



Kombimodell für die Informationssicherheit, Teil 1

Projekt zur ISO 27001-Zertifizierung erhält durch Grundschutz-Werkzeuge konkrete Gestalt

Wolf Dittmayer, externer Datenschutzbeauftragter der Gauselmann Unternehmensgruppe und IT-Sicherheitsbeauftragter der BEIT GmbH, datenschutz@dittmayer.org

Wer sich um IT-Sicherheit kümmert, benötigt dazu praxistaugliche Instrumente und muss sein Vorgehen permanent gut planen. Darüber hinaus ist es sinnvoll, eine Zertifizierung durch eine akkreditierte Zertifizierungsstelle wie zum Beispiel den TÜV NORD CERT anzustreben. Mit solch einem Label kann ein Unternehmen nach außen dokumentieren, dass es sich systematisch um IT-Sicherheit kümmert und zudem ein definiertes Sicherheitsniveau einhält. Der erste Teil des Beitrags von IT-Grundschutz-Leser Wolf Dittmayer zeigt, wie hilfreich die Grundschutzwerkzeuge des BSI bei einer ISO-27001 Zertifizierung sein können.

Die BEIT Systemhaus GmbH ist ein Unternehmen der international agierenden Gauselmann Gruppe. Das Unternehmen erbringt ein breites Spektrum von Application-Management-Leistungen für Kunden innerhalb und außerhalb des Konzerns. Anfang 2008 wollte das Systemhaus seine Informationssicherheit und insbesondere die Sicherheit seines Rechenzentrums auf der Basis der internationalen Norm ISO 27001 unabhängig prüfen und zertifizieren lassen. Das Unternehmen stellte an sich selbst den Anspruch, den strategischen Stellenwert nachhaltiger Informationssicherheit durch die dauerhafte Einrichtung eines ISMS (Information Security Management Systems) zu unterstreichen.

„Zu Beginn unserer Überlegungen für eine Zertifizierung waren der Umzug in ein neues Rechenzentrum sowie bereits ein Zertifizierungsprozess nach ISO 9001 abgeschlossen. Wir wussten, dass wir damit bereits in Bezug auf unsere Informationssicherheit technisch und organisatorisch gut aufgestellt waren“, sagt



Organisationsberater Wolf Dittmayer

Dr. Steinau, Geschäftsführer der BEIT. „Dennoch wollten wir unsere Informationssicherheit auf Herz und Nieren prüfen. Zusätzlich sollte ein Managementsystem aufgebaut werden, mit dem das erreichte Sicherheitsniveau abgesichert und stetig verbessert werden konnte.“

BEIT ließ sich von vornherein von der Erkenntnis leiten, dass Informationssicherheit als fortlaufender Prozess begriffen und gesteuert werden muss. Das jeweils erreichte Sicherheitsniveau sollte ständig

aktiv geprüft werden, und das ISMS sollte in der Lage sein, neue Risiken, Anforderungen und geeignete Maßnahmen zu identifizieren. Um die kontinuierlichen Verbesserungsprozesse zu stützen, begann BEIT damit, ein Monitoringsystem zu implementieren. Als Modell fungierte dabei das simple Prinzip eines Regelkreislaufs: PDCA – Plan, Do, Check, Act.

Wahl der Instrumente

Die ISO 27001, entstanden aus dem BS-7799, legt den Fokus auf Managementmodelle und die Etablierung von Prozessen sowie auf Steuerungs- und Controlling-Instrumente. Die Anforderungen der ISO 27001 sind überwiegend allgemein gehalten. Damit beschreibt die Norm zwar, was man tun soll, sagt aber vergleichsweise wenig darüber, wie die Vorgehensweise aussieht. Selbst die 133 „Controls“ des zur Norm gehörigen Anhangs „Annex A“, die weitgehend auch technische Themenfelder abdecken, sind generischer Art und bedürfen der Konkretisierung im Einzelnen.

Die Norm fordert durch Beschreibungen und allgemeine Zielvorgaben

- den Aufbau einer organisatorischen Struktur eines ISMS,
- die Festlegung eines Geltungsbereichs und
- die Ermittlung der darin enthaltenen Informationswerte,
- die Identifizierung der Bedrohungen und Einschätzung der Risiken mit anerkannten Analyse-Instrumenten sowie
- die Auswahl und Umsetzung geeigneter Maßnahmen, um den Risiken zu begegnen.

Anders sieht es beim BSI-Grundschutzmodell aus. Dort wird neben der generellen Strategie auch äußerst ausführlich über die Art und Weise der Umsetzung gesprochen. Das Sicherheitsmanagement-Team von BEIT erkannte sehr früh den Wert des BSI-Grundschutz-Modells für sein Vorhaben. So war bald klar, dass man dessen reichhaltigen Fundus an Werkzeugen, Konzepten, Richtlinien- und Musterlösungen nutzen wollte, um sich wie an einem roten Faden bei der internen Vorgehensweise für die ISO-Zertifizierung orientieren zu können.

Ein Vergleich des Dokumentenumfanges der ISO 27001 – etwa 40 Seiten – und des aktuellen Grundschutzkatalogs – etwa 3700 Seiten ohne die zugehörigen „BSI-Standards“ – veranschaulicht unmittelbar den Unterschied an Generik bzw. Konkretheit der beiden Ansätze, aber auch das Potenzial der beiden Instrumente, einander zu ergänzen. Das Grundschutzhandbuch geht deutlich konkreter an die Aufgabenstellung heran. Vor allen in den wichtigen Anforderungsbereichen „Risikoanalyse“ und „Risikobehandlung“ kann es von hohem Wert sein.

Risikoanalyse

Die ISO 27001 fordert neben der Auswahl eines methodischen Ansatzes zur Risikoanalyse die Definition von Risikostufen sowie die Ermittlung

von Informationswerten, Bedrohungen und Schwachstellen, um eine Risikobewertung durchführen zu können. Dafür ist die zweistufige Risikoanalyse der Grundschutzsystematik ein ebenso pragmatischer wie zuverlässiger Ansatz. Anhand von ausgewählten Schutzbedarfskategorien wird normaler Schutzbedarf von höheren Schutzbedarfsanforderungen getrennt und der jeweilige Level kenntlich gemacht.

BEIT definierte für das Unternehmen zutreffende Kategorien, um in Workshops zunächst den Schutzbedarf auf der Ebene der Anwendungen und der damit verarbeiteten Informationen festzustellen. Hierauf aufbauend leiteten die Spezialisten dann den Schutzbedarf für die betroffenen Systeme und Räumlichkeiten nach dem Maximumprinzip ab. Dabei „erbt“ ein System den Schutzbedarf der Anwendung und ihrer Daten, für die der höchste Schutzbedarf an Verfügbarkeit, Integrität oder Vertraulichkeit festgestellt wurde. Hieraus ließ sich eine vollständige Landschaft aller Schutzobjekte (Anwendungen, Daten, Systeme und Infrastruktur) ableiten. Über den jeweiligen Schutzbedarf und die dazu passende weitere Vorgehensweise verschaffte sich das Sicherheitsmanagement-Team anschließend detaillierte Kenntnisse. Nach der Grundschutz-Systematik wurde in der ersten Risikostufe für den gesamten Geltungsbereich und alle betroffenen Schutzobjekte zunächst ein normaler Schutzbedarf mit einem komplexen Szenario an Standard-Risiken angenommen. In der zweiten Stufe der Risikoanalyse wurden für die Objekte, für die ein normaler Schutzbedarf nicht ausreicht, die verbleibenden Risiken oberhalb der bereits abgedeckten Standard-Risiken betrachtet. Diese höheren Risiken mussten nach Art und Größe bewertet und unterschiedlich behandelt werden. Das in der ISO 27001 geforderte Risk Assessment konnte auf der Basis dieser Vorgehensweise vollständig abgebildet werden.

Risikobehandlung

Die ISO 27001 fordert nach der Risikoanalyse die Behandlung der festgestellten Risiken, also vornehmlich die Auswahl und Umsetzung wirksamer Maßnahmen und im Einzelfall auch den Transfer von Risiken oder, auch dies ist möglich, deren Akzeptanz.

Auch hierbei erwies sich die Vorgehensweise des Grundschutzmodells in mehrfacher Hinsicht als geeignetes und mächtiges Instrument, um das in der ISO 27001 geforderte „Risk Treatment“ vollständig umzusetzen. Ausgehend von seinem theoretischen Ansatz, nämlich der Annahme, dass ein gewisses Bündel an Standard-Risiken stets vorhanden ist, bietet das Grundschutzmodell einen umfangreichen Maßnahmenkatalog an, mit dem diesen Standardrisiken begegnet werden kann. Die Auswahl der Maßnahmen, die überhaupt für den Geltungsbereich in Frage kommen, erfolgt durch einen Modellierungsprozess, bei dem anhand von Bausteinen die IT-Struktur schematisch nachgebildet wird. Alle Maßnahmen eines modellierten Bausteins sind dabei anschließend obligatorisch anzuwenden.

Die Modellierung der BEIT-IT-Landschaft ergab eine Auswahl von 44 Bausteinen mit einer Gesamtzahl von etwa 1000 empfohlenen Einzelmaßnahmen. Mit einer Mapping-Tabelle, die diese Maßnahmen und Bausteine mit den entsprechenden Forderungen der ISO-27001-Controls des Annex A in Beziehung setzte, konnten die Anforderungen der ISO-Norm sehr differenziert abgebildet werden. ■