safe hAAven 5G++
Echtzeit- Verkehrsflussoptimierung

ZDE ZENTRUM FÜR DIGITALE ENTWICKLUNG

CYBERSICHERHEIT IN DEUTSCHEN SMART CITIES

Status quo und Handlungsfelder für die Zukunft

Impressum

Herausgeber

Zentrum für Digitale Entwicklung GmbH

Projektkoordination

Zentrum für Digitale Entwicklung GmbH

Fachliche Betreuung, Konzept und Redaktion

Fachliche Betreuung: Felix Unseld, Carina Nitschke, Wolfgang Weiß

Konzept: Felix Unseld, Bastian Hiergeist

Redaktion: Felix Unseld, Bastian Hiergeist, Georg Würffel, Johannes Röder

Stand

09/2024

Inhalt

0 Executive Summary

Im Rahmen des durch das Bundesamt für Sicherheit in der Informationstechnologie (BSI) geförderten Projektes „safe hAAven 5G++“ zur sicheren Datenübertragung für die Verkehrsflussoptimierung in Smart Cities entwickelte die Zentrum für Digitale Entwicklung GmbH eine Umfrage zur Cybersicherheit in deutschen Smart-City-Projekten. Diese richtete sich explizit an Projektverantwortliche aus Kommunen, Landkreisen und interkommunalen Kooperationen, die entweder ein Teil der vom Bund geförderten Smart-City-Modellkommunen sind oder im Smart-City-Index der bitkom gelistet werden.

Das übergeordnete Ziel der Befragung war es hierbei, ein besseres Verständnis in Bezug auf den Umgang mit Datensicherheit und Datenschutz in deutschen Smart-City-Kommunen zu erhalten. Die Ergebnisse erlauben einen interessanten Einblick in den Stand, den Umgang mit und die Entwicklungspotenziale von IT-sicherheitsrelevanten Themen in der deutschen Smart-City-Landschaft.

1 Einleitung

An jedes Smart-City-Projekt ist die Vision gekoppelt, den öffentlichen Raum mithilfe einer Vielzahl vernetzter Geräte und Sensoren dank Datenanalyse und intelligenter Steuerung technologisch fortschrittlicher, ökologischer und inklusiver zu gestalten und damit die Lebensqualität der Bevölkerung zu steigern.

In einer Smart City herrscht eine ständige Interaktion zwischen der Infrastruktur, den Einwohner*innen, den Prozessen sowie den technischen Geräten wie beispielsweise Sensoren vor. Als Ergebnis dieses enormen Datenaustausches, der Interaktion verschiedener IoT-Geräte sowie der sich ständig verändernden dynamischen Prozesse entstehen engmaschige Verflechtungen, die durch die Komplexität dieses digitalen Ökosystems noch verstärkt werden. Kommunen, die Bürgerschaft und Dienstleistende tauschen immer mehr Daten über immer mehr Systeme und Schnittstellen aus.

Nur, wenn die Bewohner*innen einer Smart City ihrer Infrastruktur vollständig vertrauen können, wird diese auch zu einem Erfolg.

Für die erfolgreiche Implementierung von Smart-City-Modellen ist es von höchster Bedeutung, sämtliche Aspekte rund um die Themen Cybersicherheit und Datenschutz frühzeitig und ganzheitlich in die Konzeption mit einzubeziehen.

Cyberangriffe auf digitale Infrastrukturen oder sonstige technische Probleme in ebenjenen können zukünftig gravierende Einschränkungen bei der Versorgung mit lebenswichtigen Gütern und Dienstleistungen auslösen oder zu ernsthaften Problemlagen in der öffentlichen Sicherheit führen. Beispiele für diese kritischen Bereiche sind die Gebäudeautomatisierung, die digitale Patientenakte im Gesundheitswesen oder Eingriffe in die digitale Bürgerschaftsbeteiligung. Auch auf die für Smart City essenziellen Stromnetze, insbesondere in Form von Smart Grids, können Cyberattacken schwere Auswirkungen haben und diese im Falle einer vernachlässigten Cyber-Sicherheit zu einem vulnerablen Teil der Infrastruktur machen.

Denn: Die Bedrohungslage durch Cyberattacken ist nicht nur unverändert hoch, sondern nimmt durch die zunehmende Abhängigkeit digitaler Systeme stetig zu.

Nachdem in der Vergangenheit hauptsächlich privatwirtschaftliche Unternehmen im Fokus dieser Angriffe standen, gerät zunehmend die öffentliche Verwaltung ins Visier der Angreifer*innen. Die größte Herausforderung im Bereich Cybersicherheit besteht für die Kommunalverwaltungen darin, die verschiedenen Funktionsebenen einer Smart City bestmöglich zu schützen und so ihre Funktionsfähigkeit auch im Falle eines kritischen Cyberangriffs aufrecht zu erhalten.

Besonders bedeutsam ist hierbei, dass alle relevanten Dienste im Kontext der gewachsenen, dezentralen IT-Systeme miteinbezogen werden. Zahlreiche digitale Teilhaber*innen und Anbieter*innen digitaler Infrastrukturen und Dienste agieren mit variierenden Standards. Je komplexer die zugrundeliegende Datenarchitektur gestaltet wurde, desto komplexer ist es auch, sie zu schützen.

Die Integration in ein gemeinsames, interoperables System stellt daher aus Cybersicherheitsperspektive eine große Herausforderung dar.

Eine resiliente und funktionsfähige Smart City benötigt ein umfassendes und aktuelles Cybersicherheitskonzept mit einer entsprechenden personellen und finanziellen Ausstattung. Dies umfasst die Entwicklung und Implementierung eines risikobasierten Smart-City-Cybersicherheitskonzepts, eine konsequente Beachtung von Prinzipien wie geplanter IT-Sicherheit (Security-by-Design) und geplantem Datenschutz (Privacy-by-Design) sowie eine Erhöhung des Bewusstseins bei allen Individuen und Organisationen, die in einer Smart City agieren. Des Weiteren können die Verwaltungen durch innovative und proaktive Partnerschaften eventuell vorhandene Qualifikationslücken schließen, Cybertalente anwerben und Verträge mit externen Dienstleistenden ausbauen. Die letztendliche Kompetenz und Hoheit im Bereich Cybersicherheit sollte jedoch intern verortet sein.

Vor dem beschriebenen Hintergrund wurde eine Befragung aufgesetzt, die den aktuellen Stand der Daten- und Cybersicherheit in deutschen Smart-City-Modellkommunen erfassen sollte und damit ein konkretes Bild der aktuellen Situation in den digitalsten Städten und Regionen Deutschlands zeichnet. Zur weiteren Exploration und der Schaffung eines vertiefenden Verständnisses wurden zudem Qualitative Leitfadeninterviews mit kommunalverantwortlichen durchgeführt.

2 Die Befragung

Die Befragung wurde im Rahmen des vom Bundesamt für Sicherheit und Informationstechnik geförderten Projekts safe hAAven 5G++ durchgeführt und befasste sich mit den Anforderungen an den Datenschutz und die Cybersicherheit bei der Umsetzung von Smart-City-Projekten in deutschen Kommunen. Gleichzeitig zielte sie auch auf den aktuellen Umsetzungsstand in Bezug auf ebendiese Themen ab.

Das übergeordnete Ziel der Befragung war es, ein besseres Verständnis in Bezug auf den Umgang mit Datensicherheit und Datenschutz in deutschen Smart-City-Kommunen zu erlangen. Darüber hinaus orientierte sich die Konzeption der Befragung an folgenden konzeptionellen Fragestellungen:

- Inwieweit spielt Cybersicherheit bei der Umsetzung von Smart-City-Projekten eine Rolle?
- Welchen Stellenwert nimmt der Datenschutz bei der Umsetzung von Smart-City-Projekten ein?
- In welchem Umfang können Projektverantwortliche und Entscheidende die Folgen ihrer Entscheidung in Bezug auf Datenschutz und Cybersicherheit überblicken?
- Inwieweit wollen Projektverantwortliche und kommunale Entscheidende Einfluss auf die konkrete Ausdefinierung von Einstellungen zu Datenschutz und Fragen rund um Cybersicherheit nehmen?
- Welche Maßnahmen zum Kompetenzaufbau in Bezug auf Datenschutz und Cybersicherheit werden in der Organisation ergriffen?
- Welche Maßnahmen werden ergriffen um Entscheidende, Projektverantwortliche und Mitarbeitende zu Fragen des Datenschutzes und der Cybersicherheit zu sensibilisieren?

2.1 Der Fragebogen

Die Umfrage wurde mittels eines Microsoft-Forms-Dokuments aufgesetzt und an die relevanten Zielgruppen verschickt. Für die Bearbeitung wurden 15 bis 20 Minuten veranschlagt.

Sie gliederte sich in folgende vier Blöcke:

- Screening
- Daten
- Cybersecurity
- Statistik

Im Screening standen primär das Herkunftsbundesland der Umfrageteilnehmenden, die Art der Gebietskörperschaft der befragten Smart-City-Modellprojekte sowie deren Bevölkerungszahl im Vordergrund. Auch wurden die jeweiligen Organisationsformen und -einheiten des Smart-City-Projektes sowie die Anzahl der Mitarbeitenden in Vollzeitäquivalenten ermittelt.

Der umfangreiche Block Daten umfasste mannigfaltige Fragen rund um die Themen Datensicherheit und Datenschutz: Die Implementierung von Sicherheitsvorkehrungen bei der Erfassung und Verbreitung von Daten in den jeweiligen Smart-City-Kommunen, Ort und Regelmäßigkeit der Speicherung, Formen und Themenfelder der Datenerhebung und -übertragung, Rahmen, Form und Möglichkeiten der Datenanalyse und der daraus gewonnenen Kenntnisse sowie der aktuelle Entwicklungsstand beim Internet der Dinge sowie bei themenspezifischen Daten wie Verkehrs- und Umweltdaten. Außerdem wurden die Zielgruppen von Daten(-analysen), das Vorhandensein von Open-Data für Bürger*innen sowie von Dienstanweisungen und Konzepten zur Datensicherheit abgefragt und die Existenz von Partner*innen bei der Datenauswertung ermittelt.

Der Block Cybersicherheit fokussierte sich auf die Bedeutung von Cybersicherheit, anderer relevanter IT-Sicherheitsthemen im Allgemeinen und der Existenz eines Notfallplans für den Umgang mit Cyberangriffen oder Sicherheitsvorfällen im Besonderen.

Im abschließenden Statistikblock wurde noch die Einbindung der Bürgerschaft in die Stadtentwicklungsprozesse hinterfragt sowie das Geschlecht, das Alter und die persönlichen Präferenzen der Teilnehmenden im Hinblick auf technische Neuerungen eruiert.

2.2 Auswahl der befragten Kommunen

Die Befragung richtete sich explizit an Gesamtprojektverantwortliche eines bundesgeförderten Smart-City-Modellprojekts sowie einer im bitkom Smart-City-Index gelisteten Kommune. Bei den Modellprojekten handelt es sich um 73 deutsche Städte, Landkreise und interkommunale Verbünde, die vom Bund seit 2019 in drei Staffeln ausgewählt und mit insgesamt 820 Millionen Euro bezuschusst wurden. Die bitkom-Kommunen sind deutsche Großstädte, die in den firmeneigenen Smart-City-Index inkludiert wurden. Dabei wurde pro Modellprojekt eine Person kontaktiert, bei interkommunalen Projekten wurde eine Person pro geförderter Kommune zur Befragung eingeladen. Insgesamt wurden so 152 Verantwortliche dieser Kommunen zur Teilnahme an der Umfrage aufgefordert, davon stammten rund zwei Drittel aus den Smart-City-Modellkommunen ein Drittel aus nicht bundesgeförderten und damit ausschließlich im bitkom Smart-City-Index gelisteten Kommunen. Die Rücklaufquote betrug rund 14 Prozent.

3 Auswertung

3.1 Screening

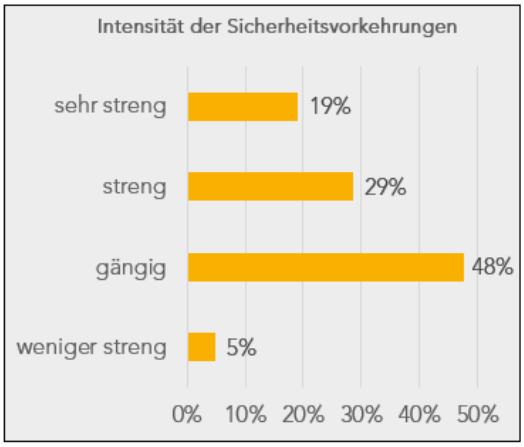
An der Befragung nahmen Projektverantwortliche aus zehn Bundesländern teil, die ihre Projekte hauptsächlich auf kommunaler Ebene (76 Prozent), seltener in interkommunalen Kooperationen (14 Prozent) und Landkreisen (10 Prozent) umsetzen. Die Einwohnerzahl der repräsentierten Kommunen und Kreise verteilte sich auf alle abgefragten Größenklassen, jedoch waren solche mit mehr als 300.000 Bewohner*innen am stärksten vertreten (34 Prozent). Abgesehen von den drei Stadtstaaten waren Smart-City-Projektverantwortliche aus allen Flächenbundesländern außer Rheinland-Pfalz, Mecklenburg-Vorpommern und Sachsen-Anhalt in die Umfrage involviert.

Eine deutliche Mehrheit der erfassten Smart-City-Projekte ist innerhalb der kommunalen Verwaltung organisiert (81 Prozent), andere Organisationsformen wie Gesellschaften mit beschränkter Haftung (GmbH), eingetragene Vereine (e.V.) oder sonstige Formen waren zahlenmäßig geringer vertreten (zusammen 19 Prozent). Die

kommunale Organisationseinheit, in der das jeweilige Smart-City-Projekt verankert ist, variierte sehr stark und umfasste eine Vielzahl an Ämtern, Direktorien, Stabsstellen, Abteilungen und Dezernaten. Nur 41 Prozent dieser Einheiten ließen sich eindeutig Digitalisierungs- und IT-Abteilungen zuordnen, eine Mehrheit von 59 Prozent ist in anderen Abteilungen beheimatet. Im Durchschnitt beschäftigen die befragten Smart-City-Teams Mitarbeitende mit sechs Vollzeitäquivalenten.

3.2 Daten

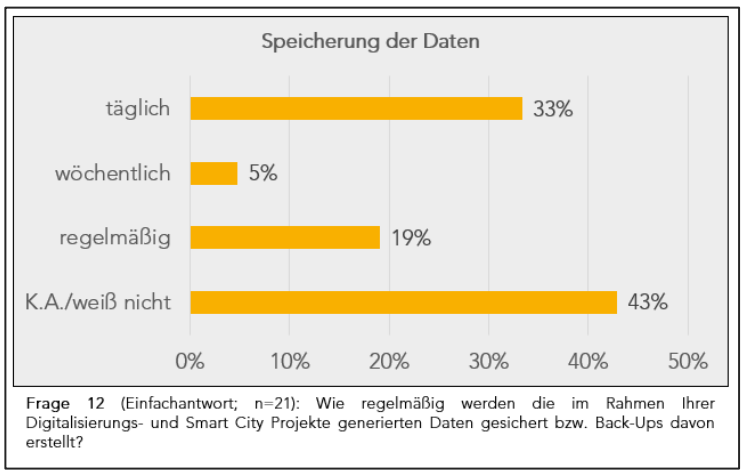
Sämtliche Teilnehmende betonten eine hohe (29 Prozent) bis sehr hohe (71 Prozent) Bedeutung von Datensicherheit und -schutz in ihrer jeweiligen Kommune. Allerdings bezeichnete fast die Hälfte von ihnen die interne Intensität der Sicherheitsvorkehrungen nur als „gängig" (48 Prozent). Nur in 19 Prozent aller Smart-City-Projekte gelten sehr strenge, in 29 Prozent strenge Sicherheitsvorkehrungen.



Frage 10 (Einfachantwort; n=21): Wie streng würden Sie persönlich die angewandten Sicherheitsvorkehrungen zur Erfassung und Verarbeitung von Daten einschätzen, die im Rahmen Ihrer Digitalisierungs- und Smart City Projekte generiert werden?

„Bei der Erfassung und Bearbeitung der Daten aus den Digitalisierungs- und Smart City-Projekten werden… getroffen"

Die Speicherung der im Rahmen der Digitalisierungs- und Smart-City-Projekte generierten Daten findet zu einem großen Teil (67 Prozent) in verwaltungseigenen, lokalen Rechenzentren statt. 38 Prozent speichern die Daten bei einem privatwirtschaftlichen Anbieter und 33 Prozent an einem sonstigen Ort (z. B. bei einem Zweckverband, einem öffentlich-rechtlichen Anbieter oder einer Tochter der Stadtverwaltung). Nur jede fünfte Smart-City-Kommune (19 Prozent) speichert die Daten in einer verwaltungseigenen Cloud.

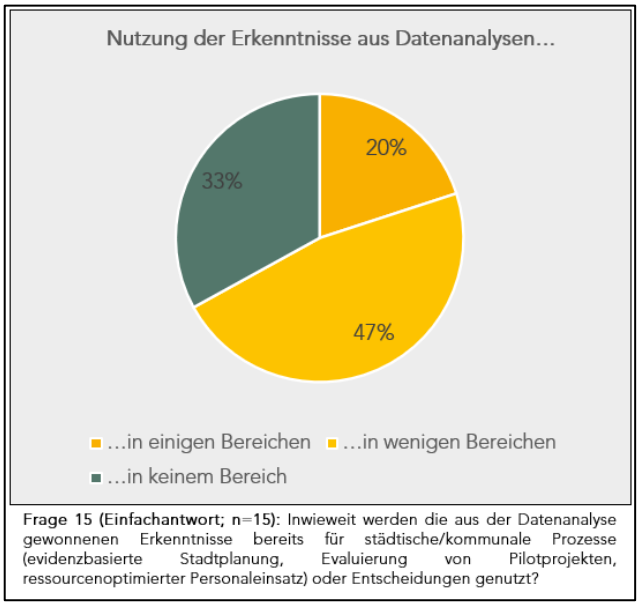


Frage 12 (Einfachantwort; n=21): Wie regelmäßig werden die im Rahmen Ihrer Digitalisierungs- und Smart City Projekte generierten Daten gesichert bzw. Back-Ups davon erstellt?

In jeder dritten Smart-City-Kommune werden die generierten Daten täglich gesichert bzw. Back-Ups erstellt, bei fünf Prozent aller Kommunen findet dies wöchentlich, bei 19 Prozent aller Kommunen zumindest regelmäßig statt. Auffallend ist bei dieser Frage, dass sich 43 Prozent aller Teilnehmenden für die Option „keine Angabe / weiß nicht" entschieden, und die konkreten Zeitpunkte der Datenspeicherung damit bei vielen Projektverantwortlichen unbekannt zu sein scheinen.

71 Prozent aller Smart-City-Projekte analysieren die Daten nach der Erfassung und Speicherung, nur bei jeder zehnten Kommune geschieht dies nicht. Fast die Hälfte aller Smart Cities analysiert die Daten mithilfe von (teil-)automatisierten sowie manuellen Datenanalysen durch kommunale Mitarbeitende (47 Prozent). Zwei von fünf Smart Cities verlagern die Datenanalyse an Externe (40 Prozent).

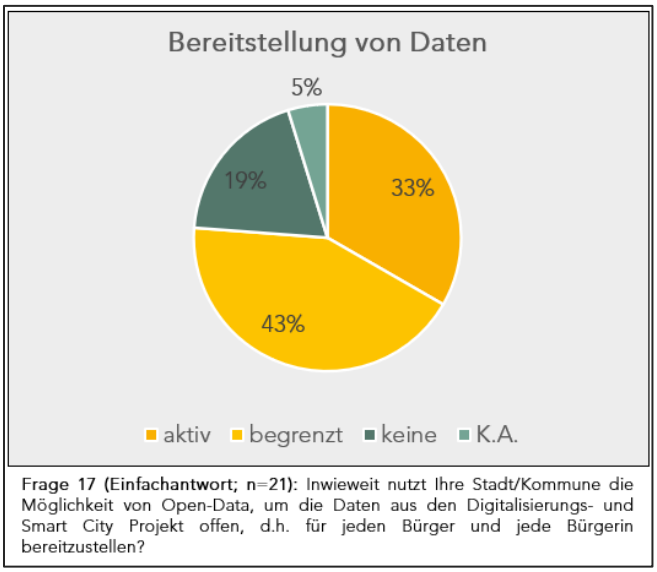
Die Erkenntnisse aus den Datenanalysen werden noch von keiner Smart City vollumfänglich genutzt, vielmehr fokussieren sie sich bei einem Löwenanteil nur auf bestimmte Ressorts.



Frage 15 (Einfachantwort; n=15): Inwieweit werden die aus der Datenanalyse gewonnenen Erkenntnisse bereits für städtische/kommunale Prozesse (evidenzbasierte Stadtplanung, Evaluierung von Pilotprojekten, ressourcenoptimierter Personaleinsatz) oder Entscheidungen genutzt?

So werden die gewonnenen Erkenntnisse von 20 Prozent aller an der Umfrage teilnehmenden Smart Cities in einigen Bereichen genutzt, 47 Prozent verwenden sie explizit nur in wenigen Bereichen. Dabei stehen kommunale Mitarbeitende als Zielgruppe im Fokus: In sämtlichen teilnehmenden Smart Cities gehören sie zur Zielgruppe der aus den Digitalisierungs- und Smart-City-Projekten erhobenen Daten. Aber auch externe Dritte (81 Prozent) und die Bürgerschaft (76 Prozent) werden besonders häufig miteinbezogen.

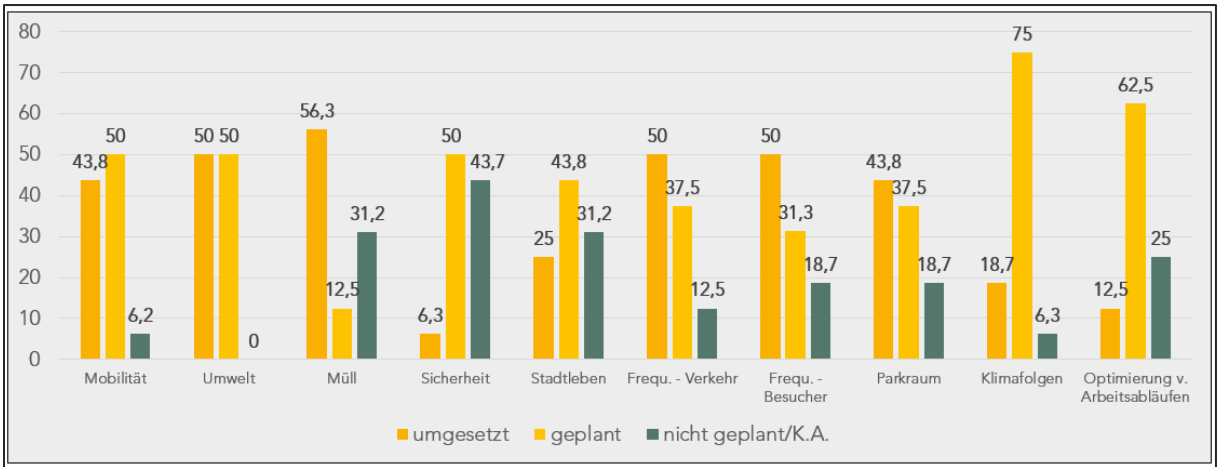
Nur eine von drei Smart Cities in Deutschland nutzt aktiv die Möglichkeit, generierte Daten via Open Data der Bevölkerung vollumfänglich zur Verfügung zu stellen.



Frage 17 (Einfachantwort; n=21): Inwieweit nutzt Ihre Stadt/Kommune die Möglichkeit von Open-Data, um die Daten aus den Digitalisierungs- und Smart City Projekt offen, d.h. für jeden Bürger und jede Bürgerin bereitzustellen?

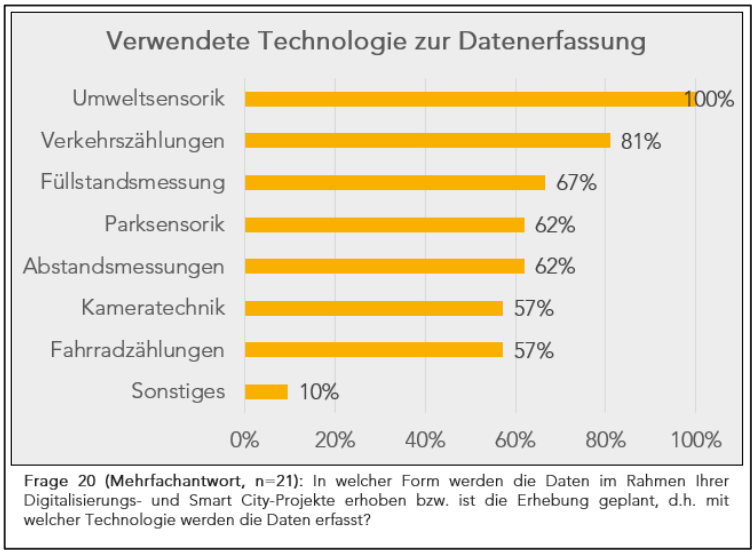
In weniger als der Hälfte der an der Umfrage teilnehmenden Kommunen (43 Prozent) findet dies immerhin in einem begrenzten Rahmen statt. Eine Datenerhebung findet perspektivisch in sämtlichen Smart-City-Kommunen statt: 71 Prozent haben dies bereits umgesetzt, 29 Prozent planen eine Umsetzung.

Bei einer konkreten Aufschlüsselung der Datenerhebungen anhand konkreter Themenfelder ergibt sich ein detaillierteres Bild über den Stand der eingesetzten Sensorik in deutschen Smart-City-Kommunen. So wurden bislang nur Datenerhebungen im Bereich Müllmanagement von einer Mehrheit (56,3 Prozent) der Kommunen erfolgreich realisiert. Zudem hat exakt die Hälfte der erfassten Projekte bereits Sensorik in den Bereichen Umwelt und Frequenzmessungen, sowohl im Verkehr als auch bei den Besucherströmen, implementiert.



Frage 19 (Mehrfachantwort; n=16): In welchen der nachfolgenden Themenfelder bzw. Bereiche werden im Rahmen Ihrer Digitalisierungs- und Smart City-Projekte Daten erhoben?

Verhältnismäßig wenig interessiert sind die befragten Kommunen bislang an Datenerhebungen im Bereich Sicherheit und Stadtleben. Zwar plant jeweils die Hälfte aller Kommunen zukünftige Erhebungen in diesem Themenbereich, 43,7 Prozent (Sicherheit) bzw. 31,2 Prozent (Stadtleben) haben allerdings auch perspektivisch kein Interesse daran.

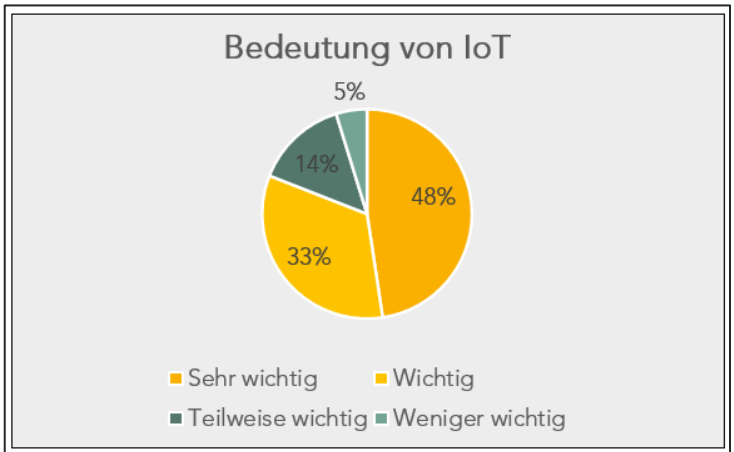


Frage 20 (Mehrfachantwort, n=21): In welcher Form werden die Daten im Rahmen Ihrer Digitalisierungs- und Smart City-Projekte erhoben bzw. ist die Erhebung geplant, d.h. mit welcher Technologie werden die Daten erfasst?

Die Befragten Smart Cities nutzen ein breites Spektrum an Sensorik zur Datenerfassung: So werden flächendeckend Umweltsensoren verwendet, aber auch Sensorik für Verkehrszählungen (81 Prozent), Füllstandsmessungen (67 Prozent), Parksensoren und Abstandsmessungen (62

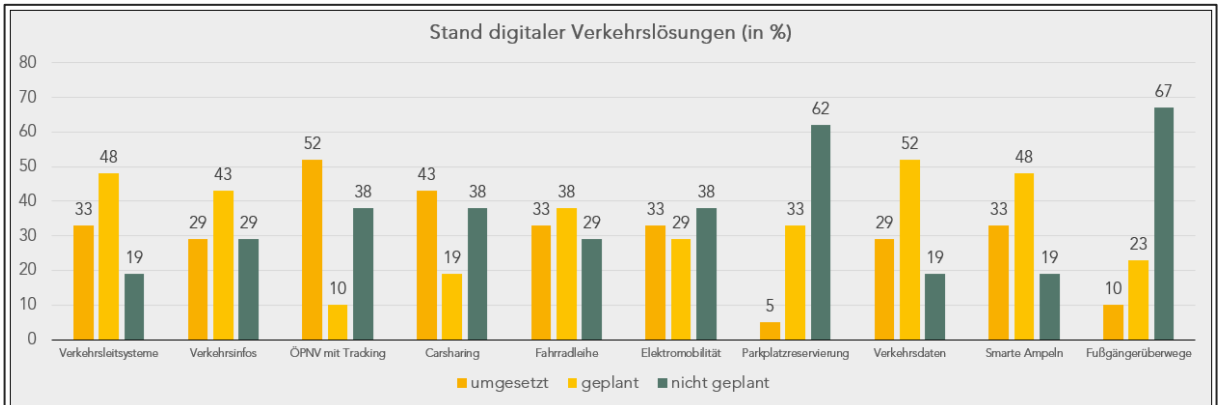
Prozent) sowie Kameratechnik und Fahrradzählungen (57 Prozent) werden von einer Mehrheit der Smart Cities verwendet. Ein Großteil der Datenübertragung findet mithilfe von Mobilfunk und LoRaWAN (jeweils 62 Prozent) statt. Nur eine Minderheit nutzt dafür kabelgebundene Lösungen (33 Prozent), NBIoT (29 Prozent), WLAN (19 Prozent) oder Bluetooth (14 Prozent).

Eine deutliche Mehrheit der Umfrageteilnehmenden erkennt die hohe Bedeutung des Internets der Dinge für die Umsetzung von Smart-City-Projekten an und bezeichnet es als sehr wichtig (33 Prozent) oder wichtig (48 Prozent).



Frage 22 (Einfachantwort; n=21): Einmal unabhängig davon, mit welcher Art von Sensorik die Daten derzeit bereits erfasst werden oder Sie geplant haben diese zu erfassen: wie wichtig ist das Thema IoT für die Umsetzung Ihrer aktuellen oder geplanten Digitalisierungs- bzw. Smart City-Projekte insgesamt?

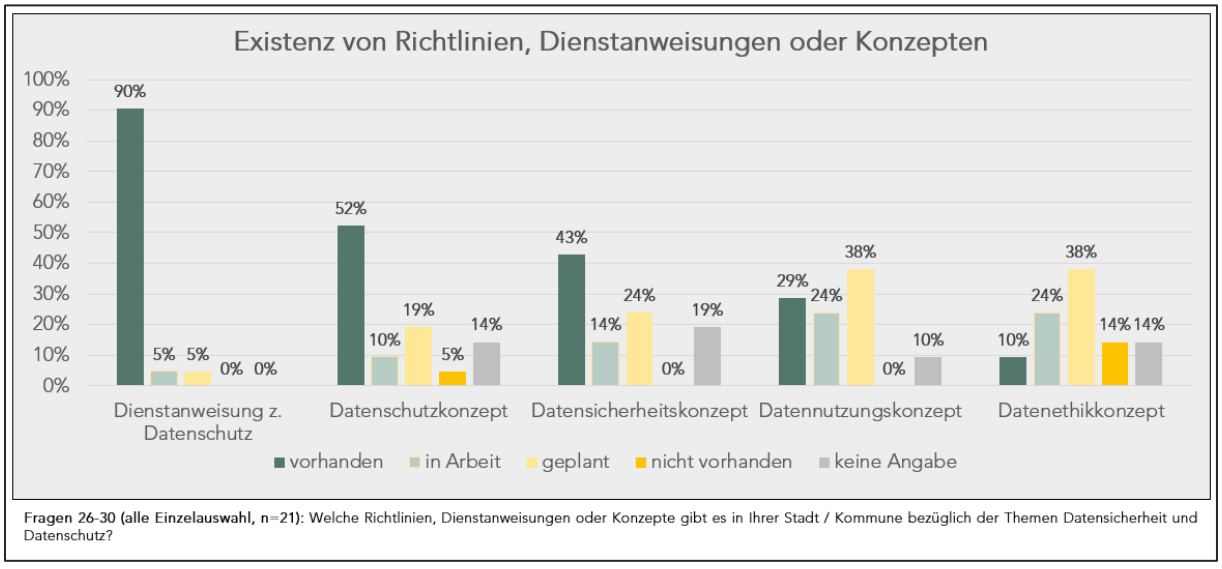
Umweltdaten werden in den untersuchten deutschen Smart Cities hauptsächlich mittels Echtzeiterfassung (71 Prozent), automatisiertem Monitoring (52 Prozent) sowie seltener mit Monitoring durch das Personal (33 Prozent) erfasst.



Frage 24 (Mehrfachantwort; n=21): Welche digitalen Verkehrslösungen werden in Ihrer Stadt/ Kommune genutzt, bzw. sind geplant, um Verkehrsflüsse zu optimieren?

Digitale Verkehrslösungen befinden sich in Deutschland häufig noch in Planung, hierbei insbesondere beim Aufbau intelligenter Verkehrsleitsysteme, bei der Installation smarter Ampeln (beide von 48 Prozent geplant) sowie bei der Verkehrsdatenerfassung (von 52 Prozent geplant).

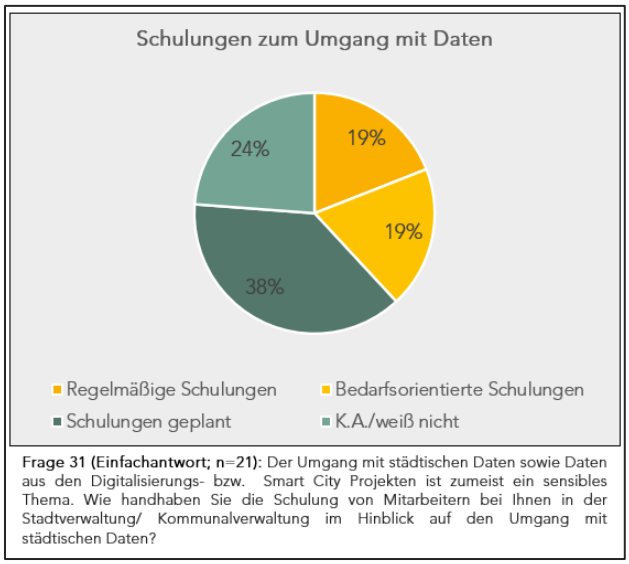
Bislang wurden einzig digitale Tracking-Optionen im öffentlichen Nahverkehr (52 Prozent) von einer Mehrheit der teilnehmenden Kommunen realisiert. Systeme der Parkplatzreservierung und Sensorik an Fußgängerüberwegen spielen hingegen auch mittelfristig kaum eine Rolle und werden von 62 Prozent respektive 67 Prozent aller Kommunen nicht für die Planung in Betracht gezogen. Im konkreten Bezug auf den Öffentlichen Personennahverkehr (ÖPNV) werden primär Verkehrsdaten (33 Prozent), Überwachungssysteme (29 Prozent) sowie Fahrgastdaten, Pünktlichkeitsmessungen und Planungserfassungen (24 Prozent) erhoben.



Fragen 26-30 (alle Einzelauswahl, n=21): Welche Richtlinien, Dienstanweisungen oder Konzepte gibt es in Ihrer Stadt / Kommune bezüglich der Themen Datensicherheit und Datenschutz?

Die an der Befragung teilnehmenden Smart-City-Projekte verfügen fast flächendeckend über Dienstanweisungen zum Datenschutz. Konkrete Konzepte bezüglich der Themen Datensicherheit und -schutz sind hingegen rarer gesät.

So verfügt nur eine knappe Mehrheit der Kommunen (52 Prozent) über ein fertiges Datenschutzkonzept und eine relative Mehrheit über ein Datensicherheitskonzept (43 Prozent). Datennutzungs- und Datenethikkonzepte sind bislang noch häufiger geplant (zu je 38 Prozent) als umgesetzt oder in Arbeit.

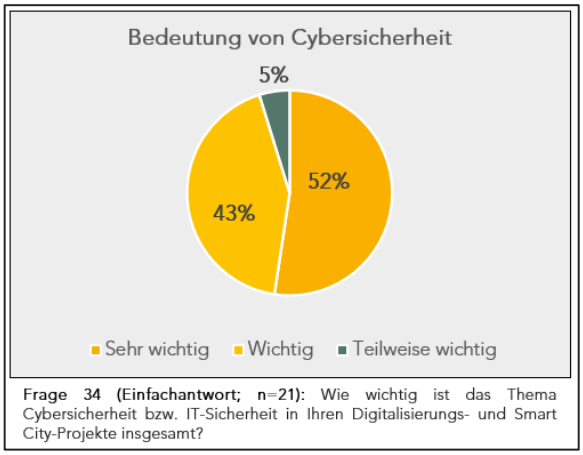


Frage 31 (Einfachantwort; n=21): Der Umgang mit städtischen Daten sowie Daten aus den Digitalisierungs- bzw. Smart City Projekten ist zumeist ein sensibles Thema. Wie handhaben Sie die Schulung von Mitarbeitern bei Ihnen in der Stadtverwaltung/ Kommunalverwaltung im Hinblick auf den Umgang mit städtischen Daten?

Nur eine von fünf deutschen Smart-City-Verwaltungen bietet regelmäßige Schulungen zum Umgang mit Daten an, ebenso viele veranstalten bedarfsorientierte Schulungen zu relevanten Themen (je 19 Prozent). 38 Prozent bieten keinerlei Schulungen an, ebenso zeigt sich fast ein Viertel der Umfrageteilnehmenden unwissend über die Existenz und Durchführungen von Weiterbildungsmaßnahmen.

Insgesamt fast die Hälfte aller Smart Cities (48 Prozent) sucht sich im Rahmen der Datenauswertung Unterstützung durch externe Partner. Die wichtigsten Kriterien bei der Auswahl von externen Partnern sind eine DSGVO-konforme Auswertung der Daten (90 Prozent), Partner, die Daten in Deutschland speichern und verwalten (60 Prozent) sowie wirtschaftliche Gesichtspunkte und eine gute Erreichbarkeit.

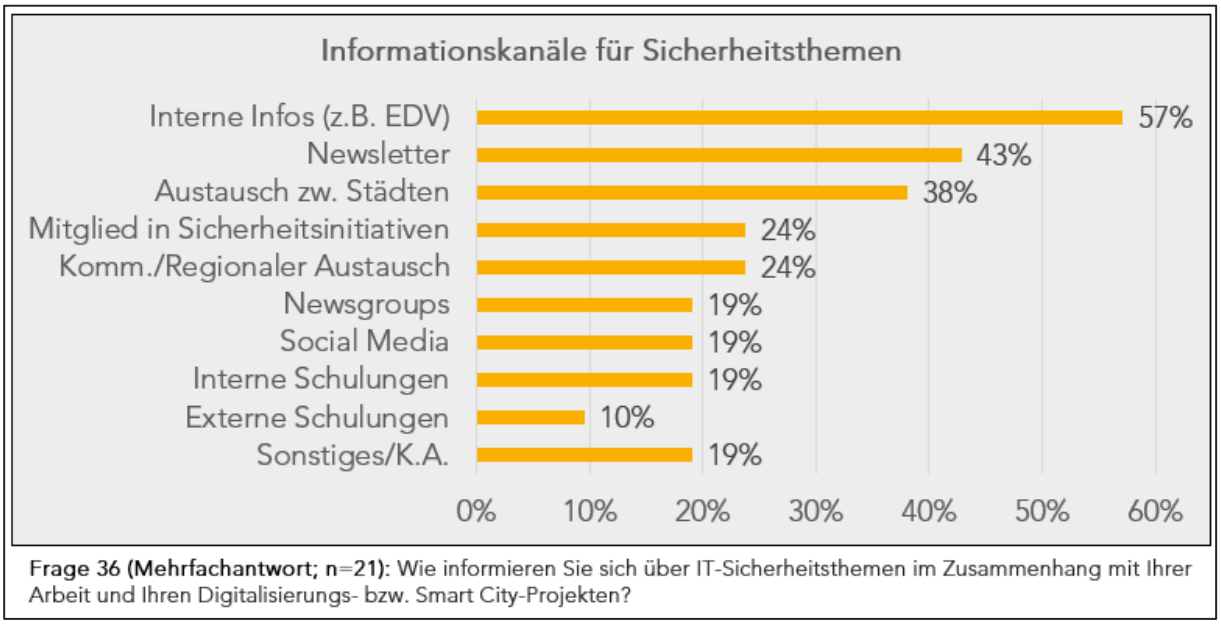
3.3 Cybersecurity



Frage 34 (Einfachantwort; n=21): Wie wichtig ist das Thema Cybersicherheit bzw. IT-Sicherheit in Ihren Digitalisierungs- und Smart City-Projekte insgesamt?

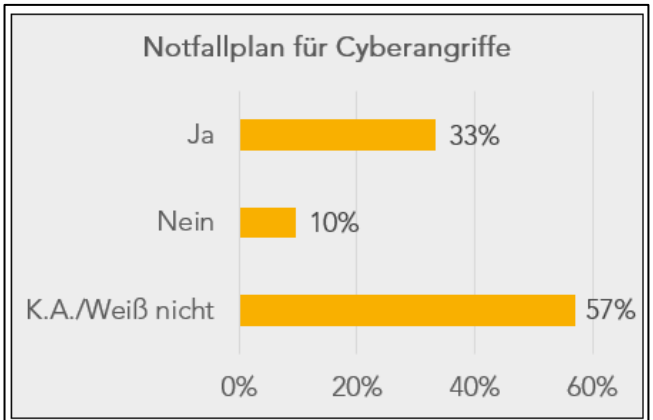
Die Umfrageteilnehmenden sind sich der Relevanz der Cybersicherheit für Smart Cities grundsätzlich bewusst. Knapp über die Hälfte (52 Prozent) von ihnen bezeichneten die Bedeutung von Cybersicherheit bzw. IT-Sicherheit in ihren Digitalisierungs- und Smart-City-Projekten als sehr wichtig, weitere 43 Prozent als wichtig. Dementsprechend informieren sich 14 Prozent aller Smart-City-Gesamtprojektverantwortlichen sehr oft und 43 Prozent regelmäßig über IT-Sicherheitsthemen.

Es gibt ein breites Spektrum an Kanälen, über die sich die Umfrageteilnehmenden über Neuigkeiten zu Sicherheitsthemen informieren. Am häufigsten fungieren hierbei mit 57 Prozent interne Informationen, beispielsweise über die EDV-Abteilungen, Newsletter (43 Prozent) sowie der interkommunale Austausch zwischen den Städten (38 Prozent). 24 Prozent aller Teilnehmenden informieren sich über Sicherheitsinitiativen oder interregionalen Austausch. Newsgroups, Soziale Medien und interne Schulungen werden von 19 Prozent genutzt.

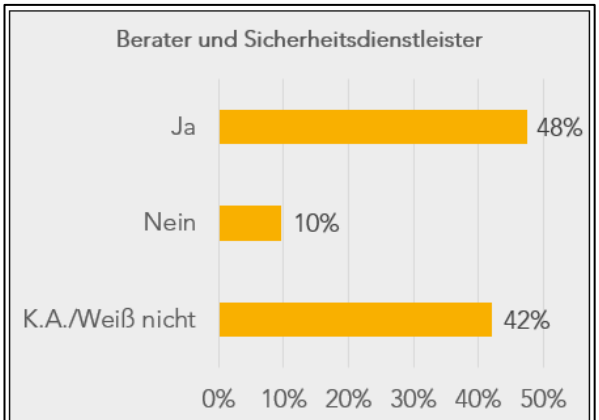


Frage 36 (Mehrfachantwort; n=21): Wie informieren Sie sich über IT-Sicherheitsthemen im Zusammenhang mit Ihrer Arbeit und Ihren Digitalisierungs- bzw. Smart City-Projekten?

*Jede dritte Smart City verfügt über einen Notfallplan für den Umgang mit Cyberangriffen und anderweitigen Sicherheitsvorfällen und fast die Hälfte (48 Prozent) aller Smart Cities setzt externe Berater*innen und andere Sicherheitsdienstleistende ein, um die IT-Sicherheit zu gewährleisten.*



Frage 37 (Einfachantwort; n=21): Verfügt Ihre Verwaltung/ Organisation über einen Notfallplan für den Umgang mit Cyberangriffen oder Sicherheitsvorfällen?



Frage 38 (Einfachantwort; n=21): Werden in Ihrer Stadt/ Kommune Sicherheitsdienstleister oder Berater eingesetzt, um Cybersicherheit bzw. IT-Sicherheit zu gewährleisten?

Zu beachten ist hier allerdings der hohe Prozentsatz an „Weiß nicht"-Angaben mit 57 Prozent (Cyberangriffe) und 42 Prozent (Dienstleister).

Die Smart-City-Projekte stellen ihren Bürger*innen eine Vielzahl unterschiedlicher Plattformen zur Kommunikation zur Verfügung. 71 Prozent verwenden eine Beteiligungsplattform, 67 Prozent arbeiten mit Online-Umfragen oder einem Bürgerportal, etwas mehr als die Hälfte (52 Prozent) nutzt die Sozialen Medien und 29 Prozent mobile Anwendungen.

3.4 Statistik

Ein Großteil der Umfrageteilnehmenden war männlich (76 Prozent), zwischen 30 und 59 Jahre alt (80 Prozent) und ausgiebig interessiert oder aufgeschlossen gegenüber technischen Neuerungen (90 Prozent).

4 Ableitungen aus den Experteninterviews

Aufbauend auf den Ergebnissen der Befragung wurden vertiefende Leitfadeninterviews mit Expertinnen und Experten durchgeführt. Hauptziel Die interviewten Personen wurden aus einer Liste an Smart City-Modellkommunen sowie anderer relevanter Smart City-Projekte repräsentativ ausgewählt. Mithilfe des Leitfadens wurden rund ein Dutzend Interviews mit Projektverantwortlichen in Smart Cities durchgeführt, deren Kommunen sich über das ganze Bundesgebiet erstreckten.

4.1 Übersicht über die in der Verwaltung vorliegenden Datensätze

Die bloße Übersicht über die in der Verwaltung im Rahmen einer Smart-City-Strategie generierten und vorliegenden Datensätze ist in den meisten befragten Kommunen nicht gegeben. Nur ein Experte bejahte die Frage nach dem Überblick, fügte aber ebenfalls hinzu, dass die stetige Zunahme der Datensätze eine große Herausforderung ist. Ansonsten muss eine differenzierte Betrachtung angelegt werden. So ist etwa in einer Kommune die fachbereichsübergreifende Übersicht über die Datensätze „undurchsichtig", während die Fachbereiche ihre spezifischen Daten kennen. Es wird dabei angemerkt, dass Datensätze mehrfach erhoben werden, weil die Fachbereiche nicht wissen, dass ihre Kolleginnen und Kollegen dieselben Sätze zuvor schon erhoben haben. Andere geben an, dass zwar „ein Gefühl für die Daten" vorhanden, eine tatsächliche Übersicht jedoch nicht gegeben ist. Grundsätzliche Zuständigkeiten fehlen häufig. Eine interviewte Person gab an, dass das Projektteam keine Übersicht hat, „gegebenenfalls aber der Fachbereich IT". In anderen Projekten erfolgt keine Absprache, da häufig mit Externen kooperiert wird, die jedoch auch nicht bekannt sind.

Handlungsempfehlung: Daten zusammenfassen und Silos aufbrechen

Die Bündelung von Datensätzen und das Aufbrechen von Datensilos sind die ersten und relevantesten Schritte hin zu einer aktiven Daten- und Cybersicherheit. Eine gesamtheitliche Überführung der Daten unter ein Dach verhindert nicht nur Mehrfacherhebungen, sie beucht auch potenziellem Datenverlust sowie Angriffe auf ungeschützte Datensätze vor.

4.2 Stellenwert der Daten- und Cybersicherheit bei der Konzeption von Smart-City-Umsetzungsprojekten

Der Stellenwert von Themen der Daten- und Cybersicherheit bei der Konzeption von Smart-City-Umsetzungsprojekten wird von sämtlichen Interviewpartnern als hoch angesehen. Daten- und Cybersicherheit werden stets mitgedacht und iterativ weiterentwickelt, Datenschutz und Informationssicherheit werden bei der Konzeption in den „Loop" genommen. Perspektivisch erwarten die Interviewten einen enormen Arbeitsaufwand für die Zukunft sowie eine verstärkte Rolle der Thematik bei Ausschreibungen. Auch Partner sind durch die Smart-City-Projekte aufmerksamer geworden und planen die Umsetzung einer Cyber-Versicherung. Auch das Thema Datenhaltung nimmt einen hohen Stellenwert ein, insbesondere im Kontext der angedachten Urbanen Datenplattformen sowie neuer dynamischer Daten aus Sensorik-Anwendungen. Allerdings wird auch die hohe „Diskrepanz zwischen Theorie und Praxis" betont. Außerdem wurde hierbei der „Unterschied zwischen Anspruch und Wirklichkeit moderner Arbeitsbedingungen" moniert.

4.3 Fragestellungen im Use-Case-Design

Große Differenzen ergeben sich bei den Befragten im Kontext der Berücksichtigungen der Sicherheitsfragen im Use-Case-Design. Für manche Teilnehmende war das Themenfeld nicht relevant, andere gaben knapp eine Use-Case abhängige Betrachtung an. Die Vertreterin einer Kommune sagte, dass die Fragestellungen im Use-Case-Design formal noch nicht berücksichtigt werden. Vielmehr entwickelt das Smart-City-Team die Use-Cases zusammen mit den Fachbereichen, wobei die

Schwerpunkte zunächst auf den Funktionalitäten liegen. Andere Teams sind noch ganz am Anfang und wollen diese Thematik zukünftig berücksichtigen.

Handlungsempfehlung: Verantwortlichkeiten benennen

In sämtlichen Firmen und Organisationen der öffentlichen Verwaltung sind Datenschutzbeauftragte längst Pflicht geworden. Dies sollte auch bei Smart City-Projektteams die Norm werden, insbesondere, wenn sich ein Projekt in der Umsetzungsphase befindet. Es bietet sich an, sowohl eine fest verantwortliche Person als Ansprechpartner für Datensicherheitsfragen zu benennen, aber auch eine stellvertretende Person, die über genügend Fachkompetenz verfügt, um als Vertretung zu fungieren.

4.4 Kompetenzen der Teams in Bezug auf Cybersicherheit

Die Kompetenzen der Teams im Bezug auf Cybersicherheit unterliegen starken Schwankungen, die stark an die Größe der Teams sowie der Gebietskörperschaften gekoppelt zu sein scheinen. Generell sind viele Smart-City-Projekte zu einem hohen Grad von Know-how und Kompetenzen externer Dienstleister abhängig. Andere Kommunen hängen dagegen stark von Fachpersonen aus ihren Verwaltungen ab: Ein Projektteam nutzt den IT-Sicherheitsbeauftragten als Sparringspartner, eine andere Kommune hat eine Datenanalystin im Team. Eine Kommune gibt offen und ehrlich zu, dass bei den internen Kompetenzen noch „Luft nach oben" herrscht, eine weitere attestiert ihren Teammitgliedern „angelerntes Wissen". Beim Ausreizen dieses Wissens erfolgt ein Rückgriff auf das Know-how der Informations- und Kommunikationsabteilung, es herrsche aber auch ein Vertrauen in diese. Ein gemeinsamer Tenor ist, dass zumindest die Grundlagen im Team vorhanden sind, bei übergeordneten und/oder tiefergreifenden Fragestellungen aber stets auf Akteure außerhalb des Projektteams zurückgegriffen werden muss. Häufig sind die Teams relativ klein, sodass man zwangsweise auf Externe angewiesen ist und diese schon allein aus Kapazitätsgründen ins Boot holen muss.

Handlungsempfehlung: Kompetenzen inhouse aufbauen

Die Ergebnisse der Befragung sowie insbesondere der Interviews mit Expertinnen und Experten aus den Smart City-Projektteams zeigt deutlich eine gewisse Abhängigkeit zu Akteuren außerhalb der Teams bei Datenschutzfragen auf, und zwar sowohl zu den hausinternen IT-Abteilungen als auch zu externen Dienstleistern. Der Kompetenzaufbau innerhalb des Teams stärkt nicht nur die Kompetenzen des gesamten Teams bei Fragen der Daten- und Cybersicherheit, er verkürzt im Ernstfall auch die Reaktionszeit auf Bedrohungen.

4.5 Aufbau von Kompetenzen in den Teams und in den Verwaltungen

Der Aufbau von teaminternen Kompetenzen in Bezug auf Cybersicherheit wird von den interviewten Fachleuten variabel gehandhabt und unterscheidet sich stark von Kommune zu Kommune. Insbesondere beim Vorhandensein von Online-Schulungen zum Thema unterliegen die Antworten starken Schwankungen im Bezug auf die Größe der Gebietskörperschaft bzw. der Verwaltung. In einigen Kommunen wird „Awareness" in Bezug auf Sicherheitsthemen in Form von Schulungen geschaffen. Andere bieten keine Online-Schulungen an, sondern vertrauen weiterhin auf das Know-how von externen Dienstleistern, IT-Abteilungen und Datenschutzbeauftragten und planen keinen Kompetenzaufbau innerhalb des Teams. Viele Projektleiterinnen und -leiter betonen die zukünftig hohe Bedeutung von Online-Schulungen und Workshops zum Thema Cybersicherheit. Eine Verwaltung plant den Beginn solcher Schulungen für das Ende der Förderperiode im Jahr 2027 ein. Eine andere Kommune setzt den Fokus auf Sensibilisierung, wiederum eine andere auf die Vereinheitlichung der Systeme. Prozesse sollen aufgezeigt und fortlaufend bewertet werden. In einer Kommune wird zwar Wissen über Cybersicherheit und Datenschutz bei der Smart-City-Arbeitsgruppe aufgebaut, dieser Wissensaufbau ist aber nicht in der restlichen Personalentwicklung der Stadt verankert.

Handlungsempfehlung: Schulungen als Schlüssel zum Erfolg

Die Ergebnisse der Befragungen und Interviews zeigen deutlich, dass Online-Schulungen zur Daten- und Cybersicherheit noch nicht von allen Smart City-Projekten vollumfänglich wahrgenommen werden. Sie stellen aber das wichtigste Mittel dar, um zeit- und kostengünstig größtmögliches Know-how aufzubauen. Daher bietet es sich an, diese regelmäßig allen Mitarbeitenden zur Verfügung zu stellen und den Verantwortlichen auch zusätzliche fachintensivere Formate anzubieten. Selbstverständlich eignen sich dazu auch Workshops und Schulungen in Präsenzformaten.

4.6 Cybersicherheit bei der Ausschreibung von Hard- und Softwarekomponenten

Die Fragestellungen der Daten- und Cybersicherheit werden von fast allen interviewten Personen bei Ausschreibungen berücksichtigt. In einigen Kommunen gibt es Vorgaben seitens des IT-Zentrums, andere beschränken sich auf das jeweilige Leistungsverzeichnis. In einer Kommune wird das Thema als „geübte Praxis" bezeichnet. Verschlüsselte Verbindungen sind aktuell abhängig von den Anforderungen. Ein Partner erwähnte die Beteiligung eines IT-Sicherheitsbeauftragten bei Ausschreibungen sowie die frühzeitige Einbindung in das Projektdesign sowie in die Use-Case-Konzeption. Kommunen inkludieren die Fragestellungen in die Ausschreibungen, denn diese sind laut Smart-City-Förderung Pflicht.

4.7 Richtlinien, Dienstanweisungen und Konzepte zu Datenschutz und -sicherheit

Besonders steht in vielen Projektgruppen das Thema Datenstrategie im Vordergrund. Ein Interviewpartner bezeichnet die schriftlichen Anweisungen als „umfangreich". Es werden dennoch einige offene Flanken angesprochen: Viele der Unterlagen sind in den hauseigenen Intranets abgelegt, diese müssen häufig selbst recherchiert werden und sind wohl auch nicht in standardmäßige Prozesse miteingebunden. Eine Person

erwähnte, dass neue Mitarbeitende „eventuell über das Onboarding sensibilisiert werden". Datenethikkonzepte sind bislang kaum vorhanden, viele der Interviewpartnerinnen und -partner betonen aber die immens zunehmende Bedeutung solcher Konzepte für Smart-City-Strategien. Übergeordnetes Ziel für die Befragten sind „atmende" Dokumente, die kontinuierlich erweitert werden und auf die jüngsten Trends miteingehen können: Die gegenwärtigen technischen Innovationstrends (z. B. Künstliche Intelligenz) sind zu schnelllebig, um immer aktuell festgehalten zu werden.

Handlungsempfehlung: Konzepte sichtbar machen und proaktiv vermitteln

Datenschutzkonzepte, Dienstanweisungen und andere relevante Dokumente „verstecken" sich offensichtlich noch viel zu häufig im hauseigenen Intranet oder werden von den zuständigen Abteilungen nicht klar genug kommuniziert. Die Inhalte dieser Konzepte und Richtlinien sollten jedoch für alle Mitarbeitende möglichst barrierefrei zur Verfügung gestellt und auch außerhalb des Onboarding-Prozesses laufend vermittelt werden. Ziel sollte auch die Erstellung von passgenauen, „atmenden" Konzepten sein, die aktuelle Trends berücksichtigen und laufend aktualisiert werden.

4.8 Größte Herausforderungen für die Umsetzung von cybersicheren Smart-City-Projekten

Die größten Herausforderungen im Bezug auf die Umsetzung von cybersicheren Smart City-Projekten sehen die interviewten Personen in den folgenden Feldern:

- Aufbau von Kompetenzen („Der Wille ist grundlegend vorhanden")
- Erstellung von Leistungsverzeichnissen trotz „Technik-Unkenntnis"
- föderale Struktur Deutschlands und damit einhergehende Unklarheiten hinsichtlich rechtlicher Rahmenbedingungen
- mangelnde Anonymisierung von Daten
- fehlende Absicherung des Gesamtsystems
- hohes Konfliktpotenzial zwischen Cybersicherheit und kommerziellen Interessen
- kontraproduktive politische Entscheidungen
- Schaffung von Routinen und Strukturen und die Etablierung von Standards als Basis für Ausschreibungen

Zusätzlich werden die mangelnden Personalkapazitäten in den Kommunen thematisiert, die verhindern, dass Maßgaben in die Fläche gebracht werden. Die Abhängigkeiten von externen Dienstleistern seien nicht immer die beste Lösung, entscheidend sei vielmehr ein Grundverständnis auf allen Ebenen.

Handlungsempfehlung: Von rechtlichen Rahmenbedingungen nicht verunsichern lassen

Rechtliche Rahmenbedingungen, insbesondere im Kontext der föderalistischen Struktur Deutschland mit uneinheitlichen, variierenden Gesetzgebungen machen eine enorme Herausforderung aus. Es gilt hierbei, sich auf eindeutige Anforderungen aus Förderungen zu fokussieren und eventuelle Lücken und offene Flanken proaktiv zu schließen.

5 Zusammenfassende Analyse

Die Befragungsergebnisse geben Aufschluss über den Status quo zum Thema Cybersicherheit in deutschen Smart-City-Kommunen. Sie legen die aktuelle Bestandssituation offen, zeigen aber auch deutlich die Herausforderungen und offenen Flanken, mit denen sich Kommunen in Deutschland bei der Umsetzung konfrontiert sehen.

Zwar betonen die Projektverantwortlichen die hohe theoretische Bedeutung von Cybersicherheit bei der Umsetzung ihrer Smart-City-Projekte, allerdings zeigte sich eine Vielzahl der Umfrageteilnehmenden über zahlreiche sicherheitsrelevante Themen weitestgehend uninformiert.

Besonders das große Unwissen über das Vorhandensein von Notfallplänen zu Cyberangriffen sowie über den Einsatz externer Sicherheitsdienstleistender oder Berater*innen deutlich, dass die enorme Bedrohung durch Cyberattacken mit all ihren potenziell katastrophalen Auswirkungen noch nicht überall erkannt und dementsprechend priorisiert wird. Das Thema Cybersicherheit ist zwar in den Kommunen präsent, aber besitzt offensichtlich noch nicht die allerhöchste Priorität.

Durch Sensorik werden zwar bereits reichlich Daten generiert und gesichert, dies allerdings noch nicht mit vollem Nutzen für die Bevölkerung.

Anweisungen zu Datenschutz und -sicherheit sind kaum innerhalb einer Kommune geregelt, insbesondere das Fehlen konkreter Konzepte zu diesem Themenfeld stellt einen erheblichen Nachteil für die Smart-City-Kommunen dar (Fragen 26-30.). In diesem Hinblick bedarf es einer weitaus größeren Transparenz und Weitsichtigkeit. Kommunen müssen schon in der Konzeptions-, spätestens aber in der Umsetzungsphase eines Smart-City-Projektes konkrete Überlegungen darüber anstellen, wie dies für die Dauer des Projektes, insbesondere aber auch darüber hinaus, geregelt sein wird.

Die Umfrage zeigt ebenso, dass sich die Datenerhebungen und Messungen durch Sensorik bislang stark auf die Handlungsfelder Mobilität, Umwelt, Müllmanagement und Frequenzmessungen fokussieren. Besonders bei den Dimensionen Sicherheit und Ordnung sowie bei der Steigerung der Attraktivität des Stadtlebens werden die Potenziale der Sensorik noch nicht erkannt bzw. noch nicht genutzt. Auch die Datenschutzfragen treten hierbei noch in den Hintergrund. Aktuell werden Daten in Themenfeldern erhoben, die datenschutzrechtlich wenig relvant sind (z. B. Mülleimer). Dabei bilden die hier etablierten Standards und IT-Architekturen die Grundlage für die Entwicklung und Integration weitere Anwendungsfälle in der Zukunft. Das heute gewählte Design stellt also die Grundlage für die IT- und Cybersichere Ausgestaltung der Smart City Ökossysteme von morgen dar.

Im Bereich Cybersicherheit sind nur selten Verknüpfungen zu privatwirtschaftlichen Akteuren aufgebaut, von deren Know-how man profitieren und Synergieeffekte entwickeln könnte.

Trotz der omnipräsenten Bedeutung, die dem Konzept „Smart City" bzw. „Smart Region" mittlerweile zugerechnet wird und die sich in Bundesförderungen wie dem Smart-City-Modellkommunenprogramm widerspiegelt, sind diese bislang noch immer nicht vollends in der Breite angekommen und führen teilweise noch ein Nischendasein, das mit einem Konzept abgewickelt wird und anschließend nur eine Nebenrolle bei der fortlaufenden Stadtentwicklung innehat. Behörden wie das Bundesamt für Sicherheit in der Informationstechnik können die Kommunen dazu befähigen, ermutigen und inspirieren, Strukturen im Bereich von Datenschutz und -sicherheit aufzubauen, um Folgeprobleme zu vermeiden und resilientere und krisensicherere Smart-City-Strukturen zu etablieren.