Generische Liste von Schwachstellen

Technische Verwundbarkeiten

- Unklare oder schwer verständliche Benutzeroberflächen, die Fehlbedienungen begünstigen
- Fehlende oder unvollständige technische Dokumentation
- Geräteanfälligkeit gegenüber Umwelteinflüssen wie Temperatur, Feuchtigkeit, Staub oder Spannungsschwankungen
- Mangelhafter Schutz physischer Leitungen und Netzwerkkabel
- Veraltete oder nicht ersetzte Hardware-Komponenten
- Veraltete Betriebssysteme (End-of-Life, End-of-Service, deaktivierte Updatemechanismen, …)
- Ungeschützte oder schlecht gesicherte Netzwerkzugänge, insbesondere im öffentlichen Raum
- Unzureichender Schutz vor Schadsoftware oder fehlende Aktualisierung von Sicherheitsmechanismen (Antivirus, Malware-Schutz, …)
- Fehlende Systeme für sichere Identifizierung und Authentifizierung
- Schwache oder unzureichend geschützte kryptografische Schlüssel (zB. Keine Verwendung eines Passwort-Safe)
- Unzureichende Trennung von Test- und Produktionssystemen
- Fehlende oder ineffiziente Redundanzen für kritische Systeme

Prozessuale und organisatorische Schwächen

- Fehlende oder unklare Klassifizierung sensibler Informationen
- Unzureichende Prozesse, um Änderungen kontrolliert einzuführen (Change Management)
- Unstrukturierte oder veraltete interne Dokumentation
- Lückenhafte Wartungs- und Pflegeprozesse für IT-Systeme
- Unzureichend geregelte Verantwortlichkeiten für Zugangs- und Zugriffskontrolle
- Mangelhafte Backup-Strategien oder unregelmäßige Sicherungen
- Unzureichende Kontrolle eingehender und ausgehender Daten
- Fehlende Validierung der verarbeiteten Daten
- Unklare oder nicht etablierte Vorgaben für den Umgang mit mobilen Endgeräten
- Nichtexistenz einer Clear-Desk- und Clear-Screen-Regelung

Menschliche Faktoren

- Niedriges Sicherheitsbewusstsein bei Mitarbeitenden
- Unzureichende Schulungen zur sicheren Nutzung von Informationssystemen
- Mangelnde Sensibilisierung für Social Engineering
- Unzureichende Überprüfung von Mitarbeitenden oder externen Dienstleistern
- Nutzung von Standardpasswörtern oder fehlende Passwortüberprüfungen
- Unkontrollierte oder nicht autorisierte Nutzung von Internetdiensten oder Software

Physische Schwachstellen

- Lücken in der physischen Zugangskontrolle zu Gebäuden und IT-Räumen
- Unzureichende Absicherung sensibler Bereiche oder Geräte
- Fehlende Konzepte zur sicheren Entsorgung von Datenträgern und Hardware
- Standorte mit erhöhter Exposition gegenüber äußeren Risiken wie Wasser, Feuer, Explosionen oder Naturkatastrophen

Rechtliche und administrative Defizite

- Unzureichende Personalprozesse, insbesondere bei Eintritt, Rollenwechsel und Austritt
- Fehlende Einbindung von rechtlichen Anforderungen in interne Prozesse
- Unklare Verantwortlichkeiten im Umgang mit Compliance-Anforderungen
- Mangelhafte interne Revision oder fehlende Überprüfung sicherheitsrelevanter Maßnahmen

Daten- und Informationsmanagement

- Unkontrolliertes Kopieren oder Exportieren von Informationen
- Unzureichende Nachvollziehbarkeit bei Datenverarbeitung und Datenfluss
- Fehlende oder unzureichende Richtlinien zur Informationsverarbeitung
- Unkontrollierter Einsatz zusätzlicher oder privater IT-Systeme (Schatten-IT)