Warum sich eine Analyse lohnt

Gemeinsamkeiten und Unterschiede bei der Risikobetrachtung für Governance, Risk & Compliance

Erst nach gründlichem Vergleich der Risikobetrachtung in den verschiedenen Bereichen der Compliance und Informationssicherheit können die Gemeinsamkeiten genutzt werden, um softwaregestützte Prozesse miteinander zu verbinden und in einem Integrated-Risk-Management (IRM) zusammenzuführen. Die daraus resultierende Zeiteinsparung kommt den Verantwortlichen und anderen Beteiligten zugute.

Von Daniel Linder, HiScout GmbH

©SimpLine – Stock.adobe.com

Die Betrachtung und Behandlung von Risiken in den Fachrichtungen Datenschutz, Business-Continuity-Management (BCM) und Informationssicherheit dreht sich immer um dieselbe Fragestellung: Welche Bedrohung trifft auf welche Schwachstelle und wie geht man mit dem daraus resultierenden Risiko um? Die zugehörigen Regelwerke wie DSGVO, BSI-Standards 200-1 bis 200-4, ISO 27001, ISO 27005 und ISO 22301 beantworten diese Frage jeweils aus ihrem besonderen Blickwinkel und setzen daher unterschiedliche Schwerpunkte. Die verschiedenen Ausprägungen desselben Sachverhalts dennoch fachbereichsübergreifend zu verstehen und zu nutzen – darin liegt die hohe Kunst einer übergreifenden Software für Governance Risk and Compliance (GRC).

Wie wird eine Risikoanalyse erstellt?

Zuerst wird eine Schwellwertanalyse durchgeführt. Diese berechnet auf Grundlage verschiedener Faktoren mit zuvor festgelegten Grenzwerten, ob eine formelle Risikoanalyse notwendig ist. Bei der Erstellung der Risikoanalyse werden die einen Sachverhalt betreffenden und als wahrscheinlich angesehenen Gefährdungen systematisch erfasst und evaluiert. Wenn zu einer Gefährdung eine Schwachstelle identifiziert wird, spricht man von einem Risiko, das nach seiner Eintrittswahrscheinlichkeit und potenziellen Schadenshöhe zu bewerten ist. Im nächsten Schritt werden diesem Risiko geeignete Maßnahmen entgegengesetzt, um es soweit wie möglich zu mindern.

Um die Herausforderungen zu meistern, die eine übergreifende Risikoanalyse mit sich bringt, müssen die besonderen Bedürfnisse der einzelnen Fachbereiche verstanden werden: Im Datenschutz werden lediglich Risiken für die Rechte und Freiheiten natürlicher Personen betrachtet, die aus der Verarbeitung von personenbezogenen Daten erwachsen. Im Notfallmanagement werden nur Risiken für den Ausfall von Ressourcen analysiert, die für kritische Geschäftsprozesse notwendig sind. Um welche Art von Prozessen oder Ressourcen es sich dabei handelt, ist vorerst vollkommen irrelevant. In der Informationssicherheit ist der Blick weit gefasst. Es werden alle Risiken bewertet, die die Vertraulichkeit, Integrität und Verfügbarkeit der untersuchten Daten bedrohen. Im Mittelpunkt der Betrachtung stehen die Ressourcen, die für die Verarbeitung dieser Daten benötigt werden. Eine Einschränkung der Art der möglichen Risiken oder der Art der durch die Risiken bedrohten Daten findet nicht statt.

Ein weiterer Unterschied besteht in der Anzahl und Kategorisierung der Schutzbedarfe. In der Informationssicherheit werden die bereits erwähnten Schutzbe-

darfe Vertraulichkeit, Integrität und Verfügbarkeit mit einer frei wählbaren Anzahl von Ausprägungen bewertet, zum Beispiel „normal“, „hoch“ und „sehr hoch“. Im Datenschutz kommen die Kategorien Datenminimierung, Intervention, Nichtverkettung und Transparenz hinzu und es stehen die Ausprägungen „null“, „hoch“ und „sehr hoch“ zur Auswahl. Beim BCM wird ausschließlich die Verfügbarkeit ins Auge gefasst. Bei der Risikoanalyse der die Prozesse stützenden Ressourcen kann die Anzahl der Schwerestufen, mit denen Eintrittswahrscheinlichkeit und erwartete Schadenshöhe gemessen werden, ebenfalls selbst festgelegt werden.

Welche Anforderungen geben die Regelwerke und Standards vor?

Die verschiedenen Blickwinkel und Schwerpunkte spiegeln sich auch in den unterschiedlichen Anforderungen der verwendeten Rahmenwerke und Normen für die notwendige Betrachtung und Behandlung von Risiken wider: Die DSGVO schreibt in Artikel 35 in Verbindung mit den Erwägungsgründen 75 und 84 vor, dass bei der Verarbeitung personenbezogener Daten eine Risikoabwägung stattzufinden hat. Wie diese auszusehen hat, überlässt sie dem Datenschutz-Verantwortlichen nach DSGVO. Der BSI-Standard 200-2 regelt, dass im IT-Grundschutz die Risikoanalyse nach BSI Standard 200-3 vorzunehmen ist. Die ISO 27001 gibt, wie der Datenschutz, nur vor, dass eine Risikoanalyse erfolgen muss, nicht aber die zu verwendende Methodik. Im BCM nach BSI Standard 200-4 (Community Draft) kann die Organisationsleitung die Art der Risikoanalyse selbst wählen, es wird aber der BSI-Standard 200-3 beispielhaft vorgeschlagen.

Da die Risikoanalyse nach BSI-Standard 200-3 im IT-Grundschutz vorgeschrieben ist und für das BCM vom BSI-Standard 200-4 empfohlen wird, kann man diese Vorgehensweise mit guter Begründung auch bei den anderen Rahmenwerken als mögliche Option betrachten. Hinzu kommt der deutsche Sonderweg beim Datenschutz: Mit dem Standard-Datenschutzmodell (SDM) wird eine grundschutzartige Methode über die Vorgehensweise der DSGVO gelegt und man befindet sich auch hier formell beim BSI-Standard 200-3.

Wie lassen sich alle Bedürfnisse in eine Vorgehensweise integrieren?

Wenn die Risikoanalyse nach BSI Standard 200-3 als Grundlage für alle Fachbereiche verwendet wird, kommt man zu folgenden Ergebnissen und Synergieeffekten: Das BCM prüft gegen das Schutzziel Verfügbarkeit, Grundschutz und ISO 27001 gegen Vertraulichkeit, Integrität und Verfügbarkeit und der Datenschutz gegen alle oben erwähnten sieben Schutzziele. Betrachtet man dieselben Geschäftsprozesse und -tätigkeiten, so kann

BCM	Grundschutz	ISO 27001	Datenschutz
Verfügbarkeit	Verfügbarkeit	Verfügbarkeit	Verfügbarkeit
	Integrität	Integrität	Integrität
	Vertraulichkeit	Vertraulichkeit	Vertraulichkeit
			Datenminimierung
			Intervention
			Nichtverkettung
			Transparenz

Vergleich der in den Regelwerken festgelegten Schutzziele der verschiedenen GRC-Fachbereiche.

man im optimalen Fall eine gemeinsame Risikoanalyse betreiben, zumindest aber – wie beispielsweise bei den verschiedenen Blickwinkeln von Grundschutz und Datenschutz – dem anderen Fachbereich die eigene Bewertung zur Kenntnis bringen. Eine wichtige Voraussetzung dafür ist, dass alle Beteiligten dieselbe Sprache sprechen und dass man sich vor Beginn der Arbeit auf gleiche Termini einigt: Der Schutzbedarf „normal“ aus dem Grundschutz kann hier gegebenenfalls mit dem Schutzbedarf „hoch“ aggregiert und in den Schutzbedarf „hoch“ beim Datenschutz überführt werden, wenn man ein Prinzip der Maximalvererbung verwendet. Andererseits kann eine solche pauschale Vererbung auch in Sackgassen führen, wenn man die unterschiedlichen Blickwinkel vergisst. Es kann sein, dass ein im Grundschutz mit „hoch“ oder „sehr hoch“ bewertetes Schutzgut für den Datenschützer komplett irrelevant ist, da es keine personenbezogenen Daten betrifft und dieses im Datenschutz dann einen Schutzbedarf von „null“ hätte. Ebenso verhält es sich beim Notfallmanagement, das nur auf Verfügbarkeit prüft: Ein hoher Schutzbedarf aus einem anderen Fachbereich, zum Beispiel im Bereich Vertraulichkeit, taucht im Blickfeld des Business-Continuity-Managers gar nicht erst auf.

Fazit

Die Entwicklung einer übergreifenden Risikoanalyse für verschiedene GRC-Bereiche erschließt wertvolle Zeiteinsparungspotenziale, stellt aber höchste Ansprüche an eine GRC-Software. Die themenspezifischen Blickwinkel, Risikobewertungen und mitigierenden Maßnahmen müssen verständlich und transparent sichtbar gemacht werden. Erst auf dieser Grundlage können die in den Managementsystemen für Informationssicherheit, Business-Continuity und Datenschutz vorhandenen Daten und Bewertungen für andere Fachbereiche regelgerecht nutzbar gemacht werden. ■

Daniel Linder ist GRC-Praktiker mit vielseitiger Projekterfahrung. Im Rahmen dieser Projekte beriet er unter anderem Konzerne im Banken- und Energiesektor, Internetlogistiker sowie Organisationen der öffentlichen Hand.