Threat Modeling

Stakeholder:

1. Supermarkt-Anbieter
2. Zahlungsdienstleister
3. Kunde
4. Kunde, der nicht bezahlen möchte
5. Kunde, der Zahlungsdaten von anderen abgreifen möchte

Brainstorming:

zu 1.)

- Geld kommt nicht an
- Gebühr zu hoch
- Verwaltungsaufwand zu hoch

zu 2.)

- Liquidität des Kunden
- Risiko des Betrugs
- Supermarkt-Anbieter fälscht Abrechnung

zu 3.)

- Falscher Betrag (zu hoch) wird abgebucht
- App unsicher

zu 4.)

- Nutzt fremdes Handy zur Bezahlung
- Konto mit falschen Daten anlegen

zu 5.)

- Manipulation des Gerätes vor Ort
- Mitschneiden der Zahlungskommunikation

Motivation, Handlungsfähigkeit, Schadenshöhe

ID	Bedrohung	Angreifergruppe	Motivation * Handlungsfähigkeit	Schadenshöhe (1..5)	Risiko
1	Supermarkt behauptet, Geld kam nicht an	Supermarkt-Anbieter	1 * 3	2	6
2	Falscher Betrag (zu hoch) wird an Zahlungsdienstleister weitergegeben	Supermarkt-Anbieter	1 * 3	2	6
3	Verwaltungsaufwand zu hoch	Supermarkt-Anbieter			
6	Supermarkt-Anbieter habe Rechnungen gefälscht	Zahlungsdienstleister	1 * 2	2	4
7	Falscher Betrag (zu hoch) wird abgebucht	Zahlungsdienstleister	1 * 3	2	6
8	App wurde verändert	Kunde (kostenlos einkaufen)	3 * 2	2	12
9	Nutzt fremdes Handy zur Bezahlung	Kunde (kostenlos einkaufen)	2 * 1	3	6
10	Konto mit falschen Daten angelegt	Kunde (kostenlos einkaufen)	3 * 2	3	12

11	Kunde behauptet Liquidität ist gewährleistet	Kunde (kostenlos einkaufen)	3 * 1	2	6
12	Manipulation des Gerätes vor Ort	Angreifer (Zahlungsdaten)	3 * 1	4	12
13	Mitschneiden der Zahlungskommunikation	Angreifer (Zahlungsdaten)	3 * 2	5	30
14					

GEGENMAßNAHMEN

Risiko	Bewertung	Gegenmaßnahme
Mitschneiden der Zahlungskommunikation	30	Verschlüsselung der drahtlosen Kommunikation, Berechtigung durch Fingerabdruck
Manipulation des Gerätes vor Ort	12	Keine Schnittstellen offen lassen, Gerät fest gesichert, Alle nicht benötigten Dienste / Kommunikationsmodule abschalten, Kiosk-Modus
Konto mit falschen Daten angelegt	12	Post-Ident zur Verifizierung der angegebenen Daten
App wurde verändert	12	Alle Transaktionen am Server gegenprüfen