### Sicherheitsanforderungen

| **Feld** | **Beschreibung** |
| --- | --- |
| **Name des Artefakts** | Sicherheitsanforderungen |
| **Verantwortlich** | IT-Security-Spezialist |
| **Ziel des Dokuments** | Definition der Anforderungen an die IT-Sicherheit der Anwendung. |
| **Wesentliche Inhalte** | - Sicherheitsziele  - Anforderungen an Authentifizierung und Autorisierung  - Datenschutzanforderungen |
| **Erstellungszeitpunkt** | Anfangsphase des Projekts |
| **Nutzung im Projektverlauf** | Grundlage für die Implementierung und Überprüfung der Sicherheit der Anwendung |
| **Abnahme** | Durch den IT-Security-Spezialisten und die IT-Systemverantwortlichen; Überprüfung der Vollständigkeit und Korrektheit der Sicherheitsanforderungen |
| **Abhängigkeiten** | - Funktionale und nicht-funktionale Anforderungen  - Technische Spezifikationen |
| **Versionierung** | Versionskontrolle mittels Versionsmanagement-Tools |
| **Vorlagen und Tools** | Textverarbeitungssoftware (z.B. MS Word, Google Docs) |
| **Zusätzliche Anmerkungen** | Regelmäßige Überprüfung und Aktualisierung der Sicherheitsanforderungen notwendig, um sicherzustellen, dass sie den aktuellen Bedrohungen und Anforderungen entsprechen |

## Sicherheitsanforderungen für die Erweiterung des CRM-Systems

### 1. Überblick

| **Feld** | **Beschreibung** |
| --- | --- |
| **Projektname** | Erweiterung des CRM-Systems um Scoring-Daten |
| **Projektleiter** | Max Mustermann |
| **IT-Sicherheitsverantwortlicher** | Laura Sicherheit |
| **Fachbereich** | Vertrieb |
| **Erstellungsdatum** | 19. Mai 2024 |
| **Version** | 1.0 |

### 2. Ziel

Das Ziel dieses Dokuments ist es, die Sicherheitsanforderungen für die Erweiterung des bestehenden CRM-Systems zu definieren, um sicherzustellen, dass alle sicherheitsrelevanten Aspekte berücksichtigt und umgesetzt werden.

### 3. Sicherheitsanforderungen

#### 3.1 Datenübertragung

| **ID** | **Anforderung** | **Priorität** | **Beschreibung** |
| --- | --- | --- | --- |
| S1 | Verschlüsselte Übertragung | Hoch | Alle Daten, die zwischen dem Benutzer und dem CRM-System übertragen werden, müssen über HTTPS verschlüsselt sein. |

#### 3.2 Datenspeicherung

| **ID** | **Anforderung** | **Priorität** | **Beschreibung** |
| --- | --- | --- | --- |
| S2 | Verschlüsselte Speicherung | Hoch | Die Scoring-Daten müssen verschlüsselt in der Datenbank gespeichert werden. |
| S3 | Zugriffskontrollen | Hoch | Nur autorisierte Benutzer dürfen auf die Scoring-Daten zugreifen. |

#### 3.3 Authentifizierung und Autorisierung

| **ID** | **Anforderung** | **Priorität** | **Beschreibung** |
| --- | --- | --- | --- |
| S4 | Starke Authentifizierung | Hoch | Benutzer müssen sich mit starken Authentifizierungsmethoden (z.B. 2-Faktor-Authentifizierung) anmelden. |
| S5 | Rollenbasierte Zugriffskontrolle | Hoch | Der Zugriff auf die Scoring-Daten muss rollenbasiert gesteuert werden. |

#### 3.4 Audit und Protokollierung

| **ID** | **Anforderung** | **Priorität** | **Beschreibung** |
| --- | --- | --- | --- |
| S6 | Protokollierung von Zugriffen | Mittel | Alle Zugriffe auf die Scoring-Daten müssen protokolliert werden, einschließlich Benutzer-ID, Zeitstempel und Aktion. |
| S7 | Überwachung und Alarme | Mittel | Ungewöhnliche Zugriffs- oder Aktivitätsmuster müssen erkannt und gemeldet werden. |

#### 3.5 Datenintegrität

| **ID** | **Anforderung** | **Priorität** | **Beschreibung** |
| --- | --- | --- | --- |
| S8 | Integritätsprüfungen | Hoch | Regelmäßige Integritätsprüfungen der Scoring-Daten müssen durchgeführt werden, um Manipulationen zu erkennen. |

#### 3.6 Datenschutz

| **ID** | **Anforderung** | **Priorität** | **Beschreibung** |
| --- | --- | --- | --- |
| S9 | Einhaltung der DSGVO | Hoch | Alle Datenverarbeitungsprozesse müssen den Anforderungen der Datenschutz-Grundverordnung (DSGVO) entsprechen. |
| S10 | Anonymisierung und Pseudonymisierung | Mittel | Scoring-Daten müssen, wo immer möglich, anonymisiert oder pseudonymisiert werden, um den Datenschutz zu verbessern. |

### 4. Abnahmekriterien

* **Sicherheitstest**: Überprüfung, ob alle Daten verschlüsselt übertragen und gespeichert werden.
* **Penetrationstests**: Durchführung von Penetrationstests, um Sicherheitslücken zu identifizieren und zu schließen.
* **Zugriffskontrollen**: Überprüfung der Rollen- und Rechteverwaltung auf korrekte Implementierung.
* **Protokollierung**: Überprüfung der Vollständigkeit und Korrektheit der Zugriffprotokolle.

### 5. Risiken und Maßnahmen

| **Risiko** | **Maßnahme** |
| --- | --- |
| Datenlecks | Verschlüsselung der Datenübertragung und -speicherung, regelmäßige Sicherheitsüberprüfungen |
| Unbefugter Zugriff | Implementierung starker Authentifizierungsmethoden und rollenbasierter Zugriffskontrollen |
| Manipulation der Daten | Regelmäßige Integritätsprüfungen und Protokollierung aller Zugriffe |
| Datenschutzverstöße | Schulung der Mitarbeiter, Implementierung von Datenschutzrichtlinien und -verfahren |

### 6. Beteiligte Stakeholder

| **Stakeholder** | **Rolle** | **Verantwortlichkeiten** |
| --- | --- | --- |
| IT-Sicherheitsverantwortlicher | Sicherheitsmanagement | Festlegung und Überprüfung der Sicherheitsanforderungen |
| Systemadministratoren | Technische Unterstützung | Implementierung und Wartung der Sicherheitsmaßnahmen |
| Vertriebsmitarbeiter | Endbenutzer | Nutzung des CRM-Systems und der neuen Scoring-Funktion |
| Vertriebsleiter | Führungskräfte | Analyse und Entscheidungsfindung basierend auf den Scoring-Daten |
| Datenschutzbeauftragter | Datenschutz | Sicherstellung der Einhaltung der Datenschutzbestimmungen |
| Projektleiter | Projektmanagement | Koordination und Überwachung des Projekts |

### 7. Dokumentation und Versionierung

| **Version** | **Datum** | **Beschreibung** |
| --- | --- | --- |
| 1.0 | 19. Mai 2024 | Initiale Version der Sicherheitsanforderungen |
| 1.1 | XX.XXX.XXXX | Anpassungen basierend auf Feedback und neuen Erkenntnissen |

### 8. Vorlagen und Tools

* **Sicherheitsrichtlinien**: Unternehmensrichtlinien zur IT-Sicherheit.
* **Verschlüsselungstools**: Tools zur Datenverschlüsselung (z.B. OpenSSL, GPG).
* **Protokollierungstools**: Tools zur Überwachung und Protokollierung von Zugriffen (z.B. Splunk, ELK Stack).
* **Penetrationstests-Tools**: Tools zur Durchführung von Sicherheitstests (z.B. Metasploit, OWASP ZAP).