IT - Sicherheitsstandards

- warum, wieso, weshalb?
- und wenn ja, welche taugen wie für was?

- Überblick über die Standards:
  - BSI Grundschutz,
  - ISO 7799,
  - Common Criteria und
  - ITIL

IT Sicherheitsstandards - Inhalt

- Warum Standards für IT-Sicherheit?
- Welche IT- Sicherheitsstandards gibt es?
  - Erläuterung und partieller Vergleich der einzelnen Standards:
    - BSI GSHB
    - Common Criteria
    - ITIL
    - BS 7799
- Zusammenfassung
- Fazit

Warum Standards für IT-Sicherheit?

- verschiedene Sicherheitsziele:
  - **Verfügbarkeit**
  - **Vertraulichkeit**
  - **Integrität**
  - **Nicht-Abstreitbarkeit /Anonymität**
- **Komplexität** an Informationen, IT-Systemen, Applikationen, Usern, Rechten etc.
  - --> gesucht: Leitfaden, Checkliste, Anhaltspunkt
- = Standards als „eingedampfte“ Erfahrungen, wiederverwendbar, allgemein anerkannt
- für IT-Sicherheit: ISMS = Information Security Management Systems

Einsatzgebiete von IT-Sicherheitsstandards

- Design von IT- Systemen und Anwendungen, in denen Sicherheit von Vertraulichkeit bis Verfügbarkeit eine Rolle spielt
- Prüfung und Bewertung von IT Sicherheit
  - als Eigencheck
  - als Zertifikat gegenüber Dritten
- Planung, Dokumentation, Kontrolle

Welche IT-Sicherheitsstandards gibt es?

- detailliert Technik+Orga:BSI Grundschutzhandbuch
- technisch abstrakt: Common Criteria
- Betrieb / best practise: ITIL
- nur Orga: BS 7799-2
- sonst: Technical report 13335, Cobit etc.

Inhalt von IT-Sicherheitsstandards

- Technik: Applikationen, Betriebssystemen, Netzwerken, Hardware
  - BSI Grundschutzhandbuch
  - Common Criteria
- Organisation, Zuständigkeiten, Sicherheitsmgmt
  - ITIL
  - BS 7799
  - BSI Grundschutzhandbuch
- nicht: Gesetze (TKÜV, RegTP. Basel II, SOX etc.)

BSI IT-Grundschutzhandbuch

- detailliert technisch und organisatorisch
- keine Risikoabschätzung: Gießkannenprinzip in
  - Gefährungskataloge und
  - Maßnahmenkataloge
- wenig: Prozesse /Ablauf; besser bei ITIL (s.u.)
- Technik und Orga

BSI IT-Grundschutzhandbuch

- 1.Teil Einstieg
- 2. Teil Bausteine: umfaßt die Kapitel:
  - Übergeordnete Komponenten
  - Infrastruktur
  - Nicht vernetzte Systeme und Clients
  - Vernetzte Systeme und Server
  - Datenübertragungseinrichtungen
  - Telekommunikation
  - Sonstige IT-Komponenten
- /home/mirror/ccc2004/vortrag_itsecstandards/standardsitsec/bsi/deutsch/etc/inhalt.htm

BSI IT-Grundschutzhandbuch

- Gefährdungskataloge:
  - Höhere Gewalt
  - Organisatorische Mängel
  - Menschliche Fehlhandlungen
  - Technisches Versagen
  - Vorsätzliche Handlungen

BSI IT-Grundschutzhandbuch

- Maßnahmenkataloge:
  - Infrastrukturelle Maßnahmen
  - Organisatorische Maßnahmen
  - Personelle Maßnahmen
  - Maßnahmen im Bereich Hard- und Software
  - Maßnahmen im Kommunikationbereich
  - Notfallvorsorgemaßnahmen

BSI IT-Grundschutzhandbuch

- Beispiel:
- Gefährung G 4.1 Ausfall der Stromversorgung
  - G = Gefährung
  - 4 = Technische
  - .1 = erste technische Gefährdung
- /home/mirror/ccc2004/vortrag_itsecstandards/standardsitsec/bsi/deutsch/g/g4000.htm

Common Criteria

- technisch abstrakt und damit
- flexibel und technologieunabhängig
- Internationaler Standard, der Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit in der Informationstechnik beschreibt
- international, Weiterentw. von ITSEC, Orange Book
- nicht: Orga und Recht
- für verschiedenen Schutzbedarf
- für Spezifikation von IT-Sicherheitsanforderungen
  - als Teilmenge der Kriterien
  - Was soll geschützt werden?
    - **Security Target / Protection Profile**

Common Criteria

- für Spezifikation von IT-Sicherheitsanforderungen
  - als Teilmenge der Kriterien
  - Was soll geschützt werden?
    - **Security Target**
      - = implementierungsabhänge Menge von Sicherheitsanforderungen (Hersteller)
    - **Protection Profile**
      - = implementierungs**un**abhänge Menge von Sicherheitsanforderungen (Anwender)
      - für eine Kategorie von TOE
- Untersuchungsgegenstand = Target of Evaluation =**TOE**

Common Criteria

- besteht aus drei Teilen:
  - 1.Teil: Einführung und Begriffe
  - 2.Teil: 11 funktionale Klassen
  - 3.Teil: Klassen der Vertrauenswürdigkeit
- http://www.commoncriteria.de/it-sicherheit_deutsch/ccinfo.htm

Common Criteria - 2.Teil

- 11 funktionale Klassen mit Abhängigkeiten:
  - Identifikation und ***Authentisierung*** FIA
  - ***Nicht-Abstreitbarkeit*** FCO
  - ***Privatheit*** FPR
  - Kryptographische Unterstützung FCS
  - Schutz der Benutzerdaten FDP : ***Integrität***
  - Betriebsmittelnutzung FRU: ***und Verfügbarkeit***
  - Kontrolle Benutzersitzung FTA
  - Trusted Path FTP
  - Schutz der Toe-Sicherheitsfunktionen FPT
  - Sicherheitsmanagement FMT
  - Sicherheitsprotokollierung FAU

Common Criteria - 2.Teil- Beispiel

- Funktionale Klasse Audit (FAU)
  - deren Familie Generierung von Protokolldaten (FAU_GEN)
  - **„FAU_GEN1: Generierung von Protokolldaten**
  - **FAU_GEN1.1:**
  - Die TSF müssen in der Lage sein, für folgende protokollierbaren Ereignisse eine Protokollaufzeichnung zu generieren:
    - a) Starten und Beenden der Protokollierungsfunktionen;
    - b) Alle protokollierbaren Ereignisse für den Protokollierungsgrad [Auswahl: Minimal, Einfach, Detailliert, nicht angegeben]; und
    - c) [Zuweisung: sonstige speziell festgelegte protokollierbare Ereignisse].“
    - Abhängigkeit: Zeitstempel (FPT_STM.1)
- To Do: auf konkrete Situation anpassen

Common Criteria - 3.Teil

- **Vertrauen wird erreicht durch:**
  - Analyse und Überprüfung von Prozessen
  - **Überprüfung** der Anwendung von Prozessen
  - Überprüfung Design – Umsetzung
  - Überprüfung Design – Anforderungen
  - Analyse der Dokumentationen
  - Funktionale **Tests**
  - Schwachstellentest (Pentests)
  - ..

Common Criteria - 3.Teil

- **Vertrauenswürdigkeitsklassen** (Vergleiche funktionale Klassen)**:**
  - Configuration Management (ACM)
  - Delivery and Operation (ADO)
  - Development Documentation (ADV)
  - Guidance Documents (AGD)
  - Life-Cycle Support (ALC)
  - Testing (ATE)
  - Vulnerability Assessment (AVA
  - Maintenance of Assurance (AMA)

Common Criteria - 3.Teil

- Es gibt 7 **Evaluation Assurance Level (EAL):**
  - EAL 1: functionally tested
  - EAL 2: structurally tested
  - EAL 3: methodically tested and checked
  - EAL 4: methodically designed, tested and reviewed
  - EAL 5: semiformally designed and tested
  - EAL 6: semiformally verified design and tested
  - EAL 7: formally verified design and tested

Common Criteria - 3.Teil

- Vertrauenswürdigkeitsklassen und EAL:
- /home/mirror/ccc2004/vortrag_itsecstandards/standardsitsec/cc/ccpart3v2-1.2.pdf
  - Seite 54
- Beispiel: EAL 1 muss ACM_CAP.1 erfüllen (S.65)
  - ACM = Klasse Configuration Management
  - CAP = Familie (in der Klasse ACM) Configuration management capabilitites
  - .1 heißt: eindeutige Versionsnummer (S.69)
- zum Vergleich für EAL 3 muss ACM_CAP.3 erfüllt sein (S.45):
  - ACM_CAP.3 = Authorisation Controls (S.70)
  - = eindeutige Versionsnummer
  - CM system, CM doku, configuration list, eindeutige Bezeichnung aller configuration items, etc.
  - kein unauthorisierter Zugriff (Integrität)

Best practise: ITIL

- best practise für Administration:
- **„Es soll laufen!“- Verfügbarkeit**
- Einrichtung und Betrieb von IT-Service Management aus Dienstleistersicht: extern oder interne IT-Abteilung
- Ziel: hohe Qualität IT-Service und Kosteneffizienz
- ITIL = IT Infrastructure Libary: Hardware, Software, Prozesse, Kommunikation, Dokumentation
- ITIL Bücher, Training, Zertifizierung, Tools
- Was, nicht wie, d.h. keine technischen Details
- für Service Level Agreements (SLA's) und OLA (Organisation Level Agreements (innerhalb einer Firma)
- www.itil.org

ITIL: Beispiel

- Problem die auftreten können,
- zum Beispiel: bei 1.,2.,3. Level Support:
- Kunde: „Aber ich kenn' doch den Menschen vom 3.Level Support, und wenn ich den gleich anrufe, geht das viel schneller.“
- ITIL = Erfahrungen

ITIL: Sets und Bücher

- ITIL besteht aus Bänden (sets) mit je einem oder mehreren Büchern:
  - IT Service Provision und IT Infrastructure Management Sets
    - Buch: „Service Support“
    - Buch: „Service Delivery“
  - Managers Set: Orga, Quality, **Security Mgmt**
  - Software Support Set: Sw Lifecycle Support
  - Computer Operations Set: Installation & Acceptance
  - Environmental Set: u.a Strom, Brandschutz
  - Business Perspective Set = f(Unternehmensziele)

ITIL: Service Support

- ITIL Buch: „Service Support“
  - **Incident Management**
    - Service Desk: Nutzer, IT-Dienstleister
  - **Problem Management**
    - für schwerwiegende allg. Fälle > Change Mangement
  - **Configuration Management**
    - Configuration Items (CI) {Appl., Hw, Doku, Prozess}
    - CI's mit Abhängigkeiten in Configuration Management Database (CMDB) zusammengefaßt
  - **Change Mangement**
    - aus „Request for Change“
    - Änderungen testen und in CMDB speichern
  - **Release Management**
    - Versionierung und Verteilung von Sw (Lizenzen, Roll-out, Rückgängigmachen)

ITIL: Service Delivery

- ITIL Buch: „Service Delivery“
  - **Service Level Management**
    - in SLA Sicherheitsanforderungen -> Operation Level Agreements (Unterauftragnehmer)
  - **Availability Management**
    - Verfügbarkeit als Sicherheitsziel
  - **Business Continuity Management**
    - Notfallplanung
  - **Capacity Management**
    - Optimierung von IT Ressourcen
  - **Financial Management**
    - Kosten, Rechnung, mehr als Grundschutz?

ITIL: Managers Set: SecMgmt

- ITIL besteht aus Bänden (sets) mit je einem oder mehreren Büchern:
  - **Managers Set**: Orga, Quality, Security Mgmt
    - ITIL Security Management:
      - aus IT-Dienstleistersicht: -> SLA
      - SLA-> Sicherheitsanforderungen
        - -> PLANung von Sicherheitsmaßnahmen
        - -> IMPLEMENT
        - -> EVALUATE durch Audits
        - -> MAINTAIN -Verbesserungen
        - REPORT von Dienstleister an Kunde
        - CONTROL zur Steuerung der Phasen
      - wie BSI GSHB nur Grundschutz
      - **an BS 7799 angelehnt**

BS 7799

- **Information security management system** (ISMS) – Specification with guidance for use
- **Teil 1**: Sicherheitsmaßnahmen = ISO 17799 „Code of practise for security management“ (= best practise“)
- **Teil 2**: für die Beurteilung eines ISMS -> Zertifizierung
- nur Orga

BS 7799-1 = ISO 17799

- **BS 7799 Teil 1: Sicherheitsmaßnahmen** = ISO 17799 „Code of practise for security management“
  - Sicherheitspolitik an Unternehmenszielen orientieren
  - an Unternehmenskultur anpassen (Akzeptanz)
  - Unterstützung durch das Top-Management
  - Sicherheitsanforderung, Risk Management
  - Review-Cycle: Messung, Kontrolle und Verbesserung von IT-Sicherheitsmaßnahmen

BS 7799-1 = ISO 17799

- 10 Gebiete -1.Teil:
  - **Security Policy**:
    - Rückendeckung vom Mgmt
  - **Organizational Security**:
    - Initiierung, Implementierung und Kontrolle von S.maßn.
  - **Asset Classification and Control**:
    - was schützen? - Inventarisierung
  - **Personel Security**:
    - Awareness, Schulung
  - **Physical and Environmental Security**:
    - Sicherheitszonen, Gebäudeschutz
  - **Communication and Operations Management**:
    - Integrität und Verfügbarkeit von IT-Systemen & Infos

BS 7799-1 = ISO 17799

- 10 Gebiete -2.Teil:
  - **Access Control**:
    - Zugangs- und Zutrittsberechtigung
    - Protokollierung
  - **System Development and Maintenance**:
    - Sicherheitsanforderungen bereits bei Systementwicklung beachten
    - Kryptographie für Vertraulichkeit und Authentizität
  - **Business Continuity Management**:
    - Verfügbarkeit
    - vor allem für kritische Geschäftsprozesse
  - **Compliance**:
    - Einhaltung gesetzlicher Verpflichtungen
    - Einhaltung unternehmenseigener Regelungen

BS 7799-2

- Inhalt BS 7799-2:
- beschreibt Implementierung, Überwachung, Prüfung, Instandhaltung und Verbesserung eines ISMS
- **Ziel: dokumentiertes ISMS**
- 4 Aspekte:
  - Information security management system
  - Management responsibility
  - Management review of the ISMS
  - ISMS improvement

BS 7799-2

- Inhalt BS 7799-2:
- beschreibt Implementierung, Überwachung, Prüfung, Instandhaltung und Verbesserung eines ISMS
- neben den 4 Aspekten:
  - Annex B: Guidance of use of the standard
    - **Plan-Do-Check-Act (PDCA)**
    - **vgl ITIL: Plan-Implement-Evaluate-Maintain**
  - Plan including risk treatment
  - Do incl. resources, trainung and awareness
  - Check incl. learning from others and trend analysis

andere Ansätze

- Cobit: Control objectives for information and relates technology
- ISO/IEC TC 68 „Banking and other financial services“
- Technical Report (TR) 13569 „Information security Guidelines“

Zusammenfassung

- **BSI GSHB**:
  - Orga+Technik
  - detailliert
  - ohne Risikoabschätzung (nur Grundschutz)
- **Common Criteria**:
  - technisch, keine Orga
  - abstrakt und allgemein
  - Risikoabschätzung ->mit verschiedenen Schutzbedarf
- **ITIL**:
  - de-facto-Standard für Betrieb von IT- Infrastructur
  - Technik (was, nicht wie) + Orga
  - ohne Risikoabschätzung
- **BS 7799-2**:
  - nur Orga

Weitere Infos:

- BSI: http://www.bsi.de/literat/index.htm
- Studie zu ISO-Normungsaktivitäten ISO/BPM: http://www.bsi.bund.de/literat/studien/gshb/ISO-BPM-Zertifizierung
- BSI Grundschutzhandbuch: http://www.bsi.bund.de/gshb/deutsch/index.htm
- Common Criteria:http://www.bsi.de/cc/index.htm
- ITIL: www.itil.org
- BS 7799: http://www.secorvo.de/whitepapers/secorvo-wp10.pdf

Fazit

- **IT-Sicherheitsstandards sind Nachschlagewerke**
  - **-> Das Rad nicht neu erfinden!**
- nicht jedes passt für alles:
  - -->überlegen, was bezweckt werden soll!
- **pro**: Standards sind „eingedampfte“ Erfahrungen, wiederverwendbar, allgemein anerkannt
- **kontra**: viele Standards sind komplexe Werke mit langer Einarbeitungszeit; setzen breites und tiefes IT-Wissen voraus