIONSSICHERHEIT

Der Bedarf an einer aktuellen Berichterstattung zum Status Quo der Managementsysteme kommt oft aus heiterem Himmel – zum Beispiel auf Anfrage der Aufsichtsbehörden oder oberer Managementebenen. Verantwortliche für Compliance und Informationssicherheit sollen nun kurzfristig aussagekräftige Kennzahlen und professionell aufbereitete Dokumente liefern, mit denen die komplexen Zusammenhänge auf einen Blick erfasst werden können.

Wie gut sind Sie auf diese Situation vorbereitet?

Variante 1: Sie müssen alles stehen und liegen lassen und die notwendigen Informationen manuell zusammenstellen. Das Ergebnis stellt Ihre Arbeit nicht vollständig und nicht professionell genug dar. Das Management gerät unter Druck und gibt diesen Druck an Sie weiter.

Variante 2: Ihre GRC-Software bietet Ihnen die Möglichkeit, vorkonfigurierte Key Performance Indicators (KPIs) tagesaktuell abzurufen und in Managementberichten mit übersichtlichen Diagrammen aufzubereiten. Ihre Präsentation trägt zur Aufwertung Ihrer Position bei.

Leider ist es mit der Beschaffung eines leistungsfähigen Softwaretools nicht getan. Die meisten Organisationen erkennen das Bedürfnis für einen KPI erst in dem Moment, in dem er benötigt wird. Handeln Sie also vorausschauend und stellen Sie sich im ersten Schritt die Frage, welche Trends und Fakten Sie über Ihr Compliance- oder IT-Security-Rahmenwerk kennen möchten und worüber diese Ihnen in Ihrer Organisation Auskunft geben sollen. Im Datenschutz könnten es zum Beispiel folgende Punkte sein:

Informationen zum Reifegrad des Datenschutzmanagementsystems

- Wie viele Verarbeitungstätigkeiten umfasst das Verzeichnis der Verarbeitungstätigkeiten (VVT) meiner Organisation und für wie viele davon ist der Eintrag im Verzeichnis komplett angelegt und prüffähig?
- Wie viele Verarbeitungstätigkeiten benötigen eine Datenschutzfolgenabschätzung (DSFA) und wie viele davon sind bereits abgeschlossen?
- Für wie viele meiner Datenarten besitze ich ein tragfähiges Löschkonzept?

Informationen zum täglichen Betrieb

- Wie viele Anfragen zu Betroffenenrechten wurden in einem definierten Zeitraum gestellt?
- Wie viele davon sind aktuell in meiner Organisation in aktiver Bearbeitung und wie viele sind abgeschlossen?
- Wie viele Datenschutzvorfälle mit welcher Schwere kamen in einem definierten Zeitraum vor?

Im zweiten Schritt müssen Sie dafür sorgen, dass die Key Performance Indicators zur Beantwortung dieser Fragen hinreichend effektiv ermittelt werden können. Selbst wenn eine Organisation die entsprechenden Kennzahlen definiert hat und die notwendigen Basisdaten abrufbar bereitstehen, kann es einen erheblichen Aufwand verursachen, die für die aktuelle Situation relevanten Rohdaten aus dem vorgehaltenen Datenpool zu extrahieren und die benötigten KPIs akkurat zu berechnen.

Im besten Fall bietet Ihre GRC-Software hierfür komfortable Funktionen an, wie zum Beispiel das „KPI Management Summary Dashboard" von HiScout. Es ermöglicht dem Nutzer, vorkonfigurierte Kennzahlen in einer Übersicht zusammenzustellen und bei Bedarf tagesaktuell automatisch berechnen zu lassen. Wenn Ihnen dieser Komfort nicht zur Verfügung steht, müssen Sie selbst ein Verfahren für den Datenexport und die Berechnungsmethoden entwickeln.

Fazit: Die Anforderung, kurzfristig belastbare Informationen über den Status Quo von Managementsystemen ausgeben zu können, wird häufig erst im Ernstfall erkannt. Eine GRC-Software kann Sie dabei mit vorkonfigurierten Kennzahlen, Diagrammen und Managementberichten unterstützen.

Daniel Linder | www.hiscout.com