SICHERE PLATTFORM-ARCHITEKTUREN

RECHTLICHE HERAUSFORDERUNGEN UND TECHNISCHE LÖSUNGSANSÄTZE

Smart Service Welt

Impressum

Herausgeber
Begleitforschung Smart Service Welt – Internetbasierte Dienste für die Wirtschaft
iit – Institut für Innovation und Technik in der VDI/VDE Innovation + Technik GmbH
10623 Berlin

Autoren
Lutz Ashauer
Corinna Brecht
Dr. Uwe Breitenbücher
Prof. Dr. Dr. Jürgen Ensthaler
Olaf-Gerd Gemein
Jan-Hinrich Gieschen
Thomas Günther
Dr. Martin S. Haase
Michael Hahn
Kálmán Képes
Ekkart Kleinod
Dr. Oliver Kopp
Roman Korf
Arndt Kritzner
Prof. Dr. Dr. h. c. Frank Leymann
Andreas Liebing
Prof. Dr. Bernhard Mitschang
Benedikt Moser
Günter Müller-Czygan
Peter Niehues
Detlef Olschewski
Henrik Oppermann
Christine Rösner
Dr. Inessa Seifert
Karen Semmler
Ana Cristina Franco da Silva
Ronald Steinke
Sebastian Straub
Nico Suchold
Martin Virtel
Joost van Well

Gestaltung
Loesch*Hund*Liepold Kommunikation GmbH

Bilder
Logic Way GmbH und FIR e. V. (S. 12), Logic Way GmbH (S. 13, S. 16, S. 18), Smart-Farming-Welt-Konsortium (S. 14), USU Software AG (S. 21, S. 22), StoneOne AG (S. 28), GEISER-Projekt (S. 33), Institut für Automation und Kommunikation e. V. (S. 40, S. 41)

Stand
Mai 2019

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

INHALT

1 EINFÜHRUNG ZUM TECHNOLOGIE-PROGRAMM SMART SERVICE WELT

Im Technologieprogramm Smart Service Welt I des Bundesministeriums für Wirtschaft und Energie sind zahlreiche digitale Plattformen entwickelt worden, die Technologieanbieter und Dienstleister aus unterschiedlichen Branchen miteinander verbinden. Die einzelnen Akteure können über diese Plattformen beispielsweise hardwarebasierte Sensoren und Aktoren zur Gebäudesteuerung, aktuelle Verkehrsinformationen oder auch Daten ihrer Produktionssysteme zur Verfügung stellen. Durch die Kombination dieser Daten können neuartige Smart Services entwickelt und bereitgestellt werden. Neben dem Umgang mit personenbezogenen Daten stellt auch der sichere Umgang mit unternehmenssensiblen Daten eine zentrale Herausforderung für Smart Services dar. Dies gilt insbesondere im B2B-Bereich. Die damit verbundenen Themen sicherer Datenaustausch, Datenschutz, Datenhoheit und Haftung der Plattformbetreiber wurden in den Arbeitsgruppen „Sichere Plattformarchitekturen" und „Recht" von den Experten der Begleitforschung und den Smart-Service-Welt-Projekten diskutiert.

Die Regulierung des digitalen europäischen Binnenmarktes durch die Europäische Datenschutz-Grundverordnung (DSGVO) wird momentan als die größte Herausforderung für datengetriebene Smart-Service-Plattformen gesehen.[1] Es herrscht eine starke Verunsicherung für viele Marktakteure, da die Auswirkungen der DSGVO auf ihre Geschäftsmodelle noch unklar sind.

Die Smart-Service-Welt-Projekte übernehmen in dieser Hinsicht eine Vorreiterrolle bei der Gestaltung von Plattformarchitekturen, die sowohl Datenschutz und -sicherheit als auch Vertrauenswürdigkeit durch Berücksichtigung der Privatsphäre gewährleisten sollen. Darüber hinaus zeigen die Projekte erste Lösungsansätze zum Umgang mit Haftungsaspekten für Plattformbetreiber hinsichtlich der von ihnen angebotenen Dienstleistungen und Services auf.

Im Rahmen der Begleitforschung zum Technologieprogramm Smart Service Welt I haben die Fachgruppen „Recht" und „Sichere Plattformarchitekturen" eng zusammengearbeitet. In mehreren Workshops wurden die technologischen Ansätze zur Gestaltung der Plattformarchitekturen aus rechtlicher Perspektive bewertet und gemeinsam mit den Projekten diskutiert. Die Zusammenarbeit mündete in einen intensiven zweitägigen gemeinsamen Workshop der beiden Fachgruppen im Mai 2018, in dessen Folge diese Publikation entstand.

Die Anwendungsfelder der hier vorgestellten Lösungsansätze für sichere Serviceplattformen sind vielfältig und umfassen Bereiche wie Smart Home, Smart Building, Mobilität, Smart Farming, kommunale Dienstleistungen, geobasiertes Marketing bis hin zur Technikereinsatzplanung für das produzierende Gewerbe.

Kapitel 2 fasst die wesentlichen Herausforderungen, Lösungsansätze sowie offenen Fragen zusammen und verschafft einen Überblick über das aktuelle Spannungsfeld zwischen Recht und Technik.

Kapitel 3 präsentiert den Gastbeitrag „Bedeutsame Rechtsbereiche für die Smart Service Welt – Vermeidung von Haftung und Rechtsverstößen" der Fachgruppe „Recht", der übergreifend für das gesamte Technologieprogramm Smart Service Welt I die zentralen rechtlichen Herausforderungen – Datenhoheit, Haftung der Plattformbetreiber und Datenschutz – zusammenfasst. Dabei werden neben einer juristischen Einordnung auch mögliche Lösungsansätze im Umgang mit diesen Herausforderungen vorgestellt.

In Kapitel 4 folgen die einzelnen Beiträge aus den Projekten des Technologieprogramms, die die jeweiligen Anwendungsbereiche, den Umgang mit den rechtlichen Herausforderungen, daraus resultierenden Entscheidungen hinsichtlich Design und Konzeption der Plattformarchitekturen sowie die gewählten Lösungsansätze und Empfehlungen an die künftigen Plattformarchitekten und Serviceentwickler beinhalten.

Wir bedanken uns bei den beteiligten Autorinnen und Autoren für die Zusammenarbeit und die wertvollen Einblicke in ihre Projekte und wünschen den Leserinnen und Lesern eine spannende Lektüre.

1 https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart%20service%20welt_positionspapier_recht.html.

2 RECHT UND TECHNIK – EIN ÜBERBLICK ÜBER RECHTLICHE HERAUSFORDERUNGEN UND TECHNISCHE LÖSUNGSANSÄTZE

Dr. Inessa Seifert

In diesem Sammelband stellen ausgewählte Smart-Service-Welt-Projekte Lösungsansätze für das Design und die technische Umsetzung von Plattformarchitekturen vor, die Anforderungen an die rechtlichen Rahmenbedingungen wie Datenschutz, Datenhoheit und Haftung der Plattformbetreiber erfüllen.

Serviceplattformen verbinden verschiedene Stakeholder in einem bestimmten Ökosystem miteinander und gestalten auch zum Teil konservative Märkte neu, wie beispielsweise kommunale Dienstleistungen und die Verwaltung öffentlicher Gebäude. Im Folgenden werden die Anwendungsbereiche der Serviceplattformen von Smart-Farming-Welt[2], SmartOrchestra[3], KOMMUNAL 4.0[4], STEP[5] und GEISER[6] sowie relevante rechtliche Rahmenbedingungen, verfolgte technische Lösungsansätze und offene Fragestellungen vorgestellt.

2 https://smart-farming-welt.de.
3 https://smartorchestra.de.
4 https://www.kommunal4null.de.
5 https://www.projekt-step.de.
6 https://www.projekt-geiser.de.

Smart Farming

Anwendungsbereich

Smart-Farming-Welt ist eine herstellerübergreifende Plattform, welche Landwirte, Landmaschinenhersteller und Servicemitarbeiter miteinander verbindet. Die Smart-Farming-Welt-Plattform setzt auf einen herstellerübergreifenden IoT- und Multicloud-Ansatz, welcher über ein speziell dafür entwickeltes Kommunikationsmodul einen Fernzugriff auf die einzelnen Landmaschinen ermöglicht. Ein weiterer spezieller Sensorknoten, die „nPotato“, fungiert als digitaler Zwilling einer normalen Kartoffel, reagiert auf Erschütterungen und ermöglicht eine weitere Ernteoptimierung.

Recht	Aus rechtlicher Perspektive standen im Vordergrund der Smart-Farming-Welt die Bewahrung der Privatsphäre der Servicemitarbeiter und Landwirte, der Datenschutz, die Gewährleistung der Datensparsamkeit und die Geheimhaltung der Daten, welche während eines Erntevorgangs anfallen und zwischen den einzelnen Stakeholdern ausgetauscht werden.
Technik	Die Anforderungen wurden in Form eines digitalen Fingerabdrucks umgesetzt, der die Daten verschlüsselt und einen aufgaben- und ortsbezogenen Zugang zu den Daten der einzelnen Partner in dem landwirtschaftlichen Ökosystem gewährt.
Offene Fragen	Der praktische Einsatz der Smart-Farming-Lösung benötigt eine flächendeckende Mobilfunk-Abdeckung im ländlichen Raum. An dieser Stelle sind staatliche Infrastrukturmaßnahmen oder auch Vergünstigungen für die Mobilfunkbetreiber im ländlichen Raum erforderlich, um Smart-Farming-Welt in die Praxis zu bringen. Rechtlich bleiben die Fragen zum Beschäftigtendatenschutz offen. Der Austausch und vor allen Dingen die Kombination der Daten zwischen verschiedenen Stakeholdern können unerlaubte Rückschlüsse auf das Arbeitnehmerverhalten zulassen. Hier ist intensive Forschung sowohl im technologischen als auch im rechtswissenschaftlichen Bereich notwendig.

SmartOrchestra

Anwendungsbereich

SmartOrchestra ermöglicht auf der Basis der IoT-Plattform FIWARE die Erfassung von Sensordaten sowie die Steuerung und Verwaltung von SmartHome/Building-Sensoren und -Aktuatoren in komplexen Gebäuden. Potenzielle Schäden in Räumen, wie beispielsweise durch Schimmelbildung, werden durch Analyse der Sensordaten erkannt und somit rechtzeitig verhindert. Der technologische Ansatz basiert auf einer hochflexiblen Beschreibungssprache für Services, dem Framework OpenTOSCA sowie einer cloudbasierten FIWARE-Infrastruktur zur Kombination und Steuerung von herstellerspezifischen IoT-Anwendungen. Auf dem Online-Marktplatz der Plattform können Services und Datenquellen unterschiedlicher Hersteller miteinander zu neuen Diensten verbunden werden.

Recht	Die Nutzung von Daten (Datenhoheit) sowie die Bewahrung der Privatsphäre (Datenschutz) von Bewohnern und Nutzern stellten die zentralen rechtlichen Herausforderungen dar. Für die Plattformbetreiber und Serviceentwickler waren insbesondere die Haftungsaspekte für die angebotenen Dienste entscheidend für die Vermarktung der Services über die SmartOrchestra-Serviceplattform, etwa wegen der Steuerung von sicherheitskritischen internetfähigen Aktoren und Geräten.
Technik	Die Daten werden den Serviceentwicklern nur mit Zustimmung des Anbieters, d. h. des Datenlieferanten, auf der Plattform zur Verfügung gestellt. Technisch wurde diese Anforderung mit einem Datennotar auf Blockchain-Basis mit Smart Contracts umgesetzt. Zum Datenschutz wurden einerseits die personenbezogenen Daten anonymisiert bzw. pseudonymisiert und andererseits Security-by-Design-Prinzipien eingehalten. Die Verschlüsselung der Kommunikation sowie ein Rechte- und Zugriffsmanagementkonzept sorgen für einen vertrauensvollen Umgang auch mit den sicherheitskritischen Sensorik- und Aktuator-Komponenten. Die Haftungsfragen werden durch individuelle Verträge zwischen dem Plattformbetreiber und den Serviceentwicklern geregelt.
Offene Fragen	Künftig sollen offene Standards für die Anonymisierung/Pseudonymisierung von Daten geschaffen werden, um eine einheitliche Basis für die Modellierung, Komposition, den sicheren Betrieb und die Vermarktung von Smart Services zu schaffen. Die Zertifizierung von Services nach den Privacy- und Security-by-Design-Prinzipien für Datenschutz- und IT-Sicherheit wäre ein wichtiger Schritt für die Akzeptanz der Serviceplattformen bei den Endnutzern und Plattformbetreibern.

KOMMUNAL 4.0

Anwendungsbereich

KOMMUNAL 4.0 bietet smarte Dienste für kritische Infrastrukturen im Wasser- und Abwasserversorgungssektor an. Auch hier ermöglichen intelligente und vernetzte IoT-Technologien eine bedarfsgerechte Wartung alter Maschinen.

Recht	Bei der Entwicklung der sicheren IoT-Plattform für die städtische Wasserversorgung stand die Berücksichtigung besonderer IT-Sicherheitsanforderungen an kritische Infrastrukturen nach dem IT-Sicherheitsgesetz im Vordergrund. In diesem Zusammenhang war insbesondere die Haftungsregelung zwischen dem Plattformbetreiber und dem Betreiber der kritischen Infrastruktur wichtig.
Technik	Bereits in der Anforderungsphase wurde das Konzept der KOMMUNAL-4.0-Plattformarchitektur nach dem Security-by-Design-Prinzip entworfen und dadurch die Informationssicherheit der einzelnen Plattformbereiche von Anfang an fest integriert. Als Grundlage dienten die IT-Sicherheitsstandards ISO 27001 und der branchenspezifische Sicherheitsstandard Wasser/Abwasser (B3S) des BSI. Die Haftungsaspekte wurden durch eine speziell dafür ausgelegte Vertragsgestaltung und durch Monitoringmaßnahmen umgesetzt.
Offene Fragen	Insbesondere die Bündelung von Diensten und Daten auf einer Plattform stellt nach wie vor eine Herausforderung für die Betreiber kritischer Infrastrukturen dar. Das Risikomanagement nach dem BSI-Gesetz bleibt weiterhin die Aufgabe des Betreibers der kritischen Infrastruktur. Die Plattformbetreiber brauchen Zertifikate und Tests für die Services nach den gängigen IT-Sicherheitsstandards, die momentan noch nicht existieren. Darüber hinaus besteht das Risiko, Rückschlüsse auf die persönlichen Daten der Mitarbeiter der Wasserversorgungsbetriebe zu ziehen, weil die Daten der im Betrieb tätigen Personen mit den Prozessdaten vermischt werden können. Hier stellt sich die Frage des Beschäftigtendatenschutzes in Verbindung mit der Analyse und Verarbeitung dieser Daten.

STEP

Anwendungsbereich

Im Projekt STEP wurde eine Serviceplattform entwickelt, die Servicetechniker für Reparaturen und Wartungsarbeiten in der Industrie mit Einsatzplanern verbindet. Dabei werden Informationen zum Einsatzort mit Informationen zu den Servicetechnikern, wie deren Qualifikationen und mögliche Fachgebiete, sowie digitale Dienste wie Chat-Anwendungen für die Kommunikation zwischen den Technikern miteinander zu einem cyber-physischen sozialen Netzwerk kombiniert.

Recht	Bei STEP sind die rechtlichen Aspekte wie Beschäftigtendatenschutz und der Umgang mit dem Verbot der automatisierten Einzelfallentscheidung nach der DSGVO wichtig, welche sowohl für die Plattformarchitektur als auch für die Interaktion zwischen dem Techniker und dem Einsatzplaner ausschlaggebend sind.
Technik	Zur Wahrung der Privatsphäre der Servicetechniker wurden in STEP Pseudonymisierungs- und Anonymisierungsverfahren verwendet. Außerdem wurden die Standortdaten der Servicetechniker nach dem Prinzip der Datensparsamkeit nur partiell erfasst. Die finale Entscheidung über die Einsatzplanung der Servicetechniker übernimmt eine natürliche Person, der Einsatzplaner. Damit wird auch die automatisierte Einzelfallentscheidung nach der DSGVO verhindert.
Offene Fragen	Es bleibt offen, ob die Auswahl eines geeigneten Servicetechnikers anhand seiner Qualifikationen und Expertise vom Einsatzplanungstool juristisch als vollautomatisiert betrachtet wird und somit Rechte der Servicetechniker verletzt werden. Diese Fragestellungen sind noch nicht umfassend analysiert und bedürfen weiterer Diskussionen oder sogar staatlicher Regulierung.

GEISER

Anwendungsbereich

Im Projekt GEISER wurde eine Plattform entwickelt, welche durch eine Fusion von verschiedenen Datenquellen wie GPS-Daten, Verkehrsdaten, Websites, Online-Veranstaltungskalender, Foren, (sozialen) Medien und Open Data mit Absatz- und Kundendaten neue Mehrwertdienste wie Parkplatzsuche, Geomarketing oder auch Routenplanung für Servicetechniker ermöglicht.

Recht	Durch die Datenfusion entstehen Herausforderungen beim Datenschutz, besonders wenn bereits bestehende Datenpools mit einer konkreten Geoposition zusammengebracht und dadurch Rückschlüsse auf konkrete Personen ermöglicht werden. Ein weiterer Aspekt ist die Datenhoheit über die fusionierten Datenquellen und aggregierten Datensätze. Inwieweit kann der Plattformbetreiber über die aggregierten Daten bestimmen? Wie sollen die Geschäftsbeziehungen mit den Datenlieferanten geregelt werden, um die Verfügbarkeit der Daten für Serviceentwickler und -nutzer zu garantieren?
Technik	In GEISER kommen Anonymisierungs- und Pseudonymisierungsverfahren zum Einsatz, die die Identifizierbarkeit der Nutzer verhindern sollen. Darüber hinaus erlaubt die Plattform die Verarbeitung von Daten nur durch eine Einwilligung der Nutzer oder nur im Falle eines gesetzlichen Erlaubnistatbestands. Die Nutzung der Daten wurde mithilfe von Verschlüsselung und Zugriffskontrolle abgesichert, um den ausreichenden Schutz von wettbewerbsrelevanten oder auch kritischen Informationen zu gewährleisten.
Offene Fragen	Die rechtskonforme Anonymisierung von Daten ist eine offene Fragestellung, die weitere Forschung erfordert. Nutzungsrechte an Daten können nach der aktuellen Rechtslage nur vertraglich eingeräumt werden. Allerdings stellen vertragliche Regelungen mit Datenlieferanten für kleine und mittelständische Unternehmen eine Herausforderung dar, da noch wenig Erfahrung und Good-Practice-Beispiele existieren.

3 BEDEUTSAME RECHTSBEREICHE FÜR DIE SMART SERVICE WELT – VERMEIDUNG VON HAFTUNG UND RECHTSVERSTÖSSEN

Prof. Dr. Dr. Jürgen Ensthaler, Dr. Martin S. Haase, Sebastian Straub, Jan-Hinrich Gieschen

Die Analyse und Verwertung von großen Datenmengen ist integraler Bestandteil vieler Geschäftsmodelle der Smart-Service-Welt-Projekte. Dabei stehen die Anbieter vor verschiedenen rechtlichen Herausforderungen. Zum einen stellt die EU-Datenschutz-Grundverordnung hohe Anforderungen an die Verarbeitung von personenbezogenen Daten. Zum anderen ist bei der Sammlung und Zusammenführung von Daten aus verschiedenen Quellen die Frage der Nutzungsberechtigung an Daten (die sogenannte Datenhoheit) von Bedeutung. Daran anschließend müssen bei datenbasierten Geschäftsmodellen auch Haftungsfragen berücksichtigt werden, insbesondere wenn es aufgrund von fehlerhaften Daten zu Störungen kommt.

3.1 Der datenschutzkonforme Umgan mit personenbezogenen Daten

Die Projekte der Smart Service Welt bewegen sich in einem hoch innovativen Umfeld. Eines der Hauptziele vieler Projekte ist eine Fortentwicklung der Nutzungs-, Verknüpfungs- und Verarbeitungsmöglichkeiten von Daten. Dabei werden auch Daten verarbeitet, die Rückschlüsse auf einzelne Personen zulassen. Die Verarbeitung solcher personenbezogener Daten müssen den Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO) genügen. Ein Verstoß gegen die datenschutzrechtlichen Bestimmungen der DSGVO kann zu erheblichen Haftungsrisiken und der Verhängung von empfindlichen Bußgeldern führen. Aus diesem Grund stellte die datenschutzkonforme Verarbeitung von Daten eine zentrale Herausforderung für die Projekte dar.

3.1.1 Personenbezug und Anonymisierung

Die DSGVO-konforme Verarbeitung von Daten ist gerade in der Digitalwirtschaft mit hohem administrativem und personellem Aufwand verbunden. Für Anbieter von datenbezogenen Dienstleistungen ist daher von besonderer Bedeutung, unter welchen Umständen eine Datenverarbeitung in den Anwendungsbereich der DSGVO fällt. Der sachliche Anwendungsbereich der DSGVO ist nur eröffnet, wenn personenbezogene Daten verarbeitet werden. Als personenbezogene Daten werden alle Informationen bezeichnet, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die Grundsätze des Datenschutzes gelten demgegenüber nicht für anonyme Informationen[7]. Aus Anbietersicht besteht also die Möglichkeit, durch Anonymisierung den datenschutzrechtlichen Anforderungen der DSGVO zu entgehen. Die praktische Umsetzung einer Anonymisierung kann sich aber als schwierig erweisen, da es keine vorgegebene Metrik zur Feststellung der Anonymität von Daten gibt. Nach Maßgabe der DSGVO gelten Daten dann als anonym, wenn sie sich nicht auf eine natürliche Person beziehen oder in einer Weise anonymisiert worden sind, also so bearbeitet wurden, dass die betroffene Person nicht identifiziert werden kann. Bei der Feststellung, ob eine natürliche Person identifizierbar ist, sollen alle Mittel berücksichtigt werden, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person zu identifizieren. Dabei sollen alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Letzteres bedeutet, dass im Rahmen einer Risikoanalyse auch mögliche technologische Weiterentwicklungen antizipiert werden müssen, die eine Identifizierung in der Zukunft ermöglichen können.

Der Herausforderungen der Anonymisierung von Datensätzen haben sich die Projekte Smart Orchestra (S. 26), STEP (S. 20) und GEISER (S. 33) gestellt. Entsprechende Prozesse zur Verhinderung einer Identifizierbarkeit von natürlichen Personen wurden implementiert. Dies wurde zum Teil dadurch erreicht, dass von vornherein (entsprechend dem Grundsatz der Datenminimierung) nur solche Daten erhoben werden, die für die Durchführung des Service erforderlich waren. Allein durch die sparsame Erhebung von Daten kann die Wahrscheinlichkeit einer Identifizierung reduziert werden. Daneben wurden Methoden etabliert und angewendet, um den Anonymisierungsgrad von Datenquellen zu bestimmen, was oftmals eine Voraussetzung für eine Weiterverarbeitung der Daten ist. Vor dem Hintergrund einer möglichen De-Anonymisierung mussten nicht nur die eigenen Datenquellen ausgewertet, sondern auch potenzielle Verknüpfungsmöglichkeiten mit anderen Datenquellen berücksichtigt werden. Dies ist insofern von Bedeutung, als dass die Wahrscheinlichkeit einer Identifizierung steigt, je mehr verknüpfbare Datenquellen bereitstehen.

7 Vgl. Erwägungsgrund 26 DSGVO.

3.1.2 Datenschutzrechtliche Verantwortlichkeit

In Bezug auf mögliche Haftungsrisiken und die Verhängung von Bußgeldern ist die Frage der datenschutzrechtlichen Verantwortlichkeit von herausragender Bedeutung für die Projekte der Smart Service Welt. Adressat der datenschutzrechtlichen Verpflichtungen nach der DSGVO ist der sogenannte Verantwortliche. Er entscheidet allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten.[8] Gerade bei Smart Services fehlen oftmals ausreichende Kriterien zur klaren Abgrenzung der datenschutzrechtlichen Verantwortungsbereiche, da sich durch die Einbindung und Verknüpfung von weiteren Services die Einflussfaktoren auf die Verarbeitung von personenbezogenen Daten vermischen. Eine eindeutige Zuweisung von Verantwortlichkeiten stellt sich vor diesem Hintergrund als schwierig dar, insbesondere wenn Daten aus unterschiedlichen Datenquellen auf einer Plattform zusammengeführt werden. Umso wichtiger ist eine klare Zuordnung und Abgrenzung der Verantwortungsbereiche. Die DSGVO enthält in Bezug auf eine gemeinsame Verantwortlichkeit konkrete Vorgaben. So müssen die gemeinsam Verantwortlichen im Rahmen einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt. Eine Datenverarbeitung kann jedoch auch durch sogenannte Auftragsverarbeiter erfolgen. Der Auftragsverarbeiter bestimmt im Gegensatz zum Verantwortlichen nicht über die Mittel und Zwecke der Datenverarbeitung. Er ist vielmehr „der verlängerte Arm" des Verantwortlichen und hat keine eigene Entscheidungsbefugnis in Bezug auf die Datenverarbeitung. Da das Datenschutzniveau durch die Inanspruchnahme eines Auftragsverarbeiters nicht abgesenkt werden darf, muss eine Vielzahl von Vorgaben in Bezug auf eine wirksame Auftragsverarbeitung eingehalten werden.[9]

3.1.3 Haftung für Datenschutzverstöße

Datenschutzverstöße können nach der DSGVO unterschiedlich sanktioniert werden. Zunächst hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein Schaden entstanden ist, einen Anspruch auf Schadenersatz gegen den Verantwortlichen oder den Auftragsverarbeiter. Daneben können für Datenschutzverstöße auch Bußgelder durch die zuständige Aufsichtsbehörde verhängt werden. Die Höhe der möglichen Bußgelder hat sich im Vergleich zu dem vorher geltenden Bundesdatenschutzgesetz erheblich verschärft. Abzuwarten bleibt, inwieweit die Aufsichtsbehörden den hohen Bußgeldrahmen ausschöpfen werden. Wichtige Kriterien zur Entscheidung über die Geldbußen sind gesetzlich festgelegt. Zu den Kriterien[10] gehören insbesondere die Art, Schwere und Dauer des Verstoßes, die Frage, ob der Verantwortliche vorsätzlich oder fahrlässig gehandelt hat, sowie der nachträgliche Umgang mit Pflichtverletzungen und verursachten Schäden. Aus der Festlegung der Kriterien lässt sich ableiten, dass jede einzelne Maßnahme, die ein Projekt zum Schutz personenbezogener Daten vornimmt, den Umfang der Haftung letztlich (zumindest) verringern kann, auch wenn sich eine Haftung wohl nie gänzlich ausschließen lässt. Die genannten Kriterien sollten von dem Verantwortlichen bei der Umsetzung seines Geschäftsmodells stets beachtet werden, um so die rechtlichen Risiken effizient zu minimieren.

Neben der Inanspruchnahme durch natürliche Personen und der Verhängung von Bußgeldern durch die Aufsichtsbehörden ist fraglich, ob der Verantwortliche aufgrund von DSGVO-Verstößen auch von Mitbewerbern abgemahnt werden kann. In Betracht kommen hier Ansprüche auf Beseitigung, Unterlassung oder Schadensersatz. Ein abmahnfähiger datenschutzrechtlicher Verstoß könnte etwa darin bestehen, dass der Betreiber einer Plattform eine fehlerhafte Datenschutzerklärung verwendet. Bisher ist nicht abschließend geklärt, inwieweit diese wettbewerbsrechtlichen Ansprüche auf eine Verletzung der Vorschriften der DSGVO gestützt werden können. Dafür spricht, dass die DSGVO nicht nur die Grundrechte der betroffenen Personen schützen soll, sondern auch eine Förderung des Wettbewerbs angestrebt wird[11]. Dagegen spricht der abschließende Charakter der Sanktionsregelungen der DSGVO. So wird vertreten, dass die in Kapitel VIII der DSGVO genannten Regelungen zu Rechtsbehelfen, Haftung und Sanktionen abschließend sind. Weitergehende Ansprüche, wie ein wettbewerbsrechtlicher Anspruch eines Mitbewerbers, bestehen demnach nicht. Die bisher in diesem Zusammenhang ergangenen Gerichtsentscheidungen lassen keine eindeutige Tendenz erkennen. Auch wenn es bislang zu keinen großen Abmahnwellen gekommen ist, besteht für die Anbieter von Smart Services ein Restrisiko, für etwaige Datenschutzverstöße abgemahnt zu werden. In

8 Art. 4 Nr. 7 DSGVO.
9 Vgl. hierzu Art. 28 DSGVO.
10 Art. 83 Abs. 2 S. 2 DS-GVO.
11 Erwägungsgründe 9, 10.

der Konsequenz müssen Anbieter verstärkt darauf achten, dass die Angriffsflächen für mögliche Abmahnungen minimiert werden. Das bedeutet, dass insbesondere nach außen hin sichtbare Datenschutzelemente, wie z. B. die Datenschutzerklärung, unbedingt den gesetzlichen Vorgaben entsprechen müssen.

3.2 Datenhoheit

Intelligente Dienste basieren zunehmend auf der Analyse und Auswertung von großen Datenmengen. Diese Datensammlungen werden häufig aus unterschiedlichen Datenquellen gespeist und auf Plattformen mit weiteren Daten aggregiert. Vor dem Hintergrund der zunehmenden Bedeutung von Daten als Wirtschaftsgut muss sichergestellt werden, dass die Verwertung dieser Daten rechtmäßig erfolgt. Für viele Projekte der Smart Service Welt war daher die Frage der Datenhoheit eine zentrale rechtliche Herausforderung. Dabei wird ein grundsätzliches Problem adressiert, denn derzeit besteht kein gesetzlich geregeltes Verfügungsrecht an Daten.

Das Fehlen einer rechtlichen Zuordnungsregel wird besonders deutlich, wenn es um die Verwertung von maschinengenerierten Daten geht. Solche Daten könnten zum einen dem Nutzer einer Maschine zugewiesen werden. Daneben könnte aber auch der Hersteller der Maschinen Ansprüche auf die generierten Daten erheben, denn auch er hat ein Interesse an der weiteren und häufig auch ausschließlichen weiteren Verarbeitung. Die Diskussion um Datennutzungsrechte wird zurzeit sehr kontrovers geführt. So wird argumentiert, dass dem Hersteller der datenliefernden Maschinen die Nutzungsrechte zukommen sollen, weil er die entsprechende Technik eingebracht hat; andere sehen die Daten als „Früchte" der jeweiligen Maschine und damit dem zuzuordnen, der die Maschine betreibt. Der derzeitige gesetzliche Rahmen bietet keine Ansatzpunkte zur Lösung dieses Interessenkonflikts. Die größte Sicherheit für den Umgang mit dieser Herausforderung gibt zurzeit die vertragliche Regelung. Das bedeutet: Werden Daten im Rahmen von Smart Services ausgetauscht, müssen sich die Beteiligten zuvor darauf einigen, wer in welchem Umfang Daten nutzen darf. Einschränkend gilt aber, dass bei Einräumung von Nutzungsrechten im Rahmen von Allgemeinen Geschäftsbedingungen diese einer Inhaltskontrolle unterliegen können. Nach § 307 Abs. 1 BGB sind Bestimmungen in Allgemeinen Geschäftsbedingungen unwirksam, wenn sie den Vertragspartner entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Von einer solchen unangemessenen Benachteiligung wird in der Regel auszugehen sein, wenn eine vertragliche Einräumung von Nutzungsrechten, evtl. auch noch eine ausschließliche, ohne angemessene Gegenleistung erfolgt.

Das beschriebene Problem der Datenhoheit und der damit einhergehenden fehlenden Zuordnung von Daten wird dadurch vergrößert, dass, trotz der Ungewissheit über die Nutzungsbefugnis, Daten an Dritte (etwa den Plattformbetreiber) weitergeben werden. Hier kommen mehrere Probleme zusammen. Hat schon der Datenlieferant seine Daten auf einer unsicheren Rechtsgrundlage erhalten, besteht diese Unsicherheit beim Plattformbetreiber fort. Gerade im produzierenden Gewerbe lassen sich Hersteller regelmäßig nur ein einfaches Nutzungsrecht an Maschinendaten einräumen. Dem Hersteller ist es dann nicht ohne Weiteres möglich, einem Dritten, wie z. B. einem Plattformbetreiber, weitere Nutzungsrechte zu gewähren. Diese Befugnis hätte er nur, wenn er sich von vornherein ein ausschließliches Nutzungsrecht an den Maschinendaten hat einräumen lassen. Soweit er ein ausschließliches Nutzungsrecht vereinbart hat, dürfte eine solche Vereinbarung an einer Inhaltskontrolle (§ 307 BGB) scheitern, es sei denn, es wurde eine konkrete Gegenleistung erbracht. Die Nutzung einer Datensammlung ohne die Sicherheit, ob diese Daten verarbeitet werden dürfen, ist äußerst riskant. Sollen solche Daten Grundlage für ein erfolgreiches Geschäftsmodell werden, ist mit einem Streit über die Nutzungsberechtigung zu rechnen. Es sollte stets darauf geachtet werden, dass die „Quelle" zur Weitergabe der Daten berechtigt ist. Solange es noch kein neues Leistungsschutzrecht in Bezug auf maschinengenerierte Daten gibt, sollte der Plattformbetreiber seinen Datenlieferanten den Rat geben, entsprechende vertragliche Regelungen zu treffen, d. h. auch eine Vereinbarung dahingehend zu treffen, dass die Daten zu bestimmten Zwecken (z. B. für Wartungsarbeiten) weitergenutzt werden dürfen.

3.3 Haftung

Einige Geschäftsmodelle sehen vor, dass Sensor- und Maschinendaten an Plattformen übermittelt und dort weiterverarbeitet werden. Auf Grundlage einer Analyse dieser Daten können dann Geräte, Sensorik oder Aktuatoren gesteuert werden. Als Beispiel kann hier das Projekt SmartOrchestra (S. 26) mit einem Marktplatz für intelligente Gebäudesteuerung genannt werden. Durch eine fehlerhafte Ansteuerung kann es zu Schäden oder Systemausfällen kommen. Daraus ergibt sich eine Reihe von haftungsrechtlichen Fragestellungen: Dies betrifft zum einen die Beschaffenheit der Ursprungsdaten. Dabei ist zu klären, ob die übersandten Daten überhaupt durch die eigene Software entsprechend verarbeitet werden können. Zur Vermeidung von Haftungsrisiken müssen die Datenbeschaffenheit und Datenqualität vorab geklärt werden. Darüber hinaus ist zu klären, ob die Daten nach dem Verarbeitungsprozess kompatibel mit der anzusteuernden Hardware sind.

Um die Gefahr für Anbieter von Services zu reduzieren, für entstandene Schäden in Anspruch genommen zu werden, können vertragliche Haftungsausschlüsse vereinbart werden. Dabei ist aber zu beachten, dass ein Haftungsausschluss nicht dazu führen darf, dass die angebotene Leistung durch den Ausschluss im Grunde wieder aufgehoben wird. Wesentliche vertragstypische Pflichten, die prägend für den Vertragstyp sind (z. B. die Zusage der Bereitstellung eines konkreten Dienstes einer Plattform), dürfen also nicht durch Haftungsausschlüsse ausgehöhlt werden. Derart widersprüchliche Klauseln in Verträgen wären unwirksam. Möglich wäre es aber, auf die eigenen Kontrollmöglichkeiten hinzuweisen (wenn sie denn bestehen) bzw. auf deren Grenze. Auch sollte auf die Bedeutung der vom Kunden übermittelten Angaben (insbesondere hinsichtlich der Hardwareelemente) hingewiesen und bestmögliche Prüfung versprochen werden. Im Übrigen sollte dann die Haftung für leichte Fahrlässigkeit ausgeschlossen werden.

3.4 Fazit

Die Regelungen der Datenschutz-Grundverordnung haben kein unüberwindbares Hindernis für die Umsetzung der Smart-Service-Welt-Projekte dargestellt. Eine datenschutzrechtskonforme Gestaltung erforderte jedoch aufgrund der Vielzahl der eingebundenen Akteure und der zahlreichen Datenverknüpfungen einen enormen Bewertungs- und Umsetzungsaufwand. Mangels einer gesetzlichen Regelung müssen Smart Services zudem die Frage der Datenhoheit klären. Inhalt und Umfang der Datennutzungsrechte müssen sich dabei an den jeweiligen Strukturen der Dienste orientieren. Mögliche Haftungsrisiken müssen antizipiert und soweit möglich vertraglich ausgeschlossen werden. Die in diesem Abschnitt benannten Herausforderungen, bestehend aus Datenschutz, Datenhoheit und Haftung, erfordern einen hohen Abstimmungsbedarf zwischen den beteiligten Akteuren. Dabei müssen die rechtlichen Rahmenbedingungen bereits bei der Konzeption der Plattformarchitekturen berücksichtigt werden, um einen problemlosen Austausch von Daten sowie Entwicklung, Angebot und Nutzung von smarten Services zu gewährleisten.

4 LÖSUNGSANSÄTZE AUS DER SMART SERVICE WELT I

4.1 Smart-Farming-Welt – Eine herstellerübergreifende Plattform[12] ermöglicht innovative Wertschöpfungsnetzwerke im Agrarbereich

Christine Rösner[13], Arndt Kritzner[14], Benedikt Moser[15]

Die Herausforderungen in der Landwirtschaft hinsichtlich Ressourceneffizienz und Ernteertrag zusammen mit steigenden Anforderungen an die Qualität von Lebensmitteln und Umweltschutz sind immens. Dies hat dazu geführt, dass digitale Technologien in der Landwirtschaft bereits seit Jahren eine Selbstverständlichkeit sind.

Im Mittelpunkt des Projekts Smart-Farming-Welt steht die Verbesserung der Produktivität des Ernteprozesses landwirtschaftlicher Betriebe sowie des gesamten Wertschöpfungsnetzwerks. Die bisherigen Digitalisierungsbestrebungen konzentrieren sich vor allem auf einzelne Maschinen, Anbieter oder Betriebe. Der nächste Schritt gilt nun der digitalen Vernetzung aller beteiligten Partner im landwirtschaftlichen Ökosystem mit einer herstellerübergreifenden Plattform und der damit einhergehenden Frage, ob damit die oben genannten Herausforderungen erfolgreich gelöst werden können.

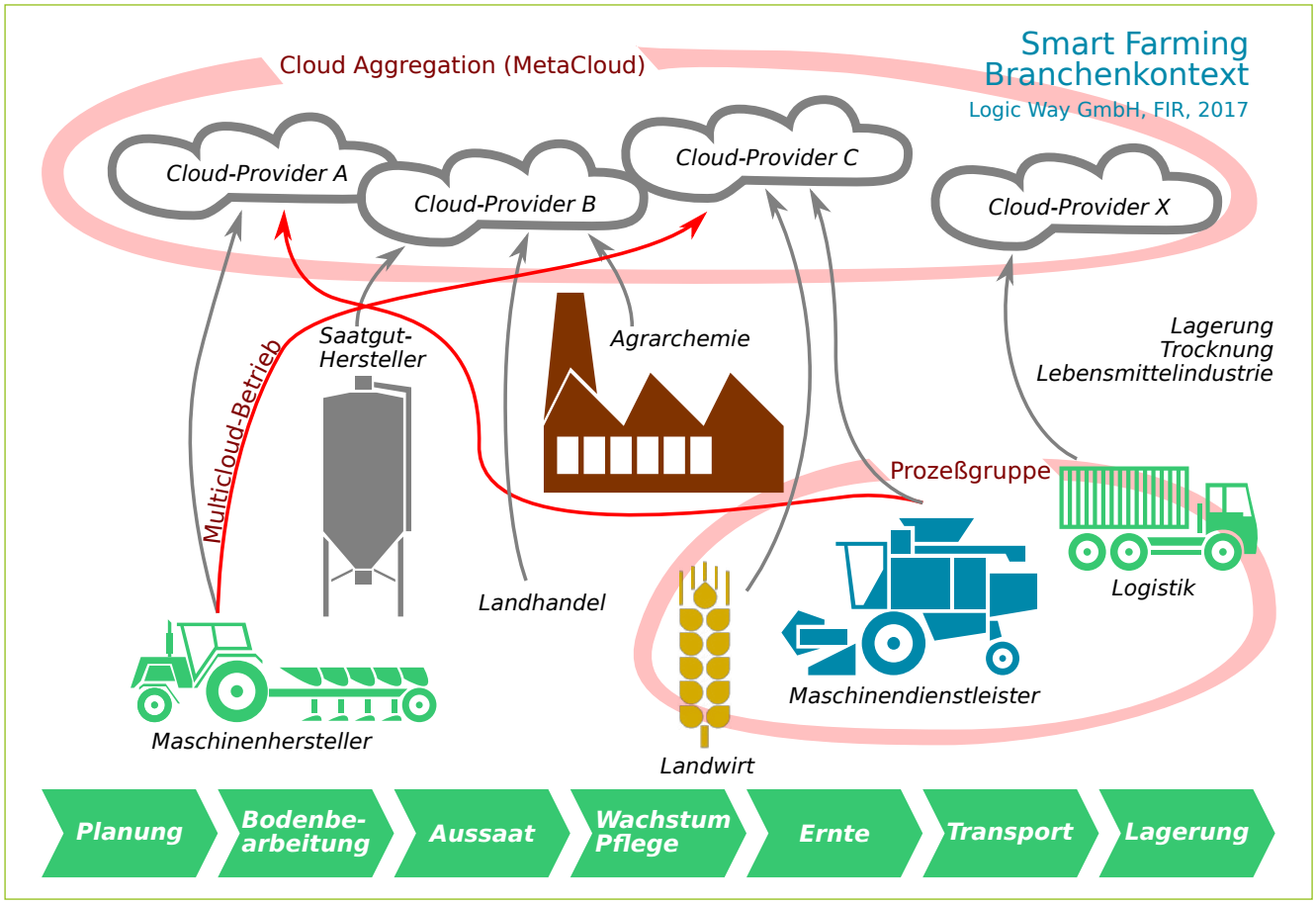

Abbildung 1: Landwirtschaftlicher Interaktionskontext

12 Der Plattform-Begriff wird im Folgenden sowohl für den verwendeten Software-Komponentenstack als auch für die abgebildete Prozesslogik und die installierte Betriebsinstanz verwendet.
13 Deutsche Telekom AG, T-Labs, Darmstadt.
14 Logic Way GmbH, Schwerin.
15 FIR e.V. an der RWTH Aachen.

Die im Rahmen des Förderprogramms Smart Service Welt [1] entwickelte Smart-Farming-Plattform vernetzt alle beteiligten Akteure des landwirtschaftlichen Ökosystems miteinander. Bei der Smart-Farming-Plattform handelt es sich um eine virtuelle Plattform, die es ermöglicht, Daten und Informationen multidirektional zwischen allen Beteiligten auszutauschen und so das Wissen um das Gesamtsystem zu steigern. Die Plattform wird dabei durch die Summe der in Smart-Farming-Welt entwickelten technischen Komponenten und deren logische Verknüpfung gebildet. Den Kunden werden dadurch Services mit höherem Nutzen angeboten, indem bereits in der Landwirtschaft bestehende Plattformen der Landmaschinenhersteller und deren Maschinen in Bezug auf Informationen und Daten miteinander verbunden werden. Es wird so beispielsweise möglich, dass ein Kunde (z. B. Landwirt oder Servicemitarbeiter) gesichert auf seine Daten oder die informationstechnische Infrastruktur von Hersteller A über die Plattform des Herstellers B zugreifen kann.

Im Rahmen des Projekts wurden sowohl die technischen als auch die organisatorischen Voraussetzungen erarbeitet und darüber hinaus zukunftsfähige Geschäftsmodelle für das Ökosystem Landwirtschaft entwickelt. Zu den organisatorischen Voraussetzungen gehören beispielsweise Verrechnungsmodalitäten oder klare Rechte- und Rollenkonzepte, die den Datenzugriff und die Datenhoheit festlegen [2].

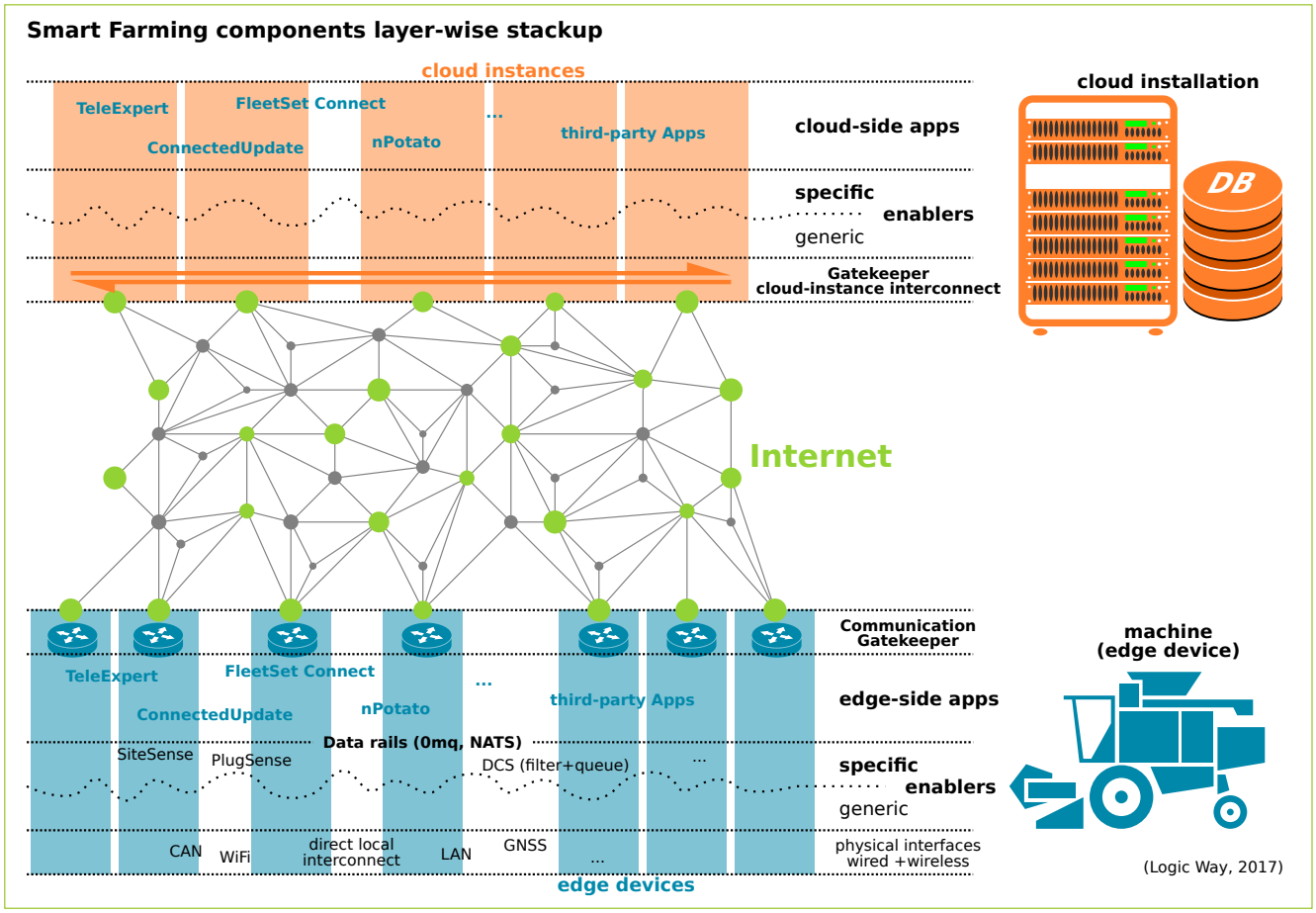

Abbildung 2: Komponenten-Schichtenmodell der Smart-Farming-Plattform

Die Smart-Farming-Plattform stellt die Komponenten bereit, um den gesamten Wertschöpfungsprozess in der Landwirtschaft detailliert abzubilden. Alle Akteure des landwirtschaftlichen Wertschöpfungsnetzwerks, die in die jeweilige Anwendung eingebunden sind, werden über die Plattform miteinander verknüpft. Grundsätzlich orientiert sich die Plattform am Schichtenmodell digitaler Infrastrukturen [3] sowie am oneM2M Framework [10]. Ausgangspunkt sind intelligente, vernetzte Maschinen, die Daten über den landwirtschaftlichen Prozess und ihre Umwelt erfassen, adaptiv filtern und untereinander sowie an die Cloud weiterkommunizieren. Auf der softwaredefinierten Plattform werden Daten aus verschiedenen Quellen miteinander verarbeitet und angereichert, sodass daraus wertvolle Informationen gewonnen werden können.

Unter Nutzung dieser Informationen werden in der obersten Ebene schließlich spezifische Services erbracht, die einen kontextbezogenen Mehrwert für die Anwender mit sich bringen.

Innerhalb des Projekts werden vier exemplarische Anwendungsfälle erarbeitet, die den Nutzen von herstellerübergreifenden Services verdeutlichen.

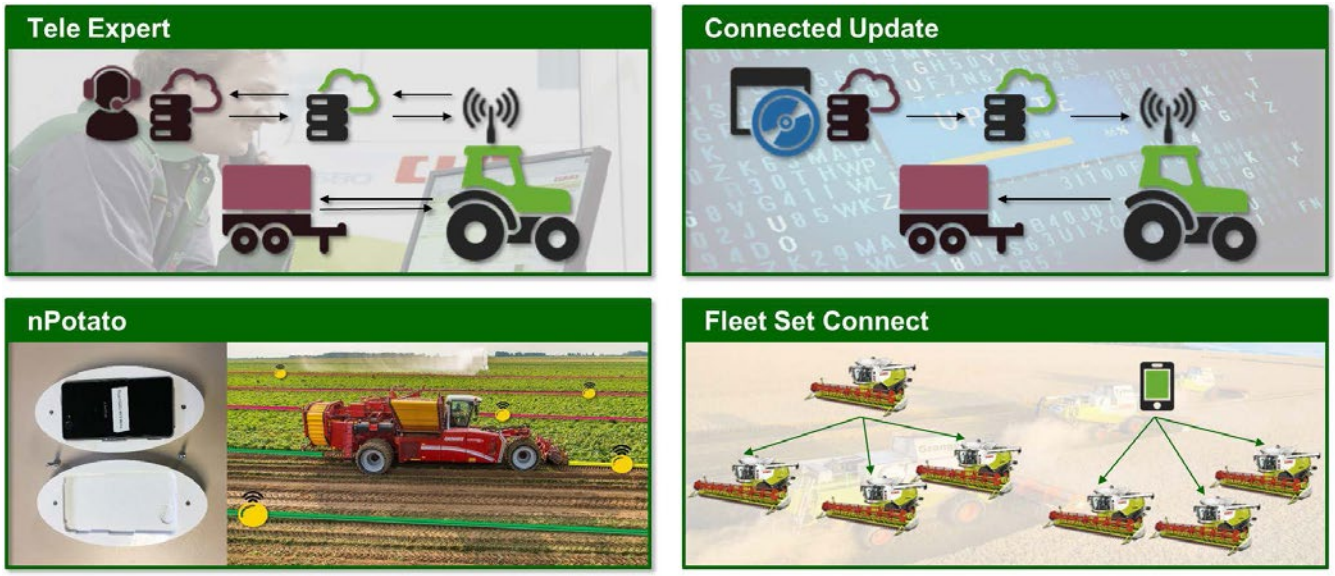

Abbildung 3: Exemplarisch innerhalb der Plattformstruktur umgesetzte Anwendungsfälle

Umsetzung in der Smart-Farming-Welt

Die bisherigen Servicestrukturen der Landmaschinenhersteller können durch eine virtuelle Plattform im Zusammenwirken mit dem auf der jeweiligen Landmaschine installierten Kommunikationsmodul deutlich schneller und effizienter gestaltet werden. Für die Entwicklung der virtuellen Plattform waren die T-Labs der Deutschen Telekom AG verantwortlich und setzten hierbei technisch auf MS Azure auf. Das auf Maschinenseite verwendete Kommunikationsmodul stammt vom Konsortialführer Logic Way. Sowohl auf Maschinen- als auch auf Cloud-Seite werden korrespondierende Apps genutzt, um den jeweiligen Service in seiner Gesamtlogik abzubilden. Durch Eigenintelligenz kann das Maschinen-Kommunikationsmodul phasenweise autonom operieren und asynchron kommunizieren und dadurch z. B. temporär fehlende Netzabdeckung verlustfrei überbrücken. Im System wurde dafür ein Edge- bzw. Fog-Computing-Ansatz in Anlehnung an das oneM2M Framework umgesetzt [4]. Lokale Aufgaben können damit vor Ort und in Echtzeit auch bei lückenhafter Netzabdeckung sicher bearbeitet werden.

Die beiden Use Cases „Tele Expert“ und „Connected Update“ zeigen, dass sowohl der Kunde als auch der Hersteller oder sein Serviceanbieter über die virtuelle Plattform in der Lage sind, herstellerübergreifend auf ihre Maschinen und Daten zuzugreifen. So können Systemverbesserungen via Updates an der Software eingespielt oder kleinere Fehler im System „remote“ behoben werden, ohne dass ein Servicemitarbeiter dafür vor Ort sein muss. Ein Servicemitarbeiter kann sich aus der Ferne aufschalten, da die technische Umsetzung eine herstellerübergreifende Sicht über die Nutzungsdaten der angeschlossenen Maschinen und Geräte ermöglicht. Dies senkt den Aufwand für Servicedienstleistungen erheblich, da Vor-Ort-Services minimiert werden können, und steigert die Effizienz, indem Ersatzteile direkt für den Servicefall angepasst bezogen werden können. Darüber hinaus wird auch der Landwirt entlastet, denn die Technik funktioniert im Zusammenspiel, auch wenn sie von unterschiedlichen Herstellern stammt. Im Industrieumfeld existieren diverse Anwendungsfälle, die von den hier gewonnenen Erkenntnissen profitieren können.

Die zwei weiteren Anwendungsfälle betreffen die Ernteoptimierung von Landmaschinen. Im Use Case „nPotato“ durchläuft der vom DFKI konzipierte Sensorknoten in Form einer künstlichen Kartoffel den Ernteprozess und liefert Informationen zur Beanspruchung innerhalb der Landmaschine. Die zusätzlichen Informationen bereichern dann den Datensatz, der zur Optimierung der Ernte zur Verfügung steht, indem sichtbar gemacht wird, welche Einstellungen an der Maschine gezielt verändert werden sollten. So hat der Landwirt die Möglichkeit, schnell zu reagieren und Beschädigungen zu vermeiden. Meldet die digitale Kartoffel zum Beispiel besonders starke Stöße, kann er die Erntemaschine sofort auf schonendere Behandlung umschalten. Der Kartoffelroderhersteller Grimme kann durch die von ihm initiierte „nPotato“ die kundenseitigen Anforderungen besser umsetzen. Die Erkenntnisse aus diesem Szenario sind übertragbar auf vielfältige Anwendungsfälle im Bereich der landwirtschaftlichen Lebensmittelproduktion.

Der Use Case „Fleet Set Connect“, für den die Firma CLAAS verantwortlich war, zeigt, wie über die Plattform eine Vielzahl von Maschinen mit optimalen Einstellungen betrieben werden kann. Hierbei wird durch einen externen Berater oder eine sogenannte Master-Maschine eine optimale Erntestrategie vorgegeben. Diese wird dann über die Plattform mit allen an der Ernte des jeweiligen Feldes beteiligten Maschinen geteilt, sodass die optimale Erntestrategie flächendeckend eingesetzt wird. Dadurch wird zum einen die Produktivität gesteigert und zum anderen werden die Fahrer der einzelnen Landmaschinen entlastet.

Im Projekt Smart-Farming-Welt wurden vier Use Cases umgesetzt, die das Potenzial einer Smart-Service-Plattform im Bereich Landwirtschaft demonstrieren. Das FIR an der RWTH Aachen zeichnet dabei für die Entwicklung der Geschäftsmodelle der Use Cases verantwortlich und stellte eine nutzerzentrierte Entwicklung durch begleitende Nutzerbefragungen sicher.

Sicherheits- und rechtsrelevante Herausforderungen

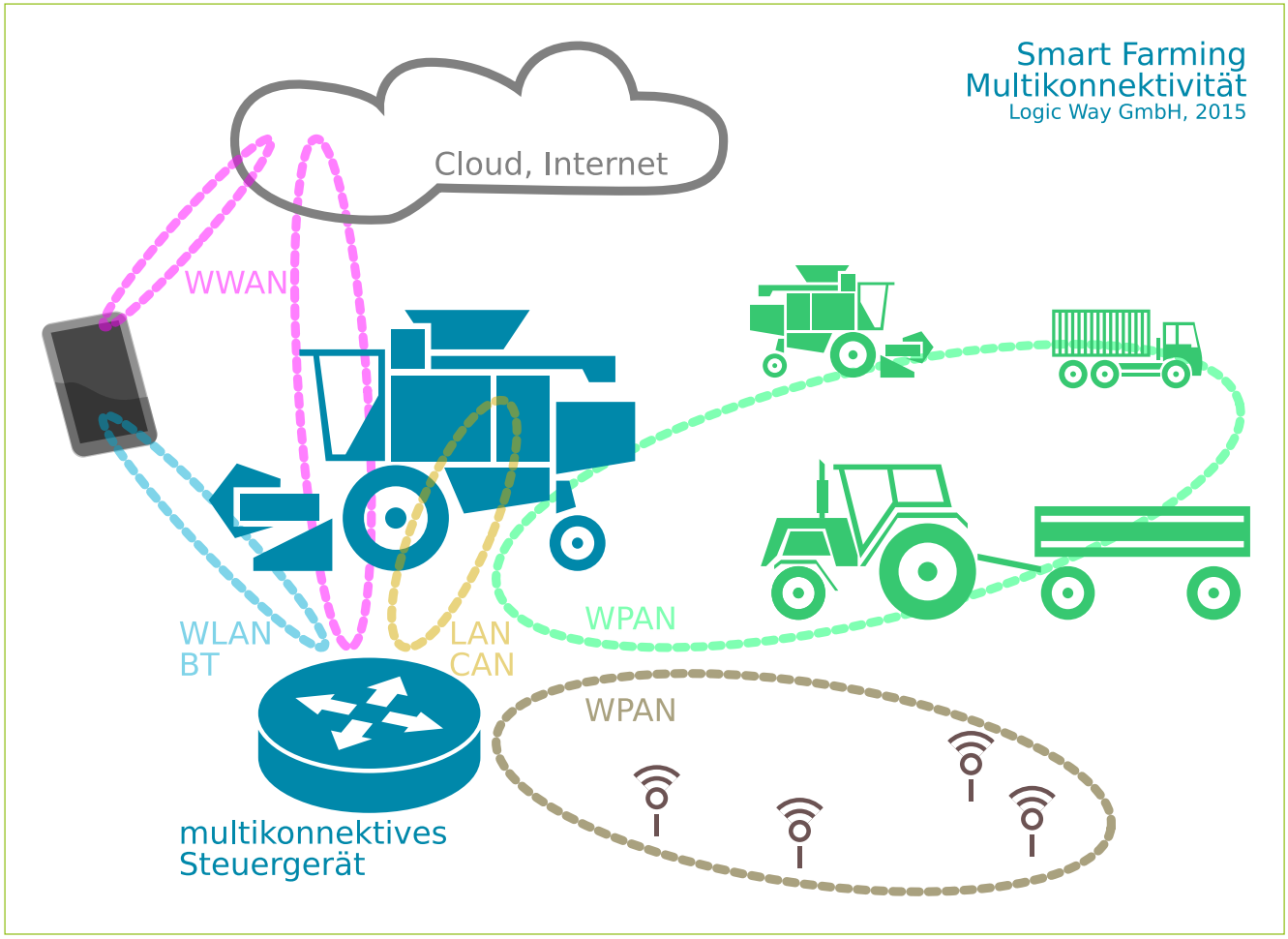

Abbildung 4: Multikonnektive Vernetzung beim Maschineneinsatz auf dem Feld

Bei dem Ansatz, einen herstellerübergreifenden Zugang zu Landmaschinen, Systemen und Services zu erhalten, spielt die Offenheit der Plattform eine zentrale Rolle [5]. Diese wird zunächst durch einheitliche Standards auf physischer Ebene (ISOBUS) und durch offene Application Programming Interfaces (API) auf IT-Ebene gewährleistet. Die klare Abgrenzung von Funktionen, Schnittstellen, Komponenten und Datenportionen innerhalb der Softwarestruktur kommt einem sicheren Betrieb zugute. Unter diesen Voraussetzungen können externe Akteure neue Applikationen entwickeln und im Rahmen der Plattform etablieren. Darüber hinaus sind bestehende Akteure in der Lage, mit anderen Partnern zu kooperieren und untereinander Informationen auszutauschen, was als entscheidendes Qualitätsmerkmal identifiziert wurde. Als eine wesentliche Grundbedingung für die Akzeptanz einer herstellerübergreifenden Smart-Farming-Plattform müssen sicherheitsrelevante Aspekte umgesetzt werden. Hierfür werden die Angriffsvektoren auf der Ebene der Anwendung, des Betriebssystems (sowie der Hardware) und auf der Ebene des Netzwerkverkehrs betrachtet und entsprechende Maßnahmen ergriffen. Die Kommunikation zwischen den jeweiligen Instanzen (Landmaschine, Hersteller, Cloud) erfolgt über standardisierte Schnittstellen (MQTT, REST). Die gegenseitige Authentisierung funktioniert dabei zertifikatsbasiert. Hier wurden im Rahmen des Projekts unterschiedliche Verfahren evaluiert, um ein sowohl aus (sicherheits-)technischer Sicht als auch hinsichtlich der Nutzerfreundlichkeit optimales Verfahren

zu verwenden. Die über die Plattform implementierten kundenspezifischen Dienste (also diejenigen, die nicht bereits vom Cloud-Anbieter bereitgestellt werden) müssen Best Practices für sichere Software-Entwürfe und sichere Software-Implementierungen folgen. Wie in anderen IT-Systemen, so werden auch im Smart-Farming-Umfeld für Plattformen Schutzziele [6] definiert, die einen sicheren Betrieb unterstützen:

- Vertraulichkeit: Daten sind gegen unautorisierten Zugriff und Modifikation geschützt. Dies gilt sowohl für die Übertragung als auch die Speicherung von Daten.
- Integrität: Unautorisierte Änderungen von Daten müssen erkannt werden. Änderungen an den Daten müssen zurechenbar sein (vgl. Zurechenbarkeit).
- Authentizität: Der Ursprung und die Echtheit von Daten sind erkennbar und nachweisbar.
- Nichtabstreitbarkeit: Kommunikationspartner können den Ursprung und die Authentizität von Daten nicht anfechten. Dies wird durch geeignete kryptografische Verfahren (z. B. Signaturen) sichergestellt.
- Zurechenbarkeit: Der Urheber einer Kommunikation bzw. eines Datums kann eindeutig zugeordnet werden.
- Verfügbarkeit: Das System muss innerhalb definierter Rahmen (also z. B. ohne vereinbarte Wartungsfenster) vorhanden und für den geplanten Einsatzzweck nutzbar sein.

Des Weiteren definiert der Betreiber Maßnahmen, die ergriffen werden, sollte ein Cyberangriff doch Erfolg haben. Dies geschieht im Rahmen einer Risikoanalyse. Die Plattform muss so schnell wie möglich wieder in Betrieb genommen werden, da eine langfristige Unterbrechung der Plattform gravierende ökonomische Folgen nicht nur für die Kunden, sondern auch für alle restlichen Beteiligten nach sich ziehen kann [7].

Im Rahmen der im Projekt gewählten Anwendungsfälle wurden reine Maschinendaten ohne Personenbezug erhoben und verarbeitet. Dennoch wird im Sinne des Arbeitnehmerschutzes darauf zu achten sein, ob durch den Austausch der Daten auf Produktionsebene nicht auch unerlaubte Rückschlüsse auf das Arbeitnehmerverhalten möglich werden. Da die herstellerübergreifende Anbindung über eine virtuelle Plattform realisiert wird, werden die jeweiligen Daten zwischen korrespondierenden Maschinen- und Cloud-Apps lediglich von Ende zu Ende durchgeleitet.

Digitaler Fingerabdruck zum optimalen Umgang mit fragmentieren Daten

Wie bereits dargestellt, werden in der landwirtschaftlichen Produktion und auch im Herstellungsprozess von Nahrungsmitteln unterschiedlichste Prozessbeteiligte in vielen Arbeitsgängen mit teilweise verschiedenen Interessen vereint. Somit ergeben sich Datenbestände, die in hohem Maße fragmentiert sind. Wenn die Inhalte aus unterschiedlichen Datensammlungen zusammengeführt werden, lässt sich der Prozess im Hinblick auf z. B. Produkteigenschaften, Bodenzustand und Prozessoptimierung durchgehend digital abbilden. Da die am Prozess beteiligten Produktionsmittel – wie Grund und Boden, Landmaschinen, Fahrzeuge oder Verarbeitungsanlagen – im Besitz unterschiedlicher Parteien sind, lässt sich auch keine generelle Eigentümerschaft einer bestimmten Partei an allen Daten bestimmen. Es könnten daher alle Prozessbeteiligten und letztendlich auch Verbraucher profitieren, wenn gegenseitig Daten ausgetauscht und somit die Abläufe und Zusammenhänge im landwirtschaftlichen Prozess durchgängig digital abgebildet werden können. Rein sachlich motiviert, ergeben sich verschiedene auszutauschende Dateninhalte und es scheint logisch und unstrittig, diese an die jeweils betreffenden Prozessteilnehmer weiterzugeben. Dabei ist der Landwirt in aller Regel gleichermaßen Produzent wie Konsument von Daten. In einem hypothetischen Idealfall, wenn alle Prozessbeteiligten Teilnehmer der gleichen Plattform sind, können sachliche Kriterien direkt und uncodiert abgefragt werden. In realen Situationen lässt sich eine vollständige digitale Informationslage allerdings nur herstellen, wenn Daten aus unterschiedlichen Plattformen (z. B. der unterschiedlichen Hersteller) zusammengeführt werden.

Bei Abfragen über Betreibergrenzen hinweg dürfen keine Informationen bereits durch diese Abfragen abfließen. Das wäre der Fall, wenn beispielsweise Uhrzeiten und Positionen, wann, wo an wen die Güter übergeben werden, im Klartext abgefragt würden. Die Herausforderung liegt somit in der berechtigten Forderung, Daten automatisiert feingranular und präzise begrenzt auszutauschen, um auf digitaler Ebene real ablaufende Vorgänge ausreichend exakt abzubilden. Die Identifikation der Parteien, die im Informationsaustausch stehen, und der jeweiligen Datenportionen muss dabei anhand von Eigenschaften dieser Informationen und Daten automatisiert erfolgen. Hierzu wird ein kryptografischer Schlüssel zum Austausch

einer bestimmten Datenportion errechnet. Die Abfrage des Schlüssels gegenüber den potenziellen Datenaustauschpartnern kann so gestaltet werden, dass für unberechtigte Empfänger der Abfrage keine Rückschlüsse auf den originalen Sachverhalt möglich sind. Berechtigte Datenanforderungen werden automatisch von solchen ohne diese Berechtigung unterscheidbar. Dazu wird aus charakteristischen Eigenschaften eines realen Prozessablaufes ein digitaler Fingerabdruck ermittelt, den beide jeweils beteiligten Parteien separat berechnen können. Für die Berechnung von Fingerabdrücken einer Interaktionssituation stehen die Ausgangsgrößen Zeitpunkt, Ort, Menge und Sorte des ausgetauschten Gutes, Fahrgeschwindigkeit etc. zur Verfügung. Die zu übertragenden Dateninhalte werden präzise eingegrenzt und minimiert. Damit wird die Datensparsamkeit als Designkriterium umgesetzt und darüber hinaus Datenschutz- und Geheimhaltungs-Belangen aller Beteiligten Rechnung getragen [8].

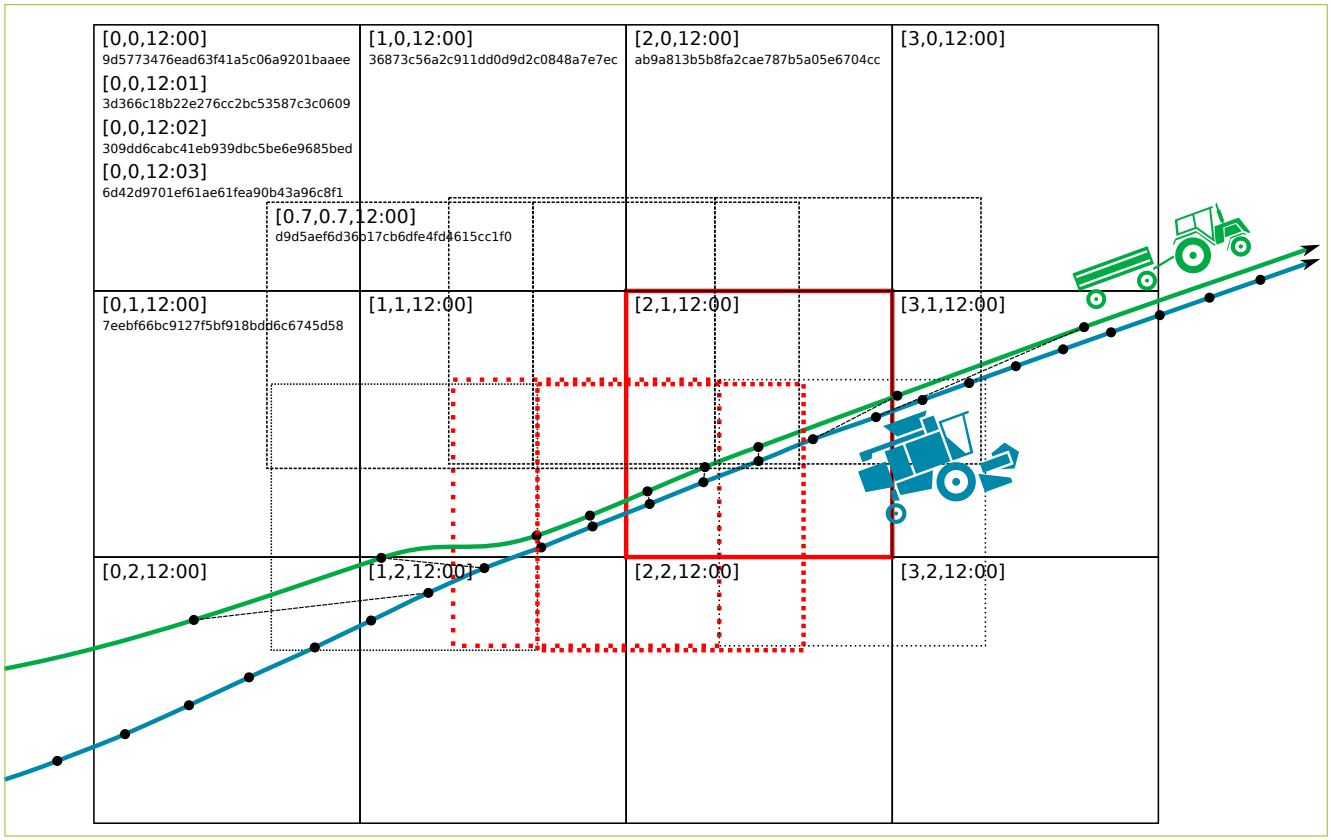

Abbildung 5: Beispielhafte Berechnung von Situations-Fingerprints für eine Gutübergabe zwischen Erntemaschine und Transportfahrzeug

Projekterkenntnisse und Ausblick

Der Erfolg einer herstellerübergreifenden Smart-Farming-Plattform ist, wie dargestellt, von unterschiedlichen Faktoren abhängig, die aber mit entsprechendem Aufwand technisch umsetzbar sind. Wichtig für eine Akzeptanz ist auch die Anlehnung der technischen Lösung an den globalen oneM2M-Standard [10].

Die vier gewählten Use Cases zeigen, dass Digitalisierung und Vernetzung Wege und Potenziale zur Bewältigung der Herausforderungen in der Landwirtschaft hinsichtlich Ressourceneffizienz, Ernteertrag, Lebensmittelqualität und Umweltschutz eröffnen. Entscheidend wird dabei sein, ob es gelingt, für alle beteiligten Akteure einen Nutzen über entsprechende Geschäftsmodelle herauszuarbeiten. Nur dadurch wird die für eine breite Anwendung von Smart Services in der Landwirtschaft erforderliche Akzeptanz herstellbar sein. Nach wie vor ist eine lückenhafte Mobilfunkabdeckung im ländlichen Raum für flächendeckende Anwendung von Smart Services hinderlich. Staatliche Infrastrukturmaßnahmen oder entsprechende Regulierung (z. B. wer für den Netzausbau sorgt, erhält anderweitige Vergünstigungen, oder bestimmte Netzressourcen werden für die Landwirtschaft bei Bedarf zur Verfügung gestellt), wären ein zukunftsträchtiges Modell. Eine Einbeziehung in die momentan stattfindende Network Slice Definition der GSMA bezüglich der Gestaltung von 5G ist daher wünschenswert. Die Landwirtschaft mit ihren speziellen Anforderungen hinsichtlich hoher Datenraten in schlecht versorgten Gebieten an wenigen Zeitpunkten im Jahr – an diesen aber stabil – bleibt derzeit hier unberücksichtigt. Zu einem möglichen Einsatz eines plattformunabhängigen Identity Management wird im Rahmen des Projekts auch „Verimi" betrachtetet. Das Ziel von Verimi, die sicherste und nutzerfreundlichste Vertrauensplattform für Identitätsdienste und Zahlungen in Europa zu schaffen [9], deckt sich mit den Anforderungen, die eine Smart-Farming-Plattform an sichere Authentifizierung stellt. Darüber hinaus sehen die Autoren einen stetigen Forschungsbedarf bezüglich der Rechtssicherheit von Plattformarchitekturen für die digitale Ökonomie, ohne die eine erfolgreiche Etablierung von herstellerübergreifenden Smart Services für Anbieter und Anwender weiterhin riskant ist.

Literaturverzeichnis

[1] Smart-Farming-Welt: https://smart-farming-welt.de/ (zuletzt geprüft 16.07.2018).

[2] Moser, B.; Rösner, C.: UdZ – Unternehmen der Zukunft 2/2017: Smart Services für die Landwirtschaft, Smart-Farming-Welt: Erfolgsfaktoren für eine herstellerübergreifende Smart-Service-Plattform in der Landwirtschaft.

[3] Kagermann, H.; Riemensperger, F.; Hoje, D.; Schuh, G.; Scheer, A.-W.; Spath, D.; Leukert, B.; Wahlster, W.; Rohleder, B.; Schweer, D. (Hrsg.): [Abschlussbericht] Smart Service Welt – Umsetzungsempfehlungen für das Zukunftsprojekt Internet-basierte Dienste für die Wirtschaft. Berlin, März 2015. BerichtSmartService2015_D_lang_bf.pdf (zuletzt geprüft 16.07.2018).

[4] IoT, from Cloud to Fog Computing. blogs@Cisco – Cisco Blogs.: http://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing (zuletzt geprüft 10.07.2018).

[5] Engels, G.; Plass, C.; Ramming, F.-J. (Hrsg.): acatech DISKUSSION. IT – Plattformen für die Smart Service Welt: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/acatech_disku tiert/acatech_DISKUSSION_IT-Plattformen_WEB.pdf (zuletzt geprüft 16.07.2018).

[6] Eckert, C.: IT-Sicherheit. Konzepte – Verfahren – Protokolle. 7., überarbeitete und erweiterte Auflage. Oldenbourg, 2012.

[7] Janzen S.; Kritzner. A.; Marquardt, S.; Rösner, C.; Mildner, F.; Moser, B.; Rusch, C.; Maaß, W.: Dokument: AP3.7 – Smart-Farming-Welt – Pflichtenheft, Version 0.28 vom 23.03.2017.

[8] Kritzner, A.; Teichmann, J.: [GIL-Jahrestagung 2018] „Situations-Fingerabdruck" – Verwaltungsstruktur-übergreifendes automatisiertes Berechtigungsmanagement für landwirtschaftliche Daten nach sachbezogenen Kriterien.

[9] Verimi: https://verimi.com/#about-us (zuletzt geprüft 16.07.2018).

[10] oneM2M - TS-0001-V2.18.1, Functional Architecture, 2018-03-12: http://www.onem2m.org/images/files/deliverables/Release2A/TS-0001-Functional_Architecture-v_2_18_1.pdf (zuletzt geprüft 17.07.2018).

4.2 STEP – Digitale Plattformen für den Mittelstand – Ein Wegbereiter für vorausschauende Instandhaltung

Corinna Brecht[16], Henrik Oppermann[17]

Motivation

Qualitätsmerkmal „Made in Germany“: Die Produktion im deutschen Mittelstand genießt einen hervorragenden Ruf. Damit das so bleibt, werden Produkte und deren Produktionswege kontinuierlich verbessert, sodass diese im Markt gegen die häufig günstigere Konkurrenz aus Niedriglohnländern bestehen können. Eine wichtige Rolle spielt dabei auch die Optimierung der Instandhaltung und des technischen Service.

Moderne Service- und Wartungskonzepte erfordern gerade im Zeitalter von Industrie 4.0 eine hohe technologische Kompetenz. Dies stellt insbesondere für Mittelständler eine Herausforderung dar, weil es sich für einzelne Unternehmen kaum lohnt, abseits ihrer Kernkompetenzen technologisches Know-how in diesen Bereichen aufzubauen. Plattformbasierte Lösungen können hier Abhilfe schaffen, indem die Entwicklungs- und Betriebskosten auf viele Teilnehmer verteilt werden. Gleichzeitig tragen Plattformen zur Standardisierung von Prozessen bei und fördern somit den Austausch und die Zusammenarbeit über Unternehmensgrenzen hinweg. Im Forschungsprojekt STEP (Smarte Techniker-Einsatzplanung) haben Partner aus Wissenschaft und Industrie gemeinsam an einer solchen Lösung gearbeitet.[18]

Heutzutage wird in Branchen wie dem Maschinen- und Anlagenbau vor allem reaktiv und präventiv gewartet. Reaktiv bedeutet, dass ein Einsatz dann stattfindet, wenn die Maschine bereits eine Fehlfunktion aufweist. Die präventive Wartung kennt man vom eigenen Auto: Es wird regelmäßig nach einem Indikator wie dem Kilometerstand oder nach Zeitintervallen geprüft, ob mit der Maschine noch alles in Ordnung ist. Das Auto muss daher alle zwei Jahre zum TÜV. Die klassischen Wartungsmodelle sind in den Serviceorganisationen der Unternehmen in aller Regel in standardisierten Prozessen und Vorgängen durchdacht und optimiert, indem beispielsweise die Auftragsverwaltung digitalisiert wurde.

Im Zeitalter von Industrie 4.0 ermöglichen intelligente Maschinen und vernetzte Anlagen bereits heute durch die Erfassung und Übertragung von Maschinen- und Betriebsdaten eine vorausschauende Wartung (Predictive Maintenance). Hierfür werden Methoden der künstlichen Intelligenz eingesetzt, um aus den erzeugten Daten vorherzusagen, wann ein Instandhaltungsbedarf besteht. Aus der Vorhersage ergibt sich dann eine komplett neue Planungsbasis für Wartungsmaßnahmen. Werden diese Informationen erfolgreich genutzt, kann die Häufigkeit von Einsätzen reduziert und gleichzeitig die Verfügbarkeit von Maschinen erhöht werden.

Damit nun allerdings zum passenden Zeitpunkt ein geeigneter Servicetechniker mit den notwendigen Ersatzteilen in die Fabrik entsendet werden kann, sind noch viele weitere Informationen notwendig. Es muss etwa ermittelt werden, wie lange der Einsatz voraussichtlich dauert, welche Lieferzeiten für Ersatzteile einzuplanen sind, welche Priorität der Einsatz hat und auf welcher Tour die geringsten Mehrkosten entstehen. Die große Menge an für die Planung notwendigen Informationen und die Kombination verschiedener Wartungsstrategien sind für die zuständigen Mitarbeiter schwer zu überblicken. Dabei können sogenannte cyber-physische Systeme helfen, die beispielsweise Maschinendaten und Informationen zur Mitarbeiterverfügbarkeit oder zu deren technischen Fähigkeiten bündeln. Die Entwicklung und der Betrieb solcher Systeme, die eine Vielzahl von Schnittstellen für Menschen und technische Systeme erfordern, sind mit hohen Investitionskosten verbunden. Die Verlagerung auf geteilte, beispielsweise von verschiedenen Maschinenherstellern ebenso wie von unterschiedlichen Beteiligten einer Wertschöpfungskette (z. B. Anlagenbetreiber und Wartungsservice) gemeinsam genutzte Plattformen, die in einer Cloud betrieben werden, bietet neben der besseren Wirtschaftlichkeit noch weitere Vorteile: Kapazitäten können flexibel erhöht werden, neue Geschäftsmodelle durch Kooperationen mit anderen Unternehmen entstehen oder eine Verknüpfung von der Produktionsplanung des Kunden mit der Einsatzplanung der Serviceorganisation hergestellt werden. Plattformen erlauben es dem deutschen Mittelstand, bei tragbaren Investitionskosten auch in Zukunft beim Service mit großen Konzernen mithalten zu können.

16 Zentrum für Angewandte Rechtswissenschaft (ZAR), KIT.
17 USU Software AG.
18 STEP-Konsortium: USU Software AG (Konsortialführer), FLS GmbH, Heidelberger Druckmaschinen AG, Karlsruher Institut für Technologie (KIT), TRUMPF Werkzeugmaschinen GmbH + Co. KG.

Informationsfluss und Plattformarchitektur

STEP hat in einem ersten Schritt eine Analyse der typischen Prozessschritte und Informationsflüsse im technischen Service mit den beiden Praxispartnern erarbeitet. Dabei lässt sich der technische Serviceprozess grob in vier wesentliche Phasen untergliedern, die in Abbildung 6 dargestellt sind:

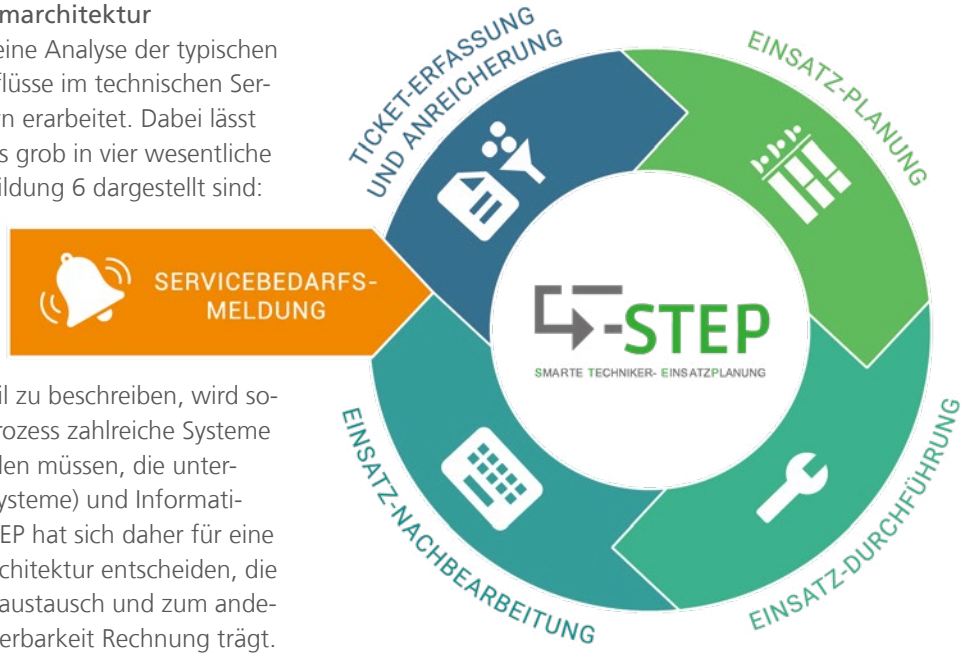

Abbildung 6: Der STEP-Prozess

Ohne die Prozessschritte im Detail zu beschreiben, wird sofort klar, dass in diesen Gesamtprozess zahlreiche Systeme und Beteiligte eingebunden werden müssen, die unterschiedliche Daten bereitstellen (Systeme) und Informationsbedarfe haben (Beteiligte). STEP hat sich daher für eine Message-orientierte modulare Architektur entscheiden, die zum einen dem intensiven Datenaustausch und zum anderen der nahezu beliebigen Erweiterbarkeit Rechnung trägt.

Eine besondere Betrachtung erhielt aufgrund der Zielstellung des Projekts die vorausschauende Wartung (Predictive Maintenance). Daher wurden in einem zweiten Schritt die verschiedenen Phasen dahingehend untersucht, ob sich durch Digitalisierung, Zusammenführung von Daten und Information und Automatisierung von Entscheidungen bestimmte Prozessschritte so automatisieren lassen, dass der Vorteil der Vorhersage von Wartungsbedarfen maximal genutzt wird.

Das Projekt identifizierte dabei zwei wesentliche Prozessschritte, die in der jetzigen betrieblichen Praxis meist manuell gehandhabt werden und zeitaufwendig sind, nämlich a) die Servicetechniker-Einsatzplanung und b) die informationstechnische Vorbereitung der Wartungsdurchführung. Gerade in großen Service-Organisationen ist die Verplanung von hunderten oder tausenden von Servicetechnikern (a) auf eine noch größere Anzahl von Maschinen eine planerische Herausforderung und daher meist wenig agil und mit Puffer versehen, um auf unvorhergesehene Ereignisse reagieren zu können. STEP setzte sich zum Ziel, diese Planung durch eine Simulation dynamisch anhand prädiktiver Servicemeldungen zu berechnen, um den Zeitfenstern gerecht zu werden. Dazu müssen eine Vielzahl von Informationen verarbeitet und Bedingungen eingehalten werden, u. a. auch die Kompetenzen oder Fähigkeiten der Servicetechniker, ihre Verfügbarkeit und der Zeitbedarf. Zur Vorbereitung des durchzuführenden Wartungsfalls (b) müssen dann zahlreiche Informationen bereitgestellt werden. Dazu gehören Reparaturanweisungen, Werkzeugeinstellungen und Bauteilinformationen, aber zunehmend auch die Maschinenhistorie. Zudem zeigt die betriebliche Praxis, dass Servicetechniker zunehmend den Einsatz sozialer Kommunikationsmedien wie Chats einsetzen, um sich mit Kollegen zu vernetzen, die die notwendige Expertise und Maschinenkenntnisse haben, um bei der Wartungsdurchführung zu helfen. STEP hat sich zum Ziel gesetzt, ein cyber-physisches soziales Ressourcen-Netzwerk (CPRN) zu entwerfen, das alle relevanten Daten und Informationen für Wartungsfälle zusammenträgt, dem Servicetechniker überall Maschinendaten zur Verfügung stellt und den Austausch mit Kollegen ermöglicht. Bei dem CPRN handelt es sich um eine Kommunikationsplattform für Personen innerhalb eines Unternehmens, welche zum Austausch von Nachrichten genutzt werden soll. Sinn und Zweck ist die gegenseitige Unterstützung bei der Lösung von technischen Problemstellungen in Bezug auf Kundeneinsätze. Darüber hinaus bietet die Plattform den Servicetechnikern Zugriffsmöglichkeit auf eine Wissensdatenbank, welche nützliche Informationen zu Fehlerdiagnosen und -behebungen bietet.

Weiterhin wurde untersucht, wie sich Dritte an dem Gesamtprozess beteiligen lassen. Dies können z. B. Subunternehmer sein, die bereitgestellte Daten und Aufträge nutzen, um für die Service-Organisation Wartungsaufträge durchzuführen, wenn die eigene Kapazität nicht ausreicht, der Wartungsauftrag durch mangelnde eigene Expertise nicht ausreichend bedient werden kann oder der Einsatz wirtschaftlich von untergeordnetem Interesse ist.

Aus diesen Anforderungen ergab sich für die STEP-Plattform folgende Architektur (Abbildung 7):

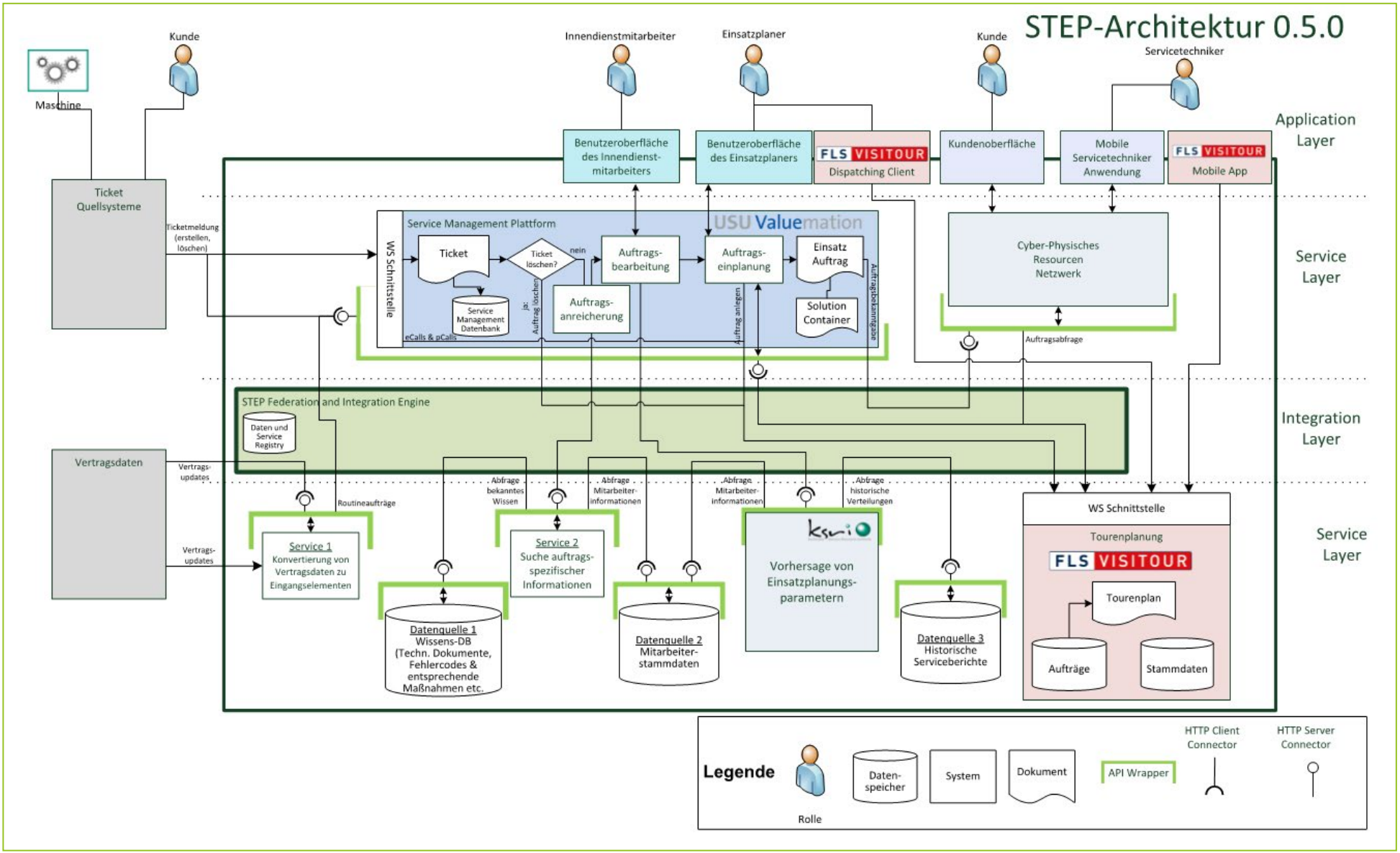

Abbildung 7: Die STEP-Architektur

Die datenschutzrechtliche Herausforderung besteht nun darin, diese Informationsströme und die Bereitstellung der Informationen zu analysieren und zu beurteilen. Daraus sollten Handlungsempfehlungen und Anforderungen an die Datensicherheit und an den Datenschutz formuliert werden, die dann in der Architektur durch Algorithmen und Methoden (z. B. Anonymisierung und Pseudonymisierung) zu berücksichtigen sind (Privacy- und Security-by-Design).

Rechtswissenschaftliche Betrachtung und Berücksichtigung in der Plattform

Im Projekt STEP war aus rechtswissenschaftlicher Sicht vorgesehen, dass die personenbezogenen Daten für die Einsatzplanung der Servicetechniker, wie deren Verfügbarkeit, Fähigkeiten, Einsatzberichte und gegebenenfalls auch Standortdaten zur Routenplanung, erhoben werden, um Entscheidungen entlang des oben beschriebenen Prozesses zu beschleunigen und zu automatisieren. Außerdem ist es denkbar, Daten Dritten zur Verfügung zu stellen, wie z. B. Services zur Vorhersage von Wartungserfordernissen, und diese am Gesamtprozess und der Wertschöpfung zu beteiligen. Dadurch werden verschiedene rechtliche Fragestellungen aufgeworfen, die im Folgenden behandelt werden.

Personenbezogene Daten

Die Gefahr der Erfassung von personenbezogenen Daten am Arbeitsplatz, durch die Servicetechniker zunehmend transparenter werden, ist nicht zu unterschätzen. Dadurch kann ein Überwachungsgefühl für sie entstehen, sodass sie sich in ihrem Verhalten stark beeinträchtigt fühlen. Es ist daher unabdingbar, das Direktionsrecht des Arbeitgebers und das Recht auf informationelle Selbstbestimmung der Arbeitnehmer gegenüberzustellen und die unterschiedlichen Interessen bei der vorliegenden Einführung neuartiger Technologien sowie bei automatisierten Entscheidungsmöglichkeiten in Einklang zu bringen. Gemäß Art. 88 DSGVO in Verbindung mit § 26 Abs. 1 BDSG dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses sowie für die Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Maßgeblich für die Beurteilung der Erforderlichkeit ist es, eine Abwägung zwischen der unternehmerischen Freiheit des Arbeitgebers, aus der sich insbesondere das Direktionsrecht ableitet, einerseits und der informationellen Selbstbestimmung des Arbeitnehmers andererseits vorzunehmen. Das Direktionsrecht umfasst die Zuweisung von Ort, Zeit und Inhalt der Arbeitsleistung, darf aber nicht zu einem unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen führen[19]. Aufgrund der in STEP erhobenen Daten ist es möglich, Bewegungsprofile zu erstellen und das Arbeitsverhalten zu analysieren. Dies kann einen psychischen Anpassungsdruck beim Arbeitnehmer erzeugen, welcher den Servicetechniker in seiner Freiheit, aus eigener Selbstbestimmung zu planen und zu entscheiden, wesentlich hemmt [20]. Die Verarbeitung der am Arbeitsplatz generierten Daten muss deshalb verhältnismäßig sein.

Bei der Verhältnismäßigkeitsprüfung ist zu berücksichtigen, dass dem Arbeitgeber ein gewisser Beurteilungsspielraum zusteht, welche Maßnahmen er für geeignet und erforderlich hält, um sein Ziel zu erreichen. Datenverarbeitungen, die zu einer Totalüberwachung des Beschäftigten führen (gegebenenfalls auch erst durch eine Zusammenführung unterschiedlicher Datenarten bzw. Datenquellen), sind jedoch nicht zulässig[21].

Deshalb und um dem Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit c) DSGVO gerecht zu werden, wurden in STEP Pseudonymisierungs- und Anonymisierungsverfahren in Bezug auf die Einsatzberichte der Servicetechniker implementiert und darauf geachtet, dass Standortdaten soweit wie möglich nur partiell erfasst werden. Des Weiteren wurden Rollen- und Zugriffsrechte festgelegt, wonach nur ein begrenzter Personenkreis im Unternehmen Zugang zu den personenbezogenen Daten besitzt.

Zur Optimierung der Techniker-Einsatzplanung wurde in STEP ein cyber-physisches soziales Ressourcen-Netzwerk (CPRN) konzipiert.

19 Wank, in: Tettinger/Wank/Ennuschat, GewO, 8. Auflage 2011, § 106 GewO Rn. 1.ff.
20 BAG, Urt. v. 27.07.2017 – 2 AZR 681/16; LAG Hessen, Urt. v. 25.10.2010 – 7 Sa 1586/09 Rn. 42.
21 Schmidl, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Auflage 2016 § 28 Rn. 367-370.

Ein bestimmter Personenkreis, im Wesentlichen die Servicetechniker und Einsatzplaner, erhalten ähnlich wie bei Facebook ein Profil, welches Eigenschaften und Charakteristika der Person ausweist. Die sogenannten Basisinformationen können nur vom Einsatzplaner geändert werden. Bestimmte von den Personen einzugebenden Zusatzinformationen können bei Bedarf für andere Personen freigegeben werden. Der Servicetechniker kann zudem seine Serviceaufträge einsehen und nach seinem Einsatz seinen Einsatzbericht ablegen. Der Bericht wird dann in einer gesonderten Datenbank pseudonymisiert bzw. anonymisiert gespeichert.

In diesem Zusammenhang stellte sich insbesondere die Frage, ob die Verwendung der Profil- und Messengerfunktion auf eine gesetzliche Erlaubnisnorm gestützt werden kann oder ob vielmehr eine Einwilligung des Beschäftigten (bzw. eine Betriebsvereinbarung etc.) erforderlich ist. Für die Abstimmung und Planung der Einsatztermine ist die CPRN-Kommunikation aufgrund der möglichen Nutzung anderer Kommunikationswege ohne Kontrollmöglichkeit durch den Arbeitgeber lediglich als nützlich und gerade nicht als erforderlich einzustufen. So kann die Nutzung des CPRN nicht auf eine gesetzliche Erlaubnisnorm gestützt werden. Allerdings kann bspw. auf eine Betriebsvereinbarung oder auch Einwilligung des Beschäftigten zurückgegriffen werden, wobei in letztem Fall die jederzeitige Widerrufbarkeit und die erhöhten Anforderungen an die Freiwilligkeit der Einwilligung im Arbeitsverhältnis zu berücksichtigen sind.[22]

Die telekommunikationsrechtliche und telemedienrechtliche Prüfung des CPRN ist aufgrund der sich noch im Gesetzgebungsverfahren befindenden ePrivacy-Verordnung, in der u. a. vorgesehen ist, dass Daten in der elektronischen Kommunikation nur nach Einwilligung genutzt werden dürfen, und den damit zusammenhängenden offenen Fragen im Zusammenhang mit der DSGVO und dem deutschen Recht offen.

Automatisierte Einzelfallentscheidungen

Bei der rechtswissenschaftlichen Betrachtung wurde auch dem Verbot der automatisierten Einzelfallentscheidung gem. Art. 22 DSGVO in Verbindung mit § 37 BDSG Rechnung getragen. Das Gesetz sieht vor, dass eine natürliche Person zu einem Objekt einer Entscheidung degradiert wird, indem sie nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen werden darf, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Es ist nicht auszuschließen, dass ein Servicetechniker mit seinen verschiedenen Eigenschaften vom Einsatzplanungstool vollautomatisiert (ohne Beteiligung einer natürlichen Person) ausgewählt und einem Kundenauftrag zugeordnet wird und dies zu erheblichen Beeinträchtigungen des Servicetechnikers führen kann. Hier stellt sich die Frage, ob der Gesetzgeber auch solche Anwendungsfälle als mitumfasst ansieht. In STEP wurde einerseits aus unternehmerischen Gesichtspunkten und andererseits aus Gründen der Rechtskonformität entschieden, dass ein Einsatzplaner die Entscheidung über die Einsatzplanung verantwortet, d. h. einen Entscheidungsspielraum besitzt und eine spezifische Richtigkeits- und Plausibilitätskontrolle vornimmt. Hierbei ist zu beachten, dass die natürliche Person sowohl die fachlichen Kenntnisse als auch den Entscheidungsspielraum haben muss[23].

Daten als Wirtschaftsgut

Zur Generierung weiterer auf Plattformen basierender Märkte ist es denkbar, dass die durch Sensoren übermittelten Rohdaten, welche bedeutende Wirtschaftsgüter sind, externen Dritten zur Analyse zu Verfügung gestellt werden. Dadurch könnten z. B. Services genutzt werden, die die Ausfallzeiten oder auch die Wartungsbedürftigkeit einer Maschine vorhersagen. Auf einem Markplatz könnte nicht nur eine Analyse, sondern auch ggf. ein Auftrag für die erforderliche Wartung angeboten werden. Inwiefern der

22 (BAG, Urt. v. 11.12.2014 – 8 AZR 1010/13, NJW 2015; vgl. Däubler, CR 2005, 767, 770).

23 von Lewinski, in Wolff/Brink, Beck OK Datenschutzrecht, 24. Edition, Art. 22 Rn. 24, 25.

Zugang zu nicht personenbezogenen Daten einer gesetzlichen Regulierung bedarf, wird derzeit diskutiert und ist noch nicht abschließend geklärt. Die Gefahr, durch eine gesetzliche Regelung gleichzeitig eine Marktzutrittsschranke zu generieren und die Wettbewerbsfreiheit unangemessen zu beschränken, ist jedenfalls nicht von der Hand zu weisen, sodass eine Heranziehung der bereits bestehenden wettbewerbsrechtlichen Vorschriften, insbesondere § 18 GWB („Marktbeherrschung"), sinnvoll ist.

Empfehlungen

Wie beschrieben, ist die telekommunikationsrechtliche und telemedienrechtliche Prüfung des CPRN aufgrund der sich noch im Gesetzgebungsverfahren befindenden ePrivacy-Verordnung und der damit zusammenhängenden Fragen im Zusammenhang mit der DSGVO und dem deutschen Recht offen. Für die Abstimmung und Planung der Einsatztermine ist die CPRN-Kommunikation aufgrund der möglichen Nutzung anderer Kommunikationswege ohne Kontrollmöglichkeit durch den Arbeitgeber lediglich als nützlich und gerade nicht als erforderlich einzustufen. Die Nutzung des CPRN kann nicht auf eine gesetzliche Erlaubnisnorm gestützt werden. Daher sollte auf eine Betriebsvereinbarung oder auch Einwilligung des Beschäftigten zurückgegriffen werden, wobei in letztem Fall die jederzeitige Widerrufbarkeit und die erhöhten Anforderungen an die Freiwilligkeit der Einwilligung im Arbeitsverhältnis zu berücksichtigen sind.[24]

Zu beachten ist bei der Prozessgestaltung auch das Verbot der automatisierten Einzelfallentscheidung gemäß Art. 22 DSGVO in Verbindung mit § 37 BDSG, welches verhindern soll, dass eine natürliche Person zu einem Objekt einer Entscheidung degradiert wird. Dies trifft vor allem bei der Generierung von Arbeitsaufträgen in der Servicetechniker-Einsatzplanung zu. In STEP wurde aus Gründen der Rechtskonformität entschieden, dass ein Einsatzplaner die Entscheidung über die Einsatzplanung trifft und verantwortet und nicht ausschließlich ein System.

Ob die Verwendung nicht personenbezogener Daten (z. B. der Sensordaten der Maschinen) als Wirtschaftsgut auf einer Art Markplatz einer gesetzlichen Regulierung bedarf, wird derzeit diskutiert und ist noch nicht abschließend geklärt. Die Gefahr, durch eine gesetzliche Regelung gleichzeitig eine Marktzutrittsschranke zu generieren und die Wettbewerbsfreiheit unangemessen zu beschränken, ist nicht von der Hand zu weisen, sodass eine Heranziehung der bereits bestehenden wettbewerbsrechtlichen Vorschriften, insbesondere § 18 GWB, vorzugswürdig erscheint. Unternehmen, die dies planen, wird empfohlen, bilaterale Verträge mit den jeweiligen Beteiligten zu schließen. So können Service-Organisationen etwa die Nutzung bestimmter digitaler Servicedienstleistungen an Zugang, Bereitstellung und Nutzungsrechte der Daten binden.

24 BAG, Urt. v. 11.12.2014 – 8 AZR 1010/13, NJW 2015; vgl. Däubler, CR 2005, 767, 770).

4.3 Sichere internetbasierte Vermarktung cyber-physischer Systeme mit SmartOrchestra

L. Ashauer, U. Breitenbücher, A. C. Franco da Silva, O. G. Gemein, T. Günther, M. Hahn, K. Képes, E. Kleinod, O. Kopp, F. Leymann, A. Liebing, B. Mitschang, P. Niehues, D. Olschewski, K. Semmler, R. Steinke, J. van Well, M. Virtel[25]

Motivation und Projektziele

In den letzten Jahren sind cyber-physische Systeme (CPS) in verschiedensten Fachdomänen jenseits von Industrie 4.0 entstanden, unter anderem getrieben durch stark gesunkene Kosten. Das Potenzial dieser Insellösungen lässt sich durch Kombination und Orchestrierung zu smarten Diensten wesentlich erhöhen. Die Vision von SmartOrchestra ist daher ein Ökosystem, in dem Smart Services aus isolierten CPS und Anwendungen durch und für kleine und mittlere Unternehmen (KMU) erstellt, angeboten, sicher betrieben und vermarktet werden können. Um diese Vision umzusetzen, entwickelt SmartOrchestra eine sichere, offene, internetbasierte und auf Standards basierende Smart Service Plattform zur Unterstützung eines solchen Ökosystems, welche die Funktionen Ausführungsumgebung, Modellierungsumgebung und Marktplatz für den Betrieb zur Verfügung stellt.

Anwendungsfelder und Szenarien

Im Anwendungsszenario von regio iT möchte ein Servicenutzer sein Vorhersagemodell zum Gebäudeenergieverbrauch durch den Einsatz externer Sensoren verbessern. Er besitzt in seinen Gebäuden bereits diverse Sensoren zur Messung von Temperaturen, Strom- und Gasverbräuchen und will zusätzlich den Faktor des Windes auf seine Gebäudefassade in das Energieverbrauchsvorhersagemodell einfließen lassen. Im Normalfall würde er auf dem Dach und an der Fassade einen oder mehrere Windmesser installieren und diese Daten in sein Modell einfließen lassen. Die Installation und Wartung wäre mit entsprechend hohen Kosten verbunden, insbesondere wenn Verkabelungsarbeiten an entlegenen Gebäudestellen notwendig werden. Viel einfacher wäre es für den Nutzer jedoch, wenn er die Winddaten vom Nachbargebäude verwenden könnte, bei dem derartige Sensoren zur Steuerung von Jalousien bereits installiert sind. In diesem Fall kann ein zukünftiger Nutzer der SmartOrchestra-Plattform im Marktplatz einen entsprechenden Sensor kaufen und in Betrieb nehmen. Die erfassten Sensordaten können anschließend in einer einfachen Visualisierung grafisch ausgewertet werden. Im Weiteren kann dem Nutzer im Marktplatz ein Angebot des Service e2watch von regio iT unterbreitet werden, sodass die Daten automatisiert an e2watch weitergeleitet und ausgewertet werden. Der Mehrwert entsteht durch die wesentlich komplexeren und intelligenteren Auswertungsmöglichkeiten von Sensordaten durch den Service e2watch. Der Service verfügt über ein Stör- und Alarmmanagement und kann nicht nur Fehlerzustände erkennen und Aktivitäten auslösen, sondern zukünftig auch automatisiert Anomalien erkennen. Durch die vollständige Integration des Service e2watch in SmartOrchestra kann regio iT als Anwendungspartner neue Kunden gewinnen, indem regio IT ihren Service mit geringem Aufwand an weitere Sensoreigentümer anbinden kann.

Im Rahmen von SmartOrchestra werden durch den Anwendungspartner Cleopa GmbH mehrere Smart Services getestet und weiterentwickelt. Der Service InHealth, ein Angebot für Wohngebäude zur Prävention von Schimmel, welcher bisher als proprietäre Lösung vorhanden ist, kann durch den SmartOrchestra-Marktplatz und die Konnektoren weiter verbessert und das Geschäftsmodell optimiert werden. Während bisher nur eigene Sensoren mit der Serviceplattform verbunden sind, können in Zukunft auch externe Sensordaten eingebunden werden. Somit könnte InHealth auch als WhiteLabel-Lösung über die SmartOrchestra-Plattform genutzt werden. Im Jahr 2018 hat der Anwendungspartner Cleopa GmbH sich auch mit Narrow Band Internet of Things (NB-IoT) im Bereich Low Power Wide Area Networks auseinandergesetzt sowie zahlreiche Tests mit den am Markt heute verfügbaren Gateways und Sensoren verschiedener Hersteller durchgeführt. Das NB-IoT ermöglicht eine besonders großflächige Abdeckung für den Empfang und die Übertragung der Funksignale und schafft es auch, besonders dicke Betonmauern zu durchdringen und dadurch auch entlegene Winkel eines Gebäudes wie beispielsweise Kellerräume zu erreichen. Diese Technologie bildet eine solide Basis für Performancetests der Cloud Server im Zusammenspiel mit den IoT-Gateways und Sensoren, um eine spätere Skalierung und Vermarktung der SmartOrchestra-Lösungen zu ermöglichen. Weitere Smart Services im Rahmen

25 Liste der Autoren alphabetisch sortiert.

des Energiemanagements und Audits sind derzeit in der technischen Vorbereitung.

Vom Konsortialpartner Datenfreunde werden die Smart Services Ambient News, Smart Mirror, Story Trolley, xMinutes, AudioRoad, OpenWeatherMap, ReportBuilder und SmartOrchestra Alexa Skill entwickelt. Exemplarisch wird im Folgenden die Nutzung der Plattform für den ReportBuilder und den SmartOrchestra Alexa Skill beschrieben. Im ReportBuilder werden aus Sensordaten durch natürliche Sprachverarbeitung (Text-to-Speech) Audio-Warnungen oder auch Mitteilungen über den aktuellen Zustand der mit Sensoren ausgestatteten Räume in Audioform, d. h. als natürliche Sprache, produziert. Damit können e2watch- und Schimmeldaten über die SmartOrchestra-Plattform zu höherwertigen Informationen weiterverarbeitet werden. Eine Ausgabe kann über SmartOrchestra sprachbasiert mithilfe des Alexa Skills erfolgen. Diese kann über den Marktplatz an e2watch und den ReportBuilder gekoppelt werden, womit gezeigt wird, dass auch hier eine Smart-Service-Komposition ermöglicht wird.

Rollen, Akteure und Geschäftsmodelle
Smart Services sind Dienste, die Endnutzern intelligente, cyber-physische Funktionalität bereitstellen und von Smart-Service-Herstellern entwickelt werden. Beispielsweise interagieren sie mit Sensoren wie Temperaturfühlern und steuern Aktuatoren, um bei bestimmten Werten die Fenster eines smarten Hauses zu schließen. Sensoren und Aktuatoren fallen typischerweise in das Eigentum verschiedener Interessengruppen wie Städte, Rechenzentren oder Privatpersonen. Es handelt sich somit um cyber-physische Umgebungen bei Eigentümern.

Der Smart-Service-Marktplatz ermöglicht es Endnutzern, nach Smart Services zu suchen, diese zu kaufen und anschließend auch zu nutzen. Dabei unterscheidet sich der Zugang aktuell zwischen den Rollen Smart-Service-Anbieter und Smart-Service-Hersteller wie folgt:

- Der Smart-Service-Anbieter registriert einen bereits laufenden Service beim Marktplatz, um diesen für Endnutzer anzubieten. In diesem Fall kümmert sich der Smart-Service-Anbieter selbst um die Bereitstellung, das Management und den Betrieb des Service. Wie der Service implementiert ist und wie der Anbieter die Bereitstellung und den Betrieb des Service umsetzt, ist für die anderen Rollen und Komponenten der Smart-Orchestra-Plattform nicht sichtbar. Beispielsweise kann der Anbieter beliebige Service-Plattformen zum Betrieb des Service einsetzen. Eine Nutzung der SmartOrchestra-Plattform zum Betrieb des Smart Service ist jedoch im Rahmen des Projekts das Hauptszenario.
- Der Smart-Service-Hersteller entwickelt einen Smart Service und übermittelt diesen in Form eines Smart-Service-Pakets an den Marktplatz. Das eingesetzte portable Smart-Service-Paketformat basiert auf dem Paketformat Cloud Service Archive (CSAR) des TOSCA-Standards [1] und ermöglicht es dem Marktplatz, dieses Paket zur Bereitstellung des jeweiligen Service auf verschiedenen Smart-Service-Plattformen einzusetzen. Das Smart-Service-Paket enthält dazu alle Daten, die zur Bereitstellung und zum Betrieb des Smart Service erforderlich sind, und ermöglicht es Marktplätzen, effizient verschiedene standardkonforme Smart-Service-Hersteller als Entwickler sowie Smart Service Plattform Provider als Infrastrukturanbieter einzubinden.

Weitere Rollen sind denkbar. Die SmartOrchestra-Plattform erlaubt es einem Stakeholder, auch mehrere Rollen einzunehmen. So kann ein Stakeholder beispielsweise sowohl ein Smart-Service-Anbieter sein als auch Services in der Rolle des Endnutzers/Kunden nutzen.

Geschäftsmodelle im Bereich der Smart Services sind hinreichend durch Kagerman u. a. [2] (acatech) oder aktuell in v. Engelhardt u. a. [3] (VDI/VDE) als „X-as-a-Service"-Ansätze beschrieben. In allen digitalen Märkten spielen Daten eine zentrale Rolle. Der Austausch von Daten – und damit Fragen der Inkompatibilität und Interoperabilität – ist für digitale Systeme zentral. SmartOrchestra adressiert genau dieses Problem und ermöglicht den Nutzern ein Maximum an Interoperabilität per Design, indem es das Servicedesign der verschiedenen Rollen (Hersteller und Anbieter) getrennt orchestriert. Die Cleopa GmbH als Konsortialpartner konnte deshalb für den Service InHealth ein völlig neues Geschäftsmodell anwenden. Bisher wurde der Service als geschlossenes Produkt (Onlineplattform, Datenspeicher und Sensor) angeboten. Jetzt werden die einzelnen Produktbestandteile entkoppelt und auf dem Marktplatz angeboten – wodurch neue Sensoren von Herstellern integriert werden können und die intelligente Auswertungssoftware neuen Anwendern als reiner Service angeboten werden kann.

Auch die Konsortialpartner regio iT und die Datenfreunde profitieren von der Plattform, welche durch den Konsortialführer StoneOne bereits in einer voll lauffähigen Beta-Version gezeigt werden kann, um jetzt den Markteintritt vorzubereiten und Pilotkunden zu gewinnen. Das Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS und die Universität Stuttgart liefern dazu die notwendigen Konzepte und Plattformkomponenten zur technischen Integration, zu Management, Betrieb und Komposition von Smart Services. Die SmartOrchestra-Plattform und ihre Komponenten werden im folgenden Abschnitt näher beschrieben.

Entscheidungen für die Festlegung der Plattformarchitektur

Die SmartOrchestra-Plattform ermöglicht eine einheitliche Beschreibung von Smart Services sowie eine sichere internetbasierte Komposition und Integration heterogener cyber-physischer Systeme und Dienste auf Basis standardisierter Cloud- und Orchestrierungstechnologien. Die Plattform liefert sowohl einen transparenten Katalog zur Bewertung geeigneter Dienste aus einem breiten Ökosystem als auch eine operative Schnittstelle zwischen Steuergeräten und Sensoreinheiten und deren jeweiligen Anwendungen. Auf diese Weise liefert SmartOrchestra eine offene, sichere und standardisierte Smart Service Plattform.

Abbildung 8 zeigt die Konzeption der SmartOrchestra-Plattform und ihrer wichtigsten Komponenten in Kombination mit Provisionierungs-Workflows und IoT-Geräten. Der zentrale Einstiegspunkt in die Plattform ist der Marktplatz, der es den Nutzern ermöglicht, bestehende Smart Services aus dem Servicekatalog zu suchen, zu bewerten, zu betreiben und zusammenzuschalten (komponieren) sowie neue Services anzubieten und zu vermarkten. Die Daten jedes laufenden Smart Service können über den Marktplatz in kundenspezifischen Dashboards mit Hilfeassistenten (Widgets) und konfigurierbaren Katalogen und Abhängigkeiten zwischen den Services und Datenpools strukturiert

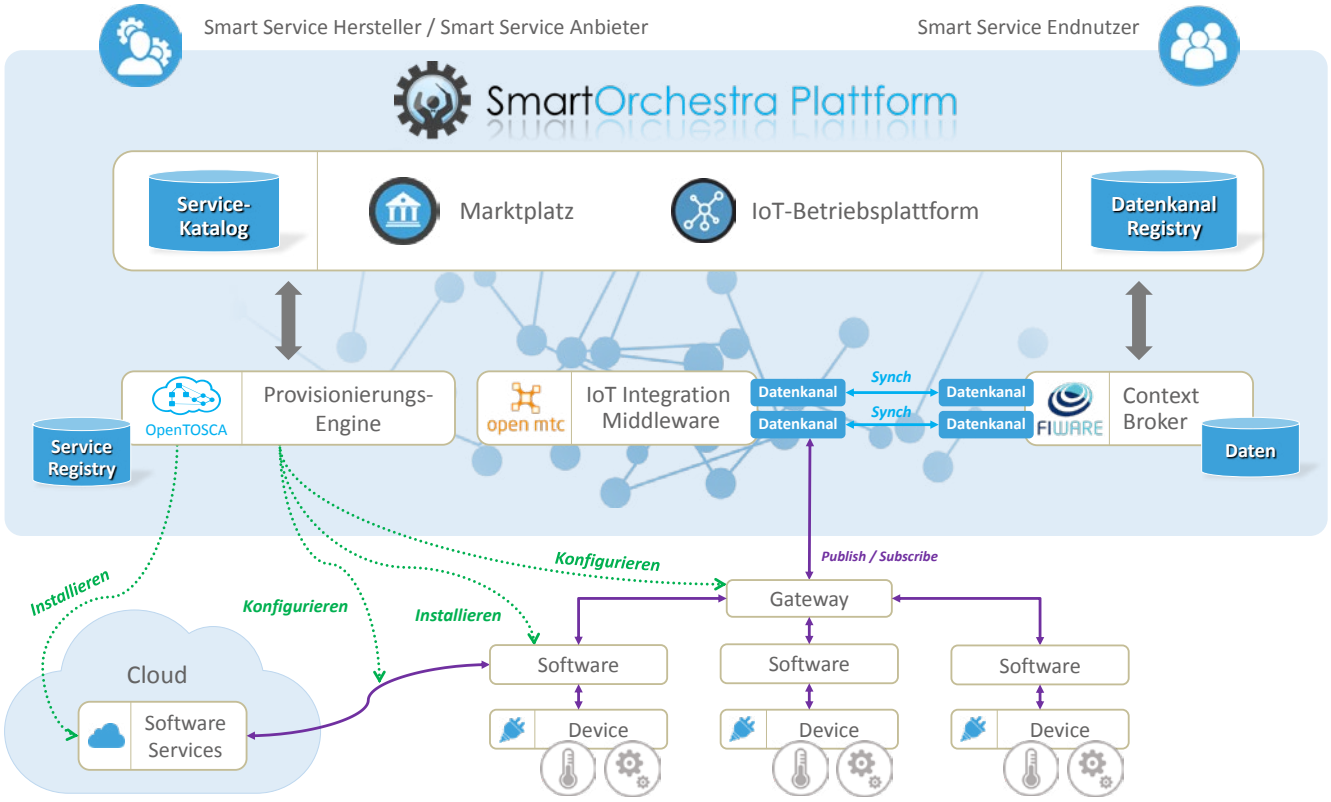

Abbildung 8: SmartOrchestra-Plattformarchitektur

dargestellt werden. Dadurch wird der Marktplatz zur IoT-Betriebsplattform.

Zur Bereitstellung und Konfiguration von Smart Services wird OpenTOSCA [4], [5] als Provisionierungs-Engine verwendet. Die Provisionierungs-Engine ist für die automatisierte Bereitstellung eines Smart Service und die Konfiguration der zugrundeliegenden Infrastruktur verantwortlich. Dies kann z. B. die Installation benötigter Software-Services in der Cloud, die die Geschäftslogik eines Smart Service bereitstellen (z. B. Datenfilterung, -verarbeitung oder -aggregation [6]), die Konfiguration von IoT-Geräten und Gateways oder die Installation der benötigten Software auf diesen umfassen. OpenTOSCA liefert zusätzlich die entsprechende Werkzeugunterstützung für die Modellierung von Smart Services auf Basis des Standards OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) [1], [7]–[14] und weiterer Konzepte für CPS und IoT [15]–[18].

Für die Integration von IoT-Geräten in Smart Services nutzt die SmartOrchestra-Plattform OpenMTC [19], [20] als IoT Integration Middleware [21], [22]. OpenMTC ist eine Open-Source-Implementierung des oneM2M-Standards [23] und darüber hinaus als FIWARE Generic Enabler [24] verfügbar. OpenMTC stellt so die erforderlichen Protokolle und Adapter zur Verfügung, um die heterogenen Geräte, Sensoren und Aktuatoren innerhalb der SmartOrchestra-Plattform zu integrieren und zwischen diesen zu vermitteln. Dafür bringt OpenMTC einen eingebetteten Service-Layer mit, der die Kommunikation zwischen den Geräten über ein Publish/Subscribe-Modell ermöglicht. Darüber hinaus stellt die SmartOrchestra-Plattform den FIWARE Orion Context Broker [25] als Context Broker zur Verfügung. Während OpenMTC für die Kommunikation zwischen Geräten, Sensoren und Aktuatoren über entsprechende generische Schnittstellen zuständig ist, wird der FIWARE Orion Context Broker in Kombination mit FIWARE STH-Comet [26] als Data Repository zur mittelfristigen Speicherung von Daten eingesetzt, um eine spätere Analyse der von IoT-Geräten gelieferten Daten zu ermöglichen. Dazu synchronisiert OpenMTC alle veröffentlichten Daten mit dem FIWARE Orion Context Broker, wie in Abbildung 8 durch die Synchronisationspfeile zwischen den Datenkanälen der beiden Komponenten dargestellt.

Umsetzung der relevanten rechtlichen Aspekte in der Plattform

Die im System gehandelten Daten sind wertvoll für den Anbieter der Daten. Je nach Stärke des Personenbezugs können sie dem Datenschutz in unterschiedlicher Ausprägung unterliegen. Dies kann im Extremfall auch Datenschutz nach dem Sozialgesetzbuch bedeuten.

Für SmartOrchestra bedeutet dies zunächst die Absicherung der Daten in Bezug auf Datenhoheit, also die Nutzung der Daten nur mit Zustimmung des Anbieters. Darunter fällt beispielsweise der Abschluss von Verträgen, die unter Einhaltung der Datenschutzgesetze entworfen und vorgelegt werden. Zum anderen müssen die Anforderungen des Datenschutzes mithilfe von Werkzeugen wie Daten- und Übertragungsverschlüsselung, Zugangskontrolle, Anonymisierung bzw. Pseudonymisierung der erhobenen Daten, die im Rahmen der Anwendung verarbeitet werden, Einsatz eines Datennotars oder einer Blockchain mit Smart Contracts u.v.m. sichergestellt werden. Welche Technik gewählt wird und wie die Zugriffskontrolle der Komponenten geregelt wird, ob die Blockchain z. B. privat oder öffentlich ist, hängt vom Einsatzzweck des Gesamtszenarios ab.

Die Absicherung der Datenhoheit ist damit innerhalb des Systems zuverlässig zu leisten. Schwieriger ist die Einhaltung des Datenschutzes, da technisch schwer abzuschätzen ist, ob

1. die Daten des Systems untereinander kreuzreferenziert werden können, und
2. die Daten ausreichend anonymisiert oder pseudonymisiert sind, um keine Rückschlüsse zuzulassen und trotzdem die Aussagekraft des Anwendungsfalls zu gewährleisten.

Wenn z. B. das Dusch- und Lüftungsverhalten von Mietern überwacht wird, sind die Einzeldaten im System abzulegen, um sowohl Vermieter als auch Mieter ausreichend Informationen zur Verfügung zu stellen. Wenn die gleichen Daten für den Wasserversorger zur Verfügung gestellt werden, müssen sie aufbereitet werden, um die Prinzipien des Datenschutzes gegenüber anderen Parteien einzuhalten. Möglichkeiten wären, Mittelwerte aus der Summe der Messdaten zwischen den verschiedenen Mietern zu errechnen, Namen zu entfernen oder ganze Straßenblöcke zusammenzufassen.

Die Vertrauenswürdigkeit des Systems wird über den Einsatz bewährter standardisierter Methoden erzielt. Dabei kommen By-Design-Ansätze zum Tragen, d. h. der jeweilige Sicherheitsaspekt wird bereits beim Design berücksichtigt, um die Umsetzung der Sicherheit nicht den Nutzern zu überlassen. So wird beispielsweise jegliche Kommunikation verschlüsselt. Dies kann nicht umgangen werden, sondern ist fest im System eingebaut. Das Rollen- und Rechtekonzept wird über Authentifizierung umgesetzt. Die Rechte werden im System hinterlegt und über OpenTOSCA ausgerollt. Sie können nicht ausgehebelt werden. Die Rechtevergabe muss einmal erfolgen, hier ist die Aufmerksamkeit der Nutzer gefragt. Sind die Rechte vergeben, werden sie vom System durchgesetzt. Für die anwendungsübergreifende Autorisierung wird auf das OAuth[26]-Protokoll zurückgegriffen. Die Verwaltung der Nutzenden erfolgt mittels LDAP[27] durch den Marktplatz.

Die Absicherung der Sensoren und Aktuatoren erfolgt z. B. mit Zertifikaten. SmartOrchestra bietet die Möglichkeit an, Zertifikate zur Absicherung des Zugriffs einzusetzen. Das Ausrollen und Ändern der Zertifikate übernimmt OpenTOSCA in Zusammenarbeit mit dem Marktplatz. Inwieweit diese Art der Absicherung nötig ist, hängt vom Anwendungsfall ab, da die Erzeugung und Verifizierung der Zertifikate Rechen- und Verwaltungsaufwand erfordert. Für sensible Sensoren oder Aktuatoren kann auch Mehrfaktorauthentifizierung definiert und ausgerollt werden. Die verwendeten Datenbanken können bei Bedarf verschlüsselt werden, dies wird besonders dann empfohlen, wenn die darin enthaltenen Informationen sensible bzw. kritische Daten darstellen. Zudem erfolgt die Wahrung der Privatsphäre über Vorverarbeitung der Daten durch Anonymisierungs- und Pseudonymisierungsverfahren.

Zusammengefasst bietet SmartOrchestra standardisierte Möglichkeiten der Systemabsicherung und zusätzlich noch systemtypische Möglichkeiten wie die erwähnte Blockchain. Der konkrete Einsatz der jeweiligen Technik wird vom System unterstützt, ist aber abhängig vom Szenario flexibel konfigurierbar. Die Standards werden auf dem Stand der Technik gehalten.

Datenkanalbasierte Komposition von Smart Services

Smart Services können mit der SmartOrchestra-Plattform auf verschiedene Arten komponiert werden. Eine davon ist eine Komposition unter Verwendung von Datenkanälen als Bindeglied. Die Daten von Smart Services mit entsprechenden CPS-Komponenten können mithilfe von OpenMTC als IoT Integration Middleware über einen Datenkanal (engl. „Channel“) an interessierte Empfänger publiziert werden. Die datenkanalbasierte Komposition ermöglicht so die Verbindung mehrerer Smart Services über gemeinsam genutzte Datenkanäle, auf die beispielsweise ein Smart Service Temperaturdaten publiziert (engl. „publish“), die ein anderer Smart Service abonniert (engl. „subscribe“) und so über alle neuen Daten automatisiert informiert wird. Datenkanäle ermöglichen es, Datenkonsumenten und Datenproduzenten als Blackbox lose miteinander zu koppeln und so zugleich flexibel und sicher zu verbinden. Auch wenn sich die technischen Umsetzungen eines entsprechenden Datenkanals in den verschiedenen IoT-Integration-Middleware-Lösungen unterscheiden [21], [22], wird das zugrunde liegende Publish/Subscribe-Konzept unterstützt. In SmartOrchestra wurden beispielsweise Mosquitto[28] und OpenMTC mittels MQTT[29] [27] gekoppelt, um zu zeigen, dass zur Umsetzung von Datenkanälen Messaging einfach verwendet werden kann. Die Technologieunabhängigkeit erlaubt es Smart-Service-Herstellern, ihre Smart Services durch die Beschreibung von eingehenden und ausgehenden Datenkanälen unabhängig und flexibel zu modellieren. Andere Smart-Service-Hersteller oder Endnutzer können dann diese Smart Services nutzen und komponieren, indem sie die benötigten und bereitgestellten Datenkanäle miteinander verbinden.

Einbindung externer Service-Anbieter in die SmartOrchestra-Plattform

Damit auch externe Service-Anbieter ihre Services einfach in das SmartOrchestra-Ökosystem integrieren können, um diese über den Marktplatz anzubieten, stellt SmartOrchestra ein entsprechendes Smart-Service-Beschreibungsformat zur Verfügung. Dies erlaubt es, wichtige Parameter wie beispielsweise Datenformate oder Einheiten von Sensordaten (z. B. °C, %, hPa) für die Datenkanäle und

26 OAuth – ein offenes Protokoll für eine standardisierte und sichere API-Autorisierung für Desktop-, Web- und Mobile-Anwendungen.
27 Das Lightweight Directory Access Protocol (LDAP) – ein Netzwerkprotokoll zur Abfrage und Änderung von Informationen verteilter Verzeichnisdienste.
28 Mosquitto – eine Messaging-Broker-Komponente für MQTT (Message Queuing Telemetry Transport).
29 MQTT (Message Queuing Telemetry Transport) – ein Nachrichtenprotokoll für Machine-to-Machine-Kommunikation für die Übertragung von Telemetriedaten in Form von Nachrichten zwischen Geräten.

CPS-Komponenten eines Smart Service zu beschreiben. Die so spezifizierten Daten werden zusammen mit dem Topologie-Modell des Smart Service als TOSCA CSAR paketiert. Im Gegensatz zu Smart Services, die innerhalb der SmartOrchestra-Plattform ausgeführt werden, beschreibt dabei das erstellte Topologie-Modell nicht eine zukünftige Provisionierung des Smart Service innerhalb der Plattform, sondern lediglich die Komponenten und deren Parameter (z. B. IP-Adressen, Endpunkte usw.) der existierenden externen Services. Dies ist notwendig, um die Komposition von Plattform-internen und -externen Smart Services zu ermöglichen. Dabei wird davon ausgegangen, dass die externen Services ebenfalls entsprechende Datenkanäle spezifizieren, um deren Komposition in SmartOrchestra zu realisieren. Die zur Instanziierung der Plattform-internen Smart Services benötigten Parameter werden durch den Marktplatz automatisiert bereitgestellt.

Lessons Learned: Empfehlungen an Plattformbetreiber und Serviceentwickler

Serviceentwickler sollten sich frühzeitig mit Sicherheitsaspekten und möglichen Haftungsproblemen auseinandersetzen, um bereits während des Designs ihrer Smart Services auf diese eingehen zu können. Im Rahmen von SmartOrchestra stellte sich eine Absicherung „by design" als am besten planbar und umsetzbar heraus. Ein entscheidender Punkt dabei ist die möglichst genaue Festlegung der Grenze zwischen technischer und rechtlicher Überprüfbarkeit, beispielweise durch das Aufsetzen entsprechender Verträge zwischen Plattformbetreiber und Serviceentwickler. Plattformbetreiber sollten klare Schnittstellen für Services und deren Komposition schaffen, um diese als Blackbox betreiben zu können und so sicherzustellen, dass vonseiten der Plattform kein Zugriff auf das Innenleben eines Service möglich ist. Darüber hinaus müssen sich Serviceentwickler auch mit Fragen der Anonymisierung/Pseudonymisierung von Daten befassen, da sie durch den Zugriff auf und die Verarbeitung von Daten in der Haftung sind. Der Einsatz bzw. die Schaffung entsprechender offener Standards ist ein entscheidender Schritt, um eine einheitliche Basis für die Modellierung, Komposition sowie den sicheren Betrieb und die Vermarktung von Smart Services zu schaffen.

Ausblick

In SmartOrchestra wurde an Konzepten zur Integration und Verarbeitung externer Sensordaten in der SmartOrchestra-Plattform sowie deren Vermarktung über den Marktplatz gearbeitet. Ziel ist die weitere Öffnung der Plattform für neue Nutzergruppen und neuartige Geschäftsmodelle. SmartOrchestra erlaubt dadurch nicht nur die Entwicklung, den Betrieb und die Vermarktung von Smart Services und deren Kompositionen, sondern ermöglicht es auch Anbietern, ihre vorhandenen Sensordaten einfach und sicher anderen Nutzern der SmartOrchestra-Plattform zur Verfügung zu stellen, damit diese die Daten in ihre Smart Services einbinden können. Zur Demonstration dieser und weiterer im Rahmen von SmartOrchestra erarbeiteten Konzepte wird ein entsprechender Showcase für das SmartOrchestra-Gesamtsystem entwickelt.

In Zukunft ist eine Vielzahl neuer Plattformen am Markt zu erwarten, die auch einen verstärkten Fokus auf die Datenverarbeitung innerhalb der Plattformen legen werden. Der Ausbau und die Akzeptanz entsprechender Standards sind dabei ein entscheidender Faktor für die Sicherstellung der Interoperabilität zwischen den Plattformen sowie für die Portabilität von Smart Services. Ebenso stellt die Absicherung von Smart Services und deren Datenverarbeitung, beispielsweise durch Zertifizierung über ein entsprechendes Prüfinstitut (z. B. TÜV), eine große und entscheidende Herausforderung für die Zukunft dar.

Literaturverzeichnis

[1] OASIS, Topology and Orchestration Specification for Cloud Applications (TOSCA) Version 1.0. 2013.

[2] H. Kagermann, „Chancen von Industrie 4.0 nutzen", in Handbuch Industrie 4.0 Bd.4: Allgemeine Grundlagen, B. Vogel-Heuser, T. Bauernhansl, und M. ten Hompel, Hrsg., Berlin, Heidelberg: Springer Berlin Heidelberg, 2017 [Online]. Verfügbar unter: https://doi.org/10.1007/978-3-662-53254-6_12

[3] S. von Engelhardt u. a., „Smart Service Welt – Innovationsbericht 2017", 2017 [Online]. Verfügbar unter: https://vdivde-it.de/publikation/smart-service-welt-innovationsbericht-2017.

[4] T. Binz u. a., „OpenTOSCA – A Runtime for TOSCA-based Cloud Applications", in ICSOC, 2013.

[5] A. C. Franco da Silva, U. Breitenbücher, K. Képes, O. Kopp und F. Leymann, „OpenTOSCA for IoT: Automating the Deployment of IoT Applications based on the Mosquitto Message Broker“, in IoT, 2016.

[6] A. C. Franco da Silva, P. Hirmer, U. Breitenbücher, O. Kopp und B. Mitschang, „Customization and provisioning of complex event processing using TOSCA“, Comput. Sci. – Res. Dev., 2017.

[7] O. Kopp, T. Binz, U. Breitenbücher und F. Leymann, „Winery – A Modeling Tool for TOSCA-based Cloud Applications“, in ICSOC, 2013.

[8] A. C. Franco da Silva u. a., „Internet of Things Out of the Box: Using TOSCA for Automating the Deployment of IoT Environments“, in CLOSER, 2017.

[9] M. P. Fischer, U. Breitenbücher, K. Képes und F. Leymann, „Towards an Approach for Automatically Checking Compliance Rules in Deployment Models“, in SECURWARE, 2017.

[10] U. Breitenbücher, T. Binz, K. Képes, O. Kopp, F. Leymann und J. Wettinger, „Combining Declarative and Imperative Cloud Application Provisioning based on TOSCA“, in IC2E, 2014.

[11] U. Breitenbücher, K. Képes, F. Leymann und M. Wurster, „Declarative vs. Imperative: How to Model the Automated Deployment of IoT Applications?“, in SummerSOC, 2017.

[12] K. Képes, U. Breitenbücher, M. P. Fischer, F. Leymann und M. Zimmermann, „Policy-Aware Provisioning Plan Generation for TOSCA-based Applications“, in SECURWARE, 2017.

[13] A. Bergmayr u. a., „A Systematic Review of Cloud Modeling Languages“, ACM Comput. Surv., Bd. 51, Nr. 1, 2018.

[14] T. Binz, G. Breiter, F. Leymann und T. Spatzier, „Portable Cloud Services Using TOSCA“, IEEE Internet Comput., Bd. 16, Nr. 03, 2012.

[15] K. Képes, U. Breitenbücher und F. Leymann, „Integrating IoT Devices Based on Automatically Generated Scale-Out Plans“, in SOCA, 2018.

[16] K. Saatkamp, U. Breitenbücher, F. Leymann und M. Wurster, „Generic Driver Injection for Automated IoT Application Deployments“, in iiWAS, 2017.

[17] A. C. Franco da Silva, P. Hirmer, U. Breitenbücher, O. Kopp und B. Mitschang, „TDLIoT: A Topic Description Language for the Internet of Things“, in ICWE, 2018.

[18] M. Zimmermann, U. Breitenbücher und F. Leymann, „A TOSCA-based Programming Model for Interacting Components of Automatically Deployed Cloud and IoT Applications“, in ICEIS, 2017.

[19] M. Corici u. a., „OpenMTC: Prototyping Machine Type communication in carrier grade operator networks“, in IEEE Globecom Workshops, 2012.

[20] Fraunhofer FOKUS, „OpenMTC Platform Architecture“, 2016. [Online]. Verfügbar unter: http://www.open-mtc.org/index.html#MainFeatures.

[21] J. Guth u. a., „A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences“, Springer, 2018.

[22] J. Guth, U. Breitenbücher, M. Falkenthal, F. Leymann und L. Reinfurt, „Comparison of IoT Platform Architectures: A Field Study based on a Reference Architecture“, in CIoT, 2016.

[23] oneM2M Partners, „oneM2M“, 2017. [Online]. Verfügbar unter: http://www.onem2m.org/

[24] Fraunhofer FOKUS, „OpenMTC Generic Enabler“, 2016. [Online]. Verfügbar unter:

https://catalogue.fiware.org/enablers/openmtc.

[25] FIWARE, „Orion Context Broker“, 2018. [Online]. Verfügbar unter: https://www.github.com/telefonicaid/fiware-orion.

[26] FIWARE, „Short Time Historic (STH) – Comet“, 2018. [Online]. Verfügbar unter: https://github.com/telefonicaid/fiware-sth-comet.

[27] „MQTT“. [Online]. Verfügbar unter: http://mqtt.org/.

Alle Links wurden zuletzt am 06. August 2018 aufgerufen.

4.4 GEISER – Von Sensordaten zu internetbasierten Geo-Services

Roman Korf[30]

Motivation und Projektziele

Vernetzte Systeme wie Produktionsmaschinen oder Fahrzeuge verfügen über vielfältige Sensoren, welche große Datenmengen produzieren. Hinzu kommt die steigende Bedeutung von Geodaten, die beispielsweise über GPS-Systeme in hohem Umfang erhoben werden. Die Erkenntnisse, welche aus diesen Daten gewonnen werden können, bergen großes wirtschaftliches Potenzial.
Im Projekt GEISER wurde eine cloudbasierte Micro-Service-Plattform entwickelt, welche diese Daten zur räumlichen Positionsbestimmung und zeitlichen Einordnung kombiniert, in ein einheitliches Format bringt und für neue intelligente Services und Produkte nutzbar macht. Basis der Architektur ist der Message-Bus, der eine Drehscheibe für die Kommunikation der datenverarbeitenden Dienste innerhalb der Plattform darstellt. Dadurch können die Potenziale, welche sich in den Daten verbergen, ausgeschöpft und somit neue Anwendungsgebiete erschlossen und neue Dienstleistungen entwickelt werden. Im Projekt wurden dazu verschiedene Dienste zur Verarbeitung und Speicherung der Daten sowie drei Anwendungsbeispiele – Intelligente Parkplatzsuche, Echtzeit Geomarketing sowie Servicetechniker-Einsatzunterstützung – entwickelt, um das Vorgehen zu evaluieren.

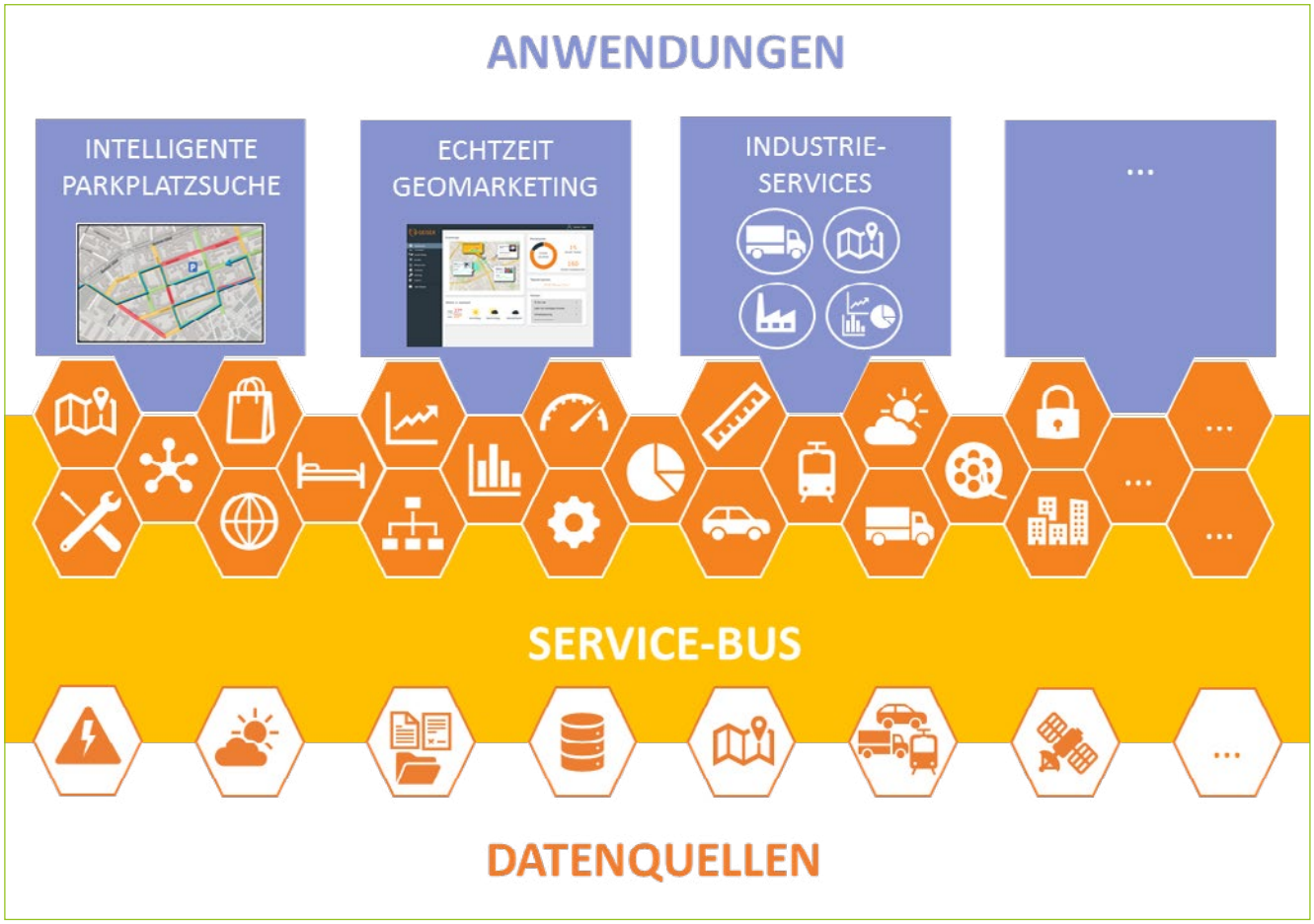

Abbildung 9: GEISER-Plattform

30 USU Software AG.

Innerhalb der Plattformökonomie ergeben sich verschiedene Rollen: Dazu gehören: (a) Plattformbetreiber, welcher die Plattform hostet, wartet und administriert, deren Nutzer verwaltet und die Nutzungsbedingungen definiert, (b) Datenlieferanten, welcher Daten bereitstellt und deren Nutzungsbedingungen definiert, (c) Diensteanbieter, welcher Dienste bereitstellt, diese integriert und deren Nutzungsbedingungen definiert, (d) Anwendungsanbieter, welcher auf Basis der Daten und Dienste konkrete Anwendungsfälle umsetzt (orchestriert) und (e) Nutzer, welcher die generierte Mehrwertinformation aus den Anwendungsfällen konsumiert. Einzelne Stakeholder der Plattformökonomie können dabei mehrere Rollen einnehmen. So kann beispielsweise der Plattformbetreiber gleichzeitig auch Diensteanbieter und Datenlieferant sein oder der Nutzer auch die Dienste- und Anwendungsumsetzung durchführen.

Der Betrieb der GEISER-Plattform und ihre Plattformökonomie stellen die Betreiber und weitere beteiligte Stakeholder vor verschiedene rechtliche Herausforderungen. Die Frage ist, welche das sind und welche Lösungen es gibt. Die folgenden Abschnitte betrachten einige der Herausforderungen und geben erste Vorschläge zu Lösungsansätzen.

Herausforderungen und Rahmenbedingungen

Sowohl aus der Architektur der Plattform und ihren Stakeholdern als auch aus den im Projekt umgesetzten Diensten und Anwendungsfällen ergeben sich rechtliche und sicherheitsrelevante Aspekte, die berücksichtigt werden müssen. Eine Auswahl von identifizierten Herausforderungen wird im Folgenden näher beleuchtet.

Datenschutz

Der Datenschutz greift innerhalb der Plattformökonomie an verschiedenen Stellen. Die Plattform erlaubt die Verarbeitung von Daten. Laut der Datenschutz-Grundverordnung (DSGVO) kann dies lediglich durch eine Einwilligung oder einen gesetzlichen Erlaubnistatbestand sichergestellt werden. Damit ist es notwendig zu prüfen, welche Daten verarbeitet werden, ob der Datenschutz greift und ob ein Erlaubnistatbestand gegeben ist oder nicht. Das ist im Einzelfall zu prüfen.

Innerhalb der Plattform soll es jedoch auch möglich sein, verschiedene Mandanten und Nutzer zu verwalten. Dazu werden Informationen der Nutzer gespeichert, was unter die DSGVO fällt.

Sicherheit

Innerhalb der GEISER-Plattform können unterschiedliche Datensätze verarbeitet werden. Es gibt verschiedene Gründe, diese zu schützen. Die DSGVO verlangt den ausreichenden technischen Schutz personenbezogener Daten. Dazu müssen ausreichende technische Mittel, wie beispielsweise Verschlüsselung und Zugriffskontrolle, eingesetzt werden. Aber auch nicht personenbezogene Daten müssen geschützt werden, wenn diese wettbewerbsrelevante oder andere kritische Informationen enthalten.

Datenhoheit

Ein weiterer Aspekt, welcher innerhalb der Lösung berücksichtigt werden muss, ist die Datenhoheit. Innerhalb der Plattform werden über Dienste Daten verarbeitet. Dabei entstehen neue, aggregierte Datensätze. Die Herausforderungen, die sich hier stellen, sind beispielsweise: Wem gehören die aggregierten Daten? Was passiert mit den aggregierten Daten, wenn die Originalquellen vom Datenlieferanten nicht mehr angeboten werden? Müssen diese gelöscht werden? Und nicht zuletzt: Wie kann ein Verrechnungsmodell für die Nutzung verarbeiteter Daten aussehen?

Verteilte Verarbeitung

Die verteilte Verarbeitung innerhalb der Plattform birgt gleich mehrere Herausforderungen. So fungiert im Falle der Plattform der Plattformbetreiber bzw. Dienstanbieter laut DSGVO ggf. als sogenannter Auftragsverarbeiter für den Datenlieferanten. Die hier definierten rechtlichen Bestimmungen müssen eingehalten werden. Wird die Plattform in der Cloud gehostet, so ist u. U. zu berücksichtigen, in welchem Land die Server des Hosters stehen und welche rechtlichen und sicherheitstechnischen Vorgaben eingehalten werden müssen. Innerhalb Deutschlands müssen zudem weitere rechtliche Bestimmungen, wie das Telekommunikationsgesetz (TKG), berücksichtigt werden.

Geschäftsmodelle und Abrechnungsmodelle

Neben den rechtlichen und sicherheitsrelevanten Aspekten spielen auch Geschäfts- und Abrechnungsmodelle eine große Rolle. Mit der Beteiligung mehrere Stakeholder (Plattformbetreiber, Datenlieferant, Diensteanbieter, An-

wendungsentwickler) im Ökosystem der Plattform müssen die geschäftsrelevanten vertraglichen Rahmenbedingungen rechtskonform umgesetzt werden.

Betrachtung der Anwendungsfälle

Im Folgenden werden die im Projekt GEISER umgesetzten Anwendungsfälle mit Blick auf die oben genannten Herausforderungen betrachtet.

Intelligente Parkplatzsuche

Die intelligente Parkplatzsuche ist ein Service, den sich Millionen Autofahrer wünschen. Derzeitige Lösungen benötigen jedoch sogenannte Infrastruktursensorik und funktionieren damit nur dort, wo solche einsetzbar und bereits verbaut ist. In GEISER soll eine unabhängige und flächendeckende Lösung entstehen. Sie soll aus Daten die Chance berechnen, (1) an einem bestimmten Ort und zu einer bestimmten Zeit einen freien bzw. (2) nach einer (kurzen) Wartezeit einen frei werdenden Parkplatz zu finden. Beides hängt davon ab, wie viele Menschen zu bestimmten Zeiten ein Gebiet aufsuchen und wozu. Lokale Datenquellen müssen dazu intelligent verknüpft und ausgewertet werden

Die Umsetzung des Anwendungsfalls der intelligenten Parkplatzsuche von TomTom basiert auf der Auswertung umfangreicher GPS-Daten. Dabei wird analysiert, wo und wann Autofahrer nach einem Parkplatz suchen. Die daraus berechneten Wahrscheinlichkeiten werden dann für die Parkplatzsuche verwendet. Die Daten zur Analyse unterstehen u. U. der DSGVO, da diese von den Kunden der TomTom kommen. Allerdings sammelt TomTom diese Daten anonymisiert. Die Anonymisierung wird im folgenden Abschnitt betrachtet.

Echtzeit-Geomarketing

Unternehmen in Einzelhandel und der Gastronomie erwirtschaften in Deutschland über 500 Mrd. Euro Umsatz pro Jahr und beschäftigen ca. vier Millionen Menschen. Erfolgreiche Unternehmen richten ihr Waren- und Serviceangebot, ihre Werbe- und Marketingstrategie, Öffnungszeiten und Aktionen an der lokalen Kundschaft aus. So steigern sie ihren Umsatz, erregen Aufmerksamkeit und erzeugen ein positives Image. Datengetriebenes Geomarketing ist heute bereits möglich. Es gibt viele digitale Informationsquellen; Websites, Online-Veranstaltungskalender, Foren, Daten aus Mobilität und Mobilfunk, (sozialen) Medien, Open Data, eigene Absatz- und Kundendaten und vieles mehr. Aber diese Quellen sind heterogen, nicht inhaltlich vernetzt und ohne expliziten Raumbezug. Die GEISER-Plattform liefert die Daten für ein Assistenzsystem für Geomarketing, welches Unternehmen in (R)Echtzeit[31] mit den nötigen Informationen zur besseren Entscheidungsfindung versorgt.

Um Bedürfnisse und Wünsche der Kunden zu berücksichtigen, müssen u. U. kundenspezifische Daten analysiert werden. Diese Verarbeitung muss dem Rechtsrahmen der DSGVO entsprechen.

Servicetechniker-Einsatzunterstützung

Der Maschinenbausektor steht in Deutschland für ca. 220 Mrd. Euro Umsatz und etwa 865.000 Beschäftigte. Neben der Produkt- ist auch die Servicequalität ein wesentliches Kaufkriterium, denn sie verhindert teure Leerlaufzeiten und Produktionsausfälle. Schon heute werden massenhaft Sensordaten aus Maschinen genutzt, um drohende Störungen und Wartungsbedarfe zu prognostizieren. Der nächste Schritt ist die Verknüpfung mit der Einsatzplanung von Serviceteams und der Ersatzteillogistik. Für eine optimale Serviceabdeckung werden jedoch viele andere Daten mit Geobezug notwendig, die mit Sensordaten verknüpft werden müssen. Die GEISER-Plattform liefert die Informationen und Daten für die Einsatzplanung von Servicetechnikern, mit denen Anfahrts- und Wartezeiten verkürzt und Serviceeinsätze qualitativ verbessert werden können.

Im Anwendungsfall der Servicetechniker-Einsatzunterstützung fallen kunden- und mitarbeiterspezifische Daten an. Diese müssen ausreichend geschützt und der Rahmen der DSGVO gewahrt sein.

Empfehlungen

Im Folgenden werden Empfehlungen zur Umsetzung von Lösungen zu einigen der oben genannten Herausforderung beschrieben.

Anonymisierung

Die DSGVO erkennt die „… Anonymisierung als Mittel für einen datenschutzschonenden Umgang [zwar] nicht unmittelbar [an], allerdings wird die Anonymisierung zumindest

31 (R)Echtzeit – gemeint ist eine schnelle Reaktionszeit auf webbasierte Anfragen und nicht sicherheitskritische Echtzeitfähigkeiten.

in Erwägungsgrund 26 angesprochen." (Smart Data – Smart Solutions, 2018).

Innerhalb des BMWi-geförderten Smart-Data-Forschungsprojekts SmartRegio (SmartRegio Abschlussveranstaltung, 2017) wurde gezeigt, wie Daten innerhalb der Data-Analytics-Plattform KatanaFlow (Katana USU, 2018) anonymisiert werden. Die umgesetzten Dienste innerhalb der Plattform basieren auf den Erkenntnissen des Statistisches Bundesamts (Höhne, 2010). Eine besondere Herausforderung ergibt sich für geodatenbasierte Datenquellen. So kann ein kleines betrachtetes Gebiet innerhalb von Ballungszentren ausreichend anonymisiert sein, während der Grad der Anonymisierung für ländliche Gegenden nicht hinreichend ist. Diesen Sachverhalt zu berücksichtigen ist beispielsweise für den Anwendungsfall „Echtzeit Geomarketing" wichtig.

Oft ist es jedoch auch notwendig, den Anonymisierungsgrad von Datenquellen zu bestimmen. Bekannte Methoden hierzu sind beispielsweise k-Anonymität, l-Diversität und t-Closeness (Kumari, Varma & Krishna, 2011). Innerhalb von SmartRegio zeigte die USU, wie diese KPIs für die Bestimmung des Anonymisierungsgrads von Datenquellen berechnet werden können. Die Methode kann beispielsweise verwendet werden, um zu verhindern, dass nicht anonymisierte Daten rechtswidrig verarbeitet werden. Dabei wird ein Dienst innerhalb der GEISER-Plattform verwendet, der den Anonymisierungsgrad ermittelt.

Werden verschiedene Datenquellen kombiniert, so kann das u. U. zu einer Deanonymisierung (Wiegert, 2003) der resultierenden Daten und Ergebnisse führen. In einer datenverarbeitenden Plattform sollte daher nicht nur vor der Verarbeitung der Ausgangsdaten, sondern auch nach der Kombination von Datenquellen die Rechtskonformität geprüft werden. Eine Fragestellung, die noch zu klären ist, ist: Welches Level müssen Daten vorweisen, um rechtskonform zu sein? Hier sind weitere Forschungsanstrengungen erforderlich.

Neben den hier genannten Anforderungen der DSGVO spielt auch die Anonymisierung von Daten aus Wettbewerbsgründen eine große Rolle. Der Grund für die Anonymisierung muss also nicht alleine aus einem Personenbezug resultieren. In Zeiten, in denen Daten ein wichtiges Gut einer Firma darstellen, wird es immer wichtiger, auch nicht personenbezogene Daten zu anonymisieren.

Sicherheit

Da Daten innerhalb der Plattform von unterschiedlichen Diensten verarbeitet werden, müssen die Übertragungswege durch sichere Protokolle geschützt werden. Das ist sowohl bei der Übertragung an die Plattform als auch innerhalb der Plattform notwendig.

Technische Lösungen, um die Übertragung in die Plattform sicher zu gewährleisten, sind mit üblichen Webtechnologien wie Hypertext Transfer Protocol Secure (HTTPS) in Verbindung mit Secure Socket Layer (SSL) und Transport Layer Security (TLS) bereits vorhanden. Zusätzliche Absicherung kann durch Clientzertifikate oder Virtual Private Network (VPN)-Verbindungen erfolgen.

Erweitere Zugriffskontroll-Mechanismen wie Multifaktor-Authentifizierung (MFA) dienen zum Schutz vor unberechtigtem Zugriff innerhalb der Plattform. Werden Daten in der Datenschicht der Plattform gespeichert, so können sensible Daten zudem verschlüsselt werden. Dazu gibt es sowohl Software- als auch Hardwarelösungen. Essenziell hierbei ist der Einsatz von offenen und bewährten Standardverschlüsselungsverfahren wie AES. Durch die Verteilung der Daten auf verschiedene Speicherknoten kann verhindert werden, dass ein einzelner Benutzer vollständigen Zugriff auf Daten erhalten kann.

Lösungsansätze für die sichere und anonymisierte Verarbeitung von Daten in verteilten Umgebungen können durch bekannte Verfahren wie Maskierung und Hashing realisiert werden. Die Software-Frameworks Apache Ranger (Apache Ranger, 2018) oder BlueTalon (BlueTalon, 2018) bieten dazu bereits passende Funktionalitäten an.

Ausblick

In den vorhergehenden Abschnitten wurden verschiedene rechtliche Herausforderungen und sicherheitsrelevante Aspekte, wie der Datenschutz, der technische Schutz durch Verschlüsselung und Zugriffkontrolle sowie die Datenhoheit insbesondere bei verteilter Verarbeitung, beim Betrieb der GEISER-Plattform und ihrer Plattformökonomie identifiziert und erste Lösungsvorschläge gegeben.

Der wissenschaftliche Fokus des Projekts GEISER lag in der Entwicklung einer Plattform als zentraler Drehscheibe für die Kommunikation der Dienste zur Datenakquise, -verarbeitung und -speicherung.

Wie im vorangegangen Abschnitt bereits angeschnitten, ist eine der noch offenen Fragen, wann Daten rechtskonform anonymisiert sind, damit sie zur Verarbeitung verwendet werden können, also welchem Level die Daten entsprechen müssen. Bisherige bekannte Aussagen von Juristen besagen, dass dies im Einzelfall zu prüfen ist. Die Frage ist jedoch, ob das in jedem Fall und durch technische Mittel durchführbar ist. Die Herausforderungen, welche sich bei der Datenhoheit ergeben, sind weitere Fragestellungen, die im Projekt bisher noch unbeantwortet bleiben. Hier können u. U. vertragliche Rahmenbedingungen zwischen Datenlieferanten und Plattformbetreibern bzw. Nutzern die Rechtslage klären.

Literaturverzeichnis

Apache Ranger. (3. Juli 2018). Von https://ranger.apache.org/ abgerufen.

BlueTalon. (3. Juli 2018). Von http://bluetalon.com/ abgerufen.

Höhne, J. (2010). Verfahren zur Anonymisierung von Einzeldaten. Band 16 der Reihe Statistik und Wissenschaft. Statistisches Bundesamt.

Katana USU. (2018). Von https://katana.usu.de/de/ abgerufen.

Kumari, V., Varma, N. & Krishna, A. (2011). Checking Anonymity Levels for Anonymized Data. ICDCIT (S. 278–289). Springer.

Ninghui, L., Tiancheng, L. & Suresh, V. (2007). t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. IEEE 23rd International Conference on Data Engineering.

(2018). Smart Data – Smart Solutions. Fachgruppe Rechtsrahmen der Smart-Data-Begleitforschung.

SmartRegio. (28. Juni 2018). Von https://www.smartregio.org/ abgerufen.

SmartRegio Abschlussveranstaltung. (07. September 2017). Von https://www.smartregio.org/workshop-von-geodaten-zu-regionalem-wissen-smartregio-laedt-ein/ abgerufen.

Wiegert, R. (2003). Matching-Verfahren und die Re-Identifikation faktisch anonymisierter Einzeldaten. In Statistisches Bundesamt, Schriftenreihe Forum der Bundesstatistik (S. 60–68).

4.5 KOMMUNAL 4.0 – Vom branchenspezifischen Sicherheitsstandard zur sicheren Plattform

Nico Suchold[32], Günter Müller-Czygan[33]

Ausgangssituation

Auf dem Weg zu einer Smart City stellt sich unter anderem die Frage, wie wasserwirtschaftliche Anwendungen (z. B. in den Bereichen Geoinformation, Betriebsführung und Simulation) in eine zukünftige übergeordnete Plattformlösung integriert werden können. Wünschenswert ist eine hohe Vernetzungsfähigkeit zwischen den Einzellösungen, etwa durch ähnliche Technologien. Dies erleichtert den Einstieg in die Digitalisierung, zumal wenn die Vernetzung mit anderen Lösungen im Smart-City-Umfeld, etwa einem Parkraum- oder Leuchtenmanagement, möglich ist. Vermehrt wird im Zusammenhang mit der Realisierung der Smart City als erster Schritt die Entwicklung einer übergeordneten Digitalisierungsstrategie empfohlen. Kleinen und mittleren Kommunen fehlen jedoch oft die Ressourcen, um eine solche zu erarbeiten. Im Rahmen des Projekts KOMMUNAL 4.0 wird u. a. ein zehn Schritte umfassendes Modell erarbeitet, das im Sinne eines agilen Prozesses angewendet werden kann. Werden schon vor der Erstellung der digitalen Strategie erste Einzelmaßnahmen identifiziert, sollten diese auch umgesetzt werden. Der Anwender kann dort anfangen, wo dringender Handlungsbedarf besteht (z. B. die Erneuerung alter Maschinen mit intelligenten Vernetzungselementen), ohne dabei die erforderliche Vernetzungskompatibilität und IT-Sicherheit von Einzelelementen zu verlieren. KOMMUNAL 4.0 verfolgte im Wesentlichen die Entwicklung einer Daten- und Serviceplattform für die kommunale Infrastruktur zur Vereinheitlichung der Datenerfassung- und -übertragung aus heterogenen CPS (cyber-physischen Systemen) mit zugehörigen Applikationen und passenden Geschäftsmodellen.

Mehr und mehr zeichnet sich ab, dass der Einstieg in die Digitalisierung mit einzelnen intelligenten technischen Komponenten, die für eine Plattformanbindung bereits vorbereitet sind, den idealen Start im Bereich kommunaler Infrastrukturen darstellt. Oftmals ist ohnehin eine technische Ausrüstung notwendig, sodass mit einem vergleichsweise geringen Zusatzaufwand ein erster praktischer Digitalisierungsschritt erfolgen kann.

Insbesondere für Betreiber kritischer Infrastrukturen im Wasser- und Abwassersektor, aber auch für Systemanbieter und Dienstleister in diesem Bereich ist die IT-Sicherheit aufgrund der immer stärkeren Vernetzung der Anlagen und Systeme von elementarer Bedeutung. Sie wurden nicht zuletzt durch die aktuelle Diskussion zum IT-Sicherheitsgesetz (ITSG) für diese Thematik sensibilisiert. Diese Sensibilisierung und bekannt gewordene Angriffe und Bedrohungsszenarien führen dazu, dass sowohl das Risikobewusstsein als auch die Akzeptanz für Investitionen in sichere Systeme und Maßnahmen zur Steigerung der IT-Sicherheit zunehmen.

Sicherheitsmanagement

Mit Einführung des branchenbezogenen IT-Sicherheitsstandards (B3S) Wasser/Abwasser, der im August 2017 vom Bundesamt für Sicherheit und Informationstechnik (BSI) anerkannt wurde, müssen Wasserversorger und Abwasserentsorger als erster Sektor der kritischen Infrastrukturen die gesetzlichen Anforderungen gemäß § 8a (21) BSI-Gesetz erfüllen. Damit sind Betreiber wasserwirtschaftlicher Anlagen und Netze bei standardkonformer Umsetzung und entsprechendem Nachweis rechtlich auf der sicheren Seite. Als wesentliche Ziele des Branchenstandards Wasser/Abwasser benennt Dr. Ludger Terhart [1] folgende Aspekte:

- Berücksichtigung aller Anlagen(typen) zur Wasserver- und Abwasserentsorgung nach BSI-KRITIS-Verordnung
- Eignung auch für nicht kritische Infrastrukturen
- unabhängig von der Ausprägung der IT-Systeme und der Anlagengröße
- Beschreibung bis auf Maßnahmenebene
- verständlich für die Betreiber (eindeutige Ableitung der zu beachtenden Grundsätze und der zu ergreifenden Maßnahmen)
- Integration in bestehende Regelwerke des Deutschen Vereins des Gas- und Wasserfaches (DVGW) und der Deutschen Vereinigung für Wasserwirtschaft, Abwasser und Abfall (DWA)
- einfach an den jeweiligen Stand der Technik und die Erkenntnisse des BSI anzupassen

Die im Projekt KOMMUNAL 4.0 entwickelte Architektur ist in die Hauptbereiche Serviceplattform und Datenplattform aufgeteilt, welche sowohl intern also auch extern Daten übertragen. Der interne Datenaustausch zwischen den

32 Institut für Automation und Kommunikation e. V.
33 HST Systemtechnik GmbH & Co. KG.

einzelnen Komponenten der Bereiche wurde im Rahmen des Projekts spezifiziert und implementiert. Im Vordergrund standen bereits während der Entwicklung umfassende Maßnahmen zur Risikobeherrschung und Gefahrenabwehr wie eine sichere industrielle Kommunikation auf Basis von OPC Unified Architecture (OPC UA), eine syntaktische und semantische Datenvalidierung und eine durchgängige Integration von Authentifizierung und Autorisierung auf Anwendungs- und Nutzerebene. Da die einzelnen Komponenten jeweils über User-Interfaces (z. B. Webapplikationen) und externe Schnittstellen mit dem Nutzer oder anderen Systemen interagieren, ist hier eine Bedrohungsquelle mit unterschiedlichen Ausprägungen zu finden. Neben den entsprechend der Risikobewertung getroffenen Maßnahmen des B3S kommen hier auch Maßnahmen zum Tragen, die speziell die Risiken von Webapplikation [2] und Cloud-Applikationen [3] adressieren. Die zweite als kritisch einzustufende Gefahrenquelle ist die Kommunikation der CPS-Komponenten (Cyber Physical System) und Feldgeräten, welche als M2M-Kommunikation (Maschine zu Maschine) bezeichnet wird. Hier sind Maßnahmen zum Schutz der CPS-Systeme von besonderer Bedeutung [4].

In Sinne des Security-by-Design-Prinzips wurden die im Rahmen der Anforderungsanalyse und Grobkonzeption gewonnen Informationen zur Informationssicherheit der einzelnen Plattformbereiche für die Evaluierung der Plattformtechnologien und Definition von Anwendungstools von Beginn an berücksichtigt. Darauf aufbauend wird, wie im B3S als auch in der ISO 27001 gefordert, das Erstellen eines umfassenden Informationssicherheitskonzepts vorangetrieben. Dieses Konzept berücksichtigt die Gesamtheit aller vorhandenen Prozesse, deren unterstützende Werte (IT-Systeme, Mitarbeiter, Dienstleister etc.) sowie deren Dokumentation.

Teil dieses Konzeptes ist ein Informationssicherheitsmanagementsystem (ISMS), welches auf Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung der Informationssicherheit abdeckt. Das Managementsystem umfasst dabei Strukturen, Richtlinien, Planungsaktivitäten, Verantwortlichkeiten, Praktiken, Verfahren, Prozesse und Ressourcen einer Organisation. Die Einführung eines ISMS nach ISO 27001 wird im Branchenstandard zwar empfohlen, ist jedoch nicht verpflichtend.

Der IT-Sicherheitsleitfaden, der neben dem Merkblatt ein Hauptbestandteil des B3S ist, basiert vollständig auf dem BSI-Grundschutz [5]. Dabei wurde jedoch eine branchenspezifische Vorauswahl von relevanten Gefährdungen sowie der entsprechenden Maßnahmen von Experten aus den Bereichen Trinkwasserversorgung und Abwasserentsorgung vorgenommen und somit die Anwendung des BSI-Grundschutz und das Risikomanagement wesentlich vereinfacht. Diese Vereinfachung stellt jedoch keine Einschränkung dar, da der Leitfaden als Best Practices für den Sektor Wasser/Abwasser angesehen werden soll. Betreiber haben jederzeit die Möglichkeit, für den spezifischen Anwendungsbereich z. B. ergänzende Maßnahmen aus dem BSI-Grundschutz anzuwenden oder begründet besser geeignete Maßnahmen umzusetzen.

Die in der ISO-Norm 27001 beschriebenen allgemeinen Anforderungen werden im BSI-Grundschutz in den Gefährdungs- und Maßnahmenkatalogen ganz konkret ausgeprägt und stellen somit eine Implementierung der Norm dar. Hierbei setzt der IT-Sicherheitsleitfaden vollständig auf den BSI-Grundschutz und setzt ausnahmslos auf die Zuordnungsketten (Bausteine, Gefährdungen, Maßnahmen), die in den Kreuzreferenztabellen [6] des BSI-Grundschutzes enthalten sind. Neben den Kreuzreferenztabellen wird ebenso die Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz [7] und die Verlinkung zu aktuellen Fassungen der Grundschutzkataloge auf den Internetseiten des BSI unterstützt, somit eine bidirektionale Verbindung zu den ISO-Normen ermöglicht und sichergestellt, dass der IT-Sicherheitsleitfaden konsistent und aktuell mit dem BSI-Grundschutz sowie mit der ISO-Norm bleibt.

Für die einzelnen Schritte auf dem Weg zu einer rechtskonformen IT-Sicherheitsstruktur stellte ein IT-gestütztes ISMS einen wichtigen Baustein dar. In die Kommunal-4.0-Plattform wurde ein entsprechendes Tool von einem der Projektpartner integriert (KANiO-ISMS von HST). Mit der Toolnutzung werden unkoordinierte Einzelmaßnahmen vermieden, die keinen ausreichend sicheren IT-Betrieb gewährleisten. Zudem ermöglicht das Tool, die eigenen Bemühungen um einen sicheren IT-Betrieb gegenüber Kunden oder dem Gesetzgeber nachzuweisen. Frühere Maßnahmen lassen sich so auch besser mit dem aktuellen Sicherheitsstandard abgleichen.

Plattformsicherheit

Die Sicherheit der Kommunal-4.0-Plattform ist durch die zugrunde liegende Technologie und die Charakteristik der Hybridität (Private Cloud, Public Cloud, On Premise) geprägt. Die Kernaufgabe der Plattform ist es, bestehende wasserwirtschaftliche Anwendungen zu integrieren, eine CPS-Anbindung zu realisieren, neue Komponenten als smarte Dienste zu entwickeln und auf wasserwirtschaftliche Daten optimierte Datenservices (z. B. Speicherung, Analyse) auszuführen. Auf Basis dieser Anforderungen wurden entsprechende Technologiecluster gebildet und eine Vorauswahl von Technologieanbietern, die zum einen alle Cluster technologisch bedienen und zum anderen im kommunalen Sektor bereits als Technologielieferant anerkannt sind, aus funktionaler als auch nicht funktionaler Sicht vorgenommen. Beispielhaft in Tabelle 1 die analysierten Technologien der drei größten Cloudanbieter im Testfeld.

	Azure	Amazon Web Services	IBM Bluemix
Hybridintegration	API Management, Logik-APS	API Gateway, Storage Gateway	API Connect, Secure Gateway
CPS-Anbindung	IoT Hub, Machine Learning, Stream Analytics	AWS IoT, Machine Learning, Kinesis	Internet of Things Platform, Watson
Microservices	Containerdienste, Service Fabric , Functions	EC2 Container Service, Elastic Beanstalk, Lambda	Cloud Foundry
Dataservices	SQL Datenbank, DocumentDB, Data Factory	RDS, DynamoDB, Data Pipeline	Compose, Data Connect
Identity and Access Management und Datensicherheit	Active Directory, Security Center, Multi-Factor Authentication	IAM, Web Application Firewall, Shield, Cognito	Adaptive Security Manager, Application Security on Cloud

Tabelle1:Technologiecluster

Im Bereich Hybridintegration steht die Integration existierender Anwendungen und Dienste in die Plattform im Vordergrund. Im Bereich der CPS-Anbindung geht es vor allen Dingen um die Anbindung von Automatisierungstechnik und Feldgeräten der nächsten Generation. Der Bereich Microservices soll die Basis für eine portable und automatisierte Bereitstellung von Diensten gewährleisten und der Bereich Dataservices organisiert das Datenmanagement. Als übergreifender Bereich wird der Bereich Identity and Access Management (IAM) und Datensicherheit betrachtet, bei dem es um Funktionalitäten der Authentifizierung, Autorisierung und Identitätsmanagement geht.

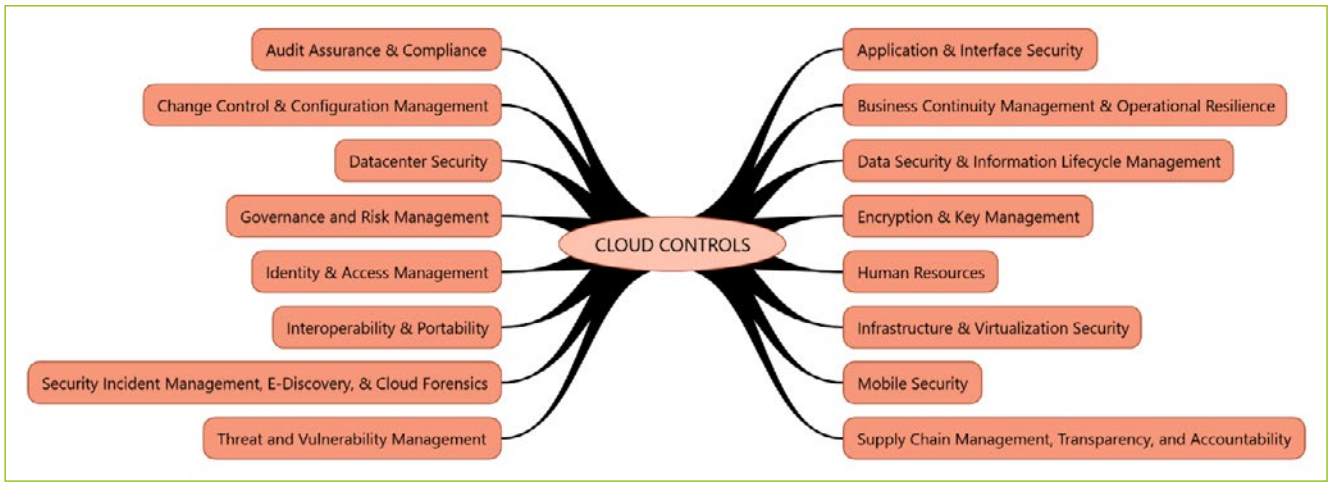

Abbildung 10: CSA Cloud Controls

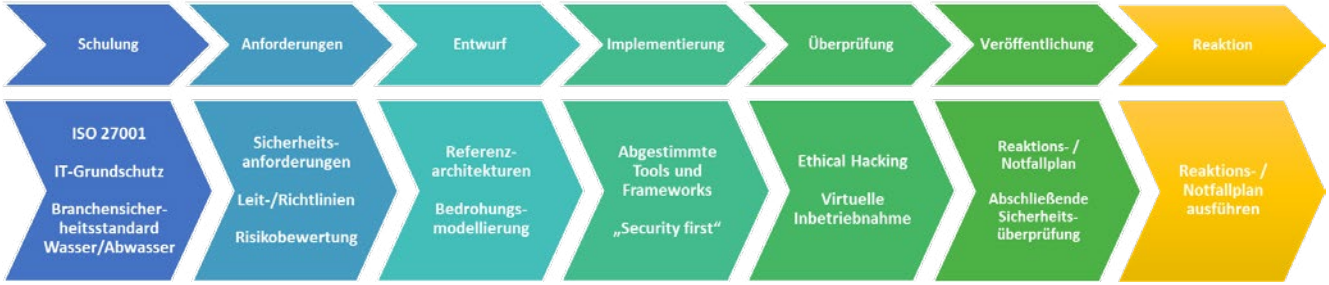

Abbildung 11: KOMMUNAL-4.0-Themen im Microsoft Security Development Lifecycle

Parallel dazu wurden verschiedene Anbieter hinsichtlich ihrer Sicherheitsarchitekturen und -maßnahmen untersucht. Relevante Sicherheitsanforderungen wurden dabei vor allen Dingen anhand existierender Standards, Normen und Regelungen identifiziert. Neben dem Anforderungskatalog Cloud Computing des BSI (C5) [8] wurden hier auch die Cloud Controls Matrix (CCM) [9] der Cloud Security Alliance (CSA) berücksichtigt.

Die darin enthaltenen Informationen der Anbieter bilden das Bindeglied zum ISMS (Datenkategorisierung, Risikomanagement) des branchenspezifischen Sicherheitsstandards und definieren somit indirekt einen Teil des branchenspezifischen Mindeststandards in Anlehnung an die Forderungen des BSI zur Nutzung externer Clouddienste [10]. Das darauf aufbauende Plattformsicherheitskonzept, welches die existierenden Maßnahmen des Technologieunterbaus ergänzt, basiert damit ebenfalls auf etablierte Standards wie der ISO 27001 und dem C5. Damit können erhebliche Synergieeffekte beim Aufbau der Plattformsicherheit genutzt werden.

Auswirkungen auf die Architektur

Die Technologieanbieter schlagen verschiedene Vorgehensmodelle und Referenzarchitekturen vor, an die sich beim Aufbau einer sicheren Plattform gehalten werden kann und werden sollte. Für die KOMMUNAL-4.0-Plattform fiel die Entscheidung auf den Technologieanbieter Microsoft. Ausschlaggebend dafür waren zum einen die bereits vorhandene Erfahrung bei den Projektpartnern bezüglich der Entwicklung auf dieser technologischen Basis, zum anderen die Untersuchungen zum Thema Plattformsicherheit, bei denen sich Microsoft insbesondere durch Transparenz und bei der Etablierung von Standards auszeichnete. Daher werden im Folgenden vorrangig die entsprechenden Referenzarchitekturen- und Vorgehensmodelle zur Beschreibung der Auswirkungen auf die Designentscheidung der Plattformarchitektur genutzt.

Die Microsoft Cybersecurity Reference Architecture [11] beschreibt die Cybersicherheitsfunktionen von Microsoft und deren Integration in bestehende Sicherheitsarchitekturen und -funktionen. Angefangen vom On-Premise-Datencenter über die entsprechenden Clients, die Azure-Dienste bis zur CPS/IoT-Anbindung enthält die Architektur alle Aspekte der hybriden Plattformsicherheit und wurde als Basissicherheitsarchitektur für die KOMMUNAL 4.0-Plattform identifiziert. Beim Entwurf dieser Architektur wurden zunächst potenzielle Bedrohungen analysiert und entsprechende Abwehrmaßnahmen definiert. Mit dem Ziel der Bedrohungsmodellierung, die beschreibt, wie ein Angreifer ein System kompromittieren kann, wurde zunächst ein Referenzmodell der Plattform im Sinne einer Grobarchitektur erstellt, um ein Verständnis des gesamten Systems zu bekommen. Dieses Modell wurde von den einzelnen Projektpartnern aufgegriffen und entsprechend ihren Verantwortlichkeiten im Kontext der Daten- bzw. Serviceplattform verfeinert.

Zusammen mit einer Liste der potenziellen Bedrohungen folgte nun das Aufbauen des Bedrohungsmodells. Dabei standen insbesondere Prozesse (z. B. Webdienste, Windowsdienste, Daemons), Datenspeicher, der Datenfluss und externe Elemente, die mit dem System interagieren, im Fokus. Die verschiedenen Elemente unterliegen bestimmten Bedrohungen. Für die Zuordnung wurde der STRIDE-Code [12] genutzt. Zum Abschluss der Modellierung werden verschiedene Zonen und Vertrauensgrenzen für die Architektur eingeführt und der Datenfluss zwischen den Komponenten skizziert. Jede Zone definiert dabei eigene Anforderungen an Daten und Zugriff und begrenzt somit die Auswirkungen von Schäden von niedrigen Vertrauenszonen auf höher gelegene Vertrauenszonen.

Das Security-by-Design-Prinzip wurde im Rahmen des Projekts nicht nur beim Entwurf der Plattformarchitektur berücksichtigt. Die beschriebene Bedrohungsmodellierung ist ebenfalls Bestandteil des im Projekt adaptierten Microsoft Security Development Lifecycle (SDL) [13]. Der SDL ist ein Prozess zur Sicherstellung der Sicherheit mit Schwerpunkt auf der Softwareentwicklung, dessen Anwendung im Projekt erprobt wird und auf die Entwicklungsmethodik für intelligente Datendienste adaptiert werden sollte. Hierbei wurden die einzelnen SDL-Methoden (Abbildung 11) der einzelnen Phasen getestet, bewertet und teilweise adaptiert.

Ausblick

Neben der Klärung vergaberechtlicher Aspekte sind sowohl der branchenspezifische Sicherheitsstandard Wasser/Abwasser als auch der im Cloud-Computing-Umfeld diskutierte Anforderungskatalog des BSI (C5) für die Sicherheit der KOMMUNAL-4.0-Plattform von elementarer Bedeutung. Der im Projekt initiierte Sicherheitsprozess verfolgt einen hybriden Ansatz und somit der Empfehlung des BSI entsprechend sicherheitskonforme Cloud-Dienste im kommunalen/behördlichen Umfeld entwickeln. In diesem Kontext wurde auch die Bedrohungsmodellierung und der Microsoft SDL weiter im Projekt erprobt und die dabei gemachten Erfahrungen sind in verschiedene Plattformspezifikationen, z. B. als Referenz für die Integration externer Dienste durch Drittparteien, eingeflossen. Die Bündelung der Dienste und Daten auf einer Plattform für Betreiber kritischer Infrastrukturen stellt eine besondere Herausforderung dar. Das Risikomanagement zur Einhaltung der Anforderungen aus dem BSI-Gesetz bleibt weiter Aufgabe des Betreibers der Infrastruktur. Er muss den Plattformbetreiber durch eine entsprechende Vertragsgestaltung und ein angemessenes Monitoring überwachen. An dieser Stelle sind die Zertifikate und Testate der erwähnten Standards das Mittel der Wahl und bieten ein gutes Fundament für ein entsprechendes Risikomanagement [14]. Auch wenn in der kommunalen Infrastruktur auf den ersten Blick keine oder nur wenige personenbezogene Daten für Big-Data-Anwendungen infrage kommen, muss dieser Aspekt auch in Zukunft weiterhin beachtet werden. Gerade bei der Zunahme von IT-Anwendungen im Bereich der softwareunterstützten Betriebsführung können die Grenzen zwischen Datenlokalisierung technischer Einrichtungen und dort tätiger Personen vermischt werden. Entsprechend ist dies bei zukünftigen Entwicklungen zu berücksichtigen.

Literaturverzeichnis

[1] Dr. Ludger Terhart: „B3S Wasser/Abwasser – Wer später anfängt, ist früher fertig“, 10 Jahre UP KRITIS, Quelle: http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/170619_Dr_Ludger_Terhart.pdf?__blob=publicationFile.

[2] OWASP Top Ten: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

[3] Sichere Nutzung von Cloud-Diensten: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf?__blob=publicationFile&v=11.

[4] ICS-Kompendium: https://www.bsi.bund.de/DE/Themen/weitereThemen/ICS-Security/Empfehlungen/Empfehlungen_node.html.

[5] BSI-Grundschutz: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html.

[6] ISO 27001 Kreuzreferenztabelle https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Check/kreuzreferenz_tabellen_zip.zip.

[7] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.pdf.

[8] Anforderungskatalog Cloud Computing (C5): https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html.

[9] Introduction to the Cloud Controls Matrix Working Group: https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview.

[10] Mindeststandard des BSI zur Nutzung externer Cloud-Dienste: https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/Nutzung_externer_Cloud-Dienste/Nutzung_externer_Cloud-Dienste_node.html.

[11] Microsoft Cybersecurity Reference Architecture: https://gallery.technet.microsoft.com/Cybersecurity-Reference-883fb54c.

[12] Threat Modeling Again, STRIDE: https://blogs.msdn.microsoft.com/larryosterman/2007/09/04/threat-modeling-again-stride/

[13] Simplified Implementation of the Microsoft SDL: The core concepts and activities of the Microsoft SDL recommended for any development organization. http://download.microsoft.com/download/F/7/D/F7D6B14F-0149-4FE8-A00F-0B9858404D85/Simplified%20Implementation%20of%20the%20SDL.doc

[14] Michael Adelmeyer, Christopher Petrick, Frank Teuteberg: IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen, HMD Best Paper Award 2017.