



Von der Qualität zur Informations-Sicherheit

Einführung eines ISMS

Informations-Sicherheits-Management-System

Reinhard Witzke, Produktmanager ISMS

8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



AGENDA

- RICHTLINIEN/GESETZE ZUR INFORMATIONSSICHERHEIT
- INHALT UND GLIEDERUNG BS 7799-2 : 1999
- AKKREDITIERER UND ZERTIFIZIERER NACH BS 7799 IN EUROPA
- NUTZEN EINER ZERTIFIZIERUNG BASIEREND AUF EINEM ISMS NACH BS 7799
- DAS ZERTIFIZIERUNGSVERFAHREN DER DQS
- WEITERE INFORMATIONEN



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



RANDBEDINGUNGEN

Die wachsende Bedeutung von E-Commerce für das Geschäft mit dem Endkunden und der Trend, immer mehr Mitarbeitern, Partnern und Dienstleistern den Zugriff auf das Unternehmensnetz zu erlauben führt dazu, dass Unternehmen sich zunehmend mit Fragen der Informations-Sicherheit auseinandersetzen müssen.



GRUNDLAGEN DATENSCHUTZ-/SICHERHEIT RICHTLINIEN/GESETZE /1

- Bundesdaten-Schutzgesetz (BDSG)
- ISO IEC 15408, Teil 1, Teil 2, Teil 3 (Common Criteria), produkt- und systembezogen
- NIST Computer Security Handbook und Canadian Handbook on Information Technology Security (allgemein, USA bzw.. Canada), generelle Anweisungen und Hinweise, keine konkrete Vorgehensweise





GRUNDLAGEN DATENSCHUTZ/-SICHERHEIT RICHTLINIEN/GESETZE /2

- ETSI Baseline Security Standard Features and Mechanisms (IT-spezifisch, Telekommunikation)
- IT-Spezifische Regelwerke für den Medizin- und den Bankenbereich
- Protection of sensitive Information not covered by Official Secrets Act- Recommendations for computer workstations (allgemein, Frankreich)
- ISO IEC TR 13335 (GMITS),
Teil 1, Teil 2, Teil 3, Teil 4 (allgemein)



GRUNDLAGEN DATENSCHUTZ/-SICHERHEIT RICHTLINIEN/GESETZE /3

- BS 7799-1, jetzt ISO IEC 17799, Dezember 2000

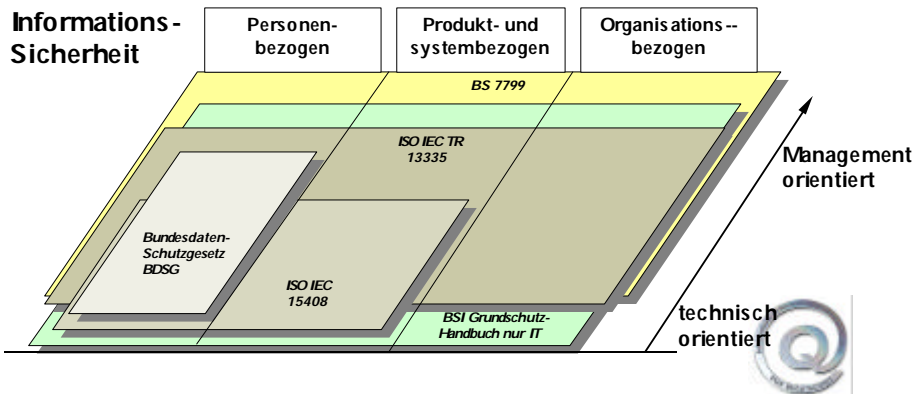
Zertifizierungsfähig:

- Bundesamt für Sicherheit in der Informationstechnik (BSI), Grundschutz-Handbuch, IT-spezifisch (sehr technisch orientiert)
- British Standards BS 7799-2 : 1999





SCHWERPUNKTE DER VERSCHIEDENEN REGELWERKE FÜR INFORMATIONSSICHERHEIT



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



ENTWICKLUNG DER NORM BS 7799 IM INTERNATIONALEN UMFELD

Von United Kingdom wurde bei der International Organization for Standardization (ISO) im sogenannten „FAST-TRACK PROCEDURE“ ein Antrag auf internationale Normung der BS 7799 gestellt.

Das Zustimmungsverfahren begann am 3 Februar 2000 und endete am 3. August 2000. Die Norm wurde als DIS ISO/IEC 17799-1 angenommen.

Im Dezember wurde die Norm als ISO IEC 17799 verabschiedet.



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



INFORMATIONEN-SICHERHEIT /1

- Häufig wird der Problematik der Integrität, der Verfügbarkeit und Vertraulichkeit von Daten zu wenig Bedeutung beigemessen.
 - Die Verantwortung für die Informations-Sicherheit liegt oft bei den DV-Abteilungen und nicht bei der Geschäftsleitung.
- > Implementation von mehr Funktionalität muss einen Mehraufwand zum Schutz zur Folge haben.

8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



INFORMATIONEN-SICHERHEIT /2

- Sicherheit im Unternehmen erfordert Organisation.
- Hier hilft die Einführung eines **ISMS**
Informations-Sicherheits-Management-System nach **BS 7799** Teil 1 und Teil 2, mit einer ähnlichen Systematik wie bei einem QMS, bei der Erreichung einer vom Unternehmen ermittelten, kalkulierbaren Informations-Sicherheit im Unternehmen.



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



INHALT UND GLIEDERUNG BS 7799-2 : 1999 /1

3. Forderungen an das Informations-Sicherheits-Management-System

Stufe 1: Risikoanalyse

- Leistungsprozesse definieren
- Ableiten der Hauptrisiken (z.B. aus KonTrAG)
- Erstellen der Sicherheitspolitik
- Risiken analysieren und bewerten
- Maßnahmen ergreifen um:
 - Risiko zu vermindern oder zu versichern.
 - In jedem Fall muss das Risiko getragen werden



INHALT UND GLIEDERUNG BS 7799-2 : 1999 /2

3. Forderungen an das Informations-Sicherheits-Management-System

Stufe 2: Prozesse beherrschen

- Management der Risiken
- Überprüfung der Maßnahmen auf Wirksamkeit
- Regelmäßige Neubewertung des Risikoinventars bzgl. der Risikolage
- Anpassung bzw. Überprüfung der Sicherheitspolitik und des ISMS





INHALT UND GLIEDERUNG BS 7799-2 : 1999 /3

3. Forderungen an das Informations-Sicherheits-Management-System

- Dokumentation in einem ISMS-Handbuch
- Periodisches Überprüfen der Dokumente
- Aufzeichnungen



INHALT UND GLIEDERUNG BS 7799-2 : 1999 /4

4. Spezifische Maßnahmen /1

- 4.1 Sicherheitspolitik
- 4.2 Organisation der Sicherheit
- 4.3 Einstufung und Kontrolle der Werte
- 4.4 Personelle Sicherheit
- 4.5 Physische und umgebungsbezogene Sicherheit





INHALT UND GLIEDERUNG BS 7799-2 : 1999 /5

Spezifische Maßnahmen /2

- 4.6 Management der Kommunikation und Betriebsabläufe
- 4.7 Zugangskontrolle
- 4.8 Systementwicklung und -wartung
- 4.9 Management des kontinuierlichen Geschäftsbetriebs
- 4.10 Einhaltung der Vorgaben



INHALT UND GLIEDERUNG BS 7799-2 : 1999 /6

4.1 SICHERHEITSPOLITIK

Ziel:

Richtungsweisung und Unterstützung des Managements für die Informations-Sicherheit.

Die **Geschäftsführung** muss eine **klare Richtung** vorgeben und ihre **Unterstützung** und ihr **Engagement** durch **organisationsweite Veröffentlichung** der Vorschriften zur Informations-Sicherheit zeigen.





INHALT UND GLIEDERUNG BS 7799-2 : 1999 /7 4.2 SICHERHEITS-ORGANISATION

Ziel:

Verwaltung von Informations-Sicherheit innerhalb der Organisation.

Rahmenbedingungen für die Verwaltung müssen geschaffen werden, um die **Implementierung** von **Informations-Sicherheit** innerhalb der **Organisation einzuführen** und zu **überwa**



INHALT UND GLIEDERUNG BS 7799-2 : 1999 /8 4.3 KLASSIFIZIERUNG UND ÜBERWACHUNG DER ANLAGEN UND BESTÄNDE

Ziel:

Inventarisierung der Hardware und Software, Festlegung des Schutzniveaus, Überwachung und Ausweisung des Schutzniveaus.





INHALT UND GLIEDERUNG BS 7799-2 : 1999 /9 4.4 PERSONELLE SICHERHEIT

Ziel:

Reduzierung der **Risiken** durch **menschlichen Irrtum, Diebstahl, Betrug oder Missbrauch** der Einrichtungen.

Die Aspekte der Informations-Sicherheit müssen bei der Einstellung besprochen und in **Stellenbeschreibungen** und **Verträge eingeschlossen**, und während der **Anstellung** der Person **überprüft** werden.



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



INHALT UND GLIEDERUNG BS 7799-2 : 1999 /10 4.5 PHYSISCHE UND UMGEBUNGSBEZOGENE SICHERHEIT

Ziel:

Verhinderung von **unberechtigtem Zugang**, von **Beschädigung** und **Störung** der informationsverarbeitenden Dienste.

Informationsverarbeitende Einrichtungen, die **wichtige** und **vertrauliche Geschäftstätigkeiten** unterstützen, müssen in **Sicherheitszonen** untergebracht werden.



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



INHALT UND GLIEDERUNG BS 7799-2 : 1999 /11 4.6 MANAGEMENT DER KOMMUNIKATION UND BETRIEBSABLÄUFE

Ziel:

Gewährleistung des korrekten und **sicheren Betriebs von Rechner- und Netzeinrichtungen**.
Verantwortlichkeiten und Verfahren für die Verwaltung und den Betrieb **aller** für den **Geschäftsprozess** notwendigen Rechner und Netze müssen **eingeführt** werden.



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



INHALT UND GLIEDERUNG BS 7799-2 : 1999 /12 4.7 ZUGRIFFSÜBERWACHUNG

Ziel:

Überwachung des Zugriffs auf
Geschäftsinformationen.

Der **Zugriff** auf **Rechnerdienste und Daten** muss unter Berücksichtigung der Unternehmensbelange **überwacht** werden.



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



INHALT UND GLIEDERUNG BS 7799-2 : 1999 /13 4.8 SYSTEMENTWICKLUNG UND -WARTUNG

Ziel:

Verlässliche Sicherheit von informationsverarbeitenden Technologien und Systemen.

Vor der **Entwicklung von informationsverarbeitenden Systemen** müssen **Sicherheitsforderungen identifiziert** und **vereinbart** werden. Bei der **Wartung** von Systemen müssen diese Forderungen berücksichtigt werden.



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



INHALT UND GLIEDERUNG BS 7799-2 : 1999 /14 4.9 GESCHÄFTSKONTINUITÄTSPLANUNG

Ziel:

Verfügbarkeit von **Plänen**, um **Unterbrechungen** von **Geschäftsaktivitäten entgegenzuwirken**.

Geschäftskontinuitätspläne müssen zum **Schutz** kritischer **Geschäftsvorgänge** vor größeren **Störungs- oder Katastrophenauswirkungen** verfügbar sein.



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



INHALT UND GLIEDERUNG BS 7799-2 : 1999 /15

4.10 EINHALTUNG DER VORGABEN

Ziel:

Vermeidung von **Verletzungen** jeglicher **Gesetze** des **Straf- oder Zivilrechts** und jeglicher **Sicherheitsforderungen des Unternehmens**.

Berücksichtigung von gesetzlichen und vertraglichen **Sicherheitsforderungen** in der **Entwicklung**, im **Betrieb** und beim **Einsatz** von informationsverarbeitenden Systemen.



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



AKKREDITIERER UND ZERTIFIZIERER NACH BS 7799 IN EUROPA

Akkreditierungsgrundlage: EA 07 / 03, Mai 2000

- Akkreditierer : UKAS, RVA, TGA
- Akkreditierte Zertifizierer:
KPMG, BSI, KEMA, DNVQA, LRQA, NQA, SIS

Anzahl der zertifizierten Unternehmen:

- BSI: ca. 30, KPMG: 5, KEMA: 10, DQS: 3, ÖQS: 1
- In Deutschland akkreditiert: DQS,
- DQS hat zertifiziert: Siemens ITS, Siemens CCN, Wien, DeteCSM, im Verfahren: 7 Unternehmen



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



NUTZEN EINER ZERTIFIZIERUNG BASIEREND AUF EINEM ISMS NACH BS 7799 /1

*Risiken können mit einem Informations-Sicherheits-
Management-System definiert, eingeschätzt und
damit beherrscht werden:*

- Schutz vor Datenmissbrauch oder Datenverlust
- Die Arbeitsfähigkeit wird gesichert
- Schutz vor Know-How-Abfluss
- Sichert den Fortbestand des Unternehmens
- Erhöht das Sicherheitsbewusstsein im Unternehmen



NUTZEN EINER ZERTIFIZIERUNG BASIEREND AUF EINEM ISMS NACH BS 7799 /2

- Politik zur Nutzung von Signaturen und
Verschlüsselungstechniken
- Fördert den sinnvollen Umgang mit
Sicherheitwerkzeugen
- Reduziert das Haftungsrisiko der verantwortlichen
Führungskräfte
- Standard berücksichtigt alle Informationen des
Unternehmens, nicht nur die IT-Prozesse





NUTZEN EINER ZERTIFIZIERUNG BASIEREND AUF EINEM ISMS NACH BS 7799 /3

Das Unternehmen kann seinen Kunden zeigen, dass es sich an einem internationalen Standard orientiert, dass es innovativ und verantwortungsbewusst handelt.

Jede Verbindung des Unternehmens nach außen ist klar definiert (z.B. bei Nutzung von Outsourcing oder Application Service Providern ASP). SLAs sollten sich am Geltungsbereich des ISMS orientieren.



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



NUTZEN EINER ZERTIFIZIERUNG BASIEREND AUF EINEM ISMS NACH BS 7799 /4

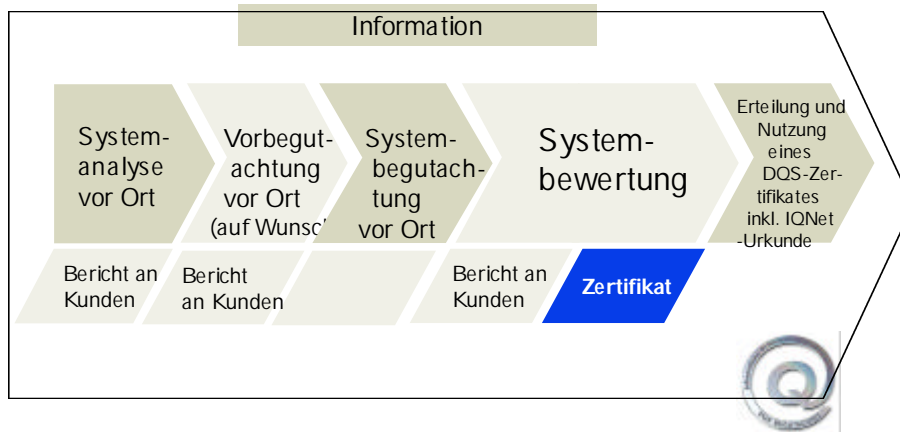
- Mitarbeiter können einen aktiven Beitrag zum Fortbestand des Unternehmens leisten
- ISMS kann als Nachweis für Wirtschaftsprüfungen herangezogen werden.
- ISMS leistet einen Beitrag zur Konzentration der Bestandführung in Unternehmen (HW und SW)



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



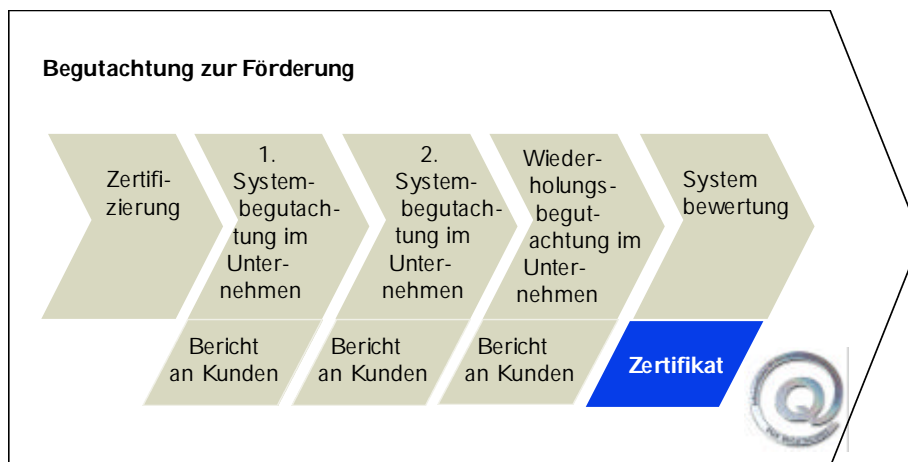
DAS ZERTIFIZIERUNGSVERFAHREN DER DQS / 1



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



DAS ZERTIFIZIERUNGSVERFAHREN DER DQS / 2



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



DAS ZERTIFIZIERUNGSVERFAHREN DER DQS /3

Vorbereitung (unabhängig von einer Zertifizierung)

- Risikobewertung:
Grad des Sicherheitsniveaus wird analysiert und die potentiellen Risiken werden aufgezeigt, das Ergebnis in einem Bericht festgehalten
- Vorbegutachtung (optional):
Beurteilung festgelegter Bereiche/Prozesse, Kurzbericht mit Handlungsbedarf



DAS ZERTIFIZIERUNGSVERFAHREN DER DQS /4

Begutachtung

(auch unabhängig von einer Zertifizierung möglich)

- Systemanalyse
- Vorbegutachtung (optional)
- Systembegutachtung
- Bewertung





DAS ZERTIFIZIERUNGSVERFAHREN DER DQS /5

Zertifizierung

- Bewertung
- Zertifikaterteilung



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



SERVICELLEISTUNGEN DER DQS

Foren/Training

- DQS-Forum (Ein-Tages-Veranstaltung)
- Inhouse-Training (Modulares Inhouse-Training - Ein- oder Zwei-Tages-Workshop)
- Intensiv-Seminar für das Management (Spezielles Modul für die 1. Führungsebene)



8. Workshop „Sicherheit in vernetzten Systemen“ © DQS Copyright



WARUM ZERTIFIZIERUNG...

- Zertifikat = Nachweis der Bewertung und damit Nachweis für den verantwortungsbewussten Umgang mit Risiken, Kundendaten und Informationen
- Belohnung und Bestätigung für die Mitarbeiter und das Unternehmen
- Motivation, da ein Etappenziel erreicht wurde
- Positiver Schub für das Gesamtsystem
- Steigert das Ansehen des Unternehmens



WARUM ISMS...

- Zertifizierungsfähiges Managementsystem
- Präventiver Ansatz
- Ganzheitlicher Ansatz und damit nahtlos in andere Systeme integrierbar
- Unabhängig bewertbar auf Basis eines international bekannten Standards
- Neutraler Nachweis mit dem Zertifikat





LITERATURHINWEIS UND WEITERE INFORMATIONEN...

Bezugsquelle für die ISO IEC 17799 bzw. BS 7799-2:

- Auslandsnormenstelle des Beuth Verlags:
Telefax: 030-2601-1801
- Beuth Verlag

DQS: „ISO 9000: Die große Revision“ von Konrad Schieber

Weitere Informationen zum Thema finden Sie im Internet unter der Seite der DQS:

<http://www.dqs.de>

8. Witzke (D) Simmering-Wittgenstein AG © 2005 Copyright



Danke für Ihre Aufmerksamkeit !

www.dqs.de
reinhard.witzke@dqs.de
Tel: (030) 26 01-27 64

