Internationalisierung der IT-Grundschutz-Zertifizierung

Isabel Münch
Referat IT-Sicherheitsmanagement und IT-Grundschutz
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
muench@bsi.de

Abstract: Mit dem IT-Grundschutz-Zertifikat können Geschäftsprozesse und IT-Verbünde auf Basis der IT-Grundschutz-Vorgehensweise des BSI zertifiziert werden. Hiermit wird nicht nur das Informationssicherheitsmanagementsystem (ISMS) einer Organisation, sondern auch die Ausgestaltung der Sicherheitsmaßnahmen für die relevanten Geschäftsprozesse untersucht und bewertet. Ein internationaler Standard für ISMS-Zertifizierung wurde im Oktober 2006 mit der Veröffentlichung der Norm ISO 27001 definiert. Sowohl die IT-Grundschutz-Vorgehensweise, als auch das Zertifizierungsschema und die IT-Grundschutz-Kataloge wurden an ISO 27001 angepasst, so dass Kompatibilität gewährleistet ist.

1 Umstrukturierung des IT-Grundschutzhandbuchs

Die Vorgehensweise nach IT-Grundschutz stellt eine einfache Methode dar, wie die dem Stand der Technik entsprechenden IT-Sicherheitsmaßnahmen identifiziert und umgesetzt werden können. Diese Vorgehensweise ist geeignet, um in typischen IT-Umgebungen in Behörden und Unternehmen ein IT-Sicherheitsmanagementsystem zu etablieren. Außerdem stellt das BSI mit der Kombination aus der IT-Grundschutz-Vorgehensweise und den IT-Grundschutz-Katalogen sowohl eine Sammlung von IT-Sicherheitsmaßnahmen als auch eine entsprechende Methodik zur Maßnahmen-Auswahl zur Verfügung. Um möglichst nah am Stand der Technik zu bleiben, werden die IT-Grundschutz-Kataloge des BSI ständig fortgeschrieben und auf dem aktuellsten Stand gehalten.

Das IT-Grundschutzhandbuch ist mit der Ausgabe 2005 in verschiedenen Bereichen umstrukturiert worden. Am auffälligsten ist hierbei, dass die Beschreibung der Grundschutz-Vorgehensweise und die IT-Grundschutz-Kataloge getrennt wurden. Außerdem wurden noch eine Vielzahl kleinerer und größerer Änderungen aufgrund der Diskussionen mit Anwendern im In- und Ausland vorgenommen.

2 Internationale Entwicklung

In der internationalen Standardisierungsorganisation ISO gab es eine Vielzahl von Diskussion um die Weiterentwicklung der Standards rund um das IT-Sicherheitsmanagement. Hierzu gehören nicht nur die Überarbeitung der Standards ISO 13335 und ISO 17799, sondern auch die Frage der Zertifizierung von Informationssicherheitsmanagement-Systemen (siehe [ISO13335], [ISO17799], [ISO27001]).

Die Überarbeitung des Standards ISO 17799 ist mittlerweile als ISO/IEC 17799:2005 verabschiedet worden. Außerdem sollen 2006 alle Standards zu Sicherheitsmanagement in einer 27000 Serie zusammengefasst werden, in Analogie zu anderen Managementsystemen wie zum Beispiel ISO 9000. Insbesondere wurde der britische Standard BS 7799:2 als Grundlage für einen ISO-Standard zur Zertifizierung genommen, der als ISO/IEC 27001:2005 verabschiedet wurde.

Das BSI hat 2002 die Zertifizierung von Geschäftsprozessen und IT-Verbünden auf Basis von IT-Grundschutz etabliert. Allen IT-Grundschutz-Anwendern soll es möglich sein, sich auch weiterhin die sorgfältige Umsetzung von IT-Grundschutz mit einem IT-Grundschutz-Zertifikat bestätigen zu lassen. Damit das IT-Grundschutz-Zertifikat aber auch die internationale Norm ISO 27001 mit abdeckt, wurden sowohl die IT-Grundschutz-Vorgehensweise, das Zertifizierungsschema und die IT-Grundschutz-Kataloge angepasst (siehe [BSI2], [GSHB] und [ZERT]).

Eine IT-Grundschutz-Zertifizierung (oder jetzt: ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz) umfasst sowohl eine Prüfung des IT-Sicherheitsmanagements als auch der konkreten IT-Sicherheitsmaßnahmen auf Basis von IT-Grundschutz. Sie beinhaltet gleichzeitig eine ISO-Zertifizierung nach ISO 27001, ist aber aufgrund der zusätzlich geprüften technischen Aspekte wesentlich aussagekräftiger als eine reine ISO-Zertifizierung. Die für die Zertifizierung notwendigen Prüfberichte müssen von einem lizenzierten Auditor erstellt werden. Die Lizenzierung von IT-Grundschutz-Auditoren wurde so angepasst, dass die vom BSI lizenzierten Auditoren alle Anforderungen erfüllen, die ISO an Auditoren für ein Informationssicherheitsmanagement-System stellt. Die Zertifizierungs- und Lizenzierungsschemata für die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz sind unter [ZERT] zu finden.

Im folgenden wird ein kurzer Überblick über die derzeit wichtigsten Standards zum IT-Sicherheitsmanagement gegeben.

2.1 ISO 13335

Der Standard ISO 13335 "Management of information and communications technology security" (früher "Guidelines on the Management of IT Security") versteht sich als allgemeine Leitlinie für die Initiierung und Umsetzung des IT-Sicherheitsmanagementprozesses (siehe [ISO13335]). Er gibt Anleitungen, jedoch keine Lösungen zum Management von IT-Sicherheit. Der Standard stellt ein Basiswerk auf diesem Gebiet dar und ist Ausgangs- oder Referenzpunktpunkt für eine Reihe von Dokumenten zum IT-Sicherheitsmanagement. Der Standard besteht derzeit aus folgenden Teilen:

- Part 1: Concepts and models for information and communications technology security management
- Part 2: Techniques for information security risk management
- Part 5: Management guidance on network security

Die früheren Teile 3 und 4 sind in den jetzigen Teilen 1 und 2 aufgegangen. Der Standard IS 13335-2 enthält verschiedene Methoden zur Risikoanalyse. Eine Zertifizierung ist nicht vorgesehen.

2.2 ISO 17799

Das Ziel von ISO 17799 "Information technology – Code of practice for information security management" ist es, ein Rahmenwerk für das IT-Sicherheitsmanagement zu definieren (siehe [ISO17799]). ISO 17799 befasst sich daher hauptsächlich mit den erforderlichen Schritten, um ein funktionierendes IT-Sicherheitsmanagement aufzubauen und in der Organisation zu verankern. Die erforderlichen IT-Sicherheitsmaßnahmen werden kurz auf den ca. 100 Seiten des ISO-Standard ISO/IEC 17799 angerissen. Die neue Version ISO 17799 beinhaltet 134 Sicherheitsmaßnahmen, gruppiert in 11 Gebiete. Diese Maßnahmenempfehlungen sind auf Management-Ebene und enthalten kaum konkrete technische Hinweise. Ihre Umsetzung ist eine von vielen Möglichkeiten, die Anforderungen des ISO-Standards 27001 zu erfüllen.

2.3 ISO 27001

Aufgrund der Komplexität von Informationstechnik und der Nachfrage nach Zertifizierung sind in den letzten Jahren zahlreiche Anleitungen, Standards und nationale Normen zur IT-Sicherheit entstanden. Der ISO-Standard 27001 "Information technology - Security techniques - Information security management systems requirements specification" ist der erste internationale Standard zum IT-Sicherheitsmanagement, der auch eine Zertifizierung ermöglicht (siehe [ISO27001]). ISO 27001 gibt auf ca. 10 Seiten allgemeine Empfehlungen. In einem normativen Anhang wird auf die Controls aus ISO/IEC 17799 verwiesen. Der Leser erhält aber keine Hilfe für die praktische Umsetzung.

3 BSI-Standards

Das BSI hat damit begonnen, eine Schriftenreihe mit Standards zu verschiedenen Bereichen der Informationssicherheit aufzubauen (siehe [BSI1], [BSI2], [BSI3]). Hierzu gehören auch die folgenden BSI-Standards zum Thema IT-Sicherheitsmanagement:

- Managementsysteme für Informationssicherheit
- Vorgehensweise nach IT-Grundschutz
- Risikoanalyse auf der Basis von IT-Grundschutz

Darüber hinaus ist das Prüfungsschema für IT-Grundschutz-Zertifizierungen sowie das Lizenzierungsschema für Auditoren im Dokument "ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz" beschrieben.

Außerdem wurde der Baustein 1.0 IT-Sicherheitsmanagement der IT-Grundschutz-Kataloge angepasst, um eine noch bessere Kompatibilität mit anderen internationalen Standards zu erreichen.

BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)

Dieser Standard definiert allgemeine Anforderungen an ein ISMS. Er ist vollständig kompatibel zum ISO-Standard 27001 und berücksichtigt weiterhin die Empfehlungen der ISO-Standards 13335 und 17799. Er bietet Lesern eine leicht verständliche und systematische Anleitung, unabhängig davon, mit welcher Methode sie die Anforderungen umsetzen möchten.

Das BSI stellt den Inhalt dieser ISO-Standards in einem eigenen BSI-Standard dar, um einige Themen ausführlicher beschreiben zu können, und so eine didaktischere Darstellung der Inhalte zu ermöglichen. Zudem wurde die Gliederung so gestaltet, dass sie zur IT-Grundschutz-Vorgehensweise kompatibel ist. Durch die einheitlichen Überschriften in beiden Dokumenten ist eine Orientierung für den Leser sehr einfach möglich.

BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise

Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein IT-Sicherheitsmanagement in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des IT-Sicherheitsmanagements und der Aufbau einer IT-Sicherheitsorganisation sind dabei wichtige Themen. Die IT-Grundschutz-Vorgehensweise geht sehr ausführlich darauf ein, wie ein IT-Sicherheitskonzept in der Praxis erstellt werden kann, wie angemessene IT-Sicherheitsmaßnahmen ausgewählt werden können und was bei der Umsetzung des IT-Sicherheitskonzeptes zu beachten ist. Auch die Frage, wie die IT-Sicherheit im laufenden Betrieb aufrecht erhalten und verbessert werden kann, wird beantwortet.

IT-Grundschutz interpretiert damit die sehr allgemein gehaltenen Anforderungen der oben genannten ISO-Standards 13335, 17799 und 27001 und hilft den Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrund Know-how und Beispielen. Die IT-Grundschutz-Kataloge erklären nicht nur, was gemacht werden sollte, sondern geben sehr konkrete Hinweise, wie eine Umsetzung (auch auf technischer Ebene) aussehen kann. Ein Vorgehen nach IT-Grundschutz ist somit eine erprobte und effiziente Möglichkeit, allen Anforderungen der oben genannten ISO-Standards nachzukommen.

BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz

Das BSI hat eine Methodik zur Risikoanalyse auf der Basis des IT-Grundschutzes erarbeitet. Diese Vorgehensweise bietet sich an, wenn Unternehmen oder Behörden bereits erfolgreich mit dem IT-Grundschutz arbeiten und möglichst nahtlos eine ergänzende Sicherheitsanalyse an die IT-Grundschutz-Analyse anschließen möchten.

4 ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz

Das BSI zertifiziert IT-Verbünde und Informationssicherheits-Managementsysteme von Unternehmen und Behörden. Die BSI-Zertifizierung umfasst sowohl eine Prüfung des ISMS als auch die Prüfung der konkreten IT-Sicherheitsmaßnahmen auf Basis von IT-Grundschutz. Die BSI-Zertifizierung beinhaltet dabei immer eine offizielle ISO-Zertifizierung nach ISO 27001, ist aber aufgrund der zusätzlich geprüften technischen Aspekte wesentlich aussagekräftiger als eine reine ISO-Zertifizierung. Die wesentlichen Anforderungen zur Prüfung des IT-Sicherheitsmanagements im Rahmen eines Audits ergeben sich aus den Maßnahmen des Grundschutz-Bausteins 1.0 IT-Sicherheitsmanagement. Die Maßnahmen dieses Bausteins sind so geschrieben, dass die wesentlichen Anforderungen des BSI-Standards zu ISMS sofort identifiziert werden können.

Literaturverzeichnis

[ISO13335] ISO/IEC 13335 "Management of information and communications technology security", ISO/IEC JTC1/SC27

[ISO17799] ISO/IEC 17799:2005 "Information technology - Code of practice for information security management", ISO/IEC JTC1/SC27

[ISO27001] ISO/IEC 27001:2005 "Information technology - Security techniques - Information security management systems requirements specification", ISO/IEC JTC1/SC27

[BSI1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.0, Dezember 2005, www.bsi.bund.de

[BSI2] IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 1.0, Dezember 2005, www.bsi.bund.de

[BSI3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Version 1.0, Februar 2004, www.bsi.bund.de

[GSHB] BSI, "IT-Grundschutzhandbuch, Standardsicherheitsmaßnahmen", Loseblattsammlung, Schriftenreihe Band 3, Bundesanzeiger-Verlag, jährlich neu, www.bsi.bund.de/gshb

[ZERT] Allgemeine Informationen zum IT-Grundschutz-Zertifikat, zum Lizenzierungsschema für Auditoren und zum Zertifizierungsschema für IT-Grundschutz unter www.bsi.bund.de/gshb/zert