Bedrohungsmodell - OTT Auth

Owner: Firma Allsecure
Reviewer: Georg Neugebauer
Contributors: Georg Neugebauer, Tri Nam Tran
Date Generated: Fri Nov 21 2025

Executive Summary

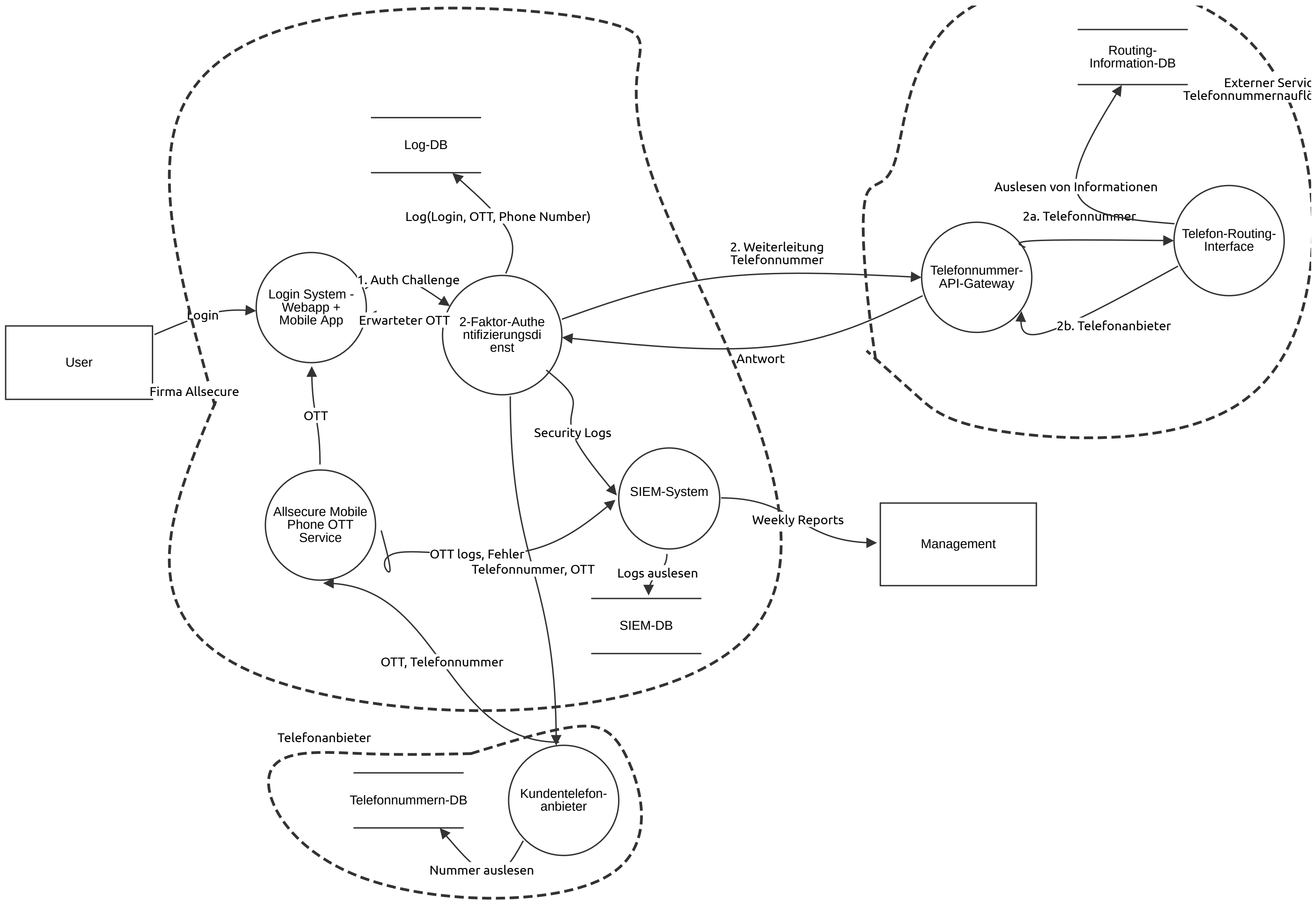
High level system description

Die Firma Allsecure betreibt unterschiedliche Anwendungen mit Hilfe einer 2-Faktorauthentifizierung via One-time token, der an das entsprechende Smartphone des Nutzers geschickt wird.

Summary

Total Threats	8
Total Mitigated	8
Total Open	0
Open / Critical Severity	0
Open / High Severity	0
Open / Medium Severity	0
Open / Low Severity	0

Architekturdiagramm



Architekturdiagramm

User (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Login System - Webapp + Mobile App (Process)

Description: Vergleicht eingegebenen OTT-Wert auf Telefon mit erwartetem OTT seitens 2-Faktor-Dienst.

Number	Title	Type	Severity	Status	Score	Description	Mitigations
101	DDoS	Denial of service	Medium	Mitigated	28	Ein DDoS Angriff kann den Login-Dienst überlasten und somit für Anwender unerreichbar machen. CAPEC-125: Flooding: An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. ATT&CK: TA0038 - Network Effects: The adversary is trying to intercept or manipulate network traffic to or from a device. D: 8 / R: 10 / E: 8 / A: 10 / DREA: 36	Firewall, Load-Balancer oder CDN einsetzen, um direkten Datenverkehr auf Login-Server zu begrenzen. DEFEND: D3-ITF - Inbound Traffic Filtering ASVS: CWE 770 (8.1.4): Verify the application can detect and alert on abnormal numbers of requests, such as by IP, user, total per hour or day, or whatever makes sense for the application. D: 4 / R: 10 / E: 4 / A: 10 / Neuer DREA: 28
107	Elevation of Privilege to find unpublic data (hidden)	Elevation of privilege	Medium	Mitigated	25	Attacker send wrong data (Routing Infomation) to Auth service CAPEC-87: Forceful Browsing: An attacker employs forceful browsing (direct URL entry) to access portions of a website that are otherwise unreachable. ATT&CK: T1187 - Forced Authentication: Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism in which they can intercept. D: 8 / R: 9 / E: 8 / A: 7 / DREA: 32	Check if the user have right to access the data DEFEND: D3-AMED: Access mediation: Access mediation is the process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances). Access mediation decisions should enforce least privilege by granting access for scoped durations to prevent privilege creep and, where applicable, implement just-in-time (JIT) access. Denial decisions may prevent initial access or terminate access that has already been granted, ensuring continuous enforcement of security policies. D: 8 /R: 5 /E: 5 /A: 7 /DREA: 25

2-Faktor-Authe ntifizierungsdi enst (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Telefonnummer- API-Gateway (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
108	Spoofing von Telco-data	Spoofing	Medium	Mitigated	18	Angreifer kann sich als Telco Service ausgeben, um an Telefonnummern von Kunden zu kommen. CAPEC-158: Sniffing Network Traffic: In this attack pattern, the adversary monitors network traffic between nodes of a public or multicast network in an attempt to capture sensitive information at the protocol level. Att&ck: T1557 (Adversary-in-the-Middle) D: 6 / R: 7 / E: 4 / A: 8 / DREA: 25	Datenverkehr zwischen Telco Service und Allsecure verschlüsseln. DEFEND: D3-MENCR: Message Encryption MASVS-CRYPTO-1: The app employs current strong cryptography and uses it according to industry best practices. D:6 /R: 2 /E: 2 /A: 8 /DREA: 18

Kundentelefon- anbieter (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
102	Spoofing von Kundendaten	Spoofing	Low	Mitigated	14	Angreifer kann sich als "legitimer" Kunde ausgeben, um an kritische Daten / Dienste zu gelangen zu denen er eigentlich keinen Zugriff haben dürfte (Social Engineering beim Kundendienst). CAPEC ID: 148: Content Spoofing: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged. Att&ck: T1557 (Adversary-in-the-Middle) D: 9 / R: 8 / E: 5 / A: 4 / DREA: 26	Personal schulen, Kritische Kundendaten als solche für Mitarbeiter in der Support-Software markieren, um Irrtümer zu vermeiden. Defend Matrix: D3-NTCD: Network Traffic Community Deviation ASVS: 1.8.1 : Verify that all sensitive data is identified and classified into protection levels. D: 4 / R: 4 / E: 2 / A: 4 / Neuer DREA: 14

Telefon-Routing- Interface (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

1. Auth Challenge (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Erwarteter OTT (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

2. Weiterleitung Telefonnummer (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

2a. Telefonnummer (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

2b. Telefonanbieter (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Alternative A (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Log(Login, OTT, Phone Number) (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Nummer auslesen (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Auslesen von Informationen (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Antwort (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Telefonnummer, OTT (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Security Logs (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Weekly Reports (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Logs auslesen (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

OTT logs, Fehler (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

OTT (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

OTT, Telefonnummer (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Log-DB (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
104	DB-Logs Tampering	Tampering	Low	Mitigated	28	Attacker alter/tampering with data on the database CAPEC-248: Command Injection: An adversary looking to execute a command of their choosing, injects new items into an existing command thus modifying interpretation away from what was intended. ATT&CK: T1565 - Data Manipulation: Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data. D: 6 / R: 9 / E: 8 / A: 9 / DREA: 32	Encrypt the data on the database DEFEND: D3-FE : Encrypting a file using a cryptographic key. D: 5 /R: 8 /E: 7 /A: 8 / DREA: 28

Telefonnummern-DB (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Routing- Information-DB (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Management (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

SIEM-System (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
103	Email Interception	Information disclosure	Low	Mitigated	23	Attacker intercept email contain SIEM report. CAPEC Id: 117: An adversary monitors data streams to or from the target for information gathering purposes. This attack may be undertaken to solely gather sensitive information or to support a further attack against the target. This attack pattern can involve sniffing network traffic as well as other types of data streams (e.g. radio). The adversary can attempt to initiate the establishment of a data stream or passively observe the communications as they unfold. In all variants of this attack, the adversary is not the intended recipient of the data stream. In contrast to other means of gathering information (e.g., targeting data leaks), the adversary must actively position themself so as to observe explicit data channels (e.g. network traffic) and read the content. However, this attack differs from a Adversary-In-the-Middle (CAPEC-94) attack, as the adversary does not alter the content of the communications nor forward data to the intended recipient. Attack: T1114 (Email Collection) D: 8 /R: 6 / E: 4 /A: 9 /DREA: 27	Send decoy file to deceive attacker. DEFEND: D3-DF: Decoy File: A file created for the purposes of deceiving an adversary. D: 4 /R: 6 /E: 4 / A: 9 /DREA: 23

SIEM-DB (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
105	Altering SIEM Logdata for repudiation	Repudiation	Medium	Mitigated	17	Altering the logdata in the SIEM database, e.g. IPS or timestamps to deny being resposible for an attack. CAPEC-248: Command Injection: An adversary looking to execute a command of their choosing, injects new items into an existing command thus modifying interpretation away from what was intended. ATT&CK: T1565 - Data Manipulation: Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data. D: 5 / R: 8 / E: 8 / A: 4 / DREA: 25	Letting just the SIEM service deliver data to DB DEFEND: D3-IOPR: IO Port Restriction D: 5 /R: 4 /E: 4 /A: 4 / DREA: 17

Allsecure Mobile Phone OTT Service (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Number	Title	Type	Severity	Status	Score	Description	Mitigations
106	Denial of Service des OTT Service	Denial of service	Medium	Mitigated	26	Attacker send wrong data (Routing Infomation) to Auth service CAPEC-148: Content Spoofing: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged. ATT&CK: T1565 - Data Manipulation: Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data. D: 6 / R: 9 / E: 8 / A: 9 / DREA: 32	Firewall einsetzen, um direkten Datenverkehr auf OTT services zu filtern. DEFEND: D3-ITF - Inbound Traffic Filtering ASVS: CWE 770 (8.1.4): Verify the application can detect and alert on abnormal numbers of requests, such as by IP, user, total per hour or day, or whatever makes sense for the application. D: 4 / R: 10 / E: 4 / A: 8 / Neuer DREA: 26