**Phase 6**

Identifizieren Sie die Nutzer des Systems

**Kunde**  schreiben

**Mitarbeiter Außendienst** lesen, schreiben

**Projekt Planer**  lesen, schreiben, bearbeiten

**Lieferant**  lesen

**ITSystemhaus DD** lesen, schreiben, bearbeiten

**Definieren Sie die Schnittstelle zwischen eigenen Software-Anwendungen und der gewählten Nutzerverwaltung.**

***Vom Kunden und Lieferanten zur ITSystemhaus DD*** **Schnittstelle**: Webserver, auf den Nutzer öffentlich zugreifen können, um Daten einzugeben und zu versenden.

***Von ITSystemhaus DD zum Projekt Planer und Mitarbeiter im Außendienst***

**Schnittstelle:** Mithilfe eines Datenbankservers können die Projekt Planer und Mitarbeiter im Außendienst die benötigten Daten, welche vom Nutzer eingegeben wurden anzeigen lassen.

**Bei einem Telefongespräch fragt der Kunde nach, ob die Daten im zu erstellenden Software-System auch sicher sind. Der Kunde äußerst Sorgen, dass Hacker oder ein nicht loyaler Mitarbeiter wichtige Unternehmensdaten unbemerkt entwenden können. Sie beruhigen Ihn und stellen Ihm ein Sicherheitskonzept in Aussicht.**

Der Datenbankserver, auf dem die Kundendaten gespeichert sind befinden sich in einer entmilitarisierten Zone im privaten Netzwerk. Diese wird durch mindestens eine Firewall abgesichert.

Die Mitarbeiter können zwar lesen und schreiben, die Daten können sie jedoch nicht bearbeiten. Bei der Anmeldung an dem Datenbankserver zur Eingabe von Daten wird das Nutzer-Account des Mitarbeiters zur Anmeldung benötigt. Dadurch können unbefugte Zugriffe erkannt und nachverfolgt werden. Die Mitarbeiter können keine Daten aus der Datenbank löschen. Die Daten werden bei einem Versuch der Löschung lediglich nicht mehr angezeigt, sind aber noch vorhanden. Die Daten werden mithilfe von regelmäßigen Backups zusätzlich abgesichert.

**Phase 7**

|  |  |
| --- | --- |
| Zutrittskontrolle | **Gebäudesicherung**  Zäune  Pforte  Videoüberwachung  **Sicherung der Räume**  Sicherheitsschlösser  Chipkartenleser  Codeschlösser  Sicherheitsverglasung  Alarmanlagen |
| Zugangskontrolle | Benutzerkennung mit Passwort  Biometrische Benutzeridentifikation  Firewall  Zugangsberechtigungen |
| Zugriffskontrolle | Berechtigungskonzept  Benutzerkennung mit Passwort  Gesicherte Schnittstellen (USB, Firewire, Netzwerk etc.)  Datenträgerverwaltung  Zugriffsberechtigungen |
| Weitergabekontrolle | **Sicherung bei elektronischer Übertragung**  Verschlüsselungen  Virtuelles Privates Netzwerk  Firewall  Fax-Protokoll  **Sicherung bei der Übermittlung**  Verfahrensverzeichnis  Protokollierungsmaßnahmen |
| Eingabekontrolle | Protokollierung  Benutzeridentifikation |
| Auftragskontrolle | Weisungsbefugnisse festlegung  Vort-Ort-Kontrollen  Datenschutzvertrag gemäß den Vorgaben nach §11 BDSG  Stichprobenprüfung  Kontrollrechte |
| Verfügbarkeitskontrolle | Brandschutzmaßnahmen  Überspannungsschutz  USV  Klimaanlage  RAID  Backupkonzept  Virenschutzkonzept  Schutz vor Datendiebstahl |
| Trennungsgebot | Trennung von Produktiv- und Testsystemen  Getrennte Ordnerstrukturen  Separate Tabellen innerhalb der Datenbanken  Getrennte Datenbanken |

Bei einer Fortbildung für Fachinformatiker kommen Sie beim Mittagessen mit einem Teilnehmer ins Gespräch. Dieser erzählt Ihnen, dass es seinem Entwicklerteam unheimlich die Arbeit erleichtert, wenn die Anzahl der Datenquellen und Datenformate intern im Software-System gering gehalten wird.

**Phase 8**

**Konzept für einen Einheitlichen Zugriff auf Datenquellen mit Berechtigungen**

Für den einheitlichen Zugriff kann ein Webserver erstellt werden. Auf diesem gibt es ein LogIn-System, welches auf eine Datenbank verweist. Durch dieses System ist es möglich, dass sich Kunden zur Kontaktaufnahme und zum Datenaustausch registrieren können. Die Mitarbeiter bekommen die Anmeldinformationen zu einem Administrativen Konto. Damit ist es möglich die eingesendeten Daten und Nachrichten der Benutzerkonten zu lesen und denen über das System einheitlich antworten zu können.

**Teil 2**

Tabellen:

Benutzer:

- Benutzer\_ID (Primärschlüssel)

- Benutzername

- Profilbild (BLOB)

Anwendung:

- Anwendung\_ID (Primärschlüssel)

- Benutzer\_ID (Fremdschlüssel)

- Anwendungsdaten (BLOB)

Einstellungen:

- Einstellung\_ID (Primärschlüssel)

- Benutzer\_ID (Fremdschlüssel)

Protokolle:

- Protokoll\_ID (Primärschlüssel)

- Benutzer\_ID (Fremdschlüssel)

- Protokolldaten (BLOB)