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

Erik Buchmann[1], Franziska Plate[2]

Abstract: Im Zuge einer Mobilitätswende 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 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. Wir untersuchen, inwieweit sich die multimodale Mobilität für den Nahverkehr in einem typischen Smart City-Szenario technisch absichern lässt. In Anlehnung an den IT-Grundschutz modellieren wir die Datenflüsse, 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.

Keywords: IT-Sicherheit, Smart City, Multimodale Mobilität

1 Einleitung

Die Ausgestaltung der urbanen Mobilität wird gerade für Ballungsräume immer wichtiger. Dabei werden integrierte Mobilitätsangebote untersucht, die schienen- oder straßengebundene öffentliche Verkehrsmittel, Car-Sharing, Car-Pooling oder Leihfahrräder intelligent zu einer multimodalen Mobilitätsform zusammenführen, welche das Mobilitätsbedürfnis des Nutzers erfüllt. Dabei sind persönliche Präferenzen wie Preis, Komfort, Reisezeit oder Umweltfreundlichkeit zu berücksichtigen und externe Faktoren wie die Verfügbarkeit von Verkehrsmitteln, Verspätungen oder Umweltparameter mit einzubeziehen [GB14].

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

[1] Hft-Leipzig, Gustav-Freytag-Straße 43-45, 04277 Leipzig, buchmann@hft-leipzig.de
[2] Detecon International GmbH, Sternengasse 14 - 16, 50676 Köln, Franziska.Plate@detecon.com

doi:10.18420/inf2019_66

komplexe Funktionen entlang der Wertschöpfungskette der multimodalen Mobilität, von der Reiseplanung des Nutzers bis zur Abrechnung der tatsächlich in Anspruch genommenen Mobilitätsdienste. Die dafür erforderlichen Daten stammen aus dem öffentlichen Internet, Smartphones der Nutzer oder IoT-Komponenten. 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 auch die Datenintegrität wesentlich. Der IT-Sicherheit [Ec18] kommt deswegen eine entscheidende Bedeutung zu [Bo19].

In dieser Arbeit analysieren wir, wie sich die multimodalen Mobilität in einem typischen Smart City-Szenario technisch absichern lässt. Dabei konzentrieren wir uns auf die Verknüpfung von Nahverkehrsmitteln. In unserem Fokus stehen nicht Schwachstellen existierender Implementierungen. Vielmehr untersuchen wir die Sicherheitsrisiken innerhalb der Wertschöpfungskette. In Anlehnung an den IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) modellieren wir die Datenflüsse und Übertragungswege, die für die multimodale Mobilität erforderlich sind. Wir untersuchen, ob derzeit verfügbaren Konzepte für diesen Anwendungsfall geeignet sind, und führen eine Risikoanalyse durch. Unser Ziel ist eine Ende-zu-Ende (E2E) Absicherung der Systeme und Übertragungswege entlang der Wertschöpfungskette. Unsere Arbeit zeigt, dass bei einer konsequenten Absicherung nach dem Stand der Technik das größte Risiko durch Fehlbedienung oder Fehlkonfiguration des Smartphones des Nutzers entsteht, und wir zeigen auf, um welche Risiken es sich handelt. Aus Platzgründen können wir hier nur eine Übersicht über unsere Erkenntnisse bieten. Details stehen in einem Arbeitsbericht [PB19] zur Verfügung.

In Abschnitt 2 beschreiben wir verwandte Arbeiten. In Abschnitt 3 führen wir eine Risikoanalyse für die multimodale Mobilität in einem Smart City-Szenario durch, gefolgt von Risikobehandlungsoptionen in Abschnitt 4. Wir schließen mit einem Fazit in Abschnitt 5.

2 Verwandte Arbeiten

Im Folgenden führen wir die multimodalen Mobilität, deren technische Grundlagen und Ansätze zur Absicherung ein. Wir setzen Grundkenntnisse zum IT-Grundschutz [Bu19] und zu Kommunikationsprotokollen wie WLAN oder LTE voraus.

2.1 Konzepte für die multimodale Mobilität

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. Bike-Sharing, Car-Sharing, Straßenbahnen, Busse und Taxen, als auch den Fernverkehr, u.a. Züge, Flugzeuge und Schiffe. Nutzer können entweder eigenständig auf die verschiedenen Verkehrsmittel zurückgreifen, oder sie nutzen einen Planungsdienst. Bereits seit 2001 verfolgt die Deutsche Bahn diese Mobilitätsstrategie, welche

den Nutzer mit entsprechenden Konzepten von Haustür zu Haustür bringen soll [Ma06]. Auch über den Karten-Dienst Google Maps können Routen multimodal geplant werden. Dafür muss der Routenplanung bekannt sein, welche Verkehrsmittel wie, wann und wo zur Verfügung stehen. Ebenfalls muss die Routenplanung wissen, wo mögliche Umsteige-Punkte zwischen den Verkehrsmitteln liegen. Die Nutzung von unterschiedlichen Verkehrsmitteln innerhalb einer Route kann über ein umfassendes E-Ticket gelöst werden [JS14]. Hierbei kann das Fahrzeug mit dem selben Ticket entsperrt, genutzt und abgerechnet werden. Die Abrechnung erfolgt auf Basis der Nutzung und stellt eine erhebliche Anforderungen an Datenschutz und Datensicherheit [Ec18].

2.2 Technische Grundlagen der multimodalen Mobilität

Im Internet of Things (IoT) [Xi12] werden physische Gegenstände lesbar, erkennbar, auffindbar, adressierbar und/oder steuerbar. IoT-Geräte erhalten Sensorik sowie einen kleinen Prozessor und Speicher, wodurch sie kontextbezogene Entscheidungen [PP+16] treffen können. Dabei können sie über eine Kommunikationsverbindung auf Daten von anderen Geräten zugreifen. IoT-Konzepte sind daher bei der Realisierung von Smart City-Anwendungsfällen unverzichtbar, beispielsweise als Umweltsensor oder zur Überwachung und Abrechnung von Verkehrsmitteln. Gleichwohl nimmt die Angriffsfläche in der IoT-Umgebung aufgrund der Heterogenität von Geräten, Kommunikationsmedien, Anwendungen und Diensten vielfältig zu [HL17], während Sicherheitsmechanismen im IoT häufig vernachlässigt werden [Bu18].

Eine Smart City zielt auf die vollständige Vernetzung aller digitalen Anwendungsfälle über eine zentrale Smart City-Plattform ab. Diese ermöglicht den Informationsaustausch zwischen den einzelnen IoT-Komponenten sowie die Steuerung und Überwachung der eingesetzten IoT-Geräte. Wie eine solche zentrale Plattform aussehen kann, zeigt Abb. 1. Eine Connectivity Management-, Solution Enabling- und eine Big Data-Plattform bilden die Smart City-Plattform ab. Innerhalb der IoT-Anwendungsfälle kann es sowohl IoT-Geräte mit als auch ohne SIM-Karte geben. Die Komponenten, welche eine SIM-Karte besitzen, können ihre Daten über das Mobilfunknetz versenden. Dazu erhalten sie eine private Adresse, die über einen Access Point Name-Dienst (APN) auf eine öffentlich sichtbare IP-Adresse übertragen wird. Komponenten ohne SIM-Karte verwenden Funkstandards wie NarrowBand-IoT. Alle Komponenten senden ihre Daten an ein Gateway, das mit der Middleware der Smart City-Plattform verbunden ist. Die Middleware ermöglicht die Kommunikation der IoT-Komponenten untereinander und mit den Plattform-Diensten. Um die gesendeten Datenmengen zu reduzieren, können erste Teile der Datenanalyse bereits auf dem Gateway realisiert werden. Hierfür muss vorab entschieden werden, welche Daten wichtig genug sind, dass sie über die SIM-Karte bzw. die Netzwerkverbindung an die Big Data-Plattform gesendet werden. Die dort aufbereiteten Daten werden von der Solution Enabling-Plattform und der darauf befindlichen Business Logik weiter verarbeitet und visualisiert. Der modulare Aufbau der Plattform kann mit Hilfe von Integrationslösungen,

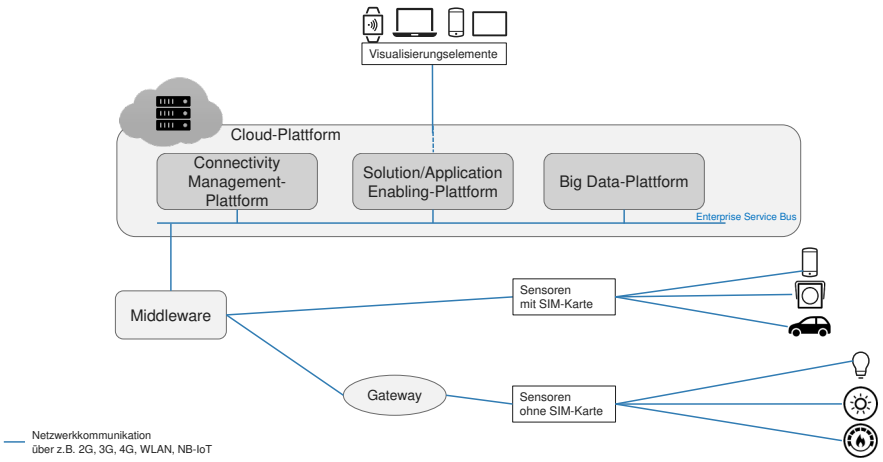

Abb. 1: Typische Smart City-Plattform

wie z.B. dem Enterprise Service Bus (ESB) oder durch Microservices und serverless-Architekturen, ermöglicht werden. Alternativen zum ESB sind die Lightweight Internet of Things Service Bus Architecture [Ne15] oder MuleESB [Br09], welche sich speziell für den Einsatz im IoT eignen. Ein Mediation-Service dient als Vermittler, welcher die einzelnen Plattformen – unabhängig vom Standort – miteinander verbindet. Über so eine Integrationslösung wird auch die Kommunikation zwischen den Plattformen ermöglicht.

2.3 Ende-zu-Ende-Sicherheit im Internet of Things

Da die IoT-Geräte und die Smart City-Plattform oft von verschiedenen Akteuren betrieben werden, schlägt [Ci18] differenzierte Eigentums- und Richtlinienkonzepte mit Zugriffskontrollen an den Schnittstellen vor. Damit die beteiligten Akteure Daten austauschen können, müssen Vertrauensbeziehungen zwischen ihnen aufgebaut werden. Da IoT-Komponenten nur über eingeschränkte Ressourcen verfügen, können klassische Authentifizierungs- und Verschlüsselungsverfahren wie AES oder RSA nicht eingesetzt werden. Daher schlägt [Ci18] leichtgewichtige Authentifizierungsverfahren vor. [OC18] definiert Sicherheit im IoT auf Basis unterschiedlicher Verantwortlichkeiten der Beteiligten im IoT-Ökosystem. Hardwarehersteller, Applikationsentwickler, Verbraucher, Betreiber und weitere Beteiligte sind dafür verantwortlich, dass Prozesse zur Erreichung der Sicherheit im IoT umgesetzt werden. Angriffe auf IoT-Geräte können die unbefugte Beschaffung von sensiblen oder privaten Daten, deren Manipulation sowie das Stören oder Verhindern von Services innerhalb des IoT-Systems mit sich bringen. Die von [OC18] vorgeschlagenen Lösungen sind jedoch nur auf einzelne Bestandteile des IoT-Ökosystems beschränkt und bilden kein E2E-Sicherheitskonzept ab.

[BA11] skizziert ein IoT-Sicherheitsframework auf Basis von leichtgewichtiger Kryptografie, physikalischer Sicherheit über ein Trusted Plattform Modul, standardisierten Sicherheitsprotokollen, sicheren Betriebssystemen, dem berücksichtigen von zukünftigen Anwendungsbereichen und sicheren Speichern. Allerdings bleibt offen, wie diese Merkmale implementiert werden können. Die Arbeit beschränkt sich auf generische Sicherheits-Ansätze für die im IoT angewendeten Protokolle, sowie für die Hard- und Softwareplattformen.

[BM16] beschreibt ein Sicherheitsframework auf verschiedenen Layern, welches auf der Blockchain-Technologie basiert. Die Layer präsentieren eine Prozesskette von den Sensoren und Aktoren über einen Kommunikations-Layer bis zu einem Layer für die Applikationen. Die Transaktionsdaten werden in einer Blockchain im Database-Layer gespeichert. Es wird jedoch nicht berücksichtigt, dass der Energiebedarf und der Overhead einer Blockchain eine Implementierung im IoT nicht unmittelbar zulassen. [Do17] definiert eine leichtgewichtige Variante der Blockchain für die Absicherung von IoT-Transaktionen. Eine Evaluierung anhand eines Smart Home-Szenarios zeigt, dass die angestrebten Schutzziele auch erreicht werden können. Es bleibt jedoch offen, ob eine Implementierung der Blockchain direkt innerhalb einer Smart Home-Anwendung möglich ist und ob sich diese Blockchain-Variante für weitere IoT-Anwendungsfälle eignet.

3 Die multimodale Mobilität

Der Nutzer legt einmalig über eine App auf seinem Smartphone oder über eine Webseite mit einer Webanwendung ein Benutzerprofil mit Zahlungsinformationen und Login-Daten an. Ist dies geschehen, läuft eine Reise wie folgt ab:

- Der Nutzer kann über eine App oder Webanwendung Routen mit verschiedenen Reisemitteln planen. Dafür werden Positions- und Verfügbarkeitsdaten benötigt.
- Tickets und Reservierungen werden in der Smart City-Plattform gebucht und über einen Abrechnungsdienstleister bezahlt. Hierbei werden die Zahlungsinformationen des Nutzers benötigt.
- Das Benutzerprofil stellt der Plattform alle Daten für den Buchungsprozess bereit.
- Buchungsinformationen inkl. Zahlungsinformationen und Nutzungsdaten werden an den jeweiligen Mobilitätsanbieter weitergeleitet.
- Positions-, Nutzungs- und Verfügbarkeitsdaten der Verkehrsmittel werden von IoT-Komponenten gesammelt und in einer Cloud weiterverarbeitet.
- Das Vernetzen der Verkehrsmittel ermöglicht eine Positionsberechnung in Echtzeit, um Verspätungen einzuplanen oder Wegezeiten zu aktualisieren.
- Sobald Anschlüsse gefährdet sind, werden auf der Basis von Positionsdaten und Daten über die Reiseroute Alternativrouten ermittelt.
- Mobilitätsanbieter nutzen die Daten, um Echtzeit-Fahrpläne zu aktualisieren.
- Die Stadtplanung nutzen die Daten, um das Mobilitätsangebot zu optimieren.

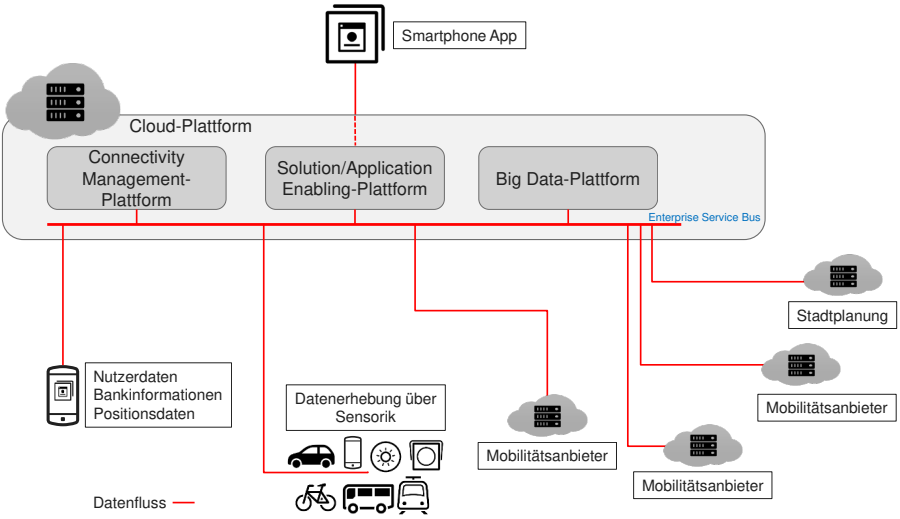

Abb. 2: Datenflüsse der multimodalen Mobilität

3.1 Datenflüsse und Wertschöpfungskette

Abbildung 2 illustriert die Datenflüsse bei der multimodalen Mobilität. Die IoT-Hardware kann in Fahrrädern, Autos, Bussen oder in Straßenbahnen verbaut sein. Auch das Mobiltelefon eines Nutzers kann als IoT-Komponente den Standort des Nutzers ermitteln. Jede Komponente nutzt verschiedene Kommunikationskanäle, um Daten zur Erfüllung der eigenen Funktion auszutauschen. Dabei werden die Mobilfunkstandards 2G, 3G und 4G sowie WLAN und kabelgebundene Übertragungswege genutzt. Abbildung 3 zeigt die Wertschöpfungskette der multimodalen Mobilität in Form einer Matrix, die den Komponenten, auf denen eine Wertschöpfung stattfindet, Rollen, Kommunikationskanäle und Daten zuordnet. Die Übersicht wurde auf Basis von Abschnitt 2 erstellt.

Welcher Schutzbedarf für diese Daten und alle Komponenten und Anwendungen besteht, die auf sie zugreifen, wird mit einer Schutzbedarfsfeststellung nach BSI-Standard 200-2 [Bu17a] ermittelt. Dazu ist eine Strukturanalyse erforderlich, welche die Daten, Dienste, Übertragungswege etc. modelliert. Aus Platzgründen verzichten wir auf eine detailliert Darstellung der Strukturanalyse sowie der Schutzbedarfsfeststellung und verweisen auf unseren Bericht [PB19]. Wir haben 6 Kategorien von Daten ermittelt, nämlich *Verfügbarkeitsdaten* (D1) der Verkehrsmittel, *Positionsdaten der IoT-Geräte* (D2), *Zahlungsdaten* (D3), *Login-Daten* (D4), *Positionsdaten der Nutzer* (D5) und *Nutzungsdaten* (D6) zur Abrechnung. Diese Daten werden von Webanwendungen, Smartphone Apps, Datenbanken und Big-Data-Analyseverfahren auf IoT-Geräten, Smartphones und der Smart City-Plattform verarbeitet und über WLAN, Mobilfunk, rechenzentrumsinterne Verbindungen, das Internet und Enterprise Service Bus-Verbindungen übertragen.

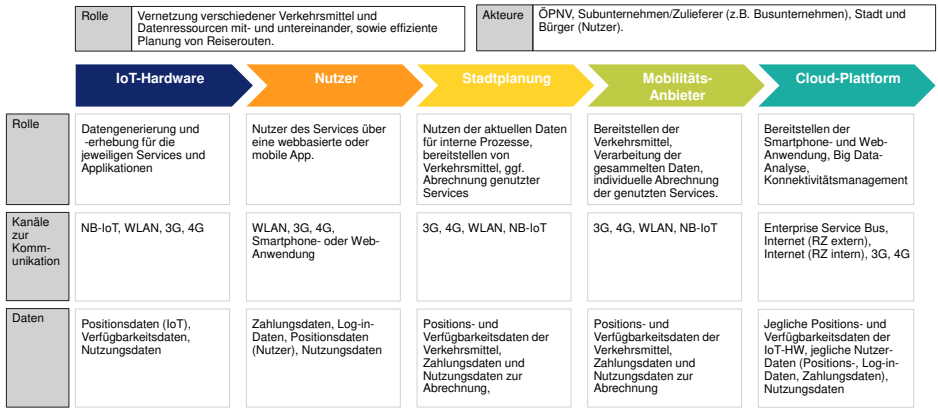

Abb. 3: Wertschöpfungskette der multimodalen Mobilität

Die Schutzbedarfsfeststellung unterscheidet *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* der zu schützenden Objekte. [Bu17a] definiert dabei die Schutzbedarfe „normal“, „hoch“ und „sehr hoch“. Der Schutzbedarf für eine IT-Komponente wird anhand der verwendeten Daten bestimmt. Da unsere Daten zur Planung und Abrechnung verwendet werden, haben wir keine existenzbedrohenden Schadensszenarien oder solche, die zu schweren gesundheitlichen Schäden führen, festgestellt. Wir haben den Schutzbedarf „sehr hoch“ also nicht vergeben. Dagegen können durch fehlerhafte Planung oder Abrechnung erhebliche materielle Schäden auftreten. Daher haben wir vielen Daten und davon abgeleitet auch vielen Komponenten den Schutzbedarf „hoch“ in den Zielen Verfügbarkeit, Vertraulichkeit und Integrität zugewiesen. Den Schutzbedarf „normal“ haben von uns die Verfügbarkeits- und Positionsdaten (D1, D2) in der Kategorie Vertraulichkeit erhalten, weil hier keine personenbezogenen Daten verarbeitet werden. Des weiteren haben wir den Zahlungs-, Login- und Positionsdaten der Nutzer (D3, D4, D5) bei der Integrität den Schutzbedarf „normal“ zugewiesen, weil Fehler in diesen Daten aufgrund Eigenschaften der Sensorik ohnehin berücksichtigt werden müssen, nur geringe Auswirkungen haben, oder leicht entdeckt und behoben werden können.

Nutzt eine IT-Anwendung Daten mit unterschiedlichen Schutzbedarfen, erhält sie den höchsten dieser Schutzbedarfe. Ebenso wird der Schutzbedarf der Kommunikationswege, IT-Systeme und Plattformen bestimmt. Daher erhalten alle in der Cloud-Plattform ablaufenden Anwendungen sowie deren Kommunikationswege den Schutzbedarf „hoch“ für Verfügbarkeit, Vertraulichkeit und Integrität. Aufgrund des Schutzbedarfs „hoch“ ist eine Risikoanalyse [Bu17b] erforderlich. Für weiterführende Details sowie für die Kritikalität der Kommunikationsverbindungen und eine Zuordnung von Elementargefährdungen wie „Feuer“ oder „Offenlegung schützenswerter Informationen“ verweisen wir auf unseren Bericht [PB19].

3.2 Risikoanalyse

Die Risikoanalyse hat das Ziel, alle anwendungsfallspezifischen Risiken aufzudecken, die von den im Grundschutz-Kompendium [Bu19] enthaltenen Standard-Maßnahmen nicht abgedeckt werden. Die Risikoanalyse wurde gemäß [Bu17b] in Form von Interviews im Workshop-Charakter mit zwei Partnern der Detecon International GmbH durchgeführt, die Experten der Themen IoT, Smart City und Connected Car sind und aufgrund langjähriger Berufserfahrung über ein breites Wissen im Bereich Netzwerk- und Plattformsicherheit verfügen. Wir haben die in Tabelle 1 aufgelisteten zusätzliche Gefährdungen für den gesamten Informationsverbund ermittelt. Für die IoT-Komponenten haben wir die in Tabelle 2 aufgeführten zusätzliche Gefährdungen identifiziert.

Gesamter Informationsverbund	
Name	Beschreibung
G z.1: Abfangen der Daten entlang der Wertschöpfungskette	Bei mangelnden Sicherheitsmaßnahmen lässt sich der Übertragungsweg der Daten D3, D4, D5 und D6 unbemerkt unterbrechen. Ein Dienstleister könnte z.B. nicht zwischen „keine Zahlung“ und „Zahlungsdaten abgefangen“ unterscheiden.
G z.2: Abhören/Lesen der Daten entlang der Wertschöpfungskette	Bei mangelnden Sicherheitsmaßnahmen lassen sich die Daten auf den IoT-Komponenten in der Wertschöpfungskette unbemerkt mitlesen, z.B. zu präferierten Routen (D5 und D6) oder Zahlungsinformationen (D3, D4 und D6) des Nutzers.
G z.3: Manipulieren der Daten innerhalb der Wertschöpfungskette	Bei mangelnden Sicherheitsmaßnahmen lassen sich die Daten von IoT-Komponenten entlang der Wertschöpfungskette unbemerkt manipulieren.

Tab. 1: Zusätzliche Gefährdungen im Informationsverbund

IoT-Komponenten	
Name	Beschreibung
G z.4: Unbefugte Übernahme der IoT-Komponente	Kann ein Angreifer eine IoT-Komponente übernehmen, kann er das dahinterliegende IT-System beeinflussen.
G z.5: Manipulation der IoT-Komponente	Kann ein Angreifer mit physischem Zugang oder über Zugang zum Kommunikationskanal eine IoT-Komponente manipulieren, ist deren Funktion nicht mehr gewährleistet.
G z.6: Sichtbarkeit der IoT-Komponente nach außen/extern	Sollte eine IoT-Komponente eine aus dem Internet sichtbare IP-Adresse besitzen, kann sie möglicherweise auch über das Internet angegriffen werden.

Tab. 2: Zusätzliche Gefährdungen für IoT-Komponenten

Für alle zusätzlichen Gefährdungen finden sich im BSI Grundschutz-Kompendium entsprechende Elementargefährdungen. Allerdings geht das BSI für unser Szenario nicht auf den Sonderfall „IoT-Komponente“ ein. Um selbst angemessene Maßnahmen festzulegen, muss das Risiko ermittelt werden, das von den Gefährdungen ausgeht. Dabei wird zwischen der Eintrittshäufigkeit und der potentiellen Schadenshöhe unterschieden.

Wir haben die Differenzierung in die Schadenshöhen „normal“, „hoch“ und „sehr hoch“ aus [Bu17b] übernommen. Bei den Eintrittshäufigkeiten unterscheiden wir zwischen „begrenzt“,

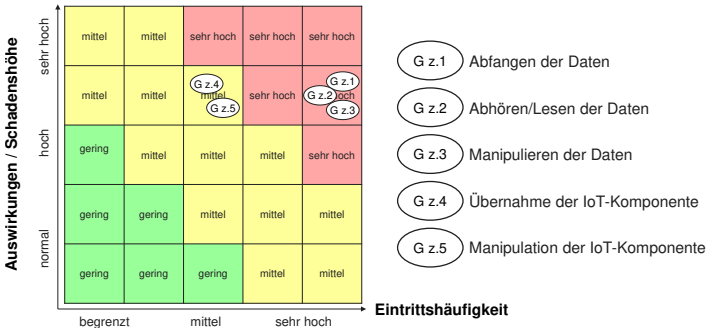

Abb. 4: Übersicht über die Risiken

„mittel“ und „sehr hoch“. Mit diesem Maßstab haben wir für die Gefährdungen G z.1 „Abfangen von Daten“, G z.2 „Abhören/Lesen der Daten“ und G z.3 „Manipulieren der Daten“ die Eintrittshäufigkeit „sehr hoch“ und die Schadenshöhe „hoch“ festgelegt, da Komponenten teilweise aus dem Internet sichtbar sind und personenbezogene Daten verarbeiten. Für G z.4 „Unbefugte Übernahme der IoT-Komponente“ und G z.5 „Manipulation IoT-Komponente“ haben wir die Eintrittshäufigkeit „mittel“ vergeben, da der Angreifer physischen Zugriff benötigt oder von innen kommen muss. Die potentielle Schadenshöhe haben wir mit „hoch“ festgelegt, da ein Angreifer auf diese Weise erhebliche finanzielle Schäden, Image-Schäden und Rechtsverletzungen verursachen kann. Abbildung 4 gibt einen Überblick über diese Risiken. „G z.6 Sichtbarkeit der IoT-Komponente“ haben wir nicht in Abbildung 4 aufgeführt. G z.6 erhöht die Eintrittswahrscheinlichkeit für viele Elementargefährdungen und muss durch Maßnahmen abgesichert werden, ist jedoch auf einer allgemeinen Ebene nicht mit einer potentiellen Schadenshöhe zu bewerten. Details und Begründungen sind wieder in [PB19] nachzuschlagen.

4 Risikobehandlung

Aus der Wertschöpfungskette der multimodalen Mobilität und den damit einhergehenden Datenflüssen ergeben sich fünf E2E-Beziehungen, die abgesichert werden müssen:

1. zwischen Nutzer und Mobilitätsanbieter
2. zwischen Nutzer und Abrechnungsdienstleister
3. zwischen IoT-Komponente und Smart City-Plattform
4. zwischen Stadtplanung und Smart City-Plattform
5. zwischen Mobilitätsanbieter und Smart City-Plattform

Dabei schützt der APN den Übertragungsweg, indem er eine Trennung zwischen den privaten Adressen der IoT-Komponenten (mit SIM-Karte) und öffentlich sichtbaren IP-Adressen schafft. Auch innerhalb der Internetverbindung von externen Plattformen zur Smart City-Plattform existieren Datensicherheitsmaßnahmen wie beispielsweise VPNs

oder X.509-authentifizierte Verbindungen. Allerdings berücksichtigen diese Maßnahmen die E2E-Sicherheit nicht. Bezieht man die im letzten Abschnitt identifizierten Risiken auf unsere fünf E2E-Beziehungen, lassen sich folgende Handlungsbedarfe identifizieren:

IoT-Komponente: Die IoT-Komponente ist dem Angreifer zugänglich, wodurch physische Manipulationen oder Sabotage möglich werden. Teilweise sind IoT-Komponenten aus dem Internet erreichbar, wodurch auch Manipulationen ohne physische Nähe zur Komponente möglich werden. Der Anwendungsfall benötigt jedoch genaue Daten, um Routen zu planen oder Abrechnungen durchzuführen.

Mobilfunk: Die Daten sind zwar innerhalb des Mobilfunknetzes mit einem Mobilfunk-Verschlüsselungsverfahren verschlüsselt. Allerdings sind die Verschlüsselungsverfahren des GSM- und UMTS-Netzes bereits gebrochen, weswegen lediglich der aktuelle LTE-Verschlüsselungsalgorithmus einen Schutz gegen das unerlaubte Lesen und Abhören von Daten bietet. Bei nicht verfügbarem LTE wird auf das unsichere GSM oder UMTS zurückgegriffen. Eine E2E-Datensicherheit ist nicht gewährleistet.

Smart City-Plattform: Die Absicherung der Übertragungswege schützt die ausgetauschten Daten nur bis zur Schnittstelle der Plattform. Es existiert keine durchgängige Verschlüsselung der Daten beispielsweise zu einer verschlüsselten Datenbank. So ist nicht sichergestellt, dass Daten nicht verändert oder von einem nicht autorisierten Gerät gesendet wurden.

4.1 Übertragungssicherheit

Eine Option zur Risikobehandlung bietet das Internet Protokoll Version 6 (IPv6). IPv6 baut ein Mesh-Netzwerk auf, das Daten mit IPsec-Verschlüsselung überträgt. Dabei können private IP-Adressen verwendet werden, wodurch das Gerät aus dem Internet nicht sichtbar ist. Allerdings ist IPv6 nicht mit IPv4 kompatibel und nicht überall verfügbar. Es wird daher eine Maßnahme gesucht, die die Datensicherheit in existierenden (IoT-)Netzwerken realisieren kann. Nachfolgend diskutieren wir, ob die Verwendung der Transport Layer Security (TLS)-Verschlüsselung für eine E2E-Absicherung geeignet ist.

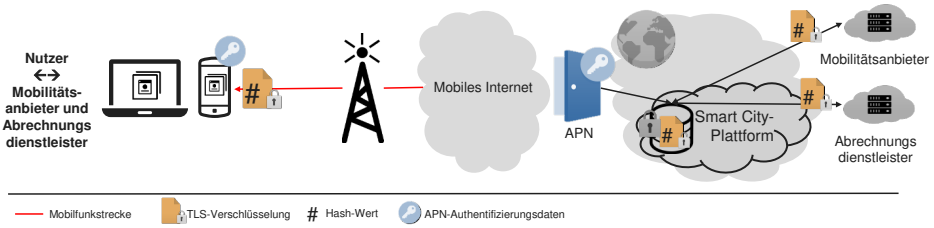

Abb. 5: E2E-Absicherung zum Nutzer

Die Abbildungen 5 bis 7 zeigen unsere E2E-Beziehungen mit integrierter TLS-Verschlüsselung. Die TLS-Verschlüsselung muss jeweils in den Endpunkten der Beziehungen

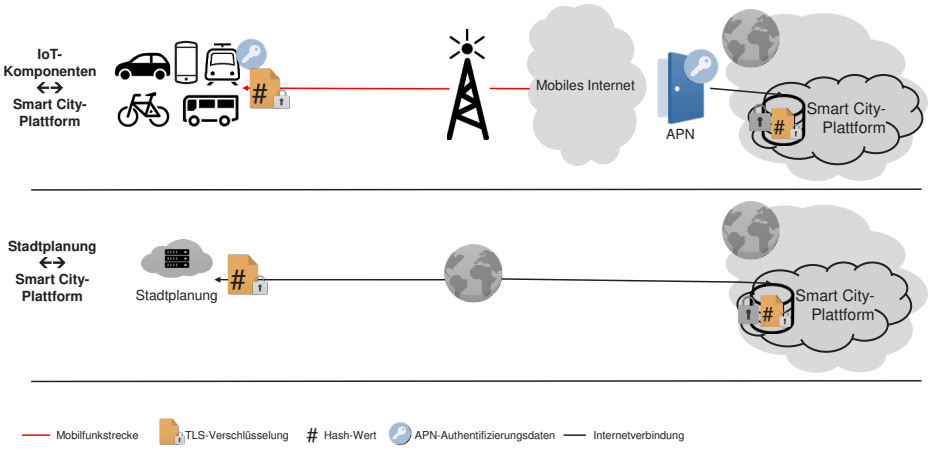

Abb. 6: E2E-Absicherung zu IoT-Komponenten und Stadtplanung

implementiert sein. In Abbildung 5 sind dies die Web-Anwendung bzw. Smartphone-App sowie die Smart City-Plattform und die Dienstleister. Werden Daten von den Anwendungen bzw. vom Nutzer generiert, werden diese mittels TLS verschlüsselt. Die verschlüsselten Daten werden über das Mobilfunknetz zur Basisstation gesendet. Das IoT-Gerät authentifiziert sich dann am APN mit dem jeweiligen Anmeldenamen. Die Smart City-Plattform entschlüsselt die TLS-verschlüsselten Daten, speichert sie in einer Datenbank und stellt sie anderen Services innerhalb der 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.

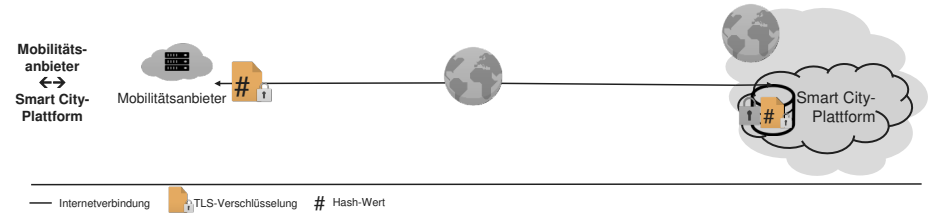

Abb. 7: E2E-Absicherung zum Mobilitätsanbieter

Die Absicherung der anderen E2E-Beziehungen erfolgt analog. Durch diese Maßnahme ist auch nach einem Bruch der LTE-Verschlüsselung oder bei einem Man-in-the-Middle-Angriff auf dem Gateway die Übertragungssicherheit sichergestellt.

4.2 Manipulationssicherheit

Da bei der multimodalen Mobilität zahlreiche Akteure miteinander interagieren, muss auch sichergestellt werden, dass die übermittelten Daten protokoll- und spezifikationsgerecht verarbeitet werden (G z.3 „Manipulieren der Daten“). Klassisch lässt sich dies über eine Trusted Third Party lösen, die Prüfsummen von allen erzeugten Daten speichert. Das heißt, bei jeder Datenübermittlung wird zusätzlich ein kryptographischer Hash-Wert als Prüfsumme über die Daten berechnet und ebenfalls TLS-verschlüsselt an eine Datenbank innerhalb der Smart City-Plattform gesendet, die hier als Trusted Third Party auftritt (s. Abbildungen 5 bis 7). Die Smart City-Plattform muss sicherstellen, dass die Datenbank nicht nachträglich verändert werden kann und jeder Akteur Zugang zu den Hash-Werten hat. In einer offenen Smart City-Umgebung ist es jedoch möglicherweise nicht wünschenswert, einen einzelnen Akteur als Trusted Third Party zu etablieren, der zugleich ein Plattformbetreiber ist und damit einen kritischen Angriffspunkt darstellt.

Eine Alternative könnte das Blockchain-Protokoll bieten. Ein Blockchain-Block [BM16] enthält neben den Transaktionsdetails Informationen über die Blocknummer, Prüfsummen über den Vorgängerblock sowie Informationen zur Validierung dieses Blocks. In einem E2E-Sicherheitskonzept könnte eine Blockchain analog zu [Fl18] Manipulationssicherheit herstellen: Die Daten werden, nachdem sie durch das IoT-Gerät generiert wurden, wie beschrieben mit TLS verschlüsselt. Zusätzlich wird mit einer kryptografischen Hash-Funktion eine Prüfsumme über die Daten berechnet. Die Prüfsumme wird dann nicht in einer Datenbank auf der Plattform, sondern mit einem Zeitstempel versehen in einer Blockchain gespeichert. Dies ermöglicht allen Akteuren jederzeit eine Verifizierung der erhaltenen Daten, ohne dabei auf zentralisierte Verfahren zurückgreifen zu müssen.

4.3 Diskussion

Die Gefährdungen G z.1, G z.2 und G z.3 werden mit den von uns betrachteten Maßnahmen erheblich reduziert. Die TLS-Verschlüsselung verhindert das Lesen, Abhören und Abfangen der Daten, eine kryptographische Prüfsumme deren Manipulation. Die Gefährdungen G z.4 und G z.5 können nicht mit den vorhandenen technischen Maßnahmen abgesichert werden. Allerdings kann hier mit manuellen und prozessualen Sicherheitsmaßnahmen entgegengewirkt werden. Hierzu zählen security-by-design-Entwicklungsansätze für die Soft- und Hardware der IoT-Komponenten.

Ein Grundschutz lässt sich also erreichen, indem alle institutionellen Teilnehmer dazu verpflichtet werden, passende ISO-Standards und ausreichende Zertifizierungen nachzuweisen. Für die Nutzer gilt dies jedoch nicht: Sie verwenden eigene Geräte, um die angebotenen Dienste zu nutzen, und müssen daher selbst für die Absicherung ihres Endpunkts sorgen. Dadurch entstehende Sicherheitsprobleme sind jedoch auf den individuellen Nutzer mit seinem unzureichend abgesicherten Gerät beschränkt. Der Schaden bei einem Sicherheitsvorfall ist also auf einzelne Nutzer begrenzt. Dies ließe sich durch vertragliche Maßnahmen auffangen, vergleichbar zu den Stornierungsmöglichkeiten bei unberechtigten Kreditkartenbuchungen.

5 Fazit

Die Digitalisierung alltäglicher Prozesse führt zu Herausforderungen für Datenschutz und Datensicherheit. Die Nutzer solcher Prozesse sind darauf angewiesen, dass die institutionellen Akteure mit diesen Herausforderungen geeignet umgehen. Die Analyse des Anwendungsfalls „Multimodale Mobilität“ nach den BSI-Standards 200-2 und 200-3 hat eine Reihe von Gefährdungen und Handlungsbedarfe aufgezeigt. Zwar enthält das IT-Grundschutz-Kompendium Bausteine zum Erreichen der Datensicherheit, jedoch machen die Besonderheiten des IoT-Einsatzes in einer Smart City detaillierte Risikoanalysen notwendig. Dabei ist das Ineinandergreifen von Sicherheitsmaßnahmen zwischen verschiedenen Akteuren über Unternehmensgrenzen hinweg eine Herausforderung. Sollte ein beteiligtes Unternehmen Sicherheitsmaßnahmen unvollständig implementieren, kann keine umfassende Datensicherheit für alle Nutzer garantiert werden. Wir konnten zeigen, dass sich ein hohes Maß an IT-Sicherheit bei der multimodalen Mobilität realisieren lässt, wenn alle institutionellen Akteure an der Wertschöpfungskette auf die Umsetzung des aktuellen Stands der Technik verpflichtet werden. Dies begrenzt Schadensfälle auf die privaten Mobilgeräte einzelner Nutzer, die selbst über die Sicherheitsmerkmale ihres Geräts verfügen können.

Literatur

[BA11] BABAR, S. et al.: Proposed Embedded Security Framework for Internet of Things. In: Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology. 2011.

[BM16] Biswas, K.; Muthukkumarasamy, V.: Securing smart cities using blockchain technology. In: 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS). IEEE, S. 1392–1393, 2016.

[Bo19] Bourne, V.: Unternehmen vernachlässigen IoT-Sicherheit und setzen das Vertrauen der Kunden aufs Spiel, https://www.trendmicro.com, Kopie s. http://www.webcitation.org/75F0WF9y4, 2019.

[Br09] Brebner, P.: Service-oriented performance modeling the mule enterprise service bus (esb) loan broker application. In: Euromicro Conference on Software Engineering and Advanced Applications. 2009.

[Bu17a] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2, IT-Grundschutz-Methodik. https://www.bsi.bund.de/, 2017.

[Bu17b] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-3, Risikomanagement. https://www.bsi.bund.de/, 2017.

[Bu18] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2018. https://www.bsi.bund.de/, 2018.

[Bu19] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium - Edition 2019. https://www.bsi.bund.de/, 2019.

[Ci18] Cisco: Securing the Internet of Things: A Proposed Framework, https://www.cisco.com, Kopie s. http://ww.webcitation.org/72ffITErR, 2018.

[Do17] Dorri, A.; Kanhere, S. S.; Jurdak, R.; Gauravaram, P.: Blockchain for IoT security and privacy: The case study of a smart home. In: IEEE Pervasive Computing and Communications Workshops. 2017.

[Ec18] Eckert, C.: IT-Sicherheit: Konzepte-Verfahren-Protokolle. Walter de Gruyter, 2018.

[Fl18] Florea, B. C.: Blockchain and Internet of Things data provider for smart applications. In: 2018 7th Mediterranean Conference on Embedded Computing (MECO). IEEE, S. 1–4, 2018.

[GB14] Gallotti, R.; Barthelemy, M.: Anatomy and efficiency of urban multimodal mobility. Nature Scientific Reports 4/, S. 6911, 2014.

[HL17] Haritha, A.; Lavanya, A.: Internet of Things: Security Issues. International Journal of Engineering Science Invention 6/11, 2017.

[JS14] Jochema, P.; Schipplb, J.: 8. Mobility 2.0: Antriebskonzepte im Zusammenspiel mit multimodaler Mobilität. ALTERNATIVE/, S. 165, 2014.

[Ma06] Maertins, C.: Die Intermodalen Dienste der Bahn: mehr Mobilität und weniger Verkehr? Wirkungen und Potenziale neuer Verkehrsdienstleistungen. Discussion Papers / Wissenschaftszentrum Berlin für Sozialforschung gGmbH. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-113845, 2006.

[Ne15] Negash, B.; Rahmani, A.-M.; Westerlund, T.; Liljeberg, P.; Tenhunen, H.: LISA: Lightweight internet of things service bus architecture. Procedia Computer Science 52/, S. 436–443, 2015.

[OC18] O'Connor, C.: Security in the era of cognitive IoT, https://www.ibm.com/blogs, Kopie s. http://www.webcitation.org/6z2eymUj9, 2018.

[PB19] Plate, F.; Buchmann, E.: Ende-zu-Ende-Sicherheit für die Multimodale Mobilität in einer Smart City, Technischer Bericht, http://nbn-resolving.de/urn:nbn:de:bsz:14-qucosa2-337880, Hochschule für Telekommunikation Leipzig, 2019.

[PP+16] Patel, K. K.; Patel, S. M. et al.: Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. International journal of engineering science and computing 6/5, 2016.

[Xi12] Xia, F.; Yang, L. T.; Wang, L.; Vinel, A.: Internet of things. International Journal of Communication Systems 25/9, S. 1101, 2012.