Der neue ISO/IEC 17799:2005

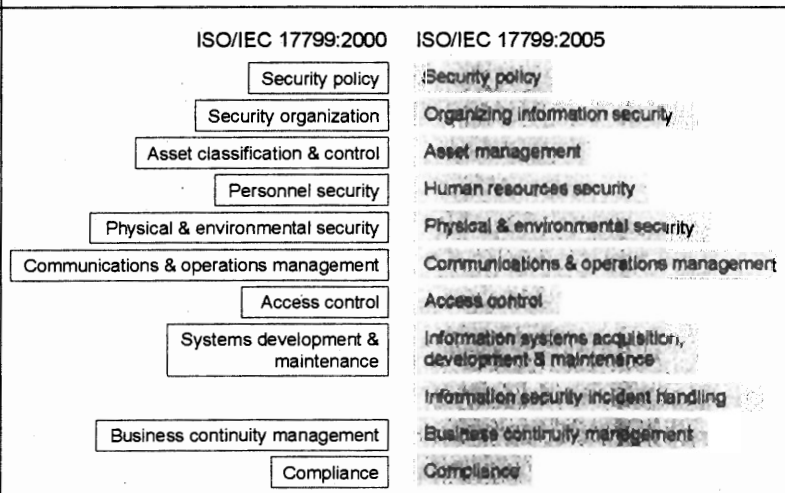
Der Sicherheits-Management-Standard ISO/IEC 17799 wird im Moment von der ISO überarbeitet – die offizielle Verabschiedung ist für Frühjahr/Sommer 2005 zu erwarten. Da die Revision bis auf editorische Korrekturen abgeschlossen ist, steht bereits fest, was sich ändert.

Von Angelika Plate, Bonn

ISO/IEC 17799 *Information technology – Code of practice for information security management,* abgeleitet aus dem British Standard BS 7799-1, wurde im Jahr 2000 erstmals als internationaler Standard verabschiedet. Wie alle Normenwerke ist auch ISO/IEC 17799 dem in der International Organization for Standardization (ISO, www.iso.ch) gültigen Revisionsprozess unterworfen: Regelmäßig alle drei Jahre steht eine Begutachtung an, um die Standards gegebenenfalls zu aktualisieren und die Inhalte neuen Entwicklungen anzupassen. Für ISO/IEC 17799 läuft diese Revision seit 2001 und hat nun einen Status erreicht, in dem der Standard als stabil angesehen werden kann und bald in der neuen Version veröffentlicht wird. Wann genau die ISO den neuen ISO/IEC 17799:2005 veröffentlichen wird, ist nicht bekannt; es ist aber anzunehmen, dass dies im Zeitraum von Mai bis Juli 2005 passiert (bis zur Veröffentlichung des neuen Standards ist die Version aus dem Jahr 2000 natürlich weiterhin uneingeschränkt gültig).

Die Revision von ISO/IEC 17799 findet in ISO/IEC JTC 1/SC27/WG1 statt, derjenigen Arbeitsgruppe, die auch andere Standards für das Management von IT-Sicherheit produziert (vgl. www.din.de/ni/sc27/). Diese Arbeitsgruppe trifft sich zweimal im Jahr, um auf der Basis von Kommentaren aus den Mitgliedsländern neue Versionen der behandelten Standards zu erstellen. Für ISO/IEC 17799 gab es Kommentare aus mehr als 20 Ländern, was das große Interesse widerspiegelt, das weltweit an diesem Standard besteht. Nach intensiven Diskussionen ist es gelungen, Konsens herzustellen – die neue Version des Standards wird von allen Mitgliedsländern unterstützt!

Die Struktur der Kapitel von ISO/IEC 17799 ist bei der Revision im Wesentlichen beibehalten worden; nur das neue Kapitel *Information Security Incident Management* fasst die verschiedenen Maßnahmen zusammen, die dieses Thema in der 2000er-Version behandeln. Einen Überblick über die alten und neuen Kapitel gibt Abbildung 1. Auch die Gliederung des Standards in Maßnahmenziele und Maßnahmen, die helfen, diese Ziele zu erreichen, wurde beibehalten. Insgesamt hat das Gremium acht neue Maßnahmenziele und 17 neue Maßnahmen in den Standard aufgenommen, um neue, wichtige Gebiete abzudecken. Fünf der bestehenden Maßnahmenziele und neun der Maßnahmen aus der Version des Jahres 2000 sind in andere integriert oder gelöscht worden.



Die Struktur und Benennung der Kapitel von ISO/IEC 17799 ist bei der Revision im Wesentlichen beibehalten worden.

Änderungen

Außerdem wurde die Terminologie überarbeitet – zum einen, um internationales Verständnis und die Akzeptanz in verschiedenen Ländern zu fördern, zum anderen, um die in verschiedenen Standards verwendeten Begriffe anzugleichen (da es bisher keine offizielle Übersetzung der neuen Version des Standards gibt, sind im Folgenden sämtliche Zitate aus ISO/IEC 17799 auf Englisch wiedergegeben). Dabei wurden Definitionen aus den folgenden Standards berücksichtigt:

- ISO Guide 73 (Risk Management Vocabulary),
- ISO/IEC TR 13335 (Guidelines for the Management of IT Security),
- ISO/IEC TR 18044 (Information Security Incident Management).

Maßnahmenstruktur

Eine der offensichtlichen Veränderungen im neuen Standard ist die Präsentationsform der Maßnahmen: In der Version aus dem Jahr 2000 besteht die Maßnahmenbeschreibung aus Text, der nicht weiter

untergliedert ist und die Maßnahme selbst sowie Hinweise zu ihrer Umsetzung und weitere Informationen enthält. Dies erschien nicht besonders benutzerfreundlich, da es schwer ist, die eigentliche Maßnahme von eventuell weniger wichtigen Informationen zu trennen. Daher wurde ein neues Format für die Maßnahmen eingeführt, das jede der Maßnahmen in die folgenden drei Teile unterteilt:

_____ *Control:* defines the specific control statement to satisfy the control objective.
_____ *Implementation guidance:* provides more detailed information to support the implementation of the control and compliance with the control objective. This information and guidance may not be suitable in all cases and so other ways of implementing may be more appropriate.
_____ *Other information:* provides further information that may need to be considered, for example legal considerations and references to other standards.

Human Resources Security

In der 2000er-Version von ISO/IEC 17799 bestand das Kapitel *Personnel Security* aus den Maßnahmenzielen:
_____ Security in job definition and resourcing,
_____ User training,
_____ Responding to security incidents and malfunctions.

Um dem inzwischen üblichen Sprachgebrauch zu folgen, wurde das Kapitel in *Human Resources Security* umbenannt. Zudem zeigte sich während der Diskussion, dass der Standard ein häufig auftretendes Problem bisher nicht adäquat behandelt: Was soll beim Ausscheiden eines Mitarbeiters passieren? Dies wird nach wie vor in vielen Firmen vernachlässigt, vielleicht kennen Sie dieses Problem sogar aus eigener Erfahrung: Ein Mitarbeiter verlässt die Firma und hat noch Wochen später die Möglichkeit, sich ins Firmennetzwerk einzuloggen oder einfach mal die alten Kollegen zu besuchen, ohne an der Pforte aufgehalten zu werden. Um diese Vorkommnisse zu vermeiden, wurden neue Maßnahmenziele und Maßnahmen hinzugefügt.

Man hat daher beschlossen, das Kapitel nach den verschiedenen Phasen eines typischen Anstellungsverhältnisses neu zu untergliedern:

Prior to employment: Dieses neue Maßnahmenziel umfasst die meisten der Maßnahmen, die vorher in dem Ziel „Security in job definitions and resourcing" zusammengefasst waren, konzentriert sich aber auf die Fragen, die vor dem Beginn eines Anstellungsverhältnisses zu klären sind.
_____ Roles and responsibilities
_____ Screening
_____ Terms and conditions of employment.

During employment: Dies ist ein neues Maßnahmenziel, das die Verantwortlichkeiten und Aktionen beschreibt, die während der Anstellung wichtig sind, einschließlich der schon vorher vorhandenen Maßnahme zum Benutzertraining.
_____ Management responsibilities
_____ Information security awareness, education and training
_____ Disciplinary process

Termination or change of employment: Dieses neue Maßnahmenziel behandelt die ordnungsgemäße Beendigung oder Veränderung des Anstellungsverhältnisses mit den folgenden neuen Maßnahmen.
_____ Termination responsibilities
_____ Return of assets
_____ Removal of access rights

Information Security Incident Management

Beim Vergleich der alten und neuen Maßnahmenziele in dem *Human-Resource*-Kapitel fällt auf, dass das Maßnahmenziel *Responding to security incidents and malfunctions* verschwunden ist – ohne Entsprechung in der

neuen Version. In ISO/IEC 17799:2000 gab es zwei verschiedene Stellen, an denen das Thema Incidents aufgegriffen wurde: zum einen im Kapitel zu *Personnel Security* und zum anderen beim *Communications and Operations Management*. Diese Aufteilung erschien nicht benutzerfreundlich, daher wurde ein eigenes, neues Kapitel für den Bereich *Information Security Incident Management* geschaffen, das alle Maßnahmen zu diesem Thema zusammenfasst.

Eine weitere Veränderung für die Maßnahmen, die das Berichten von Ereignissen behandeln, ist die Harmonisierung mit dem kürzlich erschienenen Standard ISO/IEC TR 18044 (Information Security Incident Management). Dies führte zu einer Präzisierung der verwendeten Terminologie – es wird nun zwischen *Events und Incidents* unterschieden. Dabei bezeichnet Events alle sicherheits*relevanten* Ereignisse und Incident wird nur für diejenigen Ereignisse verwendet, die ein echtes Sicherheitsproblem darstellen. Ein Beispiel für einen Event, der kein Incident ist, stellt beispielsweise ein autorisierter Nutzer dar, der sein Passwort vergessen hat und versucht, sich mit einem falschen Passwort anzumelden. Die Maßnahmenziele und Maßnahmen in dem neuen Kapitel *Information Security Incident Management* lauten wie folgt:

Reporting information security events and weaknesses: beschreibt das Berichten von sicherheitsrelevanten Ereignissen und Schwachstellen. Es basiert im Wesentlichen auf dem Maßnahmenziel *Responding to incidents and malfunctions*, das sich vorher im Kapitel *Personnel* befand. Die Maßnahmen wurden zusammengefasst, und an die Begriffe in dem Standard ISO/IEC TR 18044 angepasst:

_____ Reporting information security events
_____ Reporting security weaknesses

Management of information security incidents and improvements: soll sicherstellen, dass schadensrelevante Sicherheitsvorfälle konsistent und effektiv gemanagt werden. Die darin enthaltenen Maßnahmen wurden aus verschiedenen Teilen der 2000er-Version zusammengebracht:

_____ Responsibilities and procedures
_____ Learning from information security incidents
_____ Collection of evidence

External Parties

Auch die Behandlung der Zusammenarbeit mit Fremdunternehmen wurde signifikant überarbeitet. Das Kapitel *Organizing Information Security* wurde klarer strukturiert und in die zwei Gebiete *Internal organization* und *External parties* unterteilt.

External parties: behandelt die Risiken beim Zugang von Fremdunternehmen und die Sicherheitsanforderungen, die in Verträgen festgehalten werden können. Es enthält die früheren Maßnahmenziele zu den Themen *Third party access* und *Outsourcing* und berücksichtigt außerdem auch die Zusammenarbeit mit Kunden, da dies inzwischen immer häufiger benötigt wird:

_____ Identification of risks related to external parties
_____ Addressing security when dealing with customers
_____ Addressing security in third party agreements

Eine weitere Ergänzung, die sich mit diesem Themenkreis beschäftigt, wurde im Kapitel *Operations and Communications Management* vorgenommen. Hier gab es bislang eine Maßnahme *External facilities management*, die sich mit dem Management der Aktivitäten beauftragter Fremdunternehmen beschäftigte. Vor dem Hintergrund des IT-Service-Management-Standards BS 15000 erschien es notwendig, diese Maßnahme durch ein neues Maßnahmenziel zu ersetzen, das die sicherheitsrelevanten Aspekte im IT Service Management aufgreift:

Third party service delivery management: hat das sichere Management von Services zum Ziel, die ein Fremdunternehmen anbietet. Dies umfasst Maßnahmen für die Bereitstellung der Services im Rahmen des Vertrages und zu den dort beschriebenen Bedingungen, für die Überwachung und Überprüfung der Services sowie für das Management von Veränderungen, die sich für die gelieferten Services ergeben können:

_____ Service delivery
_____ Monitoring and review of third party services
_____ Managing changes to third party services

Monitoring

Ein weiteres neues Maßnahmenziel soll das Thema *Monitoring* adäquat behandeln und die verschiedenen Überwachungs- und Protokollierungsaktivitäten zusammenfassen. Es basiert auf dem alten Maßnahmenziel *Monitoring system access and use*, wurde aber ausgeweitet, um auch den operationalen Aspekt der Überwachungs- und Protokollierungsaktivitäten mit einzubeziehen. Daher wanderte es auch vom Kapitel *Access Control* ins *Communications and Operations Management*. Ebenfalls hinzugekommen: eine neue Maßnahme, die den Schutz von Protokollen und den darin enthaltenen Informationen adressiert. Sie wurde aus Teilen der ursprünglichen Maßnahmen *Monitoring system use* entwickelt. Die weiteren hierzu gehörenden Maßnahmen entstammen verschiedenen Maßnahmenzielen aus der Vorversion des Standards.

Monitoring: beschreibt die verschiedenen notwendigen Überwachungs- und Protokollierungsaktivitäten und enthält die folgenden Maßnahmen:

_____ Audit logging
_____ Monitoring system use
_____ Protection of log information

_____ Administrator and operator logs
_____ Fault logging
_____ Clock synchronization

Technical Vulnerability Management

Ein weiteres, neues Maßnahmenziel behandelt das Thema Schwachstellenmanagement und Software-Updates. Es ist bekannt, dass die Auswertung veröffentlichter Schwachstellen inzwischen sehr schnell geschieht und den Firmen kaum Zeit lässt, die notwendigen Updates zu installieren. Ein weiteres Problem sind die Patches selbst: ungetestete Updates können ernsthafte Probleme verursachen! Deswegen wurde ein Maßnahmenziel zum Kapitel *Information Systems Acquisition, Development and Maintenance* hinzugefügt.

Technical vulnerability management: adressiert die Sicherheitsfragen in Zusammenhang mit Updates und Software-Patches. Die darin enthaltene Maßnahme behandelt die zeitnahe Identifizierung neuer Schwachstellen und dafür vorgesehener Updates, deren notwendiges Testen und wie man solche Updates installieren sollte, um spätere Probleme zu vermeiden:
_____ Control of technical vulnerabilities

Ausblick

Soweit die wesentlichen Neuerungen und neue Maßnahmenziele in der 2005er-Version – da aber praktisch jede der in ISO/IEC 17799 enthaltenen 133 Maßnahmen in irgendeiner Weise verändert wurde, ist es im Rahmen eines solchen Beitrags unmöglich, *alle* Modifikationen wiederzugeben. Weitere Informationen finden Sie auf der Website der Autorin unter www.aexis.de.

In nächster Zeit wird auch beim Thema Information-Security-Management-System-(ISMS)-Standards noch einiges passieren – sprich: eine ISO-Version von BS 7799 Teil 2 erscheinen, die derzeit in der ISO in Arbeit ist. Wer sich generell für die 7799-Standards interessiert und auf dem neuesten Stand der Entwicklungen bleiben möchte, für den dürfte die ISMS IUG Deutschland interessant sein, der deutsche Teil der ISMS International User Group (ISMS IUG). Die Mitgliedschaft ist übrigens kostenfrei (Näheres auf www.aexis.de./IUGDeutschlandPage.htm) ■

Dr. Angelika Plate ist Geschäftsführerin der ÆXIS Sicherheitsberatung und Co-Editor von ISO/IEC 17799 in der International Organization for Standardization (ISO).