# Phase 7: Erstellen eines IT-Sicherheitskonzeptes

|  |  |  |
| --- | --- | --- |
| **Datenquelle** | **Technische Maßnahmen** | **Organisatorische Maßnahmen** |
| Server zur Angebotserstellung + DB | *Zutrittskontrolle:*   * Elektronisches Zugangssystem, um Zutritt zum Serverraum zu überwachen * Sperrung der Endgeräte bei Nichtverwendung   *Zugangskontrolle:*   * Strenges Passwortverfahren   *Zugriffskontrolle:*   * Differenziertes Berechtigungskonzept   *Verfügbarkeitskontrolle:*   * Firewalls, Anti-Viren-Software, Backups * Sicherheitsupdates   *Verschlüsselung:*   * Transportverschlüsselung * Inhaltsverschlüsselung * Website-Verschlüsselung mit SSL-Zertifikat * VPN Verbindung für Zugriff auf Firmennetzwerk   *Eingabekontrolle:*   * Zugriff auf die Systeme und auf personenbezogenen Daten werden protokolliert | *Schulungen:*   * IT-Sicherheitsschulungen * Schulungen zu neuen Software-/Hardwarelösungen   *IT-Leitlinie:*   * Passwortregelungen * Umgang mit Mobilgeräten (keine privaten Endgeräte zugelassen)   *IT-Notfallpläne:*   * Anweisungen für den Umgang mit technischen Angriffen   *Sicherheitspersonal:*   * Datenschutzbeauftragter * IT-Sicherheitsbeauftragter   *Verträge:*   * Mit Mitarbeiter vereinbarte Geheimhaltungspflicht |
| Kundendaten |
| Mitarbeiterdaten (personenbezogene Daten) |
| Projektdaten (Projektauftrag, Grundriss, Angebot, Netzplan) |
| Mobile Endgeräte |