Bedrohungsmodell - OTT Auth

Owner: Firma Allsecure
Reviewer: Georg Neugebauer
Contributors: Georg Neugebauer, DevSecOps Kursteilnehmer
Date Generated: Wed Nov 13 2024

Executive Summary

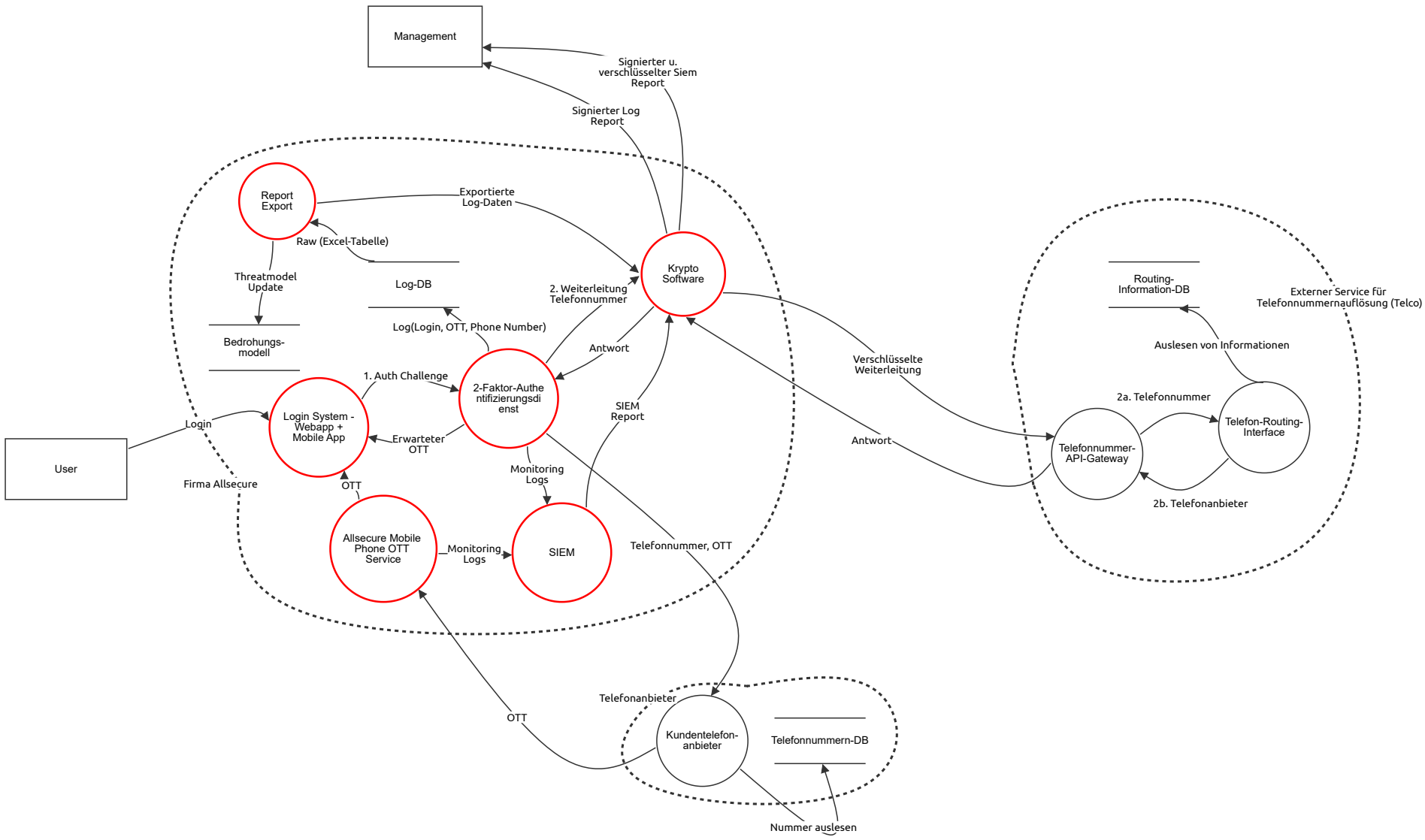
High level system description

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	2
Not Mitigated	6
Open / High Priority	0
Open / Medium Priority	6
Open / Low Priority	0
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
104	Admin Login	Elevation of privilege	Medium	Open		Ein Angreifer kann nach Login durch Misskonfiguration Adminseiten einsehen und sieht Kundendaten CAPEC-180: Exploiting Incorrectly Configured Access Control Security Levels ATT&CK: T1098.003: Additional Cloud Roles D: 10 / R: 10 / E: 8 / A: 10 / DREA: 38	Bevor Prozesse welche auf Admins beschränkt sind, muss geprüft werden ob es sich bei dem User um einen Admin handelt D: 10/R: 10/E: 0/A: 10/DREA: 30 D3-SCP: System Configuration Permissions

2-Faktor-Authentifizierungsdienst (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
106	New STRIDE threat	Tampering	Medium	Open		Ein Angreifer manipuliert die Auth Challenge so, dass die 2FA diese als bestanden wertet und Zugriff auf einen anderen Account. Angriffsvektor: Der Angreifer kann sich ohne valide Daten authentifizieren CAPEC-272: Protocol Manipulation ATT&CK: T1649: Steal or Forge Authentication Certificates D: 10 / R: 1 / E: 1 / A: 2 / DREA: 14	Es wird die normale IPs Adresse gespeichert, sollte eine Anomalie erkannt werden dann wird diese überprüft D: 2 / R: 1 / E: 1 / A: 1 / DREA: 5 D3-IPRA: IP Reputation Analysis

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

Erwarteter OTT (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

OTT (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

OTT (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Antwort (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Verschlüsselte Weiterleitung (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Telefonnummer, OTT (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Antwort (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Auslesen von Informationen (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Raw (Excel-Tabelle) (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Threatmodel Update (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

2a. Telefonnummer (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SIEM Report (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Signierter u. verschlüsselter Siem Report (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Signierter Log Report (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

1. Auth Challenge (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Monitoring Logs (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Monitoring Logs (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Erwarteter OTT (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Exportierte Log-Daten (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 (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Allsecure Mobile Phone OTT Service (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
108	New STRIDE threat	Denial of service	Medium	Open		Ein Angreifer provoziert fehlerhafte Anfragen auf den Service, weshalb richtige OTT Anfragen nicht verarbeitet werden können CAPEC-490: Amplification ATT&CK: T1499.003: Endpoint Denial of Service: Application Exhaustion Flood D: 6 / R: 10 / E: 8 / A: 10 / DREA: 34	Überprüfen der eigehenden Nachrichten auf vom Protokoll abweichende Anfragen D: 6 / R: 10 / E: 0 / A: 10 / DREA: 26 D3-CSPP: Client-server Payload Profiling

Krypto Software (Process)

Kann mit hinterlegten Schlüsseln verschlüsseln und/oder signieren

Number	Title	Type	Priority	Status	Score	Description	Mitigations
105	New STRIDE threat	Spoofing	Medium	Open		MITM kann Telefonnummern spoofen, er bricht den Key des Kryptosystems und kann somit die Kommunikation mit dem API-Gateway kontrollieren CAPEC-384: Application API Message Manipulation via Man-in-the-Middle ATT&CK: T1071.001: Application Layer Protocol: Web Protocols D: 8/R: 10/E: 1/A: 4/ DREA: 23	Die Schlüssel werden regelmäßig gewechselt und die alten widerrufen D: 8/R: 1/E: 1/A: 4/ DREA: 14 D3-CRO: Credential Rotation

Report Export (Process)

Exportiert die Logfiles, speist diese in das Bedrohungsmodell ein und leitet diese zum signieren weiter

Number	Title	Type	Priority	Status	Score	Description	Mitigations
109	New STRIDE threat	Information disclosure	Medium	Open		Angreifer kann Logs ohne Zugriffskontrolle einsehen. Angriffsvektor: Angreifer kann mittels Fuzzing API-Endunkte oder Ports finden um die darunterliegende Datenbank zu iterieren. CAPEC-28: Fuzzing T1190: Exploit Public-Facing Application D: 8 / R: 10 / E: 7 / A: 10 / DREA: 35	Es werden alle Zugriffe auf diesen Endpunkt blockiert D: 8 / R: 0 / E: 0 / A: 10 / DREA: 18 D3-ITF: Inbound Traffic Filtering

Management (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Bedrohungs-modell (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SIEM (Process)

SIEM überwacht die 2FA und den Phone OTT Service

Number	Title	Type	Priority	Status	Score	Description	Mitigations
107	New STRIDE threat	Repudiation	Medium	Open		Bestimmte Anfragen werden nicht vom SIEM überprüft, wodurch ein potentieller Angreifer seine Aktivitäten verschleiern kann. Angriffsvektor: Das SIEM System ist für bestimmte Formatierungen falsch konfiguriert, wodurch diese Pakete nicht geprüft oder geloggt werden. CAPEC-267: Leverage Alternate Encoding T1027.013: Encrypted/ Encoded File D: 3 / R: 10 / E: 3 / A: 1 / DREA: 17	Das SIEM wird auf die restlichen Arten von Formatierungen wird über prüft D: 3 / R: 10 / E: 0 / A: 1 / DREA: 14 D3-ACH: Application Configuration Hardening