

Bedrohungsmo... - OTT Auth

Owner: Firma Allsecure
Reviewer: Georg Neugebauer
Contributors: Georg Neugebauer, Tolga Sanli
Date Generated: Wed Nov 12 2025

Executive Summary

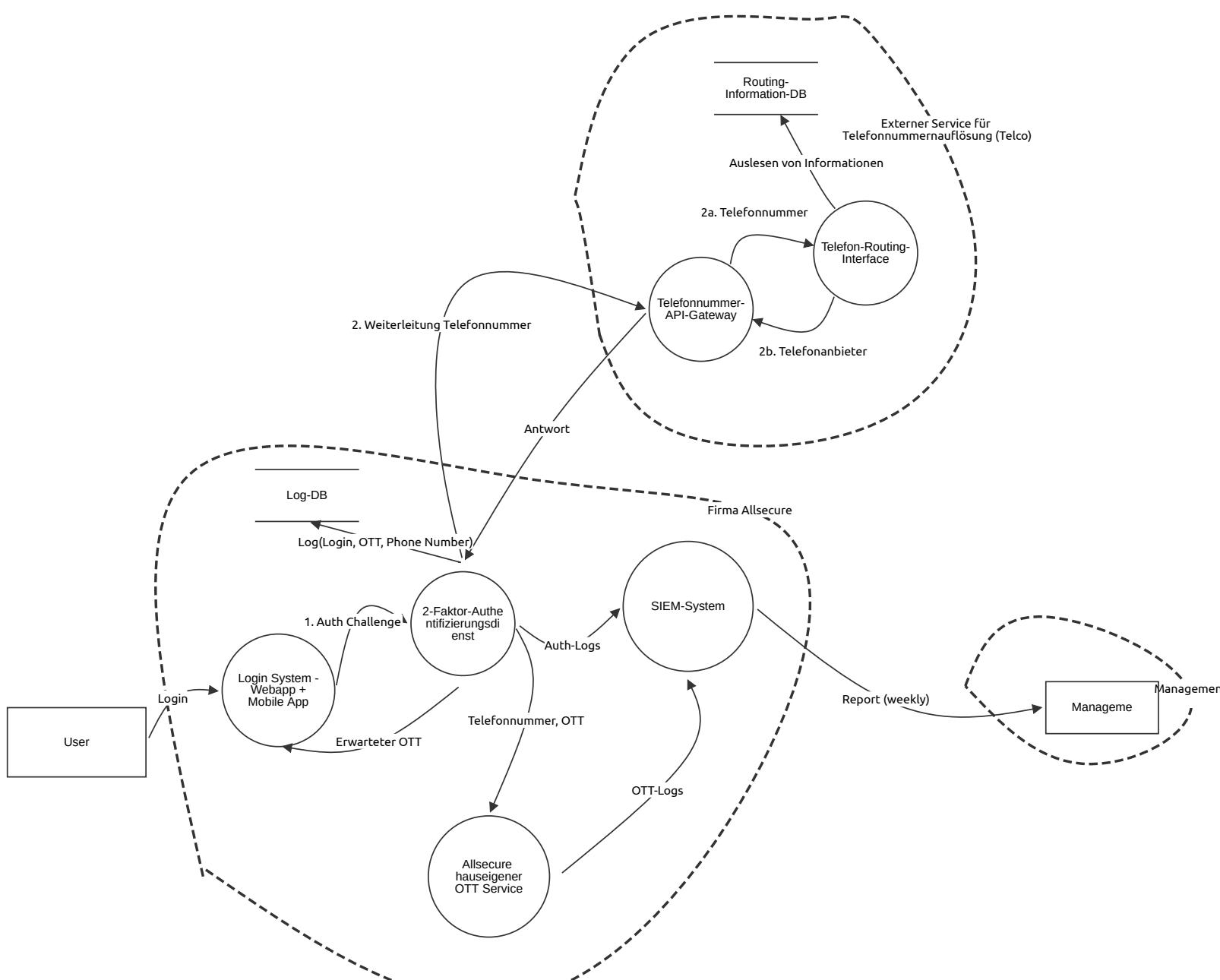
High level system description

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

Auth-Logs (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Antwort (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

2. Weiterleitung Telefonnummer (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

OTT-Logs (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Telefonnummer, OTT (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Report (weekly) (Data Flow)

Description: wöchentlicher Report per E-Mail (signiert und verschlüsselt)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
106	Manipulating the report	Tampering	High	Mitigated	33	<p>Attacker could manipulate the data in SIEM-system, before it gets signed and encrypted. Other option could be that attacker gets the keys to encrypt and manipulate the data.</p> <p>Man in the middle</p> <p>CAPEC-94: Adversary in the Middle (AiTM) https://capec.mitre.org/data/definitions/94.html</p>	<p>Protocol Metadata Anomaly Detection</p> <p>D3-PMAD</p> <p>Detect anomaly within metadata/timestamps, datasizes, missing signatures etc.</p> <p>D: 10 R: 8 E: 6 A: 9</p>

User (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
105	Login via stolen credentials	Spoofing	Medium	Mitigated	20	<p>Attacker gets somehow login credentials example trough phishing-mails and login with its credentials.</p> <p>CAPEC ID: 98 Phising https://capec.mitre.org/data/definitions/98.html</p> <p>D: 6 R: 6 E: 7 A: 1</p> <p>20/4 = 5</p>	<p>MASVS-AUTH-1 Authentication and authorization</p> <p>Force 2FA on all users to prevent attackers login with stolen credentials.</p> <p>D: 6 R: 6 E: 7 A: 1</p> <p>20/4 = 5</p>

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	<p>Ein DDoS Angriff kann den Login-Dienst überlasten und somit für Anwender unerreichbar machen.</p> <p>CAPEC-125: Flooding: An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target.</p> <p>ATT&CK: TA0038 - Network Effects: The adversary is trying to intercept or manipulate network traffic to or from a device.</p> <p>D: 8 / R: 10 / E: 8 / A: 10 / DREA: 36</p>	<p>Firewall, Load-Balancer oder CDN einsetzen, um direkten Datenverkehr auf Login-Server zu begrenzen.</p> <p>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.</p> <p>D: 4 / R: 10 / E: 4 / A: 10 / Neuer DREA: 28</p>
104	Authentication Bypass	Spoofing	Medium	Mitigated	19	<p>Bypass an authentication trough links to get to secured sites</p> <p>CAPEC ID: 115 Authentication Bypass https://capec.mitre.org/data/definitions/115.html</p> <p>CAPEC ID: 151 Identity Spoofing https://capec.mitre.org/data/definitions/151.html</p>	<p>MFA to enforce multiple authentications, makes it more difficult for attackers to bypass trough second-links or other attempts to bypass.</p> <p>D3-MFA https://d3fend.mitre.org/technique/d3f:Multi-factorAuthentication/</p> <p>D: 4 R: 7 E: 6 A: 2</p>

2-Faktor-Authentifizierungsdienst (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
109	API Request flooding	Denial of service	High	Mitigated	33	<p>An attacker can flood the external service with requests where the external service can deny the requests for security reasons.</p> <p>CAPEC-469: HTTP DoS https://capec.mitre.org/data/definitions/469.html</p> <p>CAPEC-482: TCP Flood</p> <p>CAPEC-489: SSL Flood</p> <p>and other protocol Floods..</p>	<p>Web application firewall can filter, monitor and block traffic id: d3f:WebApplicationFirewall (WAF)</p> <p>D: 8 R: 9 E: 6 A: 10</p>

Log-DB (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
108	attacker steals data	Information disclosure	High	Mitigated	35	An attacker can get entry through SQL-Injection and steal all Data, OTT-tokens, telephone numbers etc. CAPEC-150: Collect Data from Common Resource Locations https://capec.mitre.org/data/definitions/150.html CAPEC-66: SQL Injection https://capec.mitre.org/data/definitions/66.html	File Encryption D3-FE Encrypt sensitive files or tokens etc.. Secure Coding and Architecture ASVS V15 make pipelines injectionproof D: 10 R: 7 E: 8 A: 10

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

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

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Allsecure hauseigener OTT Service (Process)

Description: ein Service für die 2-Faktor-Authentifizierung mittels Telefonnummer und One-Time-Token

Number	Title	Type	Severity	Status	Score	Description	Mitigations
107	manipulating functionality	Repudiation	High	Mitigated	30	Attacker manipulates the functionality so the OTT once was approved can be set as not approved afterwards or can set its own signing certificate as trust for legitimate certification authority CAPEC-459: Creating a Rogue Certification Authority Certificate https://capec.mitre.org/data/definitions/459.html	Check communication/TLS, accept only trustworthy roots ASVS V10 D: 8 R: 6 E: 6 A: 10

SIEM-System (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Number	Title	Type	Severity	Status	Score	Description	Mitigations
110	code manipulation	Elevation of privilege	Critical	Mitigated	36	An attacker can attack through unpatched vulnerability to elevate himself to highest authorization and manipulate/inject code. CAPEC-69: Target Programs with Elevated Privileges https://capec.mitre.org/data/definitions/69.html	Application-based Process Isolation D3-ABPI Isolate the application from accessing critical/not-needed processes/infos/memory D: 10 R: 9 E: 7 A: 10

Management (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
--------	-------	------	----------	--------	-------	-------------	-------------

Telefonnummer- API-Gateway (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
--------	-------	------	----------	--------	-------	-------------	-------------

Telefon-Routing- Interface (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
--------	-------	------	----------	--------	-------	-------------	-------------

Routing- Information-DB (Store)

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
--------	-------	------	----------	--------	-------	-------------	-------------

Auslesen von Informationen (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
--------	-------	------	----------	--------	-------	-------------	-------------

1. Auth Challenge (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
--------	-------	------	----------	--------	-------	-------------	-------------