Ende-zu-Ende-Sicherheit für die Multimodale Mobilität in einer Smart City

Franziska Plate, Detecon International GmbH, Köln (Franziska.Plate@detecon.com)

Erik Buchmann, Hochschule für Telekommunikation, Leipzig (buchmann@hft-leipzig.de)

1 Abstract

Im Zuge einer Mobilitätswende hin zu umweltfreundlicheren Transportmitteln werden Konzepte der multimodalen Mobilität immer wichtiger. Multimodale Mobilität bedeutet, dass dem Nutzer in Abhängigkeit von persönlichen und externen Faktoren eine Kombination aus Reisemitteln angeboten, gebucht und abgerechnet wird, die sein Mobilitätsbedürfnis erfüllen. Zu den persönlichen Faktoren zählen dabei Präferenzen wie Preis, Komfort oder Reisezeit, zu den externen die Verfügbarkeit von Verkehrsmitteln, Staus oder Umweltparameter. Dies erfordert eine komplexe Vernetzung von Verkehrsmitteln, Umweltsensoren, Mobilitäts- und Abrechnungsdienstleistern, intelligenten Verfahren zur Stau- und Klimavorhersage, sowie eine Echtzeitüberwachung der Nutzerposition. Der IT-Sicherheit kommt deswegen eine entscheidende Bedeutung zu.

In diesem Papier untersuchen wir auf einer generischen Ebene, inwieweit sich die multimodale Mobilität in einem typischen Smart-City-Szenario technisch absichern lässt. Zu diesem Zweck fokussieren wir uns auf Nahverkehrsmittel und die für deren Buchung und Abrechnung erforderlichen Wertschöpfungsketten. In Anlehnung an den IT-Grundschutz modellieren wir die Datenflüsse und Übertragungswege, die für die Umsetzung der multimodalen Mobilität erforderlich sind. Wir untersuchen, inwiefern die derzeit verfügbaren Konzepte der IT-Sicherheit für diesen Anwendungsfall geeignet sind, und führen eine Risikoanalyse durch.

Unsere Arbeit zeigt, dass bei einer konsequenten Realisierung eines Sicherheitskonzepts das größte Risiko durch Fehlbedienung oder Fehlkonfiguration des Smartphones des Nutzers entsteht, und wir zeigen detailliert auf, um welche Risiken es sich dabei handelt.

2 Einleitung

Fragen zur urbanen Mobilität werden gerade für Ballungsräume immer wichtiger. Bereits heute ist offensichtlich, dass ein Mobilitätskonzept, welches vor allem auf den von fossilen Brennstoffen angetriebenen motorisierten Individualverkehr setzt, in dieser Form nur begrenzt in die Zukunft fortgeschrieben werden kann. Stattdessen werden integrierte Mobilitätsangebote untersucht, die verschiedene Mobilitätsangebote wie schienen- oder straßengebundene öffentliche Verkehrsmittel, Car-Sharing, Car-Pooling oder Leihfahrräder intelligent zu einer multimodalen Mobilitätsform zusammenführen, die das Mobilitätsbedürfnis des Nutzers erfüllen. Dabei sind persönliche Präferenzen wie Preis, Komfort, Reisezeit oder Umweltfreundlichkeit zu berücksichtigen. Des Weiteren sind externe Faktoren wie die Verfügbarkeit von Verkehrsmitteln, Verspätungen oder Umweltparameter mit einzubeziehen.

Die multimodale Mobilität erfordert eine komplexe Vernetzung von Verkehrsmitteln, Umweltsensoren, Mobilitäts- und Abrechnungsdienstleistern, intelligenten Verfahren zur Stau- und Klimavorhersage, sowie eine Echtzeitüberwachung der Nutzerposition. Sie ist daher eine typische Anwendung für eine Smart City-Plattform. Dabei übernimmt die Plattform verschiedene komplexe Funktionen entlang der Wertschöpfungskette der multimodalen Mobilität, von der Reiseplanung über das Smartphone des Nutzers bis zur Abrechnung der tatsächlich in Anspruch genommenen Mobilitätsdienste.

Der IT-Sicherheit [11] kommt dabei eine entscheidende Bedeutung zu [17]. Die Akzeptanz einer Lösung für die multimodale Mobilität hängt nicht nur von Fragen der Vertraulichkeit und des Datenschutzes ab, sondern auch von der täglichen Verfügbarkeit des Dienstes. Spätestens bei der Abrechnung ist die Datenintegrität wesentlich.

In diesem Papier analysieren wir, wie sich die Wertschöpfungsketten der multimodalen Mobilität in einem typischen Smart-City-Szenario technisch absichern lassen. Dabei konzentrieren wir uns auf die intelligente Verknüpfung von Nahverkehrsmitteln. In Anlehnung an den IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik modellieren wir die Datenflüsse und Übertragungswege, die für die Umsetzung der multimodalen Mobilität erforderlich sind. Wir untersuchen, inwiefern die derzeit verfügbaren Konzepte für diesen Anwendungsfall geeignet sind, und führen eine Risikoanalyse durch. Unser Ziel ist dabei eine Ende-zu-Ende (E2E) Absicherung der Systeme und Übertragungswege entlang der Wertschöpfungskette der multimodalen Mobilität.

Unsere Arbeit zeigt, dass bei einer konsequenten Realisierung eines Sicherheitskonzepts das größte Risiko durch Fehlbedienung oder Fehlkonfiguration des Smartphones des Nutzers entsteht, und wir zeigen detailliert auf, um welche Risiken es sich dabei handelt. Unsere Arbeit basiert auf einer Masterarbeit an der Hochschule für Telekommunikation Leipzig [4].

Aufbau dieser Arbeit: Im nächsten Abschnitt gehen wir auf verwandte Arbeiten ein. In Abschnitt 4 erläutern wir die Wertschöpfungskette der multimodalen Mobilität für ein Smart-City-Szenario. Die Abschnitte 5 und 6 beschreiben mögliche Ansätze zur Absicherung dieses Szenarios, gefolgt von einer Analyse der noch zu realisierenden Risikobehandlungsoptionen. Die Arbeit schließt mit einer Diskussion und einem Fazit.

3 Verwandte Arbeiten

In diesem Abschnitt diskutieren wir (3.1) das Konzept der multimodalen Mobilität, (3.2) die Grundlagen der für die multimodale Mobilität erforderlichen Technologien, (3.3) Ansätze zur Absicherung von Smart-City-Architekturen sowie (3.4) das Vorgehen bei der Absicherung von IT-Infrastrukturen nach BSI Grundschutz.

3.1 Die multimodale Mobilität

Aufgrund des Wachstums und der zunehmenden Vernetzung von Verkehrsmitteln miteinander, entsteht eine Komplexität, die es zunehmend erschwert, die zur Verfügung stehenden Verkehrsmittel effizient zu nutzen und zu kombinieren [12]. Es fehlt dabei eine Synchronisation zwischen den verschiedenen Verkehrsmittelanbietern und den jeweiligen Verkehrsmitteln, um eine effiziente Reiseplanung zu ermöglichen. Das Konzept der multimodalen Mobilität ist eine Überarbeitung der Verkehrskonzepte, die bis jetzt auf einzelnen Säulen, z.B. Individualverkehr oder lokaler öffentlicher Personennahverkehr (ÖPNV), beruhen. Da der ÖPNV nicht beliebig erweitert werden kann und beispielsweise zusätzlich eingesetzte Busse ebenfalls im Stau stehen würden, soll die multimodale Mobilität zukünftig dabei helfen, Reiserouten effizient zu planen, um das Verkehrsaufkommen, ebenso wie die CO_2-Belastung, in den Städten nachhaltig zu reduzieren.

Die multimodale Mobilität ist ein Konzept, bei dem unterschiedliche Verkehrsmittel, innerhalb einer Reiseroute, miteinander kombiniert werden. Dabei umfasst das Konzept sowohl den Nahverkehr, wie z.B. BikeSharing, CarSharing, Straßenbahnen, Busse und Taxen, als auch den Fernverkehr, u.a. Züge, Flugzeuge und Schiffe. Nutzer können entweder eigenständig auf die verschiedenen Verkehrsmittel, wie z.B. dem Miet-Fahrrad, innerhalb der Reiseroute zurückgreifen, oder sie planen die Route mit Hilfe von Planungsservices, wie z.B. Google Maps. Bereits 2001 [13] verfolgte die Deutsche Bahn (DB) die neue Mobilitätsstrategie und realisierte erste Piloten, u.a. das Miet-Rad (Call a Bike) und einen CarSharing-Dienst, welche den Nutzer „von-Haustür-zu-Haustür“ bringen sollten. Mittlerweile bietet die DB auch eine Möglichkeit Reiserouten multimodal zu planen. Auch über die Internetsuchmaschine Google bzw. deren Karten-Dienst Google Maps können Routen mittlerweile multimodal geplant werden.

Damit dies allerdings möglich ist, müssen einige Voraussetzungen geschaffen werden. Beginnend mit den notwendigen Verkehrsmitteln, müssen diese dem Nutzer uneingeschränkt zur Verfügung stehen. Hierbei ist das Problem, dass sichergestellt sein muss, dass der Nutzer zur erwarteten Zeit und am erwarteten Ort auch das entsprechende Verkehrsmittel vorfindet. Es müssen somit zentrale Stationen eingerichtet werden, an denen solche Miet-Fahrzeuge zur Verfügung stehen, um so einen reibungslosen Ablauf der Reiseroute zu gewährleisten. Wenn die Miet-Fahrzeuge an einem beliebigen Ort abgestellt werden dürfen, so wie bei DriveNow, car2go oder dem KVB-Rad, muss es z.B. über eine App die Möglichkeit für den Nutzer geben zu erkennen, wo sich das Fahrzeug befindet. Um sicherzustellen, dass der Nutzer das Fahrzeug am angezeigten Ort auch findet, bieten car2go und DriveNow eine Reservierungsfunktion für die Fahrzeuge an. Damit die Fahrzeuge nun auch aus den Randgebieten einer Stadt wieder in das Zentrum gelangen, bietet z.B. DriveNow, seinen Nutzern einen rabattierten Miet-Preis, wenn sie das Fahrzeug wieder im Stadtzentrum parken.

Es muss also im Rahmen der multimodalen Routenplanung bekannt sein, welche Verkehrsmittel wie, wann und wo zur Verfügung stehen. Ebenfalls muss das Planungssystem wissen, wo mögliche Umsteige-Punkte liegen. Die Nutzung von mehreren Verkehrsmitteln innerhalb einer Route kann über ein umfassendes E-Ticket gelöst werden [14]. Hierbei kann das Fahrzeug mit dem Ticket, z.B. eine Karte, entsperrt, genutzt und bezahlt werden. Der Nutzer benötigt nicht mehr für jedes Verkehrsmittel ein eigenes Ticket. Die Abrechnung erfolgt im Nachgang auf Basis der genutzten Services. Diese Abrechnung stellt natürlich eine erhebliche Aufgabe an den Datenschutz und bedarf der Umsetzung eines umfassenden Datensicherheits-Konzeptes [11].

3.2 Technische Grundlagen der multimodalen Mobilität

3.2.1 Das Internet of Things (IoT)

Das Internet of Things (IoT) [5] beschreibt physische Gegenstände, die über eine Netzwerkverbindung miteinander verbunden werden. IoT-Geräte bestehen im Allgemeinen aus einem Microcontroller, Kommunikations-Modul, einem Sensor und einem Aktor. Der Sensor, wobei ein IoT-Gerät auch mehrere Sensoren enthalten kann, erfasst Daten (z.B. Temperatur, Position, Bewegung oder auch Gesundheitsdaten), die über Kommunikationsverbindungen an weitere Geräte, Systeme oder Dienste zur Weiterverarbeitung versendet werden können. Der Aktor hingegen steuert und regelt das IoT-Gerät, wie z.B. den Heizungszufluss eines smarten Heizkörpers oder das Öffnen eines smarten Fahrradschlosses.

Im IoT werden die Gegenstände lesbar, erkennbar, auffindbar, adressierbar und/oder steuerbar [8]. IoT-Geräte erhalten somit eine gewisse Intelligenz, welche es ihnen ermöglicht, kontextbezogene Entscheidungen [8] zu treffen oder diese zu ermöglichen. Dabei können sie auf Informationen zugreifen, die durch andere Geräte bereitgestellt wurden.

Das führt dazu, dass IoT-Geräte vermehrt Anwendung in komplexen Diensten und Anwendungsfällen finden. Angefangen bei intelligenten (smarten) Haustechnik-Lösungen hilft das IoT mittlerweile bei der Realisierung von ganzen Smart City-Anwendungsfällen. Somit lässt sich sagen, dass das IoT die Digitalisierung von Städten ermöglicht hat.

Gleichwohl nimmt die Angriffsfläche in der IoT-Umgebung aufgrund der Heterogenität von Geräten, Kommunikationsmedien, Anwendungen und Diensten vielfältig zu [6]. Laut des BSI [10] wird die Umsetzung wichtiger Sicherheitsmechanismen im IoT häufig vernachlässigt und die IT-Sicherheit spielt bei den IoT-Geräten noch keine oder eher eine untergeordnete Rolle. Für den Anwender der IoT-Geräte stehen bei einer Kaufentscheidung eher die Funktionalitäten und der damit verbundene Komfortgewinn im Fokus.

3.2.2 Smart City-Plattformen

Der Begriff „Smart City“ [9] beschreibt ein Entwicklungskonzept für Städte. Zielgedanke einer Smart City ist die vollständige Vernetzung der verschiedenen Anwendungsfälle über eine zentrale Plattform mittels einer Netzwerkverbindung (siehe Abbildung 1). Diese ermöglicht den Daten- und Informationsaustausch zwischen den einzelnen IoT-Komponenten. Genauso wie die Steuerung, Überwachung und Fernwartung der eingesetzten IoT-Geräte.

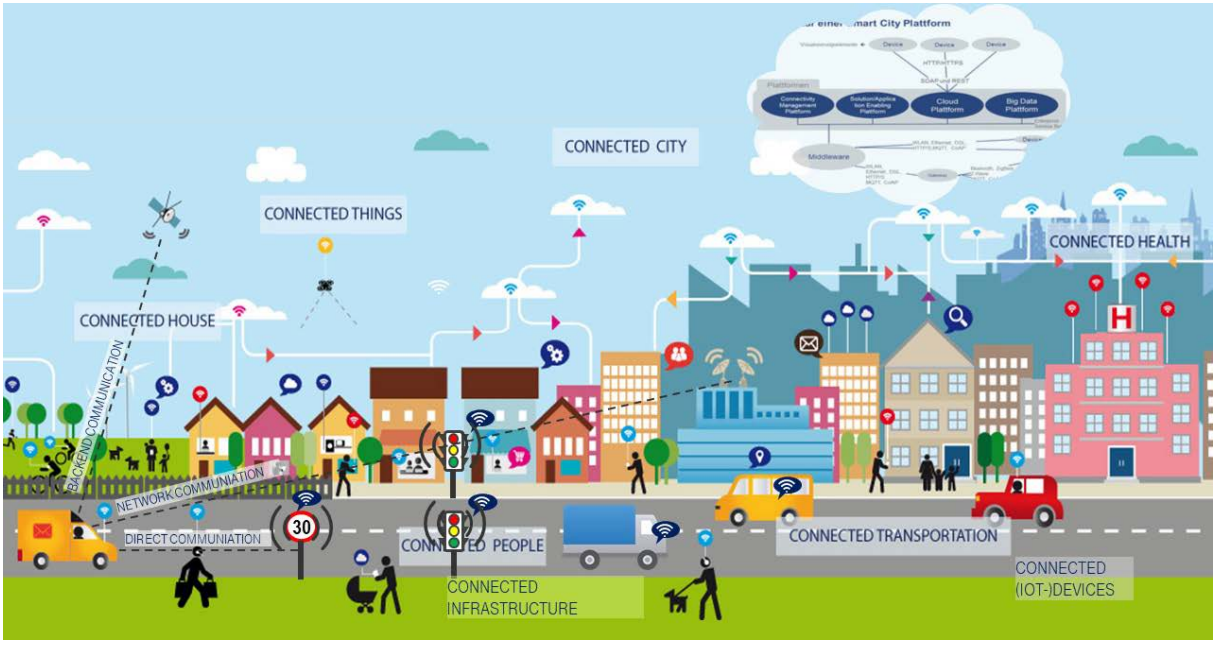

Abbildung 1: Idealisiertes Bild einer Smart City und Einblick in die digitale Zukunft [37]

Wie eine solche zentrale Plattform aussehen kann ist nachfolgend beschrieben und, auf Basis dessen, in Abbildung 2 exemplarisch dargestellt.

Eine Connectivity Management-, Solution Enabling- und eine Big Data-Plattform bilden dabei die ganzheitliche Smart City-Plattform ab.

Innerhalb der IoT-Anwendungsfälle kann es sowohl IoT-Geräte mit SIM-Karte als auch ohne SIM-Karte geben. Die Komponenten, welche eine SIM-Karte besitzen, können ihre Daten direkt über das Mobilfunknetz an die Middleware bzw. die Smart City-Plattform senden. Komponenten ohne SIM-Karte müssen zur Übertragung der Daten auf Technologien, wie z.B. NB-IoT (NarrowBand IoT) zurückgreifen. Die Komponenten senden ihre Daten an ein Gateway, das mit einer Middleware verbunden ist. Die Middleware dient als ein Interface zwischen den IoT-Komponenten und ermöglicht die Kommunikation untereinander. Um die Datenmengen, welche an die Plattform gesendet werden, vorab zu reduzieren, können erste Implementierungen zur Datenanalyse bereits auf dem Gateway realisiert werden. Hierfür muss wiederum vorab entschieden werden, welche Daten derart wichtig sind, dass sie über die SIM-Karte bzw. die Netzwerkverbindung gesendet werden müssen.

Die Daten werden dann anschließend, über verschiedene Kommunikationstechnologien, zur Analyse und weiteren Verarbeitung an die Big Data-Plattform gesendet. Die aufbereiteten Daten werden anschließend von der Solution Enabling-Plattform und der darauf befindlichen Business Logik (der Kern der Anwendung) weiter prozessiert und für eine Darstellung über Visualisierungselemente vorbereitet. Über eine App können dann die aufbereiteten Daten auf dem Smartphone, dem Tablet oder der Smart-Watch dargestellt und genutzt werden.

Der modulare Aufbau der Plattform kann mit Hilfe von Integrationslösungen, wie z.B. dem Enterprise Service Bus (ESB) oder durch Microservices und serverless-Architekturen, ermöglicht werden. Hierbei dient der jeweilige Mediation-Service als eine Art Vermittler, welcher es ermöglicht, die einzelnen Plattformen – unabhängig vom Standort – miteinander zu verbinden. Über eine solche Integrationslösung wird ebenfalls die Kommunikation zwischen den einzelnen Plattformen ermöglicht.

Mittlerweile gibt es einige Alternativen zum üblichen ESB, wie z.B. Lightweight Internet of Things Service Bus Architecture (LISA) [15] und MuleESB [16], welche sich speziell für den Einsatz im IoT eignen.

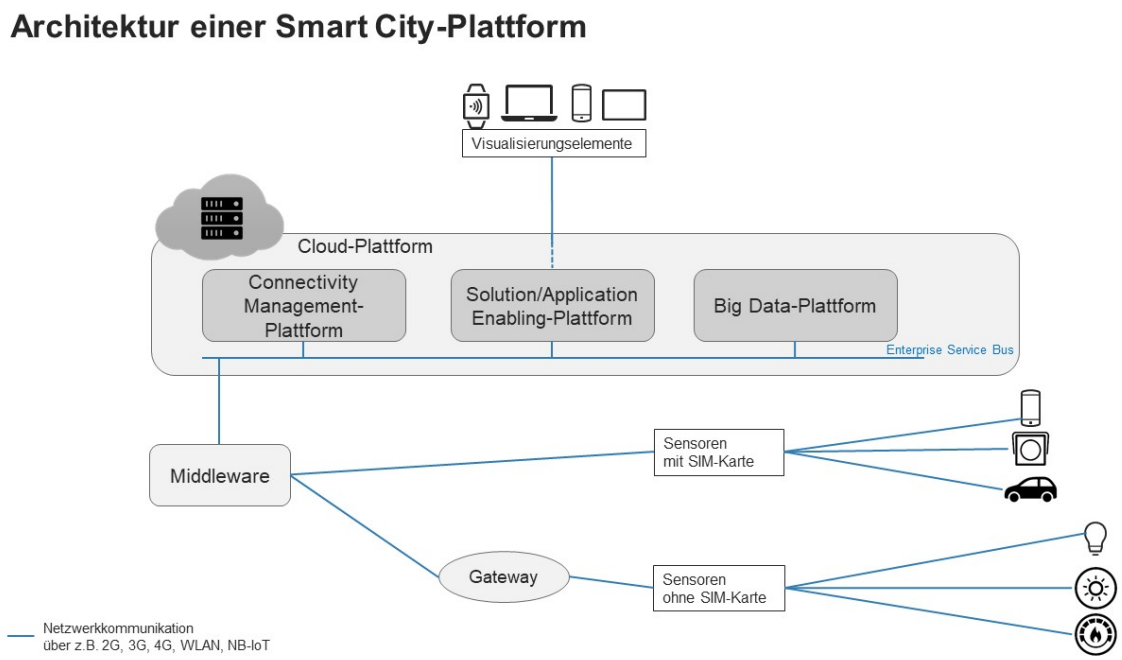

Abbildung 2: Darstellung einer möglichen Smart City-Plattform

Momentan liegt der Fokus allerdings auf der Realisierung einzelner und unabhängiger Smart City-Anwendungsfälle. Sie agieren dabei eigenständig und ohne eine Vernetzung oder Kommunikation zu weiteren Anwendungsfällen oder zu einer zentral gesteuerten Plattform. Erste Pilotprojekte werden vereinzelt umgesetzt, wie z.B. Smart Parking (Park&Joy), Smart Wastemanagement (Bonn Orange) oder Smart Lighting (Stadtwerke Bonn). Aufgrund der fehlenden Vernetzung der Anwendungsfälle untereinander, widerspricht diese isolierte Realisierung allerdings dem eingangs beschriebenen Grundgedanken einer Smart City.

3.3 Sicherheit von Smart City-Architekturen

Um die Datensicherheit innerhalb einer IoT- bzw. Smart City-Anwendung sicherzustellen, gibt es bereits eine Vielzahl an Lösungen, welche die Komponenten gegen potentielle Gefahren absichern sollen.

3.3.1 IoT-Hardware

Jedes IoT-Gerät benötigt eine Software, welche die notwendige Kommunikation ermöglicht. Um die Software [18] vor Manipulationen zu schützen müssen Sicherheitsfunktionen implementiert werden [7]. Hierzu zählen bspw. der Secure Boot, ein abgesicherter Flashspeicher und das Trusted Platform Module (TPM). Diese Implementierungen ermöglichen das sichere Ausführen des Codes und verhindern, dass dieser durch Schadcode ausgetauscht werden kann.

Um die Komponenten zusätzlich gegen unzulässige Zugriffe abzusichern, können rollenbasierte Zugriffsrechte, sowie komplexe Benutzernamen und Passwörter implementiert werden. Eine Implementierung dieser Lösungsansätze ist allerdings kein festgeschriebener Standard und liegt im Ermessen des jeweiligen Entwicklers/Programmierers, um Schwachstellen bei IoT-Geräten zu vermeiden sollten diese Ansätze jedoch, je nach Umfang und Art des Anwendungsfalls, zum Standard werden.

3.3.2 Protokolle

Protokolle [18] ermöglichen dem IoT-Gerät mit dem Internet zu kommunizieren. Da die IoT-Geräte in ihren Ressourcen (u.a. Speicherkapazität, Rechenleistung und Energiezufuhr) limitiert sind, werden kompakte und effiziente Kommunikationsprotokolle benötigt. Mittlerweile

wurden sichere Protokolle für die IoT-Kommunikation entwickelt und als Standard etabliert. Hierzu zählen u.a. das Message Queuing Telemetry Transport (MQTT)-Protokoll und das Constrained Application Protocol (CoAP).

Das Ziel von MQTT [19] ist die Bereitstellung eines leichten und einfach zu bedienenden Kommunikationsprotokolls für das IoT. Die Sicherheitsaspekte sind in mehreren Ebenen, Netzwerk-, Transport- und Anwendungsebene, aufgeteilt, welche jeweils verschiedene Arten von Angriffen verhindern. Das Protokoll selbst spezifiziert nur wenige Sicherheitsmechanismen. Allerdings nutzt MQTT eine Reihe von bereits existierenden Sicherheitsstandards, wie z.B. das VPN für die Netzwerksicherheit und die TLS für die Transportsicherheit. Auf Anwendungsebene stellt das MQTT-Protokoll eine notwendige Nutzer-Kennung, sowie Anmeldeinformationen (Benutzernamen und Passwort) zur Verfügung, so dass sich die IoT-Geräte authentifizieren können.

Das Constrained Application Protocol (CoAP) [20] ist ein spezielles Web-Transfer-Protokoll für den Einsatz in beschränkten Netzwerken, wie dem IoT. Es nutzt als Sicherheitsmaßnahmen DTLS-Parameter, was einem 3071-Bit-RSA-Schlüssel entspricht. Dennoch kann das Protokoll auf dem kleinsten System betrieben werden

3.3.3 Übertragungswege

Innerhalb des IoT müssen die jeweiligen Komponenten, wie z.B. die Plattform und die jeweiligen IoT-Geräte auf irgendeine Art und Weise miteinander kommunizieren und ihre Daten übertragen. Da die Anforderungen der einzelnen Komponenten unterschiedlich sind, kommen ebenso verschiedene Übertragungstechnologien im IoT zum Einsatz.

3.3.3.1 Mobilfunk

Der Mobilfunk entwickelt sich stetig weiter und mittlerweile ist bereits der Mobilfunkstandard der 4. Generation (4G; bekannt auch unter LTE) fast überall verfügbar. Um sich als Netzwerknutzer gegenüber dem Netzwerkbetreiber zu authentifizieren, wird die weltweit eindeutige International Mobile Subscriber Identity (IMSI) genutzt. Diese ist in der Nutzerdatenbank des Providers mit einem vorab generierten Subscriber Authentication Key (SAK), dem s.g. Shared Secret, gespeichert. Seit der Einführung des Mobilfunks der 3. Generation (UMTS) [22] ist eine gegenseitige Netzwerkauthentifizierung Standard. Somit muss sich nicht nur der Nutzer bei der Basisstation, sondern auch die Basisstation beim Nutzer authentifizieren. Zum Schutz der Privatsphäre des Netzwerkteilnehmers wird nach erfolgreicher Authentifizierung nicht mehr die IMSI übertragen, sondern die verschlüsselte Extended Encrypted Mobile Subscriber Identity (XEMSI). Diese setzt sich aus der Adresse des zuständigen Netzknotens und der verschlüsselten IMSI zusammen. Die verschlüsselte IMSI wird mit Hilfe der Nutzerdatenbank zur ursprünglichen TMSI aufgelöst. Diese TMSI wird ebenfalls verschlüsselt (Temporary Encrypted Mobile Subscriber Identity [TEMSI]) und dient als Sitzungsschlüssel für die nachfolgenden Kommunikationen. Damit keine Nachverfolgung des Nutzers möglich ist, wird die XEMSI regelmäßig gewechselt. Allerdings wird auch hier zu Beginn die IMSI unverschlüsselt übertragen und ist demnach aus dem Netzwerk sichtbar.

Der Mobilfunkstandard der 4. Generation (LTE) [23] wurde unteranderem dazu entwickelt, dem wachsenden Datenverkehr technisch gerecht zu werden. Die E2E-Sicherheit im LTE wird mit einer Sicherheits-Architektur, welche im 3GPP TS 33.401 [24] beschrieben ist, umgesetzt. Darüber hinaus nutzt LTE das TCP/IP in Kombination mit kryptografischen Algorithmen (128 Bit Verschlüsselung), welches ebenfalls Sicherheit in die Datenübertragung bringt.

Alle Mobilfunkstandards sehen als Fallback-Option ein Umschalten auf den veralteten GSM-Standard vor, der nur eine einseitige Authentifizierung des Nutzers gegenüber dem Netzwerkbetreiber enthält und einen heute zu schwachen Verschlüsselungsalgorithmus nutzt.

3.3.3.2 Wireless Local Area Network (WLAN)

Eine weitere Möglichkeit innerhalb des IoT zu kommunizieren bietet WLAN. Aktuell verwendeter Verschlüsselungsstandard im WLAN [25] ist WPA2. Gegenüber WPA nutzt WPA2 die sichere Verschlüsselungsmethode Advanced Encryption Standard (AES). Im Juli 2018 stellte die Wi-Fi Alliance allerdings einen neuen Verschlüsselungsstandard vor. WPA3 [26] soll demnach WPA2 voraussichtlich ab 2019 ablösen. WPA3 bietet gegenüber seinem Vorgänger eine robustere Authentifizierung und höhere kryptografische Stärke für hochsensible Daten. Die Authentifizierung des Nutzers gegenüber des Wireless Access Point wird mittels eines Passworts, dem Pre-Shared Key, oder durch die Abfrage von Benutzernamen und Passwort realisiert, wobei jeder Nutzer eigene Zugangsdaten erhält und diese zentral gepflegt werden können. Für letzteres wird die IEEE 802.1x-Authentifizierung mit dem verfügbaren Extensible Authentication Protocol (EAP) verwendet. EAP ermöglicht eine gegenseitige Authentifizierung der Kommunikationsteilnehmer.

3.3.4 IoT-Plattform

Wie bereits in Kapitel 3.2 beschrieben, finden verschiedene „Arten“ von Plattformen mit jeweils unterschiedlichen „Aufgaben“ im IoT Anwendung. Diese Plattformen können in einer Cloud-Implementierung als eine ganzheitliche Plattform realisiert werden. Allerdings verfolgen die Anbieter solcher IoT-Plattformen unterschiedliche Strategien und bieten demnach auch unterschiedliche IoT-Plattform-Lösungen an. Unternehmen müssen bei der Auswahl einer geeigneten IoT-Plattform ihre aktuellen Anforderungen und zukünftigen Einsatzfelder berücksichtigen. Allerdings stoßen alle Plattform-Anbieter auf dieselben Herausforderungen, wenn es um das Thema Datensicherheit geht.

Um die Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) der IT-Sicherheit bzw. Datensicherheit in der Plattform-Umgebung [27] [29] zu realisieren, müssen Anbieter mindestens einen etablierten Verschlüsselungs-Algorithmus, strenge Zugriffskontrollen – Authentifizierung sowie Autorisierung der IoT-Geräte – sowie regelmäßige Datensicherung in ihrer Plattform-Umgebung realisieren. Zusätzlich hilft ein Notfallkonzept dabei die IoT-Plattform wenige Minuten nach einem Angriff oder einer Katastrophe wieder betreiben zu können.

Ebenso bieten regelmäßige und sichere Firmware-Updates, das Monitoring der Geräte zur Warnung vor ungewöhnlichem Verhalten, sichere Kommunikationskanäle, wie z.B. TLS, IPsec und VPN, sowie die Forderung starker Passwörter und die Redundanz der Server, zusätzliche Sicherheit in die Plattformumgebung. Auch der Einsatz bekannter Verschlüsselungs-Protokolle, wie z.B. MQTT und HTTPS, können eine sichere Kommunikation zur und von der Plattform gewährleisten.

Die GSMA [21] empfiehlt außerdem den Einsatz eines s.g. Root of Trust, was ein Zertifikat oder ein Public-Key-basiertes System zur Authentifizierung von Entitäten der Computerplattform in einem Unternehmen ist, sowie das Nutzen traditioneller Firewalls.

Gleichwohl müssen die Sicherheitsmaßnahmen einheitlich und stringent innerhalb der kompletten Plattform-Landschaft um- und eingesetzt werden, auch wenn verschiedene Lieferanten beteiligt sind. Eine ISO 27001 Zertifizierung [28] bietet hierfür eine Basis, die zeigt, dass die IT-Dienstleister die notwendigen Standardsicherheitsmaßnahmen für die IT-Sicherheit nach dem IT-Grundschutz umsetzen.

3.3.5 Applikationssicherheit

Um die Vorteile der IoT-Technologien nutzen zu können, werden Business-Applikationen benötigt, welche die eigentliche Business-Logik des IoT-Anwendungsfalls enthalten. Die Business-Applikationen ermöglichen im Fall der multimodalen Mobilität beispielsweise das Planen, Prüfen und Aktualisieren der Routen. Da diese Applikationen (im Folgenden auch App

genannt) vom Nutzer sensible Daten abfragen und verarbeiten, müssen auch diese durch Sicherheitsmaßnahmen gegen potentielle Angriffe geschützt werden.

Innerhalb des Entwicklungsprozesses [30] kann der Grundsatz „security-by-design“, welcher mit Hilfe von Frameworks, Design Pattern und modernen Programmiersprachen umgesetzt werden kann, eine gewisse Grundsicherheit gewährleisten. Des Weiteren sollten Anwendungsentwickler sicherstellen, dass die Anwendung die Richtlinien für Datensicherheit einhält und nicht auf unnötige Informationen zugreift. Eine App für mobile Endgeräte sollte demnach nur jene Zugriffsberechtigungen erhalten, die für den Betrieb notwendig sind. Da Smartphone-Nutzer meistens die Werkseinstellungen verwenden, sollten die Berechtigungen vorab vom Anwendungsentwickler gesetzt werden. Hier bietet sich das Verfolgen des Konzeptes „security-by-default“ an. Ebenso müssen die Informationen aus der App sicher und verschlüsselt an die Plattform und die jeweiligen Systeme übertragen werden. Um den Zugriff auf die App serverseitig einzuschränken muss hier eine Web-Application Firewall eingesetzt werden, sowie eine starke und strenge Authentifizierung und Autorisierung. Ebenfalls sollten Apps einen E2E-Sicherheitskanal [48], wie z.B. SSL/TLS, nutzen, wenn sensible Daten übertragen werden, ebenso wie einen etablierten Verschlüsselungsalgorithmus, wie z.B. AES.

3.3.6 Ende-zu-Ende-Sicherheit (E2E) im IoT

Da die IoT-Geräte und die Steuerungsplattform, auf denen Daten konsumiert und gemeinsam genutzt werden, u.a. unterschiedliche Eigentums- und Richtliniendomänen besitzen, schlägt Cisco [31] unterschiedliche Eigentums- und Richtlinienkonzepten vor. Des Weiteren wird die Notwendigkeit für das Umsetzen entsprechender Identitätskontrollen hervorgehoben. Damit die im IoT-Anwendungsfall beteiligten Unternehmen die jeweiligen Daten austauschen können, müssen Vertrauensbeziehungen zwischen ihnen aufgebaut werden. Als Lösung für die Problematik der limitierten Ressourcenverfügbarkeit im IoT, wodurch klassische Authentifizierungs- und Verschlüsselungsmethoden, wie z.B. AES und RSA, nicht eingesetzt werden können, schlägt Cisco die Entwicklung neuer Authentifizierungsverfahren vor, die mit den Erfahrungen der heutigen starken Verschlüsselungs- und Authentifizierungsmethoden entwickelt werden können.

IBM [1] beschreibt die Sicherheit im IoT als ein Problem und eine Verantwortlichkeit, für das jeder Beteiligte eines IoT-Ökosystems zuständig ist. Das bedeutet, dass Hardwarehersteller, Applikationsentwickler, Verbraucher, Betreiber und Weitere, die am Ökosystem IoT beteiligt sind, verantwortlich dafür sind, dass die optimalen Prozessabläufe (Best Practices) zur Erreichung der Sicherheit im IoT umgesetzt werden. Mögliche Angriffe auf die IoT-Geräte können die unbefugte Beschaffung von sensiblen oder privaten Daten, deren Manipulation und deren Kontrolle sowie das Stören oder Verhindern von Services innerhalb des IoT-Systems mit sich bringen. Die vorgeschlagenen Lösungen sind jedoch nur auf einzelne Bestandteile des IoT-Ökosystems beschränkt und bilden kein E2E-Sicherheitskonzept ab.

In einem weiteren Ansatz befassen sich Suo et al. [3] mit der allgemeinen Betrachtung der Sicherheit im IoT. Dieser Beitrag stützt sich auf eine Betrachtung der Sicherheitsaspekte der IoT-Kern-Technologien. Auch hierbei wird noch einmal deutlich, dass die Sicherheitstechnologien lediglich getrennt voneinander Anwendung finden, also entweder im IoT-Gerät selber, auf den Plattformen oder in der Konnektivität. Hier ist weiterer Forschungsbedarf notwendig, um ein Konzept zu entwickeln, welches die Datensicherheit innerhalb der kompletten Wertschöpfungskette ermöglicht.

Der Gedanke und das Ziel eines integrierten Sicherheits-Frameworks für das IoT wird in der Arbeit von Babar et al. [2] thematisiert und aufgegriffen. Zu Beginn definieren die Autoren sechs wichtige Merkmale für Sicherheit im IoT, u.a. leichtgewichtige Kryptografie, physikalische Sicherheit über ein TPM, standardisierte Sicherheits-Protokolle, sichere Betriebssysteme, das Betrachten von zukünftigen Anwendungsbereichen und ein sicherer Speicher. Allerdings

wird nicht erläutert, wie diese Merkmale mit dem vorgeschlagenen Sicherheits-Framework implementiert werden können.

Grundsätzlich erläutert die Arbeit kein konkretes Sicherheits-Framework, sondern lediglich einzelne generische Sicherheits-Ansätze für die im IoT angewendeten Protokolle, sowie für die Hard- und Softwareplattformen. Eine anschließende genauere Betrachtung, ob sich dieser in der Arbeit beschriebene Ansatz wirklich für den Einsatz im IoT eignet und ob alle Beteiligten (Stakeholder) im Lösungsansatz mit einbezogen wurden, wird in der Arbeit nicht beschrieben.

Erste mögliche Ansätze und Realisierungsempfehlungen zum Eindämmen von potentiellen Risiken und zum Erreichen zusätzlicher Sicherheit im IoT werden in den Sicherheitsrichtlinien der GSMA [21] beschrieben. Diese Guidelines beschreiben u.a. eine Reihe an Risiken, welche im Rahmen von IoT aufkommen, und mögliche Vorgehen sowie Handlungsmöglichkeiten, um diese Risiken einzudämmen bzw. zu minimieren. Die vorgeschlagenen und empfohlenen Vorgehensweisen sind jedoch als eigenständige Lösungen (Standalone-Lösungen) beschrieben und werden isoliert voneinander betrachtet. Dabei unterteilt die GSMA die Lösungsansätze in Realisierungsempfehlungen mit hoher, mittlerer und niedriger Priorität. Wie diese Einteilung zustande kommt, wird in dem Dokument nicht deutlich.

Die Arbeit von Biswas et al. [34] beschreibt ein Sicherheits-Framework, basierend auf der Blockchain-Technologie. Zielgedanke von Biswas et al. ist das Vermeiden von Bedrohungen hinsichtlich der Schutzziele[1] mit Hilfe der Blockchain. Das Paper beschreibt hierfür ein Sicherheits-Framework basierend auf verschiedenen Ebenen. Die Ebenen präsentieren hierbei eine Art Prozesskette. Nachdem die Daten durch Sensoren und Aktoren generiert wurden, werden sie durch einen Kommunikations-Layer an den Database-Layer bzw. die jeweiligen Interfaces/Applikationen gesendet. Die Transaktionsdaten werden dann in einer Blockchain, welche sich im Database-Layer befindet, gespeichert. Die Arbeit schlägt zwar ein mögliches Sicherheits-Framework vor, jedoch wird nicht darauf eingegangen, wie praktikabel ein Einsatz des Frameworks sein würde. Es wird innerhalb der Arbeit nicht auf die Nachteile einer Blockchain verwiesen. Ebenfalls wird außenvorgelassen, dass die Eigenschaften einer Blockchain, wie z.B. ein hoher Energiebedarf und großer Daten-Overhead, eine Implementierung im IoT gar nicht zulassen. Mit der vorgeschlagenen Lösung wird keine E2E-Sicherheit erreicht, da eine Absicherung der Sensoren/ en, Kommunikationswege und Applikationen nicht thematisiert wird. Die Blockchain stellt hier lediglich die Integrität der übertragenen Daten sicher.

Im Gegensatz zu Biswas et al. definieren Dorri et al. [33] in ihrer Arbeit bereits eine leichtgewichtige Variante der Blockchain, die sich für den Einsatz im IoT potentiell eignen soll. Eine Evaluierung dieser leichtgewichtigen Blockchain wird in einer Folgearbeit von Dorri et al. [32] am Beispiel einer Smart Home Implementierung vorgenommen. Im Rahmen der Evaluierung der entstandenen zusätzlichen Sicherheit innerhalb der Smart Home-Anwendung unter Anwendung der leichtgewichtigen Blockchain wird deutlich, dass die Schutzziele sowie die Verfügbarkeit und Nutzerkontrolle mit Hilfe der eingesetzten Blockchain-Variante erreicht werden können. Das eigentliche Implementierungsvorgehen der Blockchain in die Smart Home-Anwendung wird in der Arbeit nicht beschrieben. Ebenso fehlt eine abschließende Betrachtung, ob sich diese Blockchain-Variante für weitere IoT-Anwendungsfälle eignet.

[1] Vertraulichkeit, Integrität und Verfügbarkeit

3.4 Vorgehen nach BSI Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist Stand der Technik im Bereich der Sicherheitskonzeptionierung, weswegen das beschriebene Vorgehen zur systematischen Strukturierung eines Problemfalls in Bezug auf Datensicherheit angewendet wird. Zunächst fordert die im BSI-Standard 200-2 [35] beschriebene Methodik die Durchführung einer Strukturanalyse. Innerhalb der Strukturanalyse werden die Schutzbedarfe der einzelnen Komponenten festgestellt. Für die Schutzbedarfsfeststellung ist eine Erfassung der relevanten IT-Systeme, IoT-Komponenten, IT-Anwendungen und Kommunikationskanäle notwendig. Diese Zusammenfassung wird als Informationsverbund bezeichnet und bietet einen Überblick über die Datenobjekte, IT-Anwendungen, eingesetzte Hardware und die Kommunikationsverbindungen.

Der Informationsverbund dient ebenso zur Abgrenzung des Geltungsbereichs des Sicherheitskonzeptes. Ein Informationsverbund umfasst sowohl technische, als auch infrastrukturelle, personelle und organisatorische Komponenten. Für die Modellierung des Informationsverbundes nach dem IT-Grundschutz müssen aus dem IT-Grundschutz-Kompendium [38] passende Bausteine ausgewählt und umgesetzt werden. Diese Bausteine sind in prozess- und systemorientierte Bausteine aufgeteilt. Die Prozess-Bausteine gliedern sich dabei in folgende Bausteine: implementierte Anforderungen, Organisation und Personal, Konzepte und Vorgehensweisen, Betrieb und Detektion & Reaktion. Die System-Bausteine umfassen die Bausteine Anwendung, IT-Systeme, industrielle IT, Netze und Kommunikation und Infrastruktur. Die Bausteine enthalten jeweils eine Beschreibung der betrachteten Komponente, der Vorgehensweise und IT-Systeme, sowie einen Überblick über spezifische Gefährdungen und Anforderungen, wie die Komponente abgesichert werden kann. Der Informationsverbund wird konkret anhand des gewählten Anwendungsfalls mit Hilfe der entwickelten Wertschöpfungskette abgegrenzt und beschrieben.

Die durch die Strukturanalyse ermittelten Schutzbedarfe dienen anschließend als Grundlage für eine Risikoanalyse nach BSI 200-3. Die Risikoanalyse wird üblicherweise im Rahmen eines Workshops oder Experteninterviews mit Domänenexperten aus dem Unternehmen durchgeführt. Die Erkenntnisse werden mit Hilfe des BSI Standards 200-3 strukturiert. Die Risikoanalyse zeigt dabei die Handlungsbedarfe auf. Der Anwendungsfall „multimodale Mobilität“

Um die multimodale Mobilität in einer Smart City realisieren zu können, erfordert es die Vernetzung der einzelnen Verkehrsmittel und Komponenten über eine Smart City-Plattform. Die Wertschöpfungsketten bestimmen, welche Komponenten dabei welche Daten untereinander austauschen.

3.5 Ablauf der multimodalen Mobilität

Der Benutzer legt einmalig über die Anwendung (nutzbar über eine App oder Webseite/Webanwendung) ein Benutzerprofil mit den notwendigen Zahlungsinformationen und Log in-Daten an. Ist dies geschehen, läuft eine Reise wie folgt ab:

- Der Benutzer kann über eine App oder Webseite/Webanwendung die Reiseroute individuell und mit verschiedenen Reisemitteln planen. Hierzu werden sowohl Positions-[2] als auch Verfügbarkeitsdaten benötigt.
- Die Tickets, sowie Reservierungen, können direkt gebucht und bezahlt werden. Hierbei werden die Zahlungsinformationen des Nutzers benötigt.

[2] Hierbei werden sowohl die Positionsdaten der Verkehrsmittel als auch die des Nutzers benötigt um die Reiseroute planen zu können.

- Der Buchungsprozess wird innerhalb der Anwendung durchgeführt.
- Das Benutzerprofil stellt der Anwendung für den Buchungsprozess alle benötigten Informationen bereit.
- Alle Buchungsinformationen (inkl. Zahlungsinformationen und Nutzungsdaten) werden an den jeweiligen Dienstleister zur weiteren Verarbeitung weitergeleitet.
- Die Daten der Verkehrsmittel werden mit Hilfe von IoT-Hardware gesammelt und in einer Cloud weiterverarbeitet. Dies können sowohl Positions-, Nutzungs- als auch Verfügbarkeitsdaten sein.
- Das Vernetzen der Verkehrsmittel ermöglicht eine sekundenaktuelle Berechnung der Position, um so Verspätungen einzuplanen, Umsteigezeiten anzupassen oder Wegezeiten zu aktualisieren.
- Sobald Anschlüsse gefährdet sind, werden Alternativrouten ermittelt. Hierzu werden sowohl Positionsdaten als auch Informationen über die angestrebte Reiseroute (Nutzungsdaten) benötigt.
- Verkehrsmitteldienstleister nutzen die erfassten Daten, um die eigenen Fahrpläne in Echtzeit anzupassen.

3.6 Wertschöpfungskette der multimodalen Mobilität

Innerhalb der multimodalen Mobilität werden verschiedene Elemente benötigt, welche im Zusammenspiel einen Wert bzw. Nutzen für die Akteure generieren. Die Wertschöpfungskette (siehe Abbildung 4) verdeutlicht die Wertegenerierung innerhalb der multimodalen Mobilität und zeigt einen vereinfachten Prozess, keine Prozesskette. Sie zeigt also wo und an welcher Stelle eine Wertschöpfung stattfindet und welche Komponenten daran beteiligt sind. Die Komponenten und Inhalte der Wertschöpfungskette wurden anhand des in Kapitel 3.1 beschriebenen Konzeptes der multimodalen Mobilität sowie der in Kapitel 4.1 vorgenommenen Abgrenzung des Anwendungsfalls hergeleitet.

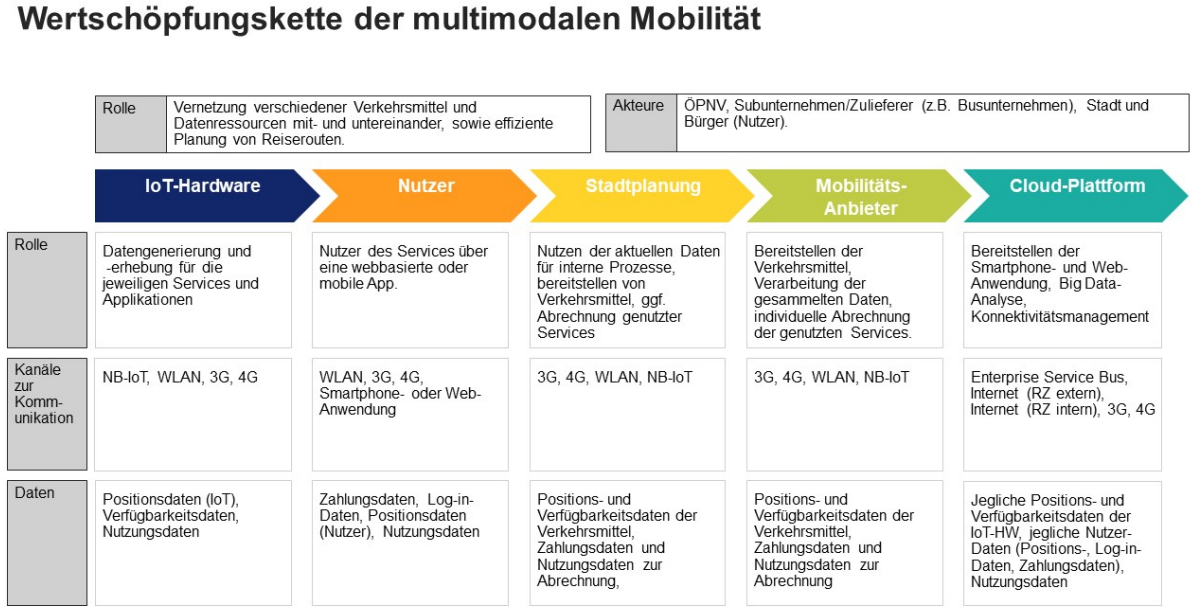

Abbildung 3: Wertschöpfungskette der multimodalen Mobilität

Übergreifend ermöglicht die multimodale Mobilität und die abgebildete Werkschöpfungskette eine Vernetzung verschiedener Verkehrsmittel und Datenressourcen mit- und untereinander,

sowie das effiziente Planen von Reiserouten. Dabei werden primär der ÖPNV, Subunternehmen/Zulieferer, wie z.B. Busunternehmen, die Stadt an sich und die Bürger (Nutzer) als Akteure definiert. Für die Wertschöpfungskette ist es unerheblich, ob eine Kommune den ÖPNV komplett selbst bereitstellt, oder private Unternehmen mit der Durchführung bzw. den Betrieb einzelner Linien oder ganzer Subnetze beauftragt.

Die Wertschöpfungskette gliedert sich in die beteiligten Komponenten IoT-Hardware, Nutzer, Mobilitätsanbieter, Stadtverwaltung/-planung und Cloud-Plattform.

Dabei hat jede Komponente einen anderen Informationsbedarf und trägt entscheidend zu der Wertschöpfung bei. Die IoT-Hardware kann dabei in Fahrrädern, Autos, Bussen und in Straßenbahnen verbaut sein. Auch das Mobiltelefon eines Nutzers enthält Sensoren und kann bzw. muss als IoT-Komponente dienen, da so der genaue Standort des Nutzers ermittelt werden kann. Ebenfalls nutzt jede der Komponenten verschiedene Kanäle zur Kommunikation und benötigt nur jene Daten und Informationen, welche für die Erfüllung der individuellen Funktion notwendig sind. Dabei werden die Daten jedoch nicht nur generiert, sondern auch über die verschiedenen Kommunikationskanäle zur weiteren Verarbeitung versendet. Dabei werden überwiegend die Mobilfunkstandards 2G, 3G und 4G sowie WLAN und kabelgebundene Übertragungswege genutzt.

Um zu verdeutlichen, welchen Weg die Daten innerhalb des Anwendungsfalls der multimodalen Mobilität nehmen, wurde der Datenfluss in Abbildung 5 illustriert. Als Grundlage für das Erstellen dieser Abbildung dienen die in der Wertschöpfungskette definierten und beschriebenen Komponenten aus, sowie die Darstellung einer möglichen Smart City-Plattform.

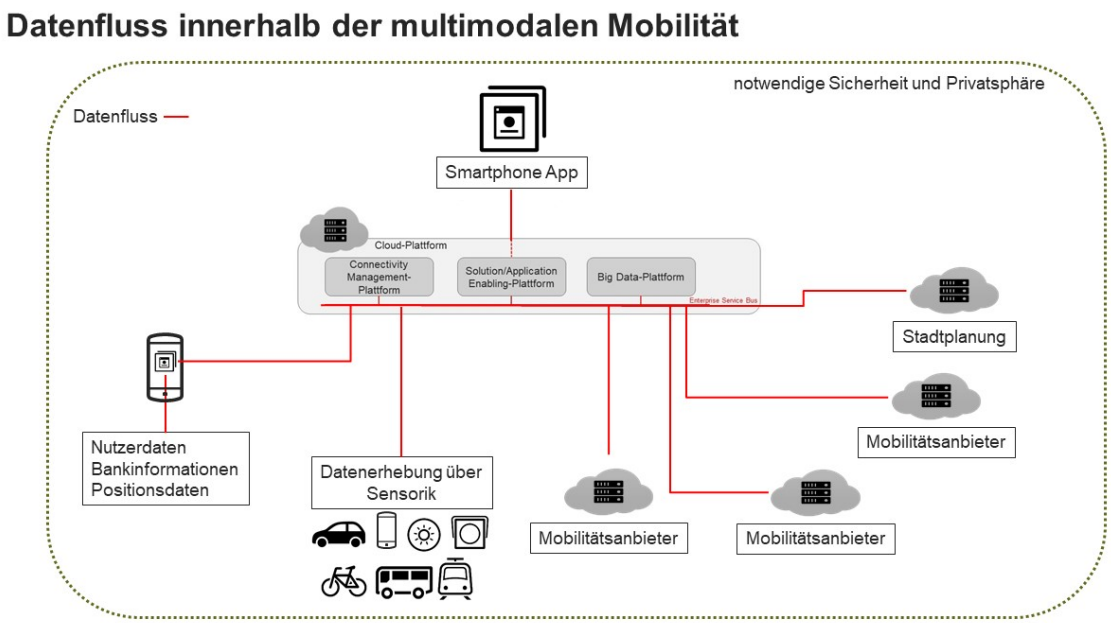

Abbildung 4: Darstellung des Datenflusses innerhalb der multimodalen Mobilität

Es soll zudem verdeutlicht werden, welche Bereiche und Bestandteile es mit einem E2E-Sicherheitskonzept abzusichern gilt. Ebenso ist die Entwicklung eines E2E-Sicherheitskonzeptes notwendig, um eine umfassende Sicherheit innerhalb des Anwendungsfalls sicherzustellen.

4 Absicherung der multimodalen Mobilität

Innerhalb der multimodalen Mobilität werden sowohl unsensible als auch sensible Daten generiert und genutzt. Welcher Schutzbedarf innerhalb der multimodalen Mobilität besteht, wird anhand der Schutzbedarfsfeststellung nach BSI 200-2 [35] definiert. Dazu ist zunächst eine

Strukturanalyse erforderlich, welche die Daten, Dienste, Übertragungswege etc. modelliert. Da bereits offensichtlich ist, dass einzelne Daten in die Schutzbedarfsklasse „hoch“ oder „sehr hoch“ fallen, ist im Anschluss eine Risikoanalyse nach BSI Standard 200-3 [36] erforderlich.

4.1 Strukturanalyse

Als Grundlage für die Beschreibung der Informationsverbunde werden sowohl die i beschriebene Wertschöpfungskette als auch die Darstellung des Datenflusses in Abbildung 5 herangezogen. Als kleinste Einheit im Informationsverbund werden jene Datengruppen beschrieben, mit denen innerhalb des Anwendungsfalls gearbeitet wird (siehe Tabelle 1).

Tabelle 1: Datenerfassung

Nr.	Komponente	Beschreibung
D1	Verfügbarkeitsdaten	Sie geben Auskunft über die aktuelle Verfügbarkeit eines Verkehrsmittels und ob es einem Nutzer innerhalb einer Reiseroute zur Verfügung steht. Auf Basis der Verfügbarkeitsdaten wird die Route geplant.
D2	Positionsdaten (IoT-Gerät)	Geben Auskunft über den aktuellen Standort des jeweiligen Verkehrsmittels. Diese Information wird zur Planung der Reiserouten benötigt.
D3	Zahlungsdaten	Enthalten personenbezogene Daten sowie die Zahlungsinformationen des Nutzers, welche für die anschließende Abrechnung der in Anspruch genommenen Services notwendig sind.
D4	Login-Daten	Bestehend aus einem Nutzernamen und einem Passwort, verschaffen die Login-Daten dem Nutzer Zugriff zu der Anwendung und auf das Benutzerprofil.
D5	Positionsdaten (Nutzer)	Geben Auskunft über den aktuellen Standort des Nutzers. Diese Information wird zur Planung der Reiserouten benötigt.
D6	Nutzungsdaten	Enthalten Informationen über die ausgewählte Reiseroute, sowie die vom Nutzer in Anspruch genommenen Services innerhalb der Route, wie z.B. genutzte Verkehrsmittel, Dauer der Inanspruchnahme, Abgabeort und entstandene Kosten. Diese Informationen werden sowohl für die anschließende Abrechnung als auch für eine mögliche Reservierung der Verkehrsmittel benötigt.

Die in Tabelle 1 erfassten Daten werden innerhalb des Informationsverbundes von verschiedenen Komponenten generiert, genutzt und/oder verarbeitet.

Tabelle 2 bietet einen Überblick über relevante IoT-Hardware-Komponenten und IT-Anwendungen mit den durch die Komponenten verarbeiteten Daten. Die im Folgenden aufgelisteten Komponenten werden sowohl aus den bisherigen Kenntnissen als auch aus den oben aufgeführten Abbildungen (siehe Abbildung 2, Abbildung 4 und Abbildung 5) abgeleitet. Im Folgenden wird von IoT-Komponenten wie Fahrrad, Auto, Bus, Straßenbahn und Mobiltelefon gesprochen (siehe Tabelle 2 [IoT1-IoT5]). Gemeint sind hier lediglich die im Verkehrsmittel oder im Gerät verbauten IoT-Komponenten. So ist beispielsweise mit „Fahrrad“ nicht

das Verkehrsmittel als solches gemeint, sondern lediglich die im Fahrrad verbaute IoT-Komponente, welche eine Kommunikation und einen Datenaustausch ermöglicht. Gleiches gilt für die weiteren aufgeführten IoT-Komponenten.

Tabelle 2: Strukturanalyse der IoT-Komponenten[3] und IT-Anwendungen

Nr.	Komponente	Verarbeitete Daten
IoT1	Fahrrad	D1, D2, D6
IoT2	Auto	D1, D2, D6
IoT3	Bus	D1, D2
IoT4	Straßenbahn	D1, D2
IoT5	Mobiltelefon	D3, D4, D5
A1	Webanwendung	D1, D2, D3, D4, D5, D6
A2	Smartphone App	D1, D2, D3, D4, D5, D6
A3	Datenbank	D1, D2, D3, D4, D5, D6
A4	Big Data-Analysen	D1, D2, D3, D4, D5, D6

In der nachfolgenden Tabelle 3 werden die relevanten Cloud-Plattformen aufgeführt. Ebenfalls erfasst die Tabelle die durch die Komponenten verarbeiteten Daten. Um Ausfälle durch elementrare Schäden zu vermeiden, werden die Plattformen redundant aufgebaut.

Da die Smart City-Plattform der Kern der Anwendung ist, muss diese jene Daten verarbeiten, die im Rahmen der Wertschöpfung entstehen. Sowohl die Stadtplanungsplattform, als auch die Plattform des Mobilitätsanbieters können die erfassten Daten für interne Prozesse und Anwendungen nutzen und weiterverarbeiten. So können die Daten beispielsweise bei der internen Planung der Verkehrsmittel behilflich sein als auch Echtzeitaktualisierung der Standorte, Verfügbarkeiten und Abfahrtszeiten ermöglichen.

Um den Service im Nachgang verursachungsgerecht abrechnen zu können, benötigen die Dienstleister neben den Zahlungsdaten des Nutzers auch die eigentlichen Nutzungsdaten Ende-zu-Ende über die in Anspruch genommenen Services.

Tabelle 3: Strukturanalyse der Plattform- und Server-Infrastruktur

Nr.	Komponente	Verarbeitete Daten	Ort
S1	Smart City-Plattform	D1, D2, D3, D4, D5, D6	RZ, Standort 1; RZ, Standort 2
S2	Stadtplanungsplattform	D1, D2, D3, D6	RZ, Standort 1; RZ, Standort 2
S3	Plattform des Mobilitätsanbieters	D1, D2, D3, D6	RZ, Standort 1; RZ, Standort 2

[3] Die Komponenten enthalten implementierte Sensorik, sowie eine SIM-Karte über die eine IP-basierte Kommunikation über das Mobilfunknetz ermöglicht wird.

Um eine umfassende Übersicht des Informationsverbundes zu schaffen, werden in der folgenden Tabelle 4 die relevanten Kommunikationskanäle und –beziehungen aufgeführt.

Tabelle 4: Strukturanalyse der Kommunikationsverbindungen

Nr.	Komponente	Daten	Quelle	Ziel
Komm1	WLAN	D1, D2, D3, D4, D5, D6	IoT5, A1, A2, A3	S1
Komm2	Mobilfunk	D1, D2, D3, D4, D5, D6	IoT1, IoT2, IoT3, IoT4, IoT5, A1, A2,	S1, A3, A4
Komm3	Internet, RZ extern	D1, D2, D3, D4, D5, D6	S1, A3, A4	IoT1, IoT2, IoT3, IoT4, IoT5, A1, A2, S2, S3
Komm4	Internet, RZ intern	D1, D2, D3, D4, D6	S1, S2, S3, A3, A4	S1, S2, S3, A3, A4
Komm5	Enterprise Service Bus	-	S1, S2, S3	S1, S2, S3

Konkret lassen sich im Standard-Verfahren [38] Webanwendungen und mobile Anwendungen mit dem Anwendungs-Baustein; Mobiltelefone, allgemeine Smartphones und Tablets mit dem IT-System-Baustein; der WLAN-Betrieb und die –Nutzung, Router und Switches mit dem Netz- und Kommunikations-Baustein und Rechenzentren sowie Serverräume und die IT-Verkabelung mit dem Infrastruktur-Baustein, absichern.

4.2 Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung erfolgt gemäß BSI 200-2 anhand der Datenobjekte. Zur Bewertung werden typische Schadszenarien [35], wie z.B. Verstoß gegen Gesetze/Vorschriften, Beeinträchtigung der Aufgabenerfüllung, monetäre Auswirkungen, etc., zugrunde gelegt.

Unter den oben aufgeführten Daten befinden sich sowohl unsensible als auch sensible Daten. Eine Offenlegung der verschiedenen Daten kann verschiedene Schadensauswirkungen annehmen. Innerhalb des IT-Grundschutzes werden vom BSI daher drei Schutzbedarfskategorien definiert, um so den Schutzbedarf in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit der einzelnen zu schützenden Objekte quantifizieren zu können. Das BSI unterscheidet die Kategorien [35] „normal“, „hoch“ und „sehr hoch“. Eine generische Abgrenzung der einzelnen Schutzbedarfskategorien ist dem BSI 200-2 [35] und der Tabelle 5 zu entnehmen.

Tabelle 5: Kritikalitätsmatrix

Schadensszenarien	Normal	Hoch	Sehr hoch
Personenbezogene Daten kommen abhanden	Preisgabe von personenbezogenen Daten ohne erhöhten Schutzbedarf.	Preisgabe besonders sensibler Daten (z.B. Zahlungsinformationen).	Massenhafte Preisgabe besonders sensibler personenbezogener Daten.

Schadensszenarien	Normal	Hoch	Sehr hoch
Gesundheitliche Schäden durch physische Manipulation der IoT-Komponente	Heilbare Gesundheitsschäden können die Folge einer Manipulation der IoT-Komponente sein.	Dauerhafte gesundheitliche Schäden können die Folge einer Manipulation der IoT-Komponente sein.	Manipulation der IoT-Komponente führt zu schweren, dauerhaften gesundheitlichen Schäden oder gar zum Tod.
Schäden durch fehlerhafte Abrechnung	Geringe materielle/immaterielle Schäden.	Beachtliche materielle/immaterielle Schäden.	Beachtliche materielle/immaterielle Schäden mit ggf. strafrechtlichen Konsequenzen.
Schäden durch fehlerhafte Routen/ verpassten Anschlüssen	Geringe materielle/immaterielle Schäden.	Beachtliche materielle/immaterielle Schäden	Beachtliche materielle/immaterielle Schäden mit ggf. strafrechtlichen Konsequenzen.
Beeinträchtigung der Aufgabenerfüllung	Web- und/oder mobile Anwendung können kurzzeitig nicht vom Kunden genutzt werden.	Web- und/oder mobile Anwendung können mittelfristig nicht vom Kunden genutzt werden.	Web- und/oder mobile Anwendung können längerfristig nicht vom Kunden genutzt werden.
Negative Innen-/Außenwirkung	Geringer Ansehens- und Vertrauensverlust in der Öffentlichkeit und gegenüber dem Kunden.	Breiter Ansehens- und Vertrauensverlust in der Öffentlichkeit und gegenüber dem Kunden.	Landesweiter Ansehens- und Vertrauensverlust mit politischen Konsequenzen.
Finanzielle Auswirkungen	Für das Unternehmen tolerable.	Beachtliche finanzielle Verluste, jedoch noch nicht existenzbedrohend.	Existenzbedrohend.

Es hat sich in der Praxis bewährt, den Schutzbedarf für die IT-Komponenten anhand der von ihnen verwendeten Daten zu bestimmen. Je nachdem, ob Zahlungs-, Login-, Positions-, Nutzungs- oder Verfügbarkeitsdaten verarbeitet werden, muss auch der Schutzbedarf angepasst werden. Der für die Daten festgestellte Schutzbedarf vererbt sich über die IT-Anwendungen bis hin zur Cloud-Plattform. Die Schutzbedarfsfeststellung für die Datenobjekte der multimodalen Mobilität wird in der nachfolgenden Tabelle durchgeführt.

Tabelle 6: Schutzbedarfsfeststellung für die Datenobjekte

Komponente	Schutzziel	Schutzbedarf	Begründung
D1: Verfügbarkeitsdaten	Vertraulichkeit	normal	Es werden keine vertraulichen Daten erzeugt oder gespeichert.
	Integrität	hoch	Fehlende oder manipulierte Verfügbarkeitsdaten werden womöglich nicht oder erst mit Verzögerung erkannt und korrigiert. Dies kann zu fehlerhaften

Komponente	Schutzziel	Schutzbedarf	Begründung
			Reiserouten führen.
	Verfügbarkeit	hoch	Aufgrund eines Ausfalls werden Routen entweder fehlerhaft oder gar nicht geplant.
D2: Positionsdaten (IoT-Gerät)	Vertraulichkeit	normal	Es werden keine vertraulichen Daten erzeugt oder gespeichert.
	Integrität	hoch	Fehlende oder manipulierte Positionsdaten werden womöglich nicht oder erst mit Verzögerung erkannt und korrigiert. Dies kann zu fehlerhaften Reiserouten führen.
	Verfügbarkeit	hoch	Aufgrund eines Ausfalls werden Routen entweder fehlerhaft oder gar nicht geplant.
D3: Zahlungsdaten	Vertraulichkeit	hoch	Die Zahlungsdaten des Nutzers sind streng vertraulich und enthalten personenbezogene Daten.
	Integrität	normal	Ein Fehlen der Zahlungsdaten kann schnell erkannt und vom Nutzer selber behoben werden.
	Verfügbarkeit	hoch	Die Verfügbarkeit der Zahlungsdaten ist notwendig für die Inanspruchnahme von kostenpflichtigen Services innerhalb einer Reiseroute und Grundlage für die anschließende Abrechnung.
D4: Login-Daten	Vertraulichkeit	hoch	Die Login-Daten können demjenigen der sie kennt Zugang zu dem System und demnach auch zu den personenbezogenen Daten des Nutzers verschaffen.
	Integrität	normal	Ein Fehlen der Login-Daten kann schnell erkannt und vom Nutzer selber behoben werden.
	Verfügbarkeit	hoch	Die Verfügbarkeit der Login-Daten ist Grundlage für die Funktionsfähigkeit der -/Web-Anwendung. Sollten die Login-Daten nicht verfügbar sein, kann der Nutzer sowohl die Web- als auch die Smartphone-Anwendung nicht nutzen und es können keine Routen geplant werden.

Komponente	Schutzziel	Schutzbedarf	Begründung
D5: Positionsdaten (Nutzer)	Vertraulichkeit	hoch	Positionsdaten enthalten personenbezogene Daten und geben Aufschluss über den Aufenthaltsort des Nutzers.
	Integrität	normal	Fehlerhafte Positionsdaten werden erkannt und nachträglich korrigiert.
	Verfügbarkeit	hoch	Die Verfügbarkeit der Positionsdaten ist die Grundlage für die Funktionsfähigkeit der Routenplanung.
D6: Nutzungsdaten	Vertraulichkeit	hoch	Nutzungsdaten enthalten Informationen über den genauen Verlauf der Reiseroute des Nutzers, sowie ausgewählte/genutzte Verkehrsmittel. Ebenfalls geben sie Aufschluss über den Abfahrtsort, mögliche Umsteigepunkte sowie das Ziel des Nutzers.
	Integrität	hoch	Fehlerhafte Nutzungsdaten werden von den Dienstleistern nicht erkannt und führen zu fehlerhaften Reservierungen und Abrechnungen.
	Verfügbarkeit	hoch	Die Verfügbarkeit der Nutzungsdaten ist die Grundlage für das Reservieren von dem jeweiligen Verkehrsmittel. Ebenfalls sind sie Basis der von den Dienstleistern durchzuführenden Abrechnungen.

Da der Schutzbedarf der IT-Anwendungen durch das Vererbungsprinzip vom jeweiligen Schutzbedarf der verarbeiten Daten abhängt wird zur Bestimmung die in Kapitel 6.3 beschriebene Strukturanalyse herangezogen.

Tabelle 7: Schutzbedarfsfeststellung für IT-Anwendungen

Komponente	Schutzziel	Schutzbedarf	Begründung
A1: Webanwendung	Vertraulichkeit	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf auf die Webanwendung.
	Integrität	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf auf die Webanwendung.
	Verfügbarkeit	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf auf die Webanwendung.
A2:	Vertraulichkeit	hoch	Die Datenobjekte D1, D2, D3, D4, D5

Komponente	Schutzziel	Schutzbedarf	Begründung
Smartphone-App			und D6 vererben deren Schutzbedarf auf die Smartphone-App.
	Integrität	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf auf die Smartphone-App.
	Verfügbarkeit	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf auf die Smartphone-App.
A3: Datenbank	Vertraulichkeit	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf auf die Datenbank.
	Integrität	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf auf die Datenbank.
	Verfügbarkeit	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf auf die Datenbank.
A4: Big Data-Tools	Vertraulichkeit	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf auf die Big Data-Tools.
	Integrität	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf auf die Big Data-Tools.
	Verfügbarkeit	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf auf die Big Data-Tools.

Tabelle 8: Schutzbedarfsfeststellung für die IoT-Komponenten

Komponente	Schutzziel	Schutzbedarf	Begründung
IoT1: Fahrrad	Vertraulichkeit	normal	Die Datenobjekte D1, D2 und D6 vererben deren Schutzbedarf auf die IoT-Komponente.
	Integrität	hoch	Die Datenobjekte D1, D2 und D6 vererben deren Schutzbedarf auf die IoT-Komponente.
	Verfügbarkeit	hoch	Die Datenobjekte D1, D2 und D6 vererben deren Schutzbedarf auf die IoT-Komponente.
IoT2: Auto	Vertraulichkeit	normal	Die Datenobjekte D1, D2 und D6 vererben deren Schutzbedarf auf die IoT-Komponente.

Komponente	Schutzziel	Schutzbedarf	Begründung
	Integrität	hoch	Die Datenobjekte D1, D2 und D6 vererben deren Schutzbedarf auf die IoT-Komponente.
	Verfügbarkeit	hoch	Die Datenobjekte D1, D2 und D6 vererben deren Schutzbedarf auf die IoT-Komponente.
IoT3: Bus	Vertraulichkeit	normal	Die Datenobjekte D1 und D2 vererben deren Schutzbedarf auf die IoT-Komponente.
	Integrität	hoch	Die Datenobjekte D1 und D2 vererben deren Schutzbedarf auf die IoT-Komponente.
	Verfügbarkeit	hoch	Die Datenobjekte D1 und D2 vererben deren Schutzbedarf auf die IoT-Komponente.
IoT4: Straßenbahn	Vertraulichkeit	normal	Die Datenobjekte D1 und D2 vererben deren Schutzbedarf auf die IoT-Komponente.
	Integrität	hoch	Die Datenobjekte D1 und D2 vererben deren Schutzbedarf auf die IoT-Komponente.
	Verfügbarkeit	hoch	Die Datenobjekte D1 und D2 vererben deren Schutzbedarf auf die IoT-Komponente.
IoT5: Mobiltelefon	Vertraulichkeit	hoch	Die Datenobjekte D3, D4 und D5 vererben deren Schutzbedarf auf die IoT-Komponente.
	Integrität	hoch	Die Datenobjekte D3, D4 und D5 vererben deren Schutzbedarf auf die IoT-Komponente.
	Verfügbarkeit	hoch	Die Datenobjekte D3, D4 und D5 vererben deren Schutzbedarf auf die IoT-Komponente.

Tabelle 9: Schutzbedarfsfeststellung für die Plattformen

Komponente	Schutzziel	Schutzbedarf	Begründung
S1: Smart City-Plattform	Vertraulichkeit	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf an die Plattform.
	Integrität	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6 vererben deren Schutzbedarf

Komponente	Schutzziel	Schutzbedarf	Begründung
			an die Plattform.
	Verfügbarkeit	hoch	Die Datenobjekte D1, D2, D3, D4, D5 und D6vererben deren Schutzbedarf an die Plattform.
S2: Stadtplanungs-plattform	Vertraulichkeit	hoch	Die Datenobjekte D1, D2, D3 und D6 vererben deren Schutzbedarf an die Plattform.
	Integrität	hoch	Die Datenobjekte D1, D2, D3 und D6 vererben deren Schutzbedarf an die Plattform.
	Verfügbarkeit	hoch	Die Datenobjekte D1, D2, D3 und D6 vererben deren Schutzbedarf an die Plattform.
S3: Mobilitäts-Anbieter	Vertraulichkeit	hoch	Die Datenobjekte D1, D2, D3 und D6 vererben deren Schutzbedarf an die Plattform.
	Integrität	hoch	Die Datenobjekte D1, D2, D3 und D6 vererben deren Schutzbedarf an die Plattform.
	Verfügbarkeit	hoch	Die Datenobjekte D1, D2, D3 und D6 vererben deren Schutzbedarf an die Plattform.

Da die Daten über Kommunikationsverbindungen übertragen werden, müssen hierfür ebenfalls die Schutzbedarfe festgestellt werden. Um nun die Entscheidung vorzubereiten, auf welchen Kommunikationsstrecken kryptografische Sicherheitsmaßnahmen umgesetzt werden sollen und über welche Verbindungen Angriffe zu erwarten sind, müssen die einzelnen Kommunikationsverbindungen analysiert werden. Dabei werden Verbindungen als kritisch angesehen, die eine Außenverbindung haben, schutzbedürftige Informationen/Daten übertragen und/oder die im produzierenden Bereich eingesetzt werden [35]. Die Kritikalität der Kommunikationsverbindungen wird erfasst, indem zunächst sämtliche „Außenverbindungen" als kritische Verbindungen identifiziert werden. Danach wird die Kritikalität der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit festgelegt. Diese orientiert sich an den zu übertragenden Datenobjekten (siehe Tabelle 1). In der nachfolgenden Tabelle wird die Kritikalität der Kommunikationsverbindungen aufgezeigt.

Tabelle 10: Kritikalität der Kommunikationsverbindungen

Nr.	Außenverbindung	Vertraulichkeit	Integrität	Verfügbarkeit
Komm1: WLAN	X	hoch	hoch	hoch
Komm2:	X	hoch	hoch	hoch

Mobilfunk				
Komm3: **Internet,** **RZ extern**	X	hoch	hoch	hoch
Komm4: **Internet,** **RZ intern**	-	hoch	hoch	hoch
Komm5: **Enterprise Service Bus**	-	hoch	hoch	hoch

Aufgrund dessen, dass innerhalb des Anwendungsfalls mit sensiblen und schützenswerten Daten gearbeitet wird, müssen jegliche Komponenten des Informationsverbundes umfassend abgesichert werden. Wie Eingangs am Beispiel des vernetzten Aquariums beschrieben, können Lücken und Schwachstellen innerhalb einer IoT-Anwendung von Angreifern dazu genutzt werden, um sich Zugang zum eigentlichen System und somit zu den schützenswerten Daten zu verschaffen. Demnach muss ein umfassendes Sicherheitskonzept alle relevanten und oben in der Strukturanalyse aufgeführten Komponenten hochgradig absichern, um das Risiko von potentiellen Lücken und Schwachstellen zu vermeiden.

4.3 Risikoanalyse

Auf Basis der identifizierten Bestandteile des Anwendungsfalls wird eine Risikoanalyse durchgeführt. Die Risikoanalyse folgt dabei dem im BSI Standard 200-3 [36] beschriebenen Vorgehen.

Dabei basiert die Risikoanalyse u.a. auch auf dem IT-Grundschutz-Kompendium [38]. Innerhalb des Kompendiums werden bereits elementare Gefährdungen beschrieben. Ebenfalls werden auf Basis der Gefährdungen notwendige Bausteine definiert, mit denen die Gefährdungen eingedämmt und die zu sichernden Komponenten geschützt werden können. Da die elementaren Gefährdungen und notwendigen Bausteine (Basis-Anforderungen) bereits im IT-Grundschutz-Kompendium ausführlich beschrieben werden, werden diese hier nicht weiter betrachtet und berücksichtigt. Folgende elementare Gefährdungen werden innerhalb dieser Risikoanalyse daher nicht betrachtet:

Tabelle 11: Bereits im IT-Grundschutz-Kompendium betrachtete elementare Gefährdungen [38]

Elementare Gefährdungen	
G0.01 Feuer	G0.03 Wasser
G0.04 Verschmutzung, Staub, Korrosion	G0.05 Naturkatastrophen
G0.06 Katastrophen im Umfeld	G0.07 Großereignisse im Umfeld
G0.08 Ausfall oder Störung der Stromversorgung	G0.09 Ausfall oder Störung von Kommunikationsnetzen

Elementare Gefährdungen	
G0.11 Ausfall oder Störung von Dienstleistern	G0.14 Ausspähen von Informationen
G0.15 Abhören	G0.19 Offenlegung schützenswerter Informationen
G0.21 Manipulation von Hard- oder Software	G0.22 Manipulation von Informationen
G0.23 Unbefugtes Eindringen in IT-Systeme	G0.26 Fehlfunktion von Geräten oder Systemen
G0.28 Software-Schwachstellen oder -Fehler	G0.29 Verstoß gegen Gesetze oder Regelungen
G0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	G0.31 Missbrauch von Berechtigungen
G0.38 Missbrauch personenbezogener Daten	G0.39 Schadprogramme
G0.40 Verhinderung von Diensten (Denial-of-Service)	G0.41 Sabotage
G0.42 Social Engineering	G0.45 Datenverlust
G0.46 Integritätsverlust schützenswerter Informationen	

Der Fokus der Risikoanalyse liegt auf den anwendungsfallspezifischen Risiken, die vom BSI in dem Umfang (noch) nicht abgedeckt werden. Daher werden im Rahmen dieser Analyse lediglich jene Gefährdungen erfasst und beschrieben, die über die elementaren Gefährdungen des IT-Grundschutz-Kompendiums hinausgehen und die sich aus dem spezifischen Anwendungsfall „multimodale Mobilität“ ergeben.

Die folgende Risikoanalyse in Form von Interviews im Workshop-Charakter mit zwei Partnern der Detecon International GmbH durchgeführt und erstellt. Beide Partner sind Experten und Treiber der Themen IoT, Smart City und Connected Car. Ebenfalls haben sie durch ihre langjährige Berufserfahrung ein breites Wissen im Bereich Netzwerk und Plattformsicherheit, weswegen ein Austausch über potentielle Risiken im beschriebenen Anwendungsfall im Rahmen einer Risikoanalyse Sinn ergibt.

Innerhalb dieser Sessions wurden zusätzliche Gefährdungen (siehe Tabelle 12 und Tabelle 13) identifiziert, sowie mögliche Schadensszenarien beschrieben. Unter Verwendung der Brainstorming-Ergebnisse wurde eine Risikoeinschätzung nach BSI 200-3 [36] (siehe Tabelle 14) vorgenommen.

Folgende zusätzliche Gefährdungen wurden für den gesamten Informationsverbund identifiziert:

Tabelle 12: Zusätzliche Gefährdungen im Informationsverbund der multimodalen Mobilität

Gesamter Informationsverbund	
Nr.	**Beschreibung**
G z.1 **Abfangen der Daten entlang der Wertschöpfungskette**	Angreifer haben die Möglichkeit, aufgrund von mangelnden Sicherheitsmaßnahmen im IoT die Daten (Fokus speziell auf D3, D4, D5 und D6) an den Schnittstellen abzugreifen. Ein mögliches Angriffsszenarium wäre hier der Man-in-the-Middle-Angriff. Das BSI beschreibt mit „G0.14 Ausspähen von Informationen“ den genannten Punkt, geht aber innerhalb der Bausteine zur Lösung der elementaren Gefährdung nicht auf den Sonderfall IoT ein. Dieser muss daher explizit in der zu entwickelnden Lösung beschrieben werden.
G z.2 **Abhören/Lesen der Daten entlang der Wertschöpfungskette**	Angreifer haben die Möglichkeit aufgrund von mangelnden Sicherheitsmaßnahmen im IoT die Daten unbemerkt mit zu hören oder zu lesen. Durch das Abhören der Daten erlangt der Angreifer Wissen über, z.B. präferierte Routen (D5 und D6), genutzte Verkehrsmittel (D1, D2, D5 und D6), Hauptreisezeit und Zahlungsinformationen (D3, D4 und D6) des Nutzers und kann so, auf Basis dessen, s.g. social hacking durchführen. Wenn der Angreifer nun auch in der Lage ist, die Daten nach G z.3 und G0.2 zu manipulieren, kann er die Route anpassen und/oder das ausgewählte Verkehrsmittel, nach G z.4, manipulieren. Das BSI beschreibt mit „G0.15 Abhören“ den genannten Punkt, geht aber innerhalb der Bausteine zur Lösung der elementaren Gefährdung nicht auf den Sonderfall IoT ein. Dieser muss daher explizit in der zu entwickelnden Lösung beschrieben werden.
G z.3 **Manipulieren der Daten innerhalb der Wertschöpfungskette**	Angreifer haben die Möglichkeit aufgrund von mangelnden Sicherheitsmaßnahmen im IoT die Daten innerhalb der Wertschöpfungskette unbemerkt zu manipulieren. Das BSI beschreibt mit „G0.22 Manipulation von Informationen“ den genannten Punkt, geht aber innerhalb der Bausteine zur Lösung der elementaren Gefährdung nicht auf den Sonderfall IoT ein. Dieser muss daher explizit in der zu entwickelnden Lösung beschrieben werden.

Neben den Gefährdungen im Informationsverbund wurden noch weitere Gefährdungen im Bereich „IoT-Komponenten“ identifiziert. Diese werden in der Tabelle 13 aufgeführt und beschrieben.

Tabelle 13: Zusätzliche Gefährdungen für IoT-Komponente der multimodalen Mobilität

IoT-Komponenten	
Nr.	**Beschreibung**
G z.4 **Unbefugte Übernahme der IoT-Komponente**	Angreifer haben die Möglichkeit aufgrund von mangelnden Sicherheitsmaßnahmen im IoT die IoT-Komponente zu übernehmen und sich so Zugang zum dahinter befindlichen IT-System zu

IoT-Komponenten	
Nr.	**Beschreibung**
	verschaffen (Beispiel des vernetzten Aquariums aus der Einleitung). Das BSI beschreibt mit „G0.23 Unbefugtes Eindringen in IT-Systeme“ den genannten Punkt, geht aber innerhalb der Bausteine zur Lösung der elementaren Gefährdung nicht auf den Sonderfall IoT ein. Dieser muss daher explizit in der zu entwickelnden Lösung beschrieben werden.
G z.5 **Manipulation der IoT-Komponente**	Angreifer haben die Möglichkeit aufgrund von mangelnden Sicherheitsmaßnahmen im IoT die IoT-Komponente nach einer erfolgreichen Übernahme zu manipulieren/sabotieren. Die Sabotage kann sowohl durch einen physischen Zugriff (z.B. ist dem Angreifer bekannt wo sich die IoT-Komponente befindet, da er zuvor die Daten abgefangen hat) als auch durch einen Zugriff über den jeweiligen Kommunikationskanal erfolgen. Durch eine Sabotage der Komponente kann nicht mehr gewährleistet werden, dass die Komponente und das System einwandfrei funktionieren. Ebenfalls kann das leibliche Wohl des Nutzers durch fehlerhafte Fahrzeugfunktionen gefährdet werden. Das BSI beschreibt mit „G0.22 Manipulation von Informationen“ und „G0.23 Unbefugtes Eindringen in IT-Systeme“ den genannten Punkt nur teilweise und geht nicht auf den Sonderfall IoT ein. Dieser muss daher explizit in der zu entwickelnden Lösung beschrieben werden.
G z.6 **Sichtbarkeit der IoT-Komponente nach außen/extern**	Sofern die IoT-Komponente eine SIM-Karte besitzt, bekommt sie automatisch eine private IP-Adresse die erst durch den APN in eine öffentlich sichtbare IP-Adresse konvertiert wird. Demnach ist eine IoT-Komponente mit SIM-Karte (GSM-Komponente) nicht nach außen sichtbar. Sollte eine IoT-Komponente jedoch eine public IP-Adresse besitzen, ist diese nach außen sichtbar und kann über das Internet und die öffentliche IP-Adresse angepingt werden. Pingt ein Angreifer die IoT-Komponente an und der ping war erfolgreich, weiß er, dass die IP-Adresse gültig ist. Die Komponente ist somit aus dem Internet sichtbar und von außen durch den Ping ansprechbar. Diese Gefährdung wird vom BSI nicht behandelt und muss daher explizit in der zu entwickelnden Lösung beschrieben werden. Da sich innerhalb des Anwendungsfalls „multimodale Mobilität“ lediglich IoT-Geräte mit SIM-Karte im Einsatz befinden, wird dieses Risiko nicht weiter betrachtet und in den Ausblick gestellt.

Nachdem alle zusätzlichen Gefährdungen identifiziert worden sind, wird im nächsten Schritt der Risikoanalyse das eigentliche Risiko, was von der jeweiligen Gefährdung ausgeht, ermittelt. Dabei hängt die Höhe des Risikos sowohl von der Eintrittshäufigkeit der Gefährdung als auch von der Höhe des Schadens ab, die die Gefährdung mit sich bringt. Daher müssen bei einer Risikoeinschätzung beide Größen berücksichtigt werden. Um die Risiken einschätzen zu

können, lassen sich in Anlehnung an den IT-Grundschutz [36] folgende Kategorien unterscheiden:

- **Potenzielle Schadenshöhe:** normal, hoch, sehr hoch (siehe Tabelle 5)
- **Eintrittshäufigkeit:**
    - Begrenzt: Angreifer muss beispielsweise ein WLAN-Signal abfangen oder physische Manipulation durchführen.
    - Mittel: Angreifer muss von „innen“ kommen, da die Komponenten von „außen“ nicht sichtbar sind.
    - Sehr hoch: Komponente ist aus dem Internet sichtbar bzw. die Kommunikation läuft über öffentliche Kanäle.

Eine detaillierte Beschreibung kann dem Standard BSI 200-3 [36] entnommen werden. Anhand der beschriebenen Kategorien können sowohl Eintrittshäufigkeit als auch Schadenshöhe der zuvor identifizierten Gefährdungen bestimmt werden (siehe Tabelle 14).

Tabelle 14: Risikoeinschätzung der identifizierten Gefährdungen

Gefährdung	Kategorie	Risikoeinschätzung	Begründung
G z.1 **Abfangen der Daten**	Eintrittshäufigkeit	sehr hoch	Komponenten sind teilweise aus dem Internet sichtbar und die Kommunikation läuft über öffentliche Netze. Sobald eine Schwachstelle bekannt wird, können Angriffe durchgeführt werden, sofern der Angreifer einen Exploit herunterladen, sowie einen Portscanner bedienen kann.
	Schadenshöhe	hoch	Der Angreifer kann durch das Abfangen der Daten in den Besitz von schützenswerten Informationen wie z.B. personenbezogen Daten kommen. Dadurch werden Vorschriften und Gesetze verletzt, wodurch es zu Sanktionen gegen die beteiligten Unternehmen kommen kann. Gleichfalls wird das informationelle Selbstbestimmungsrecht des Nutzers beeinträchtigt und aufgrund des Datendiebstahls verlieren die Nutzer gegenüber den beteiligten Unternehmen das Vertrauen, was letztendlich Umsatzeinbußen mit sich ziehen kann.
G z.2 **Abhören/Lesen der Daten**	Eintrittshäufigkeit	sehr hoch	Komponenten sind teilweise aus dem Internet sichtbar und die Kommunikation läuft über öffentliche Netze. Sobald eine Schwachstelle bekannt wird, können Angriffe durchgeführt werden, sofern der Angreifer einen Exploit herunterladen, sowie einen Portscanner bedienen kann.
	Schadenshöhe	hoch	Durch das Abhören/Lesen der Daten kann der Angreifer Wissen über vorherige Transaktionen des Nutzers bekommen, um so ‚social

Gefährdung	Kategorie	Risikoeinschätzung	Begründung
			hacking‘ durchzuführen. Auch hierbei können Vorschriften und Gesetze verletzt werden und den beteiligten Unternehmen Sanktionen drohen. Ebenso wird das informationelle Selbstbestimmungsrecht des Nutzers beeinträchtigt, indem personenbezogene Daten offenbart werden. Durch einen solchen Zwischenfall können die beteiligten Unternehmen gegenüber den Nutzern an Vertrauen verlieren, was letztendlich Umsatzeinbußen mit sich ziehen kann.
G z.3 Manipulieren der Daten	Eintrittshäufigkeit	sehr hoch	Komponenten sind teilweise aus dem Internet sichtbar und die Kommunikation läuft über öffentliche Netze. Sobald eine Schwachstelle bekannt wird, können Angriffe durchgeführt werden, sofern der Angreifer einen Exploit herunterladen, sowie einen Portscanner bedienen kann.
	Schadenshöhe	hoch	Durch das Manipulieren der Daten kann der Angreifer Transaktionen des Nutzers manipulieren. So können beispielsweise Routen verändert und gezielt Fahrzeuge manipuliert werden. Durch einen solchen Vorfall können Vorschriften und Gesetze verletzt werden, wodurch den beteiligten Unternehmen Sanktionen drohen. Durch einen solchen Zwischenfall können die beteiligten Unternehmen gegenüber den Nutzern an Vertrauen verlieren, was letztendlich Umsatzeinbußen mit sich ziehen kann.
G z.4 Unbefugte Übernahme der IoT-Komponente	Eintrittshäufigkeit	mittel	Angreifer muss von „innen“ kommen, da die Komponenten von außen (Internet o.ä.) nicht sichtbar sind. Dies gilt beispielsweise für die GSM-Komponenten (IoT-Geräte mit einer SIM-Karte).
	Schadenshöhe	hoch	Angreifer können sich Zugang zu den IT-Systemen verschaffen, indem sie die IoT-Komponente übernehmen. Dabei können Angreifer, wie bereits am Beispiel des vernetzten Aquariums in der Einleitung beschrieben, u.U. Datenbanken einsehen und auslesen. So können Unbefugte an den personenbezogenen Daten der Nutzer kommen, wodurch Gesetzte und/oder Vorschriften verletzt werden, wodurch den Unternehmen erhebliche Imageschäden und/oder finanzielle Sanktionen drohen. Gleichzeitig verlieren die Nutzer das

Gefährdung	Kategorie	Risikoeinschätzung	Begründung
			Vertrauen in die Unternehmen, was zu Umsatzeinbußen führen kann.
G z.5 **Manipulation IoT-Komponente**	Eintrittshäufigkeit	mittel	Angreifer braucht u.U. physischen Zugriff, um die Komponente direkt manipulieren/sabotieren zu können, z.B. Fahrtüchtigkeit der Verkehrsmittel durch Schäden beeinträchtigen. – Eintrittswahrscheinlichkeit begrenzt. Die Funktionalität der Komponente kann allerdings auch durch das Manipulieren/Sabotage der SW eingeschränkt werden. Der Angreifer muss hierfür jedoch von „innen“ kommen, um eine SW-Manipulation durchführen zu können, da die IoT-Geräte (Komponente mit SIM-Karte) von außen (Internet o.ä.) nicht sichtbar sind. – Eintrittswahrscheinlichkeit mittel. Um hier den schlimmsten Fall abzudecken, wird die Eintrittswahrscheinlichkeit auf mittel gesetzt.
	Schadenshöhe	hoch	Durch eine Sabotage der IoT-Komponente kann deren einwandfreie Funktionalität nicht mehr sichergestellt werden. So kann beispielsweise die Funktionalität eines Fahrzeuges dahingehend manipuliert werden, dass das leibliche Wohl des Nutzers gefährdet wird. Sollte das leibliche Wohl gefährdet werden, drohen den Beteiligten erhebliche Sanktionen und Imageschäden. Möglicherweise verliert der Nutzer das Vertrauen in die Unternehmen, was sich auf die Umsatzerlöse auswirken kann.

Auf Basis der definierten Kategorien für die potenzielle Schadenshöhe sowie der beschriebenen Klassifikation für die Eintrittshäufigkeit der Gefährdungen schlägt das BSI eine Risikomatrix vor, welche individuell angepasst werden muss. In diesem Fall wurde eine symmetrische Risikomatrix gewählt, um anhand dieser Matrix die vorher eingeschätzten Risiken einzuordnen und zu bewerten (siehe Abbildung 6). Die Einordnung der Gefährdungen erfolgt anhand der in Tabelle 14 vorgenommenen Risikoeinschätzung.

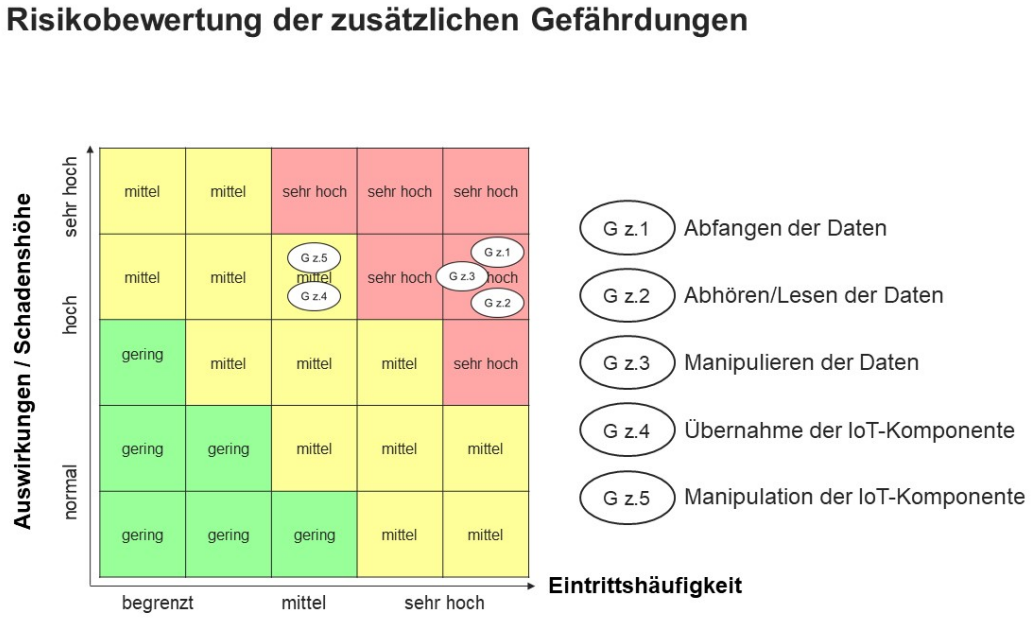

Abbildung 5: Risikomatrix der zusätzlich identifizierten Gefährdungen

5 Risikobehandlung

Im Rahmen der Risikoanalyse sind innerhalb des Anwendungsfalls Gefährdungen identifiziert worden, welche aktuell mit den Bausteinen des BSI nicht eingedämmt und/oder verhindert werden können. Die identifizierten und analysierten Risiken lassen sich in der Risikomatrix als „mittleres“ oder „sehr hohes“ Risiko einordnen, weswegen die Entwicklung von Behandlungsmaßnahmen zur Risikoeindämmung notwendig ist.

5.1 Identifikation von Handlungsbedarfen

Eine umfassende Datensicherheit kann nur dann erreicht werden, wenn die notwendigen Sicherheitsmaßnahmen von allen Stakeholdern um- und eingesetzt werden. Die einzelnen Komponenten sowie relevante E2E-Beziehungen wurden dafür sowohl aus der Abbildung 4 und Abbildung 5 als auch aus der Strukturanalyse (siehe Kapitel 5.1) entnommen.

Innerhalb der multimodalen Mobilität ergeben sich somit E2E-Beziehungen, die abgesichert werden müssen, um die vollständige E2E-Datensicherheit der multimodalen Mobilität gewährleisten zu können. Die Abbildung 7, Abbildung 8 und Abbildung 9 illustrieren die identifizierten E2E-Beziehungen und stellen dar, wo bereits existierende Maßnahmen für eine ausreichende Absicherung des Anwendungsfalls „multimodale Mobilität“ bestehen und wo noch Handlungsbedarf besteht.

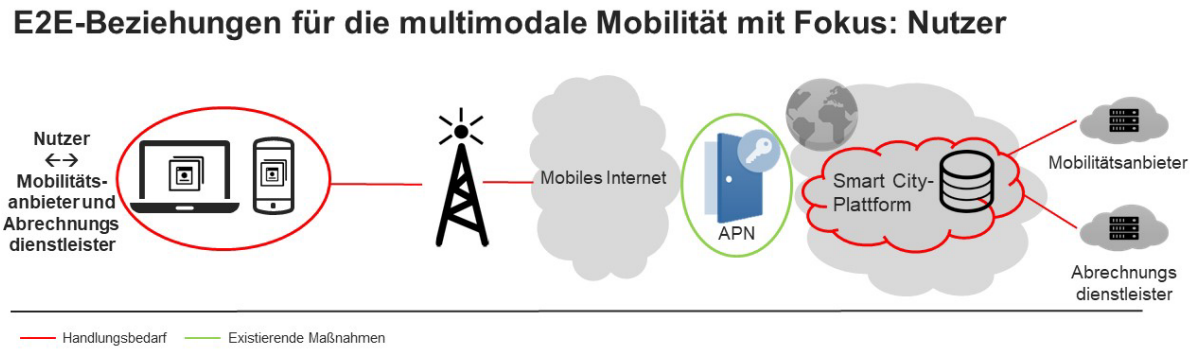

Abbildung 6: Abzusichernde E2E-Beziehungen mit Fokus auf den Nutzer

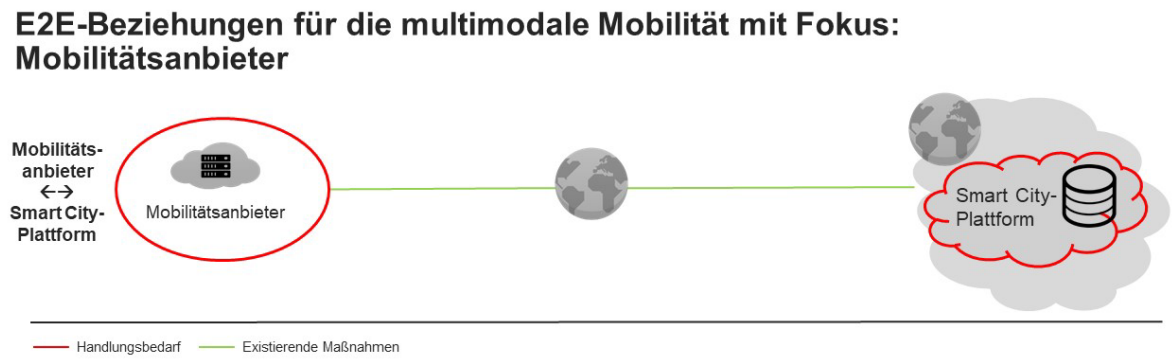

Abbildung 7: Abzusichernde E2E-Beziehungen mit Fokus auf die Mobilitätsanbieter

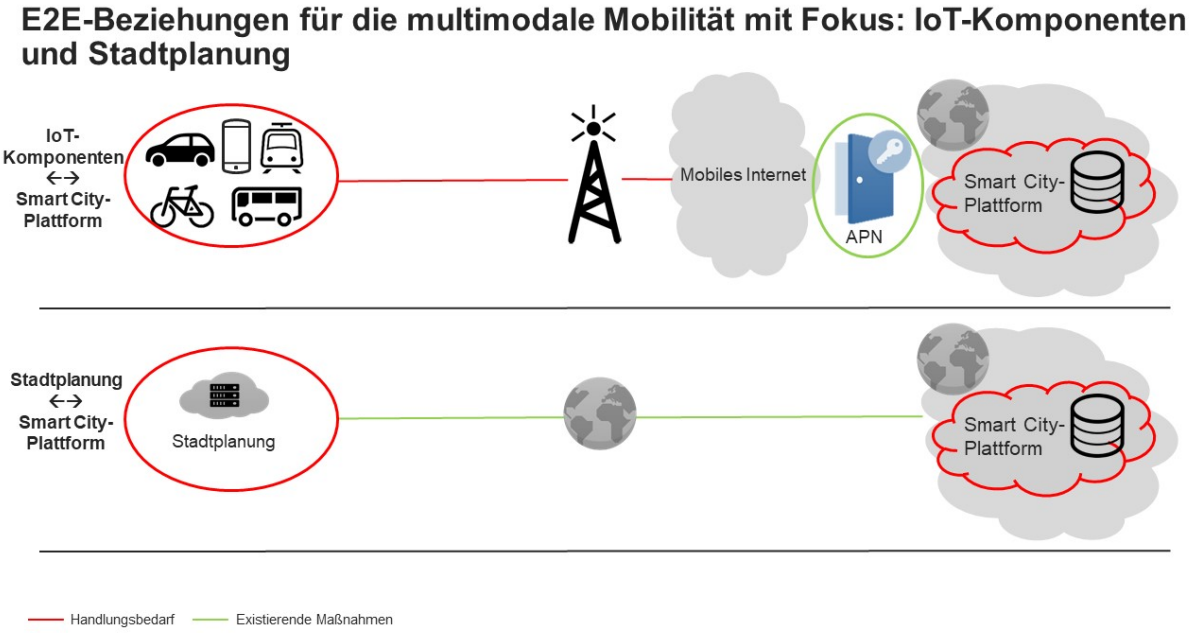

Abbildung 8: Abzusichernde E2E-Beziehungen mit Fokus auf IoT-Komponenten und Stadtplanung

Bei der Betrachtung der Abbildungen fällt auf, dass lediglich der APN eine existierende Maßnahme für Sicherheit im Anwendungsfall darstellt. Auch innerhalb der Internetverbindung von externen Plattformen zur Smart City-Plattform existieren bereits Maßnahmen zur Sicherstellung von Datensicherheit, allerdings stellen diese isolierten Maßnahmen noch keine ausreichende Sicherheit dar. Es wurden daher Handlungsbedarfe identifiziert, die für eine Erhöhung der Datensicherheit betrachtet und angegangen werden müssen.

Dabei wurden folgende Handlungsbedarfe identifiziert:

- **IoT-Komponente:** Die IoT-Komponente ist dem Angreifer frei zugänglich, wodurch physische Manipulation/Sabotage ermöglicht wird. Der Anwendungsfall benötigt akkurate Daten, um möglichst zuverlässig Routen zu planen oder Abrechnungen zu tätigen. Daher muss eine Manipulation der Daten vermieden werden. Außerdem implementieren IoT-Komponenten unzureichende Authentifizierung, unzureichend starke Benutzernamen und Passwörter und keine bzw. keine starken rollenbasierten Zugriffsrechte.
- **Mobilfunk:** Die Daten sind zwar innerhalb des Mobilfunknetzes mit einem Mobilfunk-Verschlüsselungsverfahren verschlüsselt. Allerdings sind die Verschlüsselungsverfahren des GSM- und UMTS-Netzes bereits entschlüsselt, weswegen lediglich der aktuelle LTE-Verschlüsselungsalgorithmus einen Schutz gegen das unerlaubte Lesen

und Abhören von Daten bietet. Die Verfügbarkeit von LTE ist nicht immer gegeben, wodurch in dem Falle auf andere Übertragungsstandards, wie z.B. GSM oder UMTS zurückgegriffen werden muss. Dadurch kann die Datensicherheit nicht mehr sichergestellt werden. Außerdem wird der LTE-Standard zukünftig durch 5G überholt. Ebenfalls sollte das Ziel eines E2E-Sicherheitskonzeptes sein, sich auf einen einzelnen Verschlüsselungsstandard zu konzentrieren, statt mehrere Verschlüsselungsverfahren zu implementieren. Auch durch den Wechsel in verschiedene Netze, kann eine E2E-Datensicherheit nicht gewährleistet werden. Gleichwohl kann durch die unterschiedlichen Übertragungsstandards, wie GSM, UMTS und LTE, keine kontinuierliche E2E-Datensicherheit sichergestellt werden.

- **Smart City-Plattform:** Die empfangenen Daten unterliegen der allgemeinen Übertragungssicherheit lediglich bis zur Schnittstelle der Plattform. Es existiert keine durchgängige Verschlüsselung der Daten beispielsweise zu einer verschlüsselten Datenbank. Ebenfalls kann nicht sichergestellt werden, dass die Daten vorab nicht verändert oder von einem nicht autorisierten Gerät gesendet wurden.

5.2 Analyse bestehender Verfahren

Innerhalb des Anwendungsfalls kommen lediglich GSM-Komponenten zum Einsatz. Diese bekommen, unter der Annahme, dass hierbei Mobilfunkverträge abgeschlossen wurden, ausschließlich eine private IP-Adresse zugewiesen. Das hat zum Vorteil, dass die IoT-Komponenten erst einmal nicht aus dem öffentlichen Internet sichtbar und erreichbar sind. Die private IP-Adresse wird erst am APN, welches die Schnittstelle aus dem mobilen Internet zum öffentlichen Internet darstellt, in eine öffentlich sichtbare IP-Adresse geändert. Anschließend wird die Kommunikation durch das öffentliche Internet zu der Smart City-Plattform geroutet.

Während der Mobilfunkverbindung sind Man-in-the-Middle-Angriffe möglich, indem eine kompromittierte Basisstation in die Kommunikation eingebracht wird. Der Angreifer ist dann in der Lage, die gesendeten Daten abzufangen und abzuhören.

5.3 E2E-Sicherheit mit TLS-Verschlüsselung

Einen Ausweg aus dem geschilderten Problem bietet der Einsatz des Internet Protokolls Version 6 (IPv6). Innerhalb des IPv6 wird generell ein Mesh-Netzwerk aufgebaut, in welchem die Daten mittels IPsec-Verschlüsselung übertragen werden. Dabei können ebenfalls private IP-Adressen verteilt werden, wodurch das Gerät selber aus dem öffentlichen Internet nicht sichtbar ist. Allerdings ist IPv6 nicht abwärts mit IPv4 kompatibel und nicht überall verfügbar oder in Gebrauch. In der Praxis würde der Einsatz von IPv6 auf einen teuren und fehleranfälligen Parallelbetrieb von IPv4- und IPv6-Komponenten hinauslaufen.

Es muss demnach eine Maßnahme oder eine Technologie gewählt werden, die Datensicherheit in einem bereits bestehenden (IoT-)Netzwerk realisieren kann sowie Standard unabhängig und performant ist. Eine solche Technologie wird mit TLS-Verschlüsselung bereitgestellt. Dieses Verschlüsselungsverfahren stellt die Grundlage einer E2E-Absicherung dar. Eine TLS-Verschlüsselung ist lediglich eine Standard-Internetverschlüsselung (z.B. HTTPS) und wird bereits im Rahmen von beispielsweise Online-Banking genutzt. Durch TLS würde selbst nach einem Bruch der LTE-Verschlüsselung oder bei einem Man-in-the-Middle-Angriff die Datensicherheit sichergestellt. Die nachfolgenden Abbildungen zeigen die einzelnen E2E-Sicherheitsmaßnahmen für die identifizierten Beziehungen.

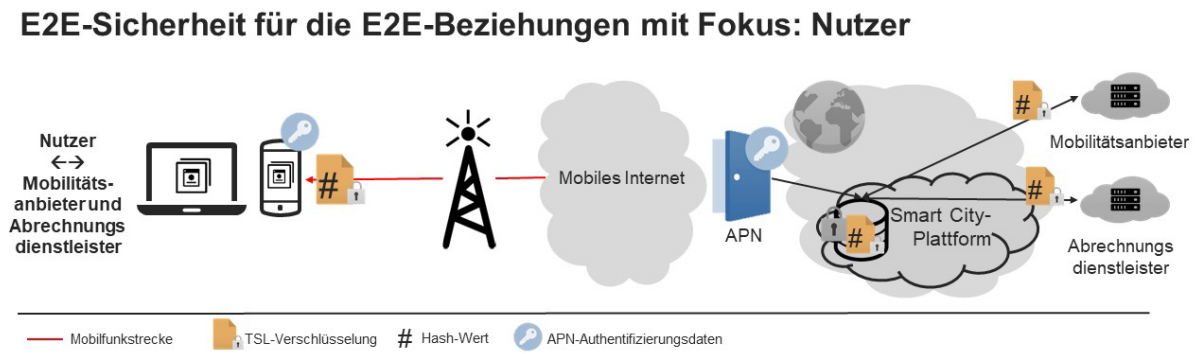

Abbildung 9: E2E-Sicherheit mit Fokus auf den Nutzer

Die vorgeschlagene TLS-Verschlüsselung wird bereits bei der Entwicklung sowohl in der Web- sowie innerhalb der Smartphone-App implementiert. Werden nun Daten von den Anwendungen bzw. vom Nutzer generiert, werden diese mittels TLS verschlüsselt. Anschließend wird eine kryptografische Hash-Funktion nach dem Stand der Technik eingesetzt. Die verschlüsselten Daten werden über das Mobilfunknetz zur Basisstation gesendet. Das IoT-Gerät authentifiziert sich dann am APN mit dem jeweiligen Anmeldenamen. Die verschlüsselte Datenbank nimmt die TLS-verschlüsselten Datenpakete auf, entschlüsselt diese und stellt sie anderen Services innerhalb der Smart City-Plattform zur weiteren Verarbeitung zur Verfügung. Sollten Daten aus der Datenbank an externe Plattformen, hinsichtlich Abrechnung oder Reservierungen, gesendet werden, geschieht dies ebenfalls durch eine TLS-Verschlüsselung. Durch dieses Vorgehen wird sichergestellt, dass die Daten über den kompletten Verlauf der Kommunikation verschlüsselt sind. Das gleiche Vorgehen wird genutzt, sollten die externen Plattformen mit dem Nutzer kommunizieren.

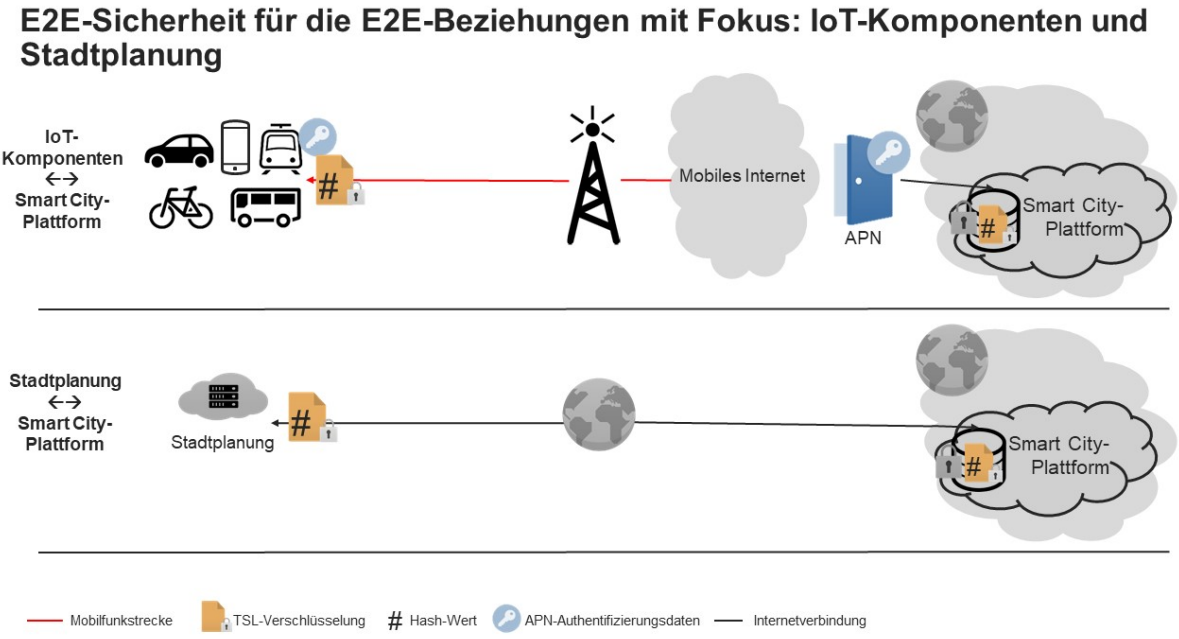

Abbildung 10: E2E-Sicherheit mit Fokus auf die IoT-Komponenten und die Stadtplanung

Die E2E-Sicherheit wird auch bei den IoT-Komponenten mit TLS-Verschlüsselung sichergestellt. Dafür wird die Verschlüsselung direkt bei der Entwicklung der Software der IoT-Komponente implementiert. Dadurch ist es möglich, die Daten TLS-verschlüsselt von der Komponente bis zur verschlüsselten Datenbank zu übertragen. Auch hier kommt eine kryptografische Hash-Funktion zum Einsatz, um sicherzustellen, dass die Datenpakete nicht verändert wurden und von dem erwarteten Gerät stammen. Der APN bildet die Schnittstelle vom

mobilen ins öffentliche Internet und verlangt die vorherige Authentifizierung des Gerätes, bevor die Daten weiter geroutet werden. Der Einsatz eines privaten oder semi-privaten APNs ist in diesem Szenario denkbar, um zusätzliche Sicherheit in den Anwendungsfall zu bringen, jedoch nicht immer umsetzbar, da ein privater APN kostspielig ist und sich daher nur für große Deployments eignet. Ein semi-privater APN, wie z.B. ein M2M-APN, wäre für den Einsatz in IoT-Netzwerken denkbar. Auch weil die APN-Authentifizierungsinformationen bereits auf der SIM-Karte vorkonfiguriert sind. Jedoch stellt auch das Mobiltelefon des Nutzers eine IoT-Komponente dar, welche Positionsdaten zur Smart City-Plattform sendet. Kommt nun ein semi-privater APN zum Einsatz, muss der Nutzer manuell die APN-Konfiguration seines Endgerätes ändern. Da dieses Szenario die Benutzbarkeit des Anwendungsfalls einschränkt, kann ein semi-privater oder auch privater APN in einem Sicherheitskonzept nicht berücksichtigt werden.

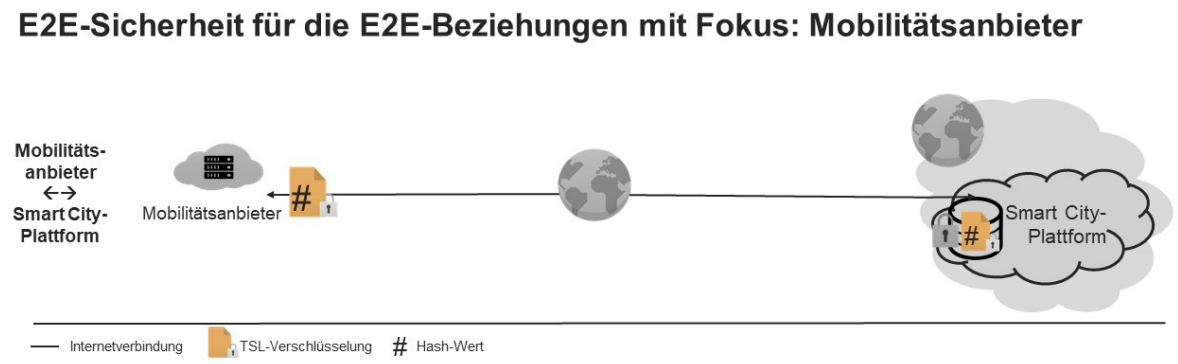

Abbildung 11: E2E-Sicherheit mit Fokus auf die Mobilitätsanbieter

Letztendlich wird auch die Kommunikation von einer externen Plattform kommend über eine Internetverbindung hin zur Smart City-Plattform bzw. zur verschlüsselten Datenbank mit TLS verschlüsselt und erhält ebenfalls einen Hash-Wert. Die verschlüsselten Daten werden in der TLS-verschlüsselten Datenbank aufgenommen, entschlüsselt und anderen Services innerhalb der Smart City-Plattform bereitgestellt.

5.4 Manipulationssicherheit

Die bisher vorgestellten Verfahren sichern die Übertragungswege ab. Da bei der multimodalen Mobilität zahlreiche Parteien miteinander Daten austauschen müssen, muss jedoch auch sichergestellt werden, dass die übermittelten Daten protokoll- und spezifikationsgerecht verarbeitet werden (G z.3 – Maniuplieren der Daten). Klassisch ließe sich dies über eine Trusted Third Party mit zentralem Logging technisch lösen. Dies ist im Rahmen einer offenen Smart City-Plattform mit freiem Zugang für beliebige Teilnehmer jedoch möglicherweise nicht wünschenswert.

Eine Alternative bietet der Einsatz eines Blockchain-Protokolls. Bekannt wurde die Blockchain [58] durch die Kryptowährung „Bitcoin“ und definiert eine dezentralisierte Transaktions- und Datenmanagement-Technologie. Sie basiert auf der so genannten Distributed Ledger Technology (dezentral geführte Kontenbuchtechnologie [DLT]). Ein Blockchain-Block [34] enthält, neben den Transaktionsdetails, noch Informationen über die jeweilige Blocknummer, Prüfsummen über den Vorgängerblock sowie Informationen zur Validierung dieses Blocks.

Im Rahmen eines E2E-Sicherheitskonzepts für Smart Cities könnte eine Blockchain analog zu [39], [40] Manipulationssicherheit herstellen: Die Daten werden direkt, nachdem sie durch das IoT-Gerät generiert wurden, verschlüsselt. Gleichzeitig wird eine kryptografische Hash-Funktion angewendet. Der daraus entstehende Hash-Wert wird mit einem Zeitstempel in einer Blockchain gespeichert. Anschließend werden die verschlüsselten Daten über die Mobilfunkstrecke versendet. Sollte hier ein Man-in-the-Middle durch eine kompromittierte Basisstation

versuchen die Daten abzufangen wird er durch die TLS-Verschlüsselung insofern daran gehindert, als dass er die verschlüsselten Daten nicht lesen und Nutzen daraus generieren kann. Um nun aus dem mobilen Internet in das öffentliche Internet Daten zu übertragen, muss sich das IoT-Gerät am APN mit den APN-Informationen (APN, Benutzername und Passwort) authentifizieren. Ist die Authentifizierung erfolgreich werden die Daten weiter zur Smart City-Plattform bzw. zur ebenfalls verschlüsselten Datenbank geleitet. Damit sichergestellt werden kann, dass die Daten nicht vorab manipuliert wurden, nutzt der Empfangsserver ebenfalls die kryptografische Hash-Funktion und berechnet den Hash-Wert der verschlüsselten Daten. Darauffolgend liest er den in der Blockchain gespeicherten Hash-Wert mit Zeitstempel. Stimmen die Hash-Werte überein, kann davon ausgegangen werden, dass die Daten nicht manipuliert wurden, obwohl die Übertragungsstrecke verschlüsselt ist.

Um die Blockchain innerhalb eines IoT-Netzwerkes einzusetzen, muss sie in ihrer Länge und in ihrer Komplexität jedoch begrenzt werden, um den limitierten Ressourcen im IoT gerecht zu werden. Das heißt, es sind noch Anpassungen am Verfahren vorzunehmen, die heute so noch nicht verfügbar sind.

6 Diskussion

Wir haben gezeigt, dass es möglich ist, mit bestehender und etablierter Technologie Schwachstellen und Risiken im Bereich Datensicherheit entgegenzuwirken, welche von dem IT-Grundschutz so noch nicht abgedeckt werden. Abbildung 14 zeigt, welche der identifizierten Gefährdungen so vollumfänglich (dunkelgrüner Haken) oder mit Restriktionen (hellgrüner Haken) abgedeckt werden.

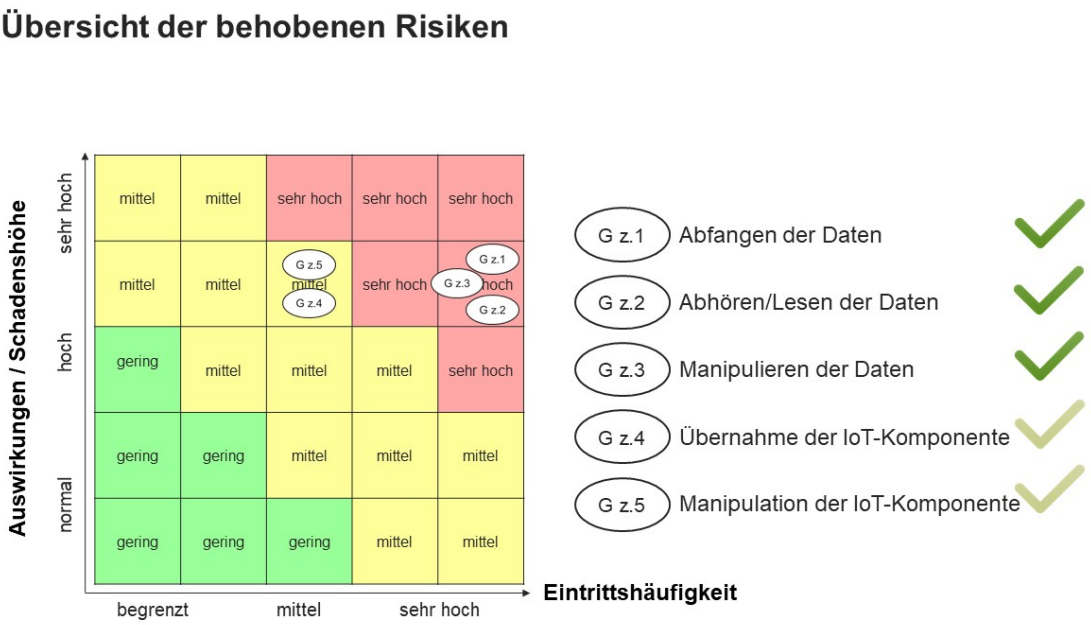

Abbildung 12: Übersicht der behobenen Risiken

Die Gefährdungen G z.1, G z.2 und G z.3 Innerhalb der Risikomatrix wurden als „sehr hoch“ eingestuft, weswegen diese Risiken mit einer sehr hohen Priorität betrachtet werden. Die von uns betrachteten Maßnahmen beheben drei der genannten Gefährdungen. Die TLS-Verschlüsselung vermeidet hierbei das Lesen und Abhören der Daten, sowie indirekt das Abfangen der Daten, da ein potentieller Angreifer aus einem verschlüsselten Datenpaket keine Informationen genieren kann. Des Weiteren bietet TLS, sowie die eingesetzte kryptografische Hash-Funktion, einen Schutz vor dem Manipulieren der Daten.

Die weiteren Gefährdungen G z.4 und G z.5 wurden in der Risikomatrix als „mittleres“ Risiko eingeordnet, trotzdem müssen sie betrachtet und behoben werden, um eine ganzheitliche

Sicherheitslösung abbilden zu können. Die beiden genannten Risiken können nicht mit den vorhandenen technischen Maßnahmen abgesichert werden, allerdings kann hier mit manuellen und prozessualen Sicherheitsmaßnahmen entgegengewirkt werden. Hierzu zählen beispielsweise security-by-design- und security-by-default-Entwicklungsansätze, sichere und starke Benutzernamen/Passwörter und erschwerter physischer Zugriff auf die Komponenten.

Wie aus Abbildung 13 hervorgeht, adressieren wir alle in der Wertschöpfungskette (siehe Abbildung 4) genannten Stakeholder. Damit die Datensicherheit gewährleistet werden kann, müssen alle, die an dem Anwendungsfall beteiligt sind, die vorgeschlagenen technologischen und manuellen/prozessualen Sicherheitsmaßnahmen umsetzen. Sollten beispielsweise der Mobilitätsanbieter und die Stadtplanung keine TLS-Verschlüsselung einsetzen, können die gesendeten sensitiven Daten von Angreifern im öffentlichen Internet abgefangen und gelesen werden. Um das Risiko zu vermeiden, kann zusätzlich zur TLS-Verschlüsselung ein VPN-Tunnel eingesetzt werden. Durch einen VPN-Tunnel wird eine sichere Verbindung zwischen den „externen“ Plattformen und der Smart City-Plattform hergestellt.

Für den Großteil unseres Anwendungsszenarios lässt sich ein Basisschutz erreichen, indem alle daran teilnehmenden institutionellen Teilnehmer dazu verpflichtet werden, passende ISO-Standards und ausreichende Zertifizierungen nachzuweisen. Für die Nutzer gilt dies jedoch nicht: Die Nutzer verwenden eigene Mobilgeräte, um die angebotenen Dienste zu nutzen, und müssen daher selbst für die Absicherung ihres Endpunkts sorgen. Auf der anderen Seite sind sich dadurch ergebende Sicherheitsprobleme jeweils auf den einzelnen Nutzer mit seinem unzureichend abgesicherten Mobilgerät beschränkt. Das heißt, der Schaden bei einem Sicherheitsvorfall ist auf jeweils einzelne Teilnehmer begrenzt. Dies ließe sich durch vertragliche Maßnahmen auffangen, beispielsweise analog zu den bekannten Stornierungsmöglichkeiten bei unberechtigten Kreditkartenbuchungen.

7 Fazit

Die zunehmende Digitalisierung von Alltagsgegenständen und alltäglicher Prozesse führt zu weitreichenden Herausforderungen im Bereich des Datenschutzes bzw. der Datensicherheit. Die Nutzer solcher Anwendungsfälle sind daher darauf angewiesen, dass die Unternehmen dem gestiegenen Verlangen nach Datensicherheit nachkommen und notwendige Maßnahmen ergreifen, um ihre Anwendungen und/oder Komponenten sicher zu gestalten und abzusichern. Zwar konzentrieren sich Unternehmen vermehrt auf den Bereich der Datensicherheit und implementieren Schutzmaßnahmen sowohl auf IoT-Geräten, IoT-Plattformen als auch auf Servern, aber es konnte noch kein Konzept gefunden werden, welches eine umfassende Sicherheit in einem IoT-Anwendungsfall beschreibt.

Das schrittweise Analysieren und Strukturieren des Anwendungsfalls nach den BSI-Standards 200-2 und 200-3 hat Gefährdungen sowie Handlungsbedarfe aufgezeigt. Diese systematische Strukturierung des Problemfalls bildet eine solide Basis, um darauf aufbauend die Sicherheit in dem Anwendungsfall untersuchen zu können. Zwar enthält der IT-Grundschutz Bausteine zur Maximierung der Datensicherheit in bestimmten Anwendungsfällen, jedoch werden die Besonderheiten des IoT hierbei noch kaum bzw. gar nicht betrachtet. Damit der IT-Grundschutz zukünftig den Anforderungen im IoT gerecht wird, muss dieser um spezielle Bausteine und Gefährdungen ergänzt werden.

Dabei müssen die einzelnen empfohlenen Sicherheitsmaßnahmen wie bei einer Kette ineinandergreifen. Sollte ein beteiligtes Unternehmen Sicherheitsmaßnahmen nur unvollständig implementieren, kann keine umfassende Datensicherheit für alle Teilnehmer mehr garantiert werden. Wir konnten zeigen, dass sich ein hohes Maß an IT-Sicherheit bei der multimodalen Mobilität realisieren lässt, wenn alle institutionellen Teilnehmer an der Wertschöpfungskette auf die konsequente Umsetzung des aktuellen Stands der Technik verpflichtet werden. Dies

beschränkt mögliche Schadensfälle auf die privaten Mobilgeräte einzelner Nutzer, die grundsätzlich selbst über die Sicherheitsmerkmale ihres Geräts verfügen können.

8 Quellenverzeichnis

[1] O'Connor, Chris: Security in the era of cognitive IoT. (2018) https://www.ibm.com/blogs/internet-of-things/security-cognitive-iot/, Kopie s. http://www.webcitation.org/6z2eymUj9

[2] Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for internet of things (iot). In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)

[3] Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the Internet of Things: A Review. In Computer Science and Electronics Engineering (ICCSEE)

[4] Plate, Franziska (2019). Entwicklung eines Sicherheitskonzeptes für die multimodale Mobilität. Masterarbeit an der Hochschule für Telekommunikation Leipzig

[5] Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of Things. International Journal of Communication Systems, 25(9), 1101-1102.

[6] Haritha, A., & Lavanya, (2017). A. Internet of Things: Security Issues.

[7] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20(8), 2481-2501.

[8] Patel, K. K., & Patel, S. M. (2016). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. International Journal of Engineering Science in Computing, 6(5).

[9] Nam, T., & Pardo, T. A. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. In Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times (pp. 282-291).

[10] Bundesamt für Sicherheit in der Informationstechnik (2018). Die Lage der IT-Sicherheit in Deutschland 2017. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=3, Kopie s. http://www.webcitation.org/71ss1ynYi

[11] Eckert, C. (2018). IT-Sicherheit: Konzepte-Verfahren-Protokolle. Walter de Gruyter.

[12] Gallotti, R., & Barthelemy, M. (2014). Anatomy and efficiency of urban multimodal mobility. Scientific Reports, 4, 6911.

[13] Maertins, C. (2006). Die Intermodalen Dienste der Bahn: Mehr Mobilität und weniger Verkehr? Wirkungen und Potenziale neuer Verkehrsdienstleistungen.

[14] Jochema, P., & Schipplb, J. (2014). Mobility 2.0: Antriebskonzepte im Zusammenspiel mit multimodaler Mobilität. In ALTERNATIVE, 165.

[15] Negash, B., Rahmani, A. M., Westerlund, T., Liljeberg, P., & Tenhunen, H. (2015). LISA: Lightweight internet of things service bus architecture. Procedia Computer Science, 52, 436-443.

[16] MuleSoft, Inc. (2018). What is Mule ESB? https://www.mulesoft.com/resources/esb/what-mule-esb, Kopie s. http://www.webcitation.org/72NFFjnyr

[17] Bourne, V. (2019). Studie von Trend Micro: Unternehmen vernachlässigen IoT-Sicherheit und setzen das Vertrauen der Kunden aufs Spiel.

https://www.trendmicro.com/de_de/about/newsroom/press-releases/2018/20180726-studie-von-trend-micro-unternehmen-vernachlassigen-iot-sicherheit-und-setzen-das-vertrauen-der-kunden-aufs-spiel.html, Kopie s. http://www.webcitation.org/75F0WF9y4

[18] Vermillard, J. (2015). Sicherheit für IoT-Geräte. Linux-Magazin 10/2015

[19] dc-square GmbH (2018). Introducing the MQTT Security Fundamentals. https://www.hivemq.com/blog/introducing-the-mqtt-security-fundamentals, Kopie s. http://www.webcitation.org/72NT5Douz

[20] Bormann, C. (2018). CoAP. http://coap.technology/, Kopie s. http://www.webcitation.org/72NU5s7P6,

[21] GSM Association. (2016). IoT Security Guidelines for Service Ecosystems. GSM Association Official Reference Document CLP, 12.

[22] Bundesamt für Sicherheit in der Informationstechnik (2018). Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Oeffentl-Mobilfunknetze.pdf?__blob=publicationFile&v=1, Kopie s. http://www.webcitation.org/72WOS9f7m

[23] 3GPP (2018). LTE. http://www.3gpp.org/technologies/keywords-acronyms/98-lte, Kopie s. http://www.webcitation.org/72WOr6h8j

[24] 3GPP (2012). 3GPP System Architecture Evolution (SAE): Security Architecture (Release 10). 3GPP TS 33.401, V10.3.0

[25] Wi-Fi Alliance (2003). Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. White paper, University of Cape Town, 492-495.

[26] Wi-Fi Alliance (2018). Wi-Fi Certifies WPA3. https://www.wi-fi.org/discover-wi-fi/security, Kopie s. http://www.webcitation.org/72Wg7IzsB

[27] Kaufman, L. M. (2009). Data security in the world of cloud computing. IEEE Security & Privacy, 7(4).

[28] Bundesamt für Sicherheit in der Informationstechnik (2018): ISO 27001 Zertifizierung auf Basis von IT-Grundschutz. https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html, Kopie s. http://www.webcitation.org/72ZXLl7RH

[29] IBM BP Network (2018). How to Secure the Internet of Things (IoT) https://www.ibmbpnetwork.com/blog/iot-security, Kopie s. http://www.webcitation.org/72ZYI3Hmf

[30] He, D., Chan, S., & Guizani, M. (2015). Mobile Application Security: Malware Threats and Defenses. IEEE Wireless Communications, 22(1), 138-144.

[31] Cisco (2018). Securing the Internet of Things: A Proposed Framework. https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html, Kopie s. http://ww.webcitation.org/72fflTErR

[32] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 618-623)

[33] Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in Internet of Things: Challenges and Solutions. arXiv preprint arXiv:1608.05187.

[34] Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. IEEE 14th International Conference on Smart City

[35] Bundesamt für Sicherheit in der Informationstechnik (2016). BSI-Standard 200-2, IT-Grundschutz-Methodik. https://www.bsi.bund.de

[36] Bundesamt für Sicherheit in der Informationstechnik (2016). BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz. https://www.bsi.bund.de

[37] Eßmann, C., Plate, F. (2018). Vom Smart Parking zur Smart City. https://www.detecon.com/de/wissen/vom-smart-parking-zur-smart-city, Kopie s. http://www.webcitation.org/73CzrCLWn

[38] Bundesamt für Sicherheit in der Informationstechnik (2018). IT-Grundschutz-Kompendium, Edition 2019

[39] Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. Banking Beyond Banks and Money (pp. 239-278)

[40] Florea, B. C. (2018). Blockchain and Internet of Things data provider for smart applications. Mediterranean Conference on Embedded Computing (MECO) (pp. 1-4)