Corporate Governance

Mehr Sorgfaltspflichten für Unternehmen und Behörden durch das IT-Sicherheitsgesetz 2.0

Das 2015 verabschiedete Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG) stellte Infrastrukturen mit hoher Relevanz für das staatliche Gemeinwesen in seinen Regelungsbereich. Mit der Neuauflage des IT-Sicherheitsgesetzes (2.0) steigt seine qualitative und quantitative Wirkung: mehr betroffene Organisationen, verschärfte Umsetzungspflichten, verstärkte Rolle des BSI als Kontrollorgan und Bußgelder auf DSGVO-Niveau.

Von Piotr W. Nürnberg, Allgeier CORE GmbH

Die Hacker-Attacke auf Krankenhäuser des Deutschen Roten Kreuzes in Rheinland-Pfalz und im Saarland im Juli 2019 zeigte einmal mehr, welche Bedeutung dem Schutz vor Cyberkriminalität und der betrieblichen Kontinuitätsstrategie im Versorgungsbetrieb zukommt. Ein erfolgreicher Angriff kann eine Rückkehr der „durchdigitalisierten" Organisation zu Bleistift und Papier bedeuten und die Geschäftstätigkeit für mehrere Tage behindern. Angesichts der strategischen Relevanz für die Bevölkerung steuert die Bundesregierung in Zusammenarbeit mit Behörden und Fachgremien entgegen und verpflichtet die Betreiber von kritischen Infrastrukturen zur Etablierung und Aufrechterhaltung von Konzepten für Informationssicherheit und Notfallmanagement als Teilmenge ihrer Geschäftsstrategie. Der Nachweis über die Umsetzung wird über einen Auditbericht erbracht. Durchdachte Planung und ein an national und international anerkannten Normen ausgerichtetes Managementsystem für Informationssicherheit und Notfallmanagement können den Aufwand zur Erfüllung der gesetzlichen Anforderungen signifikant senken.

Strukturanalyse

Eine elementare Voraussetzung für die Planung und Umsetzung eines Managementsystems für Informationssicherheit (ISMS; BSI-Standards 200-x, ISO 27001) und Notfallmanagement (BCMS; BSI-Standard 100-4, ISO 22301) ist eine genaue Kenntnis der Organisation und ihrer Werte (Assets). Deshalb legen sowohl die Methodik vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch die ISO-Normen der Etablierung und Aufrechterhaltung eines ISMS und BCMS eine Strukturanalyse (Inventarisierung) zugrunde. Das integrierte Managementsystem DocSetMinder liefert im Grundmodul „Organisation" alle notwendigen Strukturen und Vorlagen für eine normkonforme Dokumentation der Aufbau- und Ablauforganisation.

Das Modul unterstützt Unternehmen und Behörden bei der Erfassung und Pflege ihrer organisatorischen Einheiten (Bereiche, Abteilungen etc.), Geschäftsprozesse und Verantwortlichkeiten (Rollen). Für die Dokumentation der IT-Prozesse steht die ITIL-Struktur zur Verfügung. Leit- und Richtlinien der Organisation können als richtungsweisender Bestandteil von Informationssicherheit und Notfallmanagement effizient vorbereitet, genehmigt und den Stakeholdern kommuniziert werden. Die dokumentierte Aufbau- und Ablauforganisation spiegelt zusammen mit der IT-Dokumentation die logischen Zusammenhänge zwischen Prozessen, Anwendungen, Serversystemen und Speicherorten für die entstehenden Informationen (Daten) wider. Die in der übergreifenden Strukturanalyse erfassten Sachverhalte können sofort in den Managementmodulen (ISO 27001, BSI IT-Grundschutz, ISO 22301, Notfallmanagement nach BSI 100-4) referenziert werden, wodurch die Erstellung und Pflege erleichtert, die Fehleranfälligkeit gesenkt und Redundanzen vermieden werden.

Business-Impact- und Risikoanalyse

Nicht alle organisatorischen Einheiten und Prozesse sind gleichermaßen wichtig für die Leistungserstellung in Behörden und Unternehmen. Mit einer Business-Impact-Analyse können Prozesse und Ressourcen hinsichtlich des

bei ihrem Ausfall drohenden Schadens bewertet und miteinander verglichen werden. Auf dieser Basis ermittelte, geschäftskritische Abläufe müssen in Notfallvorsorge- und -bewältigung (Alarmierung und Sofortmaßnahmen, Geschäftsfortführung und Wiederanlauf) entsprechend berücksichtigt werden.

Eine Risikoanalyse liefert zusätzlich Auskunft über die möglichen Ursachen für den Ausfall und wie sie in Abhängigkeit von der Ausprägung des Risikos unterschiedlich behandelt werden (Reduktion, Vermeidung, Verlagerung, Akzeptanz). Auch hier können die Vorteile einer ganzheitlichen Betrachtung in einem integrierten Managementsystem wie DocSetMinder effektiv und effizient genutzt werden: Vereinheitlichung von Risikomanagementprozess, Dimensionierung der Risikomatrix, Risikoparameter und Risikoappetit. Damit lassen sich Risiken aus Informationssicherheit und Notfallmanagement (ggf. auch Datenschutz, internem Kontrollsystem, Qualitätsmanagement etc.) miteinander vergleichen und in einem Management-Review übersichtlich zusammenfassen.

Für die Durchführung der Risikoidentifikation, -analyse, -bewertung und -behandlung stehen in DocSetMinder eine Risikoanalyse gemäß ISO 31000 und daraus abgeleitete Risikoanalysemethoden gemäß ISO 27005 und BSI-Standard 200-3. Die Risikoidentifikation kann unter Einbeziehung diverser Kataloge für Gefährdungen und Schwachstellen (BSI-Kompendium, ISO 27005 etc.) erfolgen. Ähnliches gilt für die Definition von präventiven, reaktiven und korrektiven Maßnahmen (BSI-Kompendium und Annex A der ISO 27001, 27019).

Fazit

Die Neuauflage des IT-Sicherheitsgesetzes lässt die Absicht des Gesetzgebers erkennen, den Schutz vor Cyberbedrohungen und die betriebliche Kontinuitätsstrategie in kritischen Infrastrukturen ganzheitlich zu betrachten. Die Implementierung technischer Lösungen zur Erkennung und Abwehr von Cyberangriffen, die Vertrauenswürdigkeitserklärung der gesamten Zulieferkette für versorgungsrelevante Komponenten, die Bestellung eines Krisenmanagers, die Befugnis des BSI, Pen-Tests bei Betreibern kritischer Infrastrukturen durchzuführen, und die Anpassung der Bußgelder an das DSGVO-Level sind einige Beispiele dafür, wie KRITIS-Organisationen zu mehr Cybersicherheit verpflichtet werden sollen.

Der Erfolg der Etablierung und Aufrechterhaltung hängt dabei entscheidend von der verwendeten Methode und Integration von Informationssicherheit und betrieblichem Kontinuitätsmanagement in die Geschäftsstrategie ab. Der Nachweis wird über eine entsprechende Dokumentation erbracht. Ein integriertes Managementsystem wie DocSetMinder ermöglicht eine ganzheitliche Betrachtung der Organisation in allen Etappen (Plan-Do-Check-Act) der Arbeit zur Erfüllung der gesetzlichen und normativen Anforderungen. DocSetMinder bildet die anerkannten Standards, Richtlinien und Gesetze vollständig und auf Basis einer übergreifenden Strukturanalyse ab.

Ganzheitliche Unterstützung für KRITIS-Organisationen

Interessierten Unternehmen und Behörden bietet Allgeier CORE, neben DocSetMinder, ein ganzheitliches Leistungs- und Produktportfolio zur Abbildung der Anforderungen aus dem IT-Sicherheitsgesetz 2.0. Neben technischen Lösungen zur Optimierung des IT-Sicherheitsniveaus liefert die Allgeier passgenaue Unterstützung auf konzeptioneller und operativer Ebene: von Schwachstellen-Scan, Penetrationstest und Red-Teaming über Information Security Awareness bis hin zur Erstellung der Konzepte für Informationssicherheit, Notfallmanagement, Katastrophenschutzplan, Datenschutz und IT-Forensik. ■

Messestand: Halle 10.0, Stand 10.0-407