Bedrohungsmodell - OTT Auth

Owner: Firma Allsecure
Reviewer: Georg Neugebauer
Contributors: Georg Neugebauer, Alaeddin Bahrouni
Date Generated: Fri Nov 21 2025

Executive Summary

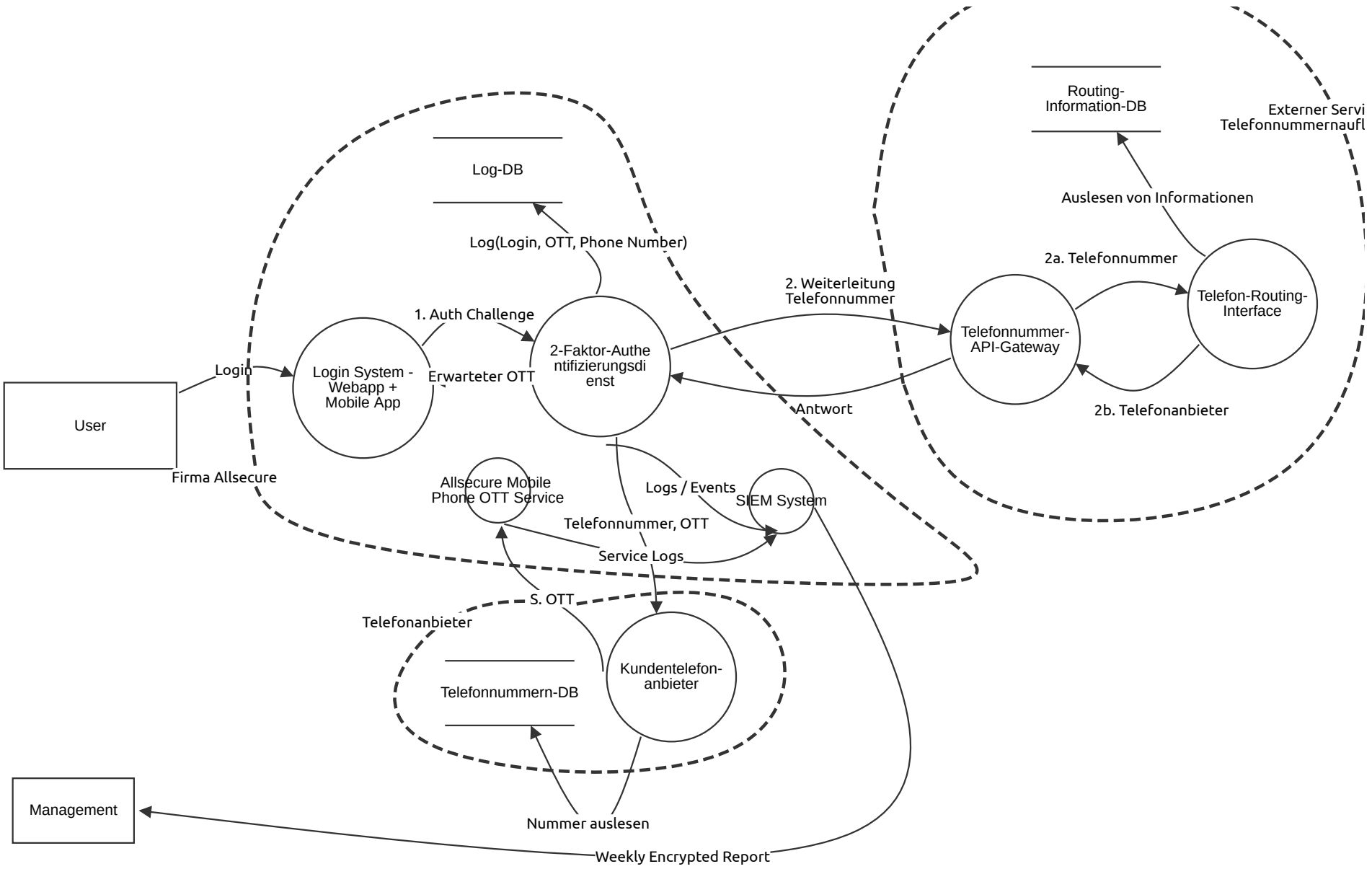
High level system description

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
103	Angreifer täuscht Identität vor durch schwachen Credential-Reset	Spoofing	High	Mitigated	30	Ein Angreifer gibt sich als legitimer Benutzer aus. Da das OTT-System zuvor eine Eigenentwicklung war, könnte die Authentifizierungslogik fehlerhaft sein und Account-Takeover ermöglichen. CAPEC-151 (Identity Spoofing) | ATT&CK: T1078 DREA Calculation: Damage: 8 | Repro: 7 | Exploit: 6 | Affected: 9 | DREA: 30	Implementierung von standardisierten, industrieerprobten Authentifizierungsprotokollen (OIDC/SAML) anstelle von Custom-Logik. Catalog: OWASP ASVS V2.1.1 (Verify that all authentication controls are enforced on the server side). New Risk Score (DREA): Damage: 4 | Repro: 4 | Exploit: 3 | Affected: 3 | DREA: 14
106	Verlust sensibler Daten durch Speicherung auf SD-Karte	Information disclosure	High	Mitigated	32	App-Daten werden auf der SD-Karte gespeichert. SD-Karten sind auf älteren Android-Versionen global lesbar oder bei physischem Zugriff auslesbar. CAPEC-203 | ATT&CK: T1596 DREA Calculation: Damage: 7 | Repro: 9 | Exploit: 8 | Affected: 8 | DREA: 32	Speicherung sensibler Daten im sicheren internen Speicher (Sandbox) des Geräts, nicht auf der externen SD-Karte. Nutzung des Android Keystore Systems. Catalog: OWASP MASVS - MSTG-STORAGE-1 (System credential storage facilities are used to store sensitive data). New Risk Score (DREA): Damage: 4 | Repro: 4 | Exploit: 4 | Affected: 4 | DREA: 16

2-Faktor-Authe ntifizierungsdi enst (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Number	Title	Type	Severity	Status	Score	Description	Mitigations
104	Modifikation unverschlüsselter Konfigurationsdateien	Tampering	Critical	Mitigated	36	Statische symmetrische Schlüssel werden in unverschlüsselten Config-Files gespeichert. Ein Angreifer mit lokalem Serverzugriff kann diese manipulieren, um Verbindungen umzuleiten oder Security zu deaktivieren. CAPEC-75: Manipulating Writeable Configuration Files: Generally these are manually edited files that are not in the preview of the system administrators, any ability on the attackers' behalf to modify these files, for example in a CVS repository, gives unauthorized access directly to the application, the same as authorized users. ATT&CK: T1552.004: Adversaries may search for private key certificate files on compromised systems for insecurely stored credentials. Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures. DREA Calculation: Damage: 9 | Repro: 9 | Exploit: 9 | Affected: 9 | DREA 36	Verschieben der Key-Materials in ein dediziertes Hardware Security Module (HSM) oder einen sicheren Key Vault. Verschlüsselung der Konfigurationsdateien "at rest". Catalog: MITRE D3FEND - D3-FE: Encrypting a file using a cryptographic key. New Risk Score (DREA): Damage: 2 | Repro: 2 | Exploit: 2 | Affected: 2 | DREA 8
107	Serviceausfall durch fehlende Redundanz	Denial of service	High	Mitigated	32	Der Service ist aus Kostengründen nicht redundant ausgelegt (Single Point of Failure). Ein Angreifer kann den Service fluten (Flooding) und Logins verhindern. CAPEC-125 (Flooding) | ATT&CK: T1498 DREA Calculation: Damage: 6 | Repro: 8 | Exploit: 8 | Affected: 10 | DREA 32	Implementierung von Load Balancing und Deployment von mindestens zwei Instanzen des Services (High Availability). Catalog: MITRE D3FEND - D3-LB (Load Balancing). New Risk Score (DREA): Damage: 3 | Repro: 3 | Exploit: 3 | Affected: 3 | DREA 12

Telefonnummer- API-Gateway (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
108	Rechteausweitung durch Kompromittierung statischer Schlüssel	Elevation of privilege	High	Mitigated	30	Wenn der statische symmetrische Schlüssel kompromittiert wird, kann ein Angreifer seine Privilegien ausweiten und den vertrauenswürdigen 2FA-Dienst imitieren. CAPEC-233 (Privilege Escalation) | ATT&CK: T1078 DREA Calculation: Damage: 9 | Repro: 6 | Exploit: 6 | Affected: 9 | DREA 30	Automatische Rotation der Schlüssel unter Verwendung von Standard-Krypto-Bibliotheken (z.B. TLS mit Perfect Forward Secrecy) statt statischer Keys. Catalog: OWASP ASVS V6.2.1 (Verify that keys are generated using cryptographically strong algorithms). New Risk Score (DREA): Damage: 2 | Repro: 3 | Exploit: 3 | Affected: 2 | DREA 10

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

Telefon-Routing- Interface (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

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

S. OTT (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Logs / Events (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Service Logs (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Weekly Encrypted Report (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Log-DB (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
105	Admin löscht Logs um Aktivität zu verbergen	Repudiation	Medium	Mitigated	25	Logs werden in einer lokalen Datenbank gespeichert. Ein böswilliger Administrator könnte Zeilen löschen, um seine Aktionen abzustreiten (Repudiation). CAPEC-93 (Log Injection-Tampering-Forging) | ATT&CK: T1070 DREA Calculation: Damage: 5 | Repro: 8 | Exploit: 7 | Affected: 5 | DREA 25	Senden der Logs in Echtzeit an das neue SIEM System (Write Once, Read Many). Das SIEM agiert als externer Validator, den der lokale Admin nicht manipulieren kann. Catalog: OWASP ASVS V7.1.1 (Verify that the application does not allow logs to be deleted or modified). New Risk Score (DREA): Damage: 3 | Repro: 3 | Exploit: 3 | Affected: 3 | DREA 12

Telefonnummern-DB (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Routing- Information-DB (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Management (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Allsecure Mobile Phone OTT Service (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

SIEM System (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations