

Bedrohungsmodell - OTT Auth

Eigentümer: Firma Allsecure

Prüfer: Georg Neugebauer

Mitwirkende: Georg Neugebauer, Malte Stühmer

Erstellungsdaten: Thu Nov 20 2025

Zusammenfassung

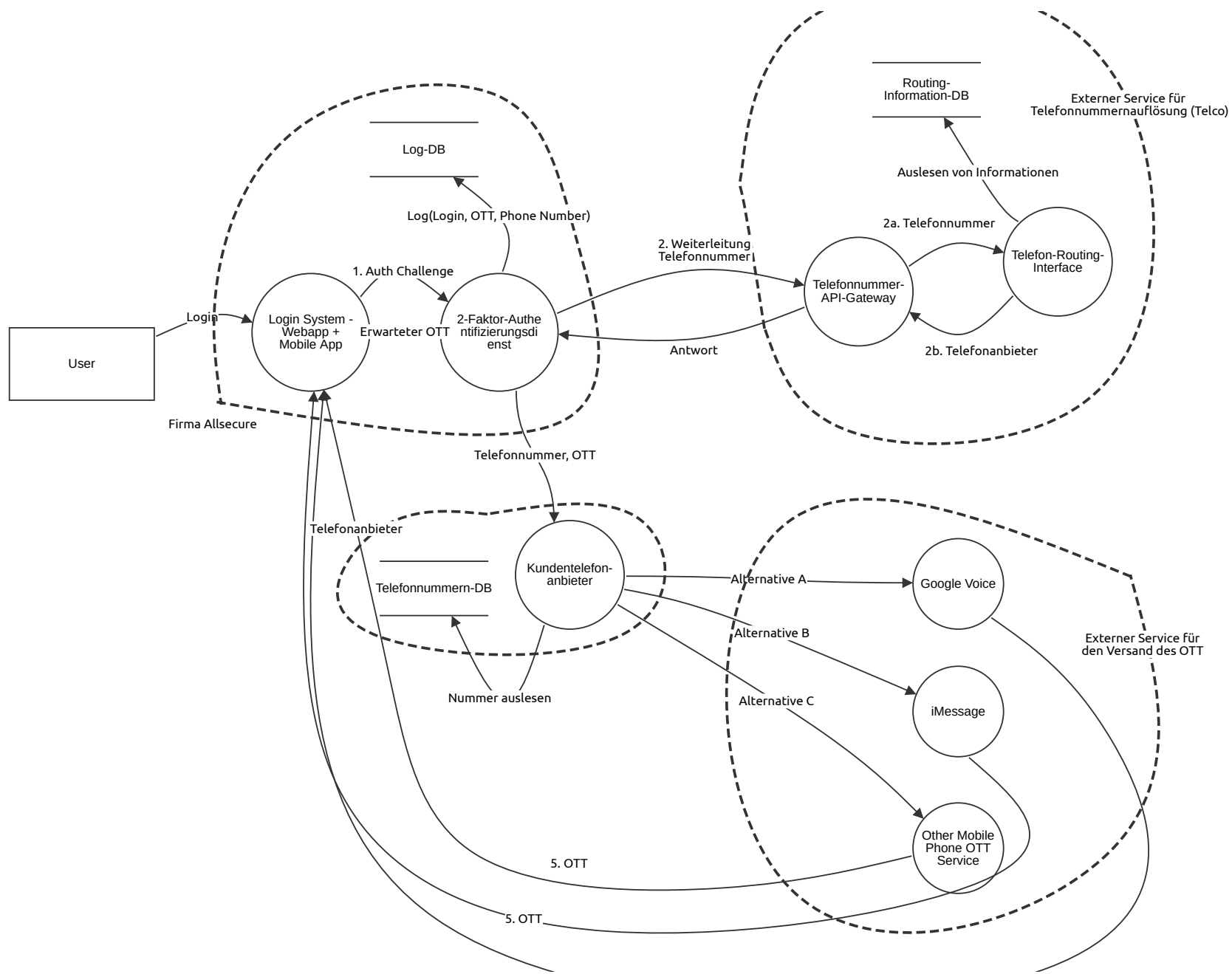
High-Level System Beschreibung

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

Zusammenfassung

Bedrohungen insgesamt	8
Bedrohungen abgeschwächt	2
Nicht abgeschwächt	6
Offen / Kritische Priorität	0
Offen / Hohe Priorität	0
Offen / Mittlere Priorität	3
Offen / Niedrige Priorität	3

Architekturdiagramm



Architekturdiagramm

User (Actor)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Login System - Webapp + Mobile App (Process)

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

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
101	DDoS	Denial of service	Mittel	Abgeschwächt	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>

2-Faktor-Authentifizierungsdienst (Process)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Telefonnummer- API-Gateway (Process)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Kundentelefon- anbieter (Process)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
102	Spoofing von Kundendaten	Spoofing	Niedrig	Abgeschwächt	14	<p>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).</p> <p>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.</p> <p>Att&ck: T1557 (Adversary-in-the-Middle)</p> <p>D: 9 / R: 8 / E: 5 / A: 4 / DREA: 26</p>	<p>Personal schulen, Kritische Kundendaten als solche für Mitarbeiter in der Support-Software markieren, um Irrtümer zu vermeiden.</p> <p>Defend Matrix: D3-NTCD: Network Traffic Community Deviation</p> <p>ASVS: 1.8.1 : Verify that all sensitive data is identified and classified into protection levels.</p> <p>D: 4 / R: 4 / E: 2 / A: 4 / Neuer DREA: 14</p>

Google Voice (Process)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Telefon-Routing- Interface (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

iMessage (Process)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Other Mobile Phone OTT Service (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

1. Auth Challenge (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Erwarteter OTT (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

2. Weiterleitung Telefonnummer (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

2a. Telefonnummer (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

2b. Telefonanbieter (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Alternative A (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Alternative B (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Alternative C (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

5. OTT (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

5. OTT (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

5. OTT (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Firma Allsecure (threatmodel.shapes.boundary)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

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

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Nummer auslesen (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Auslesen von Informationen (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Antwort (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Telefonnummer, OTT (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Log-DB (Store)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

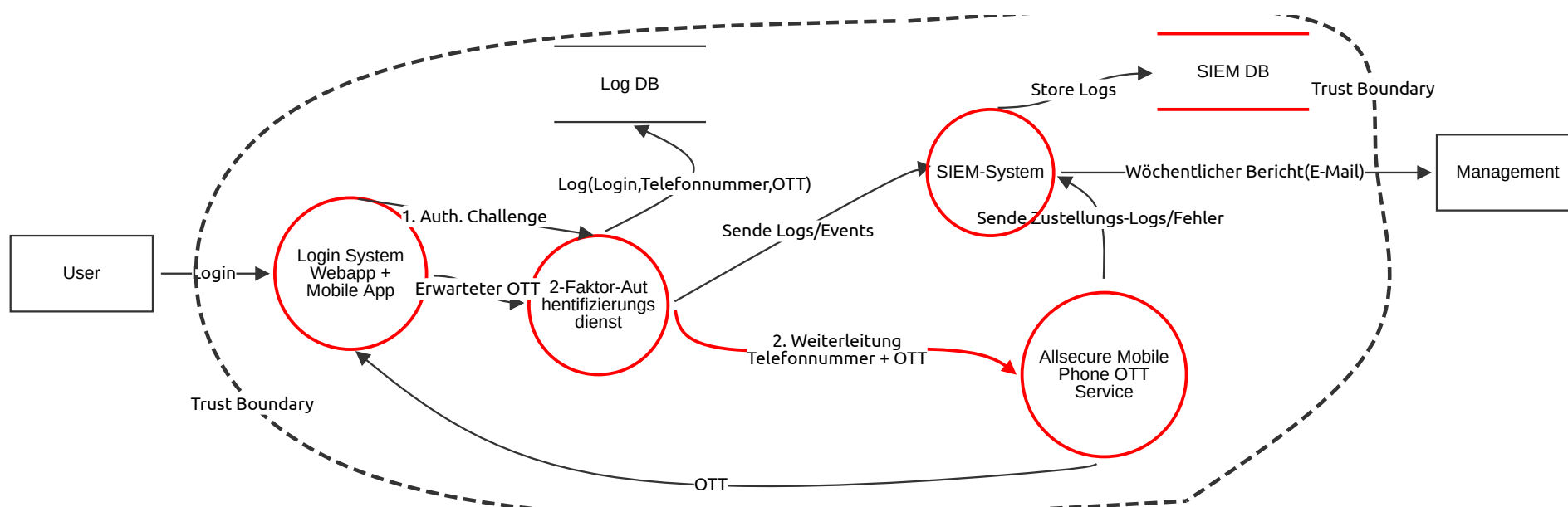
Telefonnummern-DB (Store)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Routing- Information-DB (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Datenflussdiagramm



Datenflussdiagramm

User (Actor)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Login System Webapp + Mobile App (Process)

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

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
108	Login Schwachstelle	Erhöhung von Rechten	Mittel	Offen	24	<p>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</p> <p>CAPEC-253: Remote Code Execution</p> <p>T1190: Exploit Public-Facing Application – Ausnutzen einer Schwachstelle in einem internetseitig erreichbaren Dienst als Einstiegsvektor</p> <p>DREA-Score: D: 10 / R: 6 / E: 6 / A: 10= 32</p>	<p>Ggmaßnahme: Strikte Eingabevalidierung und sichere Deserialisierung</p> <p>Umsetzung: -- Einsatz einer "Allowlist"-Validierung für alle API-Endpunkte (nur erwartete Zeichen/ Formate zulassen)</p> <p>-- SAST (Static Application Security Testing) in der CI/CD-Pipeline</p> <p>OWASP ASVS V1.2 Injection Prevention</p> <p>10 + 2 + 2 + 10</p>

2-Faktor-Authentifizierungsdienst (Process)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
105	Nicht ausreichende Protokollierung	Nichtanerkennung	Mittel	Offen	19	<p>Ein Benutzer oder Angreifer behauptet, eine bestimmte OTT-Anfrage stamme nicht von ihm. Ohne ausreichende Protokollierung kann Allsecure dies nicht nachweisen.</p> <p>CAPEC-93: Log Injection-Tampering-Forging TA0004 – Privilege Escalation -- Abstreiten oft mit Eskalation von Log-Rechten verbunden</p> <p>DREA-Score: D: 5 / R: 10 / E: 10 / A: 10=35</p>	<p>Gegenmaßnahme: Security Logging</p> <p>Umsetzung: Eigene Log-DB für Process</p> <p>OWASP ASVS V7.1.1 (Log Content)</p> <p>5 + 2 + 2 + 10</p>

1. Auth. Challenge (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Erwarteter OTT (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

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

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

2. Weiterleitung Telefonnummer + OTT (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
106	Man-in-the-Middle	Veröffentlichung von Informationen	Niedrig	Offen	12	<p>Der OTT könnte bei unzureichend gesicherter Transportverschlüsselung abgefangen werden, z. B. durch Man-in-the-Middle-Attacken.</p> <p>CAPEC-94: Adversary in the Middle</p> <p>TA0006 - Credential Access -- Man-in-the-Middle, Durchgriff auf Sitzungstokens</p> <p>DREA-Score: D: 9 / R: 4 / E: 4 / A: 5=22</p>	<p>Gegenmaßnahme: SSL/TLS Certificate Umsetzung: Hinterlegen der Server-Zertifikats im Code der Mobile App, Implementierung einer strikten HTTPS-Konfiguration auf dem Server.</p> <p>OWASP MASVS-NETWORK-2</p> <p>9 + 1 + 1 + 1 = 12</p>

Login (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

OTT (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Sende Logs/Events (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Sende Zustellungs-Logs/Fehler (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Store Logs (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Wöchentlicher Bericht(E-Mail) (Data Flow)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Log DB (Store)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------

Allsecure Mobile Phone OTT Service (Process)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
107	Überlasten durch Auth-Anfrage	Denial of service	Niedrig	Offen	11	<p>Ein Angreifer überlastet den OTT-Service mit massenhaften Auth-Anfragen, wodurch keine gültigen OTTs generiert oder versendet werden können.</p> <p>CAPEC-125: Flooding</p> <p>T1498 - Network Denial of Service</p> <p>DREA-Score: D: 8 / R: 10 / E: 9 / A: 10=37</p>	<p>Gegenmaßnahme: Rate Limiting und Traffic Throttling</p> <p>Umsetzung: Load Balancer, Einsatz von CAPTCHAs nach fehlgeschlagenen Versuchen, automatische temporäre Sperrung von IPs bei Überschreitung der Limits</p> <p>D3FEND D3-RL (Rate Limiting)</p> <p>4 + 2 + 3 + 2</p>

SIEM-System (Process)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
103	Spoofing um gefälschte Daten zu schicken	Spoofing	Niedrig	Offen	8	<p>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</p> <p>CAPEC-93 -- Log-injection-tampering</p> <p>T1036 - Masquerading --Der Angreifer maskiert seine böartigen Daten als legitimen Datenverkehr einer vertrauenswürdigen Quelle.</p> <p>DREA-Score: D: 6 / R: 8 / E: 6 / A: 10=30</p>	<p>Gegenmaßnahme: Mikrosegmentierung</p> <p>Umsetzung: Nur die IPs der Auth-Server dürfen den SIEM-Port erreichen.</p> <p>D3FEND D3-MBN (Microsegmentation)</p> <p>2 + 2 + 2 + 2</p>

SIEM DB (Store)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
104	Einträge manipulieren	Manipulation	Mittel	Offen	21	<p>Ein Angreifer mit administrativen Rechten oder durch eine SQL-Injection-Lücke im SIEM-System verändert oder löscht Einträge in der "SIEM DB"</p> <p>CAPEC-66 SQL Injection - Mangelnde Eingabevalidierung</p> <p>T1070 Indicator Removal -- Löschen von Logs oder Artefakten, um Aktivitäten zu verschleiern (Defense Evasion).</p> <p>DREA-Score: D: 9 / R: 3 / E: 3 / A: 10=25</p>	<p>Gegenmaßnahmen: Prepared Statements</p> <p>Umsetzung: Refactoring aller Datenbank-Abfragen im SIEM-Interface auf Prepared Statements</p> <p>D3FEND D3-SPQ (SQL Parameter Query Structure)</p> <p>9 + 1 + 1 + 10</p>

Management (Actor)

Nummer	Titel	Typ	Priorität	Status	Ergebnis	Beschreibung	Minderungsmaßnahme
--------	-------	-----	-----------	--------	----------	--------------	--------------------