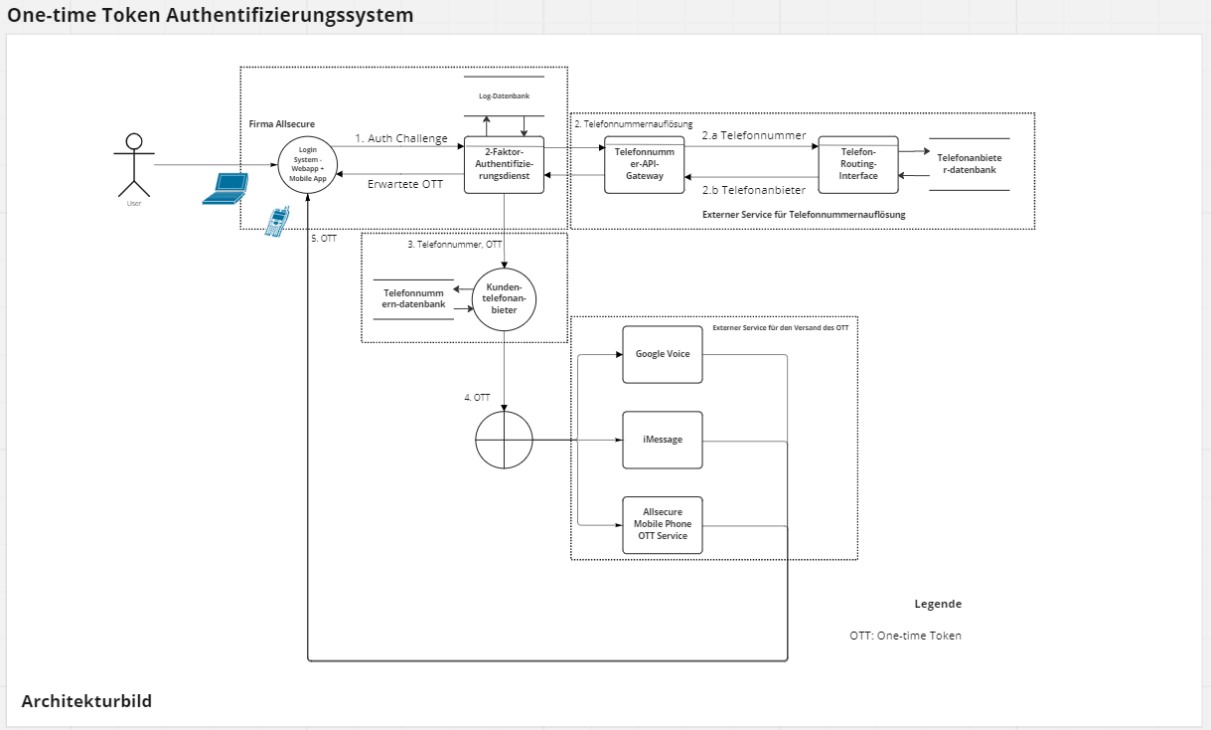
Modellieren mit Threat Dragon

Betrachten Sie noch einmal unser Beispiel aus der Vorlesung zur Bedrohungsmodellierung eines One-Time Token Authentifizierungssystems der Firma Allsecure.



Szenariobeschreibung

Eine Vielzahl von Systemen ist darauf ausgelegt, Hilfspasswörter - One-Time-Token (OTT) - über das Telefonnetz an das Telefon einer Person zu senden. Während einer Anmeldephase wird der Benutzer aufgefordert, eine Telefonnummer anzugeben, die dann mit dem Konto verknüpft wird. Das in der Abbildung gezeigte Szenario beginnt, wenn jemand versucht, sich beim "Login-System" anzumelden (bei einem Konto, dem ein Telefon zugeordnet ist). Ein Modell, wie das funktioniert, sieht folgendermaßen aus:

1. Der Anmeldeversuch löst eine Nachricht an eine Schnittstelle der Telefongesellschaft ("Telco") aus, und diese Nachricht besteht aus einer Telefonnummer und einer Nachricht, die an die Telefonnummer gesendet werden soll.
2. Die Telco-Schnittstelle führt eine Art von Lookup durch, um herauszufinden, wie die Nachricht weitergeleitet werden soll. Dies wird als "Number Routing"-Prozess in einer separaten Vertrauensdomäne modelliert. Es gibt eine Reihe von Möglichkeiten, wie sich Mobiltelefone mit anderen Telefongesellschaften verbinden können, einschließlich Roaming und Femtozellen. Das Rufnummern-Routing-System gibt einen Zeiger auf eine "kundenwirksame Telefongesellschaft" zurück. Der Service ist kostenpflichtig.
3. Die Telco-Schnittstelle sendet dann die Rufnummer und den OTT an die effektive Telco des Kunden.
4. Die OTT wird dann an ein oder mehrere Systeme gesendet, die die Nachricht übermitteln können. Das kann einfach das betreffende Telefon sein, es kann aber auch eine Schnittstelle wie Google Voice oder Apple iMessage sein.

5. Die Person gibt den OTT auf der Anmeldeseite ein, und er wird mit dem erwarteten Wert verglichen.

Das umgesetzte OTT-Verfahren (Client-App und Serveranwendung) ist eine Eigenentwicklung der Firma Allsecure, da ihr Manager Kryptoexperte ist und gerne alles selber macht. Aus diesem Grund ist der Datenschutzbeauftrage auch der Manager selber. Eine erfolgreiche Authentifizierungssession ist aus Usability-Gründen für 1 Jahr gültig und muss dann erst erneuert werden. Der 2-Faktor Authentifizierungsdienst ist aus Kostengründen nicht redundant ausgelegt und sammelt so viele Daten wie möglich, da das Management einen monatlichen Report (Export) mit RAW-Daten als Excel-Tabelle per Email enthält, um IT-Sicherheitsangriffe zu erkennen. Das Telefonnummern-API-Gateway verwendet einen statischen symmetrischen Schlüssel für den sicheren Verbindungsaufbau zum 2-Faktor-Authentifizierungsdienst, der sich in unverschlüsselten Konfigurationsdateien auf den Servern befindet. In der Client-App der Firma Allsecure werden alle App-Daten bevorzugt auf der SD-Karte gespeichert, damit andere Allsecure-Apps (Meeting App, Pay-Everywhere App) ebenfalls darauf zugreifen können. Innerhalb des Externen Services für Telefonnummernauflösung wird auf Verschlüsselung sowohl beim Speichern als auch beim Übertragen verzichtet, da alle Verbindungen über ein internes Netz (VPN-basiert) gehen.

IT-Sicherheitsanforderungen:

Die Sicherheitsanforderung besteht darin, dass der OTT einem Angreifer nicht offengelegt wird. Es gibt vier Anforderungen, die gelten müssen.

1. Erstens sollte das OTT unversehrt, d. h. frei von Manipulationen, durchkommen.
2. Zweitens sollte das System funktionsfähig bleiben.
3. Die dritte Anforderung ist der Schutz der Privatsphäre; die Menschen wollen Ihnen vielleicht nicht ihre Handynummer geben und riskieren, dass sie für Verkaufsanrufe oder andere Zwecke missbraucht wird.
4. Es sollen alle gesetzlichen Vorgaben eingehalten werden.

Aufgabe 1

Modellieren Sie das System mit Threat Dragon in einem Datenflussdiagramm nach unter Berücksichtigung der folgenden Änderungen am Gesamtsystem:

1. Die Firma Allsecure setzt eine Firmenpolicy durch, so dass nur noch der Allsecure Mobile Phone OTT Service verwendet werden darf, der nun auch vollständig unter Kontrolle der Firma Allsecure steht.
2. Für Kryptographie wird Standard-Software eingesetzt anstelle von Eigenentwicklungen.
3. Der monatliche Management-Report soll durch Signaturen abgesichert werden und in das Bedrohungsmodell aufgenommen werden und im Gesamtsystem modelliert werden, indem ein Export-Prozess modelliert wird.
4. Die Firma Allsecure setzt nun zusätzlich ein SIEM-System ein, welches selbst betrieben wird und den 2-Faktor-Authentifizierungsdienst sowie den Allsecure Mobile Phone OTT Service überwacht.

Skizzieren Sie alle wichtigen Prozesse, alle wichtigen Datenspeicherorte, alle externen Identitäten, alle Datenflüsse sowie die entsprechenden Vertrauensgrenzen.

Aufgabe 2

Führen Sie für alle definierten Prozesse, Datenspeicherorte und Datenflüsse eine Bedrohungsmodellierung durch, indem Sie die STRIDE-Methodik anwenden und folgende Randbedingungen erfüllen:

1. *Sie haben für jede STRIDE-Kategorie eine Bedrohung definiert.*
2. *Sie haben für jedes Element des DFD, welches im Vertrauensbereich der Firma Allsecure liegt, mindestens eine Bedrohung definiert.*
3. *Sie haben insgesamt 10 Bedrohungen definiert.*
4. *Sie haben jede Bedrohung beschrieben und den Angriffsvektor erläutert.*

Aufgabe 3

Priorisieren Sie ihre gefundenen Bedrohungen mit Threat Dragon (High, Medium, Low), indem Sie die Wahrscheinlichkeit und den Schweregrad der Bedrohung analysieren. Dokumentieren Sie ihre Risikobewertung im Beschreibungstext der Bedrohung.

Aufgabe 4

Definieren Sie passende Gegenmaßnahmen für alle modellierten Bedrohungen und beschreiben Sie folgende Aspekte der Gegenmaßnahme:

1. Kurze Beschreibung der Maßnahme und wie sie gegen die Bedrohung hilft.
2. Beschreibung der technischen/organisatorischen Umsetzung der Maßnahme.
3. Bewertung der Risikoreduktion der Maßnahme und Wiederbewertung des Risikos gemäß Aufgabe 3.

Aufgabe 5

1. Vervollständigen Sie das Bedrohungsmodell mit allen notwendigen Metadaten und speichern Sie ihr finales Modell in ihrem GitHub-Repository.
2. Erstellen Sie ein PDF-Export des Reports und laden Sie diesen Report als Abschlussdokument in ILIAS hoch.

Abschlussaufgabe

Präsentieren Sie einem Tutor ihr Bedrohungsmodell und die Lösung der Aufgaben 1-5.