Anforderungen an die Softwareentwicklung der TEP Thüringer Energie Speichergesellschaft mbH (Stand: 01/2026)

Thüringer Energie Speichergesellschaft

1. Architektur, Design und Angriffsrisiken

Der Auftragnehmer verpflichtet sich, die Anwendung sicher zu entwerfen und zu entwickeln. Dies umfasst die Identifizierung potenzieller Angriffsrisiken und, als Folge daraus, die Integration von Sicherheitsmaßnahmen gegen diese Angriffsrisiken in die Architektur der Anwendung. Voreinstellungen sind so zu wählen, dass die Option, die ein Angriffsrisiko am wenigsten wahrscheinlich zulässt im Standard eingestellt ist, um die Sicherheit der Anwendung von Beginn an zu gewährleisten. Der Auftragnehmer berücksichtigt dabei den aktuellen Stand der Technik und stetig die aktuellen Entwicklungen, um eine robuste und sichere Architektur zu schaffen.

2. Eingabevalidierung

Der Auftragnehmer verpflichtet sich Funktionen zu implementieren, die Benutzereingaben auf ihr Format und ihre Länge zu überprüfen, um sicherzustellen, dass sie den erwarteten Format- und Inhaltsanforderungen entsprechen. Dies umfasst die Implementierung von Mechanismen zur Validierung von Eingaben, um sicherzustellen, dass keine fehlerhaften oder schädlichen Daten verarbeitet werden. Direkte Verarbeitung von Benutzereingaben ohne vorherige Validierung ist auszuschließen, um Sicherheitsrisiken wie SQL-Injection oder Cross-Site Scripting (XSS) zu verhindern.

3. Authentifizierung und Passwortmanagement

Der Auftragnehmer implementiert ausschließlich Authentifizierungsmechanismen, die effektiv sicherstellen, dass nur berechtigte Benutzer Zugriff auf die Anwendung haben. Authentifizierungsinformationen sind nicht im Klartext im Quellcode zu verwenden. Der Auftragnehmer verpflichtet sich, starke Passwortspeichertechniken zu nutzen, die dem Stand der Technik entsprechen, um Passwörter effektiv zu schützen.

4. Zugriffsmanagement

Der Auftragnehmer stellt sicher, dass Benutzer nur auf die Daten und Funktionen zugreifen können, für die sie berechtigt sind. Dies beinhaltet die Implementierung von rollenbasierten Zugriffsmethoden und verschiedenen Berechtigungsstufen, um Berechtigungen auf das benötigte Minimum beschränken zu können.

5. Kryptografie

Der Auftragnehmer verwendet ausschließlich durch das BSI empfohlene Verschlüsselungsmethoden gemäß der BSI TR-02102 in der jeweils aktuell gültigen Fassung. Dies umfasst die Implementierung bewährter kryptografischer Algorithmen und Techniken, um Daten während der Übertragung und Speicherung zu schützen.

6. Fehler- und Ausnahmebehandlung

Der Auftragnehmer implementiert eine robuste Fehler- und Ausnahmebehandlung, die keine sensiblen Informationen preisgibt und die Anwendung vor Abstürzen schützt. Dies umfasst die Einrichtung von Mechanismen zur Erkennung und Behandlung von Fehlern, die die Anwendung stabil halten und ausschließt, dass vertrauliche Informationen in Fehlermeldungen angezeigt werden.

7. Sitzungsmanagement

Der Auftragnehmer stellt sicher, dass Sitzungen sicher verwaltet werden, einschließlich der Generierung, Speicherung und Invalidierung von Sitzungs-IDs. Sitzungsdaten sind vor unbefugtem Zugriff zu schützen, indem Maßnahmen wie die Verwendung von HTTPS und die Implementierung von Sitzungs-Timeouts ergriffen werden. Der Auftragnehmer stellt sicher, dass Sitzungsinformationen nicht in URLs oder anderen unsicheren Speicherorten gespeichert werden.

8. Datenübertragung

Der Auftragnehmer nutzt sichere Kommunikationsprotokolle wie HTTPS, um Daten während der Übertragung zu schützen. Dies umfasst die Implementierung von TLS-Verschlüsselung, um sicherzustellen, dass alle Datenübertragungen zwischen Client/Server und Server sicher sind. Der Auftragnehmer stellt sicher, dass keine Übertragung sensibler Daten über unsichere Kanäle erfolgt, um das Risiko von Datenverlust oder -diebstahl zu minimieren.

9. Sicherheitskonfiguration

Der Auftragnehmer vermeidet Standardkonfigurationen, die möglicherweise unsicher sind. Genutzte Entwicklungsumgebungen, Bibliotheken, Pakete und Protokolle müssen sich noch in der Wartung durch den Hersteller befinden. Bei der Auswahl dieser sind die Produkte mit den höchsten Sicherheitsstandards zu berücksichtigen, wobei ein Nachweis beispielsweise, aber nicht abschließend über unabhängige Prüfungen, wie Penetrationstests oder Zertifikate, erfolgen kann.

10. Protokollierung und Überwachung

Der Auftragnehmer implementiert umfassende Protokollierungsfunktionen (Logging) sicherheitsrelevanter Ereignisse, um verdächtige Aktivitäten zu erkennen und zu verhindern.

11. Sicherheitsbewusstsein und Schulung

Der Auftragnehmer fördert ein Sicherheitsbewusstsein im gesamten Entwicklungsteam und schult regelmäßig in sicheren Programmierpraktiken. Spezielle programmiersprachenabhängige Praktiken und Vorgaben, wie SAP Clean Code oder OWASP Coding Practices, sind im Vorfeld mit dem Auftraggeber abzustimmen und entsprechend der Absprache während der Entwicklung anzuwenden.

12. Systemlandschaften und Paketmanagement

Die Entwicklung hat in mehrstufigen Systemlandschaften zu erfolgen. Es ist mindestens eine Trennung zwischen Produktions- und Entwicklungssystemen abzubilden, beispielsweise in getrennten virtuellen oder physischen Umgebungen. In Abhängigkeit von der jeweiligen Sprache/Umgebung ist zu prüfen, ob Paketmanager verfügbar sind, die zur automatisierten Installation, Deinstallation und Aktualisierung von Software verwendet werden sollten.

13. Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Dokumentes ungültig/undurchführbar sein oder werden, so bleiben die übrigen Bestimmungen wirksam.
Die Parteien sind verpflichtet, die ungültige/undurchführbare Bestimmung vom Beginn der Ungültigkeit/Undurchführbarkeit an durch eine wirtschaftlich möglichst gleichartige Bestimmung zu ersetzen. Dasselbe gilt für Regelungslücken.