Management der Informationssicherheit nach ISO 17799

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg

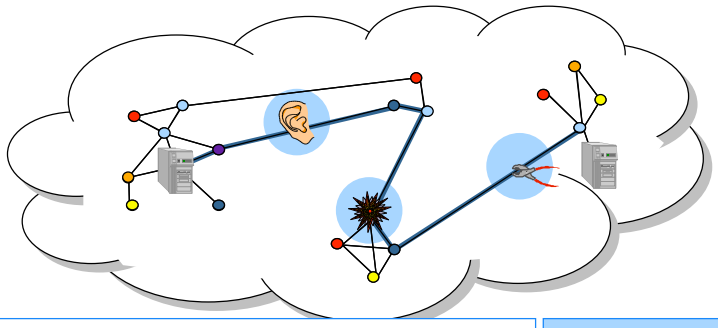
IT-Sicherheitsmanagement
Prof. Dr.-Ing.
Hannes Federrath

Management der Informationssicherheit

IT-Sicherheitsmanagement versucht, die mit Hilfe von Informationstechnik (IT) realisierten Produktions- und Geschäftsprozesse in Unternehmen und Organisationen systematisch gegen beabsichtigte Angriffe (Security) und unbeabsichtigte Ereignisse (Safety) zu schützen.

- Themen, die am Lehrstuhl bearbeitet werden:
  - Sicherheit in verteilten Systemen und Mehrseitige Sicherheit
  - Datenschutzfreundliche Techniken
  - Sicherheit im Internet
  - Digital Rights Management Systeme
  - Sicherheit im E-Commerce und in mobilen Systemen
- Weitere Informationen:
  - http://www-sec.uni-regensburg.de

Was ist Informationssicherheit?



Bedrohungen

- unbefugter Informationsgewinn
- unbefugte Modifikation
- unbefugte Beeinträchtigung der Funktionalität

Schutz der

- Vertraulichkeit
- Integrität
- Verfügbarkeit

ISO 17799

- International Standard ISO/IEC 17799
  Information technology — Code of practice for information security management, 2000
- Eigener Anspruch
  - «A comprehensive set of controls comprising best practices in information security»
- Umfang
  - 71 Seiten, umfasst 10 Gliederungspunkte bzgl. Managementaufgaben
- kontinuierliche Aktualisierung
  - keine verbindlichen Zyklen festgelegt, aber vorgesehen
  - prinzipiell nicht unbedingt nötig, da sehr generische Formulierungen

Zweck des Standards ISO 17799

- Internationaler «Code of practice» für das Management der Informationssicherheit
- Sicherheit im Großen
  - betrifft die an der Informationsverarbeitung beteiligten Menschen, Prozesse und IT-Systeme
  - behandelt die übergreifenden Aspekte der Informationssicherheit
- Ziel:
  - Schaffung unternehmensweiter Sicherheit:
    - Enterprise Security
  - Aufbau eines Information Security Management Systems

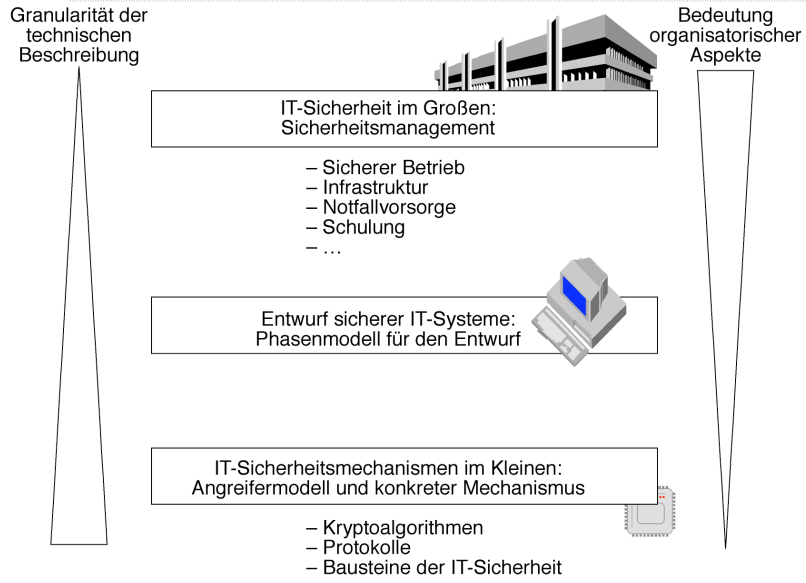
Einordnung in die Kriterienlandschaft

- Andere sicherheitsbezogene Standards für
  - kryptographische Methoden
  - Hardwaresicherheit
  - Verfahren für Schlüssel- und Zertifikatsmanagement
  - ...
    - teilweise sogar banchenspezifische Standards (z.B. Banking)
- Einordnung

		technisch	nicht-technisch
System-bezogen		IT-GSHB	ISO9000 ISO13335 ISO 17799
Produkt-bezogen	Task Force	Datenschutz-gütesiegel	
	FIPS 140 ITSEC/CC		

nach: Initiative D21: IT-Sicherheitskriterien im Vergleich. Leitfaden der Projektgruppe IT-Sicherheitskriterien und IT-Grundschutz-Zertifikat/Qualifizierung, Projekt der Arbeitsgruppe Sicherheit und Vertrauen im Internet, 20.12.2001.

Einordnung bzgl. technischem Detaillierungsgrad



Gliederungspunkte

• Security policy	• *Sicherheitspolitik*
• Organizational security	• *Organisatorische Sicherheit*
• Asset classification and control	• *Einstufung und Kontrolle der Werte*
• Personnel security	• *personelle Sicherheit*
• Physical and environmental security	• *physische und umgebungsbezogene Sicherheit*
• Communications and operations management	• *Management der Kommunikation und des Betriebs*
• Access control	• *Zugriffskontrolle*
• Systems development and maintenance	• *Systementwicklung und -wartung*
• Business continuity management	• *Management des kontinuierlichen Geschäftsbetriebs*
• Compliance	• *Einhaltung der Verpflichtungen*

Security policy

- Definiert die grundsätzliche Position des Unternehmens bzgl. Informationssicherheit

- erfordert Erstellung eines Policy-Dokuments
  a) Definition von Informationssicherheit aus Unternehmenssicht
  b) Definition des Managementziels bzgl. Informationssicherheit
  c) Kurzbeschreibung von
     1. Übereinstimmung der Maßnahmen mit geltendem Recht und bestehenden vertraglichen Vereinbarungen
     2. Anforderungen an Schulungsmaßnahmen
     3. Abwehr von Viren und anderen schädlichen Softwarecodes
     4. Business continuity management
     5. Verfahrensweise bei Verstößen gegen die Policy
  d) Definition der Zuständigkeiten für Informationssicherheit
  e) Verweise auf Dokumente, die zur Umsetzung der Policy dienen
- regelmäßiger Review und Anpassung an neue Gegebenheiten

IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

Organizational security

1. Infrastrukturmaßnahmen
   - Schaffen eines organisatorisch-technischen Rahmens für das Management der Informationssicherheit innerhalb der Organisation

   Maßnahmen
   - Festlegen der Zuständigkeit (Security Manager) für
     - Review, Bestätigung und Fortschreibung der Security Policy
     - Überwachung und Beurteilung von Sicherheitsverstößen, Änderungen der Sicherheitslage
     - Billigung von Maßnahmen zur Verbesserung des Sicherheitsniveaus
   - Schaffen einer Koordinationsgruppe für Informationssicherheit
   - Festlegen von Zuständigkeiten

Organizational security

2. Zugriff auf Unternehmensdaten durch Dritte
   - Schaffen eines organisatorisch-technischen Rahmens für den Zugriff auf Unternehmensdaten durch Dritte

   Maßnahmen
   - Festlegen von Zugriffsarten (logischer, physischer) Zugriff
   - Beschreiben, für welche Aufgaben der Zugriff nötig ist

3. Outsourcing
   - Erhaltung des festgelegten Sicherheitsniveaus beim Outsourcing

   Maßnahmen
   - Vertragliche Festlegung von Sicherheitsanforderungen, z.B.
     - Einhaltung gesetzlicher Vorschriften (z.B. Datenschutz)
     - Recht auf Überprüfung der Einhaltung der festgelegten Anforderungen

IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

Asset classification and control

1. Zuständigkeit für das Management der Erhaltung von Unternehmens-Assets
   - Führen einer «Inventarliste»
     - information assets
     - software assets
     - physical assets
     - services

2. Klassifikation von Information
   - Identifikation von Notwendigkeit und Wichtigkeit von Informationen
   - Festlegen des notwendigen Schutzgrades

Personnel security

1. Sicherheit bei der Stellenbesetzung zur Vermeidung von menschlichem Versagen, Missbrauch, Diebstahl, Betrug

   Maßnahmen
   - Formulierung von Sicherheitsanforderungen an Stelleninhaber
   - Sicherheitsüberprüfung der Mitarbeiter
   - Geheimhaltungserklärung
   - Arbeitsvertrag mit Klausel versehen, die auf die Einhaltung der Sicherheitsmaßnahmen hinweist

IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

Personnel security

2. Trainingsmaßnahmen zur Verbesserung der «Awareness»
   - Schulung und Training in der korrekten Verwendung von Software und Geräten
   - Schulung und Sensibilisierung im Umgang mit Informationen
   - ...

3. Vorgehensweise bei Sicherheitsverletzungen und Fehlfunktionen
   - Berichtswesen bzgl. Sicherheitsschwächen und Sicherheitsverletzungen
   - Vorgehen bei Entdecken von Fehlern und Sicherheitslücken in Software

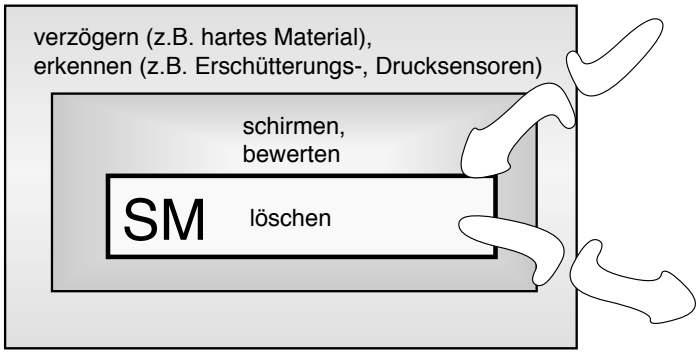
Physical and environmental security

1. Sicherheitsbereiche festlegen

Maßnahmen
- Aufbau physischer Barrieren
- Definition von Besucherbereichen
- Zugangskontrollen an Gebäuden, Räumen und Systemen
- Absicherung von Büros, Räumen und Einrichtungen
- Arbeitsplatzsicherheit
- Sicherheit von Ein-, Ausgangs- und Verladebereichen

Physische Sicherheit: Grundfunktionen

- Beobachtende Angriffe:
  - Schirmung (elektromagnetische Abstrahlung, Energieverbrauch – unabhängig von den zu schützenden Geheimnissen)
- Verändernde Angriffe:
  - Erkennen, Bewerten,Verzögern und ggf. Löschen der geheimen Informationen.



Physische Sicherheit

- Sicherheitsmodul

Bild: www.lampertz.de

- Brandschutz
- Zugangsschutz
- Klimatisierung
- Unabhängige Stromversorgung

Physical and environmental security

2. Gerätesicherheit

Maßnahmen

- Generelle Empfehlungen
  - «Nicht essen am Computer»
- Geeignete Energieversorgung
  - UPS, Notstrom
- Sicherheit der Verkabelung
- Wartung und Reparatur von Geräten
  - Sensible Daten auf Datenträgern
- Entsorgung von Geräten, Datenträgern

Physical and environmental security

3. Allgemeine Regeln am Arbeitsplatz

Maßnahmen

- Dokumente und Medien verschließbar aufbewahren
- Vertrauliche Dokumente besonders sichern (Feuerschutz, ...)
- Computer, Drucker – wenn unbeaufsichtigt – sperren
- Post-Ein- und -Ausgangsstellen, Faxgeräte (incoming) besonders sichern
- Fotokopierer mit Nutzungsberechtigung versehen (außerhalb normaler Dienstzeiten)
- Sensible Ausdrucke sofort aus dem Drucker nehmen
- ...

Communications and operations management

1. Zuständigkeiten für den sicheren Betrieb der Informationsverarbeitungseinrichtungen

Maßnahmen

- Dokumentation von Betriebsabläufen (Prozessen)
- Regeln zur Aufrechterhaltung des Sicherheitsniveaus bei Änderungen im Ablauf von Prozessen
- Prozeduren zum Management bei Zwischenfällen
- Verteilung von Verantwortung
- Nutzung von verteilten Systemen und Diversität
- Nutzung externer Dienste und Dienstleistungen

Communications and operations management

2. Systemplanung

Maßnahmen

- Ressourcenmanagement
- Planung von Kapazitäten
- Schaffung von Systemakzeptanz
  - Ausführliche Tests neuer Software-(versionen)
  - Bereitstellung von Dokumentationen und Schulungsunterlagen
  - Pläne für Fehlerbeseitigung
  - ...

IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

Communications and operations management

3. Schutz vor fehlerhafter und böswilliger Software
   - Virenscanner auf Dateien, E-Mails
   - Update-Management
   - Sicherstellung, dass Warnhinweise korrekt sind

4. «Housekeeping»
   - Backup
   - Protokollierung inkl. regelmäßiger Überprüfung im laufenden Betrieb
     - Systemstart, -ende
     - Systemfehler und Maßnahmen zur Beseitigung
     - Name des Protokollierenden
   - Protokollierung von Fehlern

Communications and operations management

5. Netzmanagement
   - Gewaltenteilung zwischen Rechner- und Netzadministration
   - Sicherheitsmaßnahmen zur Gewährleistung von Vertraulichkeit und Integrität
     - Verschlüsselung auf Übertragungsstrecken
     - Virtuelle Private Netze

6. Sicherer Umgang mit Medien
   - Löschung nicht mehr genutzter Medien
   - Autorisierung zur Löschung und Entsorgung
   - Aufbewahrung in Safe, sicherer Umgebung, ...

7. Informationsaustausch zwischen Unternehmen
   - Datenträgertransport
   - E-Commerce-Sicherheit
   - E-Mail-Sicherheit

IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

Access control

1. Access control policy

2. Mechanismen der Zugriffskontrolle
   - Nutzerregistrierung
   - Rechtevergabe und -überprüfung
   - Passwort-Management

3. Verantwortlichkeiten der Nutzer
   - Passwortsicherheit -->
   - Verhalten beim Verlassen des Rechners

4. Entfernter Zugriff (über Rechnernetze)
   - Einschränkungen beim Fernzugriff
   - Überwachung von Fernzugriffen
     - Protokollierung von Telefonnummer des Einwählenden
     - Firewalls, Intrusion Detection Systeme
   - Nutzer- und Geräteauthentikation bei Fernzugriffen

Passwortregeln

- Ändern Sie Ihr Passwort in regelmäßigen Abständen.
- Legen Sie niemals Passwörter in Dateien ab.
- Verwenden Sie in Ihrem Passwort nicht
  - Namen, Telefonnummern, Geburtsdaten, Autonummern,
  - Wörter aus Wörterbüchern, Eigennamen,
  - Tastaturmuster (vgl. «wertzuio»).
  - All dies rückwärts oder doppelt.
  - All dies mit Ziffern oder Sonderzeichen davor oder dahinter.
  - All dies in kombinierter Groß- und Kleinschreibweise.
- Beachten Sie, dass häufig nur die ersten acht Zeichen des Passwortes signifikant sind.
- Verwenden Sie
  - viele verschiedene Zeichen,
  - kombinierte Groß- und Kleinschreibweise,
  - Ziffern und Sonderzeichen.

```
hQEMAwktkZbtS
f2RAQf+NkiAnJ
ToYWKQ54OVYiQ
JBj5s5zdpmpSk
smDf617QT49QJ
gnVu3XN9mE8Pv
```

- Trick: Verwenden Sie die Anfangsbuchstaben eines «verrückten» Satzes, der auch Zahlen und Sonderzeichen enthält.

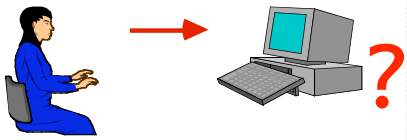
Access control

5. Zugriffskontrolle auf Betriebssystemebene
   - entspricht eigentlich einer Zugangskontrolle:
     - Identifikation des Nutzers -->
6. Zugriffskontrolle auf Anwendungsebene
7. Protokollierung
8. Sicherheit beim mobile Computing und bei Telearbeit

Identifikation von Menschen durch IT-Systeme

- Was der MENSCH IST:
  - Biometrische Merkmale
    - Aussehen*
    - eigenhändige Unterschrift*
    - Stimme, …
- Was der MENSCH HAT:
  - Papierdokument*
  - Metallschlüssel
  - Magnetstreifenkarte
  - Chipkarte
  - Taschenrechner
- Was der MENSCH WEIß:
  - Passwort
  - Antworten auf Fragen
  - Rechenergebnisse für Zahlen

*=Ausweis



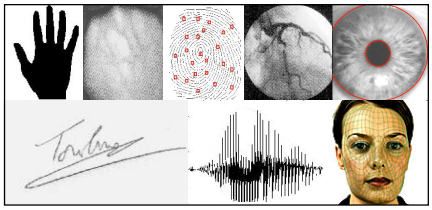
SecurID

Bild: http://www.rsasecurity.com

IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

Biometrische Merkmale

- Physiologische
  - Handgeometrie
  - Handvenenmuster
  - Fingerabdruck
  - Retina
  - Iris
  - Gesicht
  - DNA
  - Ohrmuscheln
- Verhaltensbasierte
  - Handschrift
  - Stimme
  - Lippenbewegung
  - Tipp-Charakteristik
  - Gang



Bilder:
http://biometrics.cse.msu.edu/
http://www.atica.pm.gouv.fr/dossiers/documents/biometrie.shtml
http://www.br-online.de/wissen-bildung/thema/biometrie/koerper.shtml

Bild: Acer

Systems development and maintenance

- Maßnahmen
  1. Definition von Sicherheitsanforderungen bereits beim Systemdesign
  2. Sicherheit in Anwendungssystemen
  3. Einsatz kryptographischer Verfahren
  4. Schutz von Systemdateien
  5. Sicherheit innerhalb des Entwicklungsprozesses

Business continuity management

- Verhindern von Unterbrechungen und Sicherstellung des laufenden Geschäftsbetriebs

Maßnahmen

1. Beschreibung des Prozesses
2. Analyse
3. Aufstellen eines business continuity plans
4. Test

Compliance

1. Übereinstimmung mit den gesetzlichen Rahmenbedingungen
   - Copyright, Softwarerecht
   - Datenschutz
   - Missbrauch, Strafverfolgung, ...
2. Prüfen, ob ergriffene Maßnahmen zur Informationssicherheit mit der Security Policy übereinstimmen
   - ggf. Änderungen vornehmen
3. Maßnahmen zur effektiven Systemüberprüfung
   - z.B. im Hinblick auf eine spätere Zertifizierung

Gliederungspunkte

1. Security policy
2. Organizational security
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance

Für welche Bereiche ist ISO 17799 { bevorzugt / weniger } geeignet?

- Unternehmenstypen
  - Server-Betreiber
  - Inhalte-Anbieter
  - Unternehmen als Anwender
  - Software-Hersteller
  - Kommunikationsnetzbetreiber
- Innerhalb des Unternehmens
  - Unternehmensmanagement
  - Projektmanagement
  - IT-Leitung
  - IT-Sicherheitsbeauftragte
  - Administratoren
  - Revisoren

IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

Bewertung von ISO 17799

- Zielgruppe
  - Unternehmen und Behören aller Größenordnungen
    - jedoch eher geeignet für größere Organisationen
    - Aufwand für kleinere Organisationen ist überproportional hoch
  - nicht gut geeignet für Privatanwender
  - Alternative:
    - Grundschutz-Handbuch des BSI

Bewertung von ISO 17799

- System-/Produkttypen
  - geschaffen für
    Bewertung eines sozio-technischen Gesamtsystems
    - Top-Down-Ansatz zur Schaffung von Informationssicherheit
    - hauptsächlich generische Sicherheitsmaßnahmen
  - weniger geeignet zur Zertifizierung einzelner Produkte
  - gut: Einbettung eines Produktes in das Gesamtsystem

- Problem:
  - Bei Zerlegung des Systems in Teilsysteme keine geeigneten Maßnahmenempfehlungen, die das sichere Zusammenfügen der Teilsysteme unterstützen

IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

Bewertung von ISO 17799

- Anwendungsweise
  1. Verwendung als Nachschlagewerk für Fragen zum Einsatz einzelner (High-Level)-Maßnahmen
  2. Aufbau eines Information Security Management Systems (ISMS) nach dem State-of-the-Art
  3. Aufbau eines zertifizierbaren ISMS

- 2. und 3. erfordern systematische und vollständige Abarbeitung der Maßnahmenempfehlungen

Bewertung von ISO 17799

- Erreichbares Sicherheitsniveau
  - recht umfassender Maßnahmenkatalog
  - definiert größtenteils Standard-Sicherheitsmaßnahmen
  - für Hochsicherheit weiter gehende Maßnahmen erforderlich
  - jedoch: Management von Hochsicherheit wird durch Managementansatz unterstützt
- Aufwand für Umsetzung
  - hängt vom Organisationsgrad des Unternehmens ab
  - hoher Organisationsgrad — weniger Aufwand
  - Umsetzung der Maßnahmen kann durch Tools unterstützt werden

Weitere Informationen im Internet

- Text des Standards
  - http://www.iso.ch
- Weitere Informationen und Software zu ISO 17799
  - http://www.iso17799software.com
  - http://www.iso-17799.com
  - ...
- Web-basierter 30-minütiger Test zum Benchmark der eigenen Sicherheitsvorkehrungen
  - orientiert sich u.a. an ISO 17799
  - http://www.humanfirewall.com/smi/
- Zertifizierung eines Information Security Management Systems
  - z.B. TÜV Informationstechnik
  - http://www.tuvit.de/