Fahrgastüberwachung Im Öffentlichen Personennahverkehr

Hausarbeit im Fach „Security und Privacy“. Dozentin: Prof. Dr. Ina Schiering

Tim Pröpper

Ostfalia Hochschule Wolfenbüttel, Am Exer 2, Wolfenbüttel info@ostfalia.de
https://www.ostfalia.de

Zusammenfassung Die Ausarbeitung beschäftigt sich mit den Risiken für den Datenschutz und die Informationssicherheit bei der Fahrgastüberwachung im Umfeld des Öffentlichen Personennahverkehrs (ÖPNV). Im ÖPNV werden mehrere Videokameras pro Fahrzeug verwendet, welche über einen Netzwerkswitch verbunden und über das Internet an eine zentrale Stelle des Verkehrsbetriebes gesendet werden. Dort werden die Videos temporär gespeichert und es gibt die Möglichkeit zur „Live-Ansicht“.
Die rechtliche Grundlage der Überwachung ist gegeben durch §4 Bundesdatenschutzgesetz Abs. 1 S. 2 „Videoüberwachung öffentlich zugänglicher Räume“ sowie Art. 6 Datenschutzgrundverordnung.
Durch die Netzwerkverbindung vieler Geräte im öffentlichen Raum entsteht ein hohes technisches Risiko für die Informationssicherheit, da der Zugriff von vielen Orten aus und ungestört über einen längeren Zeitraum möglich ist. Falls sich unerlaubt Zugriff auf die Netzwerkverbindung geschaffen wird, können die Daten veröffentlicht, manipuliert oder die Verbindung gestört werden. Um dies zu vermeiden, ist als Maßnahme eine Verschlüsselung der Verbindung zu empfehlen.
Ein Risiko für den Datenschutz besteht unter anderem durch die in der Zentrale arbeitenden Personen, welche Personen gewollt oder ungewollt identifizieren können. Um dem vorzubeugen, sind organisatorische Maßnahmen zur Sensibilisierung der Mitarbeiter zu empfehlen.

Keywords: ÖPNV · Überwachung · Datenschutz.

Inhaltsverzeichnis

1 Einleitung

Seit der Einführung der Videoüberwachung in den Bussen und Bahnen des Öffentlichen Personennahverkehrs (ÖPNV) sind diese Kameras ein Diskussionsthema in der deutschen Gesellschaft. Neben dem Argument des kommenden Überwachungsstaates gegenüber der Forderung nach mehr Sicherheit im öffentlichen Raum gibt es auch noch die Position der Verkehrsbetriebe, die Vandalismus in ihren Verkehrsmitteln vorbeugen möchten. Allerdings ist der Status quo eine allgemeine Überwachung aller Fahrgäste im ÖPNV, wodurch sich für diese Personen Datenschutzrisiken ergeben.

Diese Hausarbeit im Fach „Security und Privacy“ soll die Fahrgastüberwachung aus der Perspektive von Datenschutz und IT-Sicherheit darstellen und zugehörige Risiken mit entsprechenden Maßnahmen erläutern. Das Ziel ist auch die Verwendung von in der Vorlesung besprochenen Methoden und Inhalten zur Identifikation der Risiken, Beschreiben der Szenarien und dem Ableiten der Maßnahmen.

Zur Risikoidentifizierung in der IT-Sicherheit werden „Security-Cards“ verwendet und das Szenario wird durch ein „Risiko-Register“ verdeutlicht. Zugehörige Maßnahmen werden aus den Inhalten der Vorlesung ausgewählt. Für den Datenschutz werden die Risiken mit Hilfe der „Seven Types of Privacy“ identifiziert, welche auch in der Beschreibung des Szenarios Anwendung finden. Mögliche Maßnahmen werden durch die „Privacy Design Strategies“ beschrieben. Die Funktionsweise der Methoden wird jeweils in dem entsprechenden Abschnitt dargelegt.

Es wird zuerst der Begriff der Fahrgastüberwachung selbst erklärt und anschließend die rechtlichen und technischen Rahmenbedingungen aufgezeigt. Im Kapitel „Security“ werden für die IT-Sicherheit die Risiken identifiziert, ein konkretes Szenario beschrieben und dazu passende Maßnahmen abgeleitet. Im Kapitel „Privacy“ wird Selbiges für den Datenschutz wiederholt. Abschließend wird ein Fazit zu den Möglichkeiten und Risiken in der Fahrgastüberwachung gezogen.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

2 Übersicht

2.1 Abgrenzung des Begriffes

Öffentlicher Personennahverkehr bezeichnet den „räumlichen Bereich zur Beförderung von Personen im Berufs-, Ausbildungs-, Einkaufs- und sonstigen alltäglichen Verkehr mit Fahrzeugen des Straßen-, Schienen- und Schiffsverkehrs (Fähren) im Linienverkehr. “ [5]

Die Fahrgastüberwachung beschreibt die Maßnahmen, welche zur Aufzeichnung aller dem entsprechenden Verkehrsbetrieb zugehörigen Bereiche, in welchen sich Personen aufhalten, dienen. Die Einsatzgebiete umfassen also die Haltestellen sowie, (Bus-)Bahnhöfe die Verkehrsmittel selbst.

2.2 Rechtliche Rahmenbedingungen

Die rechtliche Grundlage für die Fahrgastüberwachung ist durch § 4 Bundesdatenschutzgesetz Abs. 1 S. 2 „ Videoüberwachung öffentlich zugänglicher Räume“ gegeben. Genauer heißt es dort:
„Bei der Videoüberwachung von

1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder
2. Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs

gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.“ [2]

Ebenfalls die Fahrgastüberwachung betreffend ist die europäische Datenschutzgrundverordnung, welche die Berechtigung zur Überwachung, Informationspflicht und das Recht auf Löschung festlegt:

Tabelle 1. Für die Fahrgastüberwachung im ÖPNV relevante Artikel der DSGVO [6]

Artikel	Bedeutung
Art.6 DSGVO Abs.1. S.1 Nr. d–f	Rechtmäßigkeit der Verarbeitung besteht durch den Schutz lebenswichtiger Interessen (d), die im öffentlichen Interesse liegende Aufgabe (e) und das berechtigte Interesse gemäß § 4 BDSG Abs. 1 S. 2
Art. 13 DSGVO	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
Art. 14 DSGVO	Informationspflicht bei Erhebung von personenbezogenen Daten, die nicht bei der betroffenen Person erhoben wurden
Art. 17 DSGVO	Recht auf Löschung

2.3 Technischer Hintergrund

In Abbildung 1 wird der Aufbau eines Systems zur Fahrgastüberwachung im ÖPNV dargestellt. Hierbei wird unterschieden zwischen den lokalen Komponenten, die an den Fahrzeugen und Haltestellen verbaut sind, und der zentralen Leitstelle. Über eine Netzwerkverbindung ist jede lokale Einheit mit der Zentrale verbunden.

Ein lokales System hat mehrere Kameras verbaut. Falls ältere, analoge Aufnahmegeräte verbaut sind, muss deren Bild vor Anbindung an das Netzwerk digitalisiert werden. Optional in den lokalen Systemen sind Anzeigen für die Kamerabilder sowie Mikrofone, welche in Kameras integriert sein können [11].

In der zentralen Verwaltung stehen die Server, welche die Videoaufnahmen verwalten, sowie das „Langzeit-Archiv". In diesem werden die Aufnahmen bis zur Löschung aufbewahrt. Über den Zeitraum bis zur Löschung der Daten besteht bisher Uneinigkeit, gemäß § 27 Bundespolizeigesetz (BPolG) ist eine Speicherung von bis zu 30 Tagen zulässig. In §6b Abs. 5 BDSG steht dem die unweigerliche Löschung der Daten gegenüber. In der „Orientierungshilfe zur Videoüberwachung" der Datenschutzbeauftragten von Niedersachsen wird final eine maximale Speicherdauer von 48 Stunden angegeben[3]. Neben der Darstellung der Videos sind auch technische Möglichkeiten zur Auswertung der Videos geschaffen. Auswertung bezeichnet nicht automatisch die automatische Analyse der Daten, sondern beschreibt vielmehr das Betrachten und Beurteilen dieser durch einen Mitarbeiter. In der zentralen Leitstelle, von welcher aus der Fahrbetrieb geregelt wird, ist häufig auch die Anzeige der Überwachungskameras.

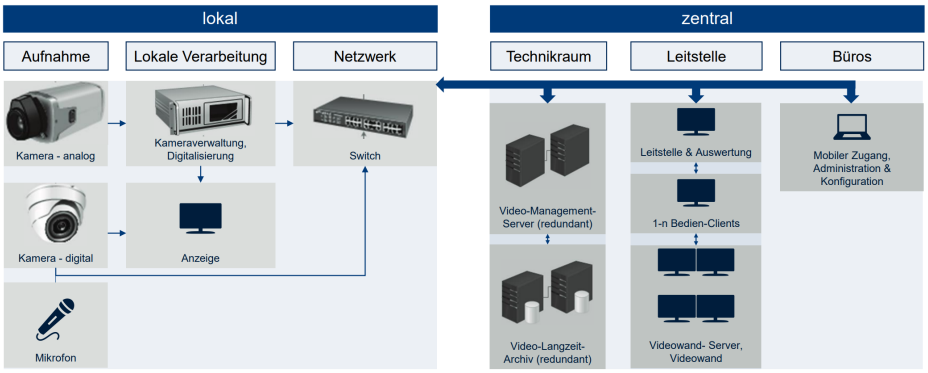

Abbildung 1. Aufbau eines typischen Systems nach [10]

Die genaue Implementierung eines Systems kann abweichen, wichtig zur Betrachtung der Risiken sind aber die Aspekte der Aufzeichnung an sich, die Datenübertragung über ein Netzwerk, die Bündelung in einer zentralen Leitstelle, temporäre Speicherung und die Möglichkeit zum mobilen Zugang.

3 Security

Der Bereich der Security beschreibt die IT-Sicherheit des Unternehmens. Dies umfasst das Gewährleisten der Schutzziele für die Informationsübermittlung, -speicherung und -Verarbeitung im System, unter anderem durch die Minimierung von Risiken [1]. Die Schutzziele sind

- Vertraulichkeit: Informationen sind ausschließlich den durch Besitzer autorisierten Personen/ Entitäten/ Prozessen zugänglich.
- Verfügbarkeit: Die Informationen stehen den Autorisierten in vereinbarter Darstellung und Zeit zur Verfügung.
- Integrität: Die Information ist weder fehlerhaft noch verfälscht

3.1 Risikoidentifizierung

Es gibt verschiedene Möglichkeiten, Risiken für die IT-Sicherheit zu identifizieren. Eine ist das Verwenden der „Security-Cards“ der University of Washington [4]. Diese Karten unterteilen Bedrohungen in verschiedene Kategorien: (1)„Human Impact“ ist der Einfluss, den ein Angriff auf das Opfer hat. (2)„Adversary's Motivation“ beschreibt die Beweggründe, (3)„Adversary's Resources“ die zur Verfügung stehenden Mittel und (4)„Adversary's Methods“ die Herangehensweise des Angreifers.

1. **Human Impact** trifft direkt auf die Karte „Personal Data“ zu, da zu jedem gefilmten Fahrgast präzise Zeit- und Ortsangaben des Aufenthaltsorts existieren. Die Karte „Financal Wellbeing“ ist ebenfalls angesprochen, da Menschen finanziell abhängig vom ÖPNV sein können. Sowohl positiv als auch negativ kann die Karte „Emotional Wellbeing“ beachtet werden, durch das Gefühl der Überwachung, welches durch die Kameras entstehen kann. Weniger Einfluss hat die Videoaufzeichnung auf das körperliche Wohlergehen, die soziale Struktur oder die Biosphäre.
2. **Adversary's Motivation** kann „Desire or Obsession“ nach einer bestimmten Person(-engruppe) sein, aber auch „Protection“ von Kindern, „Curiosity or Boredom“ oder „Acces or Convenience“, beispielsweise um Informationen über die Auslastung einer gewünschten Busverbindung zu erhalten. Weniger konkret sind politische, religiöse oder finanzielle Beweggründe.
3. **Adversary's Resources** stehen in verschiedenen Formen zur Verfügung. Zum einen viel „Time“, da das System dauerhaft erreichbar ist. Spezieller sind „Tools“, welche essenziell für eine technische Attacke sind. Ebenfalls hilfreich sind dagegen „Inside Capabilities“ und „Inside Knowledge“, durch welche sich der Angreifer einen Vorteil erschaffen kann.
4. **Adversary's Methods** hat drei primäre Karten, die auf das Thema zutreffen: „Physical Attack“- die Kameras sind an Haltestellen im öffentlichen Raum angebracht, direkt zugänglich und teilweise an spärlich besuchten Orten. „Technological Attack“ ist für den Angreifer durch die zentrale Netzwerkverbindung des Systems möglich. Dem gegenüber steht „Processes“: Große und komplexe Organisationen wie Verkehrsbetriebe bieten durch deren Bürokratie eine andere Angriffsmöglichkeit, die ausgenutzt werden kann.

3.2 Konkretes Szenario

In diesem Szenario beschafft sich ein Angreifer Zugriff zu der Netzwerkverbindung. Es kann in den meisten Fällen von einer „Technological Attack“ ausgegangen werden. Das Ziel des Angreifers ist unbekannt, ebenfalls die zur Verfügung stehenden Mittel, wobei „Inside Knowledge“ oder „Inside Resources“ nicht ausgeschlossen werden können.

In einem „Risiko-Register“ kann bei der Identifikation von Risiken die potenzielle entstehende Schadenshöhe sowie die Häufigkeit für die jeweilige Bedrohung dargestellt werden[9]. Ein simplifiziertes Risikoregister, ohne separate Felder für Bemerkungen, ist mit drei möglichen Bedrohungen in Abbildung 2 dargestellt.

Bedrohung	Schadenshöhe Einstufung			Eintritt 1 Mal in				
	Wiederherstellung integerer Zustand	Imageschaden	Finanz. Schaden	0,1 Jahr	1 Jahr	10 Jahren	30 Jahren	> 30 Jahren
Veröffentlichung der Daten	hoch	hoch	hoch			X		
Manip. der Daten	hoch	mittel	mittel				X	
Stören d. Verbindung	klein	klein	mittel		X			

Abbildung 2. Risiko-Register des Szenarios

Der gravierendste Fall für das Unternehmen wäre die Veröffentlichung der gesammelten Daten oder die Androhung dessen. Der in Kapitel 3.1 beschriebene „Human Impact“ wäre in diesem Fall am drastischesten. Da ein Verkehrsbetrieb stark von dem Vertrauen der Fahrgäste abhängig ist, kann der entstehende Imageschaden als hoch eingeordnet werden. Der Aufwand, einen integeren Zustand wiederherzustellen, ist ebenfalls als hoch anzusehen, da gegebenenfalls Teile der Systemarchitektur geändert werden müssen. So entsteht ein hoher finanzieller Schaden durch das anfallende Schließen von Sicherheitslücken, Ändern der Systemarchitektur und eventuelle Kosten zur Kompensation des Human Impact. Da das Beschaffen mit hohem Aufwand verbunden ist, aber leicht zur Erpressung genutzt werden kann, ist die Einschätzung eines Vorkommens von einem Vorfall in 10 Jahren realistisch.

Der nächste Fall ist die Manipulation der Daten, in welcher beispielsweise falsche Aufnahmen gesendet werden. Einen integren Zustand wiederherzustellen ist hier sehr aufwendig, da eine Manipulation der Daten nicht immer erkennbar ist. Der Imageschaden ist weniger hoch als bei einer möglichen Veröffentlichung,

aber dennoch zu berücksichtigen, falls die Manipulation publik gemacht wird. So entsteht ein mittlerer finanzieller Schaden, hauptsächlich bedingt durch die Wiederherstellung des integren Zustands. Durch den hohen Aufwand zur Manipulation der Daten ist diese Bedrohung als verglichen selten einzuordnen.

Die dritte mögliche Option ist das simple Stören der Verbindung. Dies kann durch eine „Physical Attack“ entstehen, beispielweise dem Durchschneiden einer Netzwerkleitung. Die Wiederherstellung des integeren Zustands ist durch eine Reparatur zu gewährleisten, der Imageschaden ist durch die geringe Signifikanz auch begrenzt und nur der finanzielle Schaden kann leicht ansteigen, durch beschädigtes Material oder entstehende Wartungskosten. Im Gegensatz zu den vorangehenden Bedrohungen tritt diese allerdings relativ häufig auf, da das Stören einer Verbindung mit wenig „Adversary's Resources“ möglich ist.

3.3 Maßnahmen

Da in diesem Szenario die nicht-technischen Systeme der Fahrgastüberwachung, wie Kontrolleure in der Zentrale, weniger stark eine Rolle spielen, kann sich auf die technische Sicherung der Netzwerkverbindung konzentriert werden. Um Maßnahmen abzuleiten, können die beeinträchtigten Schutzziele des Systems betrachtet werden. Das Stören der Verbindung ist eine Verletzung der Verfügbarkeit (Schutzziel Nr. 2). Um hier die Ausfallsicherheit zu erhöhen, kann eine Redundanz geschaffen werden. Wenn zwei voneinander getrennte Kommunikationskanäle existieren, wird es schwerer sein, die Verbindung zu stören. Das Schutzziel der Verfügbarkeit wird somit gesichert.

Um das Schutzziel der Integrität zu bestärken, muss die Architektur des Systems verändert werden. Eine Methode hierbei ist die Verwendung eines „Secure Hash Algorithm“, einem parametrisierten Hashverfahren. Der Hash wird vor dem Versenden aus den Eingabedaten und dem Shared key, einem Passwort, welches nur der Sender und Empfänger kennen, berechnet. So kann der Empfänger anhand des Hash-Wertes überprüfen, ob die Nachricht manipuliert wurde, da in diesem Falle der Hash-Wert abweicht. Die Integrität der Daten ist somit optimiert und die Manipulation der Daten kann erkannt werden.

Um das Schutzziel der Vertraulichkeit zu gewährleisten, muss die Integrität der Daten gegeben sein. Essenziell für das Sicherstellen der Vertraulichkeit ist zudem eine Verschlüsselung. Da in einem Verkehrsbetrieb alle Akteure bekannt sind (Abschnitt 2.3: Eine Zentrale und mehrere Netzwerk-Switches in den Fahrzeugen/ Haltestellen), kann eine „Public Key Infrastructure“ verwendet werden. In dieser gibt eine zentrale Stelle einen öffentlichen Schlüssel heraus, mit welchem die kleinere abhängige Akteure ihre Daten verschlüsseln und an die Zentrale senden. Dort werden die Inhalte wieder mit einem Private Key entschlüsselt. Dieser Private Key ist im Gegensatz zum Public Key geheim und nicht außerhalb der Zentrale bekannt. Die Authentizität der Keys kann innerhalb des Verkehrsbetriebes sichergestellt werden.

4 Privacy

Privacy befasst sich mit dem Datenschutz der vom System betroffenen Personen. Im Falle der Fahrgastüberwachung im ÖPNV sind dies die Fahrgäste, Mitarbeiter der Verkehrsbetriebe sind hiervon ausgenommen.

4.1 Risikoidentifizierung

Zur Identifikation der Risiken wird das Modell der „Seven Types of Privacy“ verwendet, welche erstmals 2011 in dem Projekt „Prescient“ beschrieben wurden [7]. Das Betrachten der verschiedenen Kategorien hilft bei der strukturierten Erfassung und Identifizierung von Risiken, die bei einer Verletzung des Datenschutzes entstehen können:

1. **Privacy of the Person** beschreibt die messbaren Körperwerte und -funktionen wie Blutdruck, Körpertemperatur oder medizinische Informationen. Diese können bei der Fahrgastüberwachung im ÖPNV weder durch Kameras noch Mikrofone erfasst werden.
2. **Privacy of Behavior and Action** bezeichnet die Informationen, die das persönliche Verhalten der Person beschreiben. Dies umfasst Gewohnheiten, Freizeitaktivitäten, Präferenzen, aber auch die politische Einstellung. Durch das Nutzen des ÖPNV werden Arbeitszeiten und sonstige in der Freizeit besuchte Orte auf Video aufgezeichnet. Durch Mikrofone können ausgesprochene Meinungen dokumentiert werden. Dies hängt zusammen mit dem nächsten Stichpunkt:
3. **Privacy of Communication** betrifft die Kommunikation in allen Medien wie direkte Gespräche, Telefonate oder schriftliche Kommunikation über das Internet. Gespräche können, falls Mikrofone installiert werden, aufgezeichnet werden.
4. **Privacy of Data and Image** ist zutreffend bei der Videoüberwachung und Fotos, Videos im Allgemeinen. Alle Kamerabilder der Fahrgastüberwachung fallen unter diesen Aspekt.
5. **Privacy of Thoughts and Feelings** lässt sich aus anderen Stichpunkten ableiten, da Gefühle und Gedanken nicht direkt gemessen werden können. Durch Körperhaltung, aufgezeichnete Gespräche, Gewohnheiten und gewöhnliche Aufenthaltsorte können aber Rückschlüsse gezogen werden.
6. **Privacy of Location and Space** verbietet das unerlaubte Aufzeichnen des Standortes einer Person. Im Falle der Fahrgastüberwachung ist durch die Kamerabilder, zugeordnet zu einer bestimmten Linie und versehen mit einem Zeitstempel, eine eindeutige Zuordnung der gefilmten Person zu einem Ort möglich. Die Erlaubnis ist im Fall des Verkehrsbetriebes durch die in Abschnitt 2.2 beschriebenen Bedingungen gegeben.
7. **Privacy of Association** stellt Verbindungen zwischen einzelnen Personen und Gruppierungen her. Die „Privacy of Association“ kann aus dem Inhalt der Kommunikation abgeleitet werden, aber auch aus dem gemeinsamen Aufenthaltsort von Personen. In der Videoüberwachung im ÖPNV können die Kamerabilder Rückschlüsse auf Kommunikationspartner zulassen.

4.2 Konkretes Szenario

Ein konkretes Szenario, bei dem der Datenschutz verletzt wird, ist das unerlaubte Teilen von Videoaufnahmen einer bestimmten Person. Dies kann auf verschiedene Weisen geschehen: Ein Mitarbeiter der in Kapitel 2.3 beschriebenen Zentrale entdeckt durch Zufall einen Bekannten auf dem Weg zu einer Veranstaltung oder wird durch dritte dazu gezwungen, nach einer bestimmten Person zu suchen.

Um das Risiko strukturiert analysieren zu können, wird eine Methode aus der Vorlesung verwendet. In dieser werden die betroffenen Personen und zutreffenden „Seven Types of Privacy“ sowie das Szenario selbst beschrieben und anschließend die beteiligten Personen sowie mögliche Folgen und Gründe dargestellt.

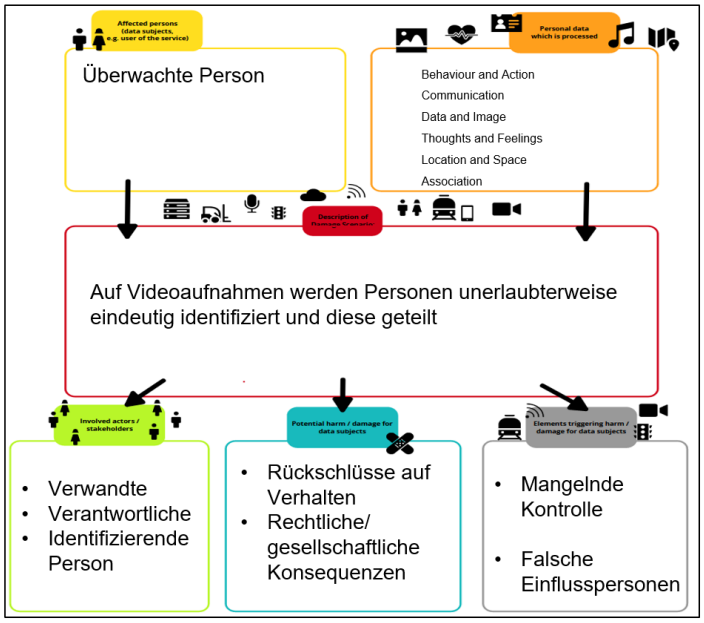

Abbildung 3. Anwendung der Methode auf das konkrete Szenario

Direkt betroffen ist in dem Szenario die Person auf den Kamerabildern eindeutig identifiziert wurde. Alle auf die Fahrgastüberwachung anwendbaren Types of Privacy können in diesem Szenario angewandt werden. Stakeholder sind in dem Szenario das soziale Umfeld der Person, aber auch die Person, die die Identifikation durchgeführt hat, sowie deren Verantwortliche. Der konkret entstehende Schaden ist das Zulassen ein Rückschlusses auf das Verhalten der Person, rechtliche oder gesellschaftliche Konsequenzen können ebenfalls nicht ausgeschlossen werden. Zu einem solchen Verstoß kann es durch mangelnde Kontrolle, falsche Einflusspersonen oder eine mangelhafte Unternehmenskultur kommen.

4.3 Maßnahmen

Maßnahmen können durch die „Privacy Design Strategies“ (PDS) abgeleitet werden [8]. Diese beschreiben Möglichkeiten, um Datenschutz zu verbessern. Aus den möglichen Strategien ist die erste Maßnahme, den Fahrgast rechtzeitig über die Aufzeichnung zu informieren. Eine übliche Möglichkeit ist in Abbildung 4 dargestellt, das Schild hängt im Eingangsbereich einer Straßenbahn und auf der Internetseite findet sich ein Kontaktformular. Damit zusammenhängend sind die Strategien „Enforce“ und „Demonstrate“. Wie in Kapitel 4.2 beschrieben, ist eine solche Art von Vorfall oft das Resultat durch ungenügenden Umgang mit Daten in der Unternehmenskultur. Nach einem solchen Ereignis ist es entsprechend wichtig, ausgehend vom Management das Thema Datenschutz stärker zu thematisieren. Dieses Vorgehen wird durch die PDS „Enforce“ beschrieben. Damit einhergehend ist die Strategie „Demonstrate“, in welcher die getroffenen Maßnahmen dokumentiert und nach außen präsentiert werden. Eine Kontrolle über die Daten gemäß PDS „Control“ kann in der Videoüberwachung allerdings nicht ermöglicht werden, da diese in den Bereichen des Verkehrsbetriebes allgemeingültig ist.

Neben den beschriebenen prozessorientierten PDS gibt es noch datenorientierte PDS. Eine Anwendbare ist die PDS „Hide“. Diese beschreibt die Einschränkung des Zugangs zu den Videoaufzeichnungen durch Zugangsbeschränkungen, aber auch durch Verschlüsselung von Daten. Weniger anwendbar dagegen ist die PDS „Separate“. Diese beschreibt das kontextabhängige Aufteilen von Daten, um kein Schließen von Korrelationen zwischen verschiedenen Daten wie Kamerabildern und Ortsangaben zuzulassen. Allerdings ist das Zuordnen der Kamerabilder zu den Orten oder Fahrzeugen essenziell, und Überwachungskameras geben meist eine Uhrzeit direkt im Bild an. Auch das Minimieren und Abstrahieren von Daten ist nur schwerlich anwendbar, da eine Videoaufzeichnung versehen mit einem Zeitstempel schon eine geringe Form der Datenerhebung darstellt.

Abbildung 4. Hinweis in einer Straßenbahn der Braunschweiger Verkehrs-GmbH. Eigene Fotografie, 19.01.2023

5 Fazit

Die Fahrgastüberwachung im ÖPNV ist in vielerlei Hinsicht ein prekäres Thema, auch aus der Perspektive von Datenschutz und IT-Sicherheit. Die einzige Kontrollmöglichkeit der betroffenen Personen über ihre Daten ist das Vermeiden der Verkehrsmittel, was für viele Menschen nicht umsetzbar ist.

Weiterhin gibt es oft nur wenig Transparenz vonseiten der Verkehrsbetriebe zu der Menge der gesammelten Daten sowie der Art der Verarbeitung. Über den Link des in Abbildung 4 dargestellten Schildes wird beispielsweise nur auf die Homepage des Verkehrsbetriebes verwiesen, ohne konkrete weiterführende Informationen bereitzustellen. Auch über die in Abschnitt 2.3 beschriebene Verwendung von Mikrofonen oder in Abschnitt 4.3 vorgeschlagenen internen Prozesse zur Sicherstellung des Datenschutzes wird wenig aufgeklärt.

Diesen Mängeln gegenüber steht die in „Abschnitt 3.1: Adversary's Methods“ beschriebene große Angriffsfläche auf welche auf verschiedene Arten und mit unterschiedlichen Motivationen zugegriffen werden kann. Eine Schmälerung des Risikos eines Angriffs selbst ist die Tatsache, dass die Videoüberwachung eines Verkehrsbetriebs selten ein lohnendes Ziel darstellt, verglichen mit anderen Unternehmen.

Die effektivsten Maßnahmen zur Sicherung der Fahrgastüberwachung umfassen also das Einrichten einer sicheren, verschlüsselten Verbindung und das Propagieren einer gesunden Unternehmenskultur. Zu Letzterem gehört insbesondere eine Schulung der Mitarbeiter, bei welcher ein besonderes Augenmerk auf den verantwortungsbewussten Umgang mit den aufgezeichneten Daten liegt.

Literatur

1. BSI Bundesamt für Sicherheit in der Informationstechnik: Bsi-standard 100-2: It-grundschutz-vorgehensweise, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile
2. Bundestag: Bundesdatenschutzgesetz: § 4 abs. 1 s. 2
3. Daniela Windelband: Flächendeckende videoüberwachung in öffentlichen verkehrsmitteln bald in allen bundesländern? (20 April 2016), https://www.datenschutz-notizen.de/flaechendeckende-videoueberwachung-in-oeffentlichen-verkehrsmitteln_-bald-in-allen-bundeslaendern-0914516/
4. Denning, T., Friedmann, B., Kohno, T.: The security cards: a security threat brainstorming toolkit (2013), http://securitycards.cs.washington.edu/index.html
5. Dr. Friedrich von Stackelberg, Dr. Robert Malina: Öffentlicher personennahverkehr (öpnv) (2018), https://wirtschaftslexikon.gabler.de/definition/oeffentlicher-personennahverkehr-oepnv-46428/version-269708
6. Europäische Union: Datenschutzgrundverordnung
7. Gutwirth, S., Gellert, R., Bellanova, R., Friedewald, M., Schütz, P., Wright, D.: Legal, social, economic and ethical conceptualisations of privacy and data protection (2011), http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf
8. Hoepman, J.H.: Privacy Design Strategies: (The Little Blue Book). Jaap-Henk Hoepman (2022), https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf
9. Königs, H.P.: Beschäftigung mit risiken und risikomanagement. In: IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken, pp. 9–44. Springer Fachmedien Wiesbaden, Wiesbaden (2017). https://doi.org/10.1007/978-3-658-12004-7{_}2
10. Landesbeauftragte für den Datenschutz Baden-Württemberg: Orientierungshilfe „videoüberwachung in öffentlichen verkehrsmitteln“: Datenschutzgerechter einsatz von optisch-elektronischen einrichtungen in verkehrsmitteln des öffentlichen personennahverkehrs und des länderübergreifenden schienengebundenen regionalverkehrs (2015), https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/oh-vue-oepnv.pdf
11. Reuter, M.: Bürgerrechtler: Berliner nahverkehr soll auf kameras mit mikrofonen verzichten. netzpolitik.org **2019** (12022019), https://netzpolitik.org/2019/buergerrechtler-berliner-verkehrsgesellschaft-soll-auf-kameras-mit_-mikrofonen-verzichten/