Pressemitteilung

SÜD IT AG
Dr. Stefan Krempl
ISO 27001 Auditor, Datenschutzbeauftragter
Stahlgruberring 11
81829 München
Tel.: 089 461 3505 12
E-Mail: krempl@sued-it.de

INTERFACE FACTORS GmbH
Dr. Ralph Klöwer
Landshuter Allee 12
80637 München
Tel.: 089-552688-18
E-Mail: SuedIT@interface-factors.de

Dr. Stefan Krempl, Süd-IT AG

IT-Sicherheit für den Mittelstand: Besser nach ISO/IEC 27001 oder IT-Grundschutz zertifizieren?

Unternehmen können Aufbau und Zertifizierung ihres Informations-Sicherheits-Management-Systems heute nach ISO/IEC 27001 oder IT-Grundschutz vornehmen. Beide Verfahren leisten im Ergebnis dasselbe – aber betriebswirtschaftlich unterscheiden sie sich erheblich. Gerade für den Mittelstand lohnt sich daher ein Vergleich.

München, 29.07.2015 – Gesetzgeber, Kunden und Auftraggeber verlangen auch vom Mittelstand zunehmend die Implementierung und Zertifizierung ihres Informations-Sicherheits-Management-Systems (ISMS). In Deutschland haben Unternehmen dazu die Wahl zwischen einer originären Zertifizierung nach ISO/IEC 27001 und einer Zertifizierung auf der Basis von IT-Grundschutz. Beide Standards sind, nach Aussage des BSI, gleichwertig, aber die Vorgehensweisen unterscheiden sich deutlich. Hat der IT-Grundschutz seine Vorteile für Behörden, so ist für den Mittelstand häufig ISO/IEC 27001 die bessere Wahl, um die Anforderungen kosteneffizient zu erfüllen. Den Ausschlag gibt hier der Zugewinn an Flexibilität in der ISMS-Anpassung an die individuellen Sicherheitsanforderungen, Prozesse und Ressourcen. Im Vergleich mit IT-Grundschutz profitiert der Mittelstand bei einer ISO/IEC 27001-Zertifizierung zudem von einer Halbierung des Zeit- und Kostenaufwands für Vorbereitung und Durchführung.

ISO/IEC 27001 – internationale Norm mit Flexibilität in der Umsetzung

ISO/IEC 27001 ist ein weltweit anerkannter Standard. Dabei ist die Norm mit rund 32 Seiten relativ knapp gehalten. Während der Hauptteil grundsätzliche Anforderungen an die Organisation, Prozesse und Dokumente formuliert, umfasst der Anhang A insgesamt 114 Controls bzw. Maßnahmenziele für Infrastruktur, Technik, Prozesse und Dokumente. Die Anforderungen aus Hauptteil und Anhang A sind im Wesentlichen allgemein gefasst: Auf diese Weise gewinnen Unternehmen bei der Zertifizierung Spielräume für eine flexible Umsetzung sowie für eine individuelle Ausgestaltung ihres ISMS. Während die ISO/IEC 27001:2013 die Zertifizierungsanforderungen definiert, werden in den zugehörenden Normen 27002 ff. praktische Hilfen zur Implementierung gegeben, ohne dass diese für eine Zertifizierung verpflichtend wären.

IT-Grundschutz – detaillierte Vorgaben, strikt geführte Umsetzung

Der IT-Grundschutz wurde vom Bundesamt für Informationssicherheit (BSI) entwickelt und in den BSI Standards 100-1 bis 100-4 sowie den umfangreichen Grundschutzkatalogen auf ca. 4000 Seiten festgeschrieben. Die Umsetzung erfolgt wesentlich anhand von über 1000 definierten Maßnahmen. Die Standards beschreiben relativ genau die Vorgehensweise und geben mit ergänzenden Dokumenten des BSI viele Hinweise, wie das System aufzusetzen ist und welche Dokumente zu erstellen sind. International ist der Standard allerdings nahezu unbekannt.

Unterschiede in der Methodik

Ein zentraler Unterschied ist die Art und Weise des Risikomanagements. Die ISO/IEC 27001 Methodik beginnt mit einer Beschreibung, wie das Risikomanagement durchgeführt werden soll. Im nächsten Schritt folgt eine Analyse der Risiken. Aus der Bewertung der gefundenen Risiken werden anschließend die erforderlichen Sicherheitsmaßnahmen abgeleitet. Die Vorgehensweise nach BSI Grundschutz weicht davon deutlich ab: Hier wird das IT-System z.B. mittels des GSTOOLs modelliert. Dann ermittelt das Tool anhand der Grundschutzkataloge die Gefährdungen sowie die Maßnahmen, die erforderlich sind, um eine Zertifizierung zu bestehen.

Schreibt der IT-Grundschutz das Sicherheitsniveau vor, liegt es im anderen Fall in der Hand des Nutzers, seine Sicherheitsziele festzulegen. ISO/IEC 27001 verlangt daher mehr Initiative zur Entwicklung individueller Strategien, dafür kann das Vorgehen sehr flexibel an das eigene Unternehmen angepasst werden. Die IT-Grundschutz-Methodik ist dagegen formalistischer; der Nutzer wird relativ stark durch die Norm geführt und hat weniger Freiheiten der Anpassung. Gleichzeitig Stärke und Schwäche der Grundschutzmethodik sind die umfangreichen Grundschutzkataloge. Sie bündeln umfangreiches Expertenwissen, sind aber in der Erstellung so aufwändig, dass sie neuen Entwicklungen, z.B. bei aktuellen Betriebssystemen, teilweise um Jahre hinterherhinken.

Unternehmen geben ISO/IEC 27001 den Vorzug

Auch im Aufwand unterscheiden sich beide Vorgehensweisen deutlich: Für eine IT-Grundschutz-Zertifizierung incl. Vorbereitung ist regelmäßig der **doppelte** Aufwand gegenüber einer reinen ISO/IEC 27001-Zertifizierung zu veranschlagen. Daher entscheidet sich die Mehrzahl der Wirtschaftsunternehmen für eine ISO/IEC 27001-Zertifizierung, während bei Behörden in der Regel der IT-Grundschutz vorgegeben ist.

ISO/IEC 27001	IT-Grundschutz
Vollständige Risikoanalyse erforderlich	Risikoanalyse entfällt im Normalfall
32 Seiten verpflichtend, ca. 250 Seiten optional 114 Controls	> 4000 Seiten incl. Grundschutzkataloge, > 1000 Maßnahmen
Allgemeine Vorgaben	Konkrete Vorgaben und Maßnahmen
Flexibel anpassbar	Umfangreich, gründlich aber relativ starr
Geringerer Aufwand, vor allem für kleine und mittlere Unternehmen	Deutlich höherer Aufwand für Vorbereitung und Zertifizierung.
Internationale Anerkennung	Nur nationale Relevanz

Fazit

Der sehr formalistische IT-Grundschutz des BSI hat seine klaren Stärken, wenn es um die Sicherheit bei Behörden geht. Dafür wurde er entworfen. Gerade kleine und mittlere Unternehmen profitieren dagegen von den Vorteilen einer reinen ISO/IEC 27001 Zertifizierung, weil das Vorgehen an die Bedürfnisse und Gegebenheiten des Unternehmens besser angepasst werden kann. Zudem ist der nationale IT-Grundschutz häufig zu eng gefasst für Mittelständler, die europaweit tätig sind oder als Zulieferer für internationale Konzerne tätig sind. Dennoch können einzelne Elemente des IT-Grundschutzes die ISO/IEC 27001-Methodik durchaus aufwerten.

Dazu Dr. Stefan Krempl: „Bei der SÜD IT nutzen wir häufig die Vorteile beider Welten. Für den Aufbau des ISMS und die Zertifizierung raten wir grundsätzlich zu einer reinen ISO/IEC 27001 Vorgehensweise. Gleichzeitig verwenden wir bei der Vorbereitung auf die Zertifizierung die Grundschutzkataloge und auch das GSTOOL, z.B. um eine Liste der Risiken zu erstellen. Der Einsatz des umfangreichen Beispiel- und Maßnahmenbestands aus dem IT-Grundschutz beschleunigt den Aufbau eines validen ISMS im Einklang mit den Qualität- und Kostenzielen unserer Kunden."

Über Süd-IT AG

Die Münchner Süd-IT unterstützt vor allem mittelständische Unternehmen im Bereich Zertifizierung, Compliance und Informations-Sicherheitsmanagement. Die Kernleistungen rund um Auditing, Beratung und Vorbereitung von ISO/IEC 27001-Zertifizierungen können von Anwendern jederzeit erweitert werden. Für Aufbau sowie Optimierung von ISMS, IT-Sicherheitssystemen und IT-Infrastrukturen stehen gegenwärtig über 250 hochkarätige Spezialisten bereit. Sie liefern Unternehmen u.a. aus den Marktsegmenten Automotive, Medizin, Energie und Dienstleistungen komplette Lösungen aus einer Hand. Dabei verfolgt die Süd-IT das Konzept „Ihre Experten vor Ort" und ist daher mit mehreren Standorten im süddeutschen Raum sowie in Berlin und Rom kundennah aufgestellt.