Bedrohungsmodell - OTT Auth

Owner: Firma Allsecure
Reviewer: Georg Neugebauer
Contributors: Georg Neugebauer, Malte Stühmer
Date Generated: Fri Nov 21 2025

Executive Summary

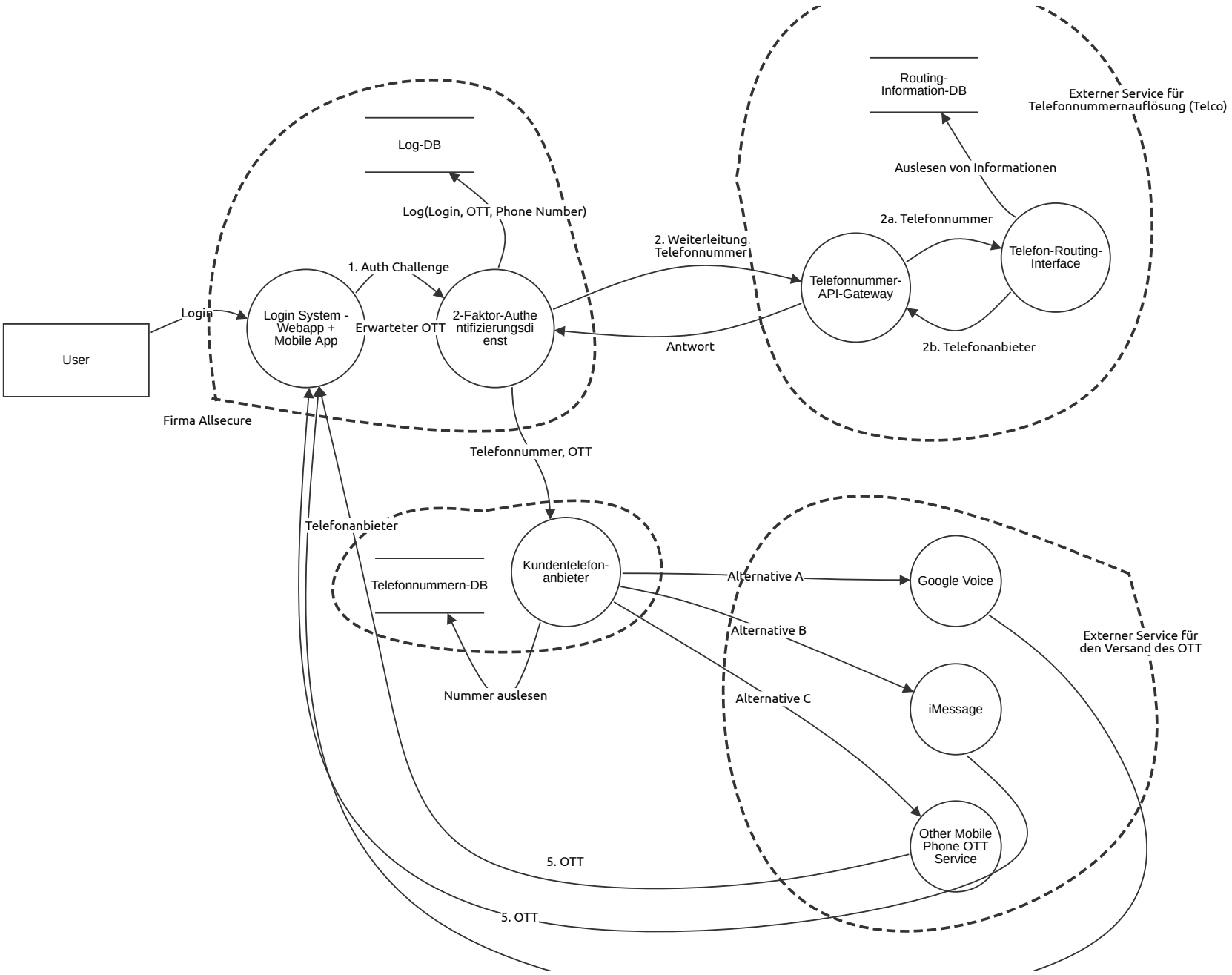
High level system description

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

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

Kundentelefon- anbieter (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

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

Google Voice (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Telefon-Routing- Interface (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

iMessage (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Other Mobile Phone OTT Service (Data Flow)

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

Alternative B (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Alternative C (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

5. OTT (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

5. OTT (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

5. OTT (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Firma Allsecure (threatmodel.shapes.boundary)

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

Log-DB (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

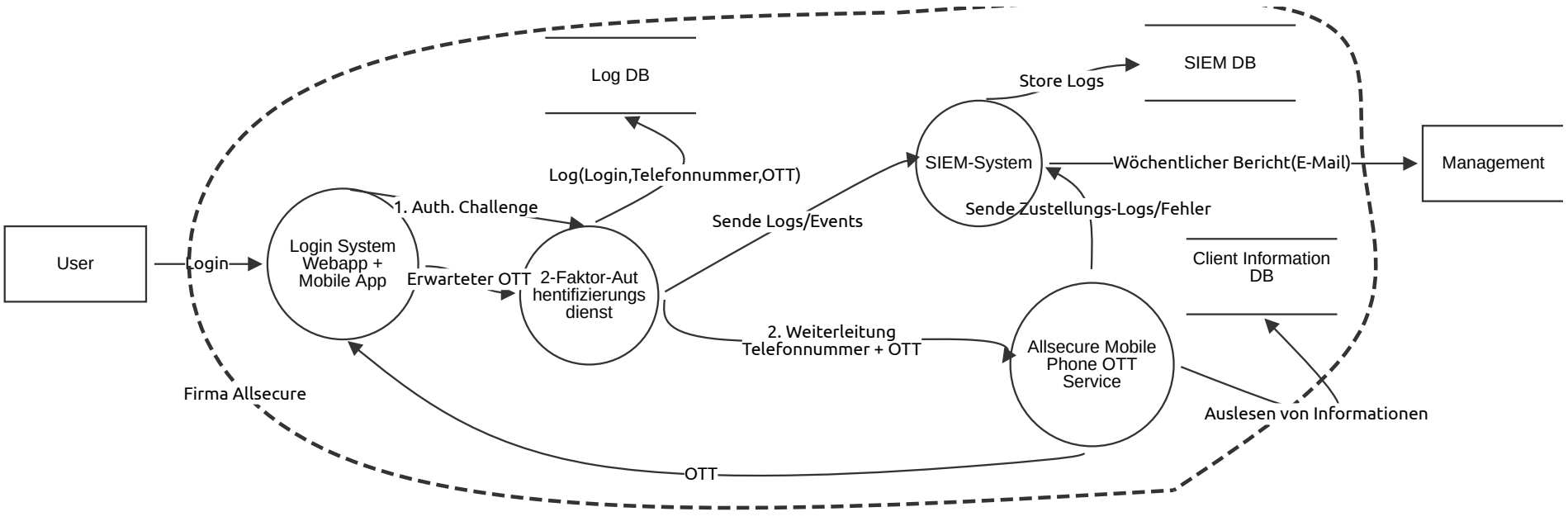
Telefonnummern-DB (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Routing- Information-DB (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Datenflussdiagramm



Datenflussdiagramm

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
108	Login Schwachstelle	Erhöhung von Rechten	Medium	Mitigated	24	Das Login-System ist das primäre Einfallstor von außen. Eine Schwachstelle im Code der Webanwendung oder der API ermöglicht es einem Angreifer, Befehle auf dem Betriebssystemebene auszuführen CAPEC-88: OS Command Injection T1190: Exploit Public-Facing Application – Ausnutzen einer Schwachstelle in einem internetseitig erreichbaren Dienst als Einstiegsvektor DREA-Score: D: 10 / R: 6 / E: 6 / A: 10= 32	Ggmaßnahme: Strikte Eingabevalidierung und sichere Deserialisierung Umsetzung: -- Einsatz einer "Allowlist"-Validierung für alle API-Endpunkte (nur erwartete Zeichen/ Formate zulassen) -- SAST (Static Application Security Testing) in der CI/CD-Pipeline OWASP ASVS V1.2 Injection Prevention 10 + 2 + 2 + 10

2-Faktor-Aut hentifizierungs dienst (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
105	Nicht ausreichende Protokollierung	Nichtanerkennung	Medium	Mitigated	19	Ein Benutzer oder Angreifer behauptet, eine bestimmte OTT-Anfrage stamme nicht von ihm. Ohne ausreichende Protokollierung kann Allsecure dies nicht nachweisen. CAPEC-93: Log Injection-Tampering-Forging TA0004 – Privilege Escalation -- Abstreiten oft mit Eskalation von Log-Rechten verbunden DREA-Score: D: 5 / R: 10 / E: 10 / A: 10=35	Gegenmaßnahme: Security Logging Umsetzung: Eigene Log-DB für Process OWASP ASVS V7.1.1 (Log Content) 5 + 2 + 2 + 10

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

Log(Login,Telefonnummer,OTT) (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

2. Weiterleitung Telefonnummer + OTT (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
106	Man-in-the-Middle	Veröffentlichung von Informationen	Low	Mitigated	12	Der OTT könnte bei unzureichend gesicherter Transportverschlüsselung abgefangen werden, z. B. durch Man-in-the-Middle-Attacken. CAPEC-94: Adversary in the Middle TA0006 - Credential Acess -- Man-in-the-Middle, Durchgriff auf Sitzungstokens DREA-Score: D: 9 / R: 4 / E: 4 / A: 5=22	Gegenmaßnahme: SSL/TLS Certificate Umsetzung: Hinterlegen der Server-Zertifikats im Code der Mobile App, Implementierung einer strikten HTTPS-Konfiguration auf dem Server. OWASP MASVS-NETWORK-2 9 + 1 + 1 + 1 = 12

Login (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

OTT (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Sende Logs/Events (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Sende Zustellungs-Logs/Fehler (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Store Logs (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Wöchentlicher Bericht(E-Mail) (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Auslesen von Informationen (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Log DB (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Allsecure Mobile Phone OTT Service (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
107	Überlasten durch AUth-Anfragne	Denial of service	Low	Mitigated	11	Ein Angreifer überlastet den OTT-Service mit massenhaften Auth-Anfragen, wodurch keine gültigen OTTs generiert oder versendet werden können. CAPEC-125: Flooding T1498 - Network Denial of Service DREA-Score: D: 8 / R: 10 / E: 9 / A: 10=37	Gegenmaßnahme: Rate Limiting und Traffic Throttling Umsetzung: Load Balancer, Einsatz von CAPTCHAs nach fehlgeschlagenen Versuchen, automatische temporäre Sperrung von IPs bei Überschreitung der Limits D3FEND D3-RL (Rate Limiting) 4 + 2 + 3 + 2

SIEM-System (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
103	Spoofing um gefälschte Log-Files zu schicken	Spoofing	Low	Mitigated	8	Ein Angreifer, der Zugriff auf das interne Netzwerk erlangt hat, könnte IP-Adressen oder Identitätsmerkmale des "2-Faktor-Authentifizierungsdienstes" fälschen, um gefälschte Log-Daten an das "SIEM-System" zu senden CAPEC-93 -- Log-injection-tampering T1036 - Masquerading --Der Angreifer maskiert seine bösartigen Daten als legitimen Datenverkehr einer vertrauenswürdigen Quelle. DREA-Score: D: 6 / R: 8 / E: 6 / A: 10=30	Gegenmaßnahme: Mikrosegementierung Umsetzung: Nur die der Auth-Server darf den SIEM-Port erreichen. D3FEND D3-MBN (Microsegmentation) 2 + 2 + 2 + 2

SIEM DB (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
104	Einträge manipulieren	Manipulation	Medium	Mitigated	21	Ein Angreifer mit administrativen Rechten oder durch eine SQL-Injection-Lücke im SIEM-System verändert oder löscht Einträge in der "SIEM DB" CAPEC-66 SQL Injection - Mangelnde Eingabevalidierung T1070 Indicator Removal -- Löschen von Logs oder Artefakten, um Aktivitäten zu verschleiern (Defense Evasion). DREA-Score: D: 9 / R: 3 / E: 3 / A: 10=25	Gegenmaßnahmen: Prepared Statements Umsetzung: Refactoring aller Datenbank-Abfragen im SIEM-Interface auf Prepared Statements D3FEND D3-SPQ (SQL Parameter Query Structure) 9 + 1 + 1 + 10

Management (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Client Information DB (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations