IT-Sicherheit

Bewertungskriterien und Zugriffskontrolle

Version vom 08.10.2024

Motivation

Beim Entwurf, Implementierung, Betrieb, Auswahl und Beschaffung von IT-Systemen stellen sich Fragen wie:

- Wie sicher muss das System sein?
- Ist das System sicher genug?
- Wie kann ich die Sicherheit des Systems messen?

Diese Fragen führen zu Katalogen von Bewertungskriterien.

TSEC – Trusted Computer System Evaluation Criteria

- ältester Kriterienkatalog (~1985), auch bekannt als „Orange Book“
- Wird nicht mehr aktiv verwendet, hat jedoch einige Konzepte und Ansätze enthalten, die heute immer noch verwendet werden, dazu zählen v.a. die sog. Sicherheitsstufen:

Stufe	Bedeutung
D	System benötigt keinen oder nur minimalen Schutz
C	Benutzer können Schutz selbst bestimmen, Identität des Benutzers muss geprüft werden (C1: grob, C2: feingranular mit Auditing)
B	Systembestimmter Schutz (mandatory) gemäß linear geordneten Sensitivitätsklassen
B2, B3	B2,B3 erfordert ein formales Sicherheitsmodell und eine Trusted Computing Base, B3 erweitert die Anforderungen an die TCB
A	formaler Nachweis der Einhaltung von Sicherheitseigenschaften

„discretionary access control“ wird unterstützt von aktuellen Betriebssystemen

z.B. „streng geheim“ > „geheim“ > „NfD“ > „offen“

- Einstufung: Sensitivitätsklasse eines Objekts
- Clearance: Sensitivitätsklasse eines Subjekts

Discretionary vs. Mandatory Access Control

Discretionary Access Control

- Objekte (z.B. Dateien) sind Subjekten (z.B. Nutzern) zugeordnet.
- Subjekte können selbst den Zugriffsschutz ihrer Objekte definieren (z.B. Dateizugriffsrechte und Windows und Linux).

Mandatory Access Control

- Das (Betriebs-)System begrenzt den Zugriff eines Subjekts auf ein Objekt anhand definierter Zugriffsregeln.
- Die Menge der Zugriffsregeln bilden die Security Policy des Systems.
- Nutzer können die Security Policy nicht ändern (nur „Security Policy Operator“)
- Beispiele: SE Linux, AppArmor

Bell-LaPadula-Sicherheitsmodell

Streng Geheim erlaubt **Streng Geheim**

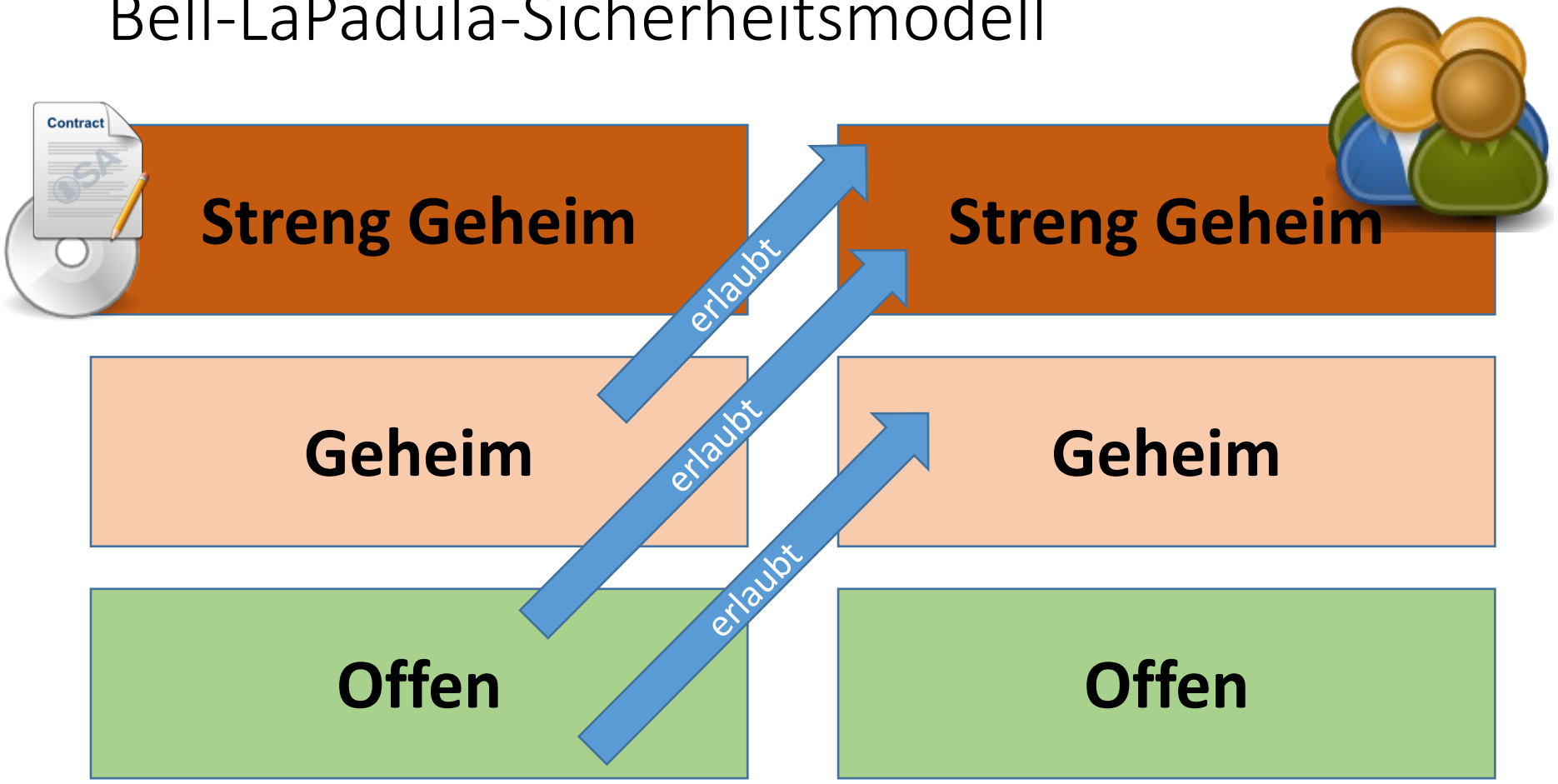
Geheim erlaubt **Geheim**

Offen erlaubt **Offen**

Einstufung

Clearance
(Ermächtigung)

Bell-LaPadula-Sicherheitsmodell



Einstufung | ***Read-Down*** | Clearance (Ermächtigung)

Bell-LaPadula-Sicherheitsmodell

Streng Geheim | **Streng Geheim**

Geheim | **Geheim**

Offen | **Offen**

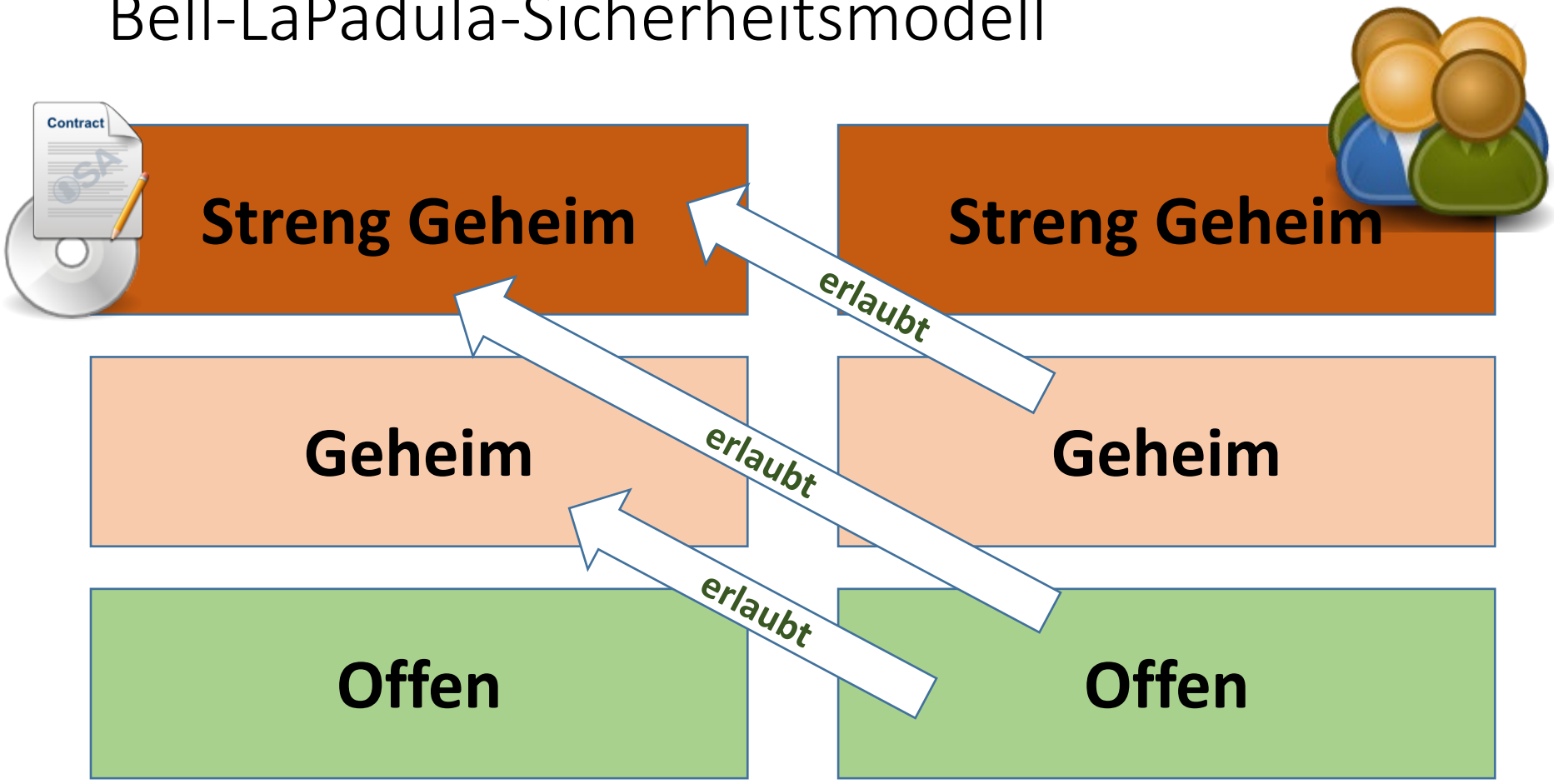
verboten

verboten

verboten

Einstufung — ***No-Read-Up*** — Clearance (Ermächtigung)

Bell-LaPadula-Sicherheitsmodell



Bell-LaPadula-Sicherheitsmodell

Streng Geheim | **Streng Geheim**

verboten

Geheim | **Geheim**

verboten

Offen | **Offen**

verboten

Einstufung — ***No-Write-Down*** — Clearance (Ermächtigung)

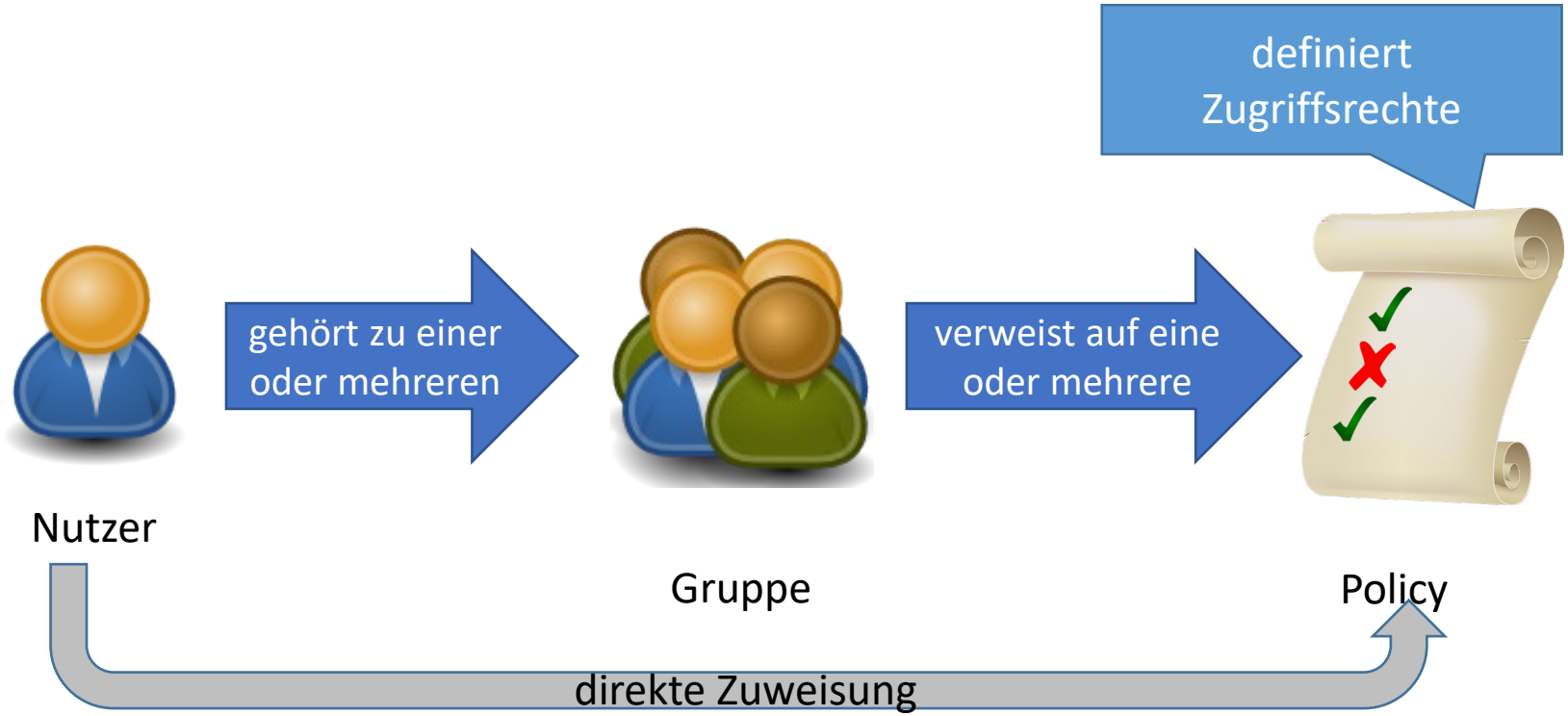
Bell-LaPadula-Sicherheitsmodell (Überblick)

- Fokus: Vertraulichkeit
- Erlaubt:
  - Lesen und Schreiben von Informationen, deren Einstufung der eigenen Ermächtigung entsprechen
  - Lesen von Informationen, deren Einstufung unterhalb der eigenen Ermächtigung liegen (Read-Down)
  - Schreiben von Informationen, deren Einstufung oberhalb der eigenen Ermächtigung liegen (Write-Up)
- Verboten:
  - Lesen von Informationen, der Einstufung oberhalb der eigenen Ermächtigung liegt (No-Read-Up, simple security property)
  - Schreiben von Informationen, der Einstufung unterhalb der eigenen Ermächtigung liegt (No-Write-Down, Star-Property)
  - Zugriffe, die dem „discretionary access“-Prinzip widersprechen

Biba-Sicherheitsmodell

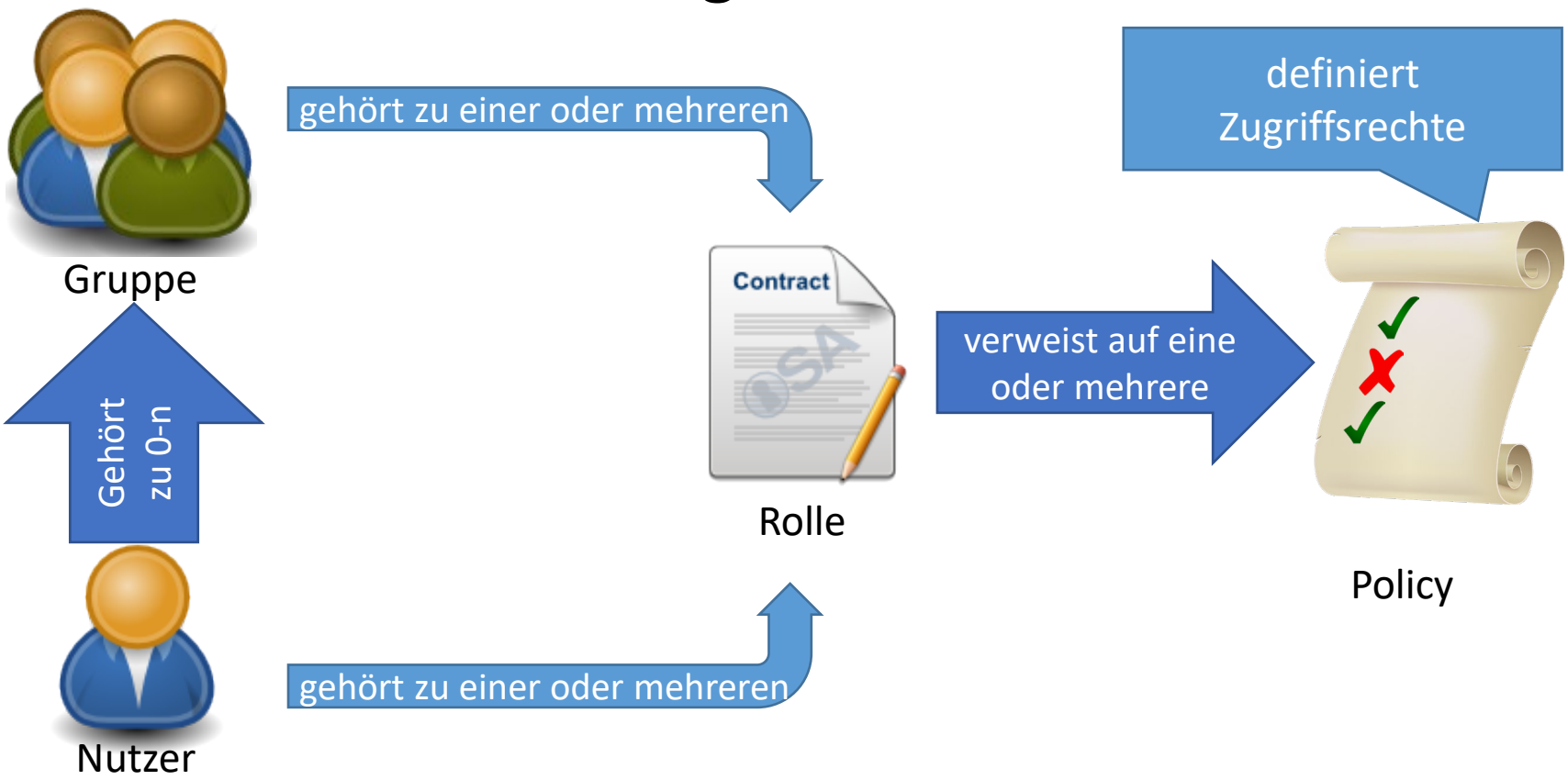
- Fokus: Integrität
- Erlaubt:
  - Lesen und Schreiben von Informationen deren (Integritäts-)Einstufung der eigenen Ermächtigung entspricht.
  - Lesen von Informationen, deren Einstufung über der eigenen Ermächtigung liegt.
  - Schreiben von Informationen, deren Einstufung unterhalb der eigenen Ermächtigung liegt.
- Verboten:
  - Lesen von Informationen mit Einstufung unterhalb der eigenen Ermächtigung.
  - Schreiben von Informationen mit Einstufung oberhalb der eigenen Ermächtigung.

Gruppenbasiertes Zugriffsmodell



Durch gruppenbasierte Zugriffsmodelle kann im Vergleich mit der individuellen Zuweisung von Zugriffsrechten eine hohe Skalierung erreicht werden.

Rollenbasiertes Zugriffsmodell



Rollenbasierte Zugriffsrechte ermöglichen eine weitere Abstraktion.

Zugriffskontrolle: allgemeine Anforderungen

- Sicherheit
  Nur autorisierte Personen und Prozesse dürfen sensible Daten oder Programme nutzen oder verändern. Zugriffe müssen mit den Vorgaben der Organisation übereinstimmen. Nutzer dürfen keine (oder kaum) Möglichkeiten haben, die Verfügbarkeit des Systems zu stören.
- Verlässlichkeit
  Die Zugriffskontrolle muss jederzeit wie erwartet funktionieren. (sonst Gefahr des Denial of Service)
- Transparenz
  Die Zugriffskontrolle darf die Nutzung des eigentlichen Systems für autorisierte Nutzer nicht beeinträchtigen. (idealerweise)
- Skalierbarkeit

Zugriffskontrolle: allgemeine Anforderungen

- Wartbarkeit
  Zugriffskontrollsysteme dürfen nicht zu komplex oder zeitintensiv in der Wartung sein, da sonst Administratoren nicht mit notwendigen Änderungen Schritt halten können und „Abkürzungen“ einbauen.
- Auditierbarkeit
  Zugriffskontrollsysteme sollen Logdaten über Systeme, Prozesse und Nutzer führen. → Problembehandlung, Erkennung von Eindringversuchen, Accountability
- Integrität
  Änderungen der Zugriffskontrolle dürfen nur autorisiert und protokolliert erfolgen.
- Authentizität (optional)
  Die Authentizität von Eingabedaten und deren Quelle werden auf Authentizität und Integrität geprüft.

Prinzip: Separation of Duties

Grundlegendes Prinzip der Zugriffskontrolle, bestehend aus zwei Teilen:

1. Keine einzelne Person darf vollständige Kontrolle über einen Prozess haben, aus dem sie selbst persönlichen Nutzen ziehen könnte.
2. Wenn die Gefahr besteht, dass mehrere Personen betrügerisch kooperieren, dann müssen die Zuständigkeiten rotiert werden.
   Erweiterung:
   Wird eine Person aus einer Zuständigkeit rotiert (turnusmäßig oder z.B. durch Beurlaubung), dann werden deren Tätigkeiten analysiert.

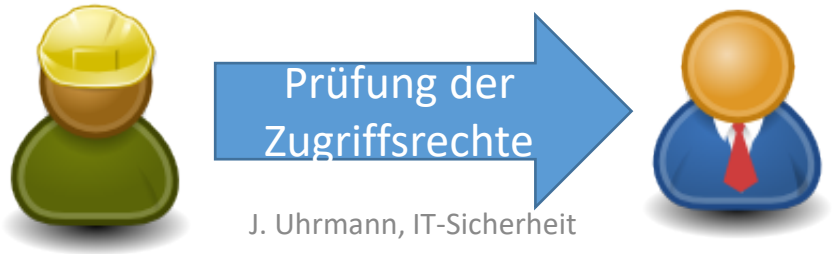
Prinzip: Least Privilege

Personen oder Prozesse dürfen nur Zugriffsrechte besitzen

1. die sie für die Durchführung ihrer zugewiesenen Tätigkeit benötigen.
2. für die Dauer dieser Tätigkeit!

Häufige Verletzungen:

- Nutzer arbeitet dauernd mit administrativen Rechten.
- Nutzer haben Zugriff auf alle Dateien eines Fileservers.
- **Personen wechseln von technischen Positionen ins Management und behalten ihre Admin-Rechte**.



Prinzip: Need to know

Nutzer sollten nur Zugriff auf Informationen haben, die sie für die Durchführung ihrer zugewiesenen Tätigkeit benötigen.

Die Umsetzung erfolgt zweistufig:

1. Der Eigentümer der Information muss entscheiden, wer Zugriff erhält („discretionary access control“ oder durch Einstufung).
2. Das Zugriffskontrollsystem muss den Zugriff entsprechend einschränken.

Hinweis:
Die Einstufung allein ist oft nicht ausreichend für die Umsetzung dieses Prinzips. Muss eine Person mit der Ermächtigung für „streng geheim“ wirklich Zugriff alle Informationen haben?

Identifikation

Prozess, um eine eindeutigen, maschinen-lesbaren Namen zuzuweisen, die die Erkennung eines Nutzers oder einer Ressource eines IT-Systems ermöglicht.

➔Zuordnung von Ressourcen und Nutzern zu Accounts

➔Accounts müssen zuvor eingerichtet sein!

Methoden der Identifikation

- Nutzernamen
- Kontonummern
- E-Mail Adresse
- Mitarbeiternummer
- RFID-Token
- MAC-Adresse
- IP-Adresse
- usw. usf.

Nicht mit Authentifizierung verwechseln!

Diese prüft, ob die behauptete Identität wirklich zutrifft!

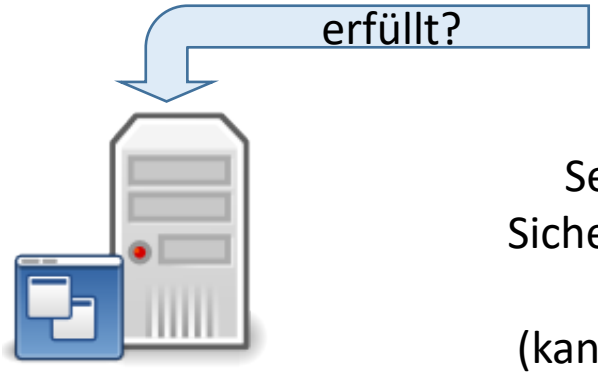
typischerweise für techn. Ressourcen im Netzwerk verwendet

Sehr leicht durch sog. Spoofing zu fälschen und daher meistens für die Authentifizierung ungeeignet.

Common Criteria (ISO/IEC 15408) Anforderungen

Protection Profile (PP)

Sicherheitsanforderungen
für Geräte-/Softwaretypen
(z.B. „Cryptograhic Modules“ [1])



Target of Evaluation (TOA)

Security Target (ST)
Sicherheitseigenschaften
der Evaluierung
(kann auf PP verweisen)
„WAS“ wird verlangt.

Security Functional Requirements (SFR)
beschreiben einzelne Sicherheitsfunktionen
„WIE“ wird Sicherheitseigenschaft erfüllt.

[1] https://www.commoncriteriaportal.org/files/ppfiles/pp0044b.pdf

Common Criteria – Evaluierung

Evaluation Assurance Level (EAL)

Tiefe und Genauigkeit der Evaluierung (Stufen 1 bis 7)

eingehalten?

Target of Evaluation (TOA)

Security Assurance Requirements (SAR)

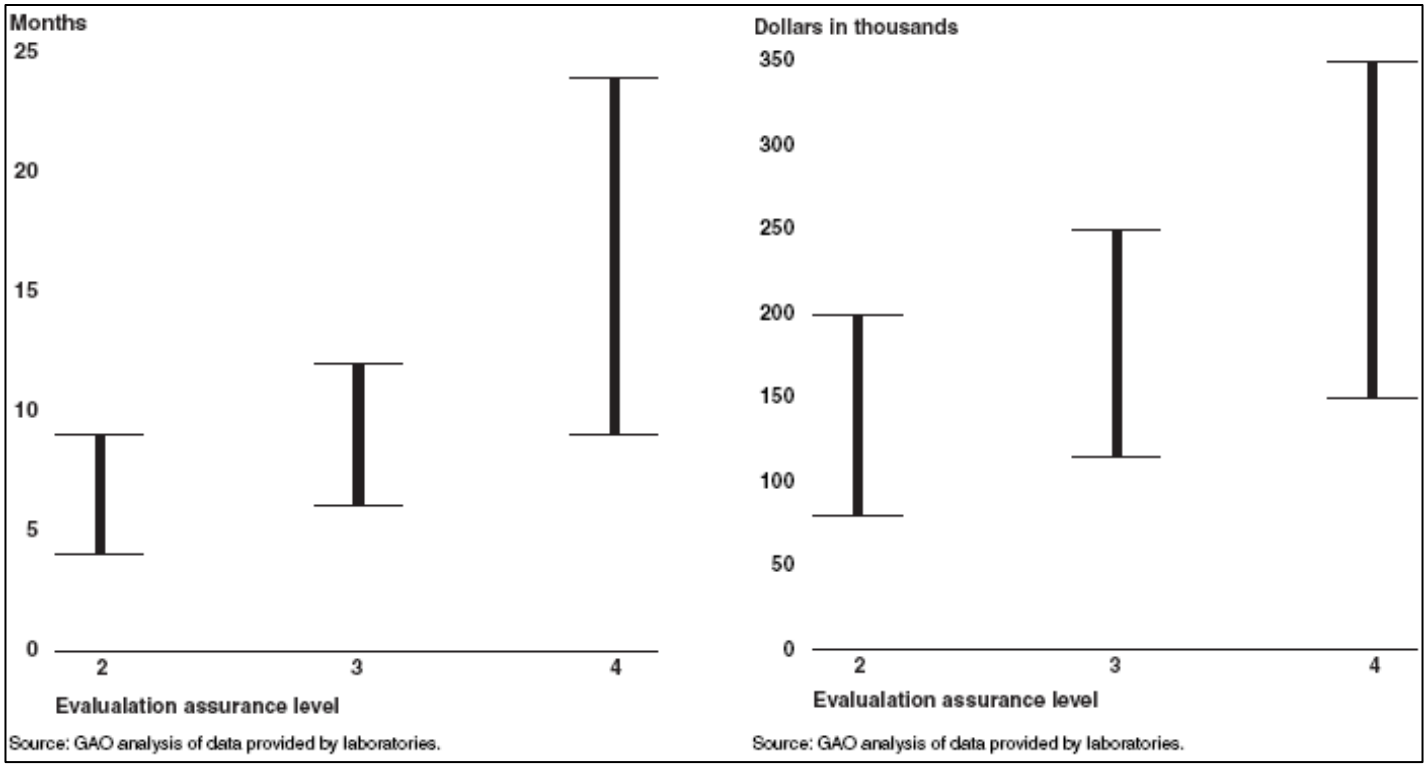
Maßnahmen bei Entwicklung und Test des TOAs, um die Sicherheitseigenschaften zu garantieren

[1] https://www.commoncriteriaportal.org/files/ppfiles/pp0044b.pdf

CC: Evaluation Assurance Level

- EAL 1 (functionally tested) unabhängiger Test gegen Spezifikation, keine Unterstützung des Entwicklers notwendig, grundlegende Schutzfunktionen des TOEs und Konsistenz mit Dokumentation
- EAL 2 (structurally tested) geringe Unterstützung durch Entwickler notwendig. Sinnvoll, wenn vollständige Entwicklungsdokumentation nicht verfügbar
- EAL 3 (methodically tested and checked)
- EAL 4 (methodically designed, tested and reviewed)
- EAL 5 (semiformally designed and tested)
- EAL 6 (semiformally verified designed and tested)
- EAL 7 (formally verified design ad tested)

Evaluierungsdauer und -kosten



Kommerzielle Betriebssysteme (MS Windows, Oracle/RedHat/SuSE Linux, AIX, …) sind EAL 4 evaluiert (bestimmte Versionen).

ISO/IEC 27001

- Internationale Norm zu „Information Security Management Systems“ – ISMS
- Ziel:
  Anforderungen definieren, um in einer Organisation Informationssicherheit
  - zu managen
  - zu etablieren
  - umzusetzen
  - aufrecht zu erhalten
  - kontinuierlich zu verbessern

ISO/IEC 27001 – Aufbau

- Kontext der Organisation verstehen, Erwartungen erfassen, Scope eines Informationsmanagementsystems definieren.
- Führungskräfte und Management sollen der Informationssicherheit verpflichtet sein und entspr. Engagement zeigen.
- Das Top-Management soll eine Security Policy etablieren.
- Bereits die Planung des ISMS soll Risiken und Chancen der Informationssicherheit für die Organisation herausarbeiten und adressieren.
- Ein Assessment-Prozess für Risiken muss etabliert werden, der Risiken identifiziert, analysiert, bewertet und adressiert.
- Ziele der Informationssicherheit müssen organisationsspezifisch definiert werden.

ISO/IEC 27001 – Aufbau (cont.)

- Die notwendigen Ressourcen zur Umsetzung müssen ermittelt und bereitgestellt werden. Dazu zählen auch Sicherheitsbewusstsein der Mitarbeiter und die Kommunikation mit Externen.
- Dokumente müssen entsprechend dem Standard behandelt werden (z.B. Definition von Formaten, Art der Speicherung, Aufbewahrung, Vernichtung)
- Interne Prüfung der Performance und Effektivität der Umsetzung muss stattfinden und dokumentiert werden.
- Regelungen zu Abweichungen müssen getroffen und umgesetzt werden.

Der Anhang A der Norm beinhaltet Security Controls.

Allgemeine Hinweise zu Zertifizierungen

- Prüfen Sie, ob die Zertifizierung unabhängig erfolgte.
- Vergleichen Sie Ihre Anforderungen mit dem Scope der Zertifizierung.
- Ermitteln Sie, ob die Zertifizierung die Dokumentation oder die Effektivität der Security prüft.
  (In welche Kategorie gehören Common Criteria und ISO27001?)

Fazit:

➔Zertifizierungen treffen immer nur Aussagen zu ihrem jeweiligen Inhalt und dem Scope der Zertifizierung.

➔Zertifizierungen geben lediglich Hinweise bzgl. der tatsächlichen Sicherheit.

➔Ein Gespräch mit den jeweiligen Entwicklern ist durch nichts zu ersetzen. (im Zweifelsfall selbst auditieren [lassen])