Security by Design - (Gruppe 1, Stromanbieter)

Liste der zu schützenden Assets:

1. **Kundenportal**

Beschreibung: Webserver, über den die eigenen Daten eingesehen werden können.
Es existiert ein Rollenkonzept um zu verschiedenen Informationen des Servers Zugriff zu erlangen

Schutzziele: Verfügbarkeit, Widerstandsfähigkeit, Vertraulichkeit, Integrität, Identität, Authentizität

Technologie: Python für Webserver, Frontend auf Clientseite Javascript

Intangible Assets: Anmeldedaten, Admin Anmeldedaten, Verbindungsdaten

Regulatorischer Kontext: DSGVO (Verschlüsselung Übertragungswege, Least privilege, Privacy by Default), Digitaler Verbraucherschutz

2. **API für Datenaustausch mit Stromzählerbetreiber**

Beschreibung: Dienst zum Austausch mit dem Stromzählerbetreiber bezüglich relevanter Daten

Schutzziele: Authentizität, Integrität, Vertraulichkeit

Technologie: Access Token austausch für die Authentifizierung, Datenformat ist JSON

Intangible Assets: Access Token, Stromzählerdaten, Kundendaten

Regulatorischer Kontext: DSGVO (sicherer Export, Verschlüsselung Übertragungswege, Identifizierung), NIS2 (Supplier)

3. **Datenbank für Konfigurations- Logdaten**

Beschreibung: Schnittstelle zwischen Kundenportal und Webserver, damit die entsprechenden Informationen im Kundenportal aufgerufen werden können. Hier werden zudem entsprechende Änderungen geloggt.

Schutzziele: Integrität, Verbindlichkeit, Vertraulichkeit, Verfügbarkeit

Technologie: MySQL, Logdatenerfassung via Python

Regulatorischer Kontext: DSGVO (Logging von Änderungen, Privacy by Default)

Intangible Assets: Konfigurationsdaten, Logdaten

4. Datenbank für Kundendaten

Beschreibung: Hier werden alle Informationen, die für den Webserver relevant sind, hinterlegt.

Schutzziele: Vertraulichkeit, Privatheit, Integrität, Authentizität, Verfügbarkeit,

Regulatorischer Kontext: DSGVO (Least privilege, Verschlüsselung aller Übertragungswege, Sicheres Löschen, Lösung für Export, Identifizierung, Pseudonymisierung für Testfälle)

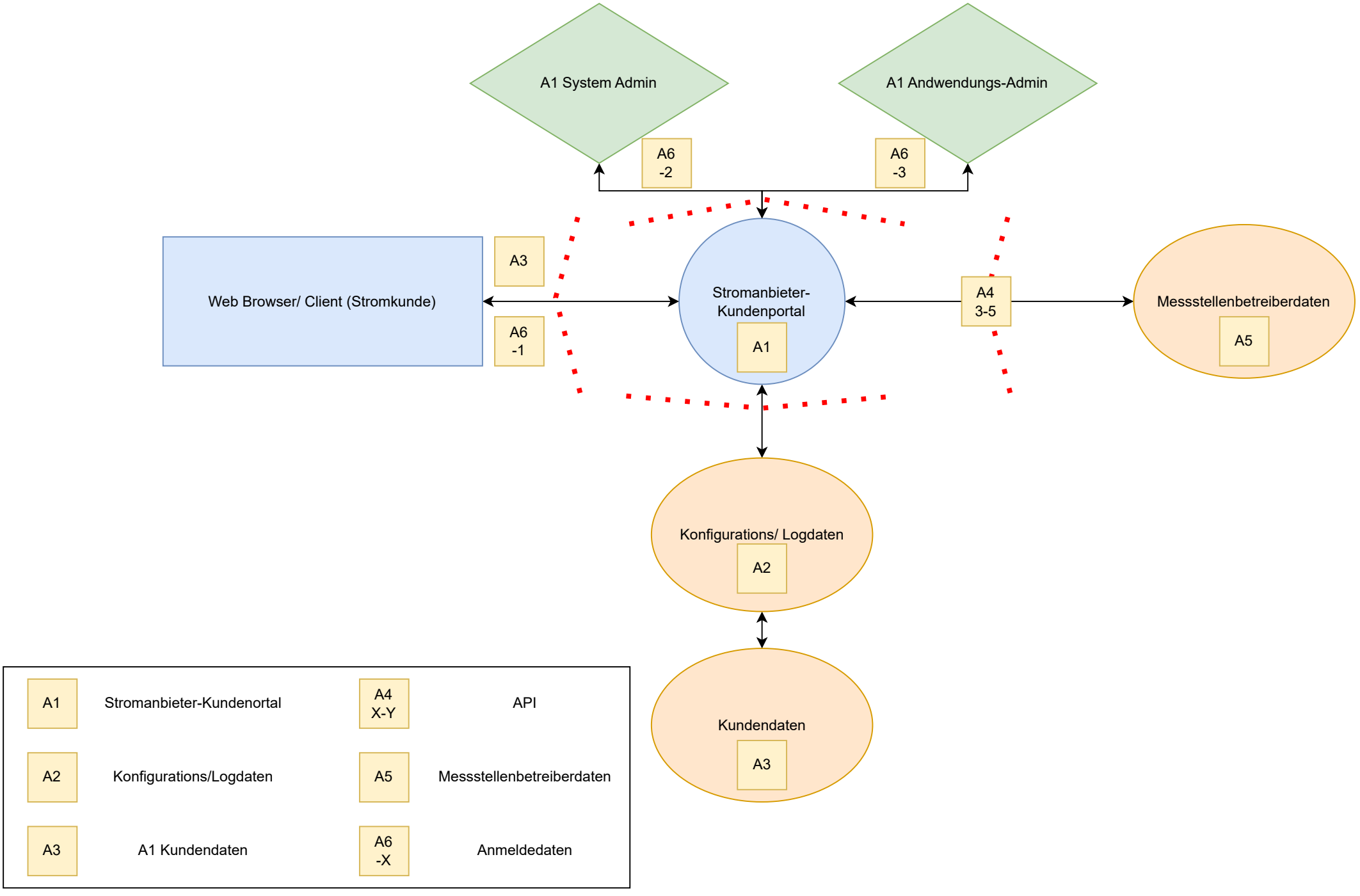
Technologie: MySQL

Intangible Assets: Anmeldedaten, Admin Anmeldedaten, Stromzählerdaten, Kundendaten

Allgemeiner Regulatorischer Kontext

Stromanbieter zählen zu Kritis Unternehmen. Dies bedeutet NIS2 und das IT-Sicherheitsgesetz sind ebenfalls relevant. Daraus ergeben sich folgende Pflichten:

- Regelmäßige Risikobewertung und Audits
- Sicherstellung der Informationssicherheit in Lieferkette
- Cybersicherheit an Normen anlehnen (bspw. ISO 27001)
- Meldepflicht


A1 System Admin
A1 Andwendungs-Admin
A6
-2
A6
-3
Web Browser/ Client (Stromkunde)
A3
A6
-1
Stromanbieter-
Kundenportal
A1
A4
3-5
Messstellenbetreiberdaten
A5
Konfigurations/ Logdaten
A2
Kundendaten
A3
A1
Stromanbieter-Kundenortal
A4
X-Y
API
A2
Konfigurations/Logdaten
A5
Messstellenbetreiberdaten
A3
A1 Kundendaten
A6
-X
Anmeldedaten

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R1	Überlastung des Webservers	Hoch	Mittel	Mittel	Reduzieren
Beschreibung					
Zu viele Anfrage führen zum Absturz des Servers					
Anforderungen					
Robustheit, Verfügbarkeit					
Maßnahmen				Überprüfung	TestID
Load-Balancer / Verteilung der Last auf mehrere Server				Pentest(DoS-Angriff)	T01

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R2	Einführung von Schadcode	Sehr hoch	Sehr hoch	Sehr hoch	Reduzieren
Beschreibung					
Injection Angriffe					
Anforderungen					
Verhinderung der Einführung von Schadcode, Wahrung der Integrität					
Maßnahmen				Überprüfung	TestID
Input Validierungen				Pentest, Code Review	T02

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R3	Unbefugter Zugang zum Kundenportal (Nutzeraccount)	Sehr hoch	Mittel	Mittel	Reduzieren
Beschreibung					
Bruteforce Angriffe					
Anforderungen					
Sicheres Login bzw. sicherer Loginvorgang					
Maßnahmen				Überprüfung	TestID
Passwortanforderungen, Limitierung der Anmeldeversuche, Hash und Salt für PWs in DB				-	-

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R4	Unbefugter Zugang zum Kundenportal (Adminaccount)	Sehr hoch	Sehr hoch	Sehr hoch	Reduzieren
Beschreibung					
Bruteforce Angriffe					
Anforderungen					
Erhöhte Schutzmaßnahmen für Adminaccounts					
Maßnahmen				Überprüfung	TestID
Zusätzlich zu R3 verpflichtende MFA				-	-

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R5	Unautorisierte Rollenänderung	Sehr hoch	Sehr hoch	Sehr hoch	Reduzieren
Beschreibung					
Unbefugte Accounts können sich weitere Rechte zuweisen					
Anforderungen					
Nur berechtigte Accounts mit Adminrechten					
Maßnahmen				Überprüfung	TestID
Privileged Access Management (Loggen und Verwalten von Rechteänderungen)				Pentest	T03

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
D1	Manipulation der Kundendaten	Sehr hoch	Mittel	Mittel	Reduzieren
Beschreibung					
Nutzer kann die Daten seiner Stromzähler manipulieren					
Anforderungen					
Wahrung der Integrität der Kundendaten					
Maßnahmen				Überprüfung	TestID
Hashing der Stromzählerdaten -> Erkennung von Manipulation				-	-

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
D2	Offenlegung der Kundendaten	Hoch	Sehr hoch	Hoch	Reduzieren
Beschreibung					
Leak der Datenbank					
Anforderungen					
Datenschutz, Compliance					
Maßnahmen				Überprüfung	TestID
Absichern der Datenbank (Zugriffskontrolle usw.)				Pentest	T04

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
L1	Manipulation der Logdaten	Hoch	Mittel	Mittel	Reduzieren
Beschreibung					
Logdaten werden unbemerkt manipuliert					
Anforderungen					
Wahrung der Integrität der Logdaten					
Maßnahmen				Überprüfung	TestID
Signatur				Code Review	T05

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
L2	Offenlegung der Logdaten	Sehr hoch	Niedrig	Niedrig	Akzeptieren
Beschreibung					
Leak der Logdaten					
Anforderungen					
-					
Maßnahmen				Überprüfung	TestID
-				-	-