



CYBERSICHERHEIT IN DEUTSCHEN SMART CITIES

Status quo und Handlungsfelder für die Zukunft

Arbeitspapier

Impressum

Herausgeber

Zentrum für Digitale Entwicklung GmbH

Projektkoordination

Zentrum für Digitale Entwicklung GmbH

Fachliche Betreuung, Konzept und Redaktion

Fachliche Betreuung: Felix Unseld, Carina Nitschke

Konzept: Felix Unseld, Carina Nitschke, Bastian Hiergeist

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

Stand

05/2024

Inhalt

0	Executive Summary	1
1	Einleitung	1
2	Die Befragung	3
2.1	Der Fragebogen	4
2.2	Auswahl der befragten Kommunen / Laufzeit	5
3	Auswertung	6
3.1	Screening	6
3.2	Daten	7
3.3	Cybersecurity	13
3.4	Statistik	15
4	Zusammenfassende Analyse	15

0 Executive Summary

Im Rahmen des 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 Gesamtprojektverantwortliche 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 den Smart-City-Modellkommunen zu erhalten. Die Ergebnisse erlauben einen interessanten Einblick in den Stand, den Umgang und die Entwicklungspotenziale von IT-sicherheitsrelevanten Themen in der deutschen Smart-City-Landschaft.

Das vorliegende Arbeitspapier beschränkt sich bislang auf die quantitativen Aspekte der Umfrage. Eine um die qualitativen Erkenntnisse ergänzte Fassung wird schon bald in Form eines ausführlicheren Whitepapers erscheinen.

1 Einleitung

An jedes Smart-City-Projekt ist die Vision gekoppelt, den urbanen 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 verbessern.

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 miteinzubeziehen.

Cyberangriffe auf digitale Infrastrukturen oder sonstige technische Probleme in ebenjenen können zukünftig gravierende Einschränkungen bei der Versorgung mit lebenswichtigen Gütern und Dienstleistungen 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 Bürgerbeteiligung. Auch auf die für Smart City essentiellen 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 unverändert hoch. Nachdem in der Vergangenheit hauptsächlich privatwirtschaftliche Unternehmen im Fokus dieser Angriffe standen, gerät zunehmend die öffentliche Verwaltung ins Visier der Angreifer. Die größte Herausforderung im Bereich Cybersicherheit besteht für die Kommunalverwaltungen darin, die verschiedenen Funktionsebenen einer Smart City bestmöglich zu schützen und ihre Funktionsfähigkeit 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. Die Integration in einem gemeinsamen, interoperables System stellt auch aus Cybersicherheitsperspektive eine bedeutsame Herausforderung dar. Je komplexer die zugrundeliegende Datenarchitektur gestaltet wurde, desto komplexer ist es, sie zu schützen.

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 Personen 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 abfragen sollte und damit ein konkretes Bild der aktuellen Situation in den Städten und Regionen zeichnet.

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), dem 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 sowie die persönlichen Präferenzen der Teilnehmenden im Hinblick auf technische Neuerungen eruiert.

2.2 Auswahl der befragten Kommunen / Laufzeit

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 Verbunde, 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 zu der Umfrage eingeladen, davon stammten 102 Personen aus den Smart-City-Modellkommunen und 50 aus bitkom-Kommunen. Die Rücklaufquote betrug 13,8 Prozent.

Nach der Einspeisung und Programmierung der Fragen wurde die Befragung im November 2023 veröffentlicht und an die ausgewählten und kontaktierten Kommunen versandt. Die Umfrage war vier Wochen online und wurde am 20.12.2023 geschlossen.

3 Auswertung

3.1 Screening

Bei 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.

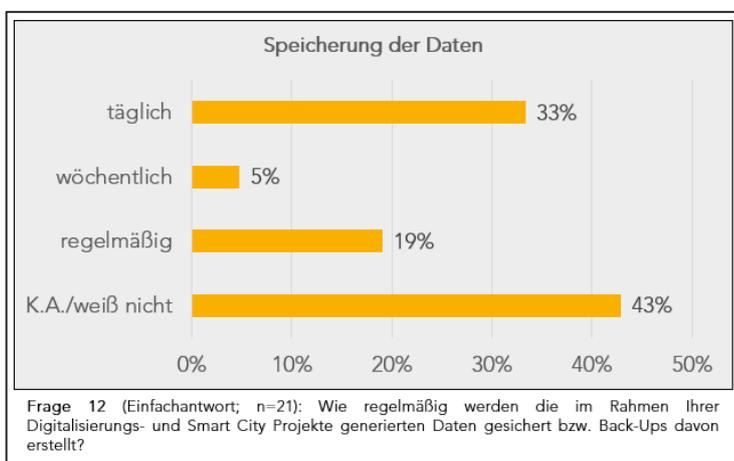
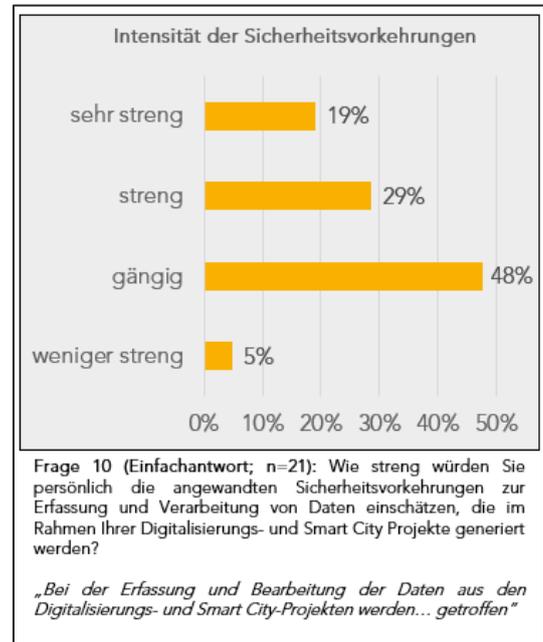
Eine deutliche Mehrheit der erfassten Smart-City-Projekte ist innerhalb der kommunalen Verwaltung organisiert (81 Prozent), andere Organisationsformen wie Gesellschaften mit beschränkter Haftung (GmbH), eingetragene Vereine oder sonstige Formen waren zahlenmäßig geringer vertreten (zusammen 19 Prozent).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

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.



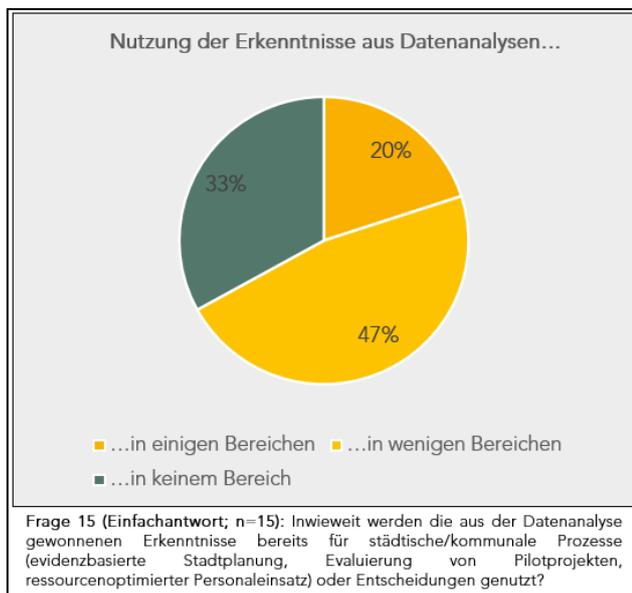
In jeder dritten Smart-City-Kommune werden die generierten Daten täglich gesichert bzw. Back-Ups erstellt, bei fünf Prozent aller Kommunen findet dies wöchentlich, bei 19 Prozent aller Kommunen zumindest regelmäßig statt. Auffallend ist bei dieser Frage, dass sich 43 Prozent

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).

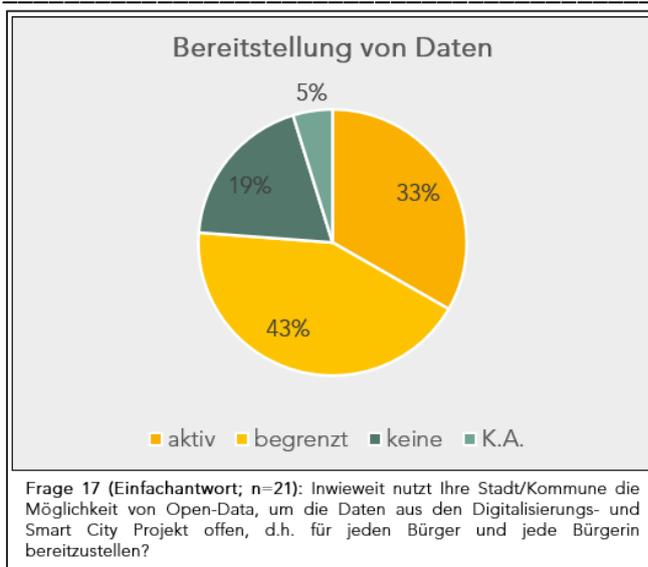
Die Erkenntnisse aus den Datenanalysen werden noch von keiner Smart City vollumfänglich genutzt, vielmehr fokussieren sie sich bei einem Löwenanteil nur auf bestimmte Ressorts.



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

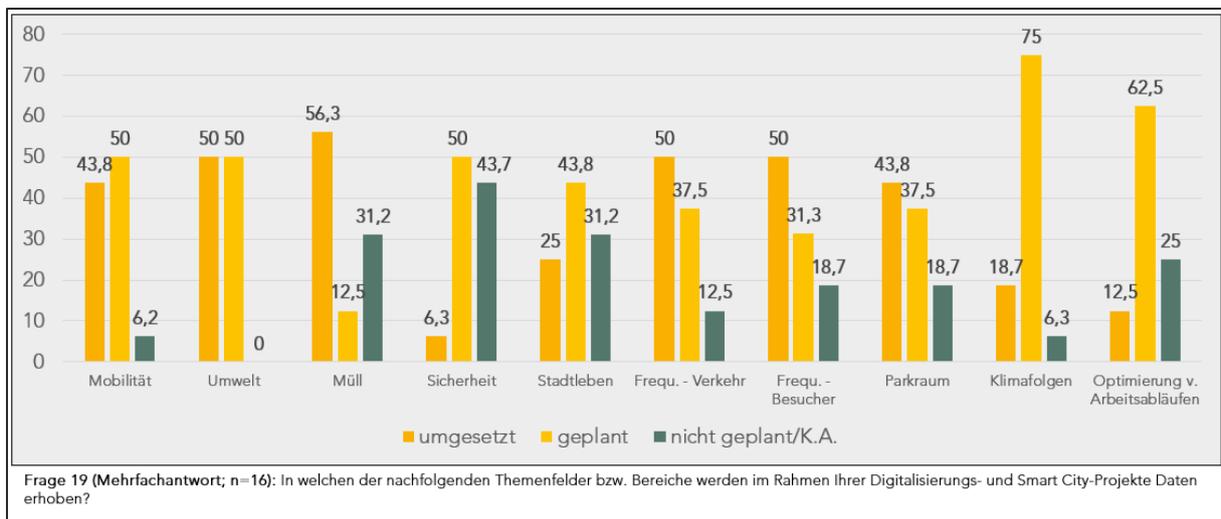
Dritte (81 Prozent) und die Bürgerschaft (76 Prozent) werden besonders häufig miteinbezogen.

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



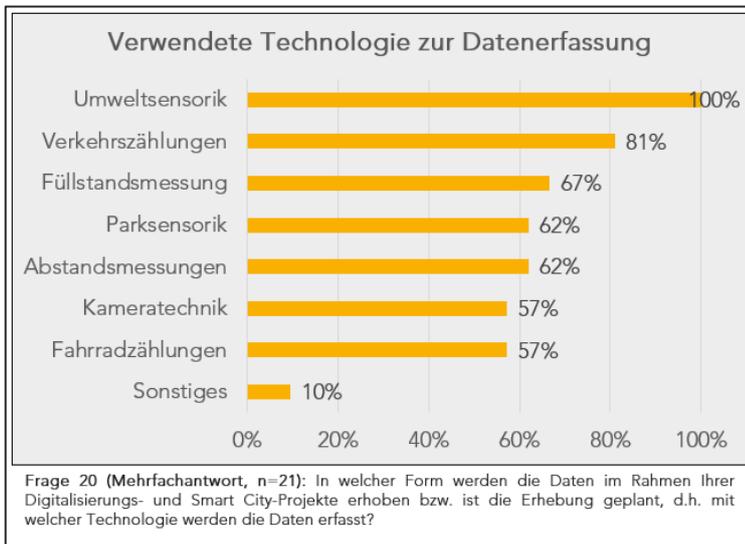
In weniger als der Hälfte der an der Umfrage teilnehmenden Kommunen (43 Prozent) findet dies immerhin in einem begrenzten Rahmen statt. Eine Datenerhebung findet perspektivisch in sämtlichen Smart-City-Kommunen statt: 71 Prozent haben dies bereits umgesetzt, 29 Prozent planen eine Umsetzung.

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.



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

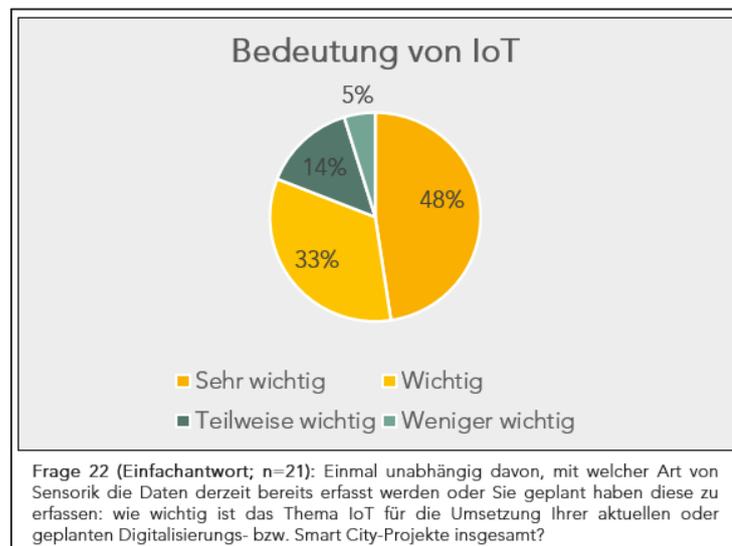
(Sicherheit) bzw. 31,2 Prozent (Stadtleben) haben allerdings auch perspektivisch kein Interesse daran.



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

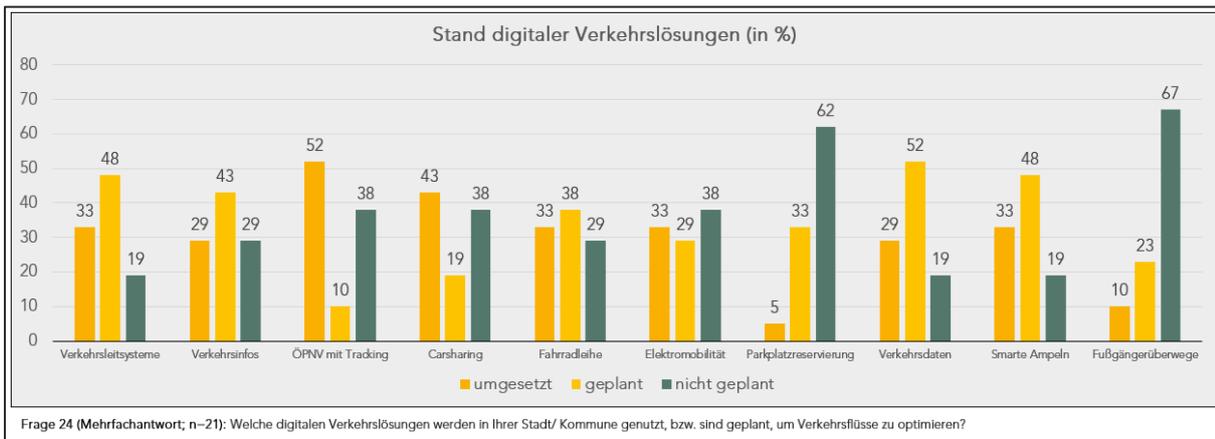
Prozent) sowie Kameratechnik und Fahrradzählungen (57 Prozent) werden von einer Mehrheit der Smart Cities verwendet. Ein Großteil der Datenübertragung findet mithilfe von Mobilfunk und LoRaWAN (jeweils 62 Prozent) statt. Nur eine Minderheit nutzt dafür kabelgebundene Lösungen (33 Prozent), NBloT (29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

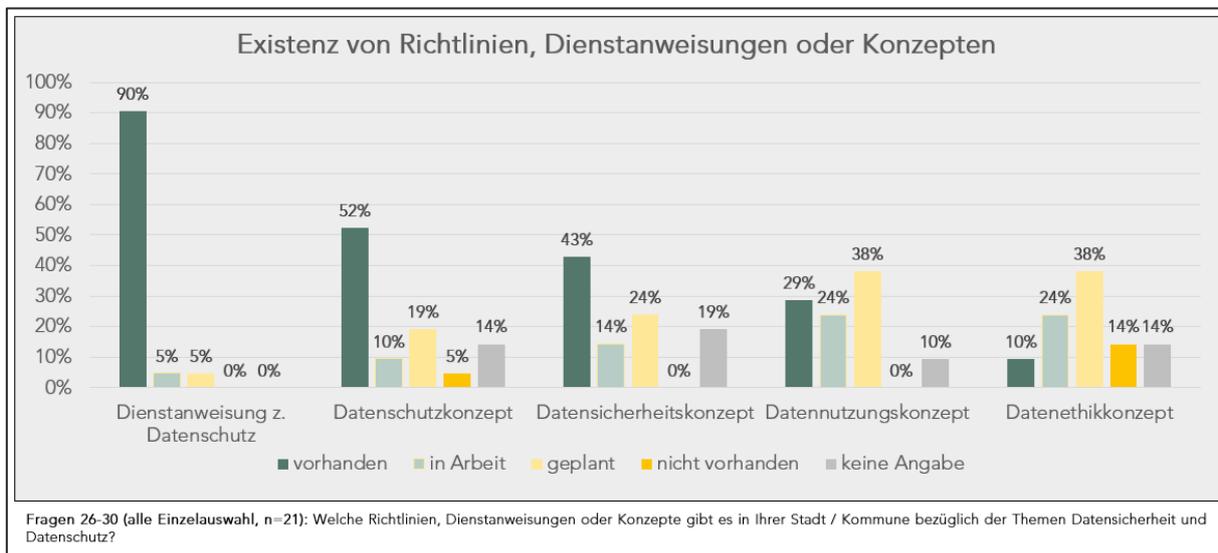


Umweltdaten werden in den untersuchten deutschen Smart Cities hauptsächlich mittels Echtzeiterfassung (71 Prozent), automatisiertem Monitoring (52 Prozent) sowie seltener mit Monitoring durch das Personal (33 Prozent) erfasst.

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).



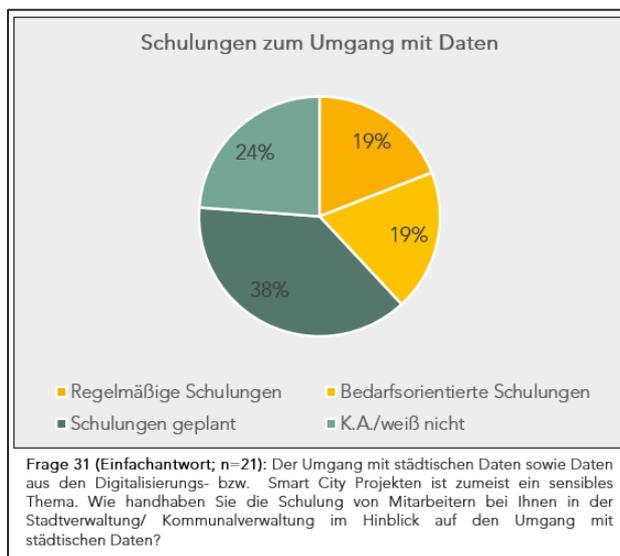
Bislang wurden einzig digitale Tracking-Optionen im öffentlichen Nahverkehr (52 Prozent) von einer Mehrheit der teilnehmenden Kommunen realisiert. Systeme der Parkplatzreservierung und Sensorik an Fußgängerüberwegen spielen hingegen auch mittelfristig kaum eine Rolle und werden von 62 Prozent respektive 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.

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.

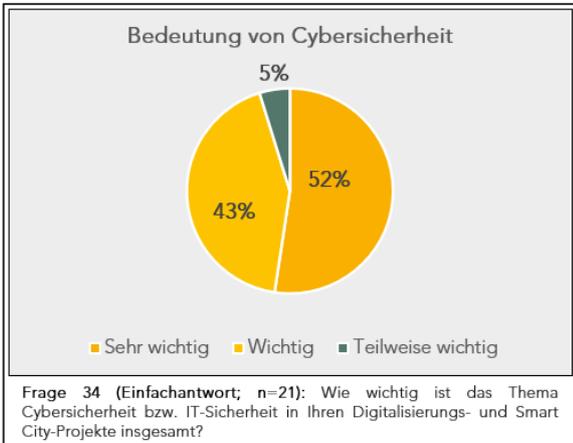
So verfügt nur eine knappe Mehrheit der Kommunen (52 Prozent) über ein fertiges Datenschutzkonzept und eine relative Mehrheit über ein Datensicherheitskonzept (43 Prozent). Datennutzungs- und Datenethikkonzepte sind bislang noch häufiger geplant (zu je 38 Prozent) als umgesetzt oder in Arbeit.



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) suchen 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.

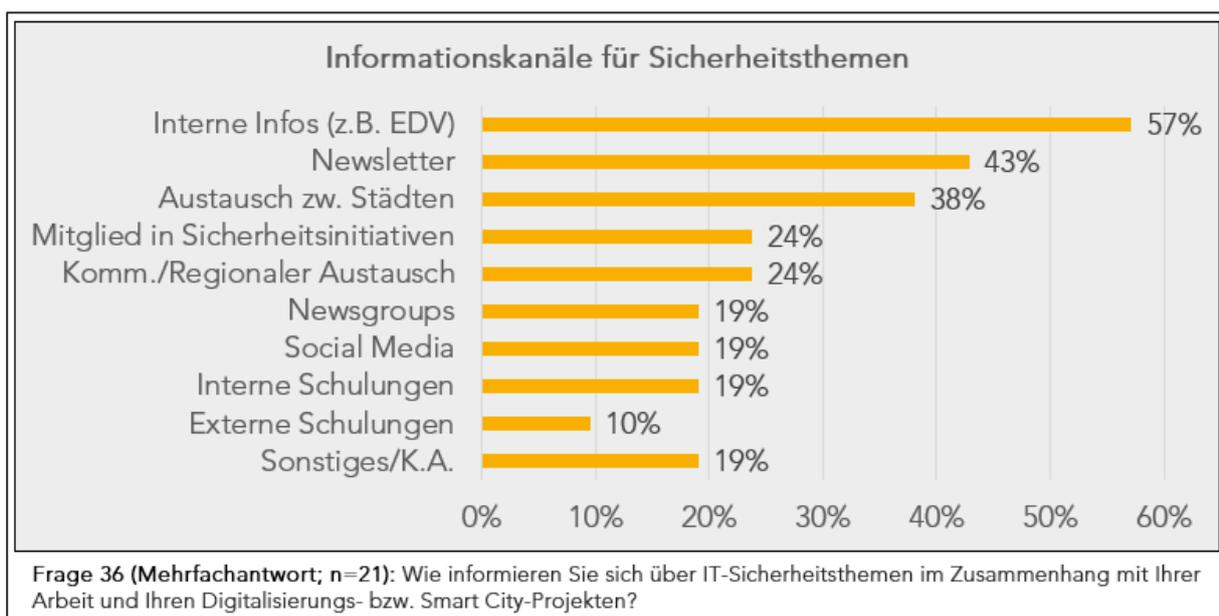
3.3 Cybersecurity



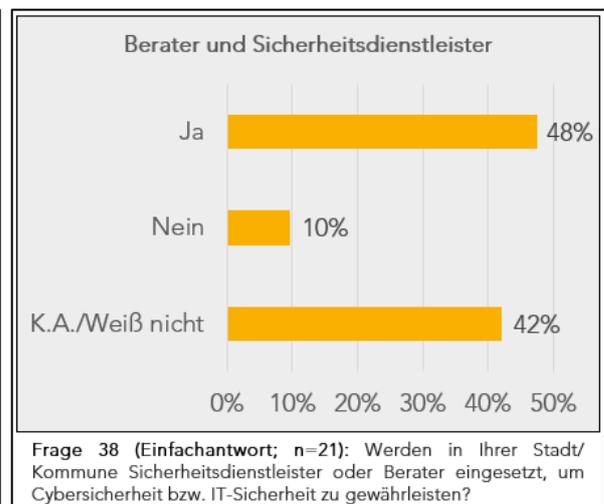
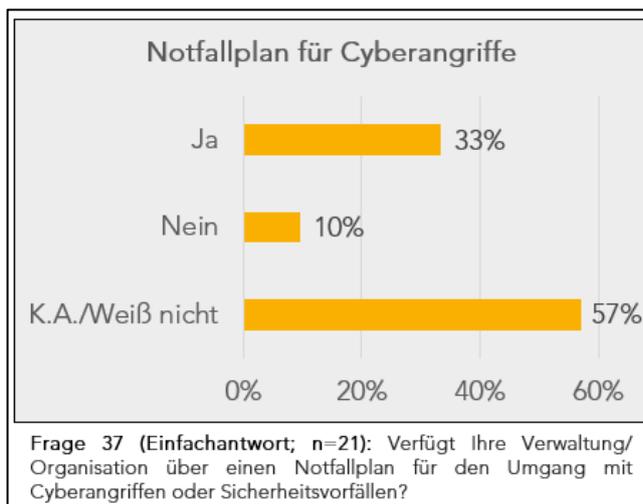
Die Umfrageteilnehmenden sind sich der die Relevanz der Cybersicherheit für Smart Cities grundsätzlich bewusst. Knapp über die Hälfte (52 Prozent) von ihnen bezeichneten die Bedeutung von Cybersicherheit bzw. IT-Sicherheit in ihren Digitalisierungs- und Smart-City-Projekten als sehr wichtig, weitere 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 Informationskanälen, über das 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.



*Jede dritte Smart City verfügt über einen Notfallplan über 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.*



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 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 (Frage 37: 57 Prozent aller Teilnehmenden antworteten mit „Keine Angabe/weiß nicht“) sowie über den Einsatz von externen Sicherheitsdienstleistenden oder Berater*innen (Frage 38: 42 Prozent antworteten mit „Keine Angabe/weiß nicht“) zeigt 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 (Fragen 10, 35).

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, 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 fokussiert. 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 (Frage 19). Auch die Datenschutzfragen treten hierbei noch in den Hintergrund. Aktuell werden Daten in Themenfeldern erhoben, die datenschutzrechtlich wenig erfasst sind (z. B. Mülleimer), dabei bilden diese schon jetzt die Grundlage für zukünftige problemfreie Entwicklungen.

Im Bereich Cybersicherheit sind nur selten Verknüpfungen zu privatwirtschaftlichen Akteuren aufgebaut, von deren Knowhow 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 den smarten Modellkommunen 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. Öffentliche 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.