Basis Prinzipien des Informationsschutzes

Principle of Least Privilege

minimale Rechtevergabe

Ein Subjekt soll zu jedem Zeitpunkt nur über diejenigen Rechte verfügen, die für die Erledigung der aktuellen Aufgabe unverzichtbar sind.

Principle of Separation of Privilege

Rechte werden aufgrund mehrerer Bedingungen gewährt

Die Gewährung eines Rechts wird von mehreren Bedingungen abhängig gemacht.

Principle of Complete Mediation

alle Zugriffe werden überwacht

Alle Zugriffe auf Objekte werden geprüft, bevor sie erlaubt werden.

Principle of Fail-Safe Defaults

was nicht explizit erlaubt ist, ist verboten

Was nicht explizit erlaubt wird ist verboten.

Principle of Open Design

Sicherheit hängt nicht von Geheimhaltung ab

Sicherheit eines Mechanismus sollte nicht von der Geheimhaltung der Funktionsweise des Mechanismus oder seiner Implementierung abhängen

Principle of Economy of Mechanism

möglichst einfach

Sicherheitsmechanismen sollen so einfach wie möglich sein. Einfache Konzepte minimieren Fehler und vereinfachen das Testen. Annahmen über komplexe Mechanismen können bei Irrtum zu Sicherheitsproblemen führen.

Principle of Psychological Acceptability

Sicherheit soll die Arbeit nicht erschweren

Die Benutzung eines Systems, Anwendungsprogramms, . . . soll mit Sicherheitsmechanismen nicht wesentlich schwerer sein als ohne die Mechanismen.

www.wenzlaff.de

Quelle: http://web.mit.edu/Saltzer/www/publications/protection