Informationssicherheit:

Sicherheitskriterien, Informationssicherheits-management

Motivation: Sicherheitskriterien

- Viele IT-Produkte müssen bestimmte Sicherheitsziele erfüllen:
  - Betriebssysteme, Anwendungen, Datenbanken, Chipkarten, ...
- **Zentrale Frage:** Wie kann man die „Sicherheit“ solcher Produkte bewerten/evaluieren?
- Allgemeine Anerkennung der Evaluationsergebnisse
- Möglichkeit des Vergleichs von IT-Produkten mit ähnlicher Funktionalität
- Einführung einer Evaluationsmethodik

Kriterienkataloge

- TCSEC (Trusted Computer Evaluation Criteria, 1980)
- ITSEC (Information Technology Security Evaluation Criteria, Europa, 1991)
- CTCPEC (Canadian Trusted Computer Product Evaluation Criteria, 1993)
- CC (Common Criteria, 1996; V3.1 aus 2006; CC:2022, Nov. 22)

Trusted Computer Evaluation Criteria – TCSEC

- US National Computer Security Center (Teil der NSA), 1980
- Auch „Orange Book“ genannt
- Älteste Kriterien zur Bewertung der Sicherheit von IT-Produkten
- Sieben Hierarchiestufen zur Sicherheitsstufen zur Klassifikation eines IT-Systems
  - Vier Hauptstufen A bis D
  - Fünf Unterstufen (C1, C2, B1, B2, B3)
  - Niedrigste Stufe ist D

Die Hierarchiestufen von TCSEC (1)

- Stufe D: Minimaler Schutz
  (Im Grunde gar keine Aussage über Schutz)
- Stufe C1: Benutzerbestimmbare Zugriffskontrolle (DAC) für Gruppen:
  - Benutzer können Rechte nur grobgranular an Gruppen vergeben
  - Beispiel: gängige Unix-Systeme
- Stufe C2: Benutzerbestimmbare Zugriffskontrolle (DAC) für einzelne Benutzer und Audit
  - Benutzer können Rechte auch an einzelne Benutzer vergeben
  - Mitprotokollieren der Aktionen einzelner Nutzer
  - Schutz der Audit- und Authentisierungsinformationen
  - Beispiel: Windows NT (ohne Netzanbindung!), RACF-OS von IBM, div. speziell für C2 umgerüstete Unix-Varianten

Die Hierarchiestufen von TCSEC (2)

- Stufe B1: Systembasierte Zugriffskontrolle (MAC)
  - Wie C2, aber zusätzlich Einführung von Sicherheitsmarkierungen (vgl. Bell-LaPadula)
- Stufe B2: Strukturierter Schutz
  - Wie B1, u.a. zusätzlich
    - Formales Sicherheitsmodell (***security model***)
    - Die Trusted Computing Base (TCB) muss strukturiert sein:

      Trusted Computing Base = die Komponenten eines IT-Systems, die korrekt arbeiten müssen, damit die Security Policy nicht verletzt wird
    - Analyse von verdeckten Kanälen
    - Strikte Tests müssen durchgeführt werden

Die Hierarchiestufen von TCSEC (3)

- Stufe B3: Security Domains
  - Wie B2, aber TCB muss minimal, ausführlich getestet und gegen unbefugte Zugriffe geschützt sein
    - Vgl. Principle of Economics of Mechanism
  - Echtzeit-Monitoring und Mechanismen zur Benachrichtigung

- Stufe A: Verifiziertes Design
  - Keine funktionalen Erweiterungen von B3, aber es wird ein formaler Nachweis gefordert, dass die TCB-Spezifikation und das zugrunde liegende Sicherheitsmodell äquivalent sind
  - Beispiel: MLS LAN Version 2.1 der Firma Boeing

Bewertung: TCSEC

- Nur auf Betriebssysteme beschränkt
- Betonung von Bell-LaPadula-Policies, Vernachlässigung anderer Schutzziele wie der Integrität und der Verfügbarkeit
- Nur auf USA beschränkt
- Keine Trennung von Sicherheitsfunktionalität und der Qualität, mit der die Sicherheitsfunktionen erbracht werden

ITSEC

- Europäische Kriterien (Großbritannien, Frankreich, Deutschland, Niederlande), 1991
- Einführung von Funktionalitätsklassen F
  - Teilweise Orientierung an den Stufen des Orange Books (F-C1, F-B1, ...)
  - Einführung weiterer Funktionsklassen: bspw. F-IN besondere Anforderungen an die Integrität
- Sieben verschiedene Evaluationsstufen E0, ..., E6 (Qualitätsstufen)
  - E0: Einstiegsstufe,
  - E6: formale Spezifikation der Sicherheitsanforderungen
- Weitere Neuerung: Der Produkthersteller muss die Kosten für Zertifizierung übernehmen
- Gegenseitige Anerkennung der Zertifizierungsergebnisse in europäischen Staaten, bis auf Stufe E6

Die Common Criteria

- Common Criteria V1.0, 1996
- Aktuelle Version:
  Common Criteria CC:2022 R1, November 2022:
  http://www.commoncriteriaportal.org/
- Zusammenführung von CTCPEC, TCSEC und ITSEC
- Im Wesentlichen Orientierung an ITSEC
- Weltweit einheitlicher Kriterienkatalog
  - u.a. unter Beteiligung von Deutschland, Frankreich, Großbritannien, Kanada, den Niederlanden und den USA
- Internationaler Standard: ISO/IEC 15408
- Ziel: Evaluation von sicherheitsrelevanten Produkten
  - EVG – Evaluationsgegenstand (***target of evaluation***, TOE) :
    ein IT-Produkt oder -System, das Gegenstand einer Prüfung ist

Zusammenhang mit ITSEC

- Weiterentwicklung von ITSEC
- Trennung von Sicherheitsfunktionalität und Qualitätskriterien
- CC-Evaluierung wird von national akkreditierten Prüfstellen (***commercial licensed evaluation facility, CLEF***) durchgeführt
  - derzeit 7 Prüfstellen in Deutschland (z.B. T-Systems International GmbH
  - TÜV Informationstechnik GmbH, DFKI); im Jahr 2013 noch 15
  - Prüfstellen werden in Deutschland vom BSI lizenziert
  - Akkreditierung in den USA von der NSA und dem NIST
- Die Kosten der Zertifizierung werden wie bei ITSEC vom Produkthersteller übernommen!

Struktur der CC-Dokumente

- Drei Teile:
  - Teil 1: Einführung in die CC und allgemeines Modell
    - Glossar, Grundlagen der Evaluation, Schutzprofile, Sicherheitsvorgaben
    - Verständliche Einführung; diese Folien beruhen auf diesem Material
  - Teil 2: Funktionale Sicherheitsanforderungen
    - Kataloge von Empfehlungen für Sicherheitsanforderungen
  - Teil 3: Anforderungen an die Vertrauenswürdigkeit (***assurance***)

- Sowie: CEM – Evaluations-Methodologie (ISO/IEC 18045, V 3.1)

Funktionale Sicherheitsanforderungen (1)

Definiert in Teil 2 der CC:

- Sicherheitsprotokollierung (FAU)
- Kommunikation (FCO)
- Kryptographische Unterstützung (FCS)
- Schutz der Benutzerdaten (FDP)
- Identifikation und Authentisierung (FIA)
- Sicherheitsmanagement (FMT)
- Privatheit (FPR)
- Schutz der EVG-Sicherheitsfunktionen (FPT)
- Betriebsmittelnutzung (FRU)
- EVG-Zugriff (FTA)
- Vertrauenswürdiger Pfad/Kanal (FTP)

Funktionale Sicherheitsanforderungen (2)

Funktionale Sicherheitsanforderungen an einen Evaluationsgegenstand (Auszug)

- Klasse FCS – Kryptographische Unterstützung
  - FCS_COP.1 Kyptographischer Betrieb („Hashen“)
    FCS_COP.1.1 ... müssen Hashfunktion gemäß SHA256 durchführen...
  - FCS_COP.2 Kyptographischer Betrieb („Verifizieren“)
    FCS_COP.2.1 ... müssen Verifikationsalgorithmus gemäß RSA (3072 Bit) durchführen...
  - FCS_CKM.1 Schlüsselerzeugung
    FCS_CKM.1.1 … müssen die Schlüssel für das Verfahren RSA mit der Größe [3072 Bit] gemäß Standard PKCS #1 erzeugen

Vertrauenswürdigkeits-anforderungen

Definiert in Teil 3 der CC:

- Konfigurationsmanagement (ACM)
- Auslieferung und Betrieb (ADO)
- Entwicklung (ADV)
- Handbücher (AGD)
- Lebenszyklus-Unterstützung (ALC)
- Testen (ATE)
- Schwachstellenbewertung (AVA)
- Erhaltung der Vertrauenswürdigkeit (AMA)

- Prüfung und Bewertung des Schutzprofils (APE)
- Prüfung und Bewertung der Sicherheitsvorgabe (ASE)

Beispiele für Vertrauenswürdigkeitsanforderungen

- Entnommen aus Teil 3, CC

ATE_DPT.3 Testing: modular design

Developer action elements:

ATE_DPT.3.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements:

ATE_DPT.3.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and modules in the TOE design.

ATE_DPT.3.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.3.3C The analysis of the depth of testing shall demonstrate that **all TSF** modules in the TOE design have been tested.

Vertrauenswürdigkeitsstufen (1)

- Vertrauenswürdigkeitsstufe (***Evaluation Assurance Level***, EAL), Bewertungsskala
  - EAL1: funktionell getestet
  - EAL2: strukturell getestet
  - EAL3: methodisch getestet und überprüft
  - EAL4: methodisch entwickelt, getestet und durchgesehen
  - EAL5: semiformal entworfen und getestet
  - EAL6: semiformal verifizierter Entwurf und getestet
  - EAL7: formal verifizierter Entwurf und getestet

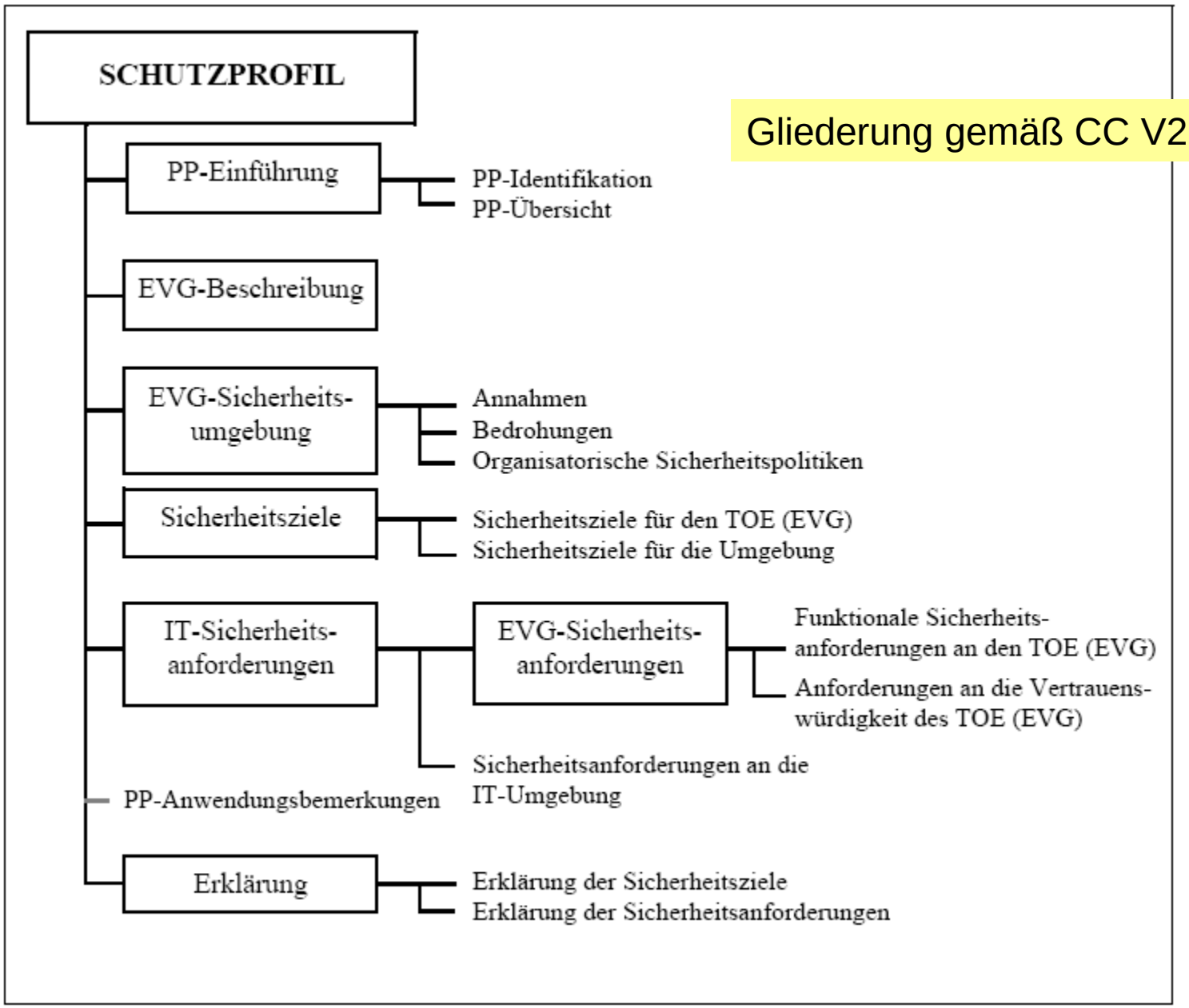
Vertrauenswürdigkeitsstufen (2)

- EALs sind Sammlungen von „Vertrauenswürdigkeitsanforderungen“ aus Teil 3 der CC
- EALs entsprechen im Wesentlichen den Evaluationsstufen von ITSEC:
  - EAL2 entspricht E1, ..., EAL 7 entspricht E6
  - Kein Pendant zu E0
  - EAL1 wurde neu eingeführt.

Schutzprofil

- Ein Schutzprofil (***protection profile***) enthält die Sicherheitsanforderungen für eine Klasse von Produkten
- Darstellung in einer implementierungsunabhängigen Form
- Beispiele:
  - Firewalls (Paketfilter/Application Gateways)
  - Rollenbasierte Zugriffskontrolle
  - Krankenhausinformationssysteme
  - Chipkarten, elektronische Ausweise
  - Heilberufsausweis für Ärzte (s. Beispielausdruck)
  - Weitere Profile siehe http://www.commoncriteriaportal.org/pps/index.cfm

Gliederung gemäß CC V2.1



Bestandteile eines Schutzprofils

1. Bedrohungen (***threats***)

   Beispiel: T.ArchivierungWahlgeheimnis

   Eine Person, die nach der Phase „Wahldurchführung inkl. der Stimmauszählung“ Zugriff auf die im EVG gespeicherten Daten hat und ggf. Zusatzdaten wie beispielsweise Entschlüsselungskeys kennt, kann an Hand der im EVG gespeicherten Daten eine Zuordnung zwischen dem Wähler und seiner Stimme (im Klartext oder in verschlüsselter Form) herstellen.

2. Sicherheitsziele (***security objectives***)

   Beispiel: O.ArchivierungWahlgeheimnis

   Die nach Feststellung des Wahlergebnisses noch auf dem Wahlserver gespeicherten Daten lassen keine Zuordnung zwischen dem Wähler und seiner Stimme (im Klartext oder in verschlüsselter Form) zu. Eine Zuordnung darf insbesondere nicht über die Reihenfolge und/oder den Zeitpunkt der Speicherung der Stimmdatensätze in der Urne geschehen.

3. Sammlung von Sicherheitsanforderungen (die, wenn möglich, schon in den CC-Dokumenten vordefiniert sein sollen)
4. Erklärungen (***rationale***), die u.a. nachweisen, dass die Sicherheitsziele und Bedrohungen sowie die Sicherheitsanforderungen einander entsprechen
5. Optional eine EAL (fast immer!)

Erklärungen – Rationale (1)

- Sicherheitsziele müssen die Bedrohungen abdecken
- Tabelle: Sicherheitsziele versus Bedrohungen

	T.UnbefugterWähler	T.Beweis	T.IntegritätNachricht	T.GeheimNachricht	T. AuthentizitätServer	T.ArchivierungIntegrität	T.ArchivierungWahlgeheimnis
O.StimmberechtigterWähler	X						
O.Beweis		X					
O.IntegritätNachricht			X				
O.Wahlgeheimnis				X			
O.GeheimNachricht				X			
O.AuthentizitätServer			X	X	X		
O.ArchivierungIntegrität						X	
O.ArchivierungWahlgeheimnis							X

Erklärungen – Rationale (2)

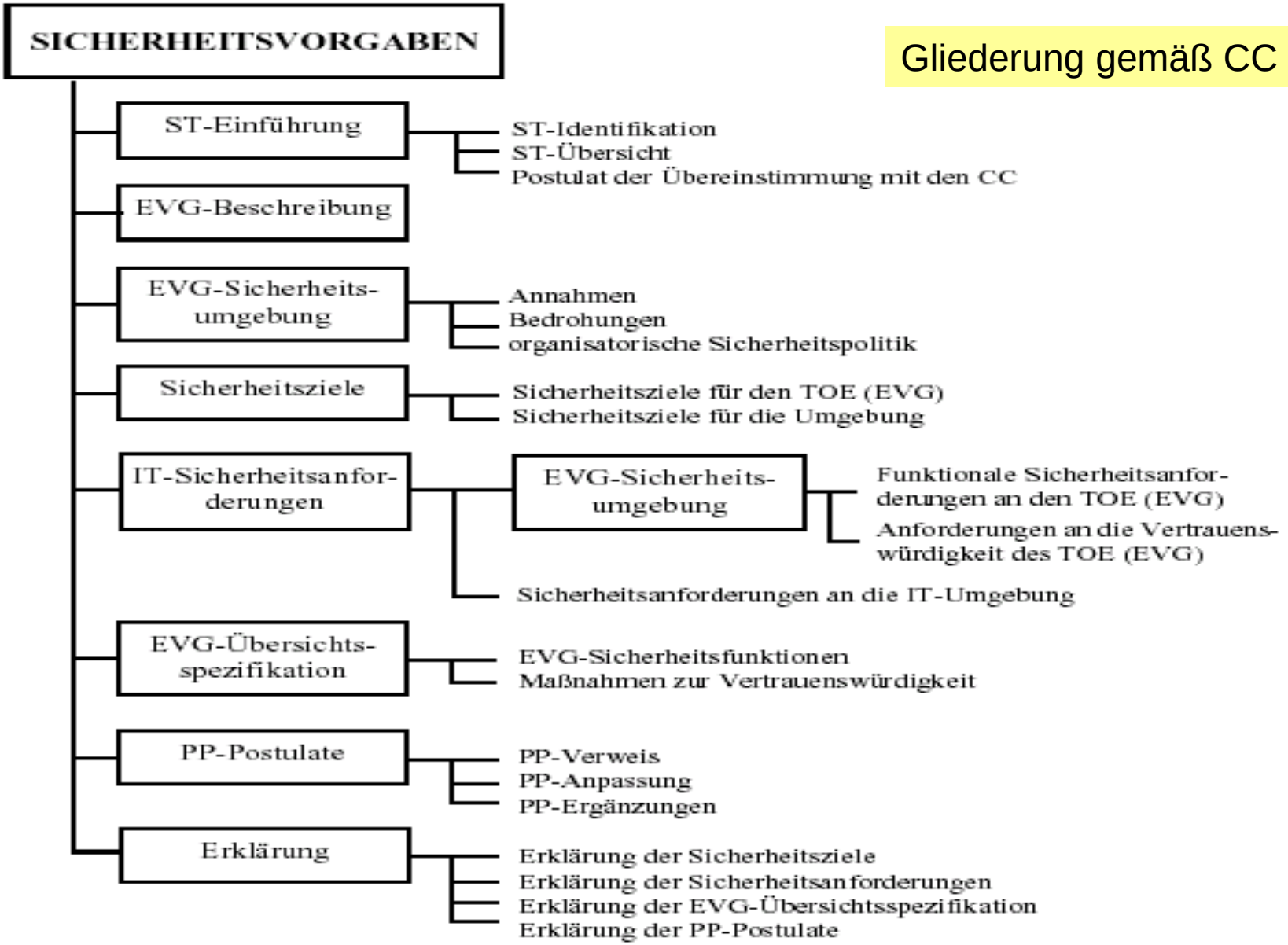
- Erklärung, dass die Sicherheitsziele und die Sicherheitsanforderungen einander entsprechen

O.ArchivierungWahlgeheimnis Die Komponente **FPR_ANO.1** stellt sicher, daß nach Wahlende eine Zuordnung zwischen Wähler und seiner Stimme nicht mehr möglich ist. Durch die Verwendung der Komponente **FPR_UNL.1B** wird darüber hinaus sichergestellt, daß über die Reihenfolge und/oder den Zeitpunkt der Speicherung der Stimme in der Urne keine Zuordnung zwischen Wähler und Stimme möglich ist. Beides wird durch die Komponente **FDP_RIP.1A** unterstützt, die gewährleistet, daß keine zwischengespeicherten Stimmzettel erhalten bleiben, die das Wahlgeheimnis gefährden könnten.

Sicherheitsvorgaben

- Sicherheitsvorgabe (***security target***): eine Menge von Sicherheitsanforderungen und Sicherheitsspezifikationen, die als Grundlage für die Prüfung und Bewertung eines angegebenen Evaluationsgegenstands dienen
- Eine Sicherheitsvorgabe kann eine Verfeinerung (Erweiterung) eines Schutzprofils sein.
  - Es gibt aber auch Sicherheitsvorgaben, die nicht auf einem Schutzprofil beruhen
- Implementierungs- und herstellerabhängig
- Für jeden EVG muss eine Sicherheitsvorgabe existieren
  - Gegen diese Sicherheitsvorgabe wird evaluiert

Gliederung gemäß CC V2.1



Vorgehensweise zur Evaluation

- Standardvorgehensweise
  1. Schutzprofil erstellen (falls ein solches noch nicht existiert)
  2. Schutzprofil auf Vollständigkeit, Konsistenz und Korrektheit hin evaluieren
  3. Sicherheitsvorgabe erstellen
  4. Ggf. überprüfen, dass die Sicherheitsvorgabe eine korrekte Verfeinerung eines Schutzprofils ist
  5. Evaluationsgegenstand (EVG) gegen die Sicherheitsvorgabe evaluieren

Zertifizierte Produkte

- Liste mit zertifizierten Produkten:
  https://www.commoncriteriaportal.org/products/index.cfm
- Z.B.: MICARDO V4.0 R1.0 eHC v1.2 von Morpho Cards GmbH (evaluiert von SRC Security Research & Consulting GmbH)
- Es gibt zertifizierte Produkte mit der Evaluationsstufe EAL 5+, z.B.:
  - Infineon Smart Card IC (Security Controller) SLE66CX322P with RSA 2048/m1484 a24/ m1484a27 and m1484b14
  - GemXplore Xpresso V3 Java Card Platform Embedded Software V3 (Core)
- Weltweite Anerkennung nur bis EAL4, **in Europa bis EAL7**

Beispiel: Protection Profile for electronic Health Card (eHC)

https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/PP0020_V3b_pdf.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0861-2014

eHealth: Smart Cards

MICARDO V4.0 R1.0 eHC v1.2

from	Morpho Cards GmbH
PP Conformance:	Protection Profile for electronic Health Card (eHC) - elektronische Gesundheitskarte (eGK), Version 2.9, 19 April 2011, BSI-CC-PP-0020-V3-2010-MA-01
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 15 May 2014
For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

SOGIS Recognition Agreement

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

Abschließende Bemerkungen & Bewertung (1)

- Vorteile der CC:
  - Weltweit anerkannter Kriterienkatalog
  - Anwendbar auf verschiedene Klassen von IT-Produkten (nicht nur auf Betriebssysteme)
  - Viele IT-Produkte sind bereits zertifiziert worden (aber viele aktuelle Main-Stream-Produkte auch nicht)
  - Sicherheitsvorgabe/Schutzprofil nützliche Hilfsmittel zur Entwicklung eines sicheren Systems

  - Hersteller können Zertifikate als Wettbewerbsvorteil nutzen;
    z.B.: Ausschreibungen bzgl. Gesundheitskarten

Abschließende Bemerkungen & Bewertung (2)

- Probleme der CC:
  - CC enthalten keine Evaluationsmethodik (Wie wird von den Prüfstellen evaluiert?).
    - Aber: zusätzliche Einführung der Common Evaluation Methodology (CEM)
  - Aufwendiger und teurer Prozess, Rezertifizierung bei veränderter Version?
  - Keine Usability-Aspekte
  - Nicht jede Prüfstelle ist für jedes Produkt kompetent
  - Abhängigkeit der Prüfstellen von den (nationalen) Behörden: Es wird so zertifiziert, wie es offiziell gewünscht wird.
  - Teilweise werden bekannte Sicherheitsprobleme ignoriert:
    - Beispiel: Schutzprofil für Krankenhausinformationssysteme setzt voraus, dass alle internen Benutzer wirklich ehrlich sind!

Cyber Resilience Act (CRA)

- Verabschiedet von der EU im Oktober 2024 als verpflichtende Verordnung
- Ähnlich wie die CC adressiert der CRA auch die **Informationssicherheit von digitalen Produkten**, aber (hoffentlich) weniger aufwendig
- Auch Produkte, die digitale Komponenten enthalten, wie z.B. smartes Spielzeug, smarte Haushaltsgeräte
- Umfasst unterschiedliche Sicherheitsanforderungen wie z.B.: Security by Design, Security by Default, Vulnerability Management, Security Updates, Dokumentationen inkl. Software-Abhängigkeiten (SBoM – Software Bill of Material = Software-Stückliste)
- Mehr Informationen in einer Technischen Richtlinie des BSI:

  BSI TR-03183 Cyber-Resilienz-Anforderungen

Teil 2: Sicherheitsmanagement

Informationssicherheits-management

- Etablierung eines Sicherheitsprozesses in einer Organisation/Unternehmen
- Systematische Ermittlung und Umsetzung von Sicherheitsmaßnahmen
- Bewertung von Risiken:
  - Manche Risiken kann man tragen
- Auf Standards basierende Vorgehensweise für ein Sicherheitsmanagement gewünscht

BSI = British Standards Institute

BS 7799

- British Standard (BS) 7799
  - Ziel: Aufbau eines IT-Sicherheitsmanagements; Verankerung in der Organisation
  - Management-orientiert, nicht technisch
  - Keine detaillierten Umsetzungshinweise, sondern übergreifende Anforderungen
  - Zertifizierung gemäß BS 7799 – Teil 2 möglich (durch lizenzierte Auditoren)

- BS 7799 – Teil 1 ist Basis für ISO/IEC 17799
  - Best Practice-Verfahren und -Methoden,
  - Keine Empfehlung für konkrete Sicherheitslösungen
  - Keine Hilfestellung zur Bewertung existierender Sicherheitsmaßnahmen
  - Keine Zertifizierung nach BS 7799 Teil 1 (Soll-Maßnahmen, nicht verpflichtend)

Themenbereiche BS 7799

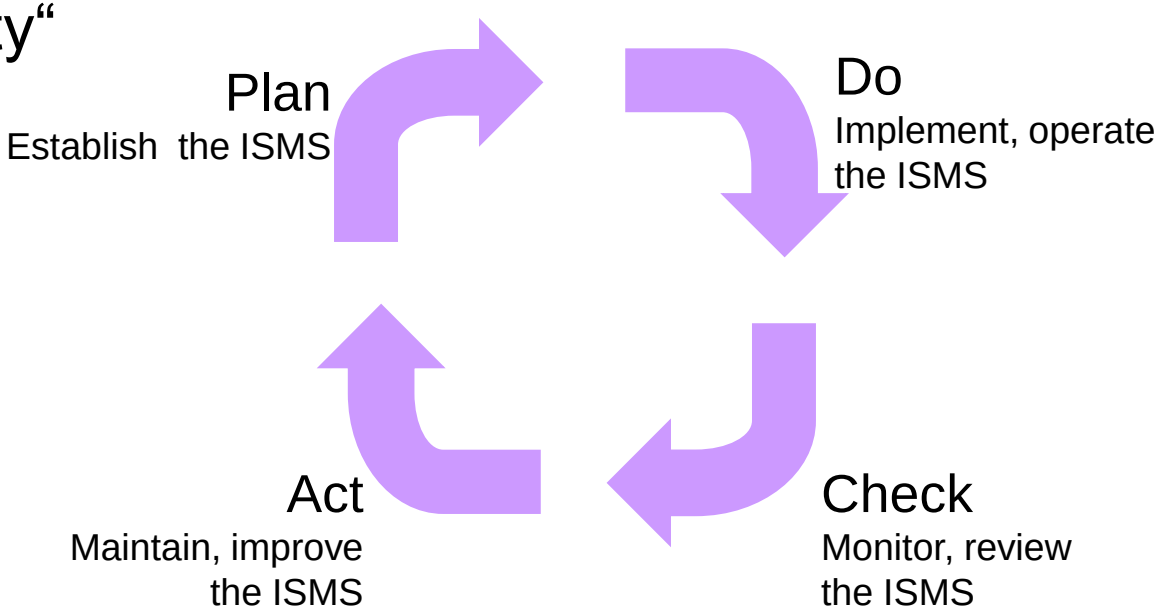
- Zehn Themenbereiche:
  1. Security policy — Provides management direction and support for information security
  2. Organisation of assets and resources — To help you manage information security within the organisation
  3. Asset classification and control — To help you identify your assets and appropriately protect them
  4. Personnel security — To reduce the risks of human error, theft, fraud or misuse of facilities
  5. Physical and environmental security — To prevent unauthorised access, damage and interference to business premises and information

Themenbereiche BS 7799

6. Communications and operations management — To ensure the correct and secure operation of information processing facilities
7. Access control — To control access to information
8. Systems development and maintenance — To ensure that security is built into information systems
9. Business continuity management — To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters
10. Compliance — To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and any security requirement

ISO 27001 / BS 7799 – Teil 2

- Information Security Management System (ISMS)
- „ISO 9000 für Security“
- Plan-Do-Check-Act (aus QM)
- Zertifizierbar (¥€$!)



Security Management nach BSI-Grundschutz

Bundesamt für Sicherheit in der Informationstechnik

- Ziel: Etablierung eines Informationssicherheitsmanagements (ISMS) in einer Organisation wie z.B. Unternehmen, Behörde (IT-Verbund)
- BSI – Bundesamt für Sicherheit in der Informationstechnik
- Grundschutzkompendium (früher: Grundschutzkataloge, Grundschutzhandbuch)
  - Webseite des BSI zum Thema „IT-Grundschutz“: www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
  - Online-Kurs IT-Grundschutz (Folien beruhen hierauf)
  - Grundschutzkataloge > 3000 Seiten!
  - Zusammengefasste Darstellung u.a. im Buch C. Eckert: „IT-Sicherheit“
- Toolunterstützung (früher GS-Tool; kommerzielle Tools: z.B. VIVA2, verinice, Save)

BSI-Grundschutzkompendium

- Sehr weit im Einsatz in Unternehmen mit niedrigem bzw. geringem Schutzbedarf
- Mehr als 50 Bausteine beschreiben verschiedene Aspekte der IT-Sicherheit (Server, PC, Firewall, E-Mail, WLAN, SAP, ...)
- Organisatorische, personelle, infrastrukturelle und technische Standardsicherheitsmaßnahmen
- Gefährdungs- und Maßnahmenkataloge

Schichtenmodell

- Gruppierung der Bausteine in Schichten
  1. Übergreifende Aspekte: IT-Sicherheitsmanagement, Organisation, Personal, …
  2. Infrastruktur: Gebäude, Verkabelung, Räume, …
  3. IT-Systeme: Windows Clients, Unix Clients, Unix Server, TK-Anlage…
  4. Netze: Heterogene Netze, Remote Access, Netzmanagement, Modem
  5. IT-Anwendungen: E-Mail, Webserver, Datenbanken, …

Beispiel für einen Baustein aus den Grundschutzkatalogen: B 3.203 Laptop

Beschreibung

Unter einem Laptop oder Notebook wird ein PC verstanden, der aufgrund seiner Bauart transportfreundlich ist und mobil genutzt werden kann. Ein Laptop hat eine kompaktere Bauform als Arbeitsplatzrechner und kann über Akkus zeitweise unabhängig von externer Stromversorgung betrieben werden. Er verfügt über eine Festplatte und meist auch über weitere Speichergeräte wie ein Disketten-, CD-ROM - oder DVD -Laufwerke sowie über Schnittstellen zur Kommunikation über verschiedene Medien (beispielsweise Modem, ISDN , LAN, USB, Firewire, WLAN). Laptops können mit allen üblichen Betriebssystemen wie Windows oder Linux betrieben werden. Daher ist zusätzlich der betriebssystemspezifische Client-Baustein zu betrachten. **(…)**

Die Einrichtungen zur Datenfernübertragung (über Modem, ISDN-Karte, etc.) werden hier nicht behandelt (siehe Baustein B 4.3). Für den Laptop wird vorausgesetzt, dass er innerhalb eines bestimmten Zeitraums nur von einem Benutzer gebraucht wird. Ein anschließender Benutzerwechsel wird berücksichtigt.

Gefährdungslage

Für den IT-Grundschutz eines Laptops werden folgende typische Gefährdungen angenommen:

Gefährdungslage für den Baustein (Auszug)

Höhere Gewalt

G 1.2 Ausfall von IT-Systemen

G 1.15 Beeinträchtigung durch wechselnde Einsatzumgebung

Organisatorische Mängel

G 2.7 Unerlaubte Ausübung von Rechten

G 2.8 Unkontrollierter Einsatz von Betriebsmitteln

G 2.16 Ungeordneter Benutzerwechsel bei tragbaren PCs

Menschliche Fehlhandlungen

G 3.2 Fahrlässige Zerstörung von Gerät oder Daten

G 3.3 Nichtbeachtung von Sicherheitsmaßnahmen

G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal

G 3.8 Fehlerhafte Nutzung von IT-Systemen

G 3.38 Konfigurations- und Bedienungsfehler

G 3.76 Fehler bei der Synchronisation mobiler Endgeräte

Technisches Versagen

G 4.9 Ausfall der internen Stromversorgung

G 4.13 Verlust gespeicherter Daten

G 4.22 Software-Schwachstellen oder -Fehler

G 4.52 Datenverlust bei mobilem Einsatz

Vorsätzliche Handlungen

G 5.1 Manipulation oder Zerstörung von Geräten oder Zubehör

Beispiel: Gefährdungslage

G 2.7 Unerlaubte Ausübung von Rechten

Rechte wie Zutritts-, Zugangs- und Zugriffsberechtigungen werden als organisatorische Maßnahmen eingesetzt, um Informationen, Geschäftsprozesse und IT -Systeme vor unbefugtem Zugriff zu schützen. Werden solche Rechte an die falsche Person vergeben oder wird ein Recht unautorisiert ausgeübt, kann sich eine Vielzahl von Gefahren für die Vertraulichkeit und Integrität von Daten oder die Verfügbarkeit von Rechnerleistung ergeben.

Beispiele

Der Arbeitsvorbereiter, der keine Zutrittsberechtigung zum Datenträgerarchiv besitzt, entnimmt in Abwesenheit des Archivverwalters Magnetbänder, um Sicherungskopien einspielen zu können. Durch die unkontrollierte Entnahme wird das Bestandsverzeichnis des Datenträgerarchivs nicht aktualisiert, die Bänder sind für diesen Zeitraum nicht auffindbar.

Ein Mitarbeiter ist erkrankt. Ein Zimmerkollege weiß aufgrund von Beobachtungen, wo dieser sein Passwort auf einem Merkzettel aufbewahrt und verschafft sich Zugang zum Rechner des anderen Mitarbeiters...

Maßnahmenempfehlungen für den Baustein (Auszug)

Planung und Konzeption		
M 2.36	(B)	Geregelte Übergabe und Rücknahme eines tragbaren PC
M 2.218	(C)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
M 2.309	(A)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
M 4.29	(Z)	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme
Beschaffung		
M 2.310	(Z)	Geeignete Auswahl von Laptops
Umsetzung		
M 5.91	(A)	Einsatz von Personal Firewalls für Clients
M 5.121	(B)	Sichere Kommunikation von unterwegs
M 5.122	(A)	Sicherer Anschluss von Laptops an lokale Netze
Betrieb		
M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
M 1.34	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
M 1.35	(Z)	Sammelaufbewahrung tragbarer IT-Systeme
M 1.46	(Z)	Einsatz von Diebstahl-Sicherungen
M 4.3	(A)	Einsatz von Viren-Schutzprogrammen
M 4.27	**(A)**	**Zugriffsschutz am Laptop**
M 4.28	(Z)	Software-Reinstallation bei Benutzerwechsel eines Laptops…

Beispiel einer Maßnahmenbeschreibung (Auszug)

M 4.27 Zugriffsschutz am Laptop

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT

Verantwortlich für Umsetzung: Benutzer

Jeder Laptop sollte mit einem Zugriffsschutz versehen werden, der verhindert, dass dieser unberechtigt benutzt werden kann. Bei Laptops sollte als Minimalschutz, wenn kein anderer Sicherheitsmechanismus vorhanden ist, der BIOS -Bootschutz aktiviert werden, wenn dessen Nutzung möglich ist. Erst nach Eingabe des korrekten Bootpasswortes wird der Rechner dann hochgefahren. Die im Umgang mit Passwörtern zu beachtenden Regeln sind in M 2.11 Regelung des Passwortgebrauchs aufgeführt worden.

Außerdem bieten nahezu alle Betriebssysteme die Möglichkeit, Anmeldepasswörter einzurichten und diese mit geeigneten Restriktionen zu versehen (z. B. Mindestlänge, Lebensdauer, etc.). Da diese Bordmittel nur eine begrenzte Sicherheit bieten, empfiehlt es sich bei Laptops, auf denen sich schnell große Mengen sensitiver Daten sammeln, zusätzliche Sicherheitshard- oder -software einzusetzen. Dazu gehören beispielsweise …

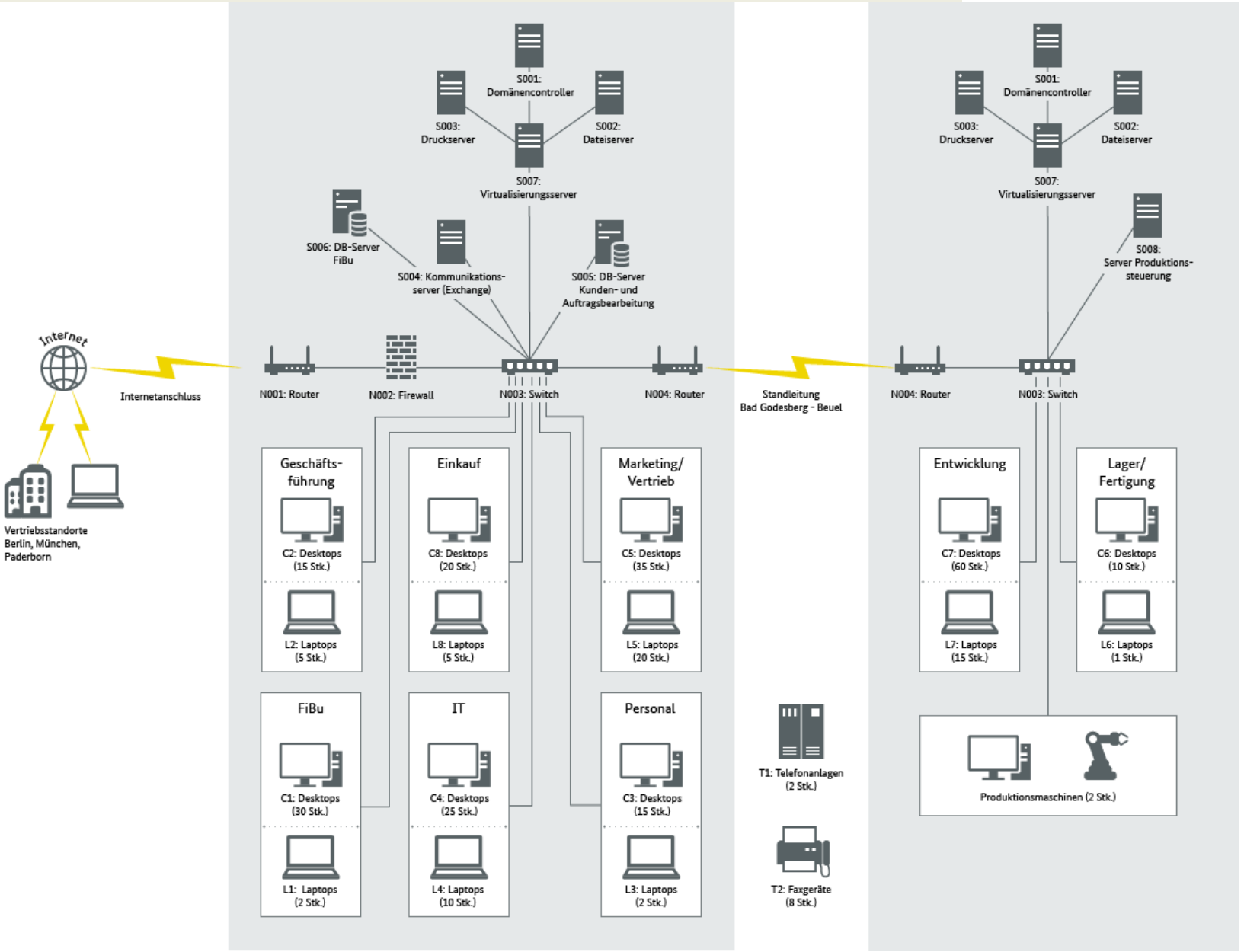
Vorgehensweise nach IT-Grundschutz

- Durchführung der folgende Schritte
  1. Infrastrukturanalyse
  2. Schutzbedarfsfeststellung
  3. Modellierung der Maßnahmen
  4. Basis-Sicherheitscheck
  5. Ergänzende Risikoanalyse (falls erforderlich)
  6. (Planung der) Realisierung

- Wiederholung der Schritte in regelmäßigen Abständen: Prozess; kompatibel zu ISO 27001?

Infrastrukturanalyse

- Festlegung des IT-Verbundes (z.B. Unternehmen, Abteilung)
- Erstellung von (vereinfachten) Netzplänen des IT-Verbundes
- Aufnahme der Anwendungen, IT-Systeme (Clients, Server, Netzkomponenten, TK-Anlagen, …)


Internet
Internetanschluss
Vertriebsstandorte
Berlin, München,
Paderborn
N001: Router
N002: Firewall
N003: Switch
N004: Router
S001:
Domänencontroller
S002:
Dateiserver
S003:
Druckserver
S004: Kommunikations-
server (Exchange)
S005: DB-Server
Kunden- und
Auftragsbearbeitung
S006: DB-Server
FiBu
S007:
Virtualisierungsserver
Standleitung
Bad Godesberg - Beuel
N004: Router
N003: Switch
S001:
Domänencontroller
S002:
Dateiserver
S003:
Druckserver
S007:
Virtualisierungsserver
S008:
Server Produktions-
steuerung
Geschäfts-
führung
C2: Desktops
(15 Stk.)
L2: Laptops
(5 Stk.)
Einkauf
C8: Desktops
(20 Stk.)
L8: Laptops
(5 Stk.)
Marketing/
Vertrieb
C5: Desktops
(35 Stk.)
L5: Laptops
(20 Stk.)
FiBu
C1: Desktops
(30 Stk.)
L1: Laptops
(2 Stk.)
IT
C4: Desktops
(25 Stk.)
L4: Laptops
(10 Stk.)
Personal
C3: Desktops
(15 Stk.)
L3: Laptops
(2 Stk.)
T1: Telefonanlagen
(2 Stk.)
T2: Faxgeräte
(8 Stk.)
Entwicklung
C7: Desktops
(60 Stk.)
L7: Laptops
(15 Stk.)
Lager/
Fertigung
C6: Desktops
(10 Stk.)
L6: Laptops
(1 Stk.)
Produktionsmaschinen (2 Stk.)

Schutzbedarfsfeststellung (1)

Schutzbedarfskategorien	
Niedrig - mittel	die Schadensauswirkungen sind begrenzt und überschaubar
Hoch	die Schadensauswirkungen können beträchtlich sein
Sehr hoch	die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen

Schutzbedarfsfeststellung (2)

- Einordnung der Anwendungen, IT-Systeme und Räume gemäß den Schutzbedarfskategorien
- Und zwar für die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit
- Einordnung mit Hilfe von Mitarbeitern des zu zertifizierenden Unternehmens

Modellierung nach IT-Grundschutz

- Auswahl der geeigneten Bausteine der Grundschutzkataloge auf Basis der Ergebnisse der IT-Infrastrukturanalyse und der Schutzbedarfsfeststellung
- Wie bekommt man die geeigneten Bausteine? Intellektuelle Leistung?
- Unterstützung durch Werkzeuge (keine neue Version des GS-Tools mehr!)
  - *Ergebnisse sollte man s*chon noch überprüfen

Basis-Sicherheitscheck

- Idee: Vergleiche die bereits umgesetzten Maßnahmen mit denen, welche die Modellierung ergeben hat
- Soll-Ist-Vergleich
- Geht nur für normalen Schutzbedarf (niedrig-mittel)
  → ergänzende Risikoanalyse

Ergänzende Risikoanalyse

- Was ist, wenn man IT-System bzw. eine Anwendung hat, für die kein Baustein in den Grundschutzkatalogen existiert?
  - Beispiele: Krankenhausinformationssystem, Bankanwendungen, Fabriksteuerung
- Was ist, wenn man einen hohen oder sogar einen sehr hohen Schutzbedarf hat?
  - Verwaltung von Patientendaten
  - Militärische Daten

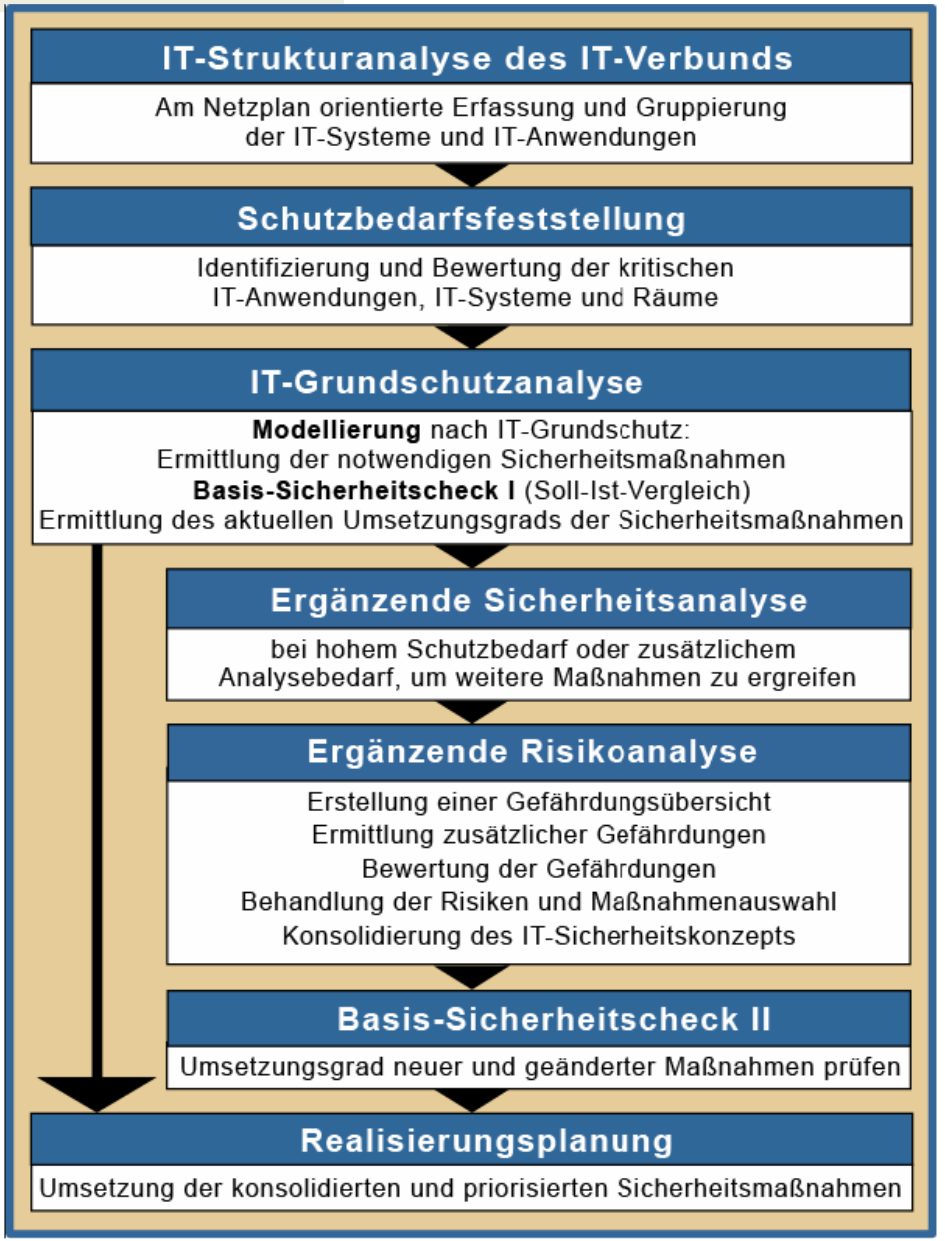
⇒ Durchführung einer ergänzenden Risikoanalyse
  - BSI macht Vorschlag zu einer vereinfachten, qualitativen Risikoanalyse

Planung der Realisierung

- Nach Bestimmung aller Maßnahmen: Planung der Realisierung
- Umsetzung fehlender Maßnahmen
- Priorisierung der Maßnahmen
- Abschätzung der Kosten der Maßnahmen

- Bestätigung durch Zertifikat möglich, wenn lizenzierte Auditoren den IT-Verbund überprüfen (stichprobenartig)

Zusammenfassung: Vorgehensweise nach GS-Grundschutz



Grundschutz-Zertifizierung

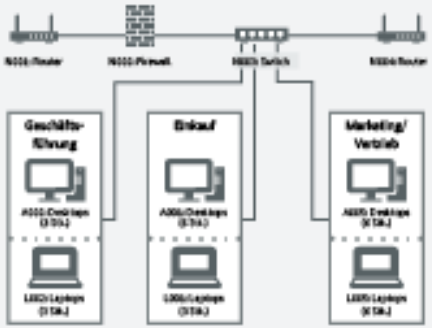
- Zertifizierung des ISMS für einen IT-Verbund:
  - ISO 27001-Zertifikat auf Basis von IT-Grundschutz
- Evaluierung durch lizenzierten Auditor
- Vergabe des Zertifikates durch das BSI

Antragsteller

Dokumente

Sicherheitsrichtlinien
Strukturanalyse
Schutzbedarfsfeststellung
Modellierung
IT-Grundschutz-Check
Risikoanalyse
usw.

Informationsverbund



Zertifizierungsstelle

prüft Audit-Report

vergibt Zertifikat

Auditor

Audit-Report

formale und inhaltliche Prüfung

Realisierungsprüfung

Einordnung

- Pro:
  - Für Standard IT-Systeme bekommt man relativ schnell geeignete und konkrete Sicherheitsmaßnahmen
  - Keine Neuerfindung des Rades: Standardvorgehensweise mit ausgefeilter Methodik
  - Möglichkeit der Zertifizierung
- Contra:
  - Gesamter Prozess etwas schwerfällig
  - „Box-Ticking“-Mentalität
  - Keine offizielle internationale Anerkennung, aber laut BSI kompatibel zu ISO 27001: ISO/IEC 27001-Zertifikat auf Basis von IT-Grundschutz

Vergleich CC/BSI GS/BS 7799

- CC:
  - Abstrakt
  - Auf verschiedene IT-Produkte anwendbar
  - Nur Technik, keine organisatorischen Maßnahmen
  - Internationaler Standard
- BSI GS
  - Konkrete Maßnahmen
  - Auf ganze IT-Verbünde, nicht aber auf einzelne IT-Produkte anwendbar
  - Sowohl technische als auch organisatorische Maßnahmen
  - Kein internationaler Standard
- BS 7799
  - Auf ganze IT-Verbünde, nicht aber auf einzelne IT-Produkte anwendbar
  - Nur organisatorische/prozessorientierte Maßnahmen
  - Internationaler Standard