HAW HAMBURG

BACHELORTHESIS
Sebastian Dreesmann

Risikoanalyse einer datenbankgestützten Android-App

FAKULTÄT TECHNIK UND INFORMATIK
Department Informatik

Faculty of Computer Science and Engineering
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Sebastian Dreesmann

Risikoanalyse einer datenbankgestützten Android-App

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang *Bachelor of Science Angewandte Informatik*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr.-Ing. Martin Hübner
Zweitgutachter: Prof. Dr. Birgit Wendholt

Eingereicht am: 10.05.2024

Sebastian Dreesmann

Thema der Arbeit

Risikoanalyse einer datenbankgestützten Android-App

Stichworte

IT-Sicherheit, IT-Grundschutz, Risikoanalyse, Gefährdungsanalyse, Android-App, Android-App mit Backend, datenbankgestützte Android-App

Kurzzusammenfassung

Das Ziel dieser Arbeit ist die Sicherheit von datenbankgestützten Android-Apps anhand einer realen Anwendung, der Soundwalk App, zu analysieren. Dazu werden die Gefährdungen und Schwachstellen betrachtet und die Risiken für das Fallbeispiel ausgewertet. Abschließend werden Vorschläge gemacht, wie ausgewählte Schwachstellen des Fallbeispiels und dadurch auch die Risiken behandelt werden können.

Sebastian Dreesmann

Title of Thesis

Risk analysis of a database-supported Android-App

Keywords

IT security, risk analysis, hazard analysis, Android-App, Android-App with backend, database-supported Android-App

Abstract

The aim of this thesis is to analyse the security of database-supported Android-Apps using a real application, the Soundwalk App. To this end, the threats and vulnerabilities are analysed and the risks for the case study are evaluated. Finally, suggestions are made as to how selected vulnerabilities of the case study and thus also the risks can be dealt with.

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Motivation

Heutzutage sind Android-Apps allgegenwärtig und sobald Daten ausgetauscht oder in größeren Mengen gespeichert werden sollen, ist eine Datenbankanbindung unumgänglich. Ohne eine Internetanbindung kommen die meisten Apps auch nicht mehr weit. Seit 2014 werden pro Quartal über 200 Millionen neue Android-Smartphones verkauft [1]. Android-Apps sind nicht nur auf Smartphones zu finden, sondern auch auf anderen Android-Smart-Devices wie z. B. Android-TVs. Die Vielzahl an Mobilgeräten und Apps macht diese zu einem lukrativen Ziel für Hacker-Angriffe, wobei die Motive unterschiedlich sein können. Einerseits können Daten erlangt werden, andererseits können die Geräte selbst für eigene Zwecke genutzt werden, beispielsweise zur Bildung von Botnetzen [2]. Daraus ergibt sich, dass die Sicherheit dieser Systeme eine immer wichtigere Rolle einnimmt. Dabei ist nicht nur das Betriebssystem von Relevanz, sondern auch die einzelnen Apps, welche durch spezifische Schwachstellen ebenfalls zu gravierenden Schäden führen können. Deshalb sollte es für Entwickler und Nutzer Gleichmaßen von Interesse sein, Android-Apps mit einem Backend so sicher wie möglich zu gestalten.

1.2 Ziel der Arbeit

Die Zielsetzung dieser Arbeit besteht in der Darstellung von Risiken, die bei der Entwicklung und Verwendung einer datenbankgestützten Android-App auftreten können, sowie deren Überprüfung anhand eines eigens entwickelten Fallbeispiels. Darüber hinaus werden anhand des Fallbeispiels Maßnahmen präsentiert, mit denen die Risiken von Bedrohungen für datenbankgestützte Android-Apps reduziert werden können.

Im Rahmen dieser Arbeit werden zwei Forschungsfragen beantwortet, die wie folgt definiert wurden:

1. Welche Gefährdungen ergeben sich bei der Entwicklung und Nutzung einer datenbankgestützten Android-App?

2. Welche Maßnahmen eignen sich zur Risikominimierung, insbesondere in Bezug auf das Fallbeispiel, für die beschriebenen Bedrohungen?

1.3 Aufbau der Arbeit

Im Folgenden werden zunächst die Grundlagen von datenbankgestützten Android-Apps erläutert und sicherheitsrelevante Konzepte eingeführt, die für ein Verständnis der Sicherheitsmaßnahmen erforderlich sind. Im Anschluss wird das Fallbeispiel beschrieben, die sicherheitsrelevanten Teilsysteme analysiert und die Motive für eine hohe IT-Sicherheit erläutert. Darauf folgt eine Bedrohungsanalyse, welche sich in zwei Teile gliedert. Zunächst werden die Gefährdungen, die sich allgemein für die Arten von erkannten Teilsysteme ergeben, identifiziert und untersucht. Im zweiten Teil der Bedrohungsanalyse erfolgt eine Risikoanalyse, in der die Auswirkungen der Gefährdungen für die spezifischen Teilsysteme des Fallbeispiels evaluiert werden. Im Kapitel 5, der Auswertung, werden konkrete Schwachstellen des Fallbeispiels betrachtet und es werden Vorschläge gemacht, wie durch welche Verbesserungen diese Schwachstellen minimiert werden können. Abschließend werden die Ergebnisse zusammengefasst und diskutiert sowie ein Ausblick auf zukünftige Entwicklungen gegeben. Zudem wird überprüft, ob die Forschungsfragen ausreichend beantwortet wurden.

1.4 Einordnung und Abgrenzung

Die vorliegende Arbeit untersucht die Sicherheit von datenbankgestützten Android-Apps an einem realen Fallbeispiel. Dabei werden insbesondere die Risikoanalyse und die Empfehlungen für Maßnahmen speziell auf das Fallbeispiel abgestimmt und sind daher nur begrenzt universell einsetzbar. Die Gefährdungsanalyse wird möglichst allgemein gehalten, damit diese als

Grundlage für die Evaluation anderer Anwendungsszenarien genutzt werden kann. Die Auswahl der Maßnahmen erfolgt anhand ihrer Praktikabilität relativ zum Risiko. Dabei werden sowohl existierende Standards als auch aktuelle Entwürfe berücksichtigt. Ein ganzheitliches IT-Sicherheitskonzept für das Fallbeispiel wird nicht erstellt. Andere Systeme im Umfeld werden nicht betrachtet. Die Vorgehensweise orientiert sich inhaltlich am IT-Grundschutz [3], sowie in Struktur und Aufbau an der Bachelorarbeit „DNS-Sicherheit am Beispiel eines mittelständischen Softwareunternehmens“ von Kevin Hüsgen [4]. Es existieren alternative Vorgehensweisen, wie beispielsweise die ISO-Reihe 27000 [5], die in dieser Arbeit jedoch nicht betrachtet werden.

2 Grundlagen

2.1 IT-Sicherheit

Nach Eckert wird eine IT-System wie folgt definiert: „Ein IT-System ist ein geschlossenes oder offenes, dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen.“ [6 S. 3] Im Rahmen der Sicherheit werden von ihr drei Schutzziele für IT-Systeme definiert:

- Authentizität: „Die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar ist.“ [6 S. 8]
- Datenintegrität: „Wir sagen, dass das System die Datenintegrität (engl. integrity) gewährleistet, Integrität wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.“ [6 S. 9]
- Informationsvertraulichkeit: „Wir sagen, dass das System die Informationsvertraulichkeit (engl. confidentiality) gewährleistet, wenn es keine unautorisierte Informationsgewinnung ermöglicht.“ [6 S. 10]

„Eine Schwachstelle (Vulnerability) bezeichnet einen Fehler in einem Programm. Wenn ein Programm beispielsweise durch eine falsche Eingabe zum Absturz gebracht werden kann, dann ist das ein Fehler.“ [7] Schwachstellen werden von Angreifern [7] ausgenutzt durch sogenannte Exploits. „ Ein Exploit wird daraus erst, wenn die Schwachstelle so ausgenutzt werden kann, dass das betroffene Programm nicht einfach abstürzt, sondern tut, was der Angreifer will, z. B. Daten preisgibt oder gezielt ändert. Hacker sind ungemein kreativ, wenn es darum geht, aus einer harmlos wirkenden Schwachstelle einen Exploit zu machen. Das ist auch der Grund, weswegen viele mit IT-Security befasste Personen gar nicht mehr zwischen »gewöhnlichen« Fehlern (Bugs) und sicherheitsrelevanten Schwachstellen (Vulnerabilities) differenzieren: Es ist

im Vorhinein ganz schwer zu sagen, ob ein Fehler nur ärgerlich oder auch sicherheitsrelevant ist.“ [7]

2.2 Android-App

„Das Android-Ökosystem setzt sich aus einer Kombination von drei Komponenten zusammen:

➤ Einem freien, opensource Betriebssystem für eingebettete Geräte

➤ Eine opensource Entwicklungsplattform zur Erstellung von Anwendungen

➤ Geräte, auf denen das Android-Betriebssystem läuft (und die dafür entwickelten Anwendungen).“ [8 S. 3]

Android-Anwendungen (oder einfach "Apps") sind Softwareprogramme, die auf Android-Geräten installiert und ausgeführt werden. [8 S. 58]

3 Fallbeispiel

3.1 Die Soundwalk App

Das Digitalisierungsprojekt Open Citizen Soundwalks [9] der HAW Hamburg beschäftigt sich mit der Virtualisierung von Windparks für die Planung zukünftiger Windparks. Um zu beurteilen, wie realistisch virtuelle Windparks sind, machen die Teilnehmenden sowohl einen Rundgang durch den virtuellen als auch durch den realen Windpark. Bei beiden Rundgängen werden dieselben Fragen zur Wahrnehmung beantwortet. Diese Rundgänge werden auch als Soundwalks [10] bezeichnet.

Um die Digitalisierung der Antworten zu vereinfachen, wurde eine Android-App entwickelt, die es den Teilnehmern der realen Soundwalks ermöglicht, die Fragen direkt von ihrem Smartphone aus zu beantworten. Jeder Teilnehmer muss lediglich die Android-App installieren, kann sich dann mit einer vom Gruppenleiter mitgeteilten User-Passwort-Kombination einloggen und nach freiwilliger Angabe persönlicher Daten an der Tour teilnehmen. Anschließend können alle Stationen des Rundgangs eingesehen und ausgewählt werden, um die Fragen zu jeder Station zu beantworten. Diese beinhalten die Aufnahme einer Audiodatei, sobald eine Station erreicht wird, um weiteres Vergleichsmaterial für die Auswertung zu erhalten. Andere Fragen werden mit Hilfe von Schiebereglern oder Textfeldern beantwortet. Wenn der Benutzer entschieden hat, dass er mit der Bearbeitung der Fragen einer Station fertig ist, kann er diese bestätigen und seine Antworten abschicken. Diese Station verschwindet dann aus der Übersicht des Benutzers und der Rundgang wird fortgesetzt. Hat man alle Stationen bearbeitet, gibt es noch einen zusätzlichen Button, über den man ein kurzes Feedback zur App geben kann. Alternativ kann man die Anwendung auch einfach schließen.

3.2 Softwarearchitektur

Das System besteht aus vier Komponenten: einer React Native [11] Android-App, einem NGINX Reverse Proxy [12], einem Node.js Server [13], der auf einem NGINX Webserver [14] betrieben wird und einer PostgreSQL [15] Datenbank. Die App ist nicht öffentlich verfügbar, sondern wird über einen Microsoft Teams Raum an alle Teilnehmer verteilt. Die Anmeldedaten werden auf demselben Weg oder mündlich übermittelt. Ab dem Zeitpunkt der Anmeldung steht die App im Hintergrund in ständigem Austausch mit dem Backend, bestehend aus NGINX Reverse Proxy, einem NGINX Webserver, auf dem ein Node.js Server betrieben wird und der PostgreSQL Datenbank, die sich auf einem Server der HAW Hamburg befinden. Der NGINX Reverse Proxy sorgt dafür, dass die Applikation über das Internet mit dem Node.js Server kommunizieren kann. Der Node.js Server wertet die Anfragen der App aus, stellt Daten zur Verfügung oder persistiert Daten, indem diese an die Datenbank weitergeleitet werden. Eine Ausnahme bilden die Audiodateien, die lokal auf dem Node.js Server gespeichert werden.

3.2.1 React Native Android-App

React Native wurde für diese App als Entwicklungsframework gewählt, da ursprünglich geplant war die App sowohl für Android als auch für IOS zu kreieren. Der Code wird in JavaScript geschrieben und auf den Geräten nativ gerendert [11]. Allerdings setzte sich die Bereitstellung der IOS-Version als komplexer heraus als zunächst erwartet, da keine Erfahrung im Umgang mit Apple Produkten bestand und diverse organisatorische Schritte abgearbeitet werden müssten und wurde deshalb mit niedriger Priorität liegen gelassen.

Als Teil der Forschungsdaten werden von jedem Nutzer die folgenden Daten erfasst:

- Das Alter in einer Reichweite von 10 Jahren
- Das Geschlecht
- Erfahrungen mit Soundwalks
- Vorkenntnisse im Bereich der Akustik
- Erfahrung mit Windparks
- Einstellung zur Windenergie

Für die Entwicklung der React Native Android-App wurden die folgenden Packages verwendet:

Package	Version	Funktion
@miblanchard/react-native-slider	2.1.0	UI
@react-native-community/check-box	0.5.12	UI
@react-native-community/slider	4.2.2	UI
@react-native-picker/picker	2.4.1	UI
@react-navigation/material-top-tabs	6.2.1	Navigation
@react-navigation/native	6.0.10	Navigation
@react-navigation/native-stack	6.6.2	Navigation
axios	0.27.2	Kommunikation
moment	2.29.3	Datenverarbeitung
react	17.0.2	Grundlagen für React Komponenten
react-native	0.68.1	Deklarative UI
react-native-audio-recorder-player	3.5.1	Mikrofonaufnahmen
react-native-device-info	10.3.0	Geräteinformationen
react-native-mime-types	2.3.0	Datenverarbeitung
react-native-pager-view	5.4.15	UI
react-native-permissions	3.3.1	Berechtigungen
react-native-ratings	8.1.0	UI
react-native-safe-area-context	4.2.4	UI

react-native-screens	3.13.1	UI
react-native-sha256	1.4.8	Datenverschlüsselung
react-native-tab-view	3.1.1	UI
rn-fetch-blob	0.12.0	Datenverarbeitung

1: Übersicht der verwendeten React Native Packages

Die Packages wurden alle vom Node Package Manager [16] bezogen .

3.2.2 NGINX Reverse Proxy

Der NGINX Reverse Proxy [12] stellt die Schnittstelle zwischen der Applikation und dem Node.js Server dar. Dies war eine Anforderung der Hochschule, da kein weiterer Port für den Node.js Server öffentlich zugänglich gemacht werden sollte. Eingehende Requests werden daher an den NGINX Reverse Proxy gesendet, der so konfiguriert wurde, dass alle Requests, die einen bestimmten Pfad enthalten, an den Node.js Server weitergeleitet werden. Ein Reverse-Proxy bietet diverse Vorteile, welche sich positiv auf die Performance und Sicherheit der dahinterliegenden Applikationen auswirken können. Der Reverse-Proxy übernimmt bereits die SSL/TLS-Verschlüsselung und -Entschlüsselung sowie die SSL-Zertifizierung [17]. Auf diese Weise ist es möglich, den dahinterliegenden Node.js-Server über den HTTP-Port 3001 zu erreichen, ohne dass dies nach außen hin erkennbar ist. Darüber hinaus wird die Implementierung und Konfiguration des Node.js-Servers erheblich vereinfacht.

3.2.3 NGINX Webserver und Node.js Server

Der Node.js Server stellt das Bindeglied zwischen der App und der Datenbank dar. Er wird auf einem NGINX Webserver der Hochschule betrieben. Der Node.js Server bietet zur Kommunikation Endpunkte durch die Bereitstellung einer API, welche die von der App benötigte Funktionalität abdeckt. Für die Dokumentation der API wurde Swagger [18] eingesetzt.

Für die Umsetzung wurden folgende Packages eingesetzt:

Package	Version	Funktion
bcryptjs	2.4.3	hashing von Passwörtern
cors	2.8.5	cross origin resource sharing
express	4.18.2	Web Application Framework
jsonwebtoken	9.0.0	Authentication
multer	1.4.5-lts.1	file storage
pg	8.10.0	Datenbankanbindung
pg-hstore	2.3.4	json serialization
sequelize	6.31.0	ORM für Datenbank
swagger-jsdoc	6.2.8	Dokumentation
swagger-ui-express	4.6.0	Dokumentation

2: Übersicht der verwendeten Node.js Packages

3.2.4 PostgreSQL Datenbank

Die Wahl der PostgreSQL Datenbank [15] war eine Vorgabe der Hochschule, da bereits andere PostgreSQL Datenbanken auf der Hardware betrieben wurden und dies die Umsetzung erleichterte. In der Datenbank werden die Forschungsdaten sowie die für die Authentifizierung notwendigen Anmeldedaten und alle notwendigen Informationen zu den Stationen der Soundwalks verwaltet. Die Version von PostgreSQL zum Zeitpunkt der Inbetriebnahme war Version 15.0.

3.3 Bedeutsamkeit der Informationssicherheit

Da für die Auswertung der Umfragedaten auch Informationen über die Nutzer nach deren eigenen Angaben erhoben werden, unterliegt die App besonderen rechtlichen Bestimmungen.

Nach Art. 4 Nr. 1 DSGVO gelten Daten auch dann als personenbezogen, wenn sie die indirekte Identifizierung des Betroffenen ermöglichen [19]. Dies ist in diesem Anwendungsfall ausfolgenden Gründen nicht auszuschließen: Durch die Angabe des Windparks liegen Standortdaten vor, die mit der Hintergrundinformation, dass es sich um ein Hochschulprojekt handelt, leicht auf die Standorte der Teilnehmer schließen lassen. Es wird ein Altersbereich angegeben, der eine einfache Identifikationsmöglichkeit für Teilnehmer bietet, die außerhalb des Altersdurchschnitts der Teilnehmer liegen. Wenn jedoch zusätzliche Informationen verfügbar sind, die nicht von der Anwendung stammen, wie z.B. die Zugehörigkeit zu einer Hochschule, steigt die Wahrscheinlichkeit, dass eine Identität kompromittiert werden kann.

Die primären Schutzziele sind laut BSI Vertraulichkeit, Integrität und Verfügbarkeit [3]. Übertragen auf den Anwendungsfall Soundwalk App sind die Begriffe wie folgt zu verstehen:

1. Vertraulichkeit
   Die Forschungsdaten sind für eine Studie der Hochschule bestimmt und enthalten Daten, die als personenbezogen eingestuft werden können. Aus diesem Grund sollen Unbefugte keinen Zugriff auf diese Informationen haben.
2. Integrität
   Damit die erhobenen Daten für wissenschaftliche Zwecke verwendet werden können und ihre Glaubwürdigkeit nicht verlieren, ist es wichtig, dass diese Daten nicht unbemerkt manipuliert werden können.
3. Verfügbarkeit
   Um regelmäßige und zeitlich flexible Touren zur Datenerfassung durchführen zu können, muss das System jederzeit verfügbar sein.

Die HAW war bereits Ende 2022 Ziel eines Hackerangriffs, dessen Folgen noch zum Zeitpunkt der Bearbeitung dieser Arbeit zu spüren sind [20]. Die Soundwalk App allein stellt aufgrund der geringen Größe des Projektes kein lukratives Ziel dar, dennoch dürfen die Schutzziele nicht vernachlässigt werden, um es potenziellen Angreifern so schwer wie möglich zu machen. Um dies zu erreichen und um den aktuellen Stand der App bewerten zu können, soll in den folgenden Kapiteln eine Bedrohungs- und Risikoanalyse durchgeführt und mögliche Verbesserungen betrachtet werden.

4 Gefährdungs- und Risikoanalyse

In diesem Kapitel werden die Bestandteile der datenbankgestützten Android-App auf mögliche Gefährdungen überprüft. Zu diesem Zweck wird eine Bedrohungsanalyse durchgeführt. Die Gefährdungsanalyse ist Teil des Security Engineering und verfolgt eine möglichst vollständige Erfassung der Gefährdungen eines IT-Systems und kann mit verschiedenen methodischen Ansätzen durchgeführt werden. Eine Gefährdung ist ein Ereignis oder eine Situation, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann [6]. Ziel einer Bedrohung ist es immer, die Schwachstellen oder Verwundbarkeiten eines Systems auszunutzen, um die Schutzgüter zu gefährden. Dadurch entsteht ein Schaden für den Besitzer oder Nutzer der Information. Die hier durchgeführte Gefährdungsanalyse orientiert sich am IT-Grundschutz für IT-Systeme mit hohem Schutzbedarf, da bei der Standardabsicherung für IT-Systeme mit normalem oder niedrigem Schutzbedarf auf eine Gefährdungsanalyse verzichtet wird [3].

Zunächst wird die Gefährdungsanalyse durchgeführt, damit im zweiten Abschnitt die Risikoanalyse durchgeführt werden kann.

4.1 Ermittlung und Analyse möglicher Gefährdungen

Eine datenbankgestützte Android-App besteht aus mindestens drei Komponenten: Der App auf dem Endgerät, einer Datenbank und einem Webserver, für die Kommunikation zwischen App und Datenbank. In diesem Abschnitt sollen die Gefährdungen der einzelnen Komponenten aufgezeigt werden, um deren Auswirkung auf das Gesamtprodukt anschließend in der Risikoanalyse zu bewerten. Quellen möglicher Gefährdungen sind nicht nur externe Bedrohungen, sondern auch systeminterne Fehler [3]. Die folgende Tabelle stellt die verwendeten Abkürzungen dar.

	Abkürzung	Beschreibung
Komponenten	A	Android-App
	D	Datenbank
	W	Webserver
Schutzziele	C	Vertraulichkeit
	I	Integrität
	A	Verfügbarkeit

3: Legende der verwendeten Abkürzungen

Das IT-Grundschutz-Kompendium des BSI gliedert sich in mehrere Bausteine. Der Baustein APP.1.4 Mobile Anwendungen umfasst den Schutz von Informationen, die mit Hilfe von Anwendungen auf mobilen Endgeräten verarbeitet werden. Dabei werden alle Arten von mobilen Anwendungen betrachtet, die auf mobilen Betriebssystemen wie Android oder iOS und entsprechenden mobilen Endgeräten installiert sind. Anforderungen an die jeweiligen Betriebssysteme bzw. an die Entwicklung wird separat im Baustein SYS.3.2.4 Android behandelt. Da eine Applikation in ihrer gesamten Client-Server-Struktur betrachtet werden muss, um eine ganzheitliche Informationssicherheit zu gewährleisten, müssen auch die in den Bausteinen SYS.1.1 Allgemeiner Server, APP.3.2 Webserver und APP.4.3 Relationale Datenbanksysteme für diese Applikation betrachteten Bedrohungen berücksichtigt werden [3]. Mit Hilfe dieser Bausteine werden zunächst alle relevanten Gefährdungen für die datenbankgestützte Android-App ausgewählt.

Grundlegende elementare Gefährdungen, auf die kein wesentlicher Einfluss genommen werden kann wie z.B. Ausfall oder Störung von Stromversorgung oder Kommunikationsnetzen, wird in den folgenden Analysen nicht eingegangen, auch wenn diese gerade für die Verfügbarkeit eine große Rolle spielen. Der Fokus soll auf Gefährdungen liegen, die realistisch beeinflusst werden können.

Nr	Gefährdung	Betroffene Komponente	Betroffene Schutzziele
1	Ausspähen von Informationen	A D W	C
2	Abhören	A D W	C
3	Diebstahl von Geräten, Datenträgern oder Dokumenten	A D W	C, A
4	Verlust von Geräten, Datenträgern oder Dokumenten	A	C, A
5	Fehlplanung oder fehlende Anpassung	A D W	C, I, A
6	Offenlegung schützenswerter Informationen	A W	C
7	Informationen oder Produkte aus unzuverlässiger Quelle	A W	C, I, A
8	Manipulation von Hard- oder Software	A W	C, I, A
9	Manipulation von Informationen	D W	I

10	Unbefugtes Eindringen in IT-Systeme	A D W	C, I
11	Ausfall von Geräten oder Systemen	A D W	A
12	Fehlfunktion von Geräten oder Systemen	A D W	C, I, A
13	Ressourcenmangel	D W	A
14	Software-Schwachstellen oder -Fehler	A D W	C, I, A
15	Unberechtigte Nutzung oder Administration von Geräten und Systemen	A D W	C, I, A
16	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	A D W	C, I, A
17	Missbrauch von Berechtigungen	A W	C, I, A
18	Identitätsdiebstahl	A	C, I, A
19	Abstreiten von Handlungen	W	C, I
20	Missbrauch personenbezogener Daten	A	C
21	Schadprogramme	A W	C, I, A

22	Verhinderung von Diensten (DoS)	A W	A
23	Sabotage	A	A
24	Social Engineering	A D W	C, I
25	Einspielen von Nachrichten	W	C, I
26	Datenverlust	D W	A
27	Integritätsverlust schützenswerter Informationen	A D W	I

4: Gefährdungen der datenbankgestützten Android-App nach BSI

Im nächsten Schritt werden die in der Tabelle 4: Gefährdungen der datenbankgestützten Android-App nach BSI identifizierten Gefährdungen näher betrachtet und es wird erläutert, wie sie die zugeordneten Sicherheitsziele gefährden.

G 1 – Ausspähen von Informationen

Es besteht die Möglichkeit, dass sämtliche Komponenten der datenbankgestützten Android-App durch sogenannte Spyware kompromittiert werden und dadurch die Vertraulichkeit der gespeicherten Daten verloren geht. Der Begriff „Spyware" bezeichnet Software, die ohne Zustimmung des Nutzers Informationen über ihn und sein System sammelt [6]. Diese Informationen umfassen jedoch nicht ausschließlich: Die Online-Aktivität, Keylogging, die Kamera und das Mikrofon sind potenzielle Angriffspunkte für Spyware. Um die Gefährdung einer Komponente durch Spyware zu beurteilen, ist eine Betrachtung der kompromittierbaren Informationen sowie der Infektionswahrscheinlichkeit erforderlich. Im Falle einer bereits erfolgten Infektion des Systems mit Spyware ist zu eruieren, inwiefern die Spyware in der Lage ist, Informationen von der spezifischen Komponente zu erlangen.

G 2 – Abhören

Unter dem Begriff des Abhörens, im Englischen „Eavesdropping", versteht man einen passiven Angriff, bei dem Kommunikationsleitungen aufgezeichnet und analysiert werden, um gegebenenfalls unverschlüsselte Daten oder Verhaltensmuster zu erlangen. Im Falle einer datenbankgestützten Android-App ist die anfälligste Stelle im System für einen derartigen Angriff die Kommunikation zwischen der App und dem Webserver. In Szenarien, in denen der Webserver und die Datenbank physisch getrennt sind, stellt diese Kommunikationsschnittstelle ebenfalls ein attraktives Ziel zum Abhören dar. Um die Gefährdung der datenbankgestützten Android-App durch Abhören einschätzen zu können, muss also zunächst betrachtet werden, wie die Kommunikation zwischen den Komponenten konzipiert ist. Durch das Abhören kann die Vertraulichkeit von Informationen verletzt werden.

G 3 – Diebstahl von Geräten, Datenträgern oder Dokumenten

Der Diebstahl von Systemkomponenten führt in erster Linie zu einer Verletzung des Schutzziels „Verfügbarkeit". Im Rahmen der Untersuchung ist zu eruieren, inwiefern das Gesamtsystem noch funktionsfähig ist, wenn einzelne Komponenten fehlen. Gleichzeitig ist bei einem Diebstahl davon auszugehen, dass der Täter bösartige Intentionen hat. Des Weiteren ist zu untersuchen, inwiefern der Täter mit dem physischen Gerät in der Lage ist, an Informationen des zu schützenden Systems zu gelangen. Mobile Geräte sind aufgrund ihrer physischen Beschaffenheit und ihrer Ortsungebundenheit besonders anfällig für Diebstahl. Der Diebstahl eines Servers ist ein seltenes Szenario, das jedoch nicht gänzlich ausgeschlossen werden kann, insbesondere wenn Mitarbeiter involviert sind. Ein besonders prominentes Beispiel für die missbräuchliche Verwendung gestohlener Smartphones ist das sogenannte Bruteforcing von Passwörtern, um sich Zugang zu persönlichen Daten zu verschaffen und damit das Schutzziel Vertraulichkeit zu verletzen.

G 4 – Verlust von Geräten, Datenträgern oder Dokumenten

Diese Gefährdung kann als Spezialfall von G3 bezeichnet werden. Der wesentliche Unterschied besteht darin, dass die Wahrscheinlichkeit, dass Vertraulichkeit verletzt wird, geringer ist als bei G3, da beim Verlust nicht direkt von einem Täter oder gar einer bösartigen Intention ausgegangen werden muss. Da jedoch aufgrund situativer Taten ein Restrisiko nicht gänzlich ausgeschlossen werden kann, ist auch diese Gefährdung zu berücksichtigen.

G 5 – Fehlplanung oder fehlende Anpassung

Die Fehlplanung birgt das Risiko, dass Schäden ohne Fremdeinwirkung entstehen, ohne dass ein Angreifer involviert ist. Dies betrifft alle Komponenten gleichermaßen. In der Android-App können die Schutzziele verletzt werden, indem bei der Planung notwendige Features nicht berücksichtigt werden oder nicht kompatible Packages bei der Entwicklung der App gewählt werden. Eine weitere Schwachstelle stellt die API des Webservers dar, die in der Planung häufig nicht ausreichend berücksichtigt wird. Dies kann dazu führen, dass eine reibungslose Kommunikation mit der Applikation von Beginn an nicht möglich ist. Fehler, die beim Planen des Datenbank-Schemas gemacht werden, können dazu führen, dass Informationen nicht korrekt abgespeichert werden können oder verloren gehen. Ein unzureichend durchdachtes Schema kann dazu führen, dass eine größere Anzahl an Operationen, die mit einem hohen Aufwand an Rechenleistung verbunden sind, erforderlich ist, um die Daten zu verarbeiten.

Eine fehlende Anpassung oder auch Fehler bei der Anpassung können bei der App entstehen, wenn Aktualisierungen von Paketen durchgeführt werden, die neuen Versionen jedoch nicht mehr kompatibel sind. Ein besonders häufig auftretendes Szenario, gerade bei der Verwendung von Frameworks wie React Native oder Flutter, ist die Entscheidung zwischen der Aktualisierung für ein neues Sicherheitsupdate und der damit einhergehenden Änderung diverser Abhängigkeiten zu anderen Paketen. Dies kann erforderlich sein, wenn die neuen Versionen der Pakete nicht mehr kompatibel sind oder Abhängigkeiten zu älteren Versionen der anderen Pakete aufweisen.

Grundsätzlich ist es schwierig, alle sicherheitstechnischen Aspekte vorausblickend in der Planung zu berücksichtigen. Dies führt in vielen Szenarien dazu, dass diese auch im weiteren Verlauf nicht ausreichend berücksichtigt werden. Die Qualität der Sicherheit leidet, und es wird mehr Angriffsfläche für Angreifer geboten. Wenn während der Entwicklung der Sicherheitsaspekt vernachlässigt wird, ermöglicht dies die Bedrohungen beschrieben in OWASP M2 [21].

G 6 – Offenlegung schützenswerter Informationen

Die Offenlegung schützenswerter Informationen ist eine Gefährdung, die durch die Verletzung der Schutzziele Vertraulichkeit und Integrität bei diversen anderen Gefährdungen entsteht. Hervorgerufen durch technisches Versagen bei den Gefährdungen G8, G11, G12 und G14; durch Unachtsamkeit bei G16 und G24; durch vorsätzliche Handlungen bei G3, G10, G15 und

G17. Da diese Gefährdungen alle individuell betrachtet werden wird die Gefährdung G6 nicht weiter in der folgenden Risikoanalyse betrachtet.

G 7 – Informationen oder Produkte aus unzuverlässiger Quelle

Im Hinblick auf Produkte aus unzuverlässiger Quelle ist insbesondere die Komponente „Android-App" zu nennen. Dies kann auf das Android-Gerät, auf welchem die App betrieben wird, bezogen werden. Wurde das Gerät aus einer unzuverlässigen Quelle bezogen, etwa als Secondhandgerät, besteht die Möglichkeit, dass es bereits vor dem Erwerb durch den Nutzer mit Malware infiziert wurde. Dadurch können Einschränkungen für Vertraulichkeit, Integrität und Verfügbarkeit entstehen. Alternativ besteht die Möglichkeit, dass Apps, sofern sie nicht aus regulierten Quellen bezogen werden, manipuliert worden sind. Der Bezug einer App aus dem offiziellen App-Store impliziert, dass diese diversen Prüfungen unterzogen wurde, was zwar nicht ausschließt, dass sie schädlich ist, jedoch die Wahrscheinlichkeit eines Schadens wesentlich verringert. Die Herkunft von Informationen kann unzuverlässig sein, wenn der Webserver keine Möglichkeit hat, die Legitimität des Versenders dieser Informationen zu verifizieren. Selbst bei Vorliegen einer Identifizierung können bestimmte Angriffsformate wie „Man in the Middle"-Angriffe nicht ausgeschlossen werden, sodass trotz Identifizierung eine Verfälschung der Informationen möglich ist.

G 8 – Manipulation von Hard- und Software

Die Manipulation von Software kann auf unterschiedliche Weise erfolgen. Eine signifikante Gefahr geht von einer Infektion während des Entwicklungsprozesses aus. Die OWASP mobile Top 10 [22] listet Risiken für mobile Geräte auf und thematisiert dabei auch die nicht ausreichende Sicherheit während des Entwicklungsprozesses. Es besteht die Möglichkeit, dass bereits Tools für das Erstellen der App so manipuliert werden, dass das daraus gefertigte Produkt Schwachstellen aufweist, die von einem eingeweihten Angreifer problemlos ausgenutzt werden können [21]. Gleichzeitig resultieren daraus Schwachstellen, deren Existenz nicht in Betracht gezogen wird. Eine weitere Möglichkeit der Manipulation von Software stellt die Modifikation oder Anpassung von Konfigurationsdateien dar, wodurch Schwachstellen im System auftreten können. Dies betrifft alle Komponenten in gleicher Weise.

G 9 – Manipulation von Informationen

Die Manipulation von Informationen betrifft die Komponenten Webserver und Datenbank. In diesem Kontext besteht die Möglichkeit, dass Daten mittels eines Man-in-the-Middle-Angriffs abgefangen und verändert weitergeleitet werden [6]. Eine weitere Ursache für manipulierte Daten könnte in Softwaremanipulationen liegen, die das Ziel der Datenverfälschung verfolgen. Die größte Gefahr für die Datenbank geht von gezielten Veränderungen bestimmter Felder oder gar ganzer Tabellen aus. In diesem Kontext ist der Berechtigungsgrad der handelnden Person von entscheidender Bedeutung. Dies macht eine Untersuchung der Gefährdungen G10, G15, G16 und G24 erforderlich.

G 10 – Unbefugtes Eindringen in IT-Systeme

Für die Untersuchung der Gefährdung des unbefugten Eindringens in IT-Systeme müssen die einzelnen Komponenten auf ihre Schnittstellen untersucht werden, da sich in den meisten Fällen unbefugte über diese Schnittstellen Zugriff auf das System verschaffen. Wesentliche Schnittstellen, die es zu betrachten gilt, sind die Kommunikationsschnittstelle der App, um mit dem Webserver zu kommunizieren, die API des Webservers und die Anbindungsschnittstelle des Webservers für die Datenbank. Wird beispielsweise eine unsichere Authentifikation und Autorisierung verwendet, wird es dem Angreifer einfacher gemacht, unbefugt auf die Schnittstellen zuzugreifen und Schaden anzurichten [23]. Besteht erstmal Zugriff auf das IT-System können alle Schutzziele aller Komponenten verletzt werden.

G 11 – Ausfall von Geräten oder Systemen

Es besteht bei jeder Komponente des Systems die Möglichkeit, dass sie ausfällt. Die Ursachen hierfür können in Hardware-Defekten begründet liegen, jedoch können auch andere Gefährdungen, wie beispielsweise DoS-Attacken gegen den Webserver, zu diesem Ergebnis führen. Der Ausfall diverser Komponenten kann divergierende Konsequenzen nach sich ziehen. Es ist zu eruieren, inwiefern der Ausfall einer Komponente das Gesamtsystem beeinflusst.

G 12 – Fehlfunktion von Geräten oder Systemen

Die Relevanz von Fehlfunktionen von Geräten oder Systemen ist höher zu bewerten als der Ausfall von Geräten oder Systemen, da nicht nur die Verfügbarkeit eingeschränkt wird, sondern auch das Potenzial für einen möglichen Datenverlust oder Zugriff durch Unbefugte

besteht. Die Ursachen für Fehlfunktionen sind vielfältig und umfassen veraltete Hardware ebenso wie fehlerhafte Softwareupdates. Bei der Android-App ist insbesondere beim Aktualisieren von Paketen darauf zu achten, dass dadurch keine Inkompatibilitäten innerhalb der App entstehen. Auch beim Webserver ist dies zu beachten, insbesondere bei Verwendung von Node.js, da Node.js auf der gleichen paketbasierten Struktur basiert. Diese Fehler manifestieren sich nicht zwangsläufig in einem Funktionsverlust, sondern können im schlimmsten Fall dafür sorgen, dass schwer nachvollziehbare Fehler in den Arbeitsprozess des Systems eingeschleust werden. Ein Beispiel für eine mögliche Fehlerquelle ist die fehlerhafte Verbindung zur Datenbank. Dadurch können Daten, die in die Datenbank eingetragen werden, verfälscht werden.

G 13 – Ressourcenmangel

Der Begriff des Ressourcenmangels beschreibt die Situation, in der die Kapazitäten der verwendeten Komponenten nicht ausreichen, um eine reibungslose Nutzung des Systems für alle Nutzer zu gewährleisten. Diesbezüglich sei darauf verwiesen, dass es sich sowohl um einen Mangel an Speicherbedarf beim Webserver handeln kann als auch um die Begrenzung parallel möglicher Anfragen an den Webserver oder die Datenbank. Es ist von essenzieller Bedeutung, dass sowohl die Webserver- als auch die Datenbankkomponente skalierbar sind, um die Verfügbarkeit der Komponenten nicht einzuschränken.

G 14 – Softwareschwachstellen oder -Fehler

Softwareschwachstellen oder -fehler stellen einen Auslöser für eine Vielzahl der in diesem Kapitel beschriebenen Gefährdungen dar. Sie können bei allen Komponenten auftreten und aus verschiedenen Gründen entstehen. Als eine typische Quelle, die unabhängig von der Komponente zu betrachten ist, kann selbst geschriebener Code identifiziert werden. Oftmals wird die Fehleranfälligkeit von Code, insbesondere wenn die Sicherheit des Codes hinter der Funktionalität zurücktritt, unterschätzt. In Kombination mit unzureichenden Tests können folglich Sicherheitslücken entstehen, die von Angreifern ausgenutzt werden können. Des Weiteren können Fehler auftreten, welche die Funktionalität des Systems beeinträchtigen. Oftmals werden Bibliotheken in den eigenen Code eingebunden, um die Entwicklung zu beschleunigen und die Wiederverwendung bereits entwickelter Komponenten zu ermöglichen. Dies resultiert in einer gesteigerten Produktivität, jedoch ist gleichzeitig eine Kenntnis der Schwachstellen verwendeter Pakete erforderlich. Gleichzeitig ist eine regelmäßige Aktualisierung dieser Bibliotheken erforderlich, wobei es zu Fehlern kommen kann, wenn sich die Abhängigkeiten zwischen den

Versionen ändern. Ein aktuelles Beispiel ist die Backdoor in XZ Tools und -Bibliotheken für Linux [24].

G 15 – Unberechtigte Nutzung oder Administration von Geräten und Systemen

Es ist zu eruieren, auf welche Weise innerhalb des Systems und der einzelnen Komponenten determiniert wird, welche Handlungen ein Nutzer vornehmen darf und auf welche Daten er Zugriff hat. Die Beantwortung dieser Frage führt zu dem Schluss, dass Berechtigungen eine entscheidende Rolle spielen. Die bloße Nutzung der Systeme führt in der Regel nicht zu einer Verletzung der Vertraulichkeit, sofern keine Administrator-Berechtigungen vorhanden sind. Andernfalls besteht die Möglichkeit, weiteren Schaden anzurichten. Im Rahmen der Applikation ist zu definieren, welche Berechtigungen seitens des Betriebssystems erforderlich sind, um die Anwendung ohne Probleme ausführen zu können. Eine manipulierte Version der App könnte beispielsweise nach zusätzlichen Berechtigungen für die Kamera fragen. Es ist zu beobachten, dass eine Vielzahl von Nutzern nicht mit der gebotenen Sorgfalt darauf achtet, welche Berechtigungen sie welchen Apps erteilt. In der Theorie genügt es bereits, wenn im Code der App die Android Manifest Konfigurationsdatei geringfügig modifiziert wird, um zusätzliche Berechtigungen anzufordern. Bei der Datenbank ist es von besonderer Relevanz, dass nicht-administrative Nutzer lediglich über die minimal erforderlichen Berechtigungen verfügen, um im Falle eines kompromittierten Nutzers das Löschen von Daten oder ähnliches zu verhindern. Aus diesem Grund wird in der Regel ein API-Service verwendet, damit Nutzer über Endpunkte nur ganz spezifische Zugriffsmöglichkeiten auf die Datenbank erhalten. Eine unzureichende oder fehlerhafte Implementierung von Nutzeridentifikation und -authentifizierung innerhalb des Gesamtsystems ermöglicht einem Angreifer den Zugriff auf Systemkomponenten. Sofern es einem Angreifer gelingt, innerhalb des Systems Administrator-Berechtigungen zu erlangen, kann der dadurch verursachte Schaden erheblich sein und im schlimmsten Fall sogar zum Einsturz des gesamten Systems führen. Es ist daher unerlässlich, die Vergabe von Berechtigungen bei allen Komponenten einer genauen Prüfung zu unterziehen und sicherzustellen, dass ein klarer Überblick über die Berechtigungen besteht, die jeder Nutzer innerhalb jeder Komponente besitzt.

G 16 – Fehlerhafte Nutzung oder Administration von Geräten und Systemen

Die fehlerhafte Nutzung von Komponenten durch Anwender kann zwar vorkommen, hat in der Regel jedoch keine großen Auswirkungen auf die Gefährdung des Systems. Ein Sonderfall bei

Android stellt die Verwendung eines gerooteten Systems dar, da dies Angreifern die Arbeit erleichtern könnte, Malware oder andere Software zur Infiltration des Systems oder einzelner Komponenten auf das Gerät zu installieren. Ein Verlust der Integrität von Daten könnte bei einer mutwilligen Eingabe falscher Daten argumentiert werden, wobei dies jedoch abhängig vom spezifischen Anwendungsfall ist. Eine kritischere Situation ergibt sich bei einer fehlerhaften Administration von Komponenten, beispielsweise bei einer zu großzügigen Vergabe von Berechtigungen. Somit gelangt man zur Gefährdung G15, der unbefugten Nutzung und Administration von Geräten, die durch einen Fehler bei der Administration entstand.

G 17 – Missbrauch von Berechtigungen

Ein weiteres Problem, das im Kontext der Berechtigungen diskutiert werden muss, ist der Missbrauch von Berechtigungen. Hierbei werden erteilte Berechtigungen zweckentfremdet. Sofern einer Applikation die Berechtigung erteilt wird, das Mikrofon des Gerätes zu verwenden, sollte dies ausschließlich für den ursprünglich geplanten Zweck erfolgen. Eine Nutzung zu anderen Zwecken, zu denen der Anwender nicht eingewilligt hat, ist unzulässig. Alternativ könnte auch ein legitimer Administrator der Datenbank seine Berechtigungen ausnutzen, um Daten zu seinen eigenen Gunsten zu manipulieren, zu löschen oder zu verbreiten. Ein besonders kritischer Fall ist gegeben, wenn der Missbrauch von Berechtigungen auf fehlerhafter oder unbefugter Administration beruht.

G 18 – Identitätsdiebstahl

Ein Identitätsdiebstahl kann dann erfolgen, wenn mit kritischen personenbezogenen Daten gearbeitet wird. Auch wenn das zu untersuchende System selbst nicht mit diesen Informationen arbeitet, besteht die Gefahr eines Identitätsdiebstahls, sofern Smartphones involviert sind. In der heutigen Zeit wird eine Vielzahl persönlicher Informationen auf Smartphones gespeichert. Als Beispiele können Wallet-Apps oder Impfzertifizierungen genannt werden. Durch das zu untersuchende System entstehende Schwachstellen, welche benachbarte Systeme, in diesem Fall andere Android-Apps auf demselben Betriebssystem, ebenfalls gefährden, erhöhen die Wahrscheinlichkeit eines Identitätsdiebstahls durch das zu untersuchende System. Szenarien, die einen Identitätsdiebstahl beinhalten, sind für die Gefährdung der Identität von besonderer Relevanz.

G 19 – Abstreiten von Handlungen

Das Abstreiten von Handlungen erlangt insbesondere dann Relevanz, wenn es darum geht, Aktionen zu vertuschen. Dies ist für Angreifer insbesondere dann von Interesse, wenn sie wünschen, dass ihre Handlungen im System unbemerkt bleiben. In der Regel werden Webserver-Logs geführt, in denen die ein- und ausgehende Kommunikationshistorie nachvollzogen werden kann. Sofern es dem Angreifer gelingt, die Logs zu manipulieren, sodass bestimmte Kommunikationsabfolgen als nie stattgefunden erscheinen, wird es schwieriger festzustellen, dass dieser Angreifer überhaupt existiert. Dies gilt insbesondere, sofern er sich nicht auf anderem Wege verrät.

G 20 – Missbrauch personenbezogener Daten

Im Rahmen der Prüfung eines etwaigen Missbrauchs personenbezogener Daten sind zwei wesentliche Aspekte zu betrachten. Zunächst ist zu eruieren, ob lediglich Daten, die für die Anwendung relevant sind, erfasst werden. Diesbezüglich ist eine explizite Zustimmung des Nutzers erforderlich. Gleichzeitig ist die Verwendung der Daten auf den angegebenen Zweck beschränkt. Ein Beispiel für die Einhaltung dieser Vorgaben wäre die Nichtnutzung von Daten, die zur Identifikation im WLAN erfasst werden, zur Aufzeichnung oder Überprüfung der Arbeitsdauer, sofern dem nicht explizit zugestimmt wurde. Die missbräuchliche Verwendung dieser Daten kann unterschiedliche Formen annehmen, die von der Art der Daten abhängig sind. In gravierenden Fällen kann es zu Identitätsdiebstahl gemäß § 269 StGB (G18) oder ähnlichen Delikten kommen.

G 21 – Schadprogramme

Der Begriff „Schadprogramm“ bezeichnet Software, die mit der Intention entwickelt wurde, in ein System einzudringen und dieses zu infiltrieren. In vielen Fällen ist das Ziel der Schadprogramme die Beschädigung oder Zerstörung des infizierten Systems. Zu den bekanntesten Beispielen zählen Trojaner, Viren und Würmer, welche die Fähigkeit besitzen, Informationen zu stehlen, zu löschen oder zu verfälschen. Im Rahmen der Überprüfung ist für jede Komponente zu eruieren, welche Schwachstellen existieren, die eine Infiltration mit den derzeit bekannten Typen von Schadprogrammen ermöglichen. Ein Beispiel hierfür wäre OWASP M2 [21] oder die mutwillige Ausnutzung von Berechtigungen. Des Weiteren ist das Szenario zu berücksichtigen, dass das Betriebssystem einer oder mehrerer Komponenten bereits mit

Schadprogrammen infiziert sein könnte. In diesem Zusammenhang ist zu eruieren, wie mit dieser Situation adäquat umgegangen werden kann.

G 22 – Verhinderung von Diensten (DoS)

Der Begriff „Verhinderung von Diensten" bezeichnet eine Situation, in der Systemkomponenten derart beeinträchtigt werden, dass sie ihre Funktionen nicht mehr in zuverlässiger Weise erfüllen können. In diesem Kontext wird auch der Begriff „Denial of Service" verwendet. Im Rahmen der Untersuchung ist zu eruieren, welche Komponenten anfällig für Denial-of-Service-Attacken sind und in welchem Umfang das Gesamtsystem dadurch beeinträchtigt werden kann. Zu den für Webserver typischen Attacken zählen DDoS-Attacken, bei denen der Server mit einer so großen Menge von Anfragen bombardiert wird, dass legitime Nutzeranfragen gar nicht mehr durchkommen. Auch Android-Apps können durch ReDoS-Attacken beeinträchtigt werden.

G 23 – Sabotage

Unter einer Sabotage versteht man eine Manipulation mit dem Ziel Schaden anzurichten. Demnach ist diese Gefährdung ein Härtefall von G8 – Manipulation von Hard- und Software.

G 24 – Social Engineering

Beim Social Engineering wird nicht die Software oder die Hardware des Systems angegriffen. Stattdessen wird versucht, die Hilfsbereitschaft oder Unwissenheit von Menschen auszunutzen, die den Angreifern geben können, was sie wollen. Dies kann in Form von Zugangsdaten, Berechtigungen oder Zugriff auf Hardware erfolgen, welche die Person eigentlich nicht erhalten sollte. So besteht die Möglichkeit, dass Unbefugte einen Weg ins System finden, ohne dass die technischen Sicherheitsvorkehrungen dies verhindern können. Es ist zu prüfen, welche Systemkomponenten anfällig für Social Engineering sein können. Dafür muss vor allem die Rolle aller Menschen, die mit dem System interagieren, betrachtet werden.

G 25 – Einspielen von Nachrichten

Das Einspielen von Nachrichten stellt eine Angriffsform dar, bei der die Kommunikation zwischen Komponenten attackiert wird. Die Verwendung von Schnittstelleninformationen oder die Aufzeichnung vergangener Kommunikationsverläufe zielt darauf ab, Informationen

abzufangen oder Zugriff auf das System zu erlangen. Als Beispiele können Replay-Attacken oder Man-in-the-Middle-Attacken genannt werden.

G 26 – Datenverlust

Eine mögliche Folge diverser Bedrohungen.

G 27 – Integritätsverlust schützenswerter Informationen

Eine mögliche Folge diverser Bedrohungen.

Die Gefährdungen G26 – Datenverlust und G27 – Integritätsverlust sind elementare Gefährdungen nach BSI allerdings treten sie in diesem Anwendungsfall nur als Folgen anderer, ebenfalls untersuchter Gefährdungen auf. Aus diesem Grund werden sie in der folgenden Risikoanalyse nicht als eigenständige Gefährdung betrachtet und analysiert.

4.2 Risikoanalyse

Die identifizierten allgemeinen Bedrohungen gegen eine datenbankgestützte Android-App werden nun in der Risikoanalyse bewertet und auf das Fallbeispiel übertragen. Das Ergebnis der Risikoanalyse bildet die Grundlage für die Bewertung, die aufzeigt, welche Mittel und Wege zur Risikominimierung eingesetzt werden können. Die durchgeführte Risikoanalyse basiert auf dem BSI-Standard 200-3 [25], der auf dem IT-Grundschutz aufbaut.

Das Risiko einer Gefährdung setzt sich aus zwei Komponenten zusammen: der Eintrittshäufigkeit der Gefährdung und der Schadenshöhe. Die Schadenshöhe wird anhand der Auswirkung der Gefährdung geschätzt, wobei direkte Schäden und Folgeschäden sowie der Aufwand zur Behebung des Schadens berücksichtigt werden. Die Eintrittshäufigkeit soll laut BSI durch geeignetes Fachpersonal, ggf. unterstützt durch Statistiken und eigene Erfahrungen, eingeschätzt werden. Da für das Fallbeispiel keine Statistiken vorliegen und die eigene Erfahrung begrenzt ist, sodass keine fundierten Einschätzungen für die Eintrittshäufigkeit gemacht werden können, wird alternativ mit einer Eintrittswahrscheinlichkeit gearbeitet. Die Eintrittswahrscheinlichkeit setzt sich aus dem geschätzten Aufwand der Durchführung für einen Angreifer und dem geschätzten Nutzen, den er daraus ziehen kann, zusammen.

Schadenshöhe	Schadensauswirkung
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß annehmen.

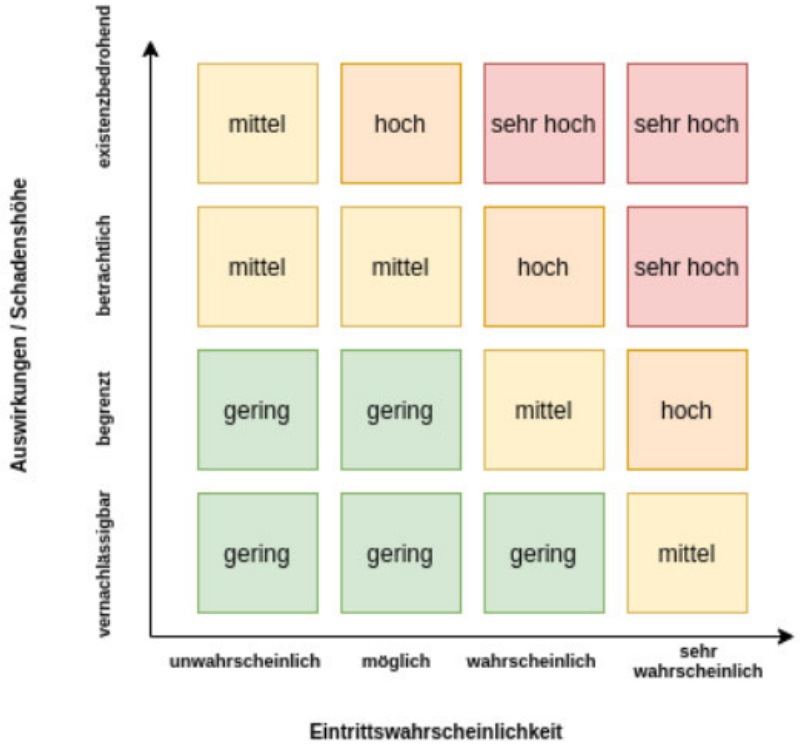
5: Klassifikation von Schadensauswirkungen [25]

Eintrittswahrscheinlichkeit	Beschreibung
unwahrscheinlich	Ein Angreifer kann kaum eine Schwachstelle finden und ausnutzen. Potenzielle Schwachstellen werden durch regelmäßige Kontrolle entdeckt und behoben. Das Risiko kann aber nicht ausgeschlossen werden.
möglich	Ein versierter Angreifer mit tiefem Verständnis über die Infrastruktur kann die Schwachstelle mit großem Aufwand ausnutzen. Entdeckte Schwachstellen können schnell behoben werden.
wahrscheinlich	Ein Angreifer kann mit vertretbarem Aufwand die Schwachstelle ausnutzen. Entdeckte Schwachstellen können nicht sofort behoben werden.
sehr wahrscheinlich	Ein Angreifer kann mittels öffentlicher Informationen und Exploits die Schwachstelle ausnutzen. Schwachstellen werden sofort ausgenutzt und können nicht entdeckt und behoben werden.

6: Klassifikation von Eintrittswahrscheinlichkeiten für Gefährdungen mit Angreifer [4]

Das Spektrum potenzieller Angreifer ist äußerst vielfältig, was ihre Ressourcen und ihr Know-how betrifft. Daher ist es sinnvoll, diese für die Risikoanalyse genauer zu spezifizieren. In der Konsequenz wird für die Risikoanalyse das Profil von Angreifern auf Skript-Kiddies, Mitarbeiter und Hacker, die mit einem geringen Budget arbeiten, begrenzt.

In den folgenden Unterkapiteln wird für jede relevante Systemkomponente auf die identifizierten Gefährdungen abgebildet und eine Eintrittswahrscheinlichkeit aus Tabelle 6: Klassifikation von Eintrittswahrscheinlichkeiten und eine Schadenshöhe aus Tabelle 5: Klassifikation von Schadensauswirkungen zugewiesen, anhand welcher Kombination das Risiko aus der Matrix ablesen lässt. Für Gefährdungen, bei denen ein Angreifer keine Rolle spielt, wird die Eintrittswahrscheinlichkeit anhand der Plausibilität für das Fallbeispiel vom Autor eingeschätzt. Bei der Risikoanalyse sollten folgende Punkte bezüglich des Fallbeispiels beachtet werden: Die Soundwalk App hat eine kleine Nutzerbasis, die sich bis auf wenige Ausnahmen aus Studenten und Angestellten der HAW zusammensetzt. Das Ziel der App liegt in der Erfassung von Forschungsdaten, weshalb das Schutzziel Integrität etwas stärker gewichtet wird als die anderen Schutzziele.



1: Risiko Matrix [4]

4.2.1 Android-App

G1 – Ausspähen von Informationen		**Gefährdete Schutzziele:** C
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
wahrscheinlich	begrenzt	mittel
Beschreibung Spyware für mobile Geräte, vor allem Android, ist weit verbreitet und kann aus verschiedensten Quellen stammen. Die Soundwalk App kann zwar dafür sorgen, dass durch sie keine Spyware auf das Gerät gelangt, allerdings hat sie keinen Einfluss auf bereits vorhandene Spyware.		
Erläuterung Ob ihr Gerät mit Spyware infiziert ist, ist den meisten Menschen nicht bewusst, sofern es nicht von einer Defaultmäßigen Schutzmaßnahme wie z.B. dem Play Protect Feature des Google Playstores aufgedeckt wird. Ein weiterer Faktor, der in die Bewertung mit einfließt, ist, dass die Soundwalk App auf vielen verschiedenen Geräten installiert wird. Solange eines davon infiziert ist, hat der Angreifer Erfolg. Die Soundwalk App erfasst nur die Daten des jeweiligen Nutzers und bekommt vom Backend nur allgemeine Informationen bezüglich des Rundgangs. Die ansatzweisen personenbezogenen Daten, sind minimal und ohne ergänzende Informationen ist ihre Kompromittierung nicht gefährlich. Insgesamt wird also pro App nur ein minimaler Anteil von Daten der Verletzung der Vertraulichkeit ausgesetzt.		

G2 – Abhören		**Gefährdete Schutzziele:** C
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	begrenzt	gering

Beschreibung

Durch das Abhören der Kommunikation zwischen Soundwalk App und Backend, kann der Angreifer die Vertraulichkeit der übermittelten Daten gefährden. Damit dem Angreifer das gelingt, muss er sich zunächst andere Gefährdungen zu Nutze machen, wie z.B. G1, G8 oder G24, um die notwendigen Informationen zu erlangen, die zum Abhören benötigt werden.

Erläuterung

Da das Abhören andere Gefährdungen voraussetzt, kann die Eintrittswahrscheinlichkeit nicht höher als bei diesen Gefährdungen sein. Gleichzeitig wird durch das Abhören dann nur der Schaden der anderen Gefährdungen erweitert. Die Eintrittswahrscheinlichkeit für das Abhören, ohne davor andere Informationen erlangt zu haben ist sehr gering, da dies voraussetzt, dass der Angreifer in der Lage ist, das HTTPS Protokoll, was für die Übermittlung der Daten verwendet wird, zu entschlüsseln.

G3 – Diebstahl von Geräten, Datenträgern oder Dokumenten		**Gefährdete Schutzziele:** C, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	begrenzt	gering

Beschreibung

Smartphones sind aufgrund der Tatsache, dass sie für die mobile Nutzung gedacht sind, besonders anfällig für Diebstähle. Oftmals liegt die Intention dabei zwar nicht bei den Daten, die sich darauf befinden könnten, sondern bei dem Geld für den Weiterverkauf. Allerdings schließt das nicht aus, dass jemand an die Daten gelangt, die sich auf dem Gerät befinden. Eine Analyse der Möglichkeiten Zugriff auf ein gestohlenes Gerät zu erhalten, überschreitet den Rahmen dieser Arbeit.

Erläuterung

Der Soundwalk App ist ziemlich egal, ob jemand unbefugtes das Gerät erhält. Es werden lokal keine Daten gespeichert und da es keine Registrierung durch Nutzer gibt, besteht auch nicht die Möglichkeit, dass Login Daten gecached sind oder ein Nutzer noch angemeldet ist. Kritischer wird es, wenn der unbefugte die .apk File der App extrahiert und per reverse Engineering [26] an den Quellcode der App gelangt. Hier erhält er dann recht ausführliche Informationen darüber, wie die App mit dem Backend kommuniziert und welche Endpunkte existieren. Ohne weiteren großen Aufwand kann der Angreifer mit dem Gerät oder der App allein nicht viel anfangen und zunächst nur das Schutzziel Verfügbarkeit direkt verletzen, da der ursprüngliche Nutzer ohne sein Gerät keine alternative Zugriffsmöglichkeit hat.

G4 – Verlust von Geräten, Datenträgern oder Dokumenten		**Gefährdete Schutzziele:** C, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	vernachlässigbar	gering

Beschreibung

Der wesentliche Unterschied zur vorherigen Gefährdung ist, dass bei einem Verlust des Gerätes die negative Intention fehlt. Die Wahrscheinlichkeit, dass das Gerät verkauft wird oder sich jemand Unbefugtes Zugriff verschafft ist geringer.

Erläuterung

Wie bei G3 ist nicht auszuschließen, dass sich jemand Unbefugtes Zugriff auf das Gerät und auf die Soundwalk App verschafft. Der Schaden, der dadurch entstehen kann, ist derselbe wie bei G3. Allerdings ist die Wahrscheinlichkeit dieses Szenarios als Folge eines zufälligen Verlustes geringer.

G5 – Fehlplanung oder fehlende Anpassung		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	beträchtlich	mittel
Beschreibung Bei der Planung der Soundwalk App mussten viele Aspekte berücksichtigt werden. Es beginnt mit der Entscheidung, mit welchen Tools die App gebaut werden soll, welche Frameworks man verwendet und welche Packages verwendet werden sollen. Die Sicherheit spielt dabei meist eine nebensächliche Rolle, was fatale Auswirkungen auf das Endprodukt haben kann. Eine Fehlplanung kann auch dazu führen, dass spätere Anpassungen in der App nicht möglich oder nur mit sehr großem Aufwand möglich sind.		
Erläuterung Die Soundwalk App wurde mit Visual Studio Code und React Native entwickelt. Es wurde auf diverse Open Source Packages zugegriffen, welche zum aktuellen Zeitpunkt gut gewartet werden, wodurch nur minimale Schwachstellen durch diese Packages verfügbar sind. Die Schwachstellen von JavaScript dürfen an dieser Stelle auch nicht außer Acht gelassen werden. Dennoch ist keine breite Angriffsfläche geboten, was die Eintrittswahrscheinlichkeit lediglich möglich macht.		

G7 – Informationen oder Produkte aus unzuverlässiger Quelle		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	beträchtlich	mittel

Beschreibung Stammt das verwendete Android Gerät aus einer unzuverlässigen Quelle, besteht die Möglichkeit, dass es mit Malware infiziert ist. Alternativ kann auch die Soundwalk App aus einer unzuverlässigen Quelle bezogen werden, sodass eine Manipulation der Software nicht auszuschließen ist.
Erläuterung Die Soundwalk App wird per MS-Teams an die Teilnehmer verteilt. Von dort eine manipulierte Version der App zu beziehen, würde demnach voraussetzen, dass entweder der MS-Teams Zugang des Bereitstellers kompromittiert wurde oder der Bereitsteller selbst ein Angreifer ist bzw. die App beim Bereitsteller unbemerkt modifiziert wurde. Diese Szenarien sind sehr unwahrscheinlich. Die Soundwalk App bezieht nur generische Informationen über Standpunkte vom Backend, entsprechend kann dieser Aspekt hier vernachlässigt werden.

G8 – Manipulation von Hard- und Software		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Für die Entwicklung wurde an zwei Rechnern gearbeitet, ein privater Rechner des Entwicklers und ein Rechner der Hochschule. Der Code wurde in einem Gitlab Repository der Hochschule für die Versionskontrolle verwaltet. Auf das Repository hatte nur der Entwickler Zugriff.		
Erläuterung Die Möglichkeiten für einen Unbefugten die Soundwalk App im Entwicklungsprozess zu manipulieren sind sehr begrenzt, da nur der Entwickler Zugriff auf den Quellcode und die verwendeten Tools hat. Szenarien, in denen ein Unbefugter Zugriff erhält, würden G3		

voraussetzen oder Zugriff auf einen Account mit sehr hohen Berechtigungen im Git der Hochschule. Gleiches gilt für die zur Entwicklung verwendete Hardware. Die Hardware der Nutzer kann auf viele verschiedene Art und Weisen manipuliert werden, nicht von der Soundwalk App ausgehend. Diese Möglichkeiten zu betrachten würde eventuell mehr Einblick in die Gefährdung liefern, überschreitet aber den Rahmen dieser Arbeit.

G10 – Unbefugtes Eindringen in IT-Systeme		**Gefährdete Schutzziele:** C, I
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	begrenzt	gering
Beschreibung Die Soundwalk App verwendet für die Kommunikation das axios Package Version 0.27.2. Dieses Package hat drei bekannte Schwachstellen in der verwendeten Version: Prototype Pollution (Integrität), ReDoS (Availability) und Cross-site Request Forgery (Confidentiality), durch welche alle Schutzziele gefährdet werden können [27].		
Erläuterung Bei der Soundwalk App handelt es sich um einen Client, welcher die Kommunikation mit dem Webserver starten muss. Wenn keine aktive Kommunikation besteht, hat ein Angreifer zunächst keine Möglichkeit Zugriff auf die Schnittstelle zu erlangen. Die bekannten Schwachstellen sind eher auszunutzen, wenn das Package auf einer Server-Anwendung verwendet wird, die über eine öffentliche Schnittstelle permanent erreichbar ist. Vor allem ReDoS wird bei der Soundwalk App keine Erfolge erzielen können, da keine Informationen, die vom Server gesendet werden mit Regex verabeitet werden müssen.		

G11 – Ausfall von Geräten oder Systemen		**Gefährdete Schutzziele:** A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	vernachlässigbar	gering
Beschreibung Die Soundwalk App kann auf verschiedene Weisen ausfallen, entweder durch Hardware-probleme des Android Gerätes, durch Internetprobleme oder etwa G3.		
Erläuterung Eine Instanz der Soundwalk App hat nur bedingte Auswirkungen auf die Gesamtmenge an gesammelten Informationen. Fällt also eine App/ein Gerät aus, so ist das für den Betrieb des restlichen Systems egal, andere Instanzen der App können ohne Probleme weiterarbeiten.		

G12 – Fehlfunktion von Geräten oder Systemen		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	begrenzt	gering
Beschreibung Durch die Ausnutzung G14 können Fehlfunktionen der Soundwalk App erzwungen werden. Wie dies das Gesamtsystem beeinflusst, ist abhängig von der Softwareschwachstelle, die ausgenutzt wird und den Möglichkeiten, die sich dem Angreifer dadurch ergeben.		
Erläuterung Die Eintrittswahrscheinlichkeit und Schadenshöhe ist hier stark abhängig von der jeweiligen Softwareschwachstelle, weshalb die Bewertung analog zu G14 stattfindet.		

G14 – Softwareschwachstellen oder -Fehler		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	begrenzt	gering
Beschreibung Bei der Entwicklung der Soundwalk App wurden viele Packages verwendet. Nur zwei Packages haben bekannte Schwachstellen. Eines davon ist axios, welches bereits in G10 betrachtet wurde. Das zweite ist moments, welches dieselbe ReDoS-Schwachstelle wie axios aufweist. Es besteht die Möglichkeit, dass der Code des Entwicklers Fehler enthält, diese müsste der Angreifer aber vorerst ausfindig machen.		
Erläuterung Ein Angreifer kann versuchen die Schwachstellen der Packages auszunutzen oder selbst nach Fehlern im Quellcode suchen, vorausgesetzt er erhält auf irgendeine Art und Weise Zugriff darauf.		

G15 – Unberechtigte Nutzung oder Administration von Geräten und Systemen		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	begrenzt	mittel
Beschreibung Unberechtigte Nutzung der Soundwalk App setzt einen Zugang zur App voraus, etwa durch G3 oder den Erhalt der App Datei auf anderen Wegen. Ob man ein Administrator in der App ist, wird von einem Flag im Quellcode der App geregelt. Diese Versionen der App wurden nur vom Entwickler auf relevanten Geräten installiert		

Erläuterung

Die Eintrittswahrscheinlichkeit ist gering, da es für einen Angreifer schwierig ist an die Soundwalk App zu gelangen. Sollte es dennoch geschafft werden, kann ohne valide Zugangsdaten kein Schaden angerichtet werden. Mit der App kann der Angreifer sich lediglich ein Bild von genutzten Datenstrukturen machen und Rückschlüsse bilden, wie die Datenstrukturen im Backend sein könnten.

G16 – Fehlerhafte Nutzung oder Administration von Geräten und Systemen		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
wahrscheinlich	vernachlässigbar	gering

Beschreibung

Unter einer fehlerhaften Nutzung oder Administration versteht man das Fehlverhalten von Nutzern oder Administratoren, die keine bösartigen Intentionen haben. Also Fehler, die beim normalen Betrieb auftreten können. Eine fehlerhafte Nutzung oder Administration können zwar zu Schäden führen, bieten aber keine neuen Möglichkeiten für Angreifer die Schutzziele zu verletzen.

Erläuterung

Die Schäden, die hier entstehen können, sind minimal und begrenzt auf verfälschte Daten durch falsche Eingaben von Nutzern.

G17 – Missbrauch von Berechtigungen		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Die Soundwalk App erfordert für die Reibungslose Nutzung die Freigabe des Mikrofons für die Aufzeichnung von Audiodateien während der Rundgänge. Eine in die Soundwalk App injizierte Malware oder Spyware auf dem Gerät könnten diese Berechtigung ausnutzen, um ohne Wissen des Nutzers Audioaufnahmen zu tätigen. Die Aktivität des Mikrofons wird bei Android Geräten in der Regel durch eine farbige LED signalisiert.		
Erläuterung Die Eintrittswahrscheinlichkeit ist gering, da die Voraussetzungen für den Missbrauch der Berechtigung unrealistisch sind. Die Malware müsste in der Lage sein, Aufzeichnungen unbemerkt zu starten und irgendwie an den Angreifer zu übermitteln. Schäden dieses Szenarios wären unter Umständen personenbezogene Daten, allerdings würde dies voraussetzen, dass sich über diese Daten während der Nutzung der Soundwalk App unterhalten wurde, was auch nicht besonders realistisch klingt.		

G18 – Identitätsdiebstahl		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	existenzbedrohend	mittel
Beschreibung Die personenbezogenen Daten, die von der Soundwalk App erfasst werden, geben allein keinen Rückschluss darauf, wer die Person ist. Ein Identitätsdiebstahl anhand dieser		

Informationen ist nicht möglich. Die App speichert diese Daten auch nicht lokal auf dem Device, sodass keine Fremdsoftware an diese Informationen gelangen könnte.
Erläuterung Ein Identitätsdiebstahl ist ausgeschlossen, hypothetisch wäre es aber mit einer der schlimmsten Schäden, die durch die App entstehen könnten.

G20 – Missbrauch personenbezogener Daten		**Gefährdete Schutzziele:** C
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	begrenzt	gering
Beschreibung Die Soundwalk App erfasst Daten, die eventuell als personenbezogen eingestuft werden könnten, wie z.B. die Altersgruppe in einer Spanne von 10 Jahren. Diese Daten werden nicht lokal gespeichert, sondern nach Eingabe direkt ans Backend geschickt. Die Teilnehmer werden vor Nutzung der App darauf hingewiesen, welche Daten erfasst werden. Sie haben auch die Option keine Angabe zu tätigen. Die angegeben Daten werden ausschließlich für die Auswertung der erfassten Forschungsdaten verwendet.		
Erläuterung Ein Angreifer hat über die Soundwalk App keine Möglichkeit personenbezogene Daten zu missbrauchen, der einzige Weg an diese Daten von der App aus zu gelangen ist das Abfangen der Nachrichten an den Server. Es ist möglich, dass dies passiert, allerdings kann dadurch kein großer Schaden entstehen.		

G21 – Schadprogramme		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Wenn das Android Gerät, auf dem die Soundwalk App installiert wurde, bereits mit Schadsoftware infiziert ist, gefährdet dies die Integrität der Daten, die von dem Gerät geschickt werden und gleichzeitig deren Vertraulichkeit. In diesem Szenario stellen andere Apps und Teile des Gerätes attraktivere Ziele für die Malware dar, da die Soundwalk App keine Daten lokal abspeichert.		
Erläuterung Ob das Gerät eines Nutzers mit Schadprogrammen infiziert ist, kann man nicht voraussagen. Allerdings wird die Soundwalk App durch Malware auf dem System nicht stark geschädigt. Der Fall, dass durch die Soundwalk App Malware auf das Gerät gelangen kann, ist unwahrscheinlich, da dies voraussetzt, dass bereits der Quellcode oder die Tools vor dem Generieren der .APK der App manipuliert/infiziert wurden. Der Entwickler ist verantwortungsvoll und sicherheitsbewusst vorgegangen, daher wird dieses Szenario ausgeschlossen. Andere Szenarien wie nachträglich modifizierte Apps werden in G8 betrachtet.		

G22 – Verhinderung von Diensten (DoS)		**Gefährdete Schutzziele:** A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	begrenzt	gering

Beschreibung

Durch Package Schwachstellen kann ein ReDoS Angriff durchgeführt werden, allerdings hat dieser auf die Soundwalk App wenig Auswirkungen, da nur minimal mit Regex gearbeitet wird.

Erläuterung

Wenn die Nachrichten vom Server an die App abgefangen und mit komplexen Regex Ausdrücken manipuliert werden, könnten durch die Schwachstellen in den Packages die Performance der Soundwalk App verschlechtert werden, im schlimmsten Fall komplett lahmgelegt. Es handelt sich um ein sehr spezielles Szenario und einen großen Aufwand für den Angreifer, mit dem wenig Schaden angerichtet wird. Diesen Prozess für die Apps verschiedener Nutzer gleichzeitig umzusetzen, erscheint unrealistisch.

G23 – Sabotage		**Gefährdete Schutzziele:** A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	begrenzt	gering

Beschreibung

Eine Sabotage verfolgt das Ziel möglichst viel Schaden anzurichten. Um mit der Soundwalk App möglichst viel Schaden anzurichten, müsste das Backend mit vielen falschen Informationen geflutet werden, um die Datenintegrität zu verletzen. Dies erfordert Zugriff auf die App und valide Zugangsdaten.

Erläuterung

Der hier angerichtete Schaden wäre gering, da ein Nutzer nur Informationen versenden kann, wenn eine Soundwalk Instanz aktiv ist. Eine solche Instanz kann nur von Administratoren geöffnet werden. In dem Zeitfenster könnte der Angreifer falsche Daten in das System einführen, indem er die Fragen alle rein zufällig beantwortet. Dies ließe sich auch hochskalieren

mit mehreren Geräten/Instanzen der App. Allerdings ist das recht viel Aufwand für einen geringen Schaden.

4.2.2 Webserver

G1 – Ausspähen von Informationen		**Gefährdete Schutzziele:** C
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Spyware kann sich auch auf dieser Systemkomponente befinden. Diese hier zu installieren ist allerdings schwierig, da man am NGINX Reverse Proxy vorbeimuss.		
Erläuterung Die Infizierung mit Spyware ist unwahrscheinlich, falls es passiert, wird die Vertraulichkeit der Daten verletzt.		

G2 – Abhören		**Gefährdete Schutzziele:** C
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	begrenzt	gering
Beschreibung Die Kommunikation zwischen Server und Datenbank wird in der Analyse dieser Gefährdung bei der Datenbank betrachtet. Die Kommunikation zwischen App und Server wird in der Analyse der Gefährdung bei der App betrachtet.		

Erläuterung Entfällt.

G3 – Diebstahl von Geräten, Datenträgern oder Dokumenten		**Gefährdete Schutzziele:** C, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Um die Hardware des Servers zu stehlen, muss sich Zugang zu den Räumlichkeiten verschafft werden, zusätzlich muss erst herausgefunden werden, wo sich die Hardware überhaupt befindet. Diese Möglichkeit und Informationen hat kein Angreifer, der nicht Mitarbeiter oder zumindest Besucher der Hochschule ist. Durch regelmäßige Backups könnten die Daten wieder hergestellt und das System mit neuer Hardware wieder in Betrieb genommen werden.		
Erläuterung Diese Gefährdung ist sehr unwahrscheinlich, da die Gruppe potenzieller Angreifer sehr klein ist und dieser schnell ausfindig gemacht werden würde. Gleichzeitig sind die Daten, die ein Angreifer dadurch erhalten würde, den Aufwand einfach nicht wert. Der Schaden wäre teils finanzieller Natur und die Schutzziele Verfügbarkeit (durch die Abwesenheit der Hardware) und Vertraulichkeit (durch was auch immer der Angreifer mit den Audiodateien macht, nachdem die Hardware gestohlen wurde) werden verletzt.		

G5 – Fehlplanung oder fehlende Anpassung		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	beträchtlich	mittel
Beschreibung Eine Fehlplanung beim Server kann sich auf die Authentifizierung und auf die API auswirken, sodass im schlimmsten Fall das Bindeglied zwischen App und Datenbank nicht funktioniert oder dadurch Fehler im Betrieb entstehen.		
Erläuterung Fehler sind nie auszuschließen, gerade bei Entwicklern mit begrenzter Erfahrung. Die Fehler am Server haben Auswirkungen auf das Gesamtsystem, nicht nur auf die Komponente selbst. Demnach könnte ein Fehler in der API zu verfälschten Daten führen oder eine fehlende Anpassung in der Authentifikation zu weiteren Schwachstellen.		

G7 – Informationen oder Produkte aus unzuverlässiger Quelle		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	beträchtlich	mittel
Beschreibung Gelingt es einem Angreifer die Authentifizierung zu umgehen oder an gültige Zugangsdaten zu gelangen, so kann er den Server mit falschen Informationen fluten.		
Erläuterung Die Authentifikation ist über einen JWT implementiert, dieser Token wird nach erfolgreicher Anmeldung vom Server an den Client geschickt. Jeder weitere Endpunkt der API prüft		

zunächst ob bei gesendeten Nachrichten ein gültiger Token mitgesandt wurde. Erhält ein Angreifer einen gültigen Token, kann er alle Endpunkte mit falschen Informationen ansprechen.

G8 – Manipulation von Hard- und Software		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Für die Entwicklung wurde an zwei Rechnern gearbeitet, ein privater Rechner des Entwicklers und ein Rechner der Hochschule. Der Code wurde in einem Gitlab Repository der Hochschule für die Versionskontrolle verwaltet. Auf das Repository hatte nur der Entwickler Zugriff. Die Hardware steht in einem Serverraum an der Hochschule und ist für Unbefugte nur sehr schwer zu erreichen.		
Erläuterung Die Möglichkeiten für einen Unbefugten den Server im Entwicklungsprozess zu manipulieren sind sehr begrenzt, da nur der Entwickler Zugriff auf den Quellcode und die verwendeten Tools hat. Szenarien, in denen ein Unbefugter Zugriff erhält, würden G3 voraussetzen oder Zugriff auf einen Account mit sehr hohen Berechtigungen im Git der Hochschule. Gleiches gilt für die zur Entwicklung verwendete Hardware. Die Hardware der Nutzer kann auf viele verschiedene Art und Weisen manipuliert werden, nicht von der Soundwalk App ausgehend. Diese Möglichkeiten zu betrachten würde eventuell mehr Einblick in die Gefährdung liefern, überschreitet aber den Rahmen dieser Arbeit.		

G9 – Manipulation von Informationen		**Gefährdete Schutzziele:** I
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	beträchtlich	mittel
Beschreibung Die Audiodateien sind die einzigen Informationen, die auf dem Server gespeichert werden. Um diese manipulieren zu können sind Administratorberechtigungen notwendig, also als Mitarbeiter oder als Angreifer mit den Zugangsdaten. Wie und ob diese erlangt werden können, wird in anderen Gefährdungen untersucht.		
Erläuterung Die Manipulation der Daten durch einen Mitarbeiter ist unwahrscheinlich, allerdings wäre der Schaden vor dem Hintergrund des Ziels der Soundwalk App beträchtlich. Wenn am Ende verfälschte Daten rauskommen leidet die Qualität des Projektes enorm.		

G10 – Unbefugtes Eindringen in IT-Systeme		**Gefährdete Schutzziele:** C, I
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	beträchtlich	mittel
Beschreibung Durch die Gefährdungen G24 und G25 werden für den Server bereits die Szenarien mit der größten Wahrscheinlichkeit auf unbefugtes Eindringen betrachtet. Die Konsequenzen sind die Gleichen.		
Erläuterung Die Bewertung entspricht den anderen Gefährdungen.		

G11 – Ausfall von Geräten oder Systemen		**Gefährdete Schutzziele:** A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Ein Ausfall des Servers würde dafür sorgen, dass das gesamte System nicht funktioniert. Es können in diesem Zeitraum keine Daten gesammelt werden.		
Erläuterung Da der Server an der Hochschule in einem Rechenzentrum betrieben wird, ist ein Ausfall unwahrscheinlich. Wartungen und regelmäßige Updates sorgen dafür. Falls dennoch ein Ausfall stattfindet, wird für diesen Zeitraum die Verfügbarkeit verletzt.		

G12 – Fehlfunktion von Geräten oder Systemen		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	beträchtlich	mittel
Beschreibung Fehlfunktionen der Server Hardware könnten im schlimmsten Fall zu einem defekten Gerät führen, wodurch die Daten verloren gehen. Dem wird durch regelmäßige Backups, Wartungen und Updates vorgebeugt. Gleiches gilt für die NGINX Software. Bei der Node.js Applikation müsste regelmäßiger eine Aktualisierung verwendeter Packages durchgeführt werden.		

Erläuterung Durch die getroffenen Vorkehrungen ist die Eintrittswahrscheinlichkeit genau so gering wie bei G11, allerdings sind die möglichen Konsequenzen gravierender, da Fehlfunktionen nicht zur zum Ausfall führen müssen, sondern auch zu verfälschten Daten.

G13 – Ressourcenmangel		**Gefährdete Schutzziele:** A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Sollte der zugewiesene Speicherplatz für Audiodateien nicht ausreichen würden Daten verloren gehen.		
Erläuterung Vor dem Hintergrund, dass es nur eine begrenzte Anzahl an Nutzern der Soundwalk App gibt, ist auch die Menge der Daten, die gesammelt wird, begrenzt. Es ist daher unwahrscheinlich, dass es zu Ressourcenmangel kommt. Der Schaden würde sich auf verlorene Daten begrenzen.		

G14 – Softwareschwachstellen oder -Fehler		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	beträchtlich	mittel

Beschreibung Die verwendete Version des Express Packages hat eine bekannte Schwachstelle [28], die Schwachstellen der Packages für die Datenbankanbindung werden bei G14 der Datenbank betrachtet.
Erläuterung Da es bekannte Schwachstellen gibt, die ein Angreifer ausnutzen könnte, wird die Eintrittswahrscheinlichkeit auf möglich geschätzt. Durch die mögliche Verletzung aller Schutzziele entsteht eine beträchtliche Schadenshöhe.

G15 – Unberechtigte Nutzung oder Administration von Geräten und Systemen		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	beträchtlich	mittel
Beschreibung Angreifer können durch alle Gefährdungen, die ihnen Zugriff zum Server verschaffen, diesen auch unberechtigt nutzen. Die unberechtigte Administration erfordert zusätzliche Privilegien, die für Angreifer schwieriger zu erreichen sind, wenn es sich nicht um Mitarbeiter handelt.		
Erläuterung Gelangt ein Angreifer an Administrationsrechte, gefährdet er alle Schutzziele. Dies ist allerdings sehr unwahrscheinlich, da nur Mitarbeiter administrative Rechte für den Server haben.		

G16 – Fehlerhafte Nutzung oder Administration von Geräten und Systemen		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Fehlerhafte Nutzung durch Anwender kann ausgeschlossen werden, da diese nur sehr spezifische Interaktionsmöglichkeiten durch die API haben. Fehler in der Administration sind z.B. versehentliche Veränderungen der Server-Config.		
Erläuterung Fehler in der Administration sind möglich, abhängig von der Art des Fehlers können auch alle Schutzziele verletzt werden. Alle Fehler sollten notfalls zumindest durch ein Backup wieder berichtigt werden können.		

G17 – Missbrauch von Berechtigungen		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Die einzigen Personen mit Berechtigungen auf diesem Server sind Mitarbeiter. Diese sind grundsätzlich vertrauenswürdig, allerdings darf das Szenario des Missbrauchs von Berechtigungen nie ausgeschlossen werden.		
Erläuterung Der Missbrauch von Berechtigungen ermöglicht viele Handlungen auf dem Server, welche alle Schutzziele verletzen können.		

G19 – Abstreiten von Handlungen		**Gefährdete Schutzziele:** C, I
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Gelingt es einem Angreifer durch etwa G8 oder G15 den Server so zu manipulieren, dass der Nachrichtenausgang und -Empfang geleugnet wird, könnte es dem Betreiber zu spät auffallen, dass Unbefugte mit dem Server interagieren und eventuell Zugriff auf das System haben.		
Erläuterung Im beschriebenen Szenario sind die Vertraulichkeit und Integrität der Audiodaten gefährdet, da diese eingesehen oder manipuliert werden können. Allerdings setzt dies die erfolgreiche Ausnutzung anderer Gefährdungen durch den Angreifer voraus.		

G22 – Verhinderung von Diensten (DoS)		**Gefährdete Schutzziele:** A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Durch das Rate-Limiting des NGINX Reverse Proxy können DoS Attacken gegen den Server verhindert werden.		

Erläuterung

Nach der Beschreibung ist die Wahrscheinlichkeit eines erfolgreichen DoS Angriffs sehr gering, falls es dennoch irgendwie funktioniert, wäre nur die Verfügbarkeit eingeschränkt.

G25 – Einspielen von Nachrichten		**Gefährdete Schutzziele:** C, I
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	begrenzt	gering

Beschreibung

Durch beispielsweise einen Man-in-the-Middle-Angriff oder Replay-Attacken können Nachrichten eingespielt werden [6] und sich potenziell Zugriff auf das System verschafft werden. Durch die Authentifizierung per JSON Web Token wird es dem Angreifer schwerer gemacht. Allerdings reicht dies nicht aus, um diese Arten von Attacken zu verhindern. Wird etwa die initiale Kontaktaufnahme replayed, kann sich der Angreifer einfach einen eigenen Token generieren lassen.

Erläuterung

Gelingt es dem Angreifer durch das Einspielen von Nachrichten Zugriff auf das System zu erlangen, kann er falsche Informationen in das System bringen und dadurch die Integrität verletzen. Außerdem kann er weitere Informationen über das System sammeln.

4.2.3 Datenbank

G1 – Ausspähen von Informationen		**Gefährdete Schutzziele:** C
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	vernachlässigbar	gering
Beschreibung Auch die PostgreSQL Datenbank kann von Spyware befallen werden. Da die Datenbank nicht öffentlich, sondern nur aus dem Netzwerk der Hochschule erreichbar ist, muss die Spyware also entweder über den Webserver kommen oder lokal von einem Angreifer aufgesetzt werden. Zweiteres Szenario setzt hohe Berechtigungen auf dem Level eines Mitarbeiters voraus.		
Erläuterung Ob die Spyware über den Webserver gelangen kann, wird in der Analyse des Webservers betrachtet und daher hier nicht berücksichtigt. Ein Mitarbeiter könnte zwar Spyware installieren, allerdings ist dies ein unwahrscheinliches Szenario, da der Mitarbeiter sowieso schon die Möglichkeit hat die Daten auf der Datenbank einzusehen. Dafür müsste er nicht zusätzliche Software verwenden. Der Schaden ist in beiden Fällen gleich, die Vertraulichkeit der Daten wird verletzt.		

G2 – Abhören		**Gefährdete Schutzziele:** C
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	vernachlässigbar	gering

Beschreibung

Die PostgreSQL Datenbank kommuniziert mit dem Node.js Server über das pg Package. Das Package hat in der verwendeten Version keine bekannten Schwachstellen, die ein Angreifer ausnutzen könnte. Demnach ist für das Abhören der Kommunikation zwischen Datenbank und Node.js Server ein Zugriff auf das interne Netz der Hochschule nötig. Falls es sich um keinen Mitarbeiter handelt, ist dieser Zugriff für die betrachteten Arten von Angreifern ein sehr großer Aufwand.

Erläuterung

Es ist unwahrscheinlich, dass ein Angreifer dazu kommt die hier beschriebene Kommunikation abzuhören. Der Mitarbeiter als Angreifer ist ein Spezialfall, der das Abhören aber nicht nötig hätte, da er alle Informationen von der Quelle beziehen kann. Schaden der hier entsteht betrifft nur die Vertraulichkeit von Daten und das auch nur begrenzt, da es sich nicht um vertrauliche Daten handelt, die niemand sehen darf. Credentials werden verschlüsselt gespeichert, sodass das Einsehen dieser ohne die korrekt Entschlüsselungsmethode nichts bringt.

G3 – Diebstahl von Geräten, Datenträgern oder Dokumenten		**Gefährdete Schutzziele:** C, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering

Beschreibung

Um die Hardware der Datenbank zu stehlen, muss sich Zugang zu den Räumlichkeiten verschafft werden, zusätzlich muss erst herausgefunden werden, wo sich die Hardware überhaupt befindet. Diese Möglichkeit und Informationen hat kein Angreifer, der nicht Mitarbeiter oder zumindest Besucher der Hochschule ist. Durch regelmäßige Backups könnten die Daten wieder hergestellt und das System mit neuer Hardware wieder in Betrieb genommen werden.

Erläuterung

Diese Gefährdung ist sehr unwahrscheinlich, da die Gruppe potenzieller Angreifer sehr klein ist und dieser schnell ausfindig gemacht werden würde. Gleichzeitig sind die Daten, die ein Angreifer dadurch erhalten würde, den Aufwand einfach nicht wert. Der Schaden wäre teils finanzieller Natur und die Schutzziele Verfügbarkeit (durch die Abwesenheit der Hardware) und Vertraulichkeit (durch was auch immer der Angreifer mit den Daten macht, nachdem die Hardware gestohlen wurde) werden verletzt.

G5 – Fehlplanung oder fehlende Anpassung		**Gefährdete Schutzziele:** I
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	beträchtlich	mittel

Beschreibung

Bei der Planung des Datenbankschemas für die PostgreSQL Datenbank wurde darauf geachtet, dass das Schema genau auf die benötigten Daten für die Soundwalk App zugeschnitten wurde. Das Schema wurde von einem Mitarbeiter, der die Datenbank betreibt, begutachtet und abgenommen. Die Datenbank wird regelmäßig mit aktuellen Versionen der PostgreSQL Software aktualisiert.

Erläuterung

Aus der Beschreibung geht hervor, dass eine Fehlplanung des Datenbankschemas für die Soundwalk App ausgeschlossen werden kann. Hypothetisch hätten Fehler einen großen Einfluss auf die Integrität der Daten, wenn diese falsch abgespeichert werden. Durch fehlende Anpassung in der Software könnten auf lange Sicht Sicherheitslücken entstehen, die ein potenzieller Angreifer dann ausnutzen kann. Dies wird durch die regelmäßigen Updates verhindert.

G9 – Manipulation von Informationen		**Gefährdete Schutzziele:** I
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
Unwahrscheinlich	beträchtlich	mittel
Beschreibung Informationen in der Datenbank können durch das Verändern von Datenbankfeldern manipuliert werden. Dafür braucht man direkten Zugriff auf die Datenbank, also als Mitarbeit mit Administrationsberechtigungen oder als Angreifer mit den Zugangsdaten zur Datenbank. Wie und ob diese erlangt werden können, wird in der Analyse des Webservers beurteilt.		
Erläuterung Die Manipulation der Daten durch einen Mitarbeiter ist unwahrscheinlich, allerdings wäre der Schaden vor dem Hintergrund des Ziels der Soundwalk App beträchtlich. Wenn am Ende verfälschte Daten rauskommen leidet die Qualität des Projektes enorm.		

G10 – Unbefugtes Eindringen in IT-Systeme		**Gefährdete Schutzziele:** C, I
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	beträchtlich	mittel
Beschreibung Um mit der PostgreSQL Datenbank interagieren zu können muss ein Angreifer im internen Netz der Hochschule sein. Wenn der Zugang über den Webserver erfolgt ist, ist die Wahrscheinlichkeit hoch, dass auch die Zugangsdaten für die Datenbank kompromittiert wurden. Wenn sich auf anderem Wege Zugang zum internen Netzwerk verschafft wurde, muss der Angreifer durch etwa das Ausnutzen von Softwareschwachstellen (G14) versuchen Zugriff auf die Datenbank zu bekommen.		

Erläuterung Gelingt es einem Angreifer Zugriff auf die Datenbank zu erhalten, wird durch den Zugriff die Vertraulichkeit der Daten verletzt. Gleichzeitig hat der Angreifer die Möglichkeit die Daten zu manipulieren. Die Wahrscheinlichkeit wird hier auf möglich geschätzt, da in G14 für die Datenbank diverse Softwareschwachstellen gefunden wurden.

G11 – Ausfall von Geräten oder Systemen		**Gefährdete Schutzziele:** A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Ein Ausfall der Datenbank würde dafür sorgen, dass das gesamte System nicht funktioniert. Es können in diesem Zeitraum keine Daten gesammelt werden.		
Erläuterung Da die Datenbank an der Hochschule in einem Rechenzentrum betrieben wird, ist ein Ausfall unwahrscheinlich. Wartungen und regelmäßige Updates sorgen dafür. Falls dennoch ein Ausfall stattfindet, wird für diesen Zeitraum die Verfügbarkeit verletzt.		

G12 – Fehlfunktion von Geräten oder Systemen		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
Unwahrscheinlich	beträchtlich	mittel

Beschreibung Fehlfunktionen der Datenbank Hardware könnten im schlimmsten Fall zu einem defekten Gerät führen, wodurch die Daten verloren gehen. Dem wird durch regelmäßige Backups, Wartungen und Updates vorgebeugt. Gleiches gilt für die Datenbank Software.
Erläuterung Durch die getroffenen Vorkehrungen ist die Eintrittswahrscheinlichkeit genau so gering wie bei G11, allerdings sind die möglichen Konsequenzen gravierender, da Fehlfunktionen nicht zur zum Ausfall führen müssen, sondern auch zu verfälschten Daten.

G13 – Ressourcenmangel		**Gefährdete Schutzziele:** A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
unwahrscheinlich	begrenzt	gering
Beschreibung Sollte der zugewiesene Speicherplatz für die Datenbank nicht ausreichen würden Daten verloren gehen.		
Erläuterung Vor dem Hintergrund, dass es nur eine begrenzte Anzahl an Nutzern der Soundwalk App gibt, ist auch die Menge der Daten, die gesammelt wird, begrenzt. Es ist daher unwahrscheinlich, dass es zu Ressourcenmangel kommt. Der Schaden würde sich auf verlorene Daten begrenzen.		

G14 – Softwareschwachstellen oder -Fehler		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
Möglich	beträchtlich	mittel
Beschreibung PostgreSQL Version 15.0 hat mittlerweile diverse Softwareschwachstellen [29], die aufgedeckt wurden. Einem Angreifer kann es durch diese Schwachstellen gelingen Zugriff auf die Datenbank zu erhalten, allerdings muss er für die Angriffe bereits im internen Netz der Hochschule sein.		
Erläuterung Das beschriebene Szenario ist nicht auszuschließen, die Einstufung findet aufgrund der Anzahl der möglich ausnutzbaren Schwachstellen statt.		

G15 – Unberechtigte Nutzung oder Administration von Geräten und Systemen		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	beträchtlich	mittel
Beschreibung Die unberechtigte Nutzung oder Administration kann nur von Personen durchgeführt werden, die bereits Zugriff auf das Netzwerk der Hochschule haben.		
Erläuterung Mit der Administration der Datenbank kann Schaden angerichtet werden, der wieder rückgängig gemacht werden kann, sofern Backups sicher gelagert werden. Es werden alle		

Schutzziele für die Datenbank gefährdet, da mit der Administration alles an der Datenbank verändert werden kann.

G16 – Fehlerhafte Nutzung oder Administration von Geräten und Systemen		**Gefährdete Schutzziele:** C, I, A
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
möglich	beträchtlich	mittel
Beschreibung Fehlerhafte Nutzung durch Anwender kann ausgeschlossen werden, da diese nur sehr spezifische Interaktionsmöglichkeiten durch die API haben. Fehler in der Administration sind z.B. versehentliche Veränderungen des Datenbankschemas oder etwa die Erteilung falscher Berechtigungen.		
Erläuterung Fehler in der Administration sind möglich, abhängig von der Art des Fehlers können auch alle Schutzziele verletzt werden. Alle Fehler sollten notfalls zumindest durch ein Backup wieder berichtigt werden können.		

4.2.4 Allgemein

Hier wird das Risiko der Gefährdungen analysiert, für die eine Unterscheidung der Komponenten keinen Unterschied macht.

G24 – Social Engineering		**Gefährdete Schutzziele:** C, I
Eintrittswahrscheinlichkeit	Schadenshöhe	Risiko
wahrscheinlich	beträchtlich	hoch
Beschreibung Social Engineering ist wahrscheinlich für jede Softwareanwendung die größte Schwachstelle, sofern Gedanken in das Sicherheitskonzept investiert wurden. Durch die Nutzer entstehen Schwachstellen, die bekannt sind, aber gegen die häufig nichts gemacht werden kann als darauf hinzuweisen und die Nutzer so gut wie möglich zu schulen, damit sie nicht Opfer von Social Engineering werden. Bei der Soundwalk App ist also zu beachten, dass Nutzer gültige Nutzername Passwort Kombinationen veröffentlichen können oder gar die ganze Soundwalk App an unbefugte aushändigen. Dabei wird keine bösartige Intention vermutet, sondern in der Regel Unachtsamkeit oder gar Hilfsbereitschaft.		
Erläuterung Hat ein Angreifer Zugriff auf den Quellcode so ist wieder G8 zu beachten. Sobald er die Credentials hat, kann er eine Verbindung zum Backend aufbauen und relevante Informationen erlangen, wie er die Authentifizierung, die über einen JWT implementiert ist, umgehen kann, um sämtlichen Verkehr zwischen Soundwalk Apps und Backend abzuhören. Fälle in denen Social Engineering erfolgt, können nie ausgeschlossen werden und deshalb hat der richtige Umgang mit Ihnen hohe Priorität in der Sicherheit.		

Anmerkung

Alle Risiken, bei denen das Vertrauen in Mitarbeiter und Administratoren eine Rolle spielt, lassen sich einfach auf andere Bereiche, die nicht eine Hochschule oder ähnliche Institution sind, übertragen. Wird online ein Server gemietet, so bestehen dieselben Risiken. Ohne ein Grundlegendes Vertrauen in Administratoren wird man diese Risiken immer hoch einschätzen müssen.

5 Auswertung

Im vorigen Kapitel wurden durch die Durchführung einer Risikoanalyse die Schwachstellen der Soundwalk App aufgezeigt. In diesem Kapitel wird untersucht, wie mit den Risiken umgegangen werden kann und welche Möglichkeiten dafür zur Verfügung stehen. Dafür werden konkrete Schwachstellen des Fallbeispiels benannt und anhand der Ergebnisse der Risikoanalyse zusammengefasst. Anschließend werden Maßnahmen vorgeschlagen, um diese Schwachstellen auszubessern.

5.1 Sicherheitsstand der Soundwalk App

Das Ergebnis der Risikoanalyse lässt sich folgendermaßen zusammenfassen: Vor dem Hintergrund, dass die App von nur einer kleinen Gruppe genutzt wird, stellen die meisten identifizierten Gefährdungen ein kleines Risiko dar. Dennoch geht daraus hervor, dass die App Schwachstellen hat, die verbessert werden können. Diese wären:

- Keine klare Trennung der Benutzerrollen innerhalb des Systems und dadurch schwache Autorisation
- Aktualisierungsstand verwendeter Software und Komponenten
- Fehleranfälligkeit des selbstgeschriebenen Codes
- Hohe Frequenz des Datenaustausches zwischen Front- und Backend. Die Höhe der Frequenz bedingt eine größere Angriffsfläche für Angreifer, die die Kommunikation angreifen wollen.

An dieser Stelle ist anzumerken, dass diverse Schwachstellen des Node.js Servers vor allem, was die Verfügbarkeit betrifft ihr niedriges Risiko dem NGINX Reverse Proxy zu verdanken haben [17]. Ohne diese Systemkomponente müsste man sich intensiver mit Möglichkeiten zur DoS Reduzierung beschäftigen.

5.2 Möglichkeiten zur Risikominimierung

Im Folgenden soll erörtert werden, welche Möglichkeiten bestehen, den Sicherheitsstandard der Sound-Walk-App zu optimieren. Die Maßnahmen werden ausgewählt anhand ihrer Möglichkeiten die Schwachstellen zu minimieren. Der damit verbundene Aufwand soll ebenfalls berücksichtigt werden.

Autorisation

Das Verwalten von Benutzerrollen muss vom Backend verwaltet werden. Ein Flag in der App ist viel zu einfach zu umgehen. Die Android-App muss den Autorisierungsgrad des Nutzers vom Backend erhalten, die relevanten Endpunkte dürfen nur ansprechbar sein, wenn ein Nutzer den richtigen Autorisierungsgrad hat. Diese Änderung ist wichtig und nicht mit besonders hohem Aufwand verbunden.

Aktualisierung von Software und Komponenten

Gerade bei der React Native Android-App und dem Node.js Server müssen die Packages regelmäßig überprüft und im Idealfall aktualisiert werden. Dies ist mit hohem Aufwand verbunden und der Entwickler muss abwägen ob eventuelle Sicherheitslücken vertretbar sind, wenn Updates oder das Austauschen von Packages einen zu großen Aufwand bedeuten.

Unit Tests

Schreiben von Unittests, um Fehler im eigenen Code zu finden und die Wahrscheinlichkeit für Fehler, die ein Angreifer ausnutzen kann zu minimieren. Es bietet sich an Geschäftslogik und interne Usecases für alle Komponenten mit Unittests zu überprüfen. Dadurch kann erreicht werden, dass beispielsweise fehlerhafte oder bösartige Nutzereingaben zu Schaden führen. Diese Aufgabe ist mit vertretbarem Aufwand verbunden.

Verwendung einer lokalen Datenbank

Durch die Implementierung einer lokalen Datenbank in der Android-App kann die Kommunikationsfrequenz gesenkt werden und gleichzeitig wird die Wahrscheinlichkeit verlorener Daten reduziert. Wenn alle Umfragedaten zu einem Soundwalk zunächst lokal gespeichert und zu einem späteren Zeitpunkt an das Backend übertragen werden, könnte man den gesamten Austausch auf die initiale Anmeldung und die finale Übergabe der Daten an das Backend beschränken. Wenn man die personenbezogenen Daten nicht lokal speichern möchte, könnten diese direkt nach der Anmeldung übermittelt werden. Fraglich ist, ob man den Authentifizierungstoken in der lokalen Datenbank abspeichern möchte. Entscheidet man sich dafür gefährdet man die Authentifizierung, allerdings muss sich der Nutzer keinen neuen Token holen sollte die App abstürzen. Die Gefährdung, die dadurch entsteht, ist größer als der Vorteil für den Nutzer sich nicht erneut authentifizieren zu müssen. Daher wird davon abgeraten Authentifizierungstokens lokal abzuspeichern. Lokale Daten sollten in den folgenden Szenarien gelöscht werden:

- Die Daten wurden erfolgreich an das Backend übertragen.
- Es ist ein bestimmter Zeitraum seit Erstellung des Soundwalks vergangen, dann ist davon auszugehen, dass der Nutzer die Daten nicht hochladen wollte.
- Die App wird deinstalliert.
- Der Nutzer startet die Teilnahme an einem neuen Soundwalk. Dieser Punkt ist diskutierbar, wenn man die Möglichkeit bieten möchte mehrere Soundwalks zu absolvieren, bevor man die Daten hochladen möchte.

Ein weiterer Ansatz, den man verfolgen könnte, wäre, die Daten auf zwei Server zu verteilen. Ein Server ist öffentlich erreichbar ohne Authentifizierung und nur dafür zuständig die Metadaten der Soundwalks an die Apps zu verteilen. Keine Forschungsdaten und keine Nutzerdaten werden an diesen Server gesandt. Somit ließen sich die Soundwalks in einem Offlinemodus durchführen. Nach der Durchführung müsste man sich dann an einem zweiten Server authentifizieren und könnte die Forschungsdaten hochladen. Die Angaben der personenbezogenen Daten erfolgen dann halt zum Schluss, sodass diese auch hier nicht lokal gespeichert werden müssen.

6 Schlussbetrachtung

6.1 Fazit

Das Ziel dieser Arbeit ist, die Risikoanalyse einer datenbankgestützten Android-App durchzuführen. Anhand eines realen Fallbeispiels wurden allgemeine Gefährdungen für datenbankgestützte Android-Apps analysiert. Die erste Forschungsfrage „Welche Gefährdungen ergeben sich bei der Entwicklung und Nutzung einer datenbankgestützten Android-App?“ wurde dadurch beantwortet.

Anschließend wurde die Risikoanalyse durchgeführt, aus deren Ergebnis sich konkrete Schwachstellen des Fallbeispiels herausarbeiten ließen. Für diese Schwachstellen wurden Maßnahmen vorgeschlagen, mit denen die Situation der Schwachstellen verbessert werden soll. Demnach kann auch die zweite Forschungsfrage „Welche Maßnahmen eignen sich zur Risikominimierung, insbesondere in Bezug auf das Fallbeispiel, für die beschriebenen Bedrohungen?“ als beantwortet angesehen werden.

6.2 Ausblick

In dieser Arbeit wurden eine Vielzahl allgemeiner Gefährdungen für datenbankgestützte Android-Apps analysiert, wodurch eine solide Grundlage für jeden geschaffen wird, der seine Anwendung ebenfalls einer Risikoanalyse unterziehen möchte. Die Risikoanalyse dient als Beispiel und bietet Anhaltspunkte, an denen man sich orientieren kann.

Die IT-Sicherheit ist ein sehr breites Thema, das in viele Richtungen verfolgt werden kann. Im Rahmen dieser Arbeit konnten diverse Risiken und die zugrunde liegenden Gefährdungen lediglich einer oberflächlichen Betrachtung unterzogen werden. Sie stellen ein solides Fundament für weiterführende Arbeiten dar, die eine vertiefte Auseinandersetzung mit den

behandelten Themengebieten anstreben. Aufgrund der schnellen Weiterentwicklung in der IT-Sicherheit ist davon auszugehen, dass es auch in Zukunft neue Bedrohungen und neue Behandlungsansätze geben wird, die einer Analyse unterzogen werden können.

Literaturverzeichnis

[1] *Absatz von Smartphones weltweit vom 1. Quartal 2009 bis zum 1. Quartal 2024 nach Betriebssystem*. URL https://de.statista.com/statistik/daten/studie/74592/umfrage/absatz-von-smartphones-weltweit-nach-betriebssystem/ – Überprüfungsdatum 08.05.2024

[2] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Die Lage der IT-Sicherheit in Deutschland*. URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=7

[3] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *IT-Grundschutz-Kompendium*. Köln (Unternehmen und Wirtschaft). URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

[4] HÜSGEN, Kevin: *DNS-Sicherheit am Beispiel eines mittelständischen Softwareunternehmens*. Bachelorarbeit der HAW Hamburg. 2018. URL https://reposit.haw-hamburg.de/bitstream/20.500.12738/15298/1/BA_DNS-Sicherheit.pdf

[5] *ISO/IEC-27000-Reihe*. URL https://www.iso.org/standard/iso-iec-27000-family – Überprüfungsdatum 08.05.2024

[6] CLAUDIA ECKERT: *IT-Sicherheit* : *Konzepte – Verfahren – Protokolle*. 11. Auflage : De Gruyter Oldenbourg. – ISBN 978-3-11-099689-0

[7] THOMAS HACKNER ; MICHAEL KOFLER ; ROLAND AIGNER ; KLAUS GEBESHUBER ; FRANK NEUGEBAUER ; ANDRÉ ZINGSHEIM ; STEFAN KANIA ; MARKUS WIDL ; PETER KLOEP: *Hacking & Security Das umfassende Handbuch*. 2. Auflage, erweiterte Ausgabe : Rheinwerk Verlag, 2020. – ISBN 9783836271929

[8] RETO MEIER: *Professional Android*. Paperback : Wrox Press, 2018. – ISBN 1118949528

[9] *HAW-Hamburg: Open Citizen Soundwalks*. URL https://www.haw-hamburg.de/digitalisierung/digitalisierungsprojekte/open-citizen-soundwalks-1/ – Überprüfungsdatum 08.05.2024

[10] ANDRÉ FIEBIG, Brigitte Schulte-Fortkamp: *Soundscape - Fortschritte in der Standardisierung auf internationaler Ebene*. URL https://www.dega-akustik.de/fileadmin/dega-akustik.de/publikationen/akustik-journal/19-01/akustik_journal_2019_01_online_artikel3.pdf

[11] *React Native · Learn once, write anywhere*. URL https://reactnative.dev/ – Überprüfungsdatum 09.05.2024

[12] *NGINX Reverse Proxy | NGINX Documentation*. URL https://docs.nginx.com/nginx/admin-guide/web-server/reverse-proxy/ – Überprüfungsdatum 09.05.2024

[13] *Express - Node.js web application framework*. URL https://expressjs.com/ – Überprüfungsdatum 09.05.2024

[14] *Web Server | NGINX Documentation*. URL https://docs.nginx.com/nginx/admin-guide/web-server/ – Überprüfungsdatum 09.05.2024

[15] *Was ist PostgreSQL? | PostgreSQL*. URL http://postgresql.de/was-ist-postgresql – Überprüfungsdatum 09.05.2024

[16] *npm | Home*. URL https://www.npmjs.com/ – Überprüfungsdatum 09.05.2024

[17] *Load Balancing Node.js Application Servers with NGINX Open Source and NGINX Plus | NGINX Documentation*. URL https://docs.nginx.com/nginx/deployment-guides/load-balance-third-party/node-js/ – Überprüfungsdatum 09.05.2024

[18] *API Documentation Tools | Swagger*. URL https://swagger.io/solutions/api-documentation/ – Überprüfungsdatum 09.05.2024

[19] EUROPÄISCHE UNION: *VERORDNUNG (EU) 2016/ 679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 27. April 2016 - zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung*

der Richtlinie 95/ 46/ EG (Datenschutz-Grundverordnung). URL https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE. URL https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

[20] *HAW-Hamburg: Angriff auf die IT-Infrastruktur*. URL https://www.haw-hamburg.de/cyberangriff/ – Überprüfungsdatum 09.05.2024

[21] *M2: Inadequate Supply Chain Security | OWASP Foundation*. URL https://owasp.org/www-project-mobile-top-10/2023-risks/m2-inadequate-supply-chain-security.html – Überprüfungsdatum 09.05.2024

[22] *OWASP Mobile Top 10 | OWASP Foundation*. URL https://owasp.org/www-project-mobile-top-10/ – Überprüfungsdatum 09.05.2024

[23] *M3: Insecure Authentication/Authorization | OWASP Foundation*. URL https://owasp.org/www-project-mobile-top-10/2023-risks/m3-insecure-authentication-authorization.html – Überprüfungsdatum 09.05.2024

[24] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Kritische Backdoor in XZ für Linux*. URL https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-223608-1032.pdf?__blob=publicationFile&v=5 – Überprüfungsdatum 09.05.2024

[25] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Standard 200-3*. URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html

[26] SHERAN GUNASEKERA: *Android-Apps Security: Mitigate Hacking Attacks and Security Breaches*. 2nd ed. : Apress, 2020. – ISBN 9781484216811

[27] *axios 0.27.2 vulnerabilities | Snyk*. URL https://security.snyk.io/package/npm/axios/0.27.2 – Überprüfungsdatum 09.05.2024

[28] *Open Redirect in express | CVE-2024-29041 | Snyk*. URL https://security.snyk.io/vuln/SNYK-JS-EXPRESS-6474509 – Überprüfungsdatum 09.05.2024

[29] *postgresql-15 vulnerabilities | Snyk*. URL https://security.snyk.io/package/linux/debian:12/postgresql-15 – Überprüfungsdatum 09.05.2024

Erklärung zur selbstständigen Bearbeitung einer Abschlussarbeit

Gemäß der Allgemeinen Prüfungs- und Studienordnung ist zusammen mit der Abschlussarbeit eine schriftliche Erklärung abzugeben, in der der Studierende bestätigt, dass die Abschlussarbeit „— bei einer Gruppenarbeit die entsprechend gekennzeichneten Teile der Arbeit [(§ 18 Abs. 1 APSO-TI-BM bzw. § 21 Abs. 1 APSO-INGI)] — ohne fremde Hilfe selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt wurden. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich zu machen."

Quelle: § 16 Abs. 5 APSO-TI-BM bzw. § 15 Abs. 6 APSO-INGI

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

_____	_____	
Ort	Datum	Unterschrift im Original