BEZIEHUNGSSTATUS: KOMPLIZIERT?

GRUNDSCHUTZ, DATENSCHUTZ UND NOTFALLMANAGEMENT

Ein Versuch der Annäherung zwischen Datenschutz, Grundschutz und Business Continuity Management (BCM) in Zeiten des Standard-Datenschutzmodells (SDM): „Gibt es Möglichkeiten, sinnvolle Synergien zwischen Datenschutz, Grundschutz und BCM herzustellen und wie kann man diese zum Wohle der jeweiligen Organisation skalieren und nutzen?"

Die drei genannten Managementsysteme besitzen auf den ersten Blick verschiedene Zielsetzungen, haben jedoch eine große Schnittmenge in Bezug auf die Mittel und Methoden zur Umsetzung der jeweiligen Regelwerke. Vor diesem Hintergrund lohnt es sich, einen Blick auf die Differenzen und die gemeinsame Basis zu werfen:

➤ Beim IT-Grundschutz liegt der Fokus auf dem Sicherheitsniveau aller (IT- gestützten) organisationseigenen Informationen. Die Risikobetrachtung erfolgt aus dem Blickwinkel der Organisation.

➤ Im BCM stehen vorrangig die für eine Organisation kritischen Prozesse und Assets und deren maximal tolerierbare Ausfallzeit im Zentrum. Hinzu kommt die Betrachtung von Risiken, welche die Aufrechterhaltung oder den abgestimmten Wiederanlauf des Normalbetriebes der kritischen Geschäftsprozesse betreffen.

SCHMERZFREIER DATENSCHUTZ IST MÖGLICH. DAFÜR HÄTTE ICH MIR IN MEINER ZEIT ALS DATENSCHUTZBEAUFTRAGTER EIN PROFESSIONELLES TOOL GEWÜNSCHT.

Daniel Linder,
Consultant, HiScout GmbH,
www.hiscout.com

➤ Im Datenschutz geht es um den Schutz personenbezogener Daten (pbD), die eine Teilmenge der oben erwähnten „organisationseigenen Informationen" sind. Für den Schutz dieser Daten werden die zugehörigen Risiken ermittelt und geeignete technische und organisatorische Maßnahmen (TOMs) zugeordnet. Der eingenommene Blickwinkel ist hier der des von der Verarbeitung Betroffenen.

Gemeinsam sind diesen drei Regelwerken die Betrachtungen der Risiken, denen Daten, (IT-) Assets und Prozesse unterliegen und die über entsprechende Maßnahmen gemindert werden. Das Management der entsprechenden Risiken soll im Idealfall die Sicherheit der organisationseigenen Systeme, der darauf befindlichen Daten und der von der Verarbeitung dieser Daten Betroffenen gewährleisten. Unterschiede ergeben sich durch die verschiedenen Perspektiven der Risikobetrachtung, die daraus abgeleiteten Interessenkonflikte in der Zielsetzung und die unterschiedliche Granularität der Schutzbedarfe. Hinzu kommt, dass im Falle des Datenschutzes ein noch größeres Augenmerk auf organisationsinterne Prozesse und Gefahren gerichtet werden muss, da die hohe Gewichtung der Betroffenenrechte nicht in Gänze durch andere Managementsysteme abgedeckt wird.

Unterschiedliche Blickwinkel

Der IT-Grundschutz und das BCM weisen hier die größte Deckungsgleichheit auf: Beide richten den Blick von der Führungsebene auf die Organisation als Ganzes. Schutzgut sind Assets und Prozesse sowie die darin vorkommenden Daten jeglicher Art. Schweregrade von Gefährdungen und Risiken sowie maxi-

Durch einen gemeinsamen Datenpool können mit HiScout sinnvolle Synergien zwischen Datenschutz, Grundschutz und BCM hergestellt, skaliert und genutzt werden.

mal tolerierbare Ausfallzeiten werden üblicherweise in drei beziehungsweise vier Kategorien eingeteilt.

Der Datenschutz weicht in seinen Bedürfnissen von den beiden vorgenannten Regelwerken ab: Für die Betrachtung der Risiken wird der Blickwinkel des Betroffenen eingenommen, es wird nur eine Teilmenge der vorhandenen Daten betrachtet und die Einteilung der Schutzbedarfe erfolgt in nur zwei Kategorien: „Hoher Schutzbedarf" (es sind pbD vorhanden) und „Sehr hoher Schutzbedarf" (es sind besondere Kategorien von pbD vorhanden).

Neben der unterschiedlichen Interessenlage der beiden Blickwinkel bei der Risikobetrachtung (Organisation versus Betroffene) liegt die größte Herausforderung für eine einheitliche Bewertung dieser Sichtweisen mit einem übergreifenden Managementsystem in den unterschiedlichen Einteilungen der Risiko- und Schutzbedarfsklassen. Hier mit einem einheitlichen System alle Bedarfe abzudecken ist vergleichbar mit dem Versuch, dreieckige Gegenstände in eine viereckige Aussparung passend einzusenken.

Integriertes Managementsystem

Am Beispiel der HiScout GRC Suite soll nun aufgezeigt werden, wie man trotz der genannten Herausforderungen die drei Bereiche IT-Grundschutz, BCM und Datenschutz in einem integrierten Managementsystem (IMS) sinnvoll und für die Organisation nutzenbringend vollumfänglich abdecken kann. Es wird gezeigt, dass sich der aus der Kombination der drei Bereiche ergebende Nutzen skalieren lässt und somit ein deutlicher Mehrwert durch den Einsatz eines einzelnen, übergreifenden Tools generiert werden kann.

Nutzt man eine einzige, der gesamten Applikation unterliegende Datenbasis, also einen Datenpool, bringt dies zunächst den Vorteil, dass man die gesamten betrachteten Stammdaten der Organisation wie Geschäftsprozesse, Daten, Anwendungen, Systeme etc. nur ein einziges Mal pflegen muss. Des Weiteren wird sichergestellt, dass in allen Systemen mit kongruenten Daten und Bewertungen gearbeitet wird. Beim Thema Risikobewertung kann der Datenschutz durch Zugriff auf die detailliert gepflegten Risikoregister der Module BCM und IT-Grundschutz aus dem Vollen schöpfen. Durch die im BSI Standard 200/2, „CON.2.A1 Umsetzung Standard-Datenschutzmodell" geforderte Umsetzung des Standard-Datenschutzmodells (SDM) bietet sich nun die hervorragende Möglichkeit, die Differenz der verschiedenen Einteilungen der Schutzbedarfe positiv zu nutzen: Die risikobasierten Teile des Datenschutzmanagementsystems folgen der Vierteilung der Risiko- und Schutzbedarfsgrade. Hier ist vor allem die Vorbereitung der Datenschutz-Folgenabschätzung (DSFA) zu nennen und die Schwellwertanalyse zur DSFA, die in HiScout komplett SDM-konform aufgesetzt ist. Die eigentliche Durchführung der DSFA wiederum basiert auf der dem Datenschutz inhärenten Zweiteilung in „hohen" und „sehr hohen" Schutzbedarf. Dabei kann der die DSFA durchführende Datenschützer die feingranulare Einschätzung der im Programm auf Basis der Daten aus BCM und Grundschutz erstellten Risikomatrix nutzen. Er kann diese mit den vom Programm ausgegebenen Bruttorisiken aus der Vorbereitung der DSFA subsummieren und in einer freitextlichen Einschätzung den vorhandenen Schutzbedarfen (hoch / sehr hoch) zuordnen. Eine abschließende Einschätzung der Verarbeitungstätigkeit wird am Ende dieses Prozesses dann aus der Gesamtsicht abgegeben. Die Differenz der verschiedenen Managementsysteme wird hier von einer Herausforderung zu einem Vorteil gewandelt.

Perspektivwechsel

Auch die im Datenschutz relevanten TOMs können direkt aus dem Pool der im BCM und/oder Grundschutz gepflegten Maßnahmen ausgewählt werden und müssen nicht „neu erfunden" werden. Die unterschiedliche Zuordnung der relevanten TOMs zu den im Datenschutz relevanten Verarbeitungstätigkeiten ermöglicht sowohl den Perspektivwechsel hin zum Betroffenen als auch die Betrachtung der Risiken aus Sicht des Verantwortlichen. So können im Datenschutz entweder nur Risiken aus Sicht des Betroffenen betrachtet werden oder alle Risiken aus Sicht des Verantwortlichen. Bei diesem sind die Risiken für die Betroffenen eine Teilmenge (realisierte Risiken des Betroffenen sind Schäden des Verantwortlichen).

Je größer und komplexer die Organisation ist, die die drei Bereiche abdecken möchte, desto lohnender wird ein einheitliches Datenmodell wie zum Beispiel in HiScout: Es reduziert Komplexität, vermeidet Fehler und Redundanzen und ermöglicht den Sprung im Blickwinkel und damit die Einpassung des dreieckigen Gegenstands in die viereckige Aussparung.

Daniel Linder