Access Control

Standart Access Control Systeme

Preventive

Unauthorisierte Aktivität wird bereits im Vornherein verhindert.

- Zaun, Schloss, Biometrie, Encrpytion, Firewalls, security-awareness training, …

Detective

Ungewollte/unauthorisierte Aktivität wird entdeckt. Detective Access Control funktioniert nach der Tat und kann Aktivität nur entdecken, wenn/nachdem sie passiert ist.

- Wächter, Überwachungskameras, Intrusion Detection Systeme (IDSs), Bewegungsmelder …

Corrective

Wird nach der Tat angewendet, um das System zurück in den normalen Zustand zu versetzen. Beispiel: Backup

- System-Reboot, Antivirus-Software (die den Virus entfernt), Backup, …

Weitere Access Control Systeme

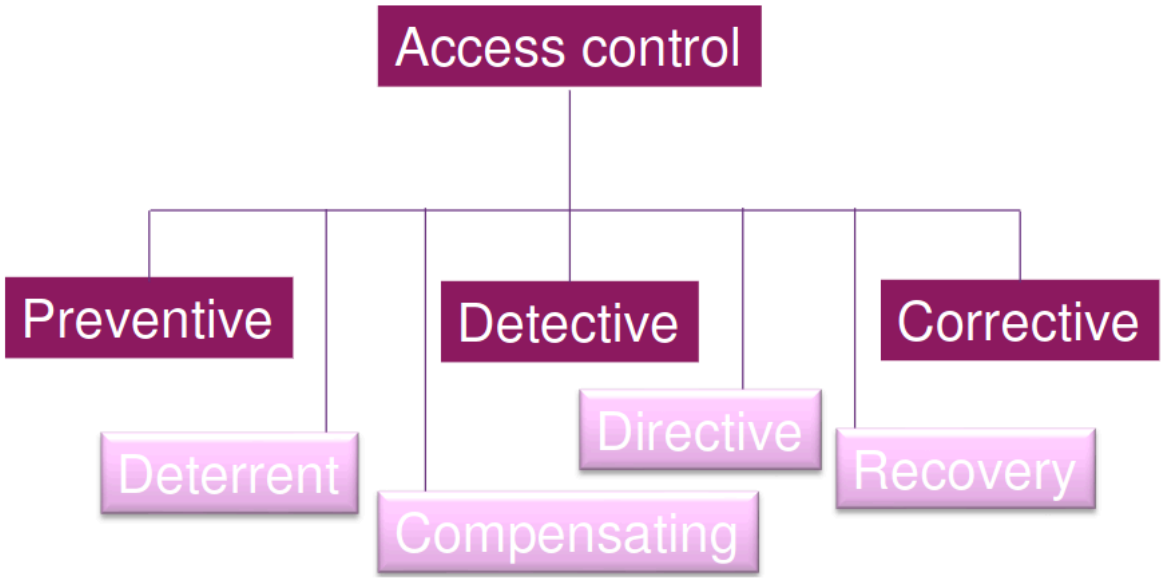

Figure 1: Access Control Types

Deterrent Access Control

Ähnlich wie Preventive Access Control. Hier wird der Angreifer vor der Tat abgeschreckt.

- Policies, Security Awareness Training, Schloss, Zaun, Security Badges, Sicherheitsbeamte, Sicherheitskameras …

Compensating Access Control

Wenn andere Access Control Systeme nicht ausreichen, wird dieses System eingesetzt. Es unterstützt und verstärkt die anderen Systeme.

- Policy, die besagt, dass alle PII (Personal Identifiable Information) verschlüsselt werden muss. Zum Beispiel wird PII in einer Datenbank gespeichert, die verschlüsselt ist, jedoch werden die Daten in Klartext über das Netzwerk übertragen. Hier kann ein Compensation Control System verwendet werden.

Recovery Access Control
Eine Erweiterung von Corrective Access Control, mit fortgeschritteneren oder komplexeren Möglichkeiten.
- Backups, System Imaging, Server Clustering, Antivirus Software, Database/VM-Shadowing, hot/cold sites, …

Directive Access Control
Hier wird dem Subjekt gesagt, was er tun soll, und was nicht. Beispiel: “Bitte geben Sie Ihr Passwort ein.”
- Policies, Excape Route Exit Signs, Systemüberwachung, …

Zugriff auf Assets konrtollieren

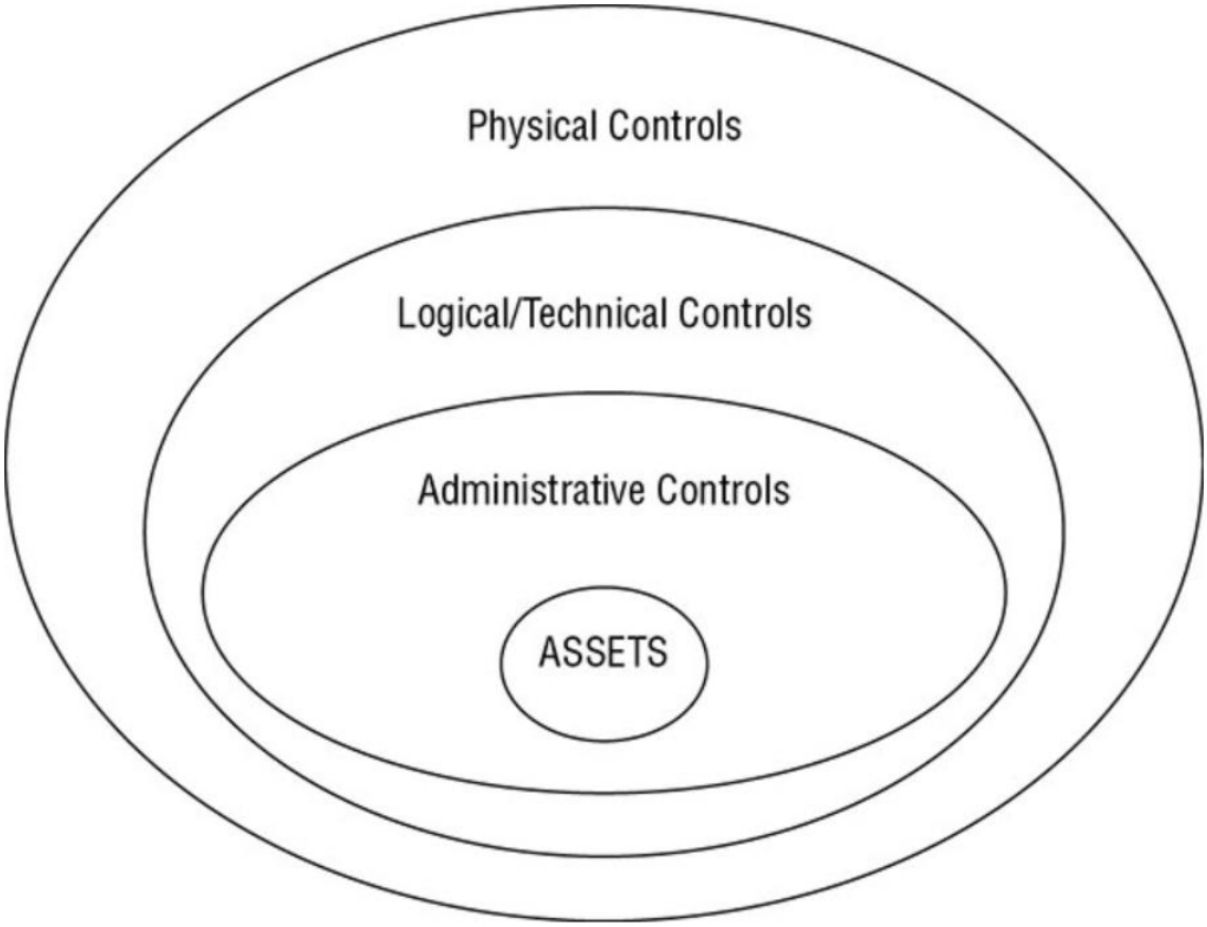

Figure 2: Access Control Layers

Physical Controls
Physikalische Barrieren innerhalb einer Einrichtung:
- Schloss, Zaun, Türen, Fenster, …

Technical/logical Controls
Hardware/Software-Mechanismen, die den Zugriff auf Systeme und Daten kontrollieren:
- Passwörter, Biometrie, Firewalls, Intrusion Detection Systems, Routers, …

Administrative Controls
Policiesm, Verfahren und Richtlinien einer Organisation, die den Zugriff auf Systeme und Daten kontrollieren:

- Security Awareness Training, Security Policies, Security Procedures, Security Guidelines, Personalkontrollen, …

Schritte der Zugriffskontrolle

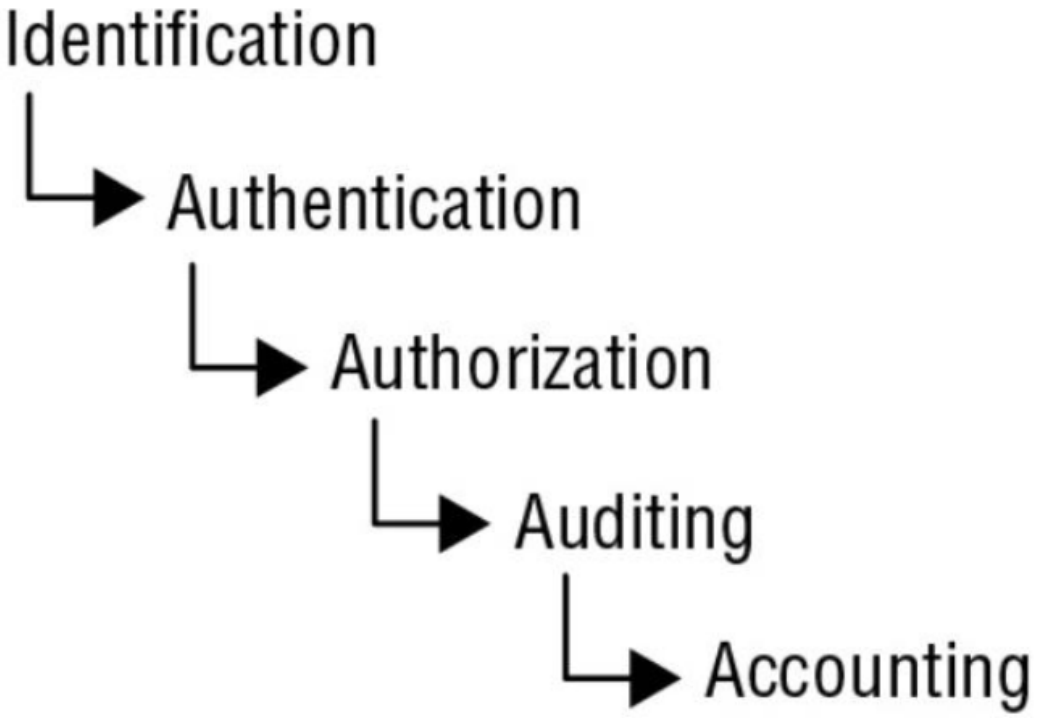

Figure 3: Access Control Steps

Identifikation
Unter Identifikaton versteht man den Prozess, bei dem das Subjekt seine Identität “behauptet” (claimt).