Bedrohungsmodell - OTT Auth

Owner: Firma Allsecure
Reviewer: Georg Neugebauer
Contributors: Georg Neugebauer, DevSecOps Kursteilnehmer
Date Generated: Fri Nov 15 2024

Executive Summary

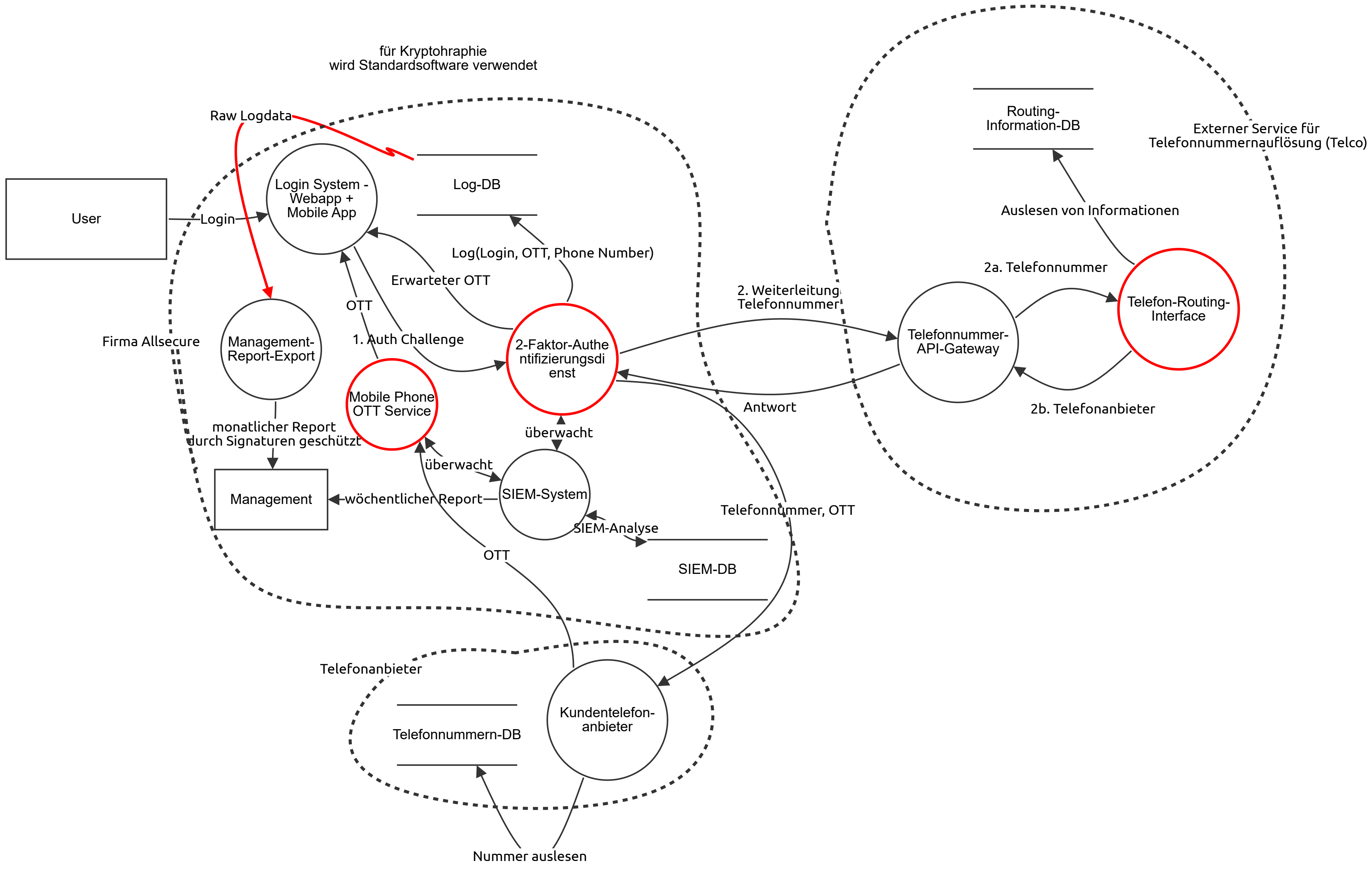
High level system description

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	4
Not Mitigated	4
Open / High Priority	0
Open / Medium Priority	0
Open / Low Priority	4
Open / Unknown Priority	0

Architekturdiagramm



Architekturdiagramm

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Login System - Webapp + Mobile App (Process)

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

Number	Title	Type	Priority	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
112	Brute-Force	Elevation of privilege	Low	Mitigated		Brute-Force auf das Login-System. CAPEC-49: Password Brute Forcing An adversary tries every possible value for a password until they succeed. A brute force attack, if feasible computationally, will always be successful because it will essentially go through all possible passwords given the alphabet used (lower case letters, upper case letters, numbers, symbols, etc.) and the maximum length of the password. ATT&CK: T1110 - Brute Force D: 7 / R: 6 / E: 5 / A: 4 / DREA: 24	Nutzer benachrichtigen, dass ein login-Versuch aus einer unüblichen Region ausgeübt wurde und weitere Anfragen ggf. sperren. ASVS 2.2.10 Verify that users are notified of suspicious authentication attempts. This may include successful or unsuccessful authentication from an unusual location or client, partially successful authentication with only one of multiple factors, successful or unsuccessful authentication after a long period of inactivity or successful authentication after several unsuccessful attempts. D: 6 / R: 3 / E: 2 / A: 3 / Neuer DREA: 14

2-Faktor-Authentifizierungsdienst (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
103	Spoofing	Spoofing	Low	Open		Ein Angreifer könnte sich als legitimer Benutzer ausgeben und unautorisierte Anfragen an den 2-Faktor-Authentifizierungsdienst senden. CAPEC-115: Authentication Bypass. An attacker gains access to application, service, or device with the privileges of an authorized or privileged user by evading or circumventing an authentication mechanism. The attacker is therefore able to access protected data without authentication ever having taken place. T1078: Valid Accounts. Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. D: 9 / R: 7 / E: 5 / A: 4 DREA: 25	Implementierung einer Multi-Faktor-Authentifizierung mit zusätzlicher Gerätebindung, um sicherzustellen, dass nur autorisierte Geräte auf den Authentifizierungsdienst zugreifen. ASVS: 4.1.1 Verify that the application enforces access control rules on a trusted service layer, especially if client-side access control is present and could be bypassed. D: 4 / R: 4 / E: 2 / A: 4 DREA: 14

Telefonnummer-API-Gateway (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Kundentelefon-anbieter (Process)

Number	Title	Type	Priority	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	Priority	Status	Score	Description	Mitigations
107	Denial of service	Denial of service	Low	Open		Ein Angreifer könnte viele Anfragen senden und diesen Service überlasten. CAPEC-125: Flooding An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. Endpoint Denial of Service - T1499 Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. D: 6 / R: 6 / E: 5 / A: 6 DREA: 23	Ungewöhnliche Mengen an Anfragen erfassen und blockieren. D3-ISVA Inbound Session Volume Analysis D: 3 / R: 2 / E: 2 / A: 3 DREA: 10

1. Auth Challenge (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Erwarteter OTT (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

2. Weiterleitung Telefonnummer (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

2a. Telefonnummer (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

2b. Telefonanbieter (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Alternative A (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

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

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Nummer auslesen (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Auslesen von Informationen (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Antwort (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Telefonnummer, OTT (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

wöchentlicher Report (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

OTT (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

OTT (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

monatlicher Report
durch Signaturen geschützt (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Raw Logdata (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
114	Tampering	Tampering	Low	Open		Ein Angreifer mit ausreichenden Rechten könnte auf den Exportprozess zugreifen und die Berichte vor der Signatur manipulieren. CAPEC-165: File Manipulation T1485 - Data Destruction D: 8 / R: 5 / E: 5 / A: 4 / DREA: 22	Log asynchron verschlüsseln. D3-MENCR (Message Encryption) D: 3 / R: 3 / E: 2 / A: 3 / Neuer DREA: 11

SIEM-Analyse (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

überwacht (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

überwacht (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log-DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Telefonnummern-DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Routing-Information-DB (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Mobile Phone OTT Service (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
111	Information disclosure	Information disclosure	Low	Open		Ein Angreifer könnte versuchen, das OTT-Token während der Übertragung abzufangen. Adversary-in-the-Middle - T1557 CAPEC-593: Session Hijacking Session sidejacking takes advantage of an unencrypted communication channel between a victim and target system. D: 8 / R: 6 / E: 5 / A: 4 / DREA: 23	TLS/SSL Verschlüsselung MASVS-NETWORK-1 The app secures all network traffic according to the current best practices. D: 3 / R: 2 / E: 2 / A: 3 / Neue DREA: 10

Management-Report-Export (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Management (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SIEM-System (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SIEM-DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
115	Repudiation	Repudiation	Low	Mitigated		Ein Angreifer könnte die Log-Daten des SIEM-Systems verändern oder löschen, um Spuren zu verwischen. CAPEC-268: Audit Log Manipulation ATT&CK: T1070 Indicator Removal Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses D: 7 / R: 5 / E: 5 / A: 4 / DREA: 21	schreibgeschütztes Format verwenden D3FEND: D3-ITDF: Immutable Log Data Format D: 3 / R: 2 / E: 2 / A: 3 / Neue DREA: 10