Fahrgastüberwachung im Öffentlichen Personennahverkehr

Tim Pröpper

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

Zusammenfassung Die Ausarbeitung beschäftigt sich mit den Risiken für den Datenschutz und die Informationssicherheit im Umfeld des Öffentlichen Personennahverkehrs.
Der Fokus liegt hierbei auf der Betrachtung des Systems bestehend aus Kameras und Mikrofonen sowie der dahinterstehenden Architektur zur Verwaltung und potenziellen Auswertung. Hierfür wird zuerst ein Überblick über die komplette Architektur sowie das rechtliche Umfeld gegeben und anschließend werden alle möglichen Risiken bezüglich Privacy und Security gegenübergestellt.
Es wird auf zwei konkrete Szenarien eingegangen:
1. Ein Security-Risiko, welchem unerlaubt auf die Netzwerkverbindung zugegriffen wird. Hieraus entstehen verschiedene Bedrohungen, wie die Veröffentlichung oder Manipulation der Daten dieser Netzwerkverbindung, oder auch das einfache Stören der Verbindung. 2. Ein Privacy-Risiko, in welchem auf Videoaufnahmen unerlaubterweise Personen eindeutig identifiziert und die Aufnahmen geteilt werden.
In diesen Szenarien wird der entstehende Schaden sowie beteiligte Komponenten dargestellt und anschließend werden zugehörige Maßnahmen erörtert.
136/ (150–250) words.

Keywords: ÖPNV · Überwachung · Datenschutz.

Inhaltsverzeichnis

1 Einleitung

Der Anteil der Überwachung im öffentlichen Personennahverkehr hat mit fortschreitender Digitalisierung beständig zugenommen.

– hat er das? – Abkürzungen: DSGVO, ÖPNV, BDSG
– Motivation
– Ziel der Hausarbeit: Anwendung von Methoden
– Aufbau: Übersicht, Analyse von 2 Risiken inklusive Maßnahmen

Tabelle 1. Table captions should be placed above the tables.

Heading level	Example	Font size and style
Title (centered)	**Lecture Notes**	14 point, bold
2nd-level heading	**2.1 Printing Area**	10 point, bold
3rd-level heading	**Run-in Heading in Bold.** Text follows	10 point, bold
4th-level heading	*Lowest Level Heading.* Text follows	10 point, italic

2 Übersicht

2.1 Einsatzgebiet

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 Einsatzgebiete von Fahrgastüberwachung betreffen alle dem entsprechenden Verkehrsbetrieb zugehörigen Gebiete, in welchen sich Personen aufhalten. Dies umfasst also die Haltestellen sowie 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:

Tabelle 2. 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 einer typischen Überwachungseinrichtung im ÖPNV dargestellt. Hierbei wird unterschieden zwischen dem lokalen Aufbau, der an den Fahrzeugen und Haltestellen anzufinden ist. Über ein Netzwerk ist jedes lokale System mit der zentralen Leitstelle verbunden.

Ein lokales System hat in der Regel mehrere Kameras (analog oder digital) verbaut. Das Bild der älteren, meist analogen Kameras muss vor Anbindung an das Netzwerk digitalisiert werden. Optional in den lokalen System sind eine Anzeige für z.B. den Fahrer des Busses, sowie Mikrofone, welche in den Kameras integriert sein können.

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 Dauer bis zur Löschung der Daten heißt 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 umfasst nicht automatisch die automatische Analyse der Daten, sondern beschreibt vielmehr das Betrachten und Beurteilen dieser durch einen Mitarbeiter.

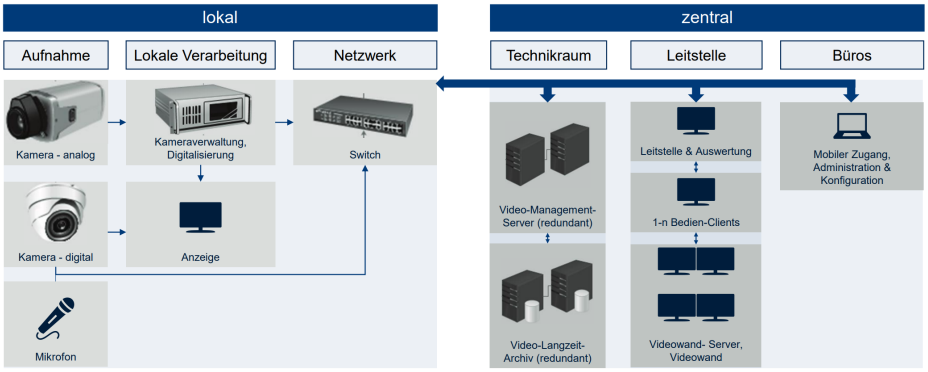

Abbildung 1. Aufbau eines typischen Systems [8]

Die genaue Implementierung eines Systems kann abweichen, wichtig zur Betrachtung der Risiken im Bereich von Datenschutz und IT-Sicherheit sind aber die Aspekte der Datenübertragung über ein Netzwerk, die Leitstelle, temporäre Speicherung und die Möglichkeit zum mobilen Zugang zum System.

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 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 Motivation, (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 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 Überwachung 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 auch „Acces or Convenience“, beispielsweise um Informationen über die Auslastung einer gewünschten Bahnverbindung 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 verfügbar ist. Spezieller sind „Tools“, welche essentiell für eine technische Attacke sind. Spezifischer 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 erreichbar und teilweise an spärlich besuchten Orten. „Technological Attack“ ist für den Angreifer durch die zentrale Netzwerkverk des Systems sehr bequem möhlich. Dem gegenüber steht „Processes“: Große und komplexe Organisationen wie Verkehrsbetriebe bieten durch die entstandene Bürokratie eine andere Art der Angriffsfläche.

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[7]. Ein simplifiziertes Risikoregister, ohne seperate 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 höchsten. 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, der durch das Schließen von Sicherheitslücken, Ändern der Systemarchitektur und eventuellen Kosten zur Kompensation des Human Impact entsteht. 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 aufwändig, da eine Manipulation der Daten nicht immer direkt erkennbar ist. Der Imageschaden ist weniger hoch als bei einer möglichen Veröffent-

lichung, 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 bestärkt.

Um das Schutzziel der Integrität zu bestärken, muss die Architektur des Systems verändert werden. Zum Einen kann das System grundlegend sicherer gemacht werden, zum Anderen kann auch die Sicherstellung der Integrität selbst gefördert 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 diesm Falle der Hash-Wert abweicht. Die Integrität der Daten ist somit sichergestellt.

Das Schutzziel der Vertraulichkeit setzt die Sicherung der Integrität der Daten voraus. Neben Secure Hashes können ebenfalls eine „Public Key Infrastructure“ oder symmetrische Kryptographie verwendet 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 „7 Types of Privacy“ verwendet.

4.2 Konkretes Szenario

4.3 Maßnahmen

5 Fazit

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. 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
8. 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