Vom Grundschutz zum BCM

Zwischen Grundschutz und Notfallmanagement gibt es viele Synergien. Wer diese konsequent nutzt, kann den Aufwand für die Einführung und Pflege eines BCM erheblich reduzieren und die Qualität beider Managementsysteme verbessern. Der demnächst verfügbare BSI-Standard 200-4 bietet eine gute Grundlage dafür.

Von Nicole Mittendorf, HiScout GmbH

Es brauchte eine weltweite Pandemie, um uns wieder bewusst zu machen, dass sich nicht alle persönlichen, gesellschaftlichen und wirtschaftlichen Risiken mit dem Abschluss von Versicherungsverträgen oder der Bildung von Rückstellungen erfolgreich abwehren lassen. Die Uneinigkeit des politischen Handelns hat uns vor Augen geführt, wie wichtig effektive Entscheidungsstrukturen im Notfall sind. Zudem sind die Risiken unserer modernen, arbeitsteiligen und vernetzten Welt komplexer geworden. Die resultierenden Schadensszenarien sind oft schwer vorhersehbar, wirken schneller und erreichen eine weite Verbreitung. Die hohe Technisierung und Spezialisierung von Unternehmen und Organisationen erfordert heute mehr Spezialwissen und mehr übergreifende Koordination als früher, um im Ernstfall erfolgreich agieren zu können. Viele Organisationen haben mit Schrecken festgestellt, dass weder ihre Risiken im Normalbetrieb abgesichert sind noch für Notfälle vorgesorgt und vorgeplant wurde.

Glücklicherweise haben mit den Bedrohungen auch die Schutz- und Vorsorgemöglichkeiten zugenommen. Diese neuen Technologien können aber nur helfen, wenn sie in einem regelmäßigen systematischen Verfahren als geeignet identifiziert, beschafft und in die praktische Nutzung überführt werden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit den BSI-Standards 200-1 bis 200-3 für den IT-Grundschutz ein etabliertes und praxiserprobtes Verfahren für die Einführung eines Informationssicherheitsmanagement-Systems (ISMS) bereit und ist im Begriff im Laufe dieses Jahres mit dem neuen BSI-Standard 200-4 ähnlich praktikable Handlungsempfehlungen für die Einführung eines Business-Continuity- oder Notfall-Managements (BCM) zu verabschieden.

Das BSI legt dabei ein besonderes Augenmerk auf Synergien zwischen BCM und anderen Sicherheitsthemen wie Informationssicherheitsmanagement (ISM) und IT-Service-Continuity-Management (ITSCM) und empfiehlt, eine themenübergreifende Sicherheitsstrategie anzustreben. Welche Gemeinsamkeiten zwischen Grundschutz und Notfallmanagement gibt es und wie können Verantwortliche diese für ihre Organisation nutzen?

Wie profitiert das BCM?

Auch wenn durch den IT-Grundschutz nur die im Normalbetrieb auftretenden Bedrohungen abgefangen werden, erhöhen diese Maßnahmen die Widerstandsfähigkeit und Belastbarkeit der Prozesse und Systeme im Notfall und heben die Schwellen für das Eintreten eines Notfalls beziehungsweise einer Krise an. Bei der Etablierung von Verantwortlichen und Prozessen, der Durchführung von Datenerhebungen und Analysen sowie der Aneignung von Wissen und Verfahren lassen sich weitere Synergien nutzen.

Grundlagen und Verantwortlichkeiten

Die in der Leitlinie des ISMS beschriebenen Ziele, Strategien und anderen Grundlagen des Managementsystems können als Vorlage für das BCM verwendet werden, ebenso die für den Grundschutz hinterlegten gesetzlichen Grundlagen. Je nach Größe der Organisation kann die Rolle des BCM-Beauftragten vom Informationssicherheits-Beauftragten wahrgenommen werden oder ein gemeinsames Gremium der für ISM und BCM verantwortlichen Personen gebildet werden.

Datenerhebung und Strukturanalyse

Das BSI empfiehlt, für ISMS und BCMS den gleichen Geltungsbe-

reich und die gleichen Stammdaten zu verwenden. Die Ergebnisse der Strukturanalyse von Informationsverbund, Geschäftsprozessen und Ressourcen können eine gemeinsame Datengrundlage für Grundschutz und BCM bilden. Das vermeidet doppelte Arbeit, doppelte Datenhaltung und eine doppelte Vorhaltung notwendiger Infrastruktur und macht viele Schnittstellen überflüssig.

Schutzbedarfsfeststellung und Maßnahmenplanung

Auch wenn aus Sicht des Grundschutzes der Schutzbedarf einzelner Prozesse und Ressourcen ein ganz anderer sein kann als der aus Perspektive des BCM, lassen sich Schutzbedarfsklassen, Schadensszenarien und Schadenskategorien laut BSI 200-2 in der Aufbauphase des BCMS als Grundlage nutzen.

Risikoanalyse und Risikobehandlung

Der BSI Standard 200-3 definiert eine Risikoanalyse für Elemente, die nicht durch die Grundschutzbausteine abgedeckt sind. Sowohl die Verfahrensweise als auch die Kataloge mit Gefährdungen, Kriterien und Methoden zur Risikobewertung können für den BSI-Standard 200-4 verwendet werden.

Vorfallbehandlung

Um Störungen des Normalbetriebes zu beheben, werden im Grundschutz Prozesse zur Benachrichtigung von Personen und zur Auslösung von Maßnahmen definiert. Bei der Erstellung von Notfallplänen für das BCM kann auf diesen bestehenden Strukturen aufgebaut werden.

Weitere Aspekte des BCM

Im BCM wird die Perspektive vom Normalbetrieb auf den Notfall erweitert. Dabei kann sich der Schutzbedarf einzelner Geschäftsprozesse und damit die Priorisierung der Maßnahmen erheblich verschieben. Viele Ressourcen und Prozesse, die im Normalbetrieb eine hohe Priorität besitzen, sind im Notfall weniger wichtig, andere nehmen an Bedeutung zu. Neben den vielen Synergien zwischen beiden Themen müssen derartige Widersprüche identifiziert werden, damit es im Notfall nicht zu Verzögerungen oder falschen Entscheidungen kommt.

Business-Impact-Analyse (BIA)

Die Business-Impact-Analyse ist ein grundlegender Prozess für den Aufbau eines BCM, um die zeitkritischen Geschäftsprozesse und Ressourcen zu ermitteln. Diese sind ein wichtiger Bestandteil der Notfallvorsorge und werden durch entsprechende Maßnahmen zusätzlich abgesichert. Dabei kann häufig auf dieselben Ansprechpartner und ähnliche Bewertungsmethoden wie im Grundschutz zurückgegriffen werden.

Besondere Aufbauorganisation (BAO)

In Notfall- und Krisensituationen müssen Entscheidungen schneller als im Normalbetrieb getroffen werden. Dafür muss eine besondere Aufbauorganisation (BAO) mit zeitlich begrenzten Zuständigkeiten, Hierarchien sowie Kommunikations- und Entscheidungswegen etabliert und befähigt werden. Unter anderem wird festgelegt, welche Personen beteiligt sind und welche Aufgaben, Rechte und Pflichten ihnen zugordnet sind.

Notfallbewältigung

In Notfallplänen werden Maßnahmen definiert, die im Ernstfall den Geschäftsbetrieb aufrechterhalten sollen. Um diese zum richtigen Zeitpunkt aktivieren zu können, muss festgelegt werden, wie die Eskalation einer Störung zu einem Notfall (drohende erhebliche Unterbrechung eines zeitkritischen Geschäftsprozesses) oder einer Krise (massive Unterbrechung eines zeitkritischen Geschäftsprozesses bei unzureichender Notfallplanung) erkannt wird und welche Alarmierungsprozesse jeweils in Gang gesetzt werden.

Nutzung von Synergien in übergreifender GRC-Software

In Kenntnis aller Gemeinsamkeiten zwischen Grundschutz und BCM ist es selbstverständlich, diese auch bei der digitalen Verwaltung und Organisation der Managementsysteme nutzen zu wollen. In einer übergreifenden Softwarelösung mit gemeinsamer Datenbasis werden die inhaltlichen und fachlichen Synergien gespiegelt und gestärkt. Die Organisationsstammdaten müssen nur einmal erfasst und gepflegt werden. Schutzbedarfsfeststellungen, Risikoanalysen und Maßnahmenplanungen können für Grundschutz und BCM verwendet werden. Schnittstellen zwischen verschiedenen Softwaretools entfallen. Themenübergreifend agierende Verantwortliche und Bearbeiter müssen nur in einer Software geschult werden.

Fazit

Unternehmen und Organisationen sollten einen Prozess starten, der sie widerstandsfähiger gegen alltägliche und außerordentliche Bedrohungen macht. Die Einführung des BSI IT-Grundschutzes oder eines ISMS nach ISO 27001/2 ist ein hervorragender Ausgangspunkt für den Aufbau eines Business-Continuity-Management-Systems, zum Beispiel nach dem bald verfügbaren neuen BSI-Standard 200-4. Die Nutzung der inhaltlichen und fachlichen Synergien kann durch die Nutzung technologischer Synergien verstärkt werden, insbesondere durch den Einsatz einer themenübergreifenden Software mit gemeinsamer Datenplattform für Grundschutz/ISM und BCM. Als bereichernde vertiefende Lektüre bietet sich der hier mehrfach zitierte Community Draft des BSI Standards 200-4 an.