Abschlussprojekt Security By Design Dokumentation

Electricity Provider

Teilnehmer in dem Projekt sind

Kevin Wagner / Kai Pistol / Luis Eckert / Cynthia Winkler

Betreuender Dozent
Herr Schneider

Zusammenfassung

In der folgenden Dokumentation geht es um die Entwicklung eines Stromanbieterportals für einen fiktiven Stromanbieter. Die Webanwendung baut auf dem Django / React - Framework auf und soll auf allen Geräten mit einem modernen Webbrowser aufrufbar sein. Des Weiteren soll eine Schnittstelle zu einem Messstellenbetreiber impleementiert werden, um Daten Messdaten für das Portal abrufen zu können.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einführung

1.1 Aufgabenstellung

1. Identifizieren, präzisieren und dokumentieren Sie zunächst die in diesem Geschäftsumfeld (business context) zu erwartenden zu schützenden Objekte, deren Schutzziele und Sicherheitsanforderungen. Berücksichtigen Sie dabei auch Ihnen bekannte rechtliche und regulatorische Vorschriften (regulatory context). Entwerfen Sie dann eine geeignete Architektur und wählen Sie eine geeignete Technologie bzw. Plattform zur Realisierung der Anwendung (technology context). Überprüfen und ergänzen Sie zu schützende Objekte, Schutzziele und Sicherheitsanforderungen mittels einer architektonischen Bedrohungsanalyse (threat modeling).

2. Erstellen Sie ausgehend von den Ergebnissen der architektonischen Bedrohungsanalyse ein Register für die in Ihrem Projekt identifizierten Sicherheitsrisiken. Bestimmen Sie dazu Eintrittswahrscheinlichkeit und mögliche Schäden der identifizierten Bedrohungen und das daraus resultierende Risiko. Entscheiden Sie für jedes Risiko wie es behandelt werden soll und im Falle einer Reduzierung, welche Maßnahmen dafür durchgeführt werden und wie diese überprüft werden sollen. Dokumentieren Sie Ihre Ergebnisse im Risikoregister Ihres Projektes.

3. Implementieren Sie die Anwendung unter Berücksichtigung der identifizierten Anforderungen, Risiken, den zur Risikobehandlung festgelegten Maßnahmen und allgemeinen Grundlagen sicheren Programmierens.

4. Testen und überprüfen Sie die Anwendung hinsichtlich der Grundfunktionalität, den identifizierten Sicherheitsanforderungen und den zur Risikobehandlung implementierten Maßnahmen. Erstellen Sie dazu einen Testplan, nutzen Sie geeignete Testmethoden und - werkzeuge und dokumentieren Sie die Testergebnisse.

5. Führen Sie die Schritte 1.-4. im Entwicklungs- und Bereitstellungsprozess in geeigneter Weise verzahnt und wiederholt durch.

1.2 Konkrete Abgaben

25.10.2023:

- Beschreibung der zu schützenden Objekte (Assets), deren Schutzziele und Sicherheitsanforderungen der Anwendung
- Architekturbeschreibung, -diagramm
- Wahl der Technologie zur Implementierung, Plattform, Komponenten
- Risikoregister

10.12.2023: Präsentation - freies Format + Dateien bzw. Angabe GitHub Repository

- Beschreibung der Modulstruktur, Build-Prozess und -Einstellungen
- Source Code (inklusive Build-Skript)
- Testplan
- Testergebnisse

2 Projektplanung

Die grundlegende Planung des Projektes wurde in Github vorgenommen. Hierbei wurden diverse Tasks für die einzelnen Mitglieder erstellt und die Projektrollen zugeordnet. Von der Planung zur Umsetzung fanden folgende Schritte statt:

1. Anforderungen Projekt in Github festlegen
2. Festlegen der zu schützenden Objekte, deren Schutzziele und Sicherheitsanforderungen
3. Festlegen der regulatorischen Vorschriften für die spätere Umsetzung
4. Festlegen der Architektur und zu nutzenden Technologien.
5. Definieren von Use Cases
6. Erstellung der Moqups
7. Erstellung von Klassendiagrammen
8. Übergang zur Coding-Phase anhand der vorab definierten Vorgehensweise
9. Erstellung der Dokumentation in Latex

3 Architektur

In diesem Abschnitt wird die Architektur des Systems und die darin anzufindenen Komponenten näher beschrieben.

3.1 Web Client A

Client A ist das Kundenportal und die Besucherwebseite. Ersteres ist Kunden vorbehalten. Letzteres kann öffentlich eingesehen werden, da es als Informationsquelle zu gebotenen Tarifen für Besucher und potentielle Kunden angedacht ist. Im Kundenportal können Daten wie eigenen Verträge, Stromzählermesswerte, Rechnungen und Abschläge eingesehen und verwaltet werden.

3.2 Web Client B

Das Mitarbeiterportal wird getrennt vom Kundenportal gehostet greift allerdings auf die selbe Datenbank zu. Der genaue Busineskontext der Mitarbeiterportals muss erst noch genauer ausgearbeitet werden.

3.3 Backend (API)

Das Backend wird zwar als eine Komponenten in der Architektur beschrieben, ist aber tatsächlich zweigeteilt. Es gibt ein Backend für das Kundenportal und eines für das Mitarbeiterportal. Der Grund für die Trennung ist der, dass das Mitarbeiterportal nur innerhalb des Firmennetzes erreichbar sein soll während das Kundenportal öffentlich verfügbar sein muss. Der Sicherheitsvorteil liegt darin, dass das System weniger Angriffsfläche nach außen bereitstellt.

3.4 Datenbank

Die zentrale Datenbank wird sowohl für das Kunden- als auch das Mitarbeiterportal zum speichern von Daten verwendet.

3.5 Messdatenanbieter API

Das erheben der Stromzählermessdaten wird zu einem externen Unternehmen ausgelagert, das die erforderlichen Messdaten über eine gesicherte Rest API bereitstellt.

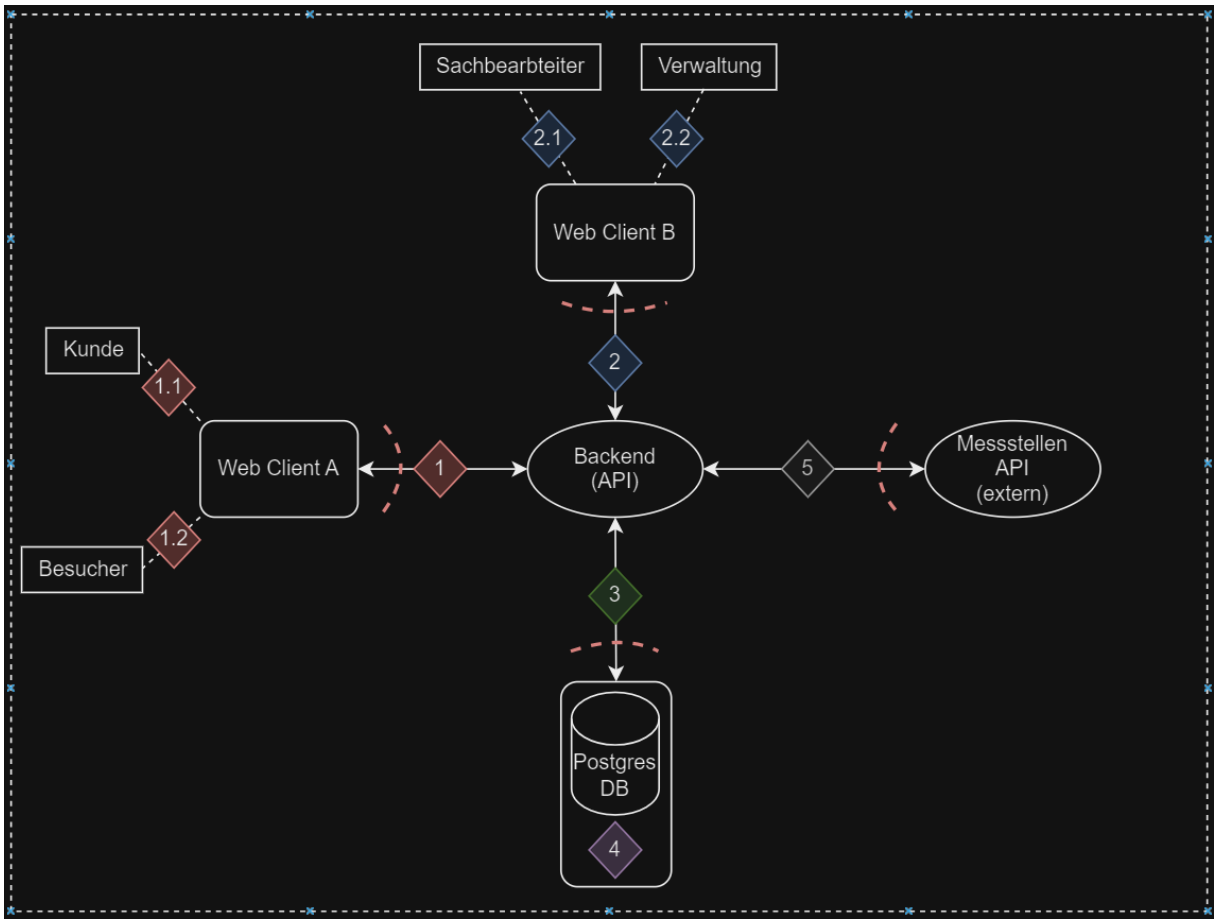

Abbildung 1: Architekturdiagramm

Assets	
ID	**Description**
A01	Zugangsdaten Kunde
A02	Messtellen API Secret
A03	Zugangsdaten Mitarbeiter
A04	DB Secret
A05	Tarifinformationen
A06.0	Kundendaten (Vertragsdaten)
A06.1	Kundendaten (Person)
A06.2	Kundendaten (Bankdaten)
A06.3	Kundendaten (Messdaten)
A06.4	Kundendaten (Rechnungen)
A07	Zugangsdaten DB Admin

Abbildung 2: Liste der Assets

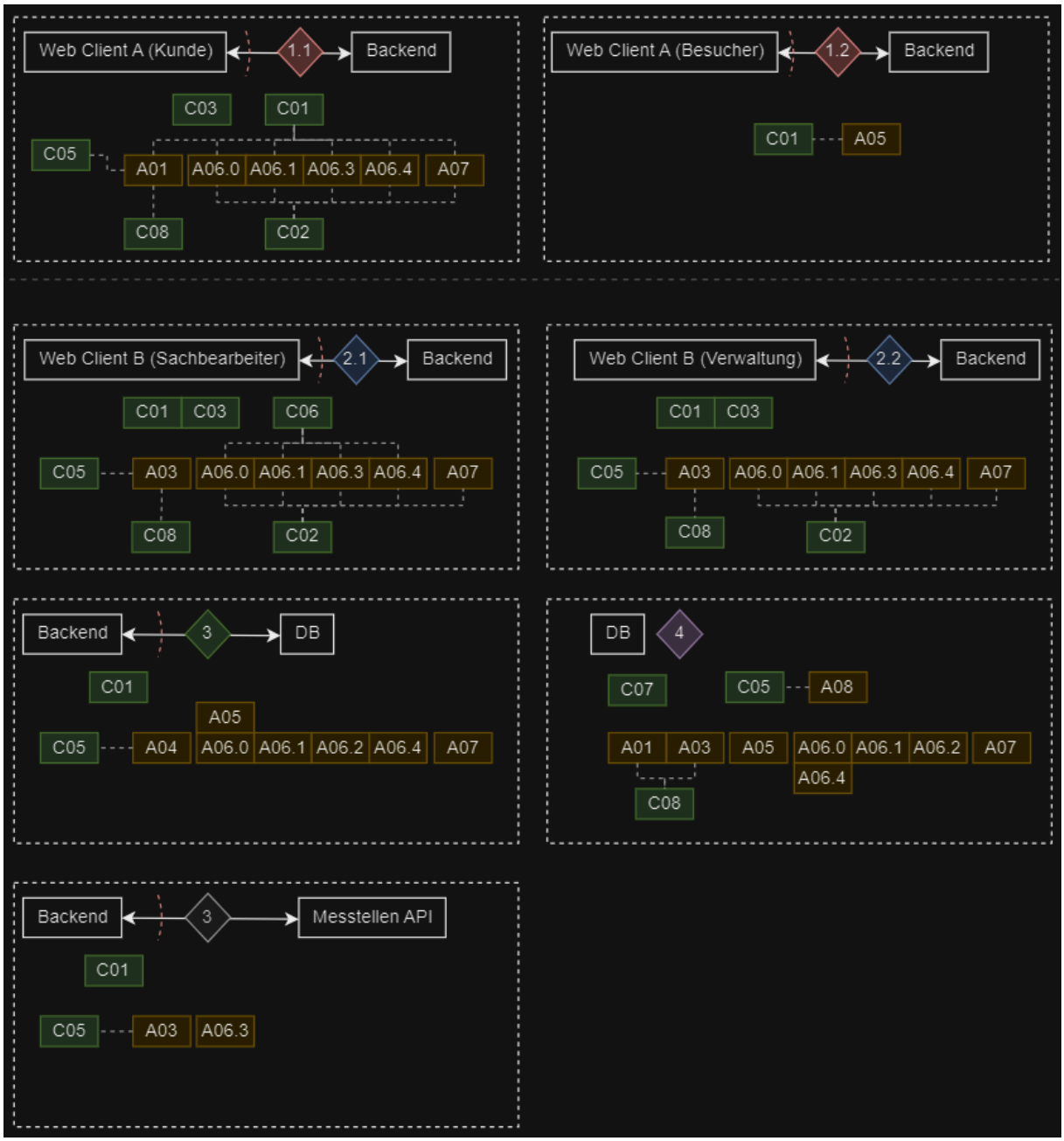

Abbildung 4: Zuteilung der Assets & Security Controls zu den Schnittstellen

Security Controls	
ID	**Description**
C01	TLS >= 1.3
C02	Input Validation
C03	DDOS Protection
C04	Cookie Security (https & secure only)
C05	Authentifizierung
C06	Autorisierung
C07	Verschlüsselung
C08	Hashing (Argon2)

Abbildung 3: Liste der Security Controls

4 Gewählte Technologien

4.1 Docker

Docker ist eine Container-Software. Diese Container ermöglichen es, bestimmte Softwarekomponenten (Webserver, Programmiersprachen und Datenbanken) ohne den Overhead einer virtuellen Maschine auszuführen. Durch die Verwendung von Docker kann innerhalb des vorliegenden Projektes auf die Nutzung einer virtuellen Maschine oder eines Webservers verzichtet werden, zumindest bei der Entwicklung. Die für das Stromanbieter-Portal benötigten Komponenten sind in dem von uns für das Projekt erstellten Docker -Container enthalten. Docker wird innerhalb des Projektes genutzt, um die Entwicklungs- / Hostsysteme unter den Entwicklern homogen zu gestalten, sodass mit möglichst wenig Aufwand der Tech-Stack stabil bei jedem Entwickler läuft. Des Weiteren wird das Auftreten von vielen Fehlern auf den lokalen Maschinen der Entwickler verhindert.

4.2 Python-Django (Backend)

Django ist ein in Python geschriebenes Webframework, welches dem sogenannten Model-View-Presenterschema folgt. Dabei handelt es sich um ein Entwurfsmuster in der Softwareentwicklung, das aus dem Model View Controller (MVC) hervorgegangen ist. Das Django Framework soll für das Backend genutzt werden und dient zur Verwaltung der eigentlichen Anwendung.

4.3 React.js (Frontend)

React.js ist eine JavaScript-Bibliothek, die für die Erstellung von von Benutzeroberflächen genutzt wird. In dem vorliegenden Projekt wird React.js für die Erstellung des Frontend genutzt. Eine React-Anwendung besteht aus wiederverwendbaren Komponenten, welche die Teile der Benutzeroberfläche bilden, mit denen der Nutzer interagiert. Durch die Nutzung von React.js wird die Entwicklung vereinfacht, da wiederkehrender Code nicht wiederholt geschrieben werden muss.

4.4 PostgreSQL-Datenbank

PostgreSQL ist ein Open-Source-Objektrelationsdatenbanksystem. Ein Vorteil von diesem Datenbank-Managementsystem ist, dass die Datenbankgröße nicht durch das System, sondern durch den zur Verfügung stehenden Speicher begrenzt wird. Die Datenbank wird über die in das Framework Django integrierte Datenbankabstraktions-API angesprochen mit dem Objekte erstellt, aktualisiert oder gelöscht werden können. Eine Umstellung auf ein anderes DBMS (Datenbankmanagementsystem) wäre aufgrund der dynamisch durch Django generierten Abfragen möglich, da kein natives SQL ausgeführt wird.

5 Assets, Schutzziele und Sicherheitsanforderungen

Asset	Schutzziele	Sicherheitsanforderungen
Persönliche Kundendaten	Vertraulichkeit Integrität Verfügbarkeit Authentizität Identität	• Zugriffskontrolle: Die Daten können nur vom Kunden und autorisiertem Personal bearbeitet werden • Verschlüsselung: Datenverschlüsselung während der Übertragung & Ruhezustand • Datensicherung & Wiederherstellung: regelmäßige Sicherung zur Vorbeugung von Datenverlusten, Notfallwiederherstellungspläne • Überwachung, Protokollierung: Überwachungssysteme, Protokollierung zur Erkennung nicht autorisierter Aktivitäten • DPIA - Datenschutz- Folgeabschätzung • Transparenz, Informationspflichten: Betroffene müssen über Erhebung, Verarbeitung der Daten informiert werden, mit Angabe des Verwendungszweckes (EnWG)

Bankdaten	Vertraulichkeit Integrität Verfügbarkeit Authentizität Verbindlichkeit	• Zugriffskontrolle: Die Daten können nur vom Kunden und autorisiertem Personal bearbeitet werden • Verschlüsselung: Datenverschlüsselung während der Übertragung & Ruhezustand • Datensicherung & Wiederherstellung: regelmäßige Sicherung zur Vorbeugung von Datenverlusten, Notfallwiederherstellungspläne • Überwachung, Protokollierung: Überwachungssysteme, Protokollierung zur Erkennung nicht autorisierter Aktivitäten • DPIA - Datenschutz-Folgeabschätzung
Vertragsdaten	Vertraulichkeit Integrität Verfügbarkeit Authentizität Verbindlichkeit Identität	• Zugriffskontrolle: Die Daten können nur von autorisiertem Personal bearbeitet und vom Kunden eingesehen werden • Verschlüsselung: Datenverschlüsselung während der Übertragung & Ruhezustand • Datensicherung & Wiederherstellung: regelmäßige Sicherung zur Vorbeugung von Datenverlusten, Notfallwiederherstellungspläne • Überwachung, Protokollierung: Überwachungssysteme, Protokollierung zur Erkennung nicht autorisierter Aktivitäten • DPIA - Datenschutz-Folgeabschätzung

Messdaten	Vertraulichkeit Integrität Verfügbarkeit Identität	• Datenschutz: Schutz der Messdaten vor unbefugtem Zugriff, Diebstahl; Zugriffskontrollen (Daten können nur von autorisiertem Personal & Kunden eingesehen werden) • Datensparsamkeit: Erfassung, Speicherung nur von notwendigen Messdaten • Transparenz, Informationspflichten: Betroffene müssen über Erhebung, Verarbeitung der Daten informiert werden, mit Angabe des Verwendungszweckes (EnWG) • Rechte der Betroffene (DSGVO): Recht auf Auskunft, Recht auf Berichtigung und Löschung, Recht auf Verarbeitungseinschränkung der Daten, Recht auf Widerspruch der Datenverarbeitung und Recht auf Datenübertragbarkeit • DPIA - Datenschutz-Folgeabschätzung
Systemschnittstellen	Vertraulichkeit Integrität Verfügbarkeit Widerstandsfähigkeit	• Zugriffskontrolle • Gesicherte Kanäle: Zugriff nur über verschlüsselte Kanäle • DB, Mitarbeiterportal ist nicht nach außen verfügbar

Produktivsystem	Vertraulichkeit Integrität Verfügbarkeit Verbindlichkeit Widerstandsfähigkeit Autorisierung	• Zugriffskontrolle/Rollenverteilung • Validierung/Bereinigung User Eingaben • Schutz vor DDOS-Angriffen
Testsystem	Vertraulichkeit Anonymität	• nicht von außen verfügbar, nur für Entwickler und Tester zugänglich • System darf nur mit verfremdeten Daten arbeiten

5.1 Regularien

Stromanbieter gehören zu den kritischen Infrastrukturen (KRITIS). Daraus leiten sich verschiedene Regularien ab, die zwingend erfüllt sein müssen. Die Überwachung der Umsetzung und Instandhaltung übernimmt das BSI. Die Grundinformationen zur KRITIS Unternehmen sind im IT-Sicherheitsgesetz 2.0 zu finden. Zusätzlich dazu gibt es weitere wichtige Regularien. Diese sind im Folgenden aufgezählt mit einer kurzen Erklärung, was sie beinhalten bzw. vorschreiben.

- IT-Sicherheitsgesetz 2.0: Sicherheitsmindestanforderungen, Meldepflicht von Sicherheitsvorfällen, Notwendigkeit zur Einrichtung von Security Information und Event Management Systemen (SIEM-Systemen) zur Angriffserkennung und Angriffsbewältigung
- DSGVO/ BDSG: Grundsätzliches zum Datenschutz
- PCIDSS: Umgang mit Bankdaten
- Energiemarkt auf Grundlage des Energiewirtschaftsgesetzes (EnWG): Regelung des Energiemarktes, nur wichtig Umgang mit erhobenen Daten(Infos); Überschneidung DSGVO
- ISO 27001: Entwicklung, Umsetzung, Instandhaltung eines ISMS
- ISO/IEC 27034-1: Informationstechnik - IT Sicherheitsverfahren - Sicherheit von Anwendungen
- ISO 15408: steht für die Durchführung von Evaluierungen und Zertifizierungen von IT-Produkten zur Verfügung
- EU Cyber Resilience Act: Anforderungen an Cybersecurity für Produkte mit digitalen Elementen
- NIS2:Cybersicherheit
- NIST:
  - NIST Cybersecurity Framework: bietet Praktiken zur Verbesserung Cybersicherheit an
  - NIST SP 800-82: Leitlinien zur Sicherung von Industriesteuerungssystemen (ICS)
- BSI - TR-03109-1: Regulierungen für Smartmeter

6. Risiko Register

Auswirkungen Eintrittswahrscheinlichkeit	Niedrig	Mittel	Hoch	Sehr hoch
Sehr hoch	Niedrig	Mittel	Hoch	Sehr hoch
Hoch	Niedrig	Mittel	Hoch	Hoch
Mittel	Niedrig	Niedrig	Mittel	Mittel
Niedrig	Niedrig	Niedrig	Niedrig	Niedrig

RisikoID	**Bedrohung**	**Eintrittswahrscheinlichkeit**	**Auswirkungen**	**Risiko**	**Behandlung**
[RId]	[Kurztext]	[Sehr hoch] [Hoch] [Mittel] [Niedrig]	[Sehr hoch] [Hoch] [Mittel] [Niedrig]	[Sehr hoch] [Hoch] [Mittel] [Niedrig]	[Vermeiden] [Reduzieren] [Transferieren] [Akzeptieren]
Beschreibung					
[Text]					
Anforderungen					
[Text]					
Maßnahmen				Überprüfung	TestID
[Text]				[Manueller Test] [Automatisierter Test] [Pentest] [Design Review] [Code Review] […]	[TId]

Risiko ID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R1	A01 - Zugangsdaten Kunde – Bruteforce Angriffe	Hoch	Mittel	Hoch	Reduzieren
Beschreibung					
Angreifer können mittels Brute Force oder Wörterbuchangriffen Passwörter der Kunden erraten					
Anforderungen					
Das System muss solche Angriffe erkennen und den Account nach mehrmaligen Versuchen sperren					
Maßnahmen				Überprüfung	TestID
Etablierung von Log2Fail mit 5 Versuchen bevor ein neues Passwort vergeben werden muss					

Risiko ID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R2	A01 - Zugangsdaten Kunde – SQL Injections	Sehr Hoch	Hoch	Sehr Hoch	Vermeiden
Beschreibung					
Angreifern können unter Verwendung von SQL-Injections den Login umgehen und sich Zugriff auf den Kundenaccount verschaffen.					
Anforderungen					
Das System muss einen solchen Angriff unterbinden und darf keine Injections zulassen.					
Maßnahmen				Überprüfung	TestID
Eingaben auf Clientseite werden prinzipiell als String übergeben, ohne die Möglichkeit, eine Injection durchzuführen.					

Risiko ID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R3	A03 - Zugangsdaten Mitarbeiter– Bruteforce Angriffe	Hoch	Mittel	Hoch	Reduzieren
Beschreibung					
Angreifer können mittels Brute Force oder Wörterbuchangriffen Passwörter der MItarbeiter erraten					
Anforderungen					
Das System muss solche Angriffe erkennen und den Account nach mehrmaligen Versuchen sperren					
Maßnahmen				Überprüfung	TestID
Etablierung von Log2Fail mit 5 Versuchen bevor ein neues Passwort vergeben werden muss					

Risiko ID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R4	A03 - Zugangsdaten Kunde – SQL Injections	Hoch	Hoch	Hoch	Vermeiden
Beschreibung					
Angreifern können unter Verwendung von SQL-Injections den Login umgehen und sich Zugriff auf den Mitarbeiter Account verschaffen.					
Anforderungen					
Das System muss einen solchen Angriff unterbinden und darf keine Injections zulassen.					
Maßnahmen				Überprüfung	TestID
Eingaben auf Clientseite werden prinzipiell als String übergeben, ohne die Möglichkeit, eine Injection durchzuführen.					

Risiko ID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R5	A03 - Zugangsdaten Mitarbeiter – Login außerhalb des Netzwerks	Hoch	Hoch	Hoch	Vermeiden
Beschreibung					
Angreifer können sich Zugriff von außerhalb des Netzwerks auf den Login der Mitarbeiter Zugriff verschaffen					
Anforderungen					
Der Login für Mitarbeit darf nur für Nutzer des firmeneigenem Netzwerks zugänglich sein.					
Maßnahmen				Überprüfung	TestID
Der Mitarbeiter Client ist nur innerhalb des Firmennetzwerks zugänglich, welches durch ein VPN mittels vorheriger MFA Authentifizierung erreicht werden kann.					

Risiko ID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R6	A03 - Zugangsdaten Mitarbeiter – Privilegierte Nutzerrechte	Hoch	Hoch	Hoch	Reduzieren
Beschreibung					
Angreifer können bewusst versuchen, die Daten von priviligierten Nutzern zu erhalten.					
Anforderungen					
Privilegierte Accounts müssen besonders geschützt und gelogged werden.					
Maßnahmen				Überprüfung	TestID
Ein einheitliches Nutzerrechtemanagement wird durch die Verwendung eines ISM und eines PAM gewährleistet, sodass Nutzer nur privilegierte Rechte auf anfrage erhalten.					

Risiko ID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R7	A06.1 - Kundendaten (Person)– Widerrechtliche Änderung	niedrig	niedrig	niedrig	Reduzieren
Beschreibung					
Angreifer können, nachdem Sie die Kontrolle über einen Account gewonnen haben, die personenbezogene Daten des Kunden ändern.					
Anforderungen					
Es muss sichergestellt werden, dass die Änderung von personenbezogenen Daten nicht ohne das konkrete Einverständnis und die Erbringung eines Nachweis des Kunden vorgenommen werden.					
Maßnahmen				Überprüfung	TestID
Die Änderung von personenbezogenen Daten können durch ein Formular beantragt werden und müssen durch das Einreichen eines entsprechenden Nachweises validiert werden.					

Risiko ID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R8	A06.1 - Kundendaten (Person)– Übersendung von Schadsoftware bei der Nachweiserbringung	Mittel	Hoch	Hoch	Reduzieren
Beschreibung					
Angreifer können bei der Nachweiserbringung Schadsoftware in den Anhang hochladen, welche durch einen Mitarbeiter zur Ausführung gebracht werden könnte.					
Anforderungen					
Es muss sichergestellt werden, dass keine Schadsoftware hochgeladen werden kann und die Anhänge in einer isolierten Umgebung gespeichert werden.					
Maßnahmen				Überprüfung	TestID
Beim Upload der Nachweise wird eine MIME-Type Validierung vorgenommen, um zunächst die Echtheit des Datentyps zu validieren. Des Weiteren wird sichergestellt, dass das File Limit gedeckelt ist um DOS Angriffe vorzubeugen. Ebenfalls wird die Signatur der hochgeladenen Datei geprüft, um					
zusätzlich sicherzustellen, dass es sich dabei wirklich um den angegebenen Dateityp handelt.					

Risiko ID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R9	A06.2 - Kundendaten (Bankdaten)– Widerrechtliche Änderung	niedrig	mittel	mittel	Reduzieren
Beschreibung					
Angreifer können, nachdem Sie die Kontrolle über einen Account gewonnen haben, die Bankdaten Daten des Kunden ändern.					
Anforderungen					
Es muss sichergestellt werden, dass die Änderung von Bankdaten nicht ohne das konkrete Einverständnis des Kunden vorgenommen werden.					
Maßnahmen				Überprüfung	TestID
Die Änderung von Bankdaten kann durch ein Formular beantragt werden und ggf. durch die Vergabe eines SEPA-Lastschriftmandats ergänzt werden.					

Risiko ID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R10	A06.3 - Kundendaten (Messdaten) - Widerrechtliche Änderung	niedrig	niedrig	niedrig	Reduzieren
Beschreibung					
Angreifer können, nachdem Sie die Kontrolle über einen Account gewonnen haben, weitere Messstationen hinzufügen oder kündigen.					
Anforderungen					
Es muss sichergestellt werden, dass jegliche Änderung von Messstationen protokolliert wird und es zu jeder Messstation einen Vertrag gibt.					
Maßnahmen				Überprüfung	TestID
Die Änderung von Messstationen wird dem Kunden sowohl per Mail als auch postalisch mitgeteilt, beim Hinzufügen einer neuen Messstation wird dem Kunden ein neuer Vertrag zugesendet, welchen er vorher ausfüllen muss.					

6 Glossar

7 Quellen

- Öggl Bernd, Koffler Michael: Docker - Das Praxisbuch für Entwickler
- Ernesti Johannes, Kaiser Peter: Python3 - Das umfassende Handbuch